Παραδοτέο

Π3.3.1 Σχέδιο εγκατάστασης 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

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Πίνακας Περιεχομένων

1 Το Σχέδιο εγκατάστασης της πλατφόρμας

Στόχος του σχεδίου εγκατάστασης της πλατφόρμας των Ηλεκτρονικών Συγγραμμάτων είναι η δημιουργία ενός συστήματος εξυπηρετητών και δικτυακών συσκευών με το απαραίτητο λογισμικό υποδομής, που θα μπορεί να εξυπηρετεί τις διαδικτυακές εφαρμογές της πλατφόρμας των Ηλεκτρονικών Συγγραμμάτων προσφέροντάς τα εξής χαρακτηριστικά:

- Υψηλές επιδόσεις
- Υψηλή διαθεσιμότητα

Για να είναι εφικτή η υψηλή αποδοτικότητα του συστήματος, ο σχεδιασμός του έγινε με γνώμονα την όσο τη δυνατόν μεγαλύτερη επεκτασιμότητα (scalability) του συστήματος. Παράλληλα, ο σχεδιασμός φρόντισε για την υψηλή διαθεσιμότητα του συστήματος ώστε να μην υπάρχουν μοναδικά σημεία αστοχίας (Single Points of Failure).

Με το παρών Σχέδιο Εγκατάστασης εξασφαλίζονται οι παρακάτω απαιτήσεις:

- Απρόσκοπτη και αδιάλειπτη λειτουργία της πλατφόρμας Ηλεκτρονικών Συγγραμμάτων, με εξασφάλιση των απαραίτητων χαρακτηριστικών:
  - Αξιοπιστίας (reliability)
  - Επίδοσης (performance)
  - Ασφάλειας (security)
- Λήψη και τήρηση (με ασφαλή και αδιάβλητο τρόπο) εφεδρικών αντιγράφων των δεδομένων που καταχωρούν οι χρήστες στην πλατφόρμα:
  - Δεδομένα που τηρούνται στη Βάση Δεδομένων της εγκατάστασης.
  - Ψηφιακά έγγραφα (βιογραφικά, ψηφιακά συγγράμματα, πολυμεσικό υλικό, κλπ) που τηρούνται στο σύστημα αρχείων της εγκατάστασης
- Ανάκαμψη της πλατφόρμας από καταστροφή της κύριας εγκατάστασης, με την άμεση μεταφορά και λειτουργία των εφαρμογών σε εναλλακτική εγκατάσταση, χωρίς την απώλεια δεδομένων.
- Εξασφάλιση συνεχούς παρακολούθησης της καλής λειτουργίας της εγκατάστασης (των διακομιστών, των δικτυακών συσκευών, του λογισμικού υποδομής, κλπ) με τη χρήση ειδικού λογισμικού παρακολούθησης των εγκαταστάσεων και την ανάπτυξη εξειδικευμένων διαχειριστικών εφαρμογών.

- Εξασφάλιση γρήγορης και ασφαλούς ενημέρωσης των εφαρμογών της πλατφόρμας από την ομάδα ανάπτυξης, με την ανάπτυξη και εγκατάσταση εξειδικευμένων εφαρμογών ενημέρωσης των εφαρμογών και ελέγχων της καλής λειτουργίας τους. Δεδομένου ότι η ομάδα ανάπτυξης πολλές φορές καλείται να ενημερώσει τις εφαρμογές της πλατφόρμας με νέα λειτουργικότητα πολλές φορές την ημέρα, η εξασφάλιση γρήγορης, αξιόπιστης και ασφαλούς διαδικασίας ενημέρωση των εφαρμογών είναι εξαιρετικής σημασίας.

2 Σχεδιασμός

Η λειτουργία του συνόλου ενός πληροφοριακού συστήματος μπορεί να διαχωριστεί στους εξής βασικούς επιμέρους τομείς:

- Σύστημα Βάσεων Δεδομένων
- File Server
- Application Server
- Firewall
- Web Publishing
- Deployment
- Monitor
- Backup
- Δοκιμαστικό Περιβάλλον

2.1 Σύστημα Βάσεων Δεδομένων

Ως Σύστημα Βάσεων Δεδομένων επιλέχθηκε ο Microsoft SQL Server 2012, καθώς χαρακτηρίζεται από μεγάλη λειτουργικότητα, ειδικά σε συνδυασμό με ανάπτυξη εφαρμογών σε περιβάλλον .Net, αλλά παράλληλα προσφέρει έντονη σταθερότητα, αξιοπιστία αλλά και ασφάλεια. Για να ικανοποιηθεί η απαίτηση της υψηλής διαθεσιμότητας του συστήματος αποφασίστηκε να στηθούν δύο SQL Servers οι οποίοι λειτουργούν συνεργατικά μεταξύ τους αξιοποιώντας την τεχνολογία “SQL Server AlwaysOn Availability Groups”. Τα Always On Availability Groups δίνουν τη δυνατότητα όταν γίνονται αλλαγές σε μία βάση δεδομένων που βρίσκεται στον έναν server, αυτές οι αλλαγές να μεταφέρονται και να εφαρμόζονται αυτόματα και στον δεύτερο. Επιπλέον διασφαλίζεται πως είτε και οι δύο servers θα αποθηκεύσουν τις αλλαγές είτε κανένας. Τέλος σε περίπτωση που ο πρωτεύον server εμφανίσει δυσλειτουργία, ο δευτερεύον αναλαμβάνει αυτόματα τον ρόλο του πρωτεύονται. Όταν ο πρώην πρωτεύον server επανέλθει σε λειτουργία, αναγνωρίζει πως κάποιος άλλος έχει αναλάβει τον πρωτεύοντα ρόλο και ο ίδιος παίρνει θέση δευτερεύοντα εξυπηρετητή.

2.2 File Server

Οι εφαρμογές που τρέχουν στο σύστημα των εξυπηρετητών έχουν ανάγκη πρόσβασης σε σύστημα αρχείων είτε για τη διάθεση αρχείων απαραίτητα για τη δικιά τους λειτουργία είτε για να αποθηκεύουν αρχεία που ανεβάζουν οι χρήστες στην εφαρμογή. Και στις δυο περιπτώσεις το σύστημα αρχείων που χρησιμοποιείται από τις εφαρμογές πρέπει να παρουσιάζει τα απαιτούμενα χαρακτηριστικά υψηλής διαθεσιμότητας. Καθώς τα

συστήματα που προσφέρουν χώρο αποθήκευσης κοινό για πολλούς εξυπηρετητές (Clustered File Systems) απαιτούν εξειδικευμένο hardware το οποίο δεν ήταν διαθέσιμο στην υποδομή (ViMa), επιλέχθηκε η λύση της τεχνολογίας Distributed File System Replication (DFSR) της Microsoft. Το DFSR, δεδομένων φάκελων που βρίσκονται σε filesystems σε δύο ή περισσότερους διαφορετικούς εξυπηρετητές και είναι προσβάσιμοι μέσω του πρωτοκόλλου Server Message Block (SMB), προσφέρει τις εξής δυνατότητες:

1. Πρόσβαση των φακέλων αυτών μέσω ενός κοινού μονοπατιού και για τους δύο, επιτρέποντας έτσι σε όσους εξυπηρετητές τους χρησιμοποιούν να μπορούν να χρησιμοποιούν όποιον από τους συμμετέχοντες στο DFSR εξυπηρετητές είναι διαθέσιμος.
2. Άμεσος και αυτόματος συγχρονισμός των φακέλων με τέτοιο τρόπο ώστε όποια αλλαγή γίνεται σε κάποιον εξυπηρετητή να γίνονται άμεσα replicate στους υπόλοιπους.

2.3 Application Server

Ως application server επιλέχθηκε ο Microsoft Internet Information Server 7.5. Για την επίτευξη των επιθυμητών χαρακτηριστικών διαθεσιμότητας και απόδοσης επιλέχθηκε να εγκατασταθούν 2 application servers σε 2 διαφορετικούς εξυπηρετητές. Οι application servers έχουν ρυθμιστεί τόσο να διαβάζουν το configuration τους και τα αρχεία των εφαρμογών όσο και να γράφουν τα αρχεία των χρηστών στο από το DFSR υποστηριζόμενο filesystem που αναφέρεται στην προηγούμενη παράγραφο. Με τον τρόπο αυτό διασφαλίζεται πως οι δύο servers έχουν πάντα κοινό configuration και πρόσβαση σε κοινά αρχεία, συνεπώς ακόμα και αν ο ένας από τους δύο σταματήσει να λειτουργεί ο άλλος μπορεί αν συνεχίσει απρόσκοπτα την εργασία του πρώτου.

2.4 Firewall

Στο σύστημα των εξυπηρετητών έχουν εγκατασταθεί ένα σύνολο από υπηρεσίες είτε κομβικές για τη λειτουργία του συστήματος (π.χ. Σύστημα Βάσεων Δεδομένων) είτε υποστηρικτικές προς άλλες υπηρεσίες (π.χ. DFSR). Από αυτές οι περισσότερες είναι γενικά προσβάσιμες μέσω δικτύου, όμως ελάχιστες είναι επιθυμητό να είναι προσβάσιμες από το όλο το διαδίκτυο. Για το λόγο αυτό επιλέχθηκε να ρυθμιστεί firewall μπροστά από τους εξυπηρετητές το οποίο να επιτρέπει μόνο ακριβώς την δικτυακή κίνηση που είναι επιθυμητή και να αποκόπτει όλη την υπόλοιπη. Για το ρόλο αυτό επιλέχθηκε η χρήση του συστήματος iptables του linux kernel.

Επιπλέον σε κάθε έναν εξυπηρετητή ρυθμίζεται επιπλέον το firewall του λειτουργικού συστήματος ως έναν δεύτερο επίπεδο προστασίας στο εσωτερικό δίκτυο.

2.5 Web Publishing

Για λόγους ασφαλείας αλλά και διασφάλισης της υψηλής διαθεσιμότητας των Application servers επιλέχθηκε να μην είναι άμεσα προσβάσιμοι από το διαδίκτυο. Αντιθέτως στήθηκε το λογισμικό haproxy το οποίο και έχει αναλάβει 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.

2.6 Υψηλή διαθεσιμότητα firewall και web publishing

Για την υψηλή διαθεσιμότητα των συστημάτων αυτών έχουν στηθεί 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 pacemaker του Linux High Availability project. Ο pacemaker 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. Αν το τρέχον σύστημα αποτύχει, τότε οι IPs μεταπίπτουν αυτόματα στο άλλο σύστημα μέσω του pacemaker, όπου αναλαμβάνουν λειτουργία τα iptables και haproxy που τρέχουν ήδη εκεί. Στο cluster συμμετέχει και τρίτος εξυπηρετητής μόνο όμως ως witness. Ο witness δεν προσφέρει ποτέ τις υπηρεσίες του cluster, χρησιμοποιείται όμως για την απόκτηση quorum από τους δύο βασικούς εξυπηρετητές.

2.7 Domain Controllers

Η χρήση Active Directory Services (Domain controllers) είναι προαπαιτούμενη τόσο για τα SQL Server Always On Availability Groups όσο και για το Distributed File System Replication. Πέρα όμως από την συστημική απαίτηση για ύπαρξή τους, η παρουσία τους θεωρήθηκε κρίσιμη για την καλή λειτουργία συνολικά του συστήματος. Προσφέρουν αυξημένες δυνατότητες κεντρικής διαχείρισης και αυτοματοποίησης πολλών διαδικασιών, ενώ παράλληλα χαρακτηριστικά όπως κεντρική διαχείριση των accounts που χρησιμοποιούν οι εφαρμογές ή η χρήση Group Policies για την αυτόματη, κοινή και επιβεβλημένη ρύθμιση των εξυπηρετητών αυξάνουν πρακτικά την ασφάλεια του συστήματος.

2.8 Deployment

Η διαδικασία ενημέρωσης των web εφαρμογών είναι ιδιαίτερα σημαντική τόσο για τη διαρκή σωστή λειτουργία τους όσο και από την άποψη της συνολικότερης ασφάλειας του συστήματος. Δημιουργήθηκε λοιπόν ειδική δικτυακή εφαρμογή η οποία είναι υπεύθυνη για το deployment των αλλαγών στις εφαρμογές. Η εφαρμογή αυτή φροντίζει:

- Να επιτρέπει μόνο τους εξουσιοδοτημένους χρήστες να κάνουν ενημερώσεις.
- Να υπάρχει αντίγραφο ασφαλείας πριν από κάθε αλλαγή ώστε να είναι άμεσα εφικτή η επιστροφή σε προηγούμενες εκδόσεις σε περίπτωση δυσλειτουργίας.
- Να διαφυλάττει την καλή λειτουργία της εφαρμογής κατά τη διάρκεια των ενημερώσεων.
- Να κάνει τις απαραίτητες ενέργειες για να ενημερωθούν όλοι οι web servers με τα νέα αρχεία.

- Να κάνει όσες ρυθμίσεις είναι απαραίτητες (π.χ. δικαιώματα πρόσβασης στο file system) ώστε οι αλλαγές να λειτουργούν σωστά.
- Να μην επιτρέπει ή να προειδοποιεί τους χρήστες για αλλαγές στις εφαρμογές που ξεφεύγουν από τα πλαίσια της απλής συντήρησης (π.χ. αλλαγές στις ρυθμίσεις πρόσβασης στη βάση δεδομένων).
- Να προσφέρει στους developers οι οποίοι δεν έχουν δικαιώματα διαχείρισης του συστήματος ορισμένες λειτουργίες που απαιτούν τέτοια δικαιώματα (π.χ. recycling των application pools).

Η παραπάνω εφαρμογή είναι εγκατεστημένη σε διαφορετικό σύστημα από τις υπόλοιπες εφαρμογές. Στο ίδιο σύστημα εγκαθίστανται και οποιαδήποτε εργαλεία απαιτούνται για τη διαχείριση του συστήματος συνολικά.

2.9 Monitor

Κομβικό σημείο της διαρκούς και σωστής λειτουργίας του συστήματος είναι η συνεχής παρακολούθησή του και η έγκαιρη ενημέρωση των διαχειριστών για τυχόν προβλήματα ή ενδείξεις επερχόμενων δυσλειτουργιών (π.χ. η σχεδόν πλήρωση ενός χώρου αποθήκευσης). Ως monitoring εργαλείο επιλέχθηκε το Nagios το οποίο χρησιμοποιεί το πρωτόκολλο SNMP για να λαμβάνει πληροφορίες για την κατάσταση των υποσυστημάτων.

2.10 Δοκιμαστικό Περιβάλλον

Κατά την ανάπτυξη των εφαρμογών είναι απαραίτητη η ύπαρξη μίας πλατφόρμας δοκιμών. Η πλατφόρμα αυτή θα πρέπει να έχει παρόμοια χαρακτηριστικά με το παραγωγικό περιβάλλον ώστε να εξασφαλίζεται η συμβατότητα μεταξύ τους. Στην προκειμένη περίπτωση τα χαρακτηριστικά αυτά είναι λειτουργικό σύστημα Windows Server 2008 R2, web server IIS 7.5 και Σύστημα Διαχείρισης Βάσεων Δεδομένων SQL Server 2012. Στο δοκιμαστικό περιβάλλον δεν αποθηκεύονται σε καμία περίπτωση παραγωγικά δεδομένα.

2.11 Backup

Η διαθεσιμότητα των εφαρμογών και των δεδομένων τους ακόμα και σε περίπτωση φυσικής καταστροφής του παραγωγικού περιβάλλοντος διασφαλίζεται από την ύπαρξη αυτοματοποιημένης διαδικασίας δημιουργίας αντιγράφων ασφαλείας και την αντιγραφή τους σε σύστημα που βρίσκεται σε διαφορετικό φυσικό χώρο. Τα αντίγραφα ασφαλείας περιλαμβάνουν:

- Τα εκτελέσιμα αρχεία των εφαρμογών και οποιαδήποτε άλλα αρχεία απαιτούνται για τη λειτουργία τους.
- Τα αρχεία δεδομένων που χρησιμοποιούνται από τις εφαρμογές.
- Τις Βάσεις Δεδομένων των εφαρμογών.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

3 Δικτυακός Σχεδιασμός

Για λόγους ασφάλειας επιλέχθηκε η δημιουργία 3 ξεχωριστών δικτύων.

1. Public network: 83.212.4.96/27. Στο δίκτυο αυτό βρίσκονται μόνο οι εξυπηρετητές που χειρίζονται το firewall και το web publishing. Αυτοί λειτουργούν και routers δρομολογώντας μόνο την απαραίτητη κίνηση προς τους υπόλοιπους εξυπηρετητές και απορρίπτοντας την υπόλοιπη.

2. Internal Network. Είναι το δίκτυο που φιλοξενεί όλους τους εξυπηρετητές που περιέχουν δεδομένα και θεωρούνται πιο κρίσιμοι από την άποψη της ασφάλειας. Καμία υπηρεσία που βρίσκεται στους εξυπηρετητές αυτούς δε θα πρέπει να είναι απευθείας προσβάσιμη από το διαδίκτυο, κάτι που σημαίνει πως για να αποκτήσει πρόσβαση στο δίκτυο αυτό ένας επιτιθέμενος θα πρέπει πρώτα να προσβάλει κάποιο από τα υπόλοιπα μηχανήματα εκτός του δικτύου.

3. DMZ Network. Είναι το δίκτυο που βρίσκονται οι application servers. Οι υπηρεσίες στους εξυπηρετητές του DMZ δικτύου είναι δυνατόν να είναι προσβάσιμες από το διαδίκτυο για αυτό και θεωρείται το πιο ευπαθές δίκτυο.

4 Υλοποίηση

4.1 Εξυπηρετητές

Για την υλοποίηση του σχεδιασμού που περιγράφηκε νωρίτερα χρησιμοποιήθηκαν οι εξής εξυπηρετητές:

Όνομα	Ρόλοι	Λειτουργικό Σύστημα	Υπηρεσίες
FW01	Firewall	Debian Linux 7	Iptables,haproxy,routeing
FW02	Firewall	Debian Linux 7	Iptables,haproxy,routeing
DC01	Domain Controller	Windows Server 2008 R2 Enterprise	Active Directory Services, File Server, DFS, DFSR
DC02	Domain Controller	Windows Server 2008 R2 Enterprise	Active Directory Services, File Server, DFS, DFSR
DB01	Database Server	Windows Server 2008 R2 Enterprise	SQL Server 2012 Enterprise
DB02	Database Server	Windows Server 2008 R2 Enterprise	SQL Server 2012 Enterprise
WEB01	Application Server	Windows Server 2008 R2 Enterprise	IIS 7.5
WEB02	Application Server	Windows Server 2008 R2 Enterprise	IIS 7.5
DEV	Deployment	Windows Server 2008 R2 Enterprise	IIS 7.5, SQL Server Management Studio
MONITOR	Monitor	Debian Linux 7	Nagios
DEMO	Δοκιμαστικό Περιβάλλον	Windows Server 2008 R2 Enterprise	IIS 7.5, SQL Server 2012 Enterprise
OFFSITE	Backup	Debian Linux 7	

4.2 Χαρακτηριστικά Εξυπηρετητών

Name	CPU	RAM(GB)	Disk1	Size(GB)	Disk2	Size(GB)
DC01	2	2	C,D	50	E	100
DC02	2	2	C,D	50	E	100
DB01	8	8	C,D	150		
DB02	8	8	C,D	150		
WEB01	4	4	C,D	60		
WEB02	4	4	C,D	60		
FW01	6	6	/	50		
FW02	4	4	/	50		
DEV	1	2	C,D	100	L	500
MONITOR	2	2	/	100		
DEMO	4	4	C,D	100		
OFFISITE	1	1	/	500		

4.3 Δικτυακές ρυθμίσεις εξυπηρετητών

Name	VLAN567:Internet			VLAN571:Intranet			VLAN568:DMZ		
	Name	Mac Address	IP	Name	Mac Address	IP	Name	Mac Address	IP
FW01	eth0	de:db:ee:4d:04:32	83.212.4.125	eth1	de:db:ee:7e:c5:ce	10.0.10.11, 10.0.10.10	eth2	de:db:ee:72:80:93	10.0.100.11, 10.0.100.10
FW02	eth0	de:db:ee:39:f0:4f	83.212.4.126	eth1	de:db:ee:b6:c2:9e	10.0.10.12, 10.0.10.10	eth2	de:db:ee:f0:f0:c1	10.0.100.12, 10.0.100.10
DC01	External	de:db:ee:51:0c:c2	-	Internal	de:db:ee:08:3c:8d	10.0.10.21			
DC02	External	de:db:ee:d9:c7:aa	-	Internal	de:db:ee:a0:a4:bc	10.0.10.22			
DB01	External	de:db:ee:37:f2:c8	-	Internal	de:db:ee:d2:52:96	10.0.10.31, 10.0.10.100, 10.0.10.101			
DB02	External	de:db:ee:ef:3f:a8	-	Internal	de:db:ee:84:79:16	10.0.10.32 ,10.0.10.100 ,10.0.10.101			
DEV	External	de:db:ee:98:ca:1b	-	Internal	de:db:ee:ba:b7:44	10.0.10.70			
WEB01	External	de:db:ee:04:85:e6	-				DMZ	de:db:ee:a0:d6:95	10.0.100.101
WEB02	External	de:db:ee:b8:4a:e0	-				DMZ	de:db:ee:07:57:e7	10.0.100.102
MONITOR	eth0	de:db:ee:f0:87:82	83.212.4.124	eth2	de:db:ee:cd:76:e5	10.0.10.80	eth1	de:db:ee:95:2a:73	10.0.100.80

Name	Mac Address	IP	Netmask
DEMO	de:db:ee:bd:c5:16	62.217.124.213	255.255.255.252
OFFSITE	aa:00:00:42:28:4c	83.212.2.58	255.255.255.252

5 Ανάλυση Εξυπηρετητών

5.1 Firewall – Web Publishing servers

5.1.1 Λογισμικό και υπηρεσίες

Στους εξυπηρετητές fw01 και fw02 εγκαταστάθηκε λειτουργικό σύστημα Debian Linux 7. Η εγκατάσταση είναι η default εγκατάσταση όπως αυτή γίνεται στο ViMa. Επιπλέον εγκαταστάθηκαν τα εξής πακέτα από τα repositories του Debian, μαζί με ότι άλλα πακέτα και βιβλιοθήκες απαιτούνται για τη λειτουργία της:

- build-essential, libssl-dev, libpcre3-dev
- Pacemaker
- snmpd
- mercurial
- tinyproxy
- ntp

Επιπλέον εγκαταστάθηκε από τα sources του ο haproxy.

Συνολικά σε κάθε εξυπηρετητή σε ρόλο firewall είναι διαθέσιμες οι εξής υπηρεσίες:

- SSH server: Για την απομακρυσμένη πρόσβαση των διαχειριστών.
- Haproxy: TCP/HTTP Load Balancer. Είναι υπεύθυνος για το web Publishing και load balancing των εφαρμογών που τρέχουν στους web servers.
- Corosync: Cluster Engine. Μέσω αυτού γίνεται η επικοινωνία μεταξύ των εξυπηρετητών που μετέχουν στο firewall cluster.
- Pacemaker: Cluster Resource Manager. Αναλόγως της κατάστασης του cluster μεταφέρει τα resources του (IPs) σε διαθέσιμο server.
- Snmpd: SNMP daemon για το monitoring των servers.
- Tinyproxy: HTTP Proxy για την πρόσβαση των υπόλοιπων servers στο web.
- Ntpd: Network Time Protocol server για το συγχρονισμό των ρολογιών όλων των εξυπηρετητών.
- Iptables: Packet filtering framework. Εκτελεί ρόλο firewall

Ρυθμίσεις

5.1.1.1 SSH server

Για λόγους ασφαλείας έχει αλλαχθεί η default πόρτα στην οποία ακούει η υπηρεσία και έχει ρυθμιστεί ώστε να ακούει μόνο για συγκεκριμένες IPs και όχι για όλες τις IPs του εξυπηρετητή. Επίσης απαγορεύεται ρητά η σύνδεση μέσω ssh χωρίς authentication με password ή με δημόσιο κλειδί.

5.1.1.2 Corosync

Για την επικοινωνία των corosync υπηρεσιών που μετέχουν στο cluster έχει ρυθμιστεί μία επιπλέον IP σε κάθε εξυπηρετητή, στο δίκτυο 10.0.20.0/24. Η επικοινωνία γίνεται μέσω UDP πακέτων στις πόρτες 5999 και 6000 είτε κατευθείαν στην IP του εξυπηρετητή, είτε με multicast στην IP 226.94.10.10.

5.1.1.3 Pacemaker

Στο pacemaker είναι ορισμένα όλα τα resources που είναι διαθέσιμα στο cluster. Δεδομένου ότι οι υπηρεσίες iptables, haproxy και tinyproxy τις οποίες εξυπηρετεί το cluster είναι πάντα διαθέσιμες σε όλους τους εξυπηρετητές, τα resources που θέλουμε να μεταπίπτουν από τον ένα εξυπηρετητή στον άλλο είναι οι IPs:

- 10.0.100.10: Το gateway που χρησιμοποιούν όλοι οι εσωτερικοί servers στο δίκτυο DMZ.
- 10.0.10.10: Το gateway που χρησιμοποιούν όλοι οι εσωτερικοί servers στο δίκτυο Intranet.
- IPs στο δίκτυο 83.212.4.96/27 στις οποίες γίνονται published οι εφαρμογές.

Ως προτιμώμενος εξυπηρετητής έχει οριστεί στο pacemaker ο fw01, δηλαδή τα resources μεταπίπτουν στον fw02 μόνο αν ο fw01 είναι μη προσβάσιμος.

5.1.1.4 Ntpd

Η υπηρεσία ntp έχει ρυθμιστεί να ενημερώνει το ρολόι του εξυπηρετητή με βάση την ώρα που προσφέρεται μέσω ntp πρωτοκόλλου από το ntp.grnet.gr. Επιπλέον έχει ρυθμιστεί να επιτρέπει ερωτήματα για την ώρα μέσω NTP από τους εξυπηρετητές που βρίσκονται στα δίκτυα DMZ και Intranet.

5.1.1.5 Tinyproxy

Για λόγους ασφαλείας η απευθείας πρόσβαση από τους servers που βρίσκονται στα δίκτυα DMZ και Intranet στο διαδίκτυο είναι αποκλεισμένη μέσω του firewall. Οι εξυπηρετητές αυτοί χρησιμοποιούν ως proxy το Tinyproxy για να μπορούν να κατεβάζουν ενημερώσεις και να συνδέονται σε sites που είναι απαραίτητα για την λειτουργία του συστήματος (π.χ.services που προσφέρονται από τρίτους). Ο Tinyproxy έχει ρυθμιστεί ώστε να επιτρέπει την πρόσβαση μόνο από τα εσωτερικά δίκτυα και μόνο για τα sites που είναι ορισμένα στο αρχείο /etc/tinyproxy.filter.

5.1.1.6 Iptables

Στον παρακάτω πίνακα είναι καταγεγραμμένες οι υπηρεσίες για τις οποίες το configuration του iptables επιτρέπει την κίνηση πακέτων.

Από	Προς	Υπηρεσίες
Διαδίκτυο	Firewalls	Haproxy
Διαχειριστικό Δίκτυο	Firewalls	SSH
Διαχειριστικό Δίκτυο	DMZ,Intranet	Remote Desktop
Διαχειριστικό Δίκτυο	DEV server	FTP, Deployment Application
OFFSITE server	DEV server	FTP
Firewalls	Firewalls	Pacemaker,Corosync,SSH
DMZ, Intranet	Firewalls	NTP,Tinyproxy,Haproxy
DMZ	Intranet	Directory Services, CIFS, Database Server, Update Server
Intranet	DMZ	SMTP, CIFS,HTTP, HTTPS,Windows Remote Management, IIS Management
DMZ	Διαδίκτυο	SMTP

Οποιοσδήποτε άλλος τύπος πακέτου απορρίπτεται και καταγράφεται στα logs.Εκτός από τον έλεγχο της κίνησης των πακέτων το iptables εκτελεί και τις εξής λειτουργίες:

- Network Address Translation μεταξύ του διαδικτύου και των δικτύων DMZ και Intranet.
- Διαφανής ανακατεύθυνση της Http κίνησης από τα εσωτερικά δίκτυα ώστε αυτή να περνά μέσω του tinyproxy.

Το configuration του iptables βρίσκεται στον φάκελο /etc/iptables και γίνεται μέσω του script /etc/iptables/iptables.conf. Το script αυτό χρησιμοποιεί:

- Το αρχείο /etc/iptables/envvars: Στο αρχείο αυτό βρίσκονται με τη μορφή μεταβλητών IP διευθύνσεις οι οποίες χρησιμοποιούνται συχνά από το υπόλοιπο configuration. Π.χ. ορίζονται ποια είναι τα δίκτυα από τα οποία επιτρέπεται η διαχείριση των servers, ποιες είναι οι IPs και οι πόρτες στις οποίες κάνει publish ο haproxy τις εφαρμογές κ.ά.
- Τα αρχεία που βρίσκονται στους υποφάκελους του /etc/iptables/rules/. Τα αρχεία αυτά περιέχουν εντολές που ρυθμίζουν το firewall και εκτελούνται με λεξικογραφική σειρά από το script /etc/iptables/iptables.conf. Συγκεκριμένα κάθε υποφάκελος περιέχει αρχεία:

- Ο φάκελος input σχετικά με τα εισερχόμενα προς το firewall πακέτα.
- Ο φάκελος output σχετικά με τα εξερχόμενα από το firewall πακέτα.
- Ο φάκελος nat βρίσκονται αρχεία σχετικά με τα πακέτα για τα οποία γίνεται Network address translation.
- Ο φάκελος forward σχετικά με τα πακέτα που επιτρέπεται να διακινούνται μεταξύ διαφορετικών υποδικτύων.

5.1.1.7 Haproxy

Η εγκατάσταση του haproxy γίνεται κατεβάζοντας τον source κώδικα της έκδοσης 1.5 από το http://haproxy.1wt.eu/. Για να είναι δυνατό το compilation του κώδικα απαιτείται να είναι εγκατεστημένα τα πακέτα build-essential, libssl-dev, libpcre3-dev. Για την εγκατάσταση εκτελούνται οι εξής εντολές:

```
make TARGET=linux2628 CPU=generic USE_PCRE=1 USE_OPENSSL=1 USE_PCRE_JIT=1 \ USE_STATIC_PCRE=1 USE_LIBCRYPT=1 USE_ZLIB=1

sudo make PREFIX=/opt/haproxy install
```

Το haproxy είναι εγκατεστημένο στο φάκελο /opt/haproxy και το configuration του βρίσκεται στον φάκελο /opt/haproxy/conf/. Από τα αρχεία που βρίσκονται στον φάκελο αυτό το haproxy χρησιμοποιεί με λεξικογραφική σειρά μόνο αυτά το όνομά τους τελειώνει σε .cfg ή σε .cfg.`το όνομα του εκάστοτε εξυπηρετητή`. Το παραπάνω γίνεται ώστε να είναι δυνατός μεν ο συγχρονισμός του configuration μεταξύ των εξυπηρετητών αλλά παράλληλα να μπορεί ο καθένας να χρησιμοποιεί configuration που αφορά μόνο αυτόν. Για λόγους καθαρότητας το configuration του haproxy έχει διαιρεθεί στα εξής αρχεία:

1. haproxy.00-defaults.cfg: Περιέχει τις βασικές ρυθμίσεις του haproxy.
2. haproxy.10-stats.cfg: Περιέχει τις ρυθμίσεις για τα παραγόμενα στατιστικά.
3. haproxy.50-mgmt.cfg: Περιέχει τις ρυθμίσεις για δοκιμαστικές ή διαχειριστικές εφαρμογές που γίνονται published μέσω του haproxy.
4. haproxy.70-pubs.cfg: Περιέχει τις ρυθμίσεις για κάθε παραγωγική εφαρμογή που γίνεται published από τον haproxy.

Για λόγους ασφάλειας το haproxy είναι ρυθμισμένο να κάνει chroot στον φάκελο /opt/haproxy/chroot και να τρέχει ως ο χρήστης haproxy.

5.1.2 Συγχρονισμός ρυθμίσεων μεταξύ των firewalls

Οι ρυθμίσεις που πρέπει να συγχρονίζονται μεταξύ των firewalls είναι αυτές του iptables και του haproxy καθώς είναι οι μόνες που αλλάζουν σχετικά συχνά και είναι αρκετά περίπλοκες. Οποιαδήποτε άλλη αλλαγή θεωρείται ότι είναι έκτακτη και θα πρέπει να γίνεται σε όλους τους εξυπηρετητές με μέριμνα του διαχειριστή.

Ο συγχρονισμός των παραπάνω ρυθμίσεων γίνεται με τη βοήθεια του Distributed Version Control συστήματος mercurial. Για το haproxy όλο το επιθυμητό configuration βρίσκεται στον φάκελο /opt/haproxy/conf. Ο φάκελος αυτός είναι ταυτόχρονα και ένα mercurial repository. Συνεπώς ότι αλλαγή γίνεται πρέπει να γίνει commit στο mercurial με την εντολή `hg commit`. Σε κάθε repository έχει οριστεί ως extra source το mercurial repository που βρίσκεται στον άλλο server, στο οποίο η σύνδεση γίνεται μέσω ssh. Συνεπώς αφού γίνει commit στον ένα server μία αλλαγή ο διαχειριστής πρέπει στον δεύτερο server, στον φάκελο του haproxy /opt/haproxy/conf να τρέξει τις εντολές:

1. `hg update`: Για να ενημερώσει το τοπικό repository με τις αλλαγές από τον άλλο server
2. `hg pull`: Για να εφαρμόσει τις τελευταίες αλλαγές στον τοπικό φάκελο /opt/haproxy/conf

Ακριβώς με τον ίδιο τρόπο προωθούνται οι αλλαγές στον φάκελο /etc/iptables που περιέχει το configuration του iptables.

Για λόγους ασφάλειας η σύνδεση από το ένα mercurial repository στο άλλο γίνεται μέσω ενός χρήστη ο οποίος δεν είναι διαχειριστής στο μηχάνημα στο οποίο αναζητούνται οι αλλαγές. Καθώς σε όλες τις περιπτώσεις το configuration είναι δυνατόν να αλλαχθεί μόνο από διαχειριστές το παραπάνω έχει το αποτέλεσμα ο ένας εξυπηρετητής να είναι σε θέση να διαβάσει το configuration του άλλου αλλά όχι και να το αλλάξει. Για το λόγο αυτό οι αλλαγές είναι μόνο δυνατόν να γίνονται pull από τον λιγότερο ενημερωμένο εξυπηρετητή και όχι push από αυτόν στον οποίο έγιναν οι αλλαγές.

Για λόγους αξιοπιστίας η παραπάνω διαδικασία δεν είναι αυτόματη. Ο διαχειριστής καλείται να εκτελεί τη διαδικασία χειροκίνητα αφού επιβεβαιώσει ότι οι αλλαγές δεν επηρεάζουν τη σωστή λειτουργία του συστήματος.

5.2 Domain Controllers

5.2.1 Λογισμικό και υπηρεσίες

Στους εξυπηρετητές dc01,dc02 έχει εγκατασταθεί λειτουργικό σύστημα Windows Server 2008 R2. Στο λειτουργικό σύστημα έχουν ενεργοποιηθεί οι εξής ρόλοι:

- Active Directory Domain Services
- DNS Server
- File Services
    - File Server
    - Distributed File System
    - DFS Namespaces
    - DFS Replication

Επίσης έχουν ενεργοποιηθεί τα εξής features:

- Group Policy Management
- Remote Server Administration Tools
    - Role Administration Tools
    - AD DS and AD LDS Tools
        - AD DS Tools
    - Active Directory module for Windows Powershell
- DNS Server Tools
- File Services Tools
    - Distributed File System Tools
- SNMP Services
- .NET Framework 3.5.1 Features

5.2.2 Ρυθμίσεις

Το Active Directory έχει στηθεί πάνω στο domain **winplatform.local.**

Ο DNS Server εξυπηρετεί τα domains:

- winplatform.local: Χρησιμοποιείται για το Active Directory και όλα τα απαραίτητα dns entries του συνολικού συστήματος.
- webapps.local: Χρησιμοποιείται μόνο για τις εφαρμογές που εξυπηρετεί το Winplatform ως host headers για τα αντίστοιχα sites. Συγκεκριμένα :
    - όλες οι εγγραφές *.dev.webapps.local δείχνουν στον DEV server.
    - όλες οι εγγραφές *.web01.webapps.local δείχνουν στον WEB01 server.

- όλες οι εγγραφές *.web02.webapps.local δείχνουν στον WEB02 server.

5.2.2.1 Group Policies

Στο σύστημα γίνεται εκτεταμένη χρήση των Group Policies. Κατά όσο είναι εφικτό όλες οι ρυθμίσεις των εξυπηρετητών με Windows γίνονται μέσω group policies. Η εφαρμογή των group policies γίνεται όπως περιγράφεται στον παρακάτω πίνακα

Εφαρμογή	Όνομα Policy	Περιγραφή
Όλους τους χρήστες και εξυπηρετητές	Domain – WSUS	Ρυθμίσεις σχετικά τη χρήση του εσωτερικά εγκατεστημένου Windows Update Service.
	Domain - Accounts	Ρυθμίσεις σχετικά με τους λογαριασμούς. Συγκεκριμένα ορίζεται ότι τα passwords πρέπει να έχουν τουλάχιστον 10 χαρακτήρες και να είναι περίπλοκα. Πρέπει να αλλάζουν το πολύ κάθε χρόνο και δεν μπορεί να ξαναμπεί κάποιο από τα τελευταία 24 χρησιμοποιημένα passwords. Μετά από 10 αποτυχημένες απόπειρες πρόσβασης ο λογαριασμός κλειδώνεται για 15 λεπτά.
	Domain – NtpConf	Ρυθμίσεις σχετικά με τη χρήση του ntp server των firewalls ως time source
	Domain User - Settings	Ρυθμίσεις στα προφίλ των χρηστών κυρίως σε επίπεδο Internet (χρήση proxy, ορισμός trusted sites)
	Domain – Various	Ρυθμίσεις που δεν εμπίπτουν στις παραπάνω κατηγορίες
Όλοι οι εξυπηρετητές	Domain – Auditing	Ρυθμίσεις σχετικά με το επίπεδο του logging. Οι συγκεκριμένες ρυθμίσεις δεν είναι δυνατόν να γίνουν override από άλλα policies.
	Domain – Security	Ρυθμίσεις ασφάλειας των εξυπηρετητών. Οι συγκεκριμένες ρυθμίσεις δεν είναι δυνατόν να γίνουν override από άλλα policies.
Database Servers	DBs – Firewall	Ρυθμίσεις του firewall
	DBs – Services	Ποια services πρέπει να είναι ενεργά

	DBs – User Rights	Ρυθμίσεις σχετικά με τα δικαιώματα χρηστών και groups
	INTRANET - NtpServer	Ρυθμίσεις σχετικά με τη χρήση του ntp server των firewalls ως time source
	INTRANET – Proxy	Χρήση του proxy σε επίπεδο συστήματος
	INTRANET – Scheduled Tasks	Εγκατάσταση scheduled tasks στους εξυπηρετητές
	SERVERS – User Rights	Ρυθμίσεις σχετικά με τα δικαιώματα χρηστών και groups που ισχύουν σε όλους τους servers
Domain Controllers	DCs – Firewall	Ρυθμίσεις του firewall
	DCs – Services	Ποια services πρέπει να είναι ενεργά
	Default Domain Controller Policy	Οι default ρυθμίσεις των Domain Controllers.
	INTRANET - NtpServer	Ρυθμίσεις σχετικά με τη χρήση του ntp server των firewalls ως time source
	INTRANET – Proxy	Χρήση του proxy σε επίπεδο συστήματος
	INTRANET – Scheduled Tasks	Εγκατάσταση scheduled tasks στους εξυπηρετητές
	SERVERS – User Rights	Ρυθμίσεις σχετικά με τα δικαιώματα χρηστών και groups που ισχύουν σε όλους τους servers
DEV Server	DEV – Firewall	Ρυθμίσεις του firewall
	DEV – Services	Ποια services πρέπει να είναι ενεργά
	DEV – User Rights	Ρυθμίσεις σχετικά με τα δικαιώματα χρηστών και groups
	DEV – Settings	Ρυθμίσεις που δεν εμπίπτουν στις υπόλοιπες κατηγορίες
	INTRANET - NtpServer	Ρυθμίσεις σχετικά με τη χρήση του ntp server των firewalls ως time source
	INTRANET – Scheduled	Εγκατάσταση scheduled tasks στους

	Tasks	εξυπηρετητές
	SERVERS – User Rights	Ρυθμίσεις σχετικά με τα δικαιώματα χρηστών και groups που ισχύουν σε όλους τους servers
WEB Servers	WEBs – Firewall	Ρυθμίσεις του firewall
	WEBs – Services	Ποια services πρέπει να είναι ενεργά
	WEBs – User Rights	Ρυθμίσεις σχετικά με τα δικαιώματα χρηστών και groups
	WEBs – Settings	Ρυθμίσεις που δεν εμπίπτουν στις υπόλοιπες κατηγορίες
	DMZ - NtpServer	Ρυθμίσεις σχετικά με τη χρήση του ntp server των firewalls ως time source
	DMZ – Proxy	Χρήση του proxy σε επίπεδο συστήματος
	DMZ – Scheduled Tasks	Εγκατάσταση scheduled tasks

5.2.2.2 Distributed File System

Στο DFS έχουν δημιουργηθεί δύο namespaces

- Το share με path \\winplatform.local\share
- Το www με path \\winplatform.local\www

Το share namespace χρησιμοποιείται για εσωτερικά shares του συστήματος ενώ το www από τις εφαρμογές. Στα παραπάνω namespaces έχουν δημιουργηθεί τα shares που περιγράφονται στους παρακάτω πίνακες:

Share Namespace:

Name	Server path	Περιγραφή
ADMIN	\\dc01\ADMIN \\dc02\ADMIN	Μόνο διαχειριστική χρήση
DBBackups-Auto	\\dev\DBBackups-Auto	Εκεί αποθηκεύονται τα αυτοματοποιημένα backups των Βάσεων Δεδομένων
DBBackups-Developers	\\dev\DBBackups-	Χώρος στον οποίο μπορούν χρήστες

	Developers	χωρίς δικαιώματα διαχειριστή να αποθηκεύσουν Backups των Βάσεων Δεδομένων
users	\\dev\users	Χρησιμοποιείται από το FTP service στον DEV server
WebAppBackups-Auto	\\dev\WebAppBackups-Auto	Εκεί αποθηκεύονται τα αυτοματοποιημένα backups των εφαρμογών

Www namespace:

Name	Server path	Περιγραφή
iisconfig	\\dc01\iisconfig \\dc02\iisconfig	Κοινό σημείο από το οποίο διαβάζουν το configuration τους οι IIS servers
staging	\\dev\staging	Χρησιμοποιείται από την εφαρμογή Deployment των webapps
webapps	\\dc01\webapps \\dc02\webapps	Χώρος στον οποίο βρίσκονται τα εκτελέσιμα αρχεία των εφαρμογών. Από το σημείο αυτό τα διαβάζουν όλοι οι IIS Servers
webdata	\\dc01\webdata \\dc02\webdata	Χώρος στον οποίο αποθηκεύονται όλα τα αρχεία δεδομένων των εφαρμογών

Στα παραπάνω DFS shares, όπου αναφέρονται δύο server paths σημαίνει ότι το share προστατεύεται όντως redundant και το DFS επιστρέφει όποιο από τα δύο paths είναι διαθέσιμο. Αν και οι δύο servers είναι online ο DFS έχει ρυθμιστεί ώστε να επιστρέφει το share που βρίσκεται στον dc01. Τα αρχεία στα διαφορετικά server paths συγχρονίζονται με χρήση του DFS Replication services το οποίο ενημερώνει τα paths με τις αλλαγές που προκύπτουν στέλνοντας μόνο τα deltas των αλλαγών.

5.3 Database Servers

5.3.1 Λογισμικό και υπηρεσίες

Στους εξυπηρετητές db01,db02 έχει εγκατασταθεί λειτουργικό σύστημα Windows Server 2008 R2 και έχει εγκατασταθεί ο ρόλος File Server. Επίσης έχουν ενεργοποιηθεί τα εξής features:

- Failover Clustering
- Remote Server Administration Tools
  - Failover Clustering Tools
- SNMP Services
- .Net Framework 3.5.1

Επίσης έχει εγκατασταθεί SQL Server 2012 Enterprise.

5.3.2 Ρυθμίσεις

Στο λειτουργικό σύστημα των εξυπηρετητών έχει ρυθμιστεί η υπηρεσία Failover Clustering η οποία αποτελεί και τη βάση πάνω στην οποία στηρίζεται το χαρακτηριστικό Always-On Availability Groups του SQL Server. Το Failover Clustering γίνεται μεταξύ των nodes db01 και db02 και χρησιμοποιεί ως witness το share \\dc01.winplatform.local\DBClusterWitness για να αποκτήσει quorum τύπου Node and File Share Majority. Στο cluster έχουν δημιουργηθεί τα εξής clustered resources:

- Cluster Network 1: Είναι η βάση του cluster και αποτελείται από την IP 10.0.10.100.
- Sql-ag-main: Το Availability Group στο οποίο ανήκουν όσες Βάσεις Δεδομένων θέλουμε να βρίσκονται σε mode Always-On. Το Availability group είναι διαθέσιμο πάντα μέσω της IP 10.0.10.101 στην οποία ακούει ο εκάστοτε primary SQL Server. Η παραπάνω IP είναι προσβάσιμη μέσω του DNS name **sql-ag-main.winplatform.local**.

Ο SQL Server σε κάθε εξυπηρετητή έχει ρυθμιστεί ώστε να τρέχουν οι υπηρεσίες SQL Server (MSSQLServer) και SQL Server Agent (MSSQLServer). Τα data files των Βάσεων Δεδομένων αποθηκεύονται στο path D:\SQLServer\Databases ενώ το log files τους στο path D:\SQLServer\Logs

Οι υπόλοιπες ρυθμίσεις του λειτουργικού συστήματος των database servers λαμβάνονται μέσω των αντίστοιχων Group Policies.

5.4 Web Servers

5.4.1 Λογισμικό και υπηρεσίες

Στους εξυπηρετητές web01,web02 έχει εγκατασταθεί λειτουργικό σύστημα Windows Server 2008 R2. Στο λειτουργικό σύστημα έχουν ενεργοποιηθεί οι εξής ρόλοι και services:

- File Services
- Web Server (IIS)
    - Web Server
    - Common HTTP Features
        - Static Content
        - Default Document
        - Directory Browsing
        - HTTP Errors
        - HTTP Redirection
    - Application Development
        - ASP.NET
        - .NET Extensibility
        - ISAPI Extensions
        - ISAPI Filters
    - Health and Diagnostics
        - HTTP Logging
        - Logging Tools
        - Request Monitor
        - ODBC Logging
    - Security
        - Basic Authentication
        - Windows Authentication
        - Digest Authentication
        - IIS Client Certificate Mapping Authentication
        - URL Authorizations
        - Request Filtering
        - IP and Domain Restrictions
    - Performance
        - Static Content Compression
        - Dynamic Content Compression
    - Management Tools
        - IIS Management Console

- IIS Management Scripts and Tools
- Management Service
- IIS 6 Management Compatibility
    - IIS 6 Metabase Compatibility
    - IIS 6 WMI Compatibility
    - IIS 6 Scripting Tools
    - IIS 6 Management Console

Επίσης έχουν ενεργοποιηθεί τα εξής features:

- Remote Server Administration Tools
    - Web Server (IIS) Tools
    - SMTP Server Tools
- SMTP Server
- SNMP Services
- Windows Process Activation Service
    - Process Model
    - .NET Environment
    - Configuration APIs
- .NET Framework 3.5.1 Features
    - .NET Framework 3.5.1

Επιπλέον έχει εγκατασταθεί Shibboleth Service Provider και έχει ρυθμιστεί ο IIS Server ώστε να επικοινωνεί με χρήση του κατάλληλου ISAPI module.

5.4.2 Ρυθμίσεις

5.4.2.1 IIS

Οι IIS σε όλους τους web servers έχουν ρυθμιστεί ώστε να διαβάζουν το configuration τους από κοινό σημείο, το DFS path \\winplatform.local\www\iisconfig .Με τον τρόπο αυτό διευκολύνεται τόσο η ταυτόχρονη ενημέρωση των web servers με νέες ρυθμίσεις όσο και η δυνατότητα προσθήκης νέων web servers στο μέλλον. Ομοίως τα αρχεία όλων των εφαρμογών διαβάζονται από την τοποθεσία \\winplatform.local\www\webapps.

Κάθε εφαρμογή που εξυπηρετείται από το σύστημα έχει το δικό της website και το δικό της application pool. Για όλες τις sites ακολουθούνται οι παρακάτω συμβάσεις:

Έστω ότι App είναι το όνομα της εφαρμογής και Type είναι ο τύπος της. Το site της εφαρμογής ονομάζεται App-Type. Το site αυτό:

- Έχει ως root το path \\winplatform.local\www\webapps\App-Type.
- Χρησιμοποιεί ως application pool το pool App-Type.
- Αποθηκεύει τα δεδομένα του στο path \\winplatform.local\www\webdata\App-Type.
- Το site της εφαρμογής ακούει στην IP διεύθυνση του web server στην πόρτα 80 μόνο για τα host headers:
    - app-type.winplatform.grnet.gr
    - app-type.web01.winplatform.grnet.gr
    - app-type.web02.winplatform.grnet.gr
    - app-type.winplatform.local
    - app-type.web01.winplatform.local
    - app-type.web02.winplatform.local
    - Τα public hostnames της εφαρμογής.
    - Χρησιμοποιεί ως SMTP για την αποστολή emails τον localhost στην πόρτα 25

5.4.2.2 SMTP

Στον IIS Server έχει ενεργοποιηθεί επίσης το service SMTP και έχουν δημιουργηθεί δύο SMTP Servers.

1. Webapps SMTP. Ακούει στην πόρτα 25 και χρησιμοποιείται για την αποστολή emails από τις εξυπηρετούμενες εφαρμογές. Επιτρέπει την αποστολή emails μόνο από τον localhost.
2. Winplatform Relay. Ακούει στην πόρτα 25000 και χρησιμοποιείται για την αποστολή emails από τα συστήματα της πλατφόρμας Winplatform. Επιτρέπει την αποστολή emails από το δίκτυο 10.0.100.0/24.

Οι δύο διαφορετικοί SMTPs έχουν δημιουργηθεί για λόγους ασφάλειας. Ο WebApps SMTP πρέπει να είναι προσβάσιμος από παντού στο διαδίκτυο ώστε να μην χαρακτηρίζεται ως αποστολέας spam από τρίτους

SMTPs. Η πρόσβαση αυτή γίνεται μέσω του haproxy το οποίο κάνει failover ανάμεσα στους SMTPs που βρίσκονται στους web servers. Λόγω όμως του τρόπου λειτουργίας του haproxy όλοι όσοι επικοινωνούν με τον SMTP αυτό εμφανίζονται με την IP του haproxy 10.0.100.10. Συνεπώς δεν είναι δυνατόν στο επίπεδο του SMTP να κάνουμε διάκριση μεταξύ των συστημάτων τα οποία επιθυμούμε να μπορούν να κάνουν relay emails και άλλων συστημάτων καθώς όλα εμφανίζονται με την ίδια IP. Για το λόγο αυτό ο δημόσια προσβάσιμος WebApps SMTP επιτρέπει το relay μηνυμάτων μόνο από το σύστημα στο οποίο τρέχει (localhost).

Για να καλυφθεί το παραπάνω κενό αυτό δημιουργήθηκε ο Winplatform Relay. Αυτός επιτρέπει μεν την αποστολή emails, η πρόσβασή σε αυτόν όμως περιορίζεται από το firewall μόνο σε συστήματα που επιθυμούμε να μπορούν να στείλουν emails.

5.5 Deployment server

5.5.1 Λογισμικό και υπηρεσίες

Στους εξυπηρετητές web01,web02 έχει εγκατασταθεί λειτουργικό σύστημα Windows Server 2008 R2. Στο λειτουργικό σύστημα έχουν ενεργοποιηθεί οι εξής ρόλοι και services:

- File Services
- Windows Server Update Services
- Web Server (IIS)
    - Web Server
    - Common HTTP Features
        - Static Content
        - Default Document
        - Directory Browsing
        - HTTP Errors
        - HTTP Redirection
    - Application Development
        - ASP.NET
        - .NET Extensibility
        - ISAPI Extensions
        - ISAPI Filters
    - Health and Diagnostics
        - HTTP Logging
        - Logging Tools
    - Security
        - Basic Authentication
        - Windows Authentication
        - Digest Authentication
        - URL Authorizations
        - Request Filtering
        - IP and Domain Restrictions
    - Performance
    - Management Tools
        - IIS Management Console
        - IIS Management Scripts and Tools
        - Management Service
        - IIS 6 Management Compatibility
            - IIS 6 Metabase Compatibility

- IIS 6 WMI Compatibility
- IIS 6 Scripting Tools
- IIS 6 Management Console

- FTP Server
  - FTP Service
  - FTP Extensibility

Επίσης έχουν ενεργοποιηθεί τα εξής features:

- Remote Server Administration Tools
  - Web Server (IIS) Tools
- SNMP Services
- .NET Framework 3.5.1 Features
  - .NET Framework 3.5.1
- Windows Internal Database

Επιπλέον έχουν εγκατασταθεί τα Management Tools του SQL Server 2012 R2.

5.5.2 Ρυθμίσεις

5.5.2.1 IIS

Στον IIS web server που είναι εγκαταστημένος στον εξυπηρετητή είναι ρυθμισμένα τα εξής sites:

- WINPLATFORM Management: Περιέχει την εφαρμογή Deployment που χρησιμοποιούν οι developers για να ανεβάζουν αλλαγές στον κώδικα. Το site αυτό γίνεται published μέσω του haproxy στη διεύθυνση mgmt.winplatform.grnet.gr. Η πρόσβαση στο site απαιτεί αφενός authentication με μόνους αποδεκτούς χρήστες τους developers και αφετέρου επιτρέπεται μόνο από τις IPs των διαχειριστικών δικτύων.
- WSUS Administration: Εξυπηρετεί τα Windows Server Update Services και δεν είναι προσπελάσιμο από το διαδίκτυο.
- Όμοια sites με αυτά που έχουν ρυθμιστεί στους web εξυπηρετητές web01 και web02. Τα sites αυτά δεν γίνονται published. Επιπλέον, αν και περιέχουν κάποια έκδοση του κώδικα των εφαρμογών, δεν είναι λειτουργικά καθώς δεν έχουν καθόλου πρόσβαση στις Βάσεις Δεδομένων. Χρησιμοποιούνται αποκλειστικά ως μεταβατικός χώρος αποθήκευσης των αρχείων των web εφαρμογών κατά τη διαδικασία Deployment.

5.5.2.2 FTP

Η πρόσβαση στον FTP Server απαιτεί authentication με μόνους αποδεκτούς χρήστες τους developers και επιπλέον επιτρέπεται μέσω του firewall μόνο από τα διαχειριστικά δίκτυα. Μέσω του FTP server μπορεί κάποιος χρήστης να έχει πρόσβαση *μόνο* στους χώρους που περιγράφονται στον παρακάτω πίνακα:

FTP Path	Path στον DEV server	Περιγραφή
/	D:\Users\USERNAME	Προσωπικός χώρος κάθε χρήστη
/DBbackups-Developers	D:\Users\DBBackups	Χώρος στον οποίο μπορούν να ανεβάζουν οι χρήστες backups των βάσεων δεδομένων.
/Developers	D:\Users\Developers	Κοινός χώρος για όλους τους developers.
/Staging	D:\WWW\WebApps	Μεταβατικός χώρος εφαρμογών κατά το deployment
/WINPLATFORM	D:\FTPRoot\WINPLATFORM	Χώρος μη εγγράψιμος από τους χρήστες

5.6 Demo Server

5.6.1 Λογισμικό και υπηρεσίες

Στον εξυπηρετητή demo έχει εγκατασταθεί λειτουργικό σύστημα Windows Server 2008 R2. Στο λειτουργικό σύστημα έχουν ενεργοποιηθεί οι εξής ρόλοι και services:

- File Services
- Web Server (IIS)
  - Web Server
  - Common HTTP Features
    - Static Content
    - Default Document
    - Directory Browsing
    - HTTP Errors
    - HTTP Redirection
  - Application Development
    - ASP.NET
    - .NET Extensibility
    - ISAPI Extensions
    - ISAPI Filters
  - Health and Diagnostics
    - HTTP Logging
    - Logging Tools
    - Request Monitor
    - ODBC Logging
  - Security
    - Basic Authentication
    - Windows Authentication
    - Digest Authentication
    - IIS Client Certificate Mapping Authentication
    - URL Authorizations
    - Request Filtering
    - IP and Domain Restrictions
  - Performance
    - Static Content Compression
    - Dynamic Content Compression
  - Management Tools
    - IIS Management Console

        - IIS Management Scripts and Tools
        - Management Service
        - IIS 6 Management Compatibility
            - IIS 6 Metabase Compatibility
            - IIS 6 WMI Compatibility
            - IIS 6 Scripting Tools
            - IIS 6 Management Console
    - FTP Server
        - FTP Service
        - FTP Extensibility

Επίσης έχουν ενεργοποιηθεί τα εξής features:

- Remote Server Administration Tools
    - Web Server (IIS) Tools
    - SMTP Server Tools
- SMTP Server
- SNMP Services
- Windows Process Activation Service
    - Process Model
    - .NET Environment
    - Configuration APIs
- .NET Framework 3.5.1 Features
    - .NET Framework 3.5.1

Επιπλέον έχει εγκατασταθεί Shibboleth Service Provider και έχει ρυθμιστεί ο IIS Server ώστε να επικοινωνεί με χρήση του κατάλληλου ISAPI module.

Επίσης έχει εγκατασταθεί SQL Server 2012 Enterprise.

5.6.2 Ρυθμίσεις

5.6.2.1 IIS

Κάθε εφαρμογή που εξυπηρετείται από το σύστημα έχει το δικό της website και το δικό της application pool. Για όλες τις sites ακολουθούνται οι παρακάτω συμβάσεις:

Έστω ότι App είναι το όνομα της εφαρμογής και Type είναι ο τύπος της. Το site της εφαρμογής ονομάζεται App-Type. Το site αυτό:

- Έχει ως root το path D:\webapps\App-Type.
- Χρησιμοποιεί ως application pool το pool App-Type.
- Αποθηκεύει τα δεδομένα του στο path D:\webdata\App-Type.
- Το site της εφαρμογής ακούει στην IP διεύθυνση του web server στην πόρτα 80 μόνο για τα host headers:
    - app-type.pilotiko.gr
    - app-type.demo.pilotiko.gr
    - Τα public hostnames της εφαρμογής.
    - Χρησιμοποιεί ως SMTP για την αποστολή emails τον localhost στην πόρτα 25.

5.6.2.2 SMTP

Στον IIS Server έχει ενεργοποιηθεί επίσης το service SMTP και έχει δημιουργηθεί ένας SMTP Server που επιτρέπει το relay μηνυμάτων μόνο από το τοπικό μηχάνημα (Localhost).

5.6.2.3 FTP

Η πρόσβαση στον FTP Server απαιτεί authentication με μόνους αποδεκτούς χρήστες τους developers και επιπλέον επιτρέπεται μέσω του firewall μόνο από τα διαχειριστικά δίκτυα. Μέσω του FTP server μπορεί κάποιος χρήστης να έχει πρόσβαση *μόνο* στους χώρους που περιγράφονται στον παρακάτω πίνακα:

FTP Path	Path στον DEV server	Περιγραφή
/	D:\FTP\LocalUser\USERNAME	Προσωπικός χώρος κάθε χρήστη
/DBbackups	D:\DB\BACKUPs	Χώρος στον οποίο μπορούν να ανεβάζουν οι χρήστες backups των βάσεων δεδομένων.
/Developers	D:\Developers	Κοινός χώρος για όλους τους developers.
/WebApps	D:\WebApps	Αρχεία εφαρμογών

5.6.2.4 Firewall

Ως firewall χρησιμοποιείται το Windows Firewall του λειτουργικού συστήματος. Έχει ρυθμιστεί ώστε να επιτρέπει μόνο την κίνηση προς:

- Την πόρτα 80 (HTTP) στην οποία ακούει ο IIS.
- Την πόρτα 443 (HTTPs) στην οποία ακούει ο IIS για εφαρμογές που απαιτούν secure σύνδεση.
- Την πόρτα 8443 για την απομακρυσμένη διαχείριση του IIS μόνο από διαχειριστικά δίκτυα.
- Την πόρτα στην οποία τρέχει ο FTP Server μόνο από διαχειριστικά δίκτυα.
- Remote Desktop Protocol μόνο από διαχειριστικά δίκτυα.

5.7 Offsite server

5.7.1 Λογισμικό και υπηρεσίες

Στον εξυπηρετητή εγκαταστάθηκε λειτουργικό σύστημα Debian Linux 7. Η εγκατάσταση είναι η default minimal εγκατάσταση όπως αυτή γίνεται στο ViMa. Επιπλέον εγκαταστάθηκαν τα εξής πακέτα από τα repositories του Debian, μαζί με ότι άλλα πακέτα και βιβλιοθήκες απαιτούνται για τη λειτουργία της:

- snmpd
- nullmailer
- lftp

Ο εξυπηρετητής offsite δεν προσφέρει καθόλου υπηρεσίες εκτός του ssh για την απομακρυσμένη πρόσβαση των διαχειριστών και του snmp για το monitoring του.

5.7.2 Ρυθμίσεις

Το iptables έχει ρυθμιστεί να επιτρέπει μόνο ssh και snmp συνδέσεις από τα διαχειριστικά δίκτυα.

Στο φάκελο /backup/bin βρίσκονται τα scripts `syncDBsWinplatform.sh` και `syncWebAppsWinplatform.sh` που αναλαμβάνουν την αντιγραφή των backups από το παραγωγικό περιβάλλον. Τα scripts χρησιμοποιούν την εφαρμογή lftp για να συνδεθούν μέσω πρωτοκόλλου FTP με χρήση TLS στον FTP server του winplatform και να συγχρονίσουν τα δεδομένα.

Για τα backups των Βάσεων Δεδομένων η σύνδεση γίνεται με τον χρήστη dbbackread και αντιγράφονται τα δεδομένα από τον φάκελο

- ftp://mgmt.winplatform.grnet.gr:17021/WebApps

στον φάκελο

- /backup/winplatform/dbs/WebApps

και από τον φάκελο

- ftp://mgmt.winplatform.grnet.gr:17021/System

στον φάκελο

- /backup/winplatform/dbs/System

Για τα backups των εφαρμογών η σύνδεση γίνεται με τον χρήστη webappbackread και αντιγράφονται τα δεδομένα από τον φάκελο

- ftp://mgmt.winplatform.grnet.gr:17021/Webdata

στον φάκελο

- /backup/winplatform/webapps/WebData

και από τον φάκελο

- ftp://mgmt.winplatform.grnet.gr:17021/WebApps

στον φάκελο

- /backup/winplatform/webapps/WebApps

Σημειώνεται ότι οι FTP φάκελοι που εμφανίζονται παραπάνω ισχύουν μόνο για τον εκάστοτε χρήστη που συνδέεται και δεν είναι προσβάσιμοι από άλλους χρήστες.

6 Λεπτομέρειες Υλοποίησης

6.1 Scripts Διαχείρισης

Στο share \\winplatform.local\share\ADMIN\Scripts υπάρχουν scripts για τη διαχείριση της πλατφόρμας. Αν και τα scripts βρίσκονται αποθηκευμένα στους dc01 και dc02 για λόγους προστασίας από το DFS Replication είναι σχεδιασμένα ώστε να εκτελούνται στον DEV server. Τα scripts είναι powershell scripts και χωρίζονται σε δύο κατηγορίες:

- Εκτελέσιμα scripts: Πρόκειται για scripts που εκτελούν κάποια συγκεκριμένη λειτουργία και είναι τα:
    - `CreateDeveloper.ps1`: Δημιουργεί ένα νέο developer χρήστη, τους εκχωρεί τα σωστά δικαιώματα και δημιουργεί τους απαραίτητους για αυτόν φακέλους . Δέχεται ως παραμέτρους το username του χρήστη, το όνομά του και το επώνυμό του. Παράδειγμα εκτέλεσης:

      ```
      powershell CreateDeveloper.ps1 –username “username” –firstname “Όνομα” –lastname “Επώνυμο”
      ```

    - `WebAppCreate.ps1`: Εκτελεί όλες τις απαραίτητες ρυθμίσεις για τη δημιουργία μίας νέας web εφαρμογής. Συγκεκριμένα για μία εφαρμογή που ανήκει στο project Project και ονομάζεται App:

        1. Δημιουργεί τον απαραίτητο χρήστη υπό τον οποίο τρέχει η εφαρμογή και τα σχετικά security Groups.
        2. Δημιουργεί τον φάκελο \\winplatform.local\webapps\Project-App.
        3. Δημιουργεί τον φάκελο \\winplatform.local\webdata\Project-App.
        4. Δημιουργεί τον φάκελο \\winplatform.local\staging\Project-App.
        5. Εφαρμόζει τα σωστά δικαιώματα στους παραπάνω φακέλους.
        6. Δημιουργεί στους web servers το application pool Project-App και το αντίστοιχο site Project-App κάνοντας παράλληλα και όλες τις απαραίτητες ρυθμίσεις.
        7. Δημιουργεί στον DEV server το application pool Project-App και το αντίστοιχο site Project-App για να χρησιμοποιηθούν κατά από την εφαρμογή deployment κάνοντας παράλληλα και όλες τις απαραίτητες ρυθμίσεις.

8. Δημιουργεί στους database servers τα απαραίτητα logins για πρόσβαση στις βάσεις δεδομένων που απαιτείται.

Το script δέχεται ως ορίσματα το project στο οποίο ανήκει η εφαρμογή, το όνομά της εφαρμογής και το public URL της. Παράδειγμα εκτέλεσης:

```
powershell WebAppCreate.ps1 –project MyProject –app Portal –url myproject-portal.gr
```

- `WebAppDbRestore.ps1`: Λαμβάνει ένα υπάρχον backup μίας βάσης δεδομένων μίας εφαρμογής και το κάνει restore στον primary database server εκτελώντας τις εξής λειτουργίες:

1. Ελέγχει αν υπάρχει ήδη βάση για την εκάστοτε εφαρμογή και ρωτά των χρήστη αν θέλει να γίνει overwrite ή rename. Αν η υπάρχουσα βάση μετέχει σε Always-On Availability Group τότε το scripts τη βγάζει από το group.
2. Κάνει restore το backup της Βάσης Δεδομένων.
3. Αφαιρεί πιθανόν προϋπάρχοντες χρήστες της βάσης και προσθέτει .με τα σωστά δικαιώματα τους χρήστες της εφαρμογής.
4. Ρωτά τον χρήστη αν η βάση πρέπει να προστεθεί στο Always-On Availability Group sql-ag-main. Αν η απάντηση είναι θετική προχωρά στα επόμενα βήματα αλλιώς τερματίζεται η λειτουργία του.
5. Αν το Recovery Model της βάσης δεν είναι Full όπως απαιτείται από τα Always-On Availability Group κάνει τις απαραίτητες ρυθμίσεις ώστε να γίνει και λαμβάνει νέο backup της Βάσης Δεδομένων.
6. Λαμβάνει log backup της Βάσης Δεδομένων.
7. Κάνει restore το τελευταίο backup της βάσης στον secondary server.
8. Κάνει restore με το option NO RECOVERY το log backup της βάσης στον secondary server.
9. Προσθέτει την βάση του primary server στο Always-On Availability Group.
10. Προσθέτει τη βάση του secondary server στο Always-On Availability Group ως replica.

Το script δέχεται ως ορίσματα το project στο οποίο ανήκει η εφαρμογή, το όνομά της εφαρμογής και το όνομα του αρχείου με το backup της Βάσης Δεδομένων. Το αρχείο με το backup πρέπει να βρίσκεται στον φάκελο \\winplatform.local\share\DBBackups-Developers\Project-App\. Παράδειγμα εκτέλεσης:

```
powershell WebAppDbRestore.ps1 –project MyProject –app Portal –bakfile MyBackup.bak
```

- DBBackup.ps1: Αναλαμβάνει τη δημιουργία backups των Βάσεων Δεδομένων και την διατήρηση ιστορικού αυτών. Ο χρήστης μπορεί να ορίσει συγκεκριμένα ποια βάση σε ποιον server θα γίνει backup ή να ζητήσει να ληφθεί backup από όλες τις User ή και System Databases. Επίσης μπορεί να ζητήσει το backup να είναι Full ή Incremental. Στην περίπτωση του incremental Backup το script θα κρίνει αν αυτό πρέπει να είναι differential backup ή log backup αναλόγως με το αν η εκάστοτε Βάση Δεδομένων είναι σε Full Recovery Model. Επιπλέον είναι διαθέσιμος και ο τύπος backup “timed” όπου το script θα πάρει full backup αν ο χρόνος εκτέλεσης είναι σε ένα ορισμένο χρονικό πλαίσιο και incremental αν όχι. Η επιλογή αυτή χρησιμοποιείται κατά την αυτοματοποιημένη λήψη backups. Το script δέχεται τα εξής ορίσματα:

  - dbs: Προαιρετικό. Σε μορφή database_name@servername,... οι Βάσεις Δεδομένων που πρέπει να γίνουν backup.
  - skippedDbs: Προαιρετικό. Στην ίδια μορφή με το όρισμα dbs τυχόν Βάσεις Δεδομένων που δεν πρέπει να γίνουν backup ακόμα και αν περιλαμβάνονται μέσω κάποιου άλλου ορίσματος.
  - servers: Προαιρετικό. Οι servers από τους οποίους πρέπει να ληφθεί το backup. Αν δε δοθεί λαμβάνεται backup από όλους τους διαθέσιμους database servers.
  - userDbs: Προαιρετικό. Οδηγεί το script να πάρει backup από όλες τις User Databases επιπλέον του ότι έχει οριστεί στο –dbs. Το όρισμα –skippedDbs λαμβάνεται υπόψη.
  - systemDbs: Προαιρετικό. Οδηγεί το script να πάρει backup από όλες τις System Databases επιπλέον του ότι έχει οριστεί στο –dbs. Το όρισμα –skippedDbs λαμβάνεται υπόψη.
  - backupType: full ή incr ή timed.

Παράδειγματα εκτέλεσης:

```
Powershell DBBackup.ps1 –dbs Project-Portal@db01 –backupType full
```

```
Powershell DBBackup.ps1 –UserDbs –backupType ‘timed’
```

- Βιβλιοθήκες functions: Περιέχουν functions που χρησιμοποιούνται από τα υπόλοιπα scripts για την επίτευξη των λειτουργιών τους. Πρόκειται για τα αρχεία:
  - DBBackupFunctions.ps1
  - Defaults.ps1
  - Defaults4WebApp.ps1
  - Utils.ps1
  - WebAppFunctions.ps1
  - WebAppScriptBase.ps1

6.2 Αυτοματοποιημένη Διαδικασία Backup

Στο πλατφόρμα Winplatform έχει ενεργοποιηθεί αυτοματοποιημένη διαδικασία λήψης αντιγράφων ασφαλείας των εφαρμογών και των δεδομένων τους. Η διαδικασία αυτή χωρίζεται σε δύο μέρη.

6.2.1 Backup εφαρμογών

Στον DEV εξυπηρετητή εκτελείται ως scheduled task καθημερινά στις 22:00 το script \\winplatform.local\share\scripts\WebAppsBackup.cmd. Το script αυτό χρησιμοποιεί το εργαλείο robocopy για να αντιγράψει τα αρχεία των εφαρμογών καθώς και τα δεδομένα τους από τους φακέλους

\\winplatform.local\share\webapps
και
\\winplatform.local\share\webdata

αντίστοιχα στους φακέλους

\\winplatform.local\share\WebAppBackups-Auto\WebApps
και
\\winplatform.local\share\WebAppBackups-Auto\WebData

Ιστορικά αντίγραφα ασφαλείας των εφαρμογών δεν κρατούνται καθώς αυτό γίνεται με διαφορετικό τρόπο από την εφαρμογή Deployment όπως θα εξηγηθεί στη συνέχεια.

6.2.2 Backup Βάσεων Δεδομένων

Και στους δύο εξυπηρετητές db01 και db02 έχει δημιουργηθεί ένα scheduled task το οποίο εκτελεί το script \\winplatform.local\share\scripts\dbbackup.cmd. Το scheduled task εκτελείται κάθε τέσσερις ώρες με διαφορά μισής ώρας από τον έναν server στον άλλο. Σε κάθε εκτέλεση το παραπάνω script καλεί το script \\winplatform.local\share\scripts\DBBackup.ps1 με τα εξής ορίσματα:

```
DBBackup.ps1 -userDBs -systemDbs -backupType 'timed' -servers %COMPUTERNAME%
```

Η παραπάνω κλήση έχει ως αποτέλεσμα μία φορά την ημέρα σε κάθε εξυπηρετητή να λαμβάνεται Full Backup των Βάσεων Δεδομένων. Το script λαμβάνει υπόψη του ποιες βάσεις ανήκουν σε Always-On Availability Group και δημιουργεί backup μόνο από τον δευτερεύοντα εξυπηρετητή. Επίσης δημιουργείται backup όλων των System Databases του κάθε server.

Τις υπόλοιπες φορές κλήσης του script δημιουργούνται incremental backups. Τα incremental backups λαμβάνονται μόνο από τις User Databases και αναλόγως με το αν η Βάση Δεδομένων βρίσκεται σε Full Recovery Model ή όχι λαμβάνεται Log backup ή differential backup. Και πάλι λαμβάνεται υπόψη αν η βάση δεδομένων βρίσκεται σε Always-On Availability Group και αν ναι το backup λαμβάνεται μόνο από τον πρωτεύοντα εξυπηρετητή.

Σε όλες τις περιπτώσεις δεν γίνεται επανεγγραφή παλαιότερων backup αλλά λαμβάνεται νέο αντίγραφο εξαρχής. Σε κάθε κλήση του script και αν η διαδικασία backup επιτύχει, γίνεται εκκαθάριση του ιστορικού των backups με βάση τις υπάρχουσες ρυθμίσεις.

6.3 Εφαρμογή Deployment

Ο έλεγχος της διαδικασίας ενημέρωσης των εφαρμογών που εξυπηρετούνται θεωρείται κομβικός τόσο για την αξιοπιστία όσο και για την ασφάλεια συνολικά του συστήματος. Για το λόγο αυτό αναπτύχθηκε μία web εφαρμογή η οποία χειρίζεται το deployment των αλλαγών στις εφαρμογές. Η εφαρμογή έχει αναπτυχθεί σε .Net framework και εκμεταλλεύεται τις δυνατότητες web deployment που προσφέρει το Management Service του IIS σε συνδυασμό με το εργαλείο ανάπτυξης Visual Studio.

Ανάμεσα στους στόχους της εφαρμογής είναι η διευκόλυνση των developers στο ανέβασμα νέων εκδόσεων πραγματοποιώντας ταυτόχρονα όσους ελέγχους είναι απαραίτητη για την ασφάλεια του συστήματος. Για το λόγο αυτό επιλέχθηκε η λογική των δύο σταδίων στην εφαρμογή των αλλαγών.

Σε πρώτο στάδιο ο developer καλείται να ανεβάσει σε ένα προσωρινό χώρο τις αλλαγές ή όλα τα αρχεία της εφαρμογή που θέλει να ενημερώσει. Ο προσωρινός χώρος αποθήκευσης βρίσκεται στον DEV εξυπηρετητή στο path \\winplatfom.local\share\staging. Το ανέβασμα μπορεί να γίνει με δύο τρόπους:

1. Κατευθείαν από το Visual Studio με χρήση του ενσωματωμένου εργαλείου msdeploy με σύνδεση στον IIS που είναι εγκατεστημένος στον DEV εξυπηρετητή. Για να είναι δυνατή η λειτουργία αυτή πρέπει στο Management Service του IIS να έχουν δοθεί τα απαραίτητα δικαιώματα στον χρήστη. Αυτό γίνεται μέσω της συμμετοχής του χρήστη στο απαραίτητο security group της εφαρμογής.
2. Μέσω του FTP που είναι εγκατεστημένος στον DEV εξυπηρετητή στο path /Staging.

Στο δεύτερο στάδιο ο χρήστης πρέπει να επισκεφθεί τη σελίδα της εφαρμογής. Εκεί, αφού κάνει login με τα στοιχεία του επιλέγει ποια από τις υπάρχουσες εφαρμογές θέλει να ενημερώσει. Οι εφαρμογές από τις οποίες μπορεί να επιλέξει είναι μόνο όσες έχει τα απαραίτητα δικαιώματα να κάνει αλλαγές. Στη συνέχεια η εφαρμογή χρησιμοποιεί το εργαλείο msdeploy για να συγκρίνει τα αρχεία της εφαρμογής που υπάρχουν στην staging περιοχή με αυτά που υπάρχουν στο παραγωγικό σύστημα. Μετά το τέλος του ελέγχου παρουσιάζει στον χρήστη τα αρχεία που πρόκειται να αλλάξουν. Στο σημείο αυτό ο χρήστης καλείται να επιλέξει:

- Αν όντως επιθυμεί να ενημερώσει και το configuration της εφαρμογής αν αυτό είναι δυνατόν.
- Αν θα αντιγραφούν απλώς τα αρχεία που βρίσκονται στην προσωρινή περιοχή ή θα γίνει πλήρης συγχρονισμό μεταξύ της προσωρινής και της παραγωγικής εφαρμογής.
- Αν μετά το τέλος της ενημέρωσης θα γίνει recycling του application pool

Οι προεπιλεγμένες ρυθμίσεις είναι να μην ενημερώνεται το configuration, να αντιγράφονται απλώς τα αρχεία και να μην γίνεται recycle το application pool.

Αφού ο χρήστης κάνει τις κατάλληλες επιλογές και αν επιβεβαιώσει τη λειτουργία deployment η εφαρμογή εκτελεί τις εξής λειτουργίες:

1. Η εφαρμογή κλειδώνεται με τη δημιουργία ενός lock file ώστε κατά τη διάρκεια των εργασιών να μην είναι δυνατόν να κάνει κάποιος τρίτος αλλαγές.
2. Δημιουργείται ένα shadow copy των αρχείων της εφαρμογής στους εξυπηρετητές dc01 και dc02. Με τον τρόπο αυτό δημιουργείται ένα ιστορικό αντίγραφο της εφαρμογής στο οποίο είναι δυνατόν να επιστρέψει ανά πάσα στιγμή.
3. Δημιουργείται στο root της εφαρμογής το ειδικό αρχείο app_offline.htm το οποίο οδηγεί τους IIS να σταματήσουν τη λειτουργία της. Η εφαρμογή γίνεται μη διαθέσιμη κατά τη διάρκεια της ενημέρωσης για να αποφευχθούν πιθανά προβλήματα από προβληματικές ή διακεκομμένες ενημερώσεις.
4. Με τη χρήση του msdeploy εργαλείου αντιγράφονται τα αρχεία από την staging περιοχή στην παραγωγική. Αναλόγως με την επιλογή του χρήστη γίνεται απλή αντιγραφή ή συγχρονισμός.
5. Αν έχει ενημερωθεί το αρχείο web.sitemap τότε διορθώνονται το file system access list ώστε να επιτρέπει την εγγραφή στο αρχείο από τον χρήστη υπό τον οποίο τρέχει η εφαρμογή καθώς είναι απαραίτητο.
6. Αν έχει ζητηθεί γίνεται recycling του application pool της εφαρμογής.
7. Αφαιρείται το app_offline.htm αρχείο ώστε να ξαναμπεί σε λειτουργία η εφαρμογή.
8. Ξεκλειδώνεται η εφαρμογή.

Σε όλες τις παραπάνω περιπτώσεις όλες οι λειτουργίες

- Απαιτούν τη σύνδεση με τα credentials του χρήστη.
- Εκτελούνται υπό τον εκάστοτε χρήστη.
- Η απομακρυσμένη σύνδεση επιτρέπεται μόνο από έμπιστα διαχειριστικά δίκτυα.

Με τον τρόπο αυτό διασφαλίζεται η ασφάλεια του συστήματος καθώς δεν είναι δυνατόν να γίνουν ενέργειες εκτός των δικαιωμάτων του χρήστη.

6.4 Χρήστες

Σε όλο το σύστημα έχει ληφθεί πρόνοια ώστε κάθε ενέργεια να γίνεται με όσο το δυνατόν πιο περιορισμένα δικαιώματα και να υπάρχει απομόνωση των εφαρμογών σε επίπεδο χρηστών. Συνεπώς όσες εφαρμογές δε χρειάζονται διαχειριστικά δικαιώματα τρέχουν ως ειδικοί χρήστες ενώ ειδική μέριμνα έχει δοθεί στα δικαιώματα των φυσικών χρηστών του συστήματος.

Στα firewalls που τρέχουν linux λειτουργικό σύστημα οι ευαίσθητες υπηρεσίες που δεν απαιτούν δικαιώματα διαχειριστή είναι το haproxy και το tinyproxy. Και τα δύο έχουν ρυθμιστεί να τρέχουν αντίστοιχα υπό τους χρήστες haproxy και tinyproxy οι οποίοι δεν έχουν δικαιώματα root.

Στους υπόλοιπους εξυπηρετητές που τρέχουν λειτουργικό σύστημα Windows η πολιτική που έχει ακολουθηθεί είναι τα δικαιώματα να εκχωρούνται σε groups και οι χρήστες να λαμβάνουν τα σχετικά δικαιώματα μέσω της συμμετοχής τους στα κατάλληλα groups. Στον παρακάτω πίνακα εμφανίζονται τα groups που έχουν δημιουργηθεί και περιγράφονται τα δικαιώματα που τους έχουν εκχωρηθεί.

Όνομα Group	Είναι μέλος των	Περιγραφή δικαιωμάτων
DeployEnvAccess		Δικαιώματα πρόσβασης και χρήσης της εφαρμογής Deployment
Developers	AdminShareAccess DBBackupFilesAccess DeployEnvAccess Remote Shadow Users Remote WinRM Users WebAppsFileAccess	Τα μέλη του Group αυτού έχουν δικαιώματα αλλαγής των αρχείων όλων των εφαρμογών καθώς και αλλαγής των δεδομένων όλων των User Databases
DevManagers		Δικαιώματα διαχειριστή στον εξυπηρετητή DEV
ExternalDevs	AdminShareAccess DBBackupFilesAccess DeployEnvAccess Remote Shadow Users Remote WinRM Users WebAppsFileAccess	Τα μέλη του group έχουν βασικά δικαιώματα πρόσβασης στους χώρους όπου βρίσκονται οι εφαρμογές και στον SQL Server, χωρίς όμως να έχουν καθεαυτό δικαιώματα πρόσβασης στα ίδια τα αρχεία των εφαρμογών ή στα δεδομένα των Βάσεων Δεδομένων

SQLManagers	AdminShareAccess Developers	Δικαιώματα διαχείρισης των SQL Servers
WebManagers	AdminShareAccess Developers	Δικαιώματα διαχείρισης των IIS servers
WinplatformManagers	Developers DevManagers SqlManagers WebManagers	Δικαιώματα διαχείρισης όλων των εξυπηρετητών εκτός των Domain Controllers
AdminShareAccess		Δικαίωμα πρόσβασης ανάγνωσης στα scripts διαχείρισης
Remote Shadow Users		Δικαίωμα χρήσης του scheduled task που δημιουργεί shadow copies στους Domain Controllers
Remote WinRM Users		Δικαίωμα πρόσβασης στο Windows Remote Management Service των Domain Controllers (χωρίς δικαιώματα διαχείρισης)
Schedulers		Δικαίωμα εκτέλεσης scheduled tasks στους εξυπηρετητές
WebAppsFileAccess		Βασικά δικαιώματα πρόσβασης στους χώρους αποθήκευσης των αρχείων των εφαρμογών, χωρίς όμως να δίνεται πρόσβαση στα ίδια τα αρχεία
DBBackupCreators	AdminShareAccess Schedulers	Δικαιώματα δημιουργίας backups των backups των Βάσεων Δεδομένων στον αντίστοιχο χώρο αποθήκευσης
DBBackupFileAccess		Βασικά δικαιώματα πρόσβασης στους χώρους αποθήκευσης των backups των Βάσεων Δεδομένων, χωρίς όμως πρόσβαση στα ίδια τα backups
DBBackupReaders	DBBackupFileAccess	Δικαίωμα πρόσβασης μόνο για ανάγνωση στα

		backups των Βάσεων Δεδομένων
SQLAgentUsers	SQLServicesUsers	Τα μέλη μπορούν να λειτουργήσουν ως οι χρήστες υπό τους οποίους τρέχει το SQL Agent Service των SQL Servers
SQLAgentUsersDB01	SQLAgentUsers	Μέρος των δικαιωμάτων που απαιτούνται για να λειτουργήσει ως χρήστης του SQL Agent Service στους DB01 και DB02. Χρησιμοποιείται μόνο ως υπερ-group των groups SQLAgentUsersDB01 και SQLAgentUsersDB02
SQLAgentUsersDB02	SQLAgentUsers	Τα μέλη μπορούν να λειτουργήσουν ως οι χρήστες υπό τους οποίους τρέχει το SQL Agent Service του SQL Server στον DB02
SQLMachineAccounts		Δικαιώματα λειτουργίας του Failover Cluster Service των db01 και db02. Μέλη του πρέπει να είναι μόνο τα Machine Accounts db01,db02 και τα εικονικά clustered Machine Accounts DBCLUSTER και SQL-AG-MAIN
SQLServerUsers	SqlServicesUsers	Μέρος των δικαιωμάτων που απαιτούνται για να λειτουργήσει ως χρήστης του SQL Server Service στους DB01 και DB02. Χρησιμοποιείται μόνο ως υπερ-group των groups SQLServerUsersDB01 και SQLServerUsersDB02.
SQLServerUsersDB01	SQLServerUsers	Τα μέλη μπορούν να λειτουργήσουν ως οι χρήστες υπό τους οποίους τρέχει το SQL Server Service του SQL Server στον DB01
SQLServerUsersDB02	SQLServerUsers	Τα μέλη μπορούν να λειτουργήσουν ως οι χρήστες υπό τους οποίους τρέχει το SQL Server Service του SQL Server στον DB02
SqlServicesUsers		Μέρος των δικαιωμάτων που απαιτούνται για να λειτουργήσει ως χρήστης κάποιου service στους DB01 και DB02. Χρησιμοποιείται μόνο ως υπερ-group των groups SQLServerUsers και SQLAgentUsers.

DevMachineUsers		Τα μέλη του μπορούν να έχουν πρόσβαση στον DEV εξυπηρετητή
IISAppConnectAsUsers	WebAppsWorkers	Τα μέλη του μπορούν να λειτουργήσουν ως οι χρήστες με τους οποίους διαβάζουν τα αρχεία των εφαρμογών οι IIS στους web servers
IISImpersonateAsUsers	WebAppsWorkers	Τα μέλη του μπορεί να λειτουργήσουν ως χρήστες με τους οποίους κάνουν Impersonate οι IIS στους web servers
IISPoolIdentities	WebAppsWorkers IISAppConnectAsUsers	Τα μέλη του μπορεί να λειτουργήσουν ως χρήστες υπό τους οποίους τρέχει ένα application pool στους IIS στους web servers
IISSharedConfigAccess		Δικαιώματα πλήρους πρόσβασης στο configuration των IIS στους web servers
WebAppBackupCreators	AdminShareAccess DevManagers Schedulers WebAppsFileAccess	Δικαιώματα ανάγνωσης σε όλα τα αρχεία των εφαρμογών και εγγραφής στον χώρο αποθήκευσης των backups τους
WebAppBackupReaders	WebAppsFileAccess	Δικαιώματα ανάγνωσης στον χώρο αποθήκευσης των backups των αρχείων των εφαρμογών
WebAppsWorkers	WebAppsFileAccess	Μέρος των δικαιωμάτων που απαιτούνται για να λειτουργήσει ένας χρήστης ως ο χρήστης που οι IIS στους web servers κάνουν impersonate ή διαβάζουν τα αρχεία των εφαρμογών ή ως ο χρήστης υπό τον οποίο τρέχει ένα application pool. Χρησιμοποιείται ως υπερ-group των groups IISAppConnectAsUsers, IISImpersonateAsUsers, IISPoolIdentities

Σημειώνεται ότι κάθε group αποκτά το σύνολο των δικαιωμάτων του τόσο από εκχωρήσεις που έχουν γίνει συγκεκριμένα σε αυτό όσο και μέσω της συμμετοχής του σε άλλα group όπως αυτό φαίνεται στον παραπάνω πίνακα. Επίσης η δημιουργία των groups έχει γίνει με βάση το σχεδιασμό της ασφάλειας του συστήματος. Αναλόγως με τις εκάστοτε ρυθμίσεις ενδέχεται κάποια groups να μην έχουν μέλη άρα

κανένας χρήστης να μην έχει τα αντίστοιχα δικαιώματα. Συγκεκριμένα στον παρακάτω πίνακα φαίνονται οι χρήστες συστήματος που έχουν δημιουργηθεί και τα groups στα οποία ανήκουν.

Username	Μέλος των	Περιγραφή
blackman	Administrators Enterprise Admins Schema Admins	Ο default administrator μετονομασμένος
adminScheduler	Domain Admins	Χρησιμοποιείται ως χρήστης για την εκτέλεση scheduled tasks που απαιτούν διαχειριστικά δικαιώματα
dbbackread	DBBackupReaders	Χρησιμοποιείται για από τον OFFSITE server για την αντιγραφή των backups των Βάσεων Δεδομένων μέσω FTP
dbbackupier	DBBackupCreators	Ο χρήστης υπό τον οποίο τρέχει η αυτοματοποιημένη διαδικασία Backup
sqlagentdb01	SQLAgentUsersDB01	Ο χρήστης υπό τον οποίο τρέχει η υπηρεσία SQL Agent στον DB01
sqlagentdb02	SQLAgentUsersDB02	Ο χρήστης υπό τον οποίο τρέχει η υπηρεσία SQL Agent στον DB02
sqlserver	SqlServerUsersDB01 SqlServerUsersDB02	Ο χρήστης υπό τον οποίο τρέχει η υπηρεσία SQL Server στους server DB01 και DB02
ftpadisol	DevMachineUsers	Χρησιμοποιείται από την FTP υπηρεσία στον server DEV ώστε να συνδέεται στο Active Directory και να βρίσκει το home των χρηστών
webdeployadmin	WebManagers	Χρήστης υπό τον οποίο τρέχει το RecycleApp feature του IIS Management Service στους web servers
iisconfig	IISSharedConfigAccess	Ο χρήστης τον οποίο χρησιμοποιούν οι IIS στους web servers για να διαβάζουν το configuration τους

webappbackread	WebAppBackupReaders	Χρησιμοποιείται για από τον OFFSITE server για την αντιγραφή των backups των webapps μέσω FTP
webappbackupier	WebAppBackupCreators	Χρήστης υπό τον οποίο τρέχει η αυτοματοποιημένη διαδικασία δημιουργίας backups των αρχείων των εφαρμογών

Ειδική μέριμνα έχει γίνει για το θέμα της ασφάλειας και της απομόνωσης των web εφαρμογών που εξυπηρετεί η πλατφόρμα καθώς πρόκειται για το πιο εκτεθειμένο κομμάτι.

Κάθε εφαρμογή τρέχει υπό ξεχωριστό application pool, το οποίο με τη σειρά του τρέχει υπό ξεχωριστό χρήστη. Ο χρήστης του application pool δημιουργείται στο Active Directory ώστε να είναι δυνατόν να έχει πρόσβαση στα αρχεία της εφαρμογής που βρίσκονται σε διαφορετικούς servers (DFS). Επιπλέον ο ίδιος χρήστης χρησιμοποιείται για την πρόσβαση στη Βάση Δεδομένων. Με τον τρόπο αυτό αυξάνεται η ασφάλεια του συστήματος καθώς παντού χρησιμοποιείται Kerberos authentication ενώ επιπλέον δεν υπάρχουν clear text passwords στα configuration files της εφαρμογής.

Κάθε εφαρμογή θεωρείται ότι έχει τρία διαφορετικά αντικείμενα πρόσβασης:

1. Τα εκτελέσιμα αρχεία της εφαρμογής, στο φάκελο \\winplatfom.local\webapps\Project-App
2. Τα αρχεία δεδομένων της εφαρμογής, στο φάκελο \\winplatfom.local\webdata\Project-App
3. Τη Βάση Δεδομένων της εφαρμογής.

Επίσης για κάθε εφαρμογή θεωρείται ότι υπάρχουν τρεις πιθανοί τύποι πρόσβασης.

1. Από τον χρήστη υπό τον οποίο τρέχει η εφαρμογή (application pool user).
2. Από χρήστες που είναι υπεύθυνοι για αλλαγές στην εφαρμογή.
3. Από χρήστες που είναι υπεύθυνοι για επίβλεψη και έλεγχο της εφαρμογής.

Για κάθε εφαρμογή και για κάθε τύπο πρόσβασης δημιουργείται ένα νέο group στο οποίο θα πρέπει να προστίθενται οι χρήστες, αντίστοιχα με τα παραπάνω:

1. w-Project-App-Workers
2. w-Project-App-Developers
3. w-Project-App-Readers

Στον ακόλουθο πίνακα φαίνονται τα δικαιώματα που έχει το κάθε group στα αντικείμενα πρόσβασης της εφαρμογής.

	Group Πρόσβασης		
	w-Project-App-Workers	w-Project-App-Developers	w-Project-App-Readers
Αντικείμενο Πρόσβασης			
\\winplatfom.local\webapps\Project-App	Ανάγνωση	Ανάγνωση και Εγγραφή	Ανάγνωση
\\winplatfom.local\webdata\Project-App	Ανάγνωση και Εγγραφή	Ανάγνωση και Εγγραφή	Ανάγνωση
Βάση Δεδομένων Project-App	Ανάγνωση και Εγγραφή	Ανάγνωση και Εγγραφή	Ανάγνωση

Ο χρήστης του application pool μίας εφαρμογής είναι μέλος του group w-Project-App-Workers. Οι developers μίας εφαρμογής γίνονται μέλος είτε του w-Project-App-Developers είτε του w-Project-App-Readers, αναλόγως με τα επιθυμητά δικαιώματα.

Με τον παραπάνω τρόπο επιτυγχάνεται η πλήρης απομόνωση των εφαρμογών καθώς κανένας χρήστης μία εφαρμογής δεν έχει πρόσβαση στη διεργασία, στα αρχεία ή στη Βάση Δεδομένων μία άλλης.