ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΠΜΣ:ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Λογισμικό Καταγραφής Χαρακτηριστικών Δικτύου

Του Βασιλόπουλου Ιωάννη,

Υποψηφίου μ.δ.

Πανεπιστήμιο Πειραιώς

Αθήνα, 2016

Table of Contents

Περίληψη

Στα σύγχρονα εταιρικά δίκτυα γίνεται ολοένα και περισσότερο απαραίτητο ο διαχειριστής τους να γνωρίζει την υπάρχουσα υποδομή σε hardware&software, αλλά και την εισαγωγή νέων. Είναι σημαντική η γνώση της αλληλεπίδρασης μεταξύ όλων των στοιχείων που απαρτίζουν ένα δίκτυο, έτσι ώστε ο διαχειριστής να μπορεί να εκμεταλλευτεί σε βέλτιστο βαθμό τις δυνατότητες της υποδομής του, να εξάγει γρήγορες και επαρκείς αναφορές καθώς και να επιλύει άμεσα βλάβες. Σημαντικότερο , όμως, όλων είναι η πρόβλεψη των προβλημάτων αυτών.

Η γνώση είναι δύναμη και το να γνωρίζεις τι συμβαίνει στο δίκτυο, σου δίνει την δυνατότητα να αποφασίσεις πώς θα είναι αυτό.
Οι κατασκευαστές συνδυάζουν εργαλεία παρακολούθησης δικτύου, packet sniffers και network probes για την παρατήρηση και τον έλεγχο της κίνησης του δικτύου.

Ένα μεγάλο trend της πληροφορικής, αυτή τη στιγμή είναι το Internet of Things (IOT). Είναι ένα αναπτυσσόμενο δίκτυο των καθημερινών αντικειμένων, από τις βιομηχανικές μηχανές έως τα καταναλωτικά αγαθά που μπορεί να μοιράζεται πληροφορίες και να ολοκληρώνει εργασίες ενώ εσείς είστε απασχολημένοι με άλλες δραστηριότητες.

Σκοπός αυτής της εργασίας είναι η μελέτη και ανάδειξη εργαλείων Open Source. Θα παρουσιαστούν οι τεχνολογίες που χρησιμοποιεί το κάθε ένα από αυτά καθώς και τα πλεονεκτήματα ή τα μειονεκτήματά τους. Θα γίνει προσπάθεια εντοπισμού των ελλείψεων και προτάσεις για την βελτίωσή τους.

Σε καμία περίπτωση δεν θα πρέπει να αφήσουμε εκτός και τις Commercial λύσεις στις οποίες επίσης θα γίνει παρουσίαση αλλά και σύγκριση μεταξύ αυτών. Έχοντας πλέον γνώση των δυνατοτήτων ενός commercial προϊόντος, θα μπορεί κάποιος να καταλάβει καλύτερα τις δυνατότητες του open source προγράμματος που θα παρουσιαστεί.

Εισαγωγή

Το Network Inventory είναι ένα πρόγραμμα που μπορεί να εντοπίσει διάφορες συσκευές, όπως υπολογιστές,εκτυπωτές, servers, routers, και άλλες που συνδέονται μεταξύ τους σε ένα δίκτυο. Το πρόγραμμα αυτό μπορεί σε συνέχεια της διαδικασίας ανίχνευσης της δικτυακής συσκευής, να παρέχει και επιπλέον πληροφορίες για αυτήν. Οι λεπτομέρειες που μπορούν να εξαχθούν από μία συσκευή, εξαρτώνται από το πρόγραμμα που χρησιμοποιείται αλλά και από το εάν έχουμε σε αυτό πρόσβαση με δικαιώματα διαχειριστή.

Το network Inventory δεν είναι μια απλή καταγραφή συσκευών, αλλά παράλληλα μπορεί να καταγράφει τι είδους software χρησιμοποιείται σε κάθε συσκευή, τυχόν ενημερώσεις που έχουν εγκατασταθεί, serial numbers και πολλά άλλα.

Ο διαχειριστής ενός δικτύου είναι απαραίτητο να έχει ένα αξιόπιστο εργαλείο network inventory. Για παράδειγμα, εάν γνωρίζει τι τύπου software έχει εγκατεστημένα στο δίκτυο του, θα μπορεί να εξοικονομήσει χρήματα, χρόνο και πολύτιμους πόρους. Επίσης, θα μπορεί να είναι συμβατός με τα πρότυπα της Εταιρείας σε σχέση με παράνομο λογισμικό.

Επίσης, στην περίπτωση που ένας χρήστης αναφέρει πρόβλημα με το λογισμικό που έχει, τότε ο διαχειριστής θα μπορεί να λύσει το πρόβλημα γρηγορότερα, εφ’όσον θα γνωρίζει εάν υπάρχουν εφαρμογές που δεν θα έπρεπε να βρίσκονται εκεί.

Υπάρχει πληθώρα λογισμικών που κάνουν αυτού του τύπου τη δουλειά. Όλα εκτελούν τις βασικές λειτουργίες, όπως το να σαρώνουν το δίκτυο, να συνδέονται πάνω σε συσκευές ή υπολογιστές και να αποστέλλουν τα δεδομένα αυτά με επιτυχία.

Κεφάλαιο 1ο: Το Network Inventory

1.1: Τρόποι λειτουργίας network inventory

Υπάρχουν δύο κύριοι τρόποι συλλογής των στοιχείων: ο πρώτος σχετίζεται με την αναζήτηση των συσκευών με agent scanning και ο δεύτερος λειτουργεί βάσει του τύπου agentless scanner.

Με τον agent scanning, θα πρέπει να εγκατασταθεί ένας agent σε κάποια συσκευή στο δίκτυο και να αποστέλλει δεδομένα στην κεντρική βάση. Έχοντας εγκαταστήσει τον agent δεν χρειάζεται να ανησυχούμε για antivirus προγράμματα ή firewall που μπορεί να βρίσκονται εγκατεστημένα στη συσκευή που ελέγχεται.

Το μειονέκτημα της λύσης αυτής είναι ότι θα πρέπει να εγκαθίσταται σε κάθε υπολογιστή ξεχωριστά, όπως επίσης και να γίνεται αναβάθμιση κάθε νέας έκδοσης του agent.

Οι agentless scanners, από την άλλη, δεν απαιτούν εγκατάσταση στην πλευρά του client αλλά όλα γίνονται από την κεντρική διαχειριστική κονσόλα. Αν το δίκτυο είναι σωστά παραμετροποιημένο, τότε η αναζήτηση είναι πολύ εύκολη. Αντίθετα, θα πρέπει να γίνουν τροποποιήσεις στο firewall του υπολογιστή ή στο antivirus.

1.2: Network Inventory σε απομακρυσμένα δίκτυα

Εάν μία Εταιρεία έχει πολλαπλά απομακρυσμένα δίκτυα και θέλει να έχει γνώση των συσκευών που υπάρχουν σε αυτά, τότε θα πρέπει να υλοποιηθούν remote scanners που θα αναφέρουν στην κεντρική βάση, είτε agentless scanners over VPN. Η δεύτερη λύση είναι σχετικά αργή λόγω σύνδεσης πάνω σε wan γραμμή.

1.3: Η Λειτουργία του Network Inventory

Η κύρια λειτουργία του προγράμματος είναι να παρακολουθεί την τωρινή κατάσταση του δικτύου. Περιοδικά σαρώνει το δίκτυο και αναγνωρίζει νέες συσκευές ή λογισμικά που μπορεί να έχουν προστεθεί ή να έχουν αφαιρεθεί. Ο διαχειριστής δύναται να ειδοποιηθεί για αυτές τις αλλαγές με διάφορους τρόπους και ανάλογα την κρισιμότητα αυτής της αλλαγής.

Επειδή το πρόγραμμα μπορεί να σαρώνει διαφορετικές δικτυακές συσκευές ταυτόχρονα, μπορεί να χρειαστεί να ρυθμιστεί ο αριθμός των αναζητήσεων που «τρέχουν» ταυτόχρονα, καθώς και ο χρόνος που θα γίνονται οι επαναλήψεις μιας αποτυχημένης αναζήτησης.

Κάποιοι τύποι παρακολούθησης του δικτύου είναι και οι ακόλουθοι με τα εξής χαρακτηριστικά:

- TCP port monitoring:

Κατά τον έλεγχο αυτό, το πρόγραμμα προσπαθεί να συνδεθεί σε συγκεκριμένη πόρτα. Αν η σύνδεση είναι επιτυχής τότε και ο έλεγχος έχει ολοκληρωθεί με επιτυχία, σε αντίθετη περίπτωση θεωρείται ότι δεν υπάρχει κάποια ενεργή υπηρεσία που να χρησιμοποιεί την πόρτα αυτή.

- ICMP ping monitoring:

Κατά την διάρκεια αυτού του ελέγχου το πρόγραμμα στέλνει πακέτα ορισμένα από το πρωτόκολλο ICMP στην συσκευή δικτύου.

- DNS monitoring:

Το πρόγραμμα κάνει ερώτημα στον DNS Server και αν αντιστοιχίσει την διεύθυνση domain με την διεύθυνση δικτύου τότε είναι και πάλι επιτυχής.

- ARP monitoring:

Το πρόγραμμα προσπαθεί να ανιχνεύσει την MAC address του μηχανήματος αν ταιριάζει με αυτή που έχει καταχωρηθεί. Μπορεί να χρησιμοποιηθεί για παρακολούθηση αλλαγών σε mac address.

- SNMP monitoring:

Κατά τον έλεγχο αυτό το πρόγραμμα ελέγχει τις αλλαγές των παραμέτρων, ενεργών συσκευών δικτύου (routers, switches, printers κ.α.) μέσω του πρωτοκόλλου SNMP. Παράμετροι όπως snmpagent,

community string και OID καθορίζουν την επιτυχή σύνδεση στην συσκευή. Παρακάτω θα δούμε εκτενέστερα στο πρωτόκολλο SNMP γιατί είναι από τα πιο κρίσιμα στοιχεία ενός inventory προγράμματος.

- SNMP traps receiving and monitoring
- Switch port monitoring:

Οι συσκευές που είναι συνδεδεμένες σε ένα switch καταγράφονται οι διευθύνσεις MAC σε έναν πίνακα. Αυτός ο πίνακας αντιστοιχίζει σε ποιες πόρτες του switch βρίσκονται οι mac addresses. Με αυτόν το τρόπο αναγνωρίζουμε τις συνδεδεμένες συσκευές.

- WMI monitoring:

Το πρόγραμμα μπορεί να παρακολουθήσει παραμέτρους των Windows με τη χρήση του WMI (Windows Management Instrumentation). Οι υπολογιστές του δικτύου θα πρέπει να παραμετροποιηθούν με τέτοιο τρόπο ώστε να δύνανται να εκτελεστούν απομακρυσμένα WMI queries.

Λαμβάνοντας υπ’όψιν το λήμμα της Wikipedia, το Windows Management Interface (WMI) περιέχει μια σειρά από επεκτάσεις στο Windows Driver Model και προσφέρει μια διεπαφή με σκοπό την απομακρυσμένη παραμετροποίηση και διαχείρηση όλων αυτών των στοιχείων που αποτελούν ένα σύστημα (hardware-software). Το WMI είναι υλοποίηση της Microsoft.

Το WMIεπιτρέπει scripting γλώσσες προγραμματισμού όπως VBScriptκαι Windows Power Shell, για την διαχείριση προσωπικών υπολογιστών Windows και Servers. Υπάρχει προεγκατεστημένο σε όλα τα λειτουργικά από Windows 2000 και μετά.

Σκοπός του WMI

Είναι να οριστούν πρότυπα για ανεξαρτήτου περιβάλλοντος προδιαγραφές, που θα επιτρέψουν την ανταλλαγή πληροφοριών σε εφαρμογές διαχείρισης. Το WM υπαγορεύει πρότυπα διαχείρισης για enterprise περιβάλλοντα ώστε να συνεργάζονται αρμονικά με άλλα πρότυπα όπως τα, Desktop Management Interface (DMI) και το SNMP.

WMI Providers

Από την πρώτη έκδοση του WMIμε τα WindowsNT 4 SP4 και μετά η Microsoft συνεχώς προσθέτει WMI Providers σε κάθε νέα έκδοση του λειτουργικού της.

Συγκεκριμένα, στα Windows 2003 Server η Microsoft προσέθεσε πάνω από 80 WMI Providers, ενώ στην έκδοση Windows 2008 Server, περιλαμβάνει providersγια τον IIS 7, το Power Shellκαι το virtualization.

Λόγω της μεγάλης ανάπτυξης από την Microsofttου WMI και της πληροφορίας που εξάγεται από αυτό, πολλοί Administrators έχουν παράξει διάφορα scripts και αυτόματες διαδικασίες.

Επίσης βλέπουμε ότι πολλές Εταιρείες που ηγούνται στον τομέα των προγραμμάτων διαχείρισης όπως το SCCM, HP OpenView, BMC Software και άλλες, είναι συμβατές με το WMI.

Χαρακτηριστικά του WMI

Αν θελήσει κάποιος να αναπτύξει δικά του WMI provider, το WMI του δίνει αυτή τη δυνατότητα και παρακάτω θα πούμε για τα πλεονεκτήματα.

- Printer monitoring
- FTP monitoring:

Κάποια προγράμματα έχουν την δυνατότητα παρακολούθησης FTPServer. Ο έλεγχος γίνεται με την χρησιμοποίηση των διαπιστευτηρίων του FTP.

- HTTP monitoring:

Άλλο ένα στοιχείο είναι το HTTP monitoring. Το πρόγραμμα συνδέεται σε έναν http serverκαι κατεβάζει ένα αρχείο. Μπορεί να παραμετροποιηθεί να στέλνει alert στον διαχειριστή αν αλλάξει το περιεχόμενο της σελίδας.

- NetBios monitoring:

Ακόμα ένας έλεγχος σωστής mac address γίνεται με την χρήση του πρωτοκόλλου netbios.

- Service monitoring
- Process monitoring

- Installed software audit (monitoring):

Το πρόγραμμα ελέγχει και παρακολουθεί λογισμικό που έχει εγκατασταθεί σε έναν απομακρυσμένο υπολογιστή. Αν προστεθεί η αφαιρεθεί, τότε αποστέλλεται ένα alert στον διαχειριστή.

- Event log monitoring:

Ένα ακόμα χαρακτηριστικό αυτών των προγραμμάτων, είναι και η συλλογή event logs και η ανάδειξη νέων κρίσιμων συμβάντων. Μπορεί να παραμετροποιηθεί ώστε να δείχνει μόνο τα σφάλματα.

- Folder existence monitoring
- File existence monitoring
- File size monitoring
- File date/age monitoring
- Disk space monitoring:

Χρήσιμη πληροφορία σε έναν διαχειριστή, είναι ο ελεύθερος χώρος του δίσκου ενός απομακρυσμένου υπολογιστή. Μπορεί να σταλεί ειδοποίηση στον διαχειριστή αν ο ελεύθερος χώρος μειωθεί κάτω από ένα ορισμένο ποσοστό ή τιμή.

- CPU load/usage monitoring:

Με την χρήση αυτών των χαρακτηριστικών, ένα πρόγραμμα μπορεί να παρακολουθήσει το φορτίο της CPU και της μνήμης. Και εδώ μπορεί να οριστεί ειδοποίηση για το ποσοστό του φορτίου. Επίσης είναι εύκολο να αναγνωριστεί μία υπηρεσία που έχει κολλήσει, απλά παρακολουθώντας την στη διάρκεια του χρόνου.

- Mapped drive monitoring
- External application monitoring
- Java-Script monitoring
- Visual Basic Script monitoring
- MS SQL server monitoring
- MySQL server monitoring
- ODBC database server monitoring

Κεφάλαιο 2ο: Γνωστά Προϊόντα Network Inventory

2.1: Fusion Inventory with GLPI

Το Fusion inventory είναι ένα plugin το οποίο χρησιμοποιεί την πλατφόρμα GLPI για να καταχωρεί τα δεδομένα που στέλνουν οι agents σε αυτό. Οι συσκευές που υποστηρίζονται έως τώρα είναι, υπολογιστές, δικτυακές συσκευές, εκτυπωτές, εικονικοί υπολογιστές και android συσκευές.

Στους εικονικούς υπολογιστές (Virtual machines) υποστηρίζονται οι τεχνολογίες

- VMware vCenter/ESX/ESXi
- Virtualbox
- Libvirt
- Xen
- OpenVZ/Virtuozzo
- Parallels
- LXC
- FreeBSD Jails
- HPVM
- Vserver

Το Fusion Inventory μπορεί να χρησιμοποιηθεί για απομακρυσμένη εγκατάσταση λογισμικού σε Windows, Linux και OSX. Τέλος, άλλο ένα χαρακτηριστικό του είναι η απομακρυσμένη αφύπνιση μέσω δικτύου ενός υπολογιστή (Wake on Lan).

2.2: OpenNMS

Το OpenNMS είναι μία πλατφόρμα δικτυακής διαχείρισης με ευρεία διείσδυση σε μεγάλες εταιρείες και παρόχους
Εκτελεί αναζήτηση δικτυακών συσκευών και ανακαλύπτει τις υπηρεσίες που τρέχουν σε αυτές. Μπορεί να παραλάβει πληροφορίες και συμβάντα από SNMP traps, Syslog ή TL1.

Η πλατφόρμα έχει αρκετούς ελεγκτές υπηρεσιών, όπως από ένα απλό icmp ping, port check, αλλά και παρακολούθηση ιστοσελίδων ή έλεγχο σωστής λειτουργίας του Mail Server.
Τέλος, υποστηρίζει πρωτόκολλα SNMP και JMX.

2.3: Open AudIT

Το Open Audit είναι ένα λογισμικό για network discovery, inventory και audit. Κυκλοφορεί σε δύο εκδόσεις, ανοιχτου κώδικα και enterprise. Από την ιστοσελίδα του κατασκευαστή βλέπουμε ένα διάγραμμα σύγκρισης μεταξύ των δύο εκδόσεων.

FEATURES	COMMUNITY	ENTERPRISE
Network Discovery	YES	YES
Device Audit	YES	YES
Software Audit	YES	YES
Configuration Changes	YES	YES
HW Warranty Status	YES	YES
Multivendor Support	YES	YES
Mobile Device Support	YES	YES
Device Port Auditing	YES	YES
Dashboard	NO	YES
Scheduled Reporting	NO	YES
Reporting Over Time	NO	YES
Advanced Report Filtering	NO	YES
Exclusive Reports	NO	YES
Location Mapping	NO	YES
Scheduled Discovery	NO	YES
Bulk Upload of Discovery Schedule	NO	YES
Product Support	Community Only	Commercial Support
Development Support	NO	YES

Είναι μια πλατφόρμα τόσο για Linux όσο και για Windows. Μπορεί να εξάγει πληροφορίες για το hardware, το software, πληροφορίες για το λειτουργικό σύστημα, ρυθμίσεις ασφαλείας, χρήστες και ομάδες, ρυθμίσεις του IIS, γραφήματα για την χρήση των δίσκων αλλά και αλλαγές στην κατάσταση μίας συσκευής (audit).

2.4: GFI Languard

Το προϊόν της GFI είναι μια ολοκληρωμένη λύση για τους IT’s και Security Administrators καθώς είναι συμβατό με αυστηρούς κανονισμούς συμμόρφωσης (Compliance). Δημιουργεί αυτόματες αναφορές για συσκευές, υπολογιστές, εφαρμογές και υπηρεσίες σε ένα δίκτυο, κάνει

σάρωση για ευπάθειες του δικτύου και εγκαθιστά κρίσιμες ενημερώσεις για την αποτροπή των ευπαθειών.

Μπορεί να εγκατασταθεί σαν διαχειριστής σε όλες τις εκδόσεις των Windows και υποστηρίζει εγκατάσταση ενημερώσεων σε Windows, Linux και MacOS.
Δυνατά σημεία της πλατφόρμας είναι τα:

- Patch management
- Vulnerability assessment
- Network auditing management
- Compliance
- BYOD reporting
- Network discovery
- Third-party software rollout
- Port scanning

2.5:Microsoft Distribution and Asset Management Services SCCM

Η πλατφόρμα της Microsoft είναι μία λύση, η οποία προσφέρει την δυνατότητα διαχείρισης υβριδικών εγκαταστάσεων, δηλαδή, συσκευών που βρίσκονται τόσο στο δίκτυο μιας εταιρείας όσο και στο cloud (Azure, Amazon, κ.α). Οι συσκευές αυτές μπορούν να είναι τόσο σε Windows περιβάλλον όσο και Linux, Vmware και OpenStack.
Μπορεί να συλλέξει, να συσχετίσει και να ενεργήσει σε συμβάντα που παρακολουθεί. Να παρακολουθεί και να ενεργεί αυτοματοποιημένες διαδικασίες. Να δημιουργεί αντίγραφα ασφαλείας τόσο στο περιβάλλον cloud όσο και στο τοπικό δίκτυο (on premise). Τέλος είναι συμβατό με κανονισμούς συμμόρφωσης, ανάλυση κινδύνων, ευπαθειών και επιδιόρθωση αυτών.

2.6: IT Asset Management (ITAM)

Το IT Asset Management, ή αλλιώς και BMC Client Management, είναι ένα προϊόν της BMC Software, η οποία εκτός από το ITAM έχει λύσεις για διαχείριση Cloud, αυτοματοποίηση του φόρτου εργασίας, αυτοματοποίηση του IT, λειτουργίες του IT και του Mainframe.

Συνοπτικά, η πλατφόρμα μπορεί να ανακαλύψει τα αγαθά ενός δικτύου με την χρήση agent ή χωρίς, να δημιουργήσει τοπολογίες και να κάνει μελέτη επιπτώσεων μεταξύ των διαφόρων συστημάτων, εφαρμογών, χρηστών και άλλα. Πιο αναλυτικά, μπορεί να εκτελέσει τα παρακάτω.

- Αναζήτηση και καταγραφή
- Εγκατάσταση λειτουργικού συστήματος και εφαρμογών
- Διαχείριση αδειών χρήσης
- Εγκατάσταση ενημερώσεων
- Διαχείριση συμβάντων
- Συμμόρφωση πολιτικής
- Ασφάλεια συσκευών
- Απομακρυσμένη διαχείριση
- Διαχείριση ενέργειας
- Διαχείριση συσκευών
- Εγκατάσταση εφαρμογών μέσω εργαλείου MyApps.

2.7: Altiris IT Management Suite

Το Symantec Altiris χωρίζεται σε δύο μέρη, την Client Management Suite (Εγκατάσταση, διαχείριση, patching, κ.α.) και το Asset Management Suite.

Προσφέρει ασφαλή επικοινωνία μεταξύ χρηστών Windows και Mac, ανεξαρτήτα το που βρίσκονται. Το επιτυγχάνει με τη χρήση ενός Internet Gateway στην DMZ και ασφαλή επικοινωνία με certificates.

Βασικές δυνατότητες της εφαρμογής είναι

- διαχείριση αγαθών
- Αναζήτηση και καταγραφή
- Εγκατάσταση Λειτουργικού
- Εγκατάσταση ενημερώσεων
- Απομακρυσμένη διαχείριση
- Αναφορές
- Διαχείριση Server
- Διαχείριση Licenses
- Διανομή Software

Μεγάλο πλεονέκτημα όμως αυτής της εφαρμογής είναι το γεγονός ότι ένας κατασκευαστής όπως η Symantec, προσφέρει μια πληθώρα εργαλείων σε έναν Διαχειριστή IT, όπως το Ghost που κάνει συγχρονισμό μεταξύ αρχείων και disk images, ο διαχωρισμός των εργασιών σε διαφορετικούς Διαχειριστές. Για παράδειγμα, ένας Administrator, μπορεί να έχει το δικαιώμα εγκατάστασης ενημερώσεων,

ένας άλλος να κάνει αναζήτηση αγαθών και όλα αυτά κάτω από μια κονσόλα διαχείρισης.

Η συγκεκριμμένη πλατφόρμα μπορεί να βρει όλα τα αγαθά σε ένα δίκτυο. Κάνει αναζήτηση είτε hardware είτε software, διαχείριση κλήσεων υποστήριξης, Service Level Agreement (SLA) και διαχείριση συμβολαίων. Μπορεί τέλος να παρακολουθεί συμβόλαια και πληρωμές ώστε να ενημερώνονται οι χρήστες που είναι υπεύθυνοι.

2.8: AuditWizard

Το AuditWizard σύφωνα με τον κατασκευαστή θέλει πολύ λίγο χρόνο από την λήψη, μέχρι την ολοκλήρωση της εγκατάστασης. Αναγνωρίζει τις συσκευές ενός δικτύου, χρησιμοποιώντας τα διαπιστευτήρια των Windows χάρις στο WMI και το SNMP πρωτόκολλο. Χρειάζεται έναν κοινόχρηστο φάκελο όπου βρίσκεται ένα logon script το οποίο εγκαθίσταται στους Η/Υ και ταυτόχρονα αποθηκεύονται εκεί τα αποτελέσματα αυτού.
Οι δυνατότητες αυτού του εργαλείου είναι

- Αναζήτηση και καταγραφή
- Διαχείριση αγαθών (hardware & software)
- Παρακολούθηση συμβάντων
- Αναφορές
- Παρακολούθηση χρήσης internet

2.9: Nagios XI – Nagios Core

Το Nagios χωρίζεται σε δύο άδειες, την εμπορική, Nagios XI και την ανοιχτου κώδικα Nagios Core.

Εγκαθίσταται σε περιβάλλον Linux και μπορεί να υποστηρίξει δίκτυα μικρών όσο και μεγάλων επιχειρήσεων. Η εγκατάσταση του είναι απλή και εύκολη, αλλά η παραμετροποίηση είναι πολύ χρονοβόρα, καθώς αποτελείται από πολλά αρχεία παραμετροποίησης και πρόσθετα.

Ακόμα, ένα πρόσθετο της εφαρμογής είναι η αυτόματη επανεκκίνηση εργασιών ή υπηρεσιών που έχουν σταματήσει ή αποτύχει.
Υποστηρίζει μεταξύ άλλων

- Σύνδεση με συστήματα Help Desk
- Παρακολούθηση δικτύου
- Παρακολούθηση εφαρμογών και υπηρεσιών

- Παρακολούθηση hardware συσκευών (routers, firewalls)
- Αναφορές
- Ειδοποιήσεις μέσω email, μυνήματων κ.α.

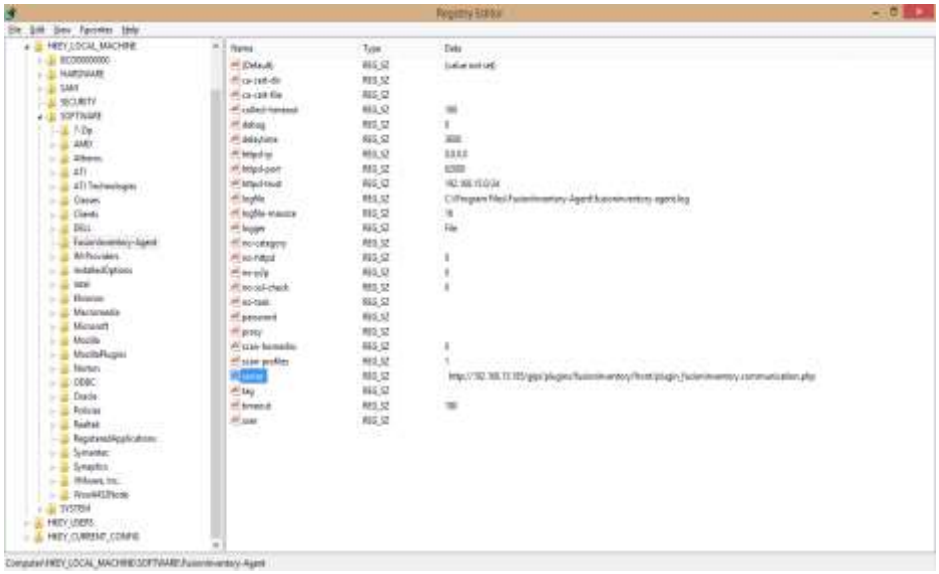
Μειονέκτημα αυτής της πλατφόρμας είναι ότι για κάθε συσκευή χρειάζεται ξεχωριστή παραμετροποίηση, καθώς δεν υποστηρίζει αυτόματη αναζήτηση και καταγραφή.

Κεφάλαιο 3ο: Εγκατάσταση Fusion Inventory

Η πτυχιακή εργασία ξεκίνησε με την υλοποίηση του Fusion Inventory. Είναι ένα plugin που εγκαθίσταται στην πλατφόρμα GLPI. Είναι μια ολοκληρωμένη λύση για αναζήτηση και καταγραφή συσκευών, διαχείριση κλήσεων για Help Desk, διαχείριση αδειών χρήσης (ITIL), διαχείριση συμβολαίων και άλλα.

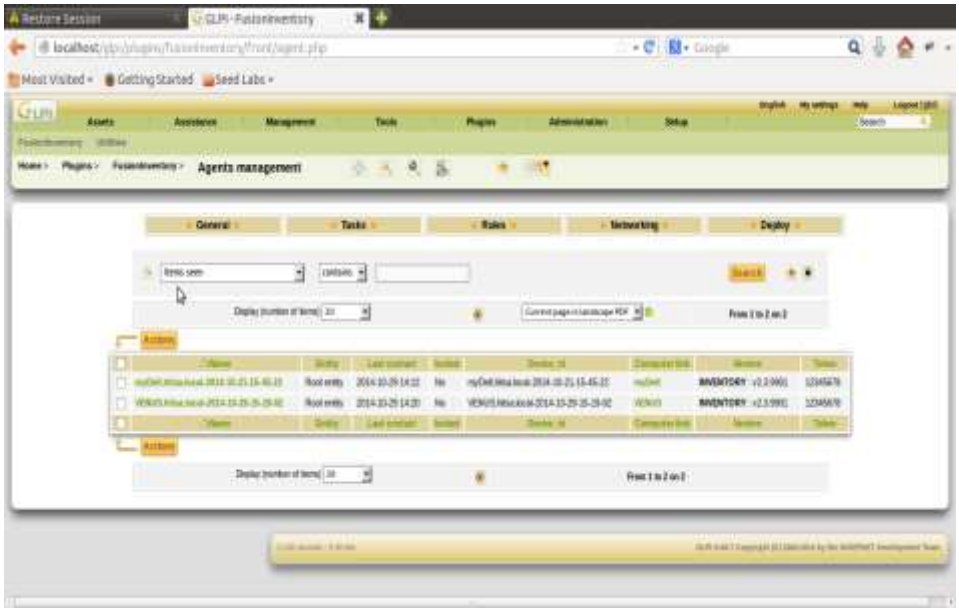
Η εγκατάσταση μπορεί να γίνει σε Windows ή και Linux μέσω της πλατφόρμας XAMPP. Προαπαιτούμενα είναι η ύπαρξη των PHP, MySQL και Apache Web Server. Αφού γίνει η εγκατάσταση του GLPI, το Fusion Inventory εγκαθίσταται ως πρόσθετο (plugin).

Επόμενο βήμα είναι η εγκατάσταση των agents σε όλα τα επιλεγμένα συστήματα Windows ή Linux. Αυτό χρησιμεύει αρχικά για την αναζήτηση των συσκευών σε ένα δίκτυο και στη συνέχεια αφού βρεθούν οι οντότητες πάλι οι agents θα παίξουν τον ρόλο της συλλογής των δεδομένων από τις συσκευές, σύμφωνα με τα στοιχεία σύνδεσης που τους έχουν δοθεί.

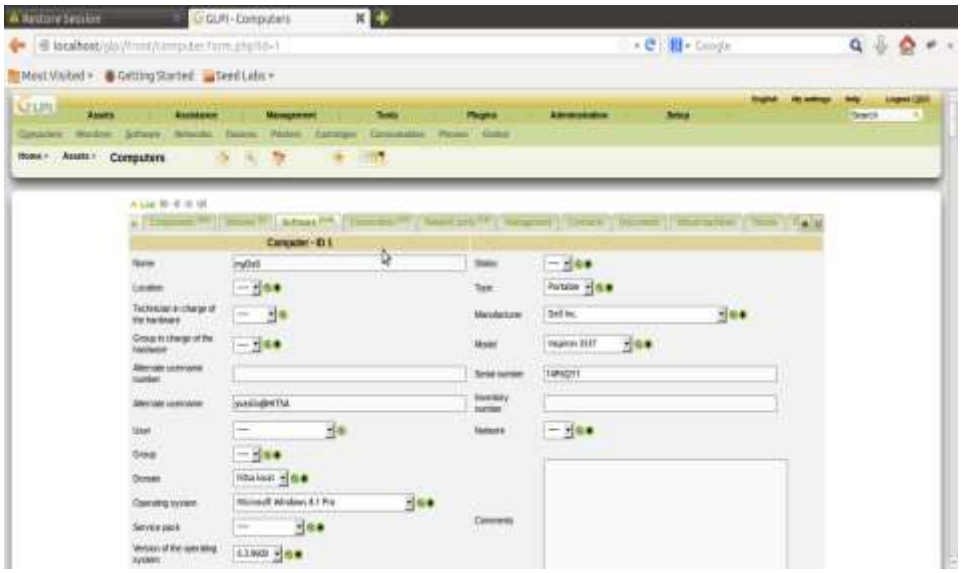


Εικ. 3.1: Εγκατάσταση και παραμετροποίηση agent

Η εγκατάσταση ενός agent όμως δίνει πληροφορίες και για την ίδια συσκευή που είναι εγκαταστημένος.



Εικ. 3.2: Agents



Εικ. 3.3: Αναλυτικές πληροφορίες

Η καταχώρηση των συσκευών γίνεται είτε με την εγκατάσταση agents είτε μέσω SNMP πρωτοκόλλου. Μειονέκτημα της εφαρμογής η έλλειψη WMI διασύνδεσης.

Η συγκεκριμένη λύση εγκαταλήφθηκε, γιατί στην επόμενη έκδοση της εφαρμογής παρουσίαζε αστάθειες.

Εικ. 3.4: Εγκατεστημένα software

Κεφάλαιο 4ο:Εισαγωγή στη λειτουργία του Spiceworks

4.1: Εισαγωγή

Η Εταιρεία ιδρύθηκε το 2006 από τους Scott Abel, Jay Hallberg, Greg Kattawar, και Francis Sullivan για την υλοποίηση προγράμματος διαχείρισης IT.

Το Spiceworks είναι μία κοινότητα από χρήστες οι οποίοι ανταλλάσουν προϊόντα και υπηρεσίες σχετικές με το IT. Το δίκτυο αποτελείται αυτή τη στιγμή από 6 εκατομμύρια επαγγελματίες IT και 3000 προμηθευτές τεχνολογίας.

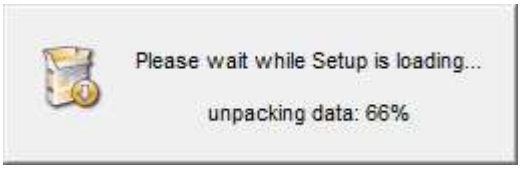
Το πρόγραμμα είναι γραμμένο σε Ruby και λειτουργεί αποκλειστικά σε Windows πλατφόρμα. Το πρόγραμμα περιλαμβάνει, επίσης, λειτουργίες Help Desk, γνωσιακής βάσης δεδομένων, παρακολούθησης δικτύου όπως και την αναζήτηση και καταγραφή συσκευών. Ακόμα, συνεργάζεται με τρίτα προγράμματα, όπως το Alien vault για vulnerability assessment και το Manage Engine patch management για εγκατάσταση κρίσιμων ενημερώσεων.

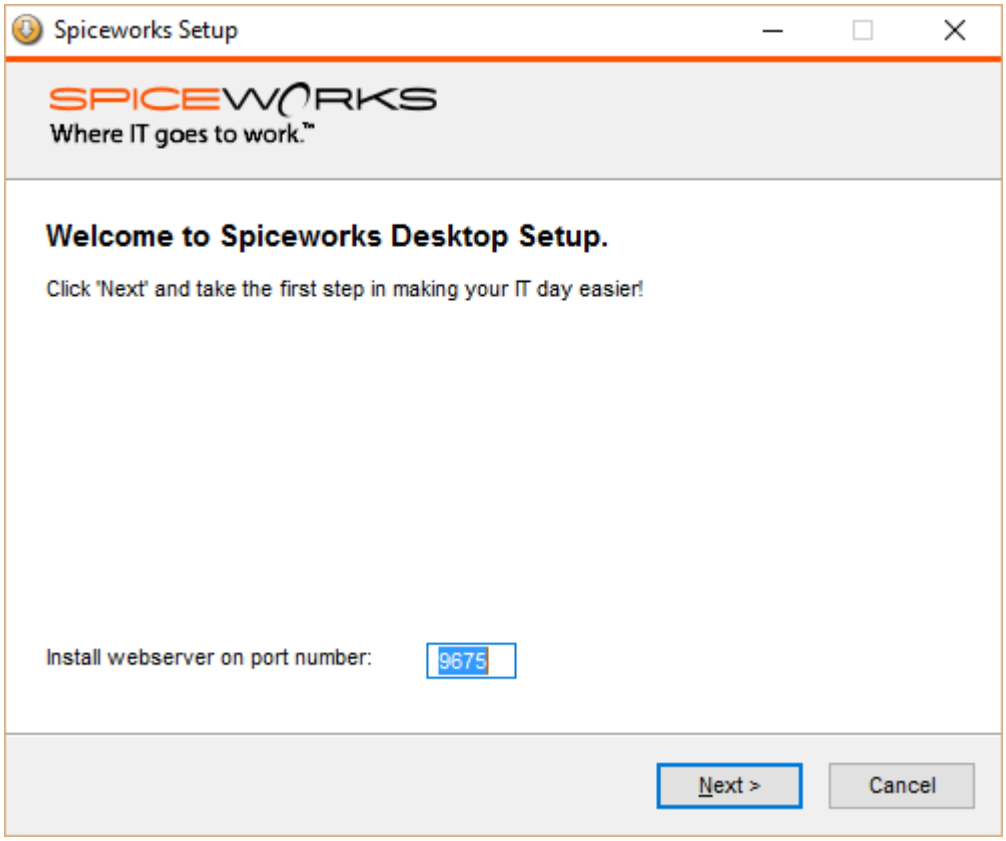
4.2: Κύρια μέρη & Εγκατάσταση Spiceworks

Το Spiceworks αποτελείται από τον εξυπηρετητή, την βάση δεδομένων, τους agents και τα επιπρόσθετα στοιχεία.

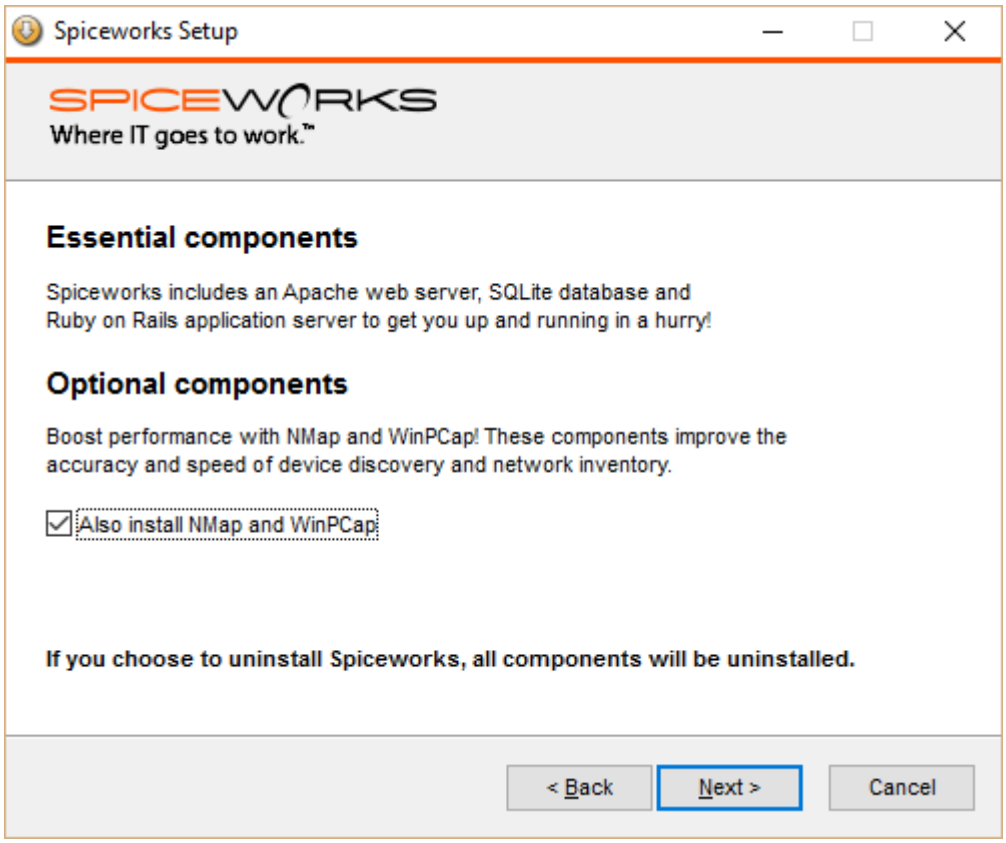
Για την λήψη του προγράμματος θα χρειαστεί να γίνει μία εγγραφή στην ιστοσελίδα του. Αυτή γίνεται με το email, το λογαριασμό του Facebook ή του Linkedin.

Όπως αναφέρθηκε και προηγουμένως, η εφαρμογή εγκαθίσταται σε Windows λειτουργικά συστήματα. Η εγκατάσταση είναι πολύ απλή και φαίνεται στα παρακάτω βήματα.

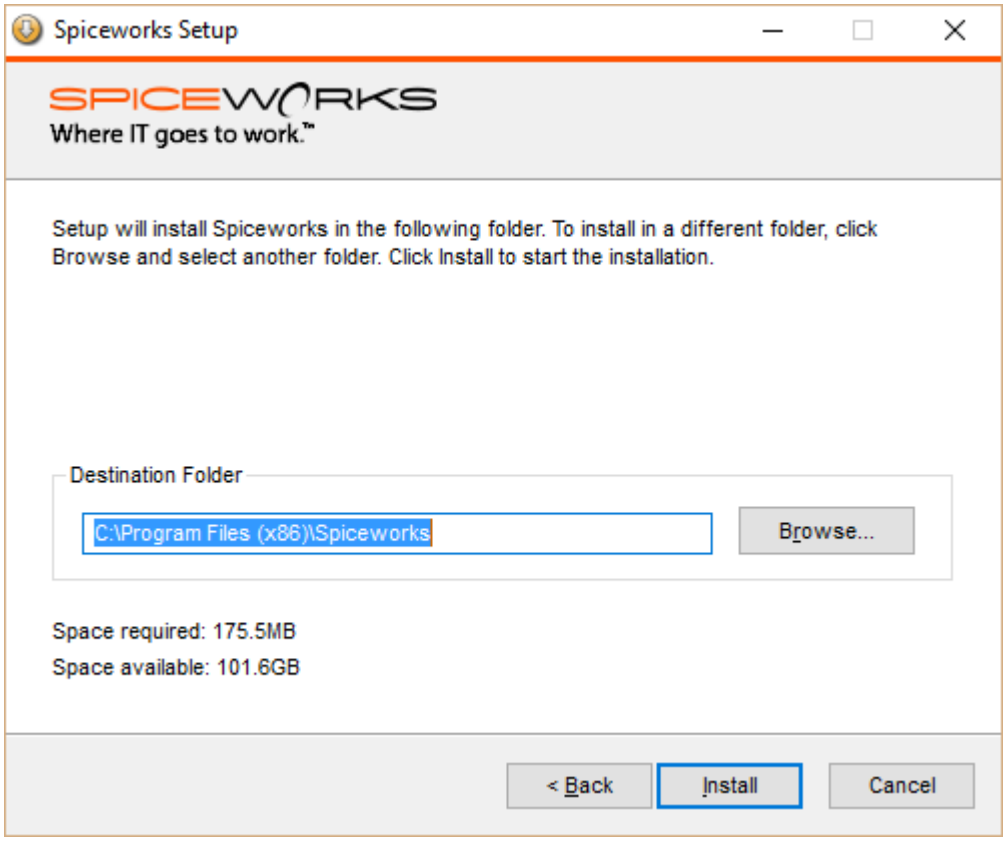




Εικ. 4.1: Δήλωση της πόρτας που θα χρησιμοποιεί ο Webserver



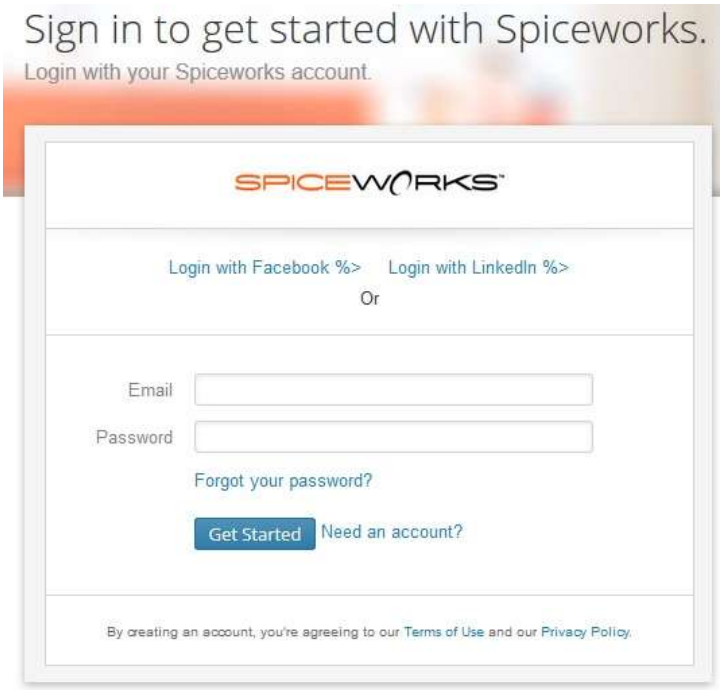
Εικ. 4.2: Εγκατάσταση εργαλείων Nmap και WinPCap



Εικ. 4.3: Εγκατάσταση

Μετά την ολοκλήρωση της εγκατάστασης, ερωτώμαστε αν θα πραγματοποιήσουμε εκκίνηση του εξυπηρετητή. Σε θετική απάντηση, εμφανίζεται κάτω δεξιά στην περιοχή ειδοποιήσεων (system tray). Κάνοντας διπλό κλικ στο εικονίδιο της εφαρμογής μας ζητάει να εισάγουμε τα στοιχεία σύνδεσης. Μπορούν να χρησιμοποιηθούν τα στοιχεία που δηλώθηκαν κατά την διαδικασία εγγραφής.

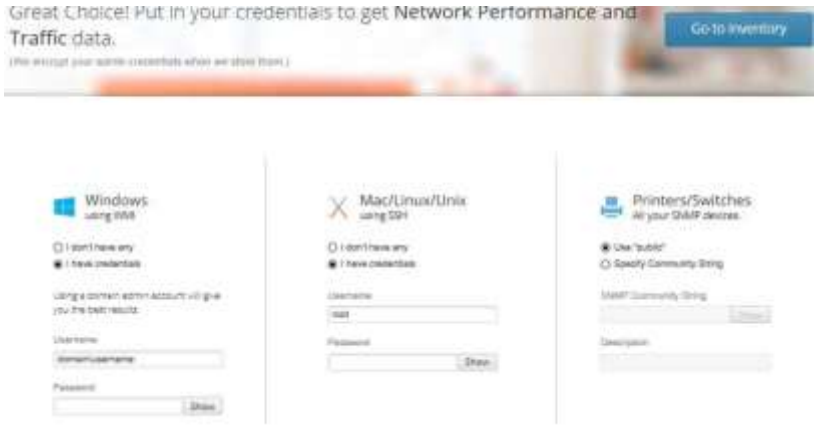
Πρέπει να επισημανθεί ότι παρόλο που χρησιμοποιείται λογαριασμός email ή κοινωνικού δικτύου, αν εγκατασταθεί η εφαρμογή σε άλλο δίκτυο με τα ίδια στοιχεία σύνδεσης, δεν μεταφέρονται οι πληροφορίες στην καινούρια εγκατάσταση, παρά μόνο αν χρησιμοποιείται ως agent. Αυτό όμως θα παρουσιαστεί παρακάτω στο κείμενο.



Εικ. 4.4: Οθόνη εισόδου

Επόμενο βήμα μετά την είσοδο είναι η ερώτηση εκ μέρους της εφαρμογής τι θέλει ο διαχειριστής να πραγματοποιήσει κατά την εκκίνηση. Είναι αυτονόητο ότι έχει την δυνατότητα να κάνει τα παρακάτω σε μεταγενέστερο χρόνο. Οπότε δεν περιορίζεται από την αρχική επιλογή.

Εικ. 4.5: Εικ. Ερώτηση παραμετροποίησης



Εικ. 4.6: Εικόνα διαπιστευτηρίων

Κατά την εκκίνηση της εφαρμογής χρησιμοποιείται το εργαλείο Nmap για την ανίχνευση των συσκευών του δικτύου. Επομένως, θα πρέπει να οριστούν τα στοιχεία σύνδεσης των συσκευών, όπως φαίνεται στην παραπάνω εικόνα.

Για τα λειτουργικά συστήματα και εφόσον η εγκατάσταση γίνεται σε τομέα, θα χρησιμοποιηθεί ο λογαριασμός ενός διαχειριστή του τομέα με την χρήση του WMI πρωτοκόλλου. Για λειτουργικά συστήματα linux και Unix με το SSH ενώ για ενεργές συσκευές όπως router, switch και printer, θα χρησιμοποηθεί το πρωτόκολλο SNMP. Εδώ προτείνεται η χρήση ενός κοινού ονόματος σε αυτές τις συσκευές (η default ονομασία είναι το public).

Αξίζει να αναφερθεί πως έχοντας τα διαπιστευτήρια του διαχειριστή τομέα, κάνει αναζήτηση στους υπολογιστές και στους χρήστες του Active Directory.

Για μεγαλύτερη επιτυχία στην αναζήτηση καλό είναι να γίνουν ορισμένες παραμετροποιήσεις πριν την εκκίνηση της αναζήτησης.
Για Windows λειτουργικά, θα πρέπει να εξαιρεθεί από το τείχος προστασίας η απομακρυσμένη διαχείριση μέσω του WMI. Αν υπάρχει διαχείριση μέσω Active Directory, τότε η πολιτική μπορεί να υλοποιηθεί μαζικά σε όλους τους υπολογιστές, ειδάλλως σε περίπτωση ομάδας εργασίας θα πρέπει να γίνει ξεχωριστά σε κάθε υπολογιστή.

- **ICMPv4 Inbound and Outbound** - This is needed so that Spiceworks can discover the devices on your network; it is more commonly known as the PING command. There are a number of types of ping commands that can be permitted or blocked by various firewalls. Generally, you will want to permit commands 0, 3, 8 and 11.

- **TCP Ports 135 and 445 Inbound** - This is needed for Windows Management Instrumentation (WMI) which Spiceworks uses to get detailed information about Windows computers.
- **UDP Port 137 Inbound** - This is needed so that Spiceworks can gather information from the Windows Registry.

  To manually configure the firewall, use these two commands:

- c:\> netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
- c:\> netsh advfirewall firewall set rule group="remote administration" new enable=yes

Για το SNMPπρωτόκολλο η παραμετροποίηση μιας κοινής συσκευής Cisco γινεται με τον παρακάτω τρόπο.

Router(config)# **snmp-server view** view-name oid-tree {**included** | **excluded**}

Router(config)# **snmp-server community***string* [**view***view-name*] [**ro** | **rw**] [*number*]

Router(config)# **snmp-server engineIDlocal***engineid-string*

Router(config)# **snmp-server engineIDremote***ip-address* [**udp-port***port-number*] *engineid-string*

Router(config)# **snmp-server group**[groupname {**v1** | **v2c** | **v3** [**auth** | **noauth** | **priv**]}][**read**readview] [**write** writeview] [**notify** notifyview] [**access** access-list]

Router(config)# **snmp-server host** host-id [**traps** | **informs**][**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] community-string [**udp-port** port-number] [*notification-type*]

Router(config)# **snmp-server user** username*groupname* [**remote***ip-address* [**udp-port**port]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** access-list]

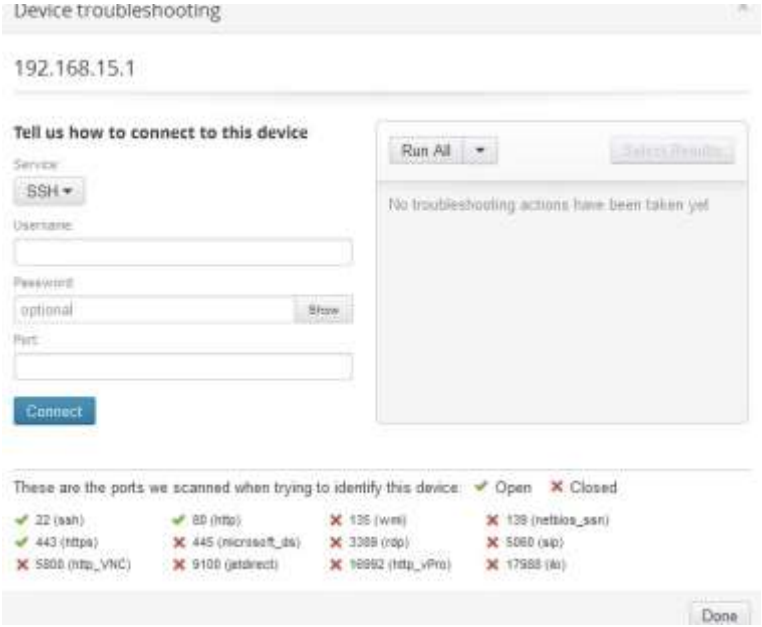
Αναλυτικές οδηγίες και εξηγήσεις για τα παραπάνω στις παραπομπές.

Εικ. 4.7: Πρόοδος αναζήτησης

Αφού ολοκληρωθεί η αναζήτηση, τότε η εφαρμογή μάς ενημερώνει για τα αποτελέσματα αυτής. Για τις συσκευές που έχει αναγνωρίσει μας δίνει τις πληροφορίες που έχει συλλέξει για αυτές αλλά και την αλληλεπίδρασή τους στο δίκτυο. Για τις συσκευές, όμως, που δεν κατάφερε να αναγνωρίσει, προτείνει να αλλαχθεί ο τρόπος αυθεντικοποίησης.

Ανάλογα την συσκευή και σε τι περιβάλλον λειτουργεί, ποικίλουν οι τρόποι διασύνδεσης. Μπορεί να είναι σύνδεση με στοιχεία πιστοποίησης για Windows (σε περίπτωση που ένας υπολογιστής ανήκει σε ομάδα εργασίας και όχι σε τομέα), τα διαπιστευτήρια SSH σε Linux λειτουργικό ή ακόμα διαπιστευτήρια SNMP εφόσον η αναζήτηση έχει υποδείξει ότι μπορεί να χρησιμοποιηθεί.

Μετά την σωστή υπόδειξη η αναζήτηση ξεκινά για την συσκευή ή τις συσκευές που διορθώθηκε ο τρόπος σύνδεσής τους.

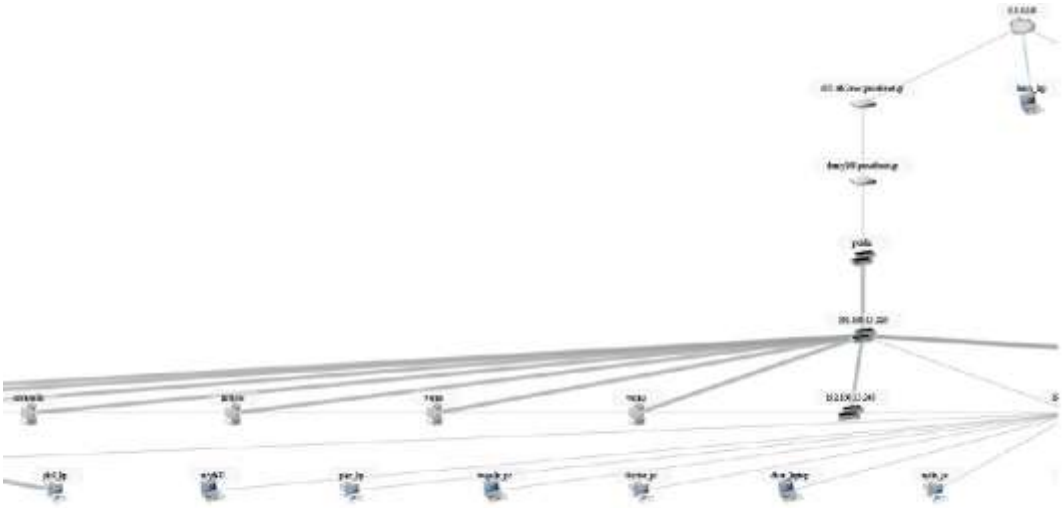


Εικ. 4.8: Αλλαγή αυθεντικοποίησης

4.3: Συλλογή δεδομένων

Αφού έχει ολοκληρωθεί η αναζήτηση, είναι η ώρα πλέον να αναλυθούν τα αποτελέσματα αυτής. Το εργαλείο για την προβολή της τοπολογίας του δικτύου μας δίνει μια εικόνα για το πως είναι δομημένο

ένα δίκτυο. Μπορεί να αναδείξει όλες τις λεπτομέρειες και το πως είναι συνδεδεμένες μεταξύ τους οι συσκευές.



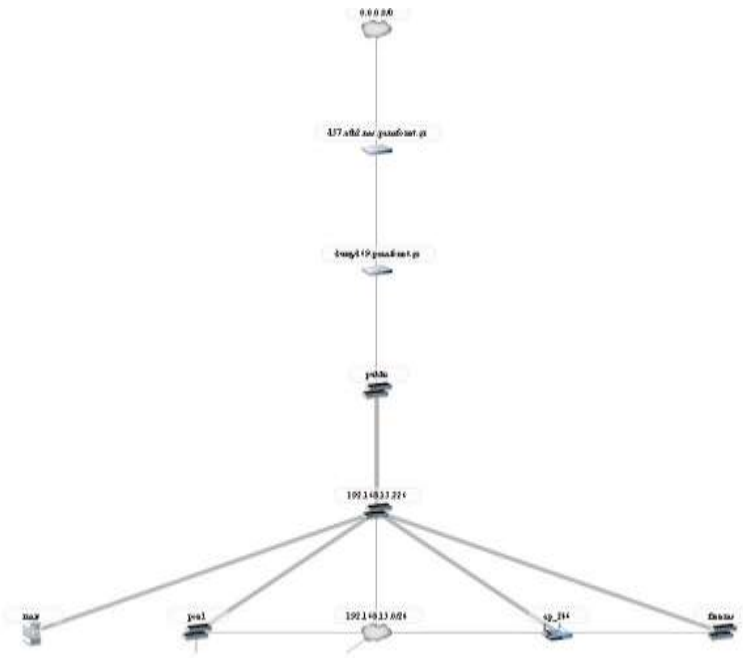
Εικ. 4.9: Τοπολογία δικτύου

Από την παραπάνω εικόνα μπορεί να παρατηρηθεί ο τρόπος σύνδεσης των συσκευών ενός δικτύου.

Στην εικόνα, παρουσιάζεται το κεντρικό Switch, οι Servers που συνδέονται σε αυτό με τα ονόματά τους, όπως επίσης και ένα access point. Πάνω σε αυτό, συνδέονται ασύρματα οι υπολογιστές του δικτύου. Τέλος η ραχοκοκαλιά (backbone) του δικτύου συμπληρώνεται με την παρουσία του κεντρικού Firewall και τον δρομολογητή προς το διαδίκτυο. Στην προκειμένη περίπτωση, η σύνδεση στο διαδίκτυο γίνεται μέσω του παρόχου Vodafone (χαρακτηρίζεται από το σύννεφο 0.0.0.0).

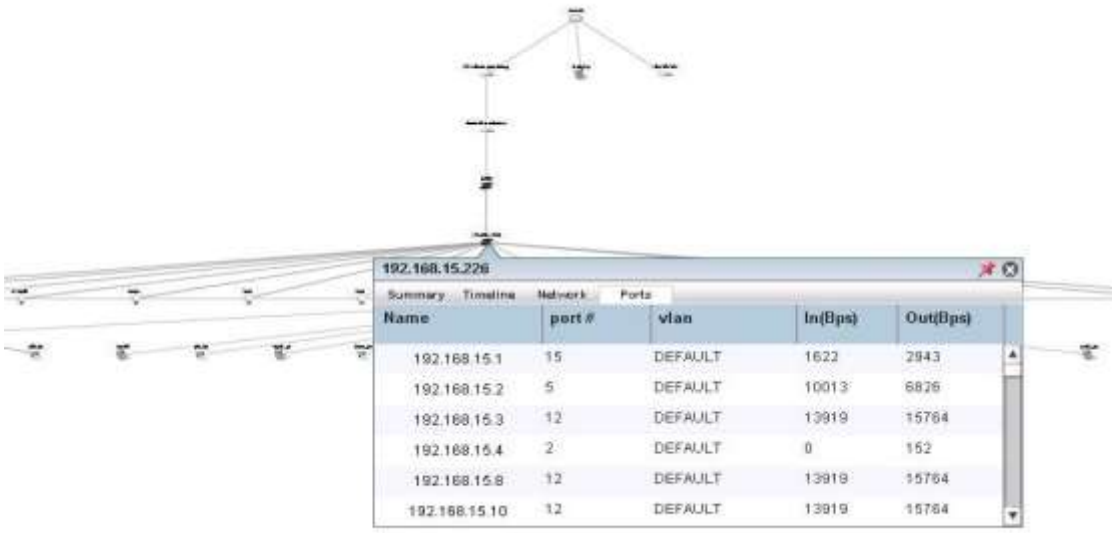
Η τοπολογία του δικτύου βοηθά στην κατανόηση της εγκατάστασης αλλά και στην επίλυση προβλημάτων που έχουν να κάνουν είτε με διακοπή κάποιας υπηρεσίας ή προβλήματα πιστοποίησης με τις κεντρικές υπηρεσίες.

Στην παρακάτω εικόνα έχουν απομονωθεί οι ενεργές συσκεύες του δικτύου και είναι πιο εύκολο να κατανοηθεί η δομή ενός Backbone. Από το κεντρικό switch, το Firewall, τα access points, αλλά και την όδευση προς το διαδίκτυο.



Εικ. 4.10: Backbone

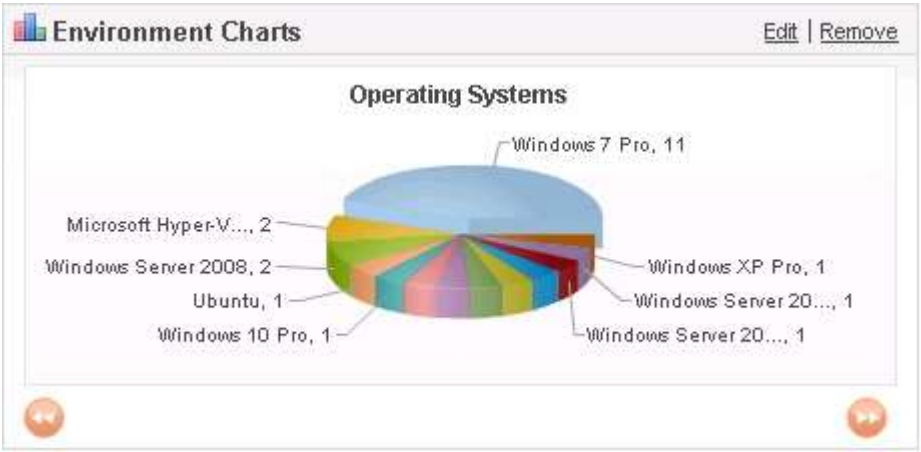
Στην παρακάτω εικόνα φαίνονται οι συσκευές βάσει της IP διεύθυνσης σε ποια πόρτα του κεντρικού Switch είναι συνδεδεμένες. Παρατηρείται ότι στην 12 πόρτα είναι τρεις συσκευές. Αυτό σημαίνει ότι πιθανόν είναι εικονικές συσκευές (Virtual machines) και μοιράζονται την ίδια κάρτα δικτύου του Server, ή η πόρτα αυτή συνδέεται σε κάποιο unmanaged switch.



Εικ. 4.11: CoreSwitch

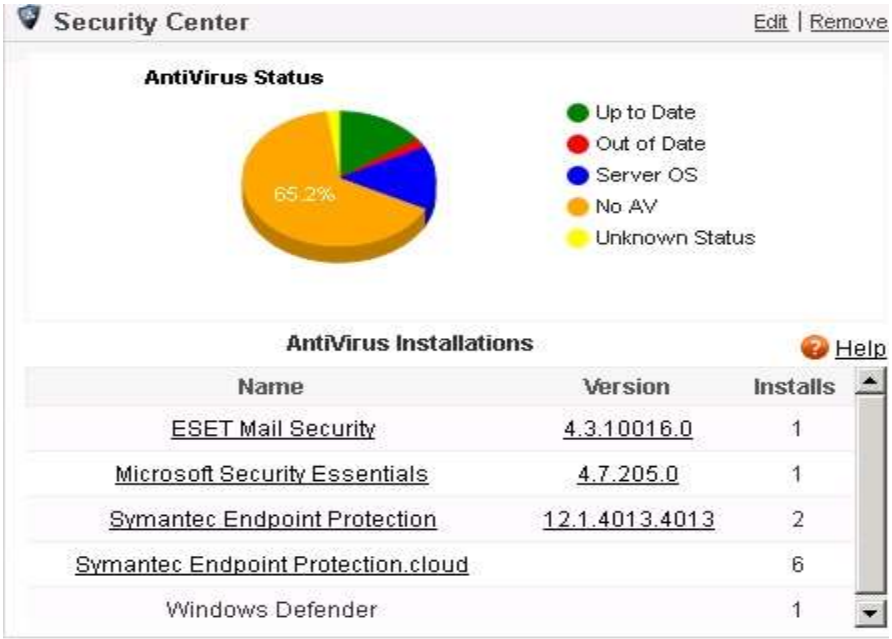
4.4: Χρήσιμες πληροφορίες

Στις επόμενες εικόνες φαίνονται καλύτερα οι δυνατότητες της εφαρμογής σε σχέση με την κατανόηση των περιεχομένων του δικτύου. Μέσω πινάκων παρατηρούνται τα ποσοστά λειτουργικών συστημάτων στο δίκτυο, αλλά και η προστασία αυτών από αντιϊκά προγράμματα.



Εικ. 4.12: Λειτουργικά συστήματα

Με αυτόν τον τρόπο είναι εύκολο να προγραμματιστεί η αλλαγή λειτουργικού σε εκτός ορίου ζωής (EOL) λειτουργικών προγραμμάτων. Π.χ. Τα Windows XP έχουν γίνει EOL από την άνοιξη του 2014, ενώ τα Windows 2003 Server από το καλοκαίρι του 2015.

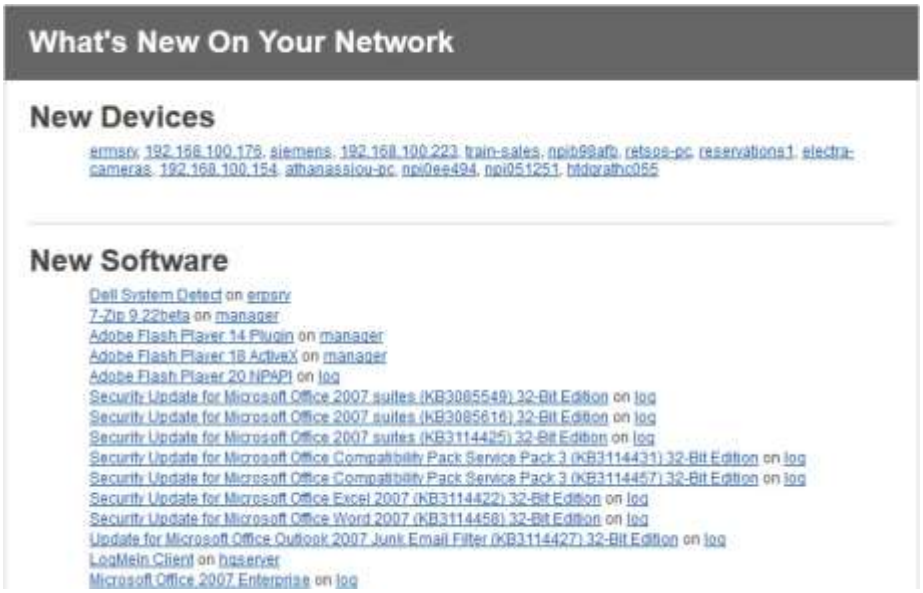


Εικ. 4.13: Antivirus

Παρομοίως, από την παραπάνω εικόνα φαίνονται όχι μόνο τα ποσοστά εγκατεστημένων αντιϊκων προγραμμάτων, αλλά και το ποσοστό αυτών που είναι ενημερωμένα ή όχι.

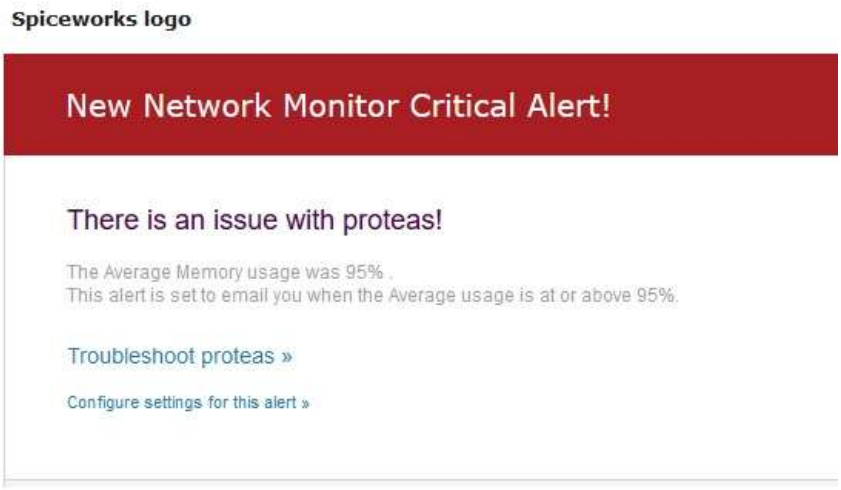
Κεφάλαιο 5ο: Alerts

Μία κρίσιμη λειτουργία της εφαρμογής, είναι η ενεργοποίηση των ειδοποιήσεων (alerts) προς τον υπεύθυνο του Δικτύου. Ορισμένα alerts περιγράφονται παρακάτω.



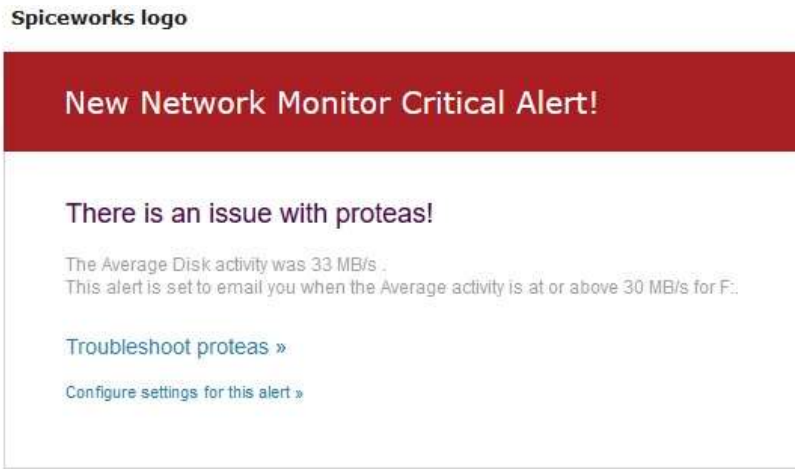
Εικ. 5.1: Ειδοποίηση για νέα συσκευή

Στην παραπάνω εικόνα φαίνεται η ειδοποίηση που στέλνει η εφαρμογή στον υπεύθυνο του Δικτύου, για την εγκατάσταση ή αναγνώριση νεου υλικού (hardware και software) που αναγνωρίστηκε κατά τον περιοδικό έλεγχο του agent.



Εικ. 5.2: Memory Alert

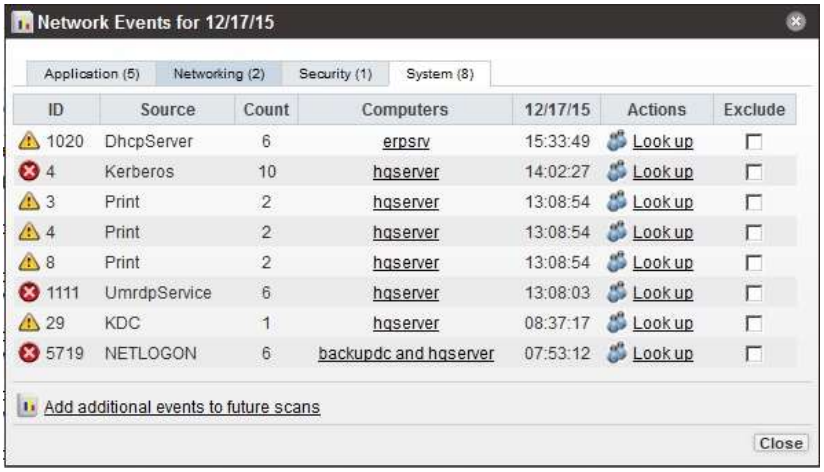
Μία ακόμη ειδοποίηση αφορά την επίβλεψη του Server,αν έχει υπερβεί το όριο που έχει τεθεί κατά την παραμετροποίηση, του ποσοστού κατειλημμένης μνήμης από τις υπηρεσίες που ‘‘τρέχουν’’ σε αυτόν.



Εικ. 5.3: Alert for disk activity

Στην παραπάνω εικόνα, φαίνεται η ειδοποίηση για την υπέρβαση του ορίου για τον μέσο όρο δραστηριότητας του δίσκου.

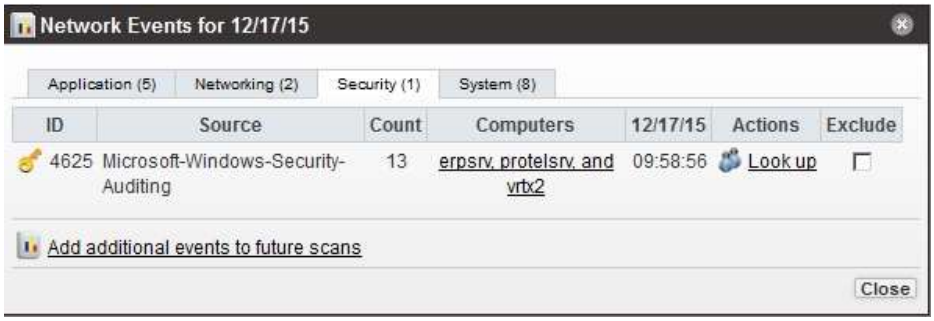
Βάζοντας τέτοιους κανόνες δύναται να παρακολουθείται το σύνολο του δικτύου και των υπηρεσιών του με ευκολία από τον διαχειριστή. Γνωρίζοντας αυτός πόσα από αυτά είναι false negative ή false positive μπορεί να αυξομειώνει τα όρια για να πετύχει τη βέλτιστη απόδοση των συστημάτων του.



Εικ. 5.4: Συμβάν συστήματος

Στην εικόνα 5.4 , φαίνονται συμβάντα κρίσιμα ή προειδοποιήσεις των Windows. Για παράδειγμα το Netlogon λάθος έχει συμβεί στους δύο

Domain Controllers του δικτύου. Αυτό σημαίνει ότι κάποιος χρήστης ή συσκευή έκανε ανεπιτυχή προσπάθεια εισόδου στο Domain. Ένα άλλο λάθος είναι ότι κάποιος χρήστης πήρε απομακρυσμένη πρόσβαση στον Server (μήνυμα λάθους UmrdpService), χωρίς αυτός να έχει εγκατεστημένο όλους του drivers των εκτυπωτών του χρήστη.



Εικ. 5.5: Συμβάν ασφάλειας

Ένα ακόμα συμβάν αναφέρεται στην εικόνα 5.5 και απεικονίζει την προσπάθεια σύνδεσης από κάποιον λογαριασμό, σε ορισμένους Servers. Πατώντας στο κουμπί Lookup οδηγεί στο Community του Spiceworks και δίνονται επεξηγήσεις περί του λάθους. Στο συγκεκριμμένο μήνυμα είναι τα εξής:

This event indicates that some attempted to log into an account, but the login failed due to an incorrect username or password.

Note looked up this is for Exchange not a problems on exchange server

Συνεχίζοντας στις δυνατότητες τις εφαρμογής, μας δίνει την πληροφόρηση για τις εγκατεστημένες εφαρμογές, με άδεια ή χωρίς, πότε αυτές έγιναν, αν εγκαταστάθηκαν ως υπηρεσίες κ.α. Πιο σημαντικό όμως είναι να αναδειχτούν ποιες από αυτές είναι ανεπιθύμητες.

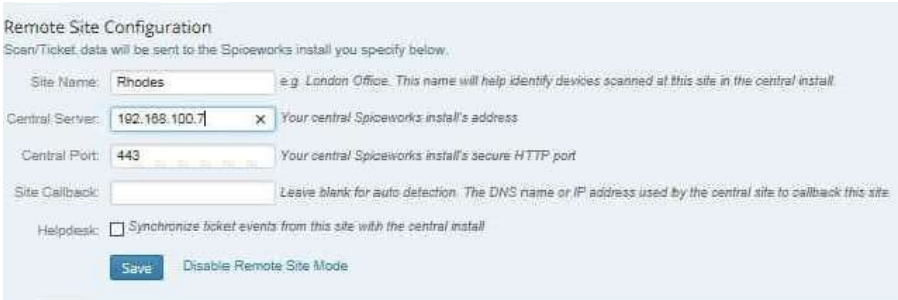
Εικ. 5.6: Ανεπιθύμητες εφαρμογές

Όπως παρατηρείται, ένας μεγάλος αριθμός ανεπιθύμητων προγραμμάτων αποτελείται από εργαλειοθήκες των περιηγητών ιστοσελίδων (browsers). Με αυτή την πληροφόρηση ο Διαχειριστής, μπορεί εύκολα να δημιουργήσει κανόνες για την αποτροπή εγκατάστασης αυτών των εργαλειοθηκών.

Κεφάλαιο 6ο: Απομακρυσμένη Τοποθεσία

Μία ακόμα λειτουργία που πρέπει να έχει ένα πρόγραμμα παρακολούθησης και ελέγχουν, είναι η δυνατότητα να ενσωματώνει απομακρυσμένα δίκτυα με την χρήση διαφόρων μέσων (agents). Η εγκατάσταση είναι κεντρικοποιημένη και οι αναφορές του συστήματος περιλαμβάνουν την πληροφορία για την υποδομή της Εταιρείας σε όποιο υποκατάστημα συνδέεται με τα Κεντρικά.

Εδώ αξίζει να αναφερθεί, ότι στην συγκεκριμένη περίπτωση δεν χρειάζεται η σύνδεση VPN μεταξύ των δύο σημείων, αλλά μπορεί να επιτευχθεί τοποθετώντας τον κεντρικό Server στην αποστρατικοποιημένη ζώνη (DMZ). Κατά την σύνδεση του απομακρυσμένου agent ορίζεται η δημόσια IP διεύθυνση και πόρτα του Server Spiceworks.



Εικ. 6.1: Απομακρυσμένο δίκτυο

Κεφάλαιο 7ο : Πρόσθετα – Plugins

Η πλατφόρμα Spiceworks μπορεί να δεχθεί πρόσθετα ανοιχτού κώδικα. Ένα από αυτά που θα περιγραφεί είναι η παρακολούθηση και επέμβαση πάνω σε Windows Service. Επειδή πολλά Service των Windows σταματούν λόγω ενός λάθους στον κώδικα ή γιατί απλά ‘έπεσε’, ο Διαχειριστής θέλει να έχει γνώση αν σταμάτησε κάποιο Service, πότε σταμάτησε και να το επαναφέρει αυτόματα ή μη.

Στην παρακάτω εικόνα φαίνεται μια επισκόπηση επικοινωνίας – αλληλεπίδρασης μεταξύ πλατφόρμας Spiceworks και Servers οι οποίοι θα παρακολουθούνται από το plugin.

Εικόνα 7.1

Σε κάθε Server που θα χρειαστεί να παρακολουθείται εγκαθισταται μια εφαρμογή NodeJS η οποία ελέγχει την κατάσταση του Windows Service μέσω του πακέτου *npm windows-service*

install :

npm install -g node-windows
npm install -g express

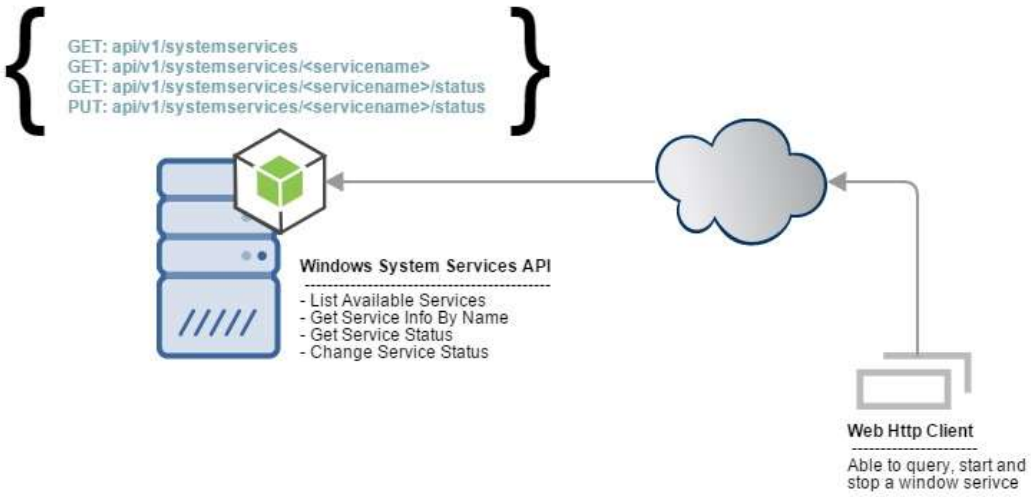
coding:

```
var wincmd = require('node-windows');

wincmd.list(function(svc){
  console.log(svc);
},true);
```

Το παραπάνω παράδειγμα δείχνει πως γίνεται η εγκατάσταση του NodeJS πακέτου για έλεγχο ενός Windows Service καθώς και ένα τυπικό παράδειγμα χρήσης του πακέτου (list all services).

Στη συνέχεια η λειτουργικότητα αυτήγίνεται διαθέσιμη για χρήση μέσω rest api όπως φαίνεται και στην εικόνα 7.2



Εικόνα 7.2

Η υλοποίηση του rest api πραγματοποιήθηκε με το πάκετο NodeJS express καθώς και το Node Windows, δίνοντας την δυνατότητα σε ένα οποιοδήποτε http client να ελέγχει απομακρυσμένα ένα ή περισσότερα windows services. Ακολουθεί ένα τυπικό κομμάτι κώδικα υλοποίησης.

```
var serviceManager =  require('node-windows').Service;
var express = require('express');
var _ = require('lodash');

var app = express();

//return all available windows services when client requests a GET on the specific URL
app.get('/api/v1/systemservices', function(req, res) {
   serviceManager.list(function(allServices){
      res.send( allServices );
   });
});
//Query information for the request service name
app.get('/api/v1/systemservices/:serviceName', function(req, res) {
```

```
  var serviceName = req.params.serviceName;
  serviceManager.list(function(allServices){
    var service = _.where(allServices,function(s){
      return s.name == serviceName;
    });
    res.send( service );
  });
});
```

//Start Stop Service by name depending on the status parameter given by the client on the specific PUT url

```
app.put('/api/v1/systemservices/:serviceName/status', function(req, res) {
  var serviceName = req.params.serviceName;
  var status = req.body.status;

    if(status == 'START') {
      serviceManager.start(serviceName);
    }
    if(status == 'STOP') {
      serviceManager.stop(serviceName);
    }
  });
});
```

Στη συνέχεια θα δημιουργηθεί και καταχωρηθεί μια νέα εφαρμογή στην πλατφόρμα με αναφορά το url από το οποίο εξυπηρετείται. Το url αυτό έχει υλοποιηθεί μέσα στο NodeJS που περιγράφηκε παραπάνω. Ένα τυπικό κομμάτι υλοποίησης είναι αυτό που ακολουθεί.

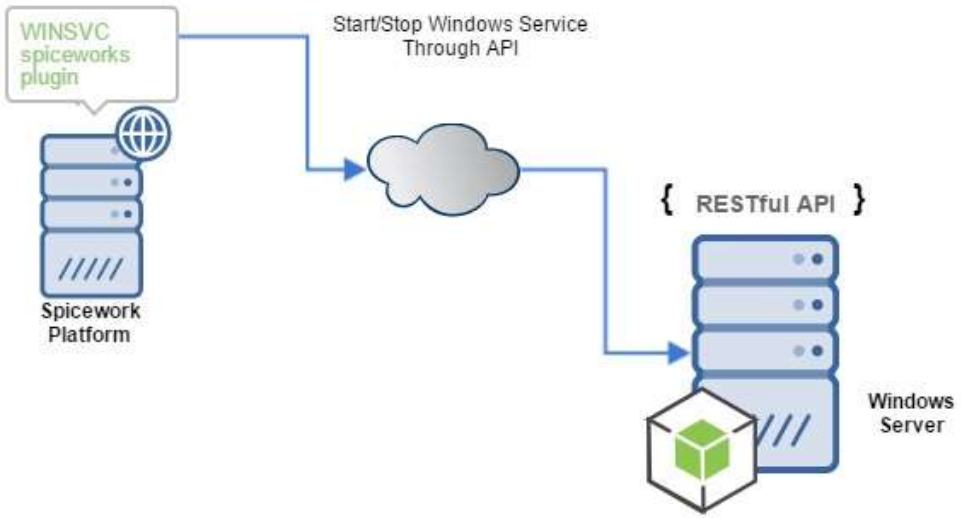
//When an http client hits the url below, if the requested service is not running the application create a Spicework ticket using the platform SDK

```
  app.get('/spicework-winsvc-app/:serviceName', function (req, res) {
 var serviceName = req.params.serviceName;
    serviceManager.list(function(allServices){
      var service = _.where(allServices,function(s){
        return s.name == serviceName;
      });
    });
    if(service.status != 'RUNNING') {
      var card = new SW.Card();
      var attributes = {
```

```
            summary: 'Windows service ' + serviceName + ' is not running',
        };

    //Open ticket
        card.services('helpdesk').request('ticket:create', attributes)
    }
});
```

Αφου προέτοιμαστηκε η εφαρμογή για την παρακολούθηση των Services, τώρα απομένει η ενσωμάτωση ενός Plugin που θα χειρίζεται την επανοφορά του service και το κλείσιμο του ticket. Αυτή είναι η υλοποίηση του Plugin το οποίο χειρίζεται ένα ticket που προέκυψε από πρόβλημα του Windows Service. Ο Χρήστης του plugin έχει τη δυνατότητα να ξεκινήσει το service μέσω του rest api και αν η κλήση είναι επιτυχής, κλείνει και το ticket. Η εικόνα 7.3 απεικονίζει τον παρακάτω κώδικα.



Εικόνα 7.3

```
    <!doctype html>
<html>
<head>
     <title>Close the Window Service Ticket</title>
</head>
<body>
  <div>

    <!—This fields contains the ticket information loaded some how through SDK→
     <input id="ticket"/>
     <input id="serviceName" />
```

```
    <!—Close the open ticket with just one click→
     <button onclick="startService()">Start Service</button>
  </div>
  <script src="jquery.js"></script>
  <script src="spiceworks-sdk.js"></script>
  <script>

    <!—Start service when user push start button→
     function startService() {
        var serviceName = $("#serviceName").val();
        $.ajax({
          url: "/api/v1/systemservices/" + serviceName,
          data: {
            status: 'START'
          },
          success: function( data ) {
              var theTicket = $("#ticket").val();
              SPICEWORKS.data.Ticket.close(theTicket);
          }
        });
     }
  </script>
</body>
</html>
```

Σύγκριση Εργαλειών Παρακολούθησης Δικτύου [Σύνοψη]

Σίγουρα ένας IT μπορεί να βρει πόσα PC βρίσκονται στο δίκτυό του, αλλά πόσο σίγουρος είναι ότι ξέρει πόσα licenses έχουν λήξει ή είναι πειρατικά?

Τα εργαλεία διαχείρισης αγαθών, χωρίζονται σε δύο κατηγορίες. Μπορεί να είναι μια εφαρμογή η οποία ανακαλύπτει όλες τις συσκευές ενός δικτύου και δημιουργεί μία καταγραφή όλων αυτών των συσκευών σε μία βάση δεδομένων. Και υπάρχει η κατηγορία εφαρμογών, που είναι μέρος μιας ολοκληρωμένης σουίτας διαχείρισης IT.

Η διαχείριση ενός αγαθού, περιλαμβάνει όλο τον κύκλο ζωής του, από την αγορά έως την απόσυρσή του. Κατά τη διάρκεια αυτής της περιόδου, η εφαρμογή διαχείρισης αγαθών, μπορεί να αποτυπώσει μία ξεκάθαρη εικόνα για την δυνατότητα εξοικονόμησης κόστους.

Οι πάρόχοι εφαρμογών διαχείρισης αγαθών, επισημαίνουν την έννοια της επιστροφής της επένδυσης (ROI). Με άλλα λόγια, μπορεί να μειωθεί το κόστος κτήσης των αγαθών με την παρακολούθηση, συμπεριλαμβανομένης της συχνότητας χρησιμοποίησης του licensed software, καθώς θα μπορεί να μεταφερθεί σε θέσεις όπου θα χρησιμοποιήται.

a/a	Ευκολία εγκατάστασης παραμετροποίησης	Πλατφόρμα	Agents	Help Desk Capabilities	Mobile Device Management (MDM)	Network Monitor	Schedule discovery	Plugins	Distributed monitor	Remote installation
Spiceworks	Πολύ εύκολη και γρήγορη. Απλή παραμετροποίηση	Μόνο Windows	Μόνο Windows	Παρακολούθηση Service tickets και πρόοδος	Με την υποστήριξη του MAAS 360	Real time monitor. Έλλειψη διασύνδεσης με Network Invetory. Έχει false positives	Υποστηρίζει αυτόματα με την εκκίνηση, με χρονοκαθυστέρηση, αλλά και εκτός ωρών εργασίας	Πολλά plugin, άλλα δωρεάν και άλλα επι πληρωμή	Υποστηρίζει remote sites και χωρίς την ύπαρξη vpn σύνδεσης	Μόνο με τη συνεργασία του ManageEngine και μέχρι 25 Η/Υ
FusionInventory	Δυσκολία στην εγκατάσταση. Πιο δύσκολη παραμετροποίηση	Windows & Linux διανομές	Windows & Linux διανομές	Παρακολούθηση Service tickets και πρόοδος	Όχι	Δεν υποστηρίζει	Μόνο με χρονοδιάγραμμα	Είναι Plugin σε άλλη πλατφόρμα	Δεν υποστηρίζει	Κάνει remote installation σε ορισμένες πλατφόρμες με προϋποθέσεις
Open NMS	Δυσκολία στην εγκατάσταση. Πιο εύκολη παραμετροποίηση	Linux	Agentless	Σύνδεση με άλλα HelpDesk	Όχι	Real time monitor	Όχι	Μόνο σε Java	Υποστηρίζει remote sites και χωρίς την ύπαρξη vpn σύνδεσης	Όχι
Open Audit	Δυσκολία στην εγκατάσταση. Πιο εύκολη παραμετροποίηση	Linux	Agentless	Όχι	Όχι	Real time monitor	Όχι στην Community έκδοση	Όχι στην Community έκδοση	Υποστηρίζει remote sites	Όχι
Nagios	ευκολία στην εγκατάσταση. Δύσκολη παραμετροποίηση	Linux	Windows & Linux διανομές	Σύνδεση με άλλα HelpDesk	Όχι	Real time monitor	Όχι	Τα περισσότερα Plugin σε σχέση με όλες τις freeware network monitor εφαρμογές	Υποστηρίζει remote sites και χωρίς την ύπαρξη vpn σύνδεσης	Όχι

Συγκριτικός πίνακας 1

a/a	Ευκολία εγκατάστασης παραμετροποίησης	Πλατφόρμα	Agents	Help Desk Capabilities	Mobile Device Management (MDM)	Network Monitor	Schedule discovery	Plugins	Distributed monitor	Remote installation
GFI languard	Πολύ εύκολη και γρήγορη. Απλή παραμετροποίηση	Μόνο Windows	All platforms	Παρακολούθηση Service tickets και πρόοδος	Ναι	Μέσω του GFI Monitor	Ναι	Ναι	Υποστηρίζει remote sites	Ναι
Microsoft SMS	Δυσκολία στην εγκατάσταση. Πιο δύσκολη παραμετροποίηση	Μόνο Windows	All platforms	Microsoft Service Manager	Ναι	Ναι	Ναι	Plugins της Microsoft	Υποστηρίζει remote sites & στο Cloud	Ναι
IT Asset Management BMC	Δυσκολία στην εγκατάσταση. Πιο δύσκολη παραμετροποίηση	Windows & Linux	All platforms	BMC Service Request Management	Ναι	Ναι	Ναι	Ναι	Υποστηρίζει remote sites & στο Cloud	Ναι
Altiris IT Management	Ευκολία στην εγκατάσταση. Πιο εύκολη παραμετροποίηση	Windows	All platforms (εκτός Unix)	Symantec ServiceDesk	Ναι	Real time monitor	Ναι	Ναι	Υποστηρίζει remote sites & στο Cloud	Ναι
AuditWizard	Ευκολία στην εγκατάσταση. Εύκολη παραμετροποίηση	Windows	Windows	Layton ServiceDesk	Όχι	Όχι	Ναι	Όχι	Υποστηρίζει remote sites	Όχι

Συγκριτικός πίνακας 2

Έχοντας πλέον ολοκληρωμένη εικόνα από την μελέτη και παρουσίαση Community και Commercial εργαλείων θα επιχειρηθεί μία ανάλυση των πλεονεκτημάτων μεταξύ αυτών, αλλά και το συμπέρασμα για την χρησιμότητα της αγοράς ενός εξ'αυτών ή χρησιμοποίησης ενός δωρεάν εργαλείου.

Η σύγκριση των εργαλείων γίνεται καταρχήν, όσον αφορά τις δυνατότητες που έχει το κάθε ένα ως προς την αναζήτηση και καταγραφή αγαθών. Όπως θα δείτε, άλλα εργαλεία είναι εργαλεία διαχείρισης αγαθών και άλλα εργαλεία παρακολούθησης δικτύου που σαν πρόσθετο έχουν την καταγραφή των αγαθών. Αυτό το χαρακτηριστικό αφορά κυρίως τα community εργαλεία, καθώς οι εμπορικές εφαρμογές που εξετάζονται, είναι ολοκληρωμένες πλατφόρμες.

Ξεκινώντας από τα **Community** εργαλεία, το **SpiceWorks** και το **FusionInventory**, ανήκουν στην πρώτη κατηγορία, ενώ το **OpenNMS**, **OpenAudit** και **Nagios** στην δεύτερη.

Το **SpiceWorks** είναι πολύ εύκολο στην εγκατάστασή του και δεν χρειάζονται ιδιαίτερες γνώσεις για την παραμετροποίησή του, καθώς πολλά υποδεικνύονται από την ίδια την εφαρμογή ή βρίσκονται σε απαντήσεις στο Community. Η εγκατάσταση των agent επίσης είναι πολύ εύκολη, αλλά και η σύνδεση με απομακρυσμένα δίκτυα. Μειονέκτημα, το ότι δεν υπάρχει ακόμα agent για Linux και MacOS. Επίσης, έχει πολύ καλά γραφήματα για καλύτερη ανάλυση των δεδομένων που εξάγει από τα συστήματα. Με μια πρώτη ματιά, μπορεί κάποιος να καταλάβει τι περιέχεται στο δίκτυό του και να δει αναλυτικά ότι χρειάζεται μέσα από μια πληθώρα αναφορών που είναι ενσωματωμένα.

Από τα πιο σημαντικά πλεονεκτήματα του **Spiceworks**, είναι η σε πραγματικό χρόνο απεικόνιση των συσκευών ενός δικτύου και παρακολούθηση αυτών μέσω του εργαλείου monitoring που διαθέτει. Κάνει διαχείριση κινητών συσκευών και επίσης συνδέεται με τρίτα προγράμματα για έλεγχο ευπαθειών όπως είναι το AlienVault, αλλά και ενημέρωση ευπαθειών που προσφέρεται από την ManageEngine. Τέλος πλεονέκτημα του είναι η ύπαρξη ενσωματωμένου Service Desk για διαχείριση tickets τα οποία συνδέονται άμεσα με τα αγαθά μιας επιχείρησης.

Αντίθετα, το FusionInventory, είναι πολύπλοκο στην εγκατάστασή του, καθώς στηρίζεται στην πλατφόρμα GLPI. Εγκαθίσταται σε Windows και Linux συστήματα και υποστηρίζει agents για όλα τα λειτουργικά. Έχει ειδική παραμετροποίηση για απομακρυσμένα δίκτυα. Ακόμα στο **FusionInventory**, υπάρχει έλλειψη γραφημάτων και αναφορών σαν αυτά που περιγράψαμε στο κείμενο και θα πρέπει ο χρήστης είτε να δημιουργήσει δικά του, έχοντας γνώσεις προγραμματισμού, είτε να αρκεστεί βλέποντας τις συσκευές μεμονωμένα.

Στο **FusionInventory** δεν παρακολουθεί κινητές συσκευές και δεν συνδέεται με αντίστοιχα προγράμματα και θεωρείται περισσότερο εφαρμογή για διαχείριση αγαθών. Παρόλο που δίνει εικόνα για παρακολούθηση των συσκευών, αυτή δεν είναι η πραγματική, καθώς πάρθηκε σε μία ορισμένη στιγμή και δεν είναι επαναλαμβανόμενη. Και αυτή η εφαρμογή έχει ενσωματωμένο περιβάλλον διαχείρισης αιτημάτων.

Αντίθετα με τα παραπάνω το **OpenNMS** είναι ένα εργαλείο παρακολούθησης δικτυακών συσκευών και Servers. Είναι λίγο δύσκολο στην εγκατάσταση, αλλά εύκολα παραμετροποιήσιμο. Δεν χρησιμοποιεί agents αλλά υποστηρίζει σύνδεση με απομακρυσμένα δίκτυα χωρίς την ανάγκη ασφαλούς σύνδεσης. Έχει σαν πλεονέκτημα την σε πραγματικό χρόνο απεικόνιση δεδομένων από τις συσκευές που ελέγχει.

Όπως θα δείτε και στον συγκριτικό πίνακα 1τα εργαλεία παρακολούθησης δικτύου δεν υποστηρίζουν αυτόματη αναζήτηση συσκευών και το OpenNMS δεν αποτελεί εξαίρεση. Επίσης δεν υποστηρίζει κινητές συσκευές αλλά και δεν έχει τη δυνατότητα για απομακρυσμένη εγκατάσταση. Τέλος, δεν έχει ενσωματωμένο περιβάλλον διαχείρισης αιτημάτων, αλλά συνδέεται με τρίτα προγράμματα.

Το **Nagios**, διατίθεται σε δύο εκδόσεις, την **Nagios Core** (community) και την **Nagios XI** (commercial). Εγκαθίσταται σε πλατφόρμα Linux και υποστηρίζει agents τόσο για Windows όσο και για Linux. Είναι πολύ εύκολο στην εγκατάστασή του, αλλά πολύ δύσκολο στην παραμετροποίηση. Υποστηρίζει απομακρυσμένα δίκτυα και έχει real time network monitor. Ένα χαρακτηριστικό που δίνεται και στις δύο

εκδόσεις, είναι η άμεση ενέργεια αποκατάστασης υπηρεσιών ή εφαρμογών σε περίπτωση αποτυχίας, εφόσον αυτές παρακολουθούνται.

Μειονεκτήματα της εφαρμογής η έλλειψη διαχείρισης συσκευών, αλλά και η εγκατάσταση ενημερώσεων και εφαρμογών. Δεν έχει Service desk αλλά δυνατότητα σύνδεσης με τρίτα προγράμματα. Στην community έκδοση, δεν υποστηρίζει αυτόματη αναζήτηση.

Τέλος το **OpenAudit** διατίθεται και αυτό στις εκδόσεις community και enterprise. Περιέχει χαρακτηριστικά και από τις δύο κατηγορίες που αναφέρθηκαν, αλλά περιορίζονται σημαντικά στην community έκδοση.

Εγκαθίσταται σε πλατφόρμα Linux και δεν χρησιμοποιεί agents. Παρακολουθεί τις συσκευές μέσω των πρωτοκόλλων SNMP και WMI και υποστηρίζει απομακρυσμένα δίκτυα.

Δεν έχει ενσωματωμένο περιβάλλον διαχείρισης αιτημάτων, αλλά ούτε και συνδέεται με τρίτα προγράμματα. Δεν υποστηρίζει κινητές συσκευές και απομακρυσμένη εγκατάσταση. Τέλος, μειονέκτημα της community έκδοσης είναι η μη αυτόματη αναζήτηση συσκευών.

Στις **Commercial** εφαρμογές συναντώνται περιπτώσεις που ταιριάζουν σε μικρές επιχειρήσεις, μεσαίες, αλλά και μεγάλες. Όλες επιλέχθηκαν σύμφωνα με το κυριότερο χαρακτηριστικό που είναι η αναζήτηση και καταγραφή αγαθών. Μαζί με αυτό συνδέονται μια σειρά ακόμα πρόσθετων για την διαχείριση του δικτύου, όπως ο έλεγχος του λογισμικού, η εγγύηση των μηχανημάτων, η απομακρυσμένη διαχείριση και πολλά ακόμα.

Ξεκινώντας από το **GFI Languard,** η εγκατάστασή του γίνεται μόνο σε πλατφόρμα Windows, αλλά υποστηρίζει agents σε όλες τις πλατφόρμες. Έχει δυνατότητες για έλεγχο ευπαθειών, απομακρυσμένη εγκατάσταση και ενημέρωση. Ελέγχει για ανοιχτές πόρτες ή ευπάθειες σε ένα δίκτυο. Χρησιμοποιήται και από IT Auditors για πραγματοποίηση ελέγχων και πιστοποιήσεων σε ένα δίκτυο.

Υποστηρίζει έλεγχο κινητών συσκευών (μοντέλο BYOD) και δίνει αναφορές για την παρουσία τους. Ακόμα έχει ενσωματωμένο σύστημα διαχείρισης αιτημάτων και παρακολούθησης δικτύου. Κοστίζει 26$ για 25-49 Η/Υ και μειώνεται ανάλογα με την αγορά επιπλέον αδειών.

Τέλος υποστηρίζει απομακρυσμένα δίκτυα τόσο on premise όσο και στο cloud, όπου δίνεται η δυνατότητα στον διαχειριστή και για antivirus GFI.

Φαίνεται από τα παραπάνω πως είναι μια ολοκληρωμένη σουίτα από λύσεις για οποιονδήποτε διαχειριστή σε προσιτή τιμή. Είναι εύκολη στην εγκατάσταση και στην παραμετροποίηση με κατανοητές αναφορές. Δεν υπάρχει κάποια έλλειψη στις ελάχιστες προδιαγραφές ενός διαχειριστή.

Το **Microsoft SMS (SCCM)**, είναι η λύση της Microsoft για την διαχείριση ενός δικτύου. Εγκαθίσταται σε πλατφόρμα Windows αλλά έχει agents για όλες τις πλατφόρμες. Υποστηρίζει help desk μέσω του Microsoft Service Desk.

Έχει σύστημα παρακολούθησης δικτύου αλλά και παραμετροποίησης συσκευών μέσω του πρωτοκόλλου SNMP, διαχείριση κινητών συσκευών αλλά και cloud υπηρεσιών, είτε Microsoft Azure είτε Amazon ή Google.

Κοστίζει η Standard έκδοση 1323$ και η Datacenter 3607$ αλλά με απεριόριστο αριθμό συσκευών για διαχείριση.

Υποστηρίζει απομακρυσμένη εγκατάσταση και ενημέρωση, αλλά δεν κάνει έλεγχο ευπαθειών. Ακόμα είναι πολύ δύσκολη η παραμετροποίησή του και η διαχείριση.

Είναι μία πολύ καλή και φθηνή σχετικά λύση, καθώς εκτός των άλλων, υποστηρίζει disaster recovery site με virtual machines.

Το **IT Asset Management της BMC** απευθύνεται σε πολύ μεγάλες επιχειρήσεις, καθώς το Asset Management είναι ένα μέρος μία ολοκληρωμένης σουίτας. Διατίθεται επιπλέον και σε μοντέλο SaaS. Όπως και το GFI είναι συμβατό με διαδικασίες auditing SCAP (Security Content Automation Protocol).

Η εγκατάστασή του γίνεται τόσο σε περιβάλλον Windows όσο και σε Linux και έχει agents για όλες τις πλατφόρμες. Υποστηρίζει διαχείριση κινητών συσκευών και σύστημα διαχείρισης αιτημάτων (BMC Service Request Management). Ακόμα συνδέεται με εξωτερικές εφαρμογές και συσκευές για μεταφορά δεδομένων που είναι ασύμβατες μεταξύ τους. Κάνει απομακρυσμένη εγκατάσταση και ενημέρωση εφαρμογών.

Η εγκατάστασή του είναι πολύ δύσκολη και απαιτητική σε hardware. Επειδή απευθύνεται σε πολύ μεγάλες επιχειρήσεις αυτό είναι κατανοητό,

καθώς θα πρέπει να υπάρχει μία συνέχεια στις λειτουργίες που προσφέρει. Για το λόγο αυτό ήταν δύσκολο να εντοπιστεί και το κόστος της λύσης αυτής.

Το **Altiris IT Management της Symantec** ξεκίνησε από μία εφαρμογή διαχείρισης Server και Η/Υ. Μετά την εξαγορά της από την Symantec, ενσωματώθηκαν σε αυτό και άλλα πρόσθετα τα οποία το μετέτρεψαν σε μια ολοκληρωμένη λύση.

Είναι εύκολο στην εγκατάστασή του και στην παραμετροποίηση και εγκαθίσταται σε περιβάλλον Windows. Έχει agents για όλα τα λειτουργικά εκτός από Unix και υποστηρίζει κινητές συσκευές. Έχει ενσωματωμένο το Service Desk της Symantec και απομακρυσμένη διαχείριση ακόμα και στο cloud.

Μεγάλο πλεονέκτημα αυτής της εφαρμογής, είναι η μαζική εγκατάσταση software αλλά και πολλαπλών λειτουργικών συστημάτων μέσω PXE boot σε διαφορετικά συστήματα hardware. Ακόμα δίνεται η δυνατότητα διαχείρισης των backup, disaster recovery και του antivirus από την ίδια κονσόλα.

Η τιμή του για όλα τα παραπάνω, εκτός του ServiceDesk είναι περίπου 100$ ανά χρήστη, κάτι που το καθιστά μια πολύ ακριβή λύση.

Τέλος, το **AuditWizard** είναι μία λύση για μικρές επιχειρήσεις από την οποία λείπουν αρκετά χαρακτηριστικά μίας ολοκληρωμένης λύσης για network inventory πρόγραμμα.

Κάνει αναζήτηση και καταγραφή, παρακολουθεί συμβάντα των συσκευών του δικτύου και στέλνει ειδοποιήσεις και παρακολουθεί την κίνηση διαδικτύου των χρηστών. Επίσης έχει ενσωματωμένο πρόγραμμα help desk το Layton ServiceDesk.

Όμως δεν έχει real time monitoring, απομακρυσμένη εγκατάσταση και ενημέρωση λογισμικού και υποστηρίζει μόνο Windows. Τελευταίο και εξίσου σημαντικό, η έλλειψη διαχείρισης κινητών συσκευών.

Τελευταίο μειονέκτημα, είναι το κόστος αγοράς που αγγίζει σχεδόν 2000$ για 250 υπολογιστές. Πολύ ακριβή λύση για ένα προϊόν που δεν προσφέρει ούτε τίς μισές δυνατότητες ενός ολοκληρωμένου προγράμματος διαχείρισης αγαθών.

Κλείνοντας αυτή τη σύγκριση και έχοντας γνώση από την ενασχόληση με αυτά τα προϊόντα, για την εξαγωγή αυτής της έρευνας, μπορώ να αναφέρω πως όλα έχουν κάτι που λείπει από κάποιο άλλο και πως ακόμη και αυτά που πρέπει να πληρώσεις έχουν ελλείψεις ή δίνουν λιγότερα αποτελέσματα από κάποιο που διατίθεται δωρεάν. Το SpiceWorks διαθέτει τα περισσότερα που μπορεί να βρει κάποιος σε open source εφαρμογή και να το αναπτύξει περαιτέρω.

Αυτό που θα μπορούσε να προστεθεί στο SpiceWorks το οποίο αποτελεί σημαντικό χαρακτηριστικό του Nagios, είναι η απομακρυσμένη επανεκκίνηση υπηρεσιών και εφαρμογών. Αυτό το χαρακτηριστικό δεν εντοπίστηκε ούτε σε commercial εφαρμογές. Ακόμα ένα χαρακτηριστικό που λείπει από το Spiceworks είναι η απομακρυσμένη εγκατάσταση λογισμικού και ενημερώσεων. Παρόλο που συνεργάζεται με το ManageEngine, αυτό προσφέρεται μόνο για 25 Η/Υ.

Από τις Commercial εφαρμογές η καλύτερη λύση είναι το Altiris Management Suite, λόγω της μεγάλης κλίμακας εγκαταστάσεων που μπορεί να διαχειριστεί, αλλά και να ενώσει τις τεχνολογίες που προσφέρει η Symantec. Το κόστος αγοράς όμως είναι πολύ υψηλό και σε αυτή την περίπτωση η επόμενη λύση είναι αυτή της Microsoft. Η οποία περιέχει αρκετά από τα χαρακτηριστικά του Altiris και έχει σχετικά προσιτή τιμή.

Όταν όμως κάποιος πρέπει να επιλέξει ένα προϊόν το οποίο θα καταγράφει με ακρίβεια τα αγαθά της επιχείρησης, τις εγγυήσεις, θα πιστοποιεί το δίκτυο του, θα ελέγχει για ευπάθειες και θα τις διορθώνει, τότε θα πρέπει να επιλέξει το GFI Languard. Η τιμή του είναι αρκετά καλή και διαθέτει όλα τα χαρακτηριστικά που θέτει ένας διαχειριστής για να ελέγχει το δίκτυό του.

Συμπεράσματα

Κλείνοντας υπενθυμίζουμε ότι στην παραπάνω εργασία, έγινε προσπάθεια να γίνει κατανόηση των τεχνολογιών που χρησιμοποιούνται για το Network Inventory και την χρησιμότητα αυτών. Να συγκριθούν τεχνολογίες που χρησιμοποιούν αυτά καθώς και τους λόγους που θα μπορούσε να επιλέξει κάποιος ένα network inventory, βασιζόμενος στην τεχνολογία που υποστηρίζει το εκάστοτε πρόγραμμα. Τέλος, έγινε σύγκριση μεταξύ των network inventory προγραμμάτων, με σκοπό την κατανόηση αυτών, τα θετικά τους στοιχεία, αλλά και τα αρνητικά.

Έτσι, θα είναι εύκολη η επιλογή σε κάποιον διαχειριστή για να επιλέξει μεταξύ μίας εμπορικής εφαρμογής ή ανοιχτού κώδικα.

Παραπομπές

Open-AudIT - The network inventory, audit, documentation and management tool. 2015. Open-AudIT - The network inventory, audit, documentation and management tool. [ONLINE] Available at: http://open-audit.org/. [Accessed 08 January 2015].

GLPI - Gestionnaire libre de parc informatique. 2015. GLPI - Gestionnaire libre de parc informatique. [ONLINE] Available at: http://www.glpi-project.org/spip.php?lang=en. [Accessed 15 December 2014].

fusioninventory-documentation/userdoc.mdwn at master · fusioninventory/fusioninventory-documentation · GitHub. 2015. fusioninventory-documentation/userdoc.mdwn at master · fusioninventory/fusioninventory-documentation · GitHub. [ONLINE] Available at: https://github.com/fusinv/fusioninventory-documentation/blob/master/documentation/fi4g/userdoc.mdwn#fusioninventory-agent. [Accessed 20 December 2014].

SpiceWorks. 2015. Help Desk Network Discovery Network Monitor. [ONLINE] Available at http://www.spiceworks.com . http://community.spiceworks.com/help/Configuring_AV_Firewall http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf014.html[Accessed 7 July 2015].

The OpenNMS Project. 2015. The OpenNMS Project. [ONLINE] Available at: http://www.opennms.org/. [Accessed 15 January 2015].

GFI LanGuard. 2015. GFI LanGuard. [ONLINE] Available at: http://languard.gfi.com/. [Accessed 02 December 2015].

BMC - Bring IT To Life with Digital Enterprise Management. 2015. BMC - Bring IT To Life with Digital Enterprise Management. [ONLINE] Available at: http://www.bmc.com/. [Accessed 04 December 2015].

Microsoft - Microsoft Operations Management Suite. 2015. Microsoft Operations Management Suite . [ONLINE] Available at: http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx . [Accessed 07 December 2015].

WikiPedia - **Comparison of network monitoring systems.** [ONLINE] Available at: https://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems. . [Accessed 04 January 2016].

NodeJS – **NodeJS Windows** [ONLINE] Available at: https://www.npmjs.com/package/node-windows

https://gist.github.com/iksose/9401758

https://github.com/spiceworks/spiceworks-js-sdk/tree/305e2175cb81270daaaed7ce1dae07c2751e437a/examples/wonkameme

[Accessed 10 February 2016].

Symantec – **Endpoind Management.** [ONLINE] Available at: https://www.symantec.com/products/threat-protection/endpoint-management

[Accessed 18 February 2016].

Nagios – **Nagios Core features.** [ONLINE] Available at: https://assets.nagios.com/datasheets/nagioscore/Nagios%20Core%20-%20Features.pdf

[Accessed 17 February 2016]

AuditWizard - **Network Inventory Software Made Easy.** [ONLINE] Available at: http://laytontechnology.com/auditwizard/

[Accessed 19 February 2016].