Πανεπιστήμιο Μακεδονίας

Μεταπτυχιακό στα Πληροφοριακά Συστήματα

Τεχνολογίες Δικτύων

Καθηγητές: Α.Α. Οικονομίδης & Α. Πομπόρτσης

Free & Open Source Tools for Network Monitoring & Management

Μαραγκάκης Αλέξανδρος (MIS0433)

Θεσσαλονίκη,
Φεβρουάριος 2005

University of Macedonia

Master Information Systems

Networking Technologies

Professors: A.A. Economides & A. Pomportsis

Free & Open Source Tools for Network Monitoring & Management

Maragakis Alexandros (MIS0433)

Thessaloniki,
February 2005

Περίληψη

Στο παρακάτω κείμενο θα γίνει μια προσπάθεια να δωθεί ένας ορισμός της διαχείρισης και παρακολούθησης των δικτύων, με αναφορές στα επιμέρους ζητήματα που ασχολούνται αυτού του είδους οι εργασίες. Στη συνέχεια θα προσδιοριστούν οι λόγοι που η χρήση του ανοικτού λογισμικού μπορεί να συντελέσει στην αποδοτική διαχείριση των δικτύων και στην μείωση του κόστους λειτουργίας του δικτυακού εξοπλισμού. Έπειτα θα αναφερθούν και θα αναλυθούν οι κατηγορίες του ανοικτού λογισμικού που αφορούν στην παρακολούθηση και την διαχείριση και τέλος θα παρουσιαστούν ορισμένα εργαλεία τα οποία υπάρχουν αυτή τη στιγμή στην αγορά με τα ανάλογα συμπεράσματα.

Abstract

In the following text will be an effort to give a definition of the network management and the monitoring, with references on the subsections regarding these types of works. Next we will define the reasons on which the use of open source software can help on the productive network management and in the decrease the cost of the network functions. After that there is a reference and a detailed description about the categories of the management and in the end there is a presentation of the most popular tools with the corresponding conclusions.

Περιεχόμενα

Table of Contents

1. Παρουσίαση Θέματος

Η εκρηκτική αύξηση της τεχνολογίας των υπολογιστών και η ολοένα αυξανόνενη ανάγκη δικτύωσής τους, έχει οδηγήσει στη δημιουργία της ανάγκης για αποδοτική διαχείριση και παρακολούθηση των δικτύων και των συσκευών που τα αποτελούν. Παράλληλα, όμως, έχει δημιουργηθεί η ανάγκη για μείωση του κόστους λειτουργίας και της πολυπλοκότητας του δικτυακού εξοπλισμού των επιχειρήσεων. Προς αυτή την κατεύθυνση, λοιπόν, αναπτύσσεται λογισμικό το οποίο δεν αποτελεί προϊόν της παραγωγικής διαδικασίας κάποιας εταιρίας λογισμικού, αλλά είναι αποτέλεσμα της προσπάθειας κάποιων ανθρώπων, οι οποίοι θέλουν να προσφέρουν υπηρεσίες στον εαυτό τους και στους υπόλοιπους. Το ανοικτό λογισμικό έχει εισχωρήσει και στις εφαρμογές της διαχείρισης δικτύων και αποτελεί καλή εναλλακτική λύση για εκείνους που επιθυμούν να το χρησιμοποιήσουν έναντι των εμπορικών εφαρμογών.

Το πρόβλημα έγκειται στο γεγονός ότι πολλές φορές δεν είναι γνωστό το πεδίο εφαρμογών που μπορεί να αντιμετωπίσει την πολυπλοκότητα των σημερινών δικτυών, αφήνοντας έτσι να θεωρείται ότι τέτοιου είδους εφαρμογές θα αυξήσουν πολύ το κόστος λειτουργίας της επιχείρησης, με αποτέλεσμα να υπάρχει σκεπτικισμός για το αν πρέπει να χρησιμοποιηθεί. Η συγκεκριμένη εργασία θα ασχοληθεί με τον προσδιορισμό αυτών των εφαρμογών, με την απόδοση ταυτότητας και την απομυθοποίηση της πολυπλοκότητα χρήσης και απόκτησής τους.

2. Εισαγωγή

Τις τελευταίες δύο δεκαετίες ο αριθμός των δικτυωμένων υπολογιστών έχει αυξηθεί με τρομακτικούς ρυθμούς. Στα μέσα της δεκαετίας του 80, όταν ο προσωπικός υπολογιστής έγινε η νέα μόδα, οι περισσότεροι άνθρωποι δεν είχαν την ανάγκη για δικτύωση των μηχανημάτων τους. Σήμερα, 20 χρόνια αργότερα, είναι δύσκολο να φανταστεί κανείς μια επιχείρηση με έναν σεβαστό αριθμό υπολογιστών οι οποίοι δεν έχουν δικτυωθεί με κάποιον από τους τρόπους που προσφέρει η σύγχρονη τεχνολογία. Στις περισσότερες περιπτώσεις μάλιστα, τα δίκτυα αυτά συνδέονται στο Παγκόσμιο Διαδίκτυο, επιτρέποντας τη διασύνδεσή τους με οποιοδήποτε άλλο μηχάνημα του Διαδικτύου, σε οποιοδήποτε σημείο του κόσμου.

Την εποχή που η τεχνολογία των δικτύων ήταν ευρέως διαδεδομένη, υπήρχε μικρή ανάγκη για την διαχείριση των δικτύων. Πολύ απλά δεν υπήρχαν πολλά να διαχειριστείς. Όταν, παρόλα αυτά, κάτι δεν πήγαινε καλά, συνήθως υπήρχε πρόβλημα στο υλικό. Σήμερα, όμως, τοο υλικό είναι πολύ αξιόπιστο και τα προβλήματα προέρχονται κυρίως από κακό λογισμικό ή κακούς χρήστες. Την ίδια στιγμή η ανάγκη για αξιοπιστία έχει αυξηθεί. Οι περισσότεροι άνθρωποι βασίζονται σε κάποιο δίκτυο για να ολοκληρώσουν την εργασία τους; μερικά δίκτυα υποστηρίζουν ακόμα και εξοπλισμό ασφάλειας ζωής. Οι δύο αυτοί οι παράγοντες, η αυξημένη ανάγκη για αξιοπιστία και το γεγονός ότι τα προβλήματα είναι περισσότερο απρόβλεπτα από ποτέ, έχουν οδηγήσει στην αυξημένη ανάγκη για διαχείριση και παρακολούθηση των δικτύων.

Παρόλο, όμως, που η ανάγκη για διαχείριση είναι μεγάλη, η αυξημένη χρήση της έχει κάποιο κόστος. Οι δικτυακές συσκευές, όπως τα switches, έρχονται είτε σε εκδόσεις με δυνατότητες διαχείρισης και παρακολούθησης, οι οποίες είναι και πιο ακριβές, είτε χωρίς αυτές. Πρέπει να αποφασιστεί, λοιπόν, πόση διαχειρισιμότητα είμαστε διατεθειμένοι να πληρώσουμε βασισμένοι στον αριθμό των μηχανημάτων που θα δικτυώσουμε και το περιβάλλον στο οποίο θα διασυνδεθούν. Εάν συνδεθούν απλά τρεις υπολογιστές στο σπίτι, δεν χρειάζεται να αγοραστούν ακριβά μηχανήματα με μεγάλες δυνατότητες διαχείρισης. Εαν κάτι πάει στραβά, η αιτία μπορεί να βρεθεί εύκολα και να απομονωθεί. Εαν, όμως, το δίκτυο περιλαμβάνει πολλά μηχανήματα τα οποία ενδεχομένως να μην είναι εφικτό να προσεγγιστούν και να απομονωθούν εύκολα, η αν χρειαστεί να παρακολουθηθεί η κίνηση στο δίκτυο, τότε πρέπει οι συσκευές να υποστηρίζουν κάποιες δυνατότητες διαχείρισης. Προφανώς όταν υπάρχουν δεκάδες χιλιάδες μηχανήματα σε κάποιο δίκτυο, η διαχείριση είναι απαραίτητη για να εξασφαλιστεί η σταθερότητα του δικτύου σε κάποιο πιθανό πρόβλημα.

3. Τι είναι η διαχείριση και η παρακολούθηση δικτύων

Το πρώτο πράγμα που πρέπει να προσδιοριστεί είναι ο ορισμός της διαχείρισης και της παρακολούθησης δικτύων. Ένας καλός ορισμός αναφέρει ότι η διαχείριση και η παρακολούθηση είναι ένα σύνολο ενεργειών, το οποίο ακολουθεί το μοντέλο FCAPS και χρησιμοποιείται από συνήθως από Κέντρα Διαχείρισης Δικτύων (NOCs). Ο όρος FCAPS αποτελείται από τα αρχικά των παρακάτω επιμέρους κατηγοριών διαχείρισης:

- Διαχείριση Λαθών (Fault Management)
- Διαχείριση Διάρθρωσης (Configuration Management)
- Διαχείριση Λογαριασμών (Accounting Management)
- Διαχείριση Απόδοσης (Performance Management)
- Διαχείριση Ασφάλειας (Security Management)

Ο ισχυρισμός ότι τέτοιου είδους ενέργειες πρέπει να πραγματοποιούνται από NOCs σήμερα είναι μάλλον ξεπερασμένος, εφόσον στα σύγχρονα συστήματα είναι δυνατό να γίνεται η διαχείριση και από μενονωμένα άτομα, ακόμα και με απομακρυσμένο έλεγχο του δικτύου.

4. Γιατί Ανοικτό Λογισμικό;

Τι σημαίνει ο όρος ανοικτό λογισμικό; Περιληπτικά αναφέρεται σε λογισμικό του οποίου ο πηγαίος κώδικας είναι ανοικτός στο κοινό χωρίς περιορισμούς. Επιπλέον εννοεί ότι ο κώδικας αυτός μπορεί να τροποποιηθεί από οποιοσδήποτε και για οποιοδήποτε σκοπό, καθώς και να διανεμηθεί εκ νέου ως ανοικτό λογισμικό.

Παρόλο που το ανοικτό λογισμικό είναι ελεύθερο και δωρεάν, έχει κάποια άδεια η οποία ορίζει την χρήση του. Συνήθως η άδεια αυτή υπάρχει για να εξασφαλιστεί ότι το λογισμικό παραμένει ανοικτό. Επιπλέον, το ανοικτό λογισμικό μπορεί να πουληθεί παρόλο που είναι δωρεάν. Για παράδειγμα μπορεί να αγοραστεί ένα αντίγραφο της διανομής Red Hat Linux, παρόλο που μπορεί να γίνει download από το διαδίκτυο. Γιατί κάποιος να πληρώσει για κάτι ενώ μπορεί να το βρει δωρεάν; Στην περίπτωση του Red Hat, πληρώνει κάποιος για να αγοράσει την διανομή για να αγοράσει και την υποστήριξη που παρέχει η εταιρία, η οποία δεν είναι δωρεάν.

4.1 Η τιμή είναι το πλεονέκτημα.

Η πιο προφανής αιτία για την χρήση Ανοικτού Λογισμικού είναι η τιμή. Ενώ άλλα πακέτα λογισμικού Διαχείρισης και Παρακολούθησης Δικτύων κοστίζουν δεκάδες χιλιάδες ευρώ, το Ανοικτό Λογισμικό είναι δωρεάν. Αυτό, βέβαια, δεν σημαίνει ότι δεν πρέπει να πληρώνεται η ποιότητα. Εάν κάποιο εργαλείο είναι ακριβώς το ιδανικό εργαλείο για την δουλειά για την οποία προορίζεται, έχει όλες τις δυνατότητες που χρειάζονται, βελτιώνει σε μεγάλο βαθμό την διαχειρισιμότητα του δικτύου και προσφέρεται σε λογική τιμή, είναι προτιμότερο να αγοραστεί ανεπιφύλακτα. Αλλά αν υπάρχει κάποιο εργαλείο το οποιο είναι το ίδιο καλο ή και καλύτερο και δεν κοστίζει τίποτα, ποιο από τα δύο είναι πιο λογικό να αγοραστεί;

Το γεγονός ότι το πρόγραμμα είναι δωρεάν έχει δύο ακόμα πλεονεκτήματα. Το πρώτο είναι ότι μπορείς να το δοκιμάσεις απεριόριστα. Δεν είναι σίγουρο ότι το εργαλείο είναι το κατάλληλο; Δοκίμασέ το όσο χρειάζεται και αν δεν είσαι ικανοποιημένος, δεν έχεις πληρώσει τίποτα. Το μόνο που χάθηκε είναι ο χρόνος που επενδύθηκε για την εγκατάσταση και την εκμάθησή του. Παρόλα αυτά, όμως, η αύξηση των ικανοτήτων και των γνώσεων του προσωπικού σε αυτό τον τομέα είναι προτιμότερη από την αγορά κάποιου εργαλείου και η εκμάθησή του, έστω και αν τελικά δεν ανταποκρίνεται στις απαιτήσεις της επιχείρησης.

Το δεύτερο πλεονέκτημα είναι ότι δεν υπάρχει δέσμευση με κάποιο προϊόν εάν κάποιο καλύτερο εμφανιστεί στην αγορά. Εάν έχουν ξοδευτεί 20000 ευρώ για την αγορά ενός προϊόντος τον προηγούμενο χρόνο και τον επόμενο εμφανιστεί κάτι καλύτερο, είναι πιθανό να μην γίνει η μετάβαση λόγω των εξόδων που έγιναν και την δικαιολόγησή τους στην διοίκηση.

4.2 Δυνατότητα επίλυσης περίεργων προβλημάτων

Η αγορά ενός εργαλείου στο οποίο δεν υπάρχει πρόσβαση στον πηγαίο κώδικα μπορεί να αποδειχθεί μεγάλο μειονέκτημα. Ας υποτεθεί ότι κάτι πάει στραβά με το πρόγραμμα: μια σοβαρή αδυναμία στην ασφάλεια ή μια αλλαγή στο δίκτυο η οποία κάνει το πρόγραμμα να μην λειτουργεί. Εάν η εταιρία που το έφτιαξε δεν υπάρχει πια ή αν δεν είναι πρόθυμη να βοηθήσει, τότε δεν υπάρχει τρόπος επιδιόρθωσης.

Ένα ακόμα πιο πιθανό σενάριο: η εταιρία που αναπτύσσει το πρόγραμμα είναι πολύ μεγάλη και εμείς ένας μικρός πελάτης. Υπάρχει συμβόλαιο υποστήριξης, αλλά εάν το πρόβλημα επηρρεάζει όλους τους πελάτες της, ποιος θα εξυπηρετηθεί πρώτος αν όλο το δυναμικό της εταιρίας είναι απασχολημένο; Ασφαλώς οι μεγάλοι πελάτες έχουν ξοδέψει

περισσότερα χρήματα, άρα θα εξυπηρετηθούν πρώτοι. Οι υπόλοιποι πρέπει να περιμένουν, έστω και αν το πρόβλημα είναι κρίσιμο για την λειτουργία της επιχείρησης.

Με ένα προϊόν ανοικτού λογισμικού έχεις την πιθανότητα να αντιμετωπιστεί το πρόβλημα με πόρους της επιχείρησης. Αυτό δεν σημαίνει ότι απαραίτητα θα είναι δύσκολο να γίνει. Μερικά προβλήματα λογισμικού είναι εύκολο να λυθούν και μερικά άλλα όχι. Μπορεί να χρειαστεί κάποιος έμπειρος προγραμματιστής για να βοηθήσει. Ακόμα και αν δεν υπάρχει κάποιος διαθέσιμος στην επιχείρηση, μπορεί να βρεθεί κάποιος σύμβουλος, πράγμα που δίνει κάποια δυνατότητα επίλυσης, σε αντιδιαστολή του να μην υπάρχει καθόλου αυτή η δυνατότητα.

Μια αναλογία του να αγοράζεις ένα κλειστό λογισμικό είναι να αγοράζεις αυτοκίμητο χωρίς να μπορείς να έχεις πρόσβαση στην μηχανή, ενώ αν χρησιμοποιείς ανοικτό λογισμικό είναι σαν να έχεις πρόσβαση στο μηχανικό μέρος του αυτοκινήτου. Έστω και αν δεν μπορείς να επιδιορθώσεις μόνος σου την μηχανή, μπορείς τουλάχιστον να αλλάξεις τα λάδια ή να την πας σε μηχανικό.

Είναι αλήθεια, επίσης, ότι αν ένα πρόγραμμα ανοικτού λογισμικού χρησιμοποιείται ευρέως, οι ανανεώσεις του και οι επιδιορθώσεις θα εμφανίζονται πολύ πιο σύντομα από κάποιο κλειστό πρόγραμμα. Τα μάτια χιλιάδων προγραμματιστών μπορούν να βρουν σφάλματα πιο γρήγορα από τα μάτια κάποιων δεκάδων υπαλλήλων. Γι' αυτό πρέπει να επιλέγονται προγράμματα τα οποία χρησιμοποιούνται από πολλούς. Όσο πιο πολύ χρησιμοποιείται, τόσο πιο γρήγορα διορθώνεται.

4.3 Μπορεί να βρεθεί αυτό που χρειαζόμαστε

Το ανοικτό λογισμικό κυρίως φτιάχνεται από άτομα που θέλουν να το χρησιμοποιήσουν για τον εαυτό τους. Αντί να εξαρτώνται από τα τμήματα μάρκετινγκ για να βρούν τι θέλουν, οι πελάτες φτιάχνουν αυτά που χρειάζονται μόνοι τους. Οι υπόλοιποι έχοντας πρόσβαση στο ανοικτό λογισμικό το τροποποιούν για να ικανοποιήσουν τις δικές τους ανάγκες. Επειδή, λοιπόν, οι ανάγκες κάποιου μπορεί να συμπίπτουν με τις ανάγκες κάποιου άλλου, συνήθως δεν είναι δύσκολο να βρεθεί κάτι που να ικανοποιεί και τις δικές μας ανάγκες.

Επιπλέον, όταν ένα εργαλείο ανοικτού κώδικα δεν κάνει αυτά που χρειαζόμαστε, μπορούμε να το τροποποιήσουμε, συχνά εύκολα, για να ικανοποιήσει τις ανάγκες μας. Όχι μόνο αυτό, αλλά μπορεί να τροποποιηθεί και όσο γρήγορα όσο απαιτείται. Ένα παράδειγμα: έχουμε ένα εργαλείο ανοικτού κώδικα αλλά έχει έναν περιορισμό στο μέγεθος των αρχείων που διαχειρίζεται. Ένας προγραμματιστής από το προσωπικό μπορεί να τροποποιήσει το πρόγραμμα το ίδιο βράδυ και το πρωί η εταιρία να είναι έτοιμη να κάνει την δουλειά της. Σε περίπτωση, ομως, ενός εμπορικού προϊόντος, αυτο μπορεί να έπερνε και μήνες για να γίνει.

4.4 Το θέμα της ποιότητας

Ο πιο συχνός φόβος που αφορά στην χρήση του Ανοικτού Λογισμικού, ειδικά σε ευαίσθητα περιβάλλοντα όπως αυτής της διαχείρισης και παρακολούθησης δικτύων, είναι ότι δεν έχουν την ποιότητα των εμπορικών προϊόντων. Υπάρχει η αντίληψη ότι όταν πληρώνεις για κάτι, αυτό θα είναι και καλό. Εκ πείρας η απάντηση είναι πως αυτό δεν ισχύει. Μερικά ελεύθερα προϊόντα είναι όσο καλά, αν όχι και καλύτερα από τους εμπορικούς ανταγωνιστές τους. Για παράδειγμα ας πάρουμε το Multi Router Traffic Grapher (MRTG). Είναι το βασικό εργαλείο σε επιχειρήσεις για την γραφική απεικόνιση της χρήσης του bandwidth πάνω σε γραμμές δικτύου. Όταν ένα εργαλείο ανοικτού λογισμικού χρησιμοποιείται στην βιομηχανία,

ενώ θα μπορούσε να αγοραστεί άλλο εργαλείο με κόστος χιλιάδων ευρώ, τότε σημαίναι ότι αυτό που κάνει το κάνει σωστά και ποιοτικά.

Ασφαλώς, όπως υπάρχουν καλές και κακές εμπορικές εφαρμογές, υπάρχουν και καλά και κακα προϊόντα ανοικτού λογισμικού. Οι υποστηρικτές του ανοικτού λογισμικού υποστηρίζουν ότι το μοντέλο ανάπτυξης τέτοιου λογισμικού βοηθάει στη δημιουργία ποιοτικών προϊόντων. Ο μεγάλος αριθμός των ατόμων που το αναπτύσσουν είναι ένα πλεονέκτημα, καθώς και το γεγονός ότι επειδή είναι ανοικτό το σύστημα δεν μπορούν να κρύψουν κακής ποιότητας κώδικα. Από την άλλη πλευρά, υποστηρίζουν ότι ο μεγάλος αριθμός ατόμων δεν εξασφαλίζει απαραίτητα την ποιότητα και σε ορισμένα είδη λογισμικού, όπως τα open source device drivers, ο κώδικας μπορεί να αναγνωριστεί από τόσους λίγους που μερικές φορές περνάει απαρατήρητος.

Άξιο αναφοράς είναι το γεγονός ότι τα άτομα που αναπτύσσουν τέτοιου είδους λογισμικό είναι επαγγελματίες προγραμματιστές. Δουλεύουν σε ένα περιβάλλον στο οποίο το προϊόν τους δεν είναι ανάγκη να γίνει εμπορικό, αφού είναι λογισμικό το οποίο προέρχεται από πανεπιστήμια ή είναι αποτέλεσμα προσωπικής ενασχόλησης σε ελεύθερες ώρες. Η ποιότητα του λογισμικού πηγάζει απλά από την αγάπη τους για αυτο που κάνουν.

4.5 Είναι ασφαλές;

Μια κοινή κριτική για το ανοικτό λογισμικό αναφέρει ότι εφόσον ο κώδικας είναι ανοικτός για όλους, είναι πιο εύκολο για τους hackers να βρουν τις αδυναμίες τους και να τις εκμεταλλευτούν. Η προσδοκίες σχετικά με τα κλειστά συστήματα έχουν να κάνουν με το γεγονός ότι μπορούν να κρύψουν τις αδυναμίες τους. Η αλήθεια, όπως έχει επανελημμένα αποδειχθεί, παρουσιάζει ότι αυτό δεν ισχύει. Το Internet έχει αποκαλύψει πολλα σοβαρά προβλήματα ασφάλειας τόσο στα εμπορικά όσο και στα ανοικτού λογισμικού συστήματα. Το μόνο που διαφοροποιεί την κατάσταση μεταξύ των δύο κατηγοριών είναι ότι στα συστήματα ανοικτού λογισμικού τα λα΄θη διορθώνονται πιο γρήγορα, περιορίζοντας τις βλάβες που πιθανώς να προκληθούν.

Επιπλέον, ο μεγάλος αριθμός των ‘καλών’ προγραμματιστών αυξάνει την πιθανότητα μια αδυναμία να βρεθεί και να διορθωθεί πριν ανακαλυφθεί από τους hackers και να χρησιμοποιηθεί για κακούς σκοπούς. Την ίδια στιγμή, οι προγραμματιστές δεν θα δώσουν την ίδια προσοχή σε εμπορικά προϊόντα για αδυναμίες, ενώ οι hackers θα το κάνουν με σκοπό να βλάψουν κάποιο γνωστό software house.

4.6 Υποστήριξη

Ο μικρός βαθμός χρήσης του ανοικτού λογισμικού έγκειται στο γεγονός ότι συνήθως έρχεται χωρίς υποστήριξη. Εαν το λογισμικό δεν λειτουργεί σωστά, δεν υπάρχει κάποιος στον οποίο να παραπονεθείς ουτε κάποιος στον οποίο να αποδώσεις ευθύνες. Εάν είναι απαραίτητο να υπάρχει κάποιος για υποστήριξη σε περίπτωση αστοχίας του λογισμικού, τότε το ανοικτό λογισμικό δεν αποτελεί καλή λύση.

Αντίθετα, η πρώτη γραμμή υποστήριξης είναι το προσωπικό της εταιρίας. Όσο πιο πολύ έχει επενδύσει η εταιρία στην εκμάθηση του λογισμικού και της εσωτερικής λειτουργίας του, τόσο μεγαλύτερη πιθανότητα υπάρχει για να επιλυθεί το πρόβλημα. Μετά από αυτό, η γνώση μπορεί να μεταφερθεί και σε άλλους μέσω του διαδικτύου. Αν και αυτή η δυνατότητα αποτύχει, μπορεί πάντα να βρεθεί κάποιος σύμβουλος ο οποίος θα κάνει την δουλειά.

Τέλος, αν βρεθεί ανοικτό λογοσμικό το οποίο συνοδεύεται και από υποστήριξη, τότε αποτελεί την καλύτερη δυνατή λύση που μπορεί να προσφερθεί.

5. Κατηγορίες Προϊόντων Διαχείρισης & Παρακολούθησης Δικτύων

Πολλά προϊόντα λογισμικού που είναι διαθέσιμα αυτή τη στιγμή προσφέρουν αναλυτικές πληροφορίες με σκοπό να υποστηρίξουν τη διαχείριση των σχετικών με το δίκτυο συστημάτων, καλούμενων συνήθως ως "Το Δίκτυο".

Πολλές φορές αυτό το λογισμικό περιγράφεται γενικά ως ‘όργανα ελέγχου δικτύων’. Αυτά τα προϊόντα τοποθετούνται κάτω από μια συγκεχυμένη σειρά όρων. Αν και αυτά τα προϊόντα ελέγχουν, μπορούν να είναι πολύ συγκεκριμένα ή ένα πακέτο λογισμικού που περιέχει διάφορα προϊόντα που ελέγχουν λειτουργίες που περιγράφονται παρακάτω.

Οι κατηγορίες που μπορούν να διακριθούν αυτά τα συστήματα ανοικτου λογισμικού είναι

- Enterprise Management: πλήρεις λύσεις για την επιχείρηση, με την ολοκληρωμένη διαχείριση δικτύων & συστημάτων, βάσεων δεδομένων, εφαρμογών. Δεν είναι ασυνήθιστο για αυτά τα προϊόντα να αποτελελούνται από ενότητες και να είναι πολύ εκτεταμένα, καλύπτοντας χαρακτηριστικά γνωρίσματα όπως η το Job Scheduling.

- Network & System Monitoring: ενισχυμένα με πολλές δυνατότητες εμπορικά εργαλεία ελέγχου δικτύων & συστημάτων. Αυτός ο χρήστης να είναι ένα NOC (Network Operations Center), ο οποίος θέλει να διαχειριστεί το Δίκτυο και τους διακομιστές.

- Network Traffic Analyzing & Performance Monitoring: Παρακολούθηση της ροής από και προς τις κρίσιμες συσκευές δικτύου, στατιστικές χρήσης, παρακολούθηση της επίδοσης του δικτύου.

- Application Monitoring: έλεγχος απόδοσης και συμπεριφοράς της εφαρμογής. Είναι η εφαρμογή, το δίκτυο, ο client ή ο server που προκαλεί πρόβλημα;

- Device Monitoring: Παρακολούθηση και καταγραφή των ενεργιών στους διακομιστές και στις συσκευές του δικτύου.

- Protocol Analyzers and Packet Capture Tools: Εργαλεία σύλληψης πακέτων, sniffers δικτύων, παρακολούθηση απόδοσης.

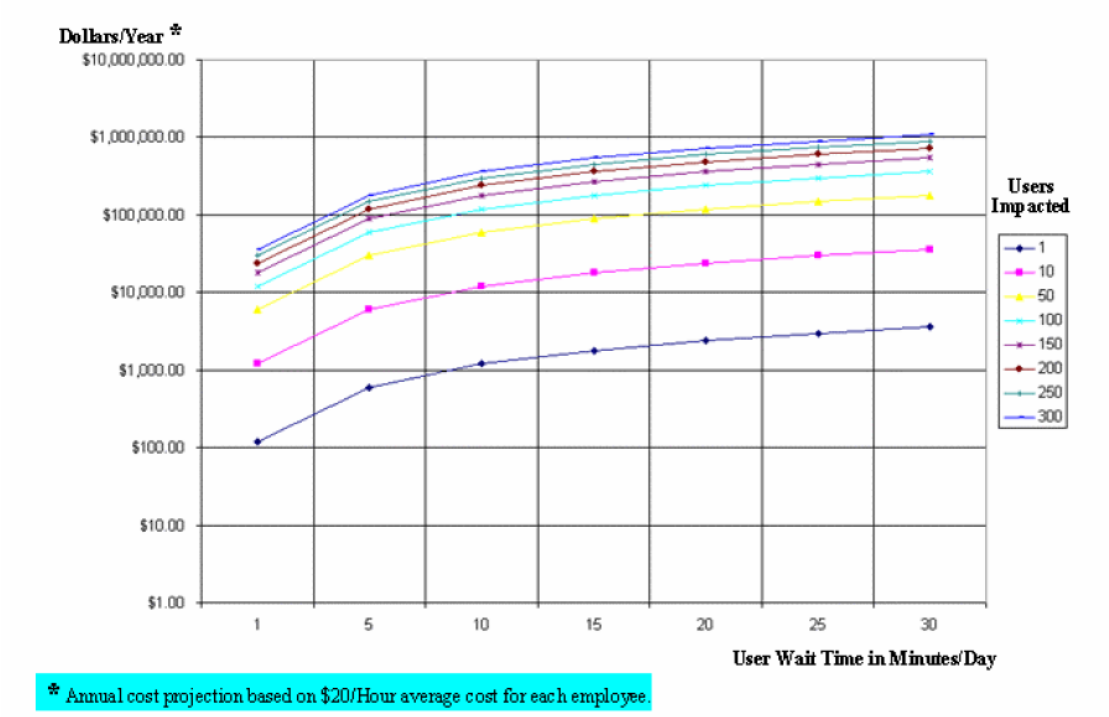
- Security Monitoring: Παρακολούθηση της ασφάλειας του δικτύου, των σταθμών εργασίας και των διακομιστών

- Web Monitoring: Παρακολούθηση του διαδικτύου και ανάλυση των επιμέρους παραμέτρων του.

Τα παραπάνω προϊόντα έχουν ένα κοινό σκοπό: να υποστηρίζουν, να παρακολουθούν και να παρέχουν αποδοτικές εργασίας δικτύου. Εργαλεία τα οποία προσφέρουν ανάλυση σε βαθμό ρίζας του προβλήματος εξοικονομούν πολλές ώρες εργασίας και σε πολλές περιπτώσεις μπορούν να λύσουν προβλήματα που διαφορετικά δεν θα ήταν δυνατό να ανακαλυφθούν. Και σε περιπτώσεις κατάρρευσης του δικτύου, και μεγάλες αναμονές απόκρισης σε εφαρμογές προκαλούν απώλεια πωλήσεων, δυσαρεστημένους πελάτες και μειωμένη παραγωγικότητα χρηστών.

Το παρακάτω γράφημα δείχνει ένα από τα κόστη που προκαλεί η παρατεταμένη κατάρρευση του δικτύου και η μεγάλη αναμονή στην απόκριση του συστήματος.

Η παρατεταμένη κατάρρευση δικτύου και μεγάλη αναμονή στην απόκριση εφαρμογής προκαλούν σημαντικά κόστη τα οποία εμφανίζονται γρήγορα.



Εικόνα 1: Κόστη από προβλήματα στο δίκτυο

Για παράδειγμα, αν 10 χρήστες χάνουν 10 λεπτά από την ημέρα τους είτε από προβλήματα δικτύου είτε από προβλήματα στην επίδοση, έχουν κόστος $10000 τον χρόνο και οι 30 χρήστες πλησιάζουν τα $500000. Αυτό δείχνει ότι το θέμα αφορά και τις μεγάλες και τις μικρές επιχειρήσεις.

Ανάλογα με τις ανάγκες της επιχείρησης, χρειάζεται να χρησιμοποιηθούν διαφορετικά εργαλεία για να εμποδίσουν τα κόστη που προκαλούν τα προβλήματα στο δίκτυο. Η απόφαση αυτή, σε συνδιασμό με την χρήση ανοικτού και ελεύθερου λογισμικού μπορεί να μειώσει το κόστος λειτουργίας μιας επιχείρησης στο ελάχιστο.

5.1 Protocol Analyzer

Τα εργαλεία αυτά έχουν συχνά ενσωματωμένη νοημοσύνη που βοηθά εκείνον που διαχειρίζεται και ανιχνεύει λάθη στο φυσικό δίκτυο. Οι συσκευές ανάλυσης παρέχουν ένα παράθυρο για την κατάσταση του δικτύου και επιδεικνύουν μια στιγμιαία εικόνα της κατάστασης κυκλοφορίας με τον έλεγχο της κυκλοφορίας του δικτύου σε πραγματικό χρόνο. Κυριολεκτικά κυνηγούν , προσδιορίζουν, και απομονώνουν τα προβλήματα και την κυκλοφοριακή συμφόρηση στο δίκτυο. Τα προηγμένα χαρακτηριστικά γνωρίσματα των συστημάτων εξαλείφουν την ανάγκη για ταξινόμηση χιλιάδων πακέτων για να ανακαλύψουν και να ποσοτικολογήσουν τις καταστάσεις προβλημάτων. Παρέχουν, επίσης, συμβουλές για τους τρόπους επιδιορθόρθωσης των προβλημάτων.

Οι Protocol Analyzers συναντώνται είτε ως υλικό είτε ως λογισμικό. Καθώς είναι συνήθως εγκατεστημένοι στα PC με Windows, πρέπει να είναι χρησιμοποιήσιμες από οποιοδήποτε διαχειριστή δικτύων, ανεξάρτητα από το επίπεδο εμπειρίας. Οι διαχειριστές και οι μηχανικοί δικτύων χρησιμοποιούν αυτά τα εργαλεία για να επιλύσουν τα προβλήματα δικτύων, να μειώσουν το κόστος του χρόνου μη λειτουργίας του δικτύου και να αυξήσουν την παραγωγικότητα.

5.2 Application Performance Software

Η πρωταρχική αιτία της απόδοσης μιας εφαρμογής δεν είναι τετριμμένη ερώτηση. Ο κώδικας λογισμικού, η αρχιτεκτονική του συστήματος, το υλικό των διακομιστών και η διαμόρφωση των δικτύων μπορούν όλα να επηρρεάσουν την απόδοση μιας εφαρμογής. Αυτά τα εργαλεία αναπτύσσονται για να παρέχουν συγκεκριμένες πληροφορίες για τον τρόπο με τον οποίο το σύστημα συμπεριφέρεται συνολικά.

Τα εργαλεία απόδοσης των εφαρμογών θα καθορίσουν την απόδοση των clients και του κεντρικού υπολογιστή, το εύρος ζώνης του δικτύου και την καθυστέρηση. Παρέχουν έναν χάρτη της συναλλαγής, όπου ο ύποπτος κώδικας μπορεί να αξιολογηθεί. Τα περιπλοκότερα εργαλεία σε αυτήν την περιοχή έχουν υψηλού επιπέδου δυνατότητα αναζήτησης και μπορούν να παρέχουν πληροφορίες που συγκεντρώνονται από τις συνομιλίες πελατών και κεντρικών υπολογιστών ή από διακομιστή σε διακομιστή. Οι διαχειριστές των δικτύων καθώς επίσης και οι προγραμματιστές μπορούν να χρησιμοποιήσουν αυτά τα εργαλεία. Ο αργός χρόνος απόκρισης μπορεί να είναι δαπανηρός αλλά ακόμα και αν αποτελεί είναι ένα μικρό μέρος της ημέρας, μπορεί πραγματικά να προσθέσει μεγάλο κόστος όταν υπάρχουν εκατοντάδες χρήστες, όπως φαίνεται στη γραφική παράσταση ανωτέρω.

5.3 Network Planning and Modelling Software

Αυτά τα προϊόντα συνήθως έχουν ενσωματωμένη την ειδική γνώση για το πώς οι συσκευές δικτύων, τα πρωτόκολλα δικτύων, οι εφαρμογές, ακόμη και οι κεντρικοί υπολογιστές λειτουργούν. Αυτή η νοημοσύνη επιτρέπει στους μηχανικούς δικτύων, τους αρμόδιους για το σχεδιασμό δικτύων, τους μηχανικούς λογισμικού και τις ομάδες επέκτασης εφαρμογών να προγραμματίσουν ή να προβλέψουν τον αντίκτυπο των αλλαγών στο δίκτυο ή της επέκτασης μιας εφαρμογής. Οι περισσότεροι παρέχουν γραφική ικανότητα χαρτογράφησης ώστε να απεικονιστεί το δίκτυο. Η αιτιολόγηση για την ύπαρξη αυτών των εργαλείων είναι ο δαπανηρός μπελάς μιας κακής εφαρμογής.

5.4 Device Monitor

Τυπικά αυτό ελέγχει την κατάσταση των συσκευών του δικτύου και παρέχει έναν γραφικό χάρτη της κατανομήςτου δικτύου, επιτρέποντας την διαχείριση ενός μεγάλου δικτύου από μια διεπαφή χαρτών. Αυτοί είναι ο συχνότερα κεντρικοί υπολογιστές και εκτυπωτές. Πολλοί παρέχουν χαρακτηριστικά γνωρίσματα όπως ο έλεγχος uptime των χρόνων απόκρισης συσκευών, και ένα σύστημα ανακοίνωσης βασισμένο σε triggers για να προειδοποιήσουν για τα προβλήματα δικτύων. Τα εργαλεία θα ελέγξουν ακόμη και τα services και τα ports. Αυτό δημιουργεί ένα δυναμικό περιβάλλον που μειώνει το χρόνικό διάστημα στο οποίο οι χρήστες επηρρεάζονται. Παρέχουν συνήθως και τον τοπικό και μακρινό έλεγχο σε ένα συνδεδεμένο δίκτυο και είναι πιθανότερο να χρησιμοποιηθεί από τους διαχειριστές συστημάτων.

5.5 SNMP Device Monitor

Η συντομογραφία SNMP (Simple Network Management Protocol) παρέχει ένα σύνολο πρωτοκόλλων για τη διαχείριση σύνθετων δικτύων. Οι πρώτες εκδόσεις του SNMP αναπτύχθηκαν στην αρχή της δεκαετίας του '80. Το SNMP λειτουργεί με την αποστολή μηνυμάτων στα διαφορετικά μέρη ενός δικτύου.

Οι SNMP-συμβατές συσκευές, αποκαλούμενες πράκτορες (agents), αποθηκεύουν τα στοιχεία για τους στις βάσεις διοικητικών πληροφοριών (Management Information Bases, MIBs) και επιστρέφουν αυτό το στοιχείο στους αιτούντες SNMP. Παραδείγματα των διοικούμενων συσκευών σε ένα δίκτυο περιλαμβάνουν τους κεντρικούς υπολογιστές, τους διακόπτες και τους δρομολογητές.

Τα SNMP Device Monitors μπορούν να λάβουν τη μορφή ενός διοικητικού σταθμού που συγκεντρώνει και που επιδεικνύει τις πληροφορίες από τους διοικούμενους πράκτορες. Ένας διοικητικός σταθμός είναι η θέση όπου ένας διαχειριστής μπορεί να δει, να αναλύσει και ακόμη να διαχειριστεί τις συσκευές δικτύου. Αυτό δημιουργεί πάλι ένα δυναμικό περιβάλλον που μειώνει τον χρόνο στον οποίο οι χρήστες επηρρεάζονται. Στο σημερινό μεταβαλλόμενο περιβάλλον, παρέχει τις πληροφορίες στους αναλυτές δικτύων για το πώς να απομονώσει τις συσκευές που μπορεί να δημιουργούν προβλήματα, μειώνοντας κατά συνέπεια το χρόνο ανίχνευσης λαθών.

5.6 Network Application Monitoring

Αυτός ο τύπος λογισμικού μπορεί να βοηθήσει τους διαχειριστές δικτύων και συστημάτων να καταλάβουν πώς οι εφαρμογές διατρέχουν την υποδομή του WAN/LAN. Αυτά τα εργαλεία συλλέγουν λεπτομέρειες μέτρησης απόδοσης για την κυκλοφορία δικτύων, τις εφαρμογές, την καθυστέρηση και τους χρόνους απόκρισης.

Έχοντας μια άποψη των εφαρμογών πέρα από τα συγκεκριμένα πρωτόκολλα, επιτρέπει στο προσωπικό δικτύωσης να προσδιορίσει σαφώς και γρήγορα τα λάθη με την παροχή των απαραίτητων πληροφοριών, ώστε να καταλάβουν την αλληλεπίδραση μεταξύ των εφαρμογών και του δικτύου. Οι διαχειριστές συστημάτων, ο διαχειριστής δικτύων, ο μηχανικός και οι αρμόδιοι για το σχεδιασμό δικτύων χρησιμοποιούν αυτά τα εργαλεία.

5.7 Client Monitoring

Αυτά τα πιό συγκεκριμένα εργαλεία ελέγχου συσκευών παρέχουν ένα πλήρες μέτρο της εμπειρίας τελικών χρηστών με την καταγραφή των χρόνων απόκρισης, της χρήσης των πόρων, των ελαττωμάτων εφαρμογής και της διαθεσιμότητας. Αυτά τα εργαλεία όχι μόνο ελέγχουν ότι τα επίπεδα υπηρεσιών επιτυγχάνονται, αλλά μπορούν και να χρησιμοποιηθούν ενεργά όταν τα επίπεδα υπηρεσιών τείνουν προς τα κάτω.

5.8 Security Monitoring

Αυτά τα προϊόντα παρέχουν δοκιμές ασφάλειας δικτύων, πληροφορίες ασφάλειας, υπηρεσίες ασφάλειας δικτύων και εκθέσεις αξιολόγησης της ασφάλειας. Πολλά από αυτά είναι πολύ εξειδικευμένα προϊόντα.

5.9 Server Monitoring

Αυτά τα όργανα ελέγχου παρέχουν πληροφορίες για την ΚΜΕ, τη μνήμη και τη χρήση του χώρου των δίσκων. Μπορούν επίσης να ελέγξουν τη διαθεσιμότητα και την απόδοση των εφαρμογών, των βάσεων δεδομένων και των κεντρικών υπολογιστών. Πάλι, αυτή η κατηγορία λογισμικού τείνει να είναι μια πολύ προηγμένη και συγκεκριμένη μορφή ελέγχου συσκευών και μπορεί να περιλάβει τον έλεγχο SNMP.

5.10 Web Monitoring

Αυτός τον τύπο ελέγχου εστιάζει στους κεντρικούς υπολογιστές διαδικτύου και τα σχετικά πρωτόκολλα δικτύων. Μπορούν να ποικίλουν, από τον έλεγχο των συνομιλιών μέχρι την απόδοση κεντρικών υπολογιστών. Πολλά από τα εργαλεία συσκευών ανάλυσης και ελέγχου έχουν πολύ ειδικευμένα χαρακτηριστικά γνωρίσματα του Ιστού.

6 Εργαλεία Ανοικτού Λογισμικού για παρακαλούθηση δικτύων

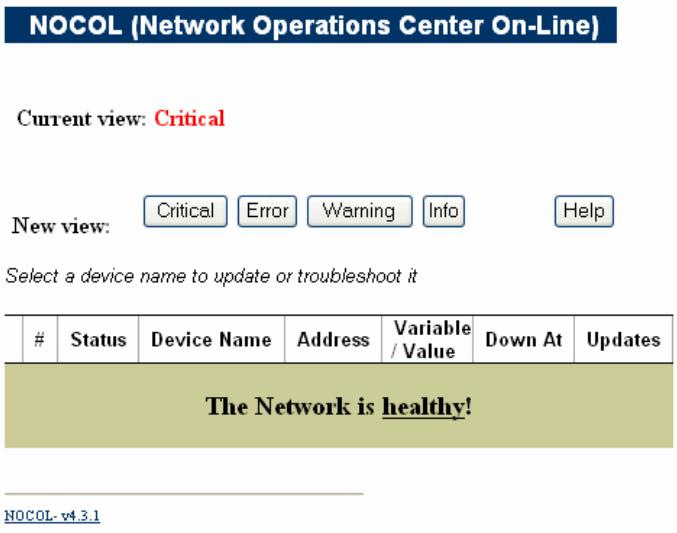
Πολλές επιχειρήσεις θέλουν να παρακολουθήσουν τις μηχανές στα δίκτυά τους. Εάν μια υπηρεσία αποτύχει, οι σχετικοί άνθρωποι πρέπει να ενημερωθούν γρήγορα. Υπάρχει μεγάλη ποικιλία εμπορικού λογισμικού το οποίο μπορεί να το κάνει αυτό: HPOpenView, Patrol και Netcool/Omnibus είναι μεταξύ των καλύτερων και ιδιαιτέρως γνωστών πακέτων. Παρόλα αυτά, είναι όλα πολύ ακριβά και απαιτούν εξειδιευμένες συσκευές, όπως αφιερωμένους κεντρικούς υπολογιστές ελέγχου.

Η κοινότητα του ελεύθερου λογισμικού έχει παράγει διάφορα προγράμματα που εξυπηρετούν τον ίδιο στόχο. Ενώ τείνουν να μην έχουν γραφικές διεπαφές όπως τις εμπορικές εφαρμογές, είναι είναι γενικά λιγότερο απαιτητικοί από την άποψη των πόρων συστημάτων, μην απαιτώντας έναν αφιερωμένο κεντρικό υπολογιστή αλλά κάποιον ικανό να εκτελέσει πολλά προγράμματα ταυτόχρονα. Τείνουν επίσης να γίνουν περισσότερο ανοικτά και επεκτάσιμα από τα εμπορικά πακέτα, που αποτελεί όφελος ειδικά όταν αναπτύσσονται εξειδικευμένες υπηρεσίες. Όλες οι εφαρμογές που περιγράφονται εδώ παρέχονται με μορφή πηγαίου κώδικα, και τρέχουν σε Windows, Linux, FreeBSD, και στις περισσότερες εκδόσεις Solaris.

6.1 Nocol

Το NOCOL (Network Operations Centre On-Line) ήταν στην ανάπτυξη για μερικά έτη, και παρέχει ένα αρκετά περιεκτικό σύνολο δοκιμών. Η ανάπτυξη είναι αργή, αν και είναι ακόμα ενεργή. Η δοκιμή των υπηρεσιών Διαδικτύου μπορεί πραγματοποιηθεί μέσω του portmon, το οποίο συνδέεται με συγκεκριμένα ports, στέλνει κείμενο και ελέγχει τις απαντήσεις. Ο έλεγχος SNMP είναι διαθέσιμος, αλλά είναι μάλλον δύσκολος να εγκατασταθεί.

Το κύριο αποτέλεσμα είναι μια εφαρμογή κονσόλας, αλλά μπορούν να παραχθούν και ιστοσελίδες. Αυτό επιτρέπει την προσθήκη σημειώσεων στις μηχανές με τα προβλήματα, αλλά όχι αλλαγές στον έλεγχο. Η οδήγηση ενός συστήματος σελιδοποίησης επιτυγχάνεται εύκολα. Οι απομακρυσμένες επεκτάσεις οργάνων ελέγχου υπάρχουν για μια σειρά συστημάτων, αλλά πάλι μπορούν να δύσκολες να εγκατασταθούν, και η ασφάλεια είναι ελάχιστη. Δεν υπάρχει καμία ιεραρχία δικτύων, έτσι μια αποτυχία των δρομολογητών οδηγεί σε έναν μεγάλο αριθμό ταυτόχρονων μηνυμάτων. Το σύστημα πρέπει να επανεκινηθεί για να προσθέσει τα νέα όργανα ελέγχου. Οι δοκιμές γίνονται παράλληλα για τα περισσότερα όργανα ελέγχου.

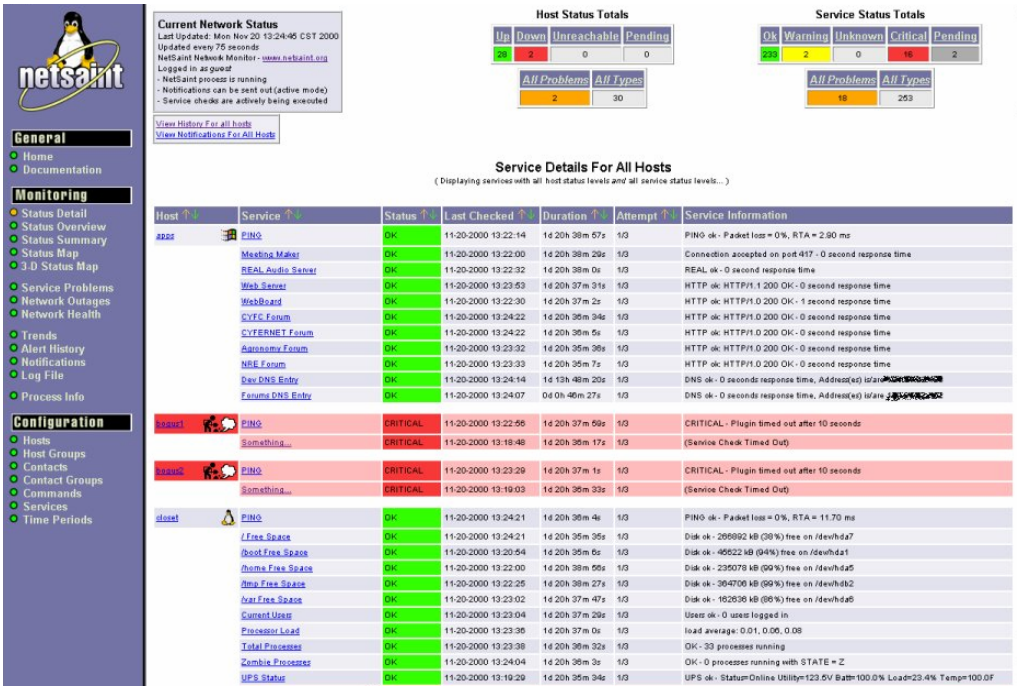


Εικόνα 2: Nocol

6.2 Netsaint

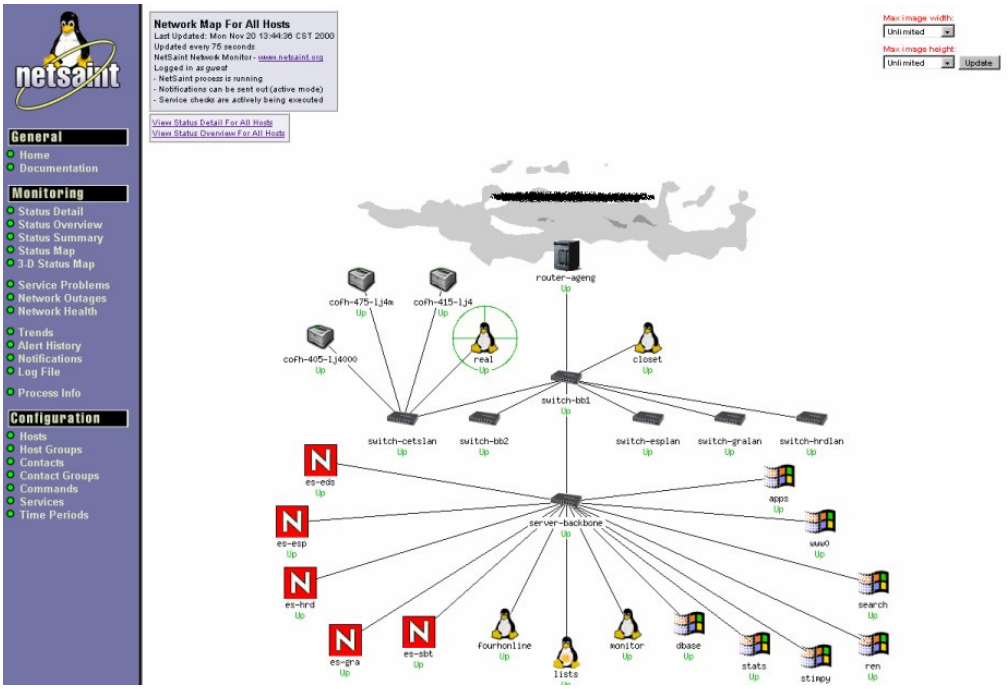
Το Netsaint είναι ένα λεπτομερές, εκτάσιμο σύστημα. Έρχεται με μια εντυπωσιακή σειρά οργάνων ελέγχου (plug-ins), η οποία αναπτύσσεται χωριστά από τον κώδικα του πυρήνα. Η σειρά των δοκιμών είναι μεγάλη, συμπεριλαμβανομένων βάσεων δεδομένων, SNMP, ακόμη και κεντρικοί υπολογιστές παιχνιδιών. Η εγκατάσταση είναι εξαιρετικά εύκολη, και ένας νέος χρήστης μπορεί να πάρει μια διαμόρφωση οργάνων ελέγχου εργασίας σε μερικές ώρες ακόμη και για ένα μέσο ή μεγάλο δίκτυο.

Η κύρια παραγωγή των οθονών είναι web-based, αλλά είναι μόνο για ανάγνωση. Για να αλλάξει η διαμόρφωση, τα αρχεία οργάνωσης πρέπει να τροποποιηθούν και η εφαρμογή να επανεκινήσει. Η εξελιξιμότητα είναι ικανοποιητική. Το λογισμικό τρίτων είναι διαθέσιμο για να επιτρέψει την εκτέλεση των πακέτων ελέγχων στις μακρινές μηχανές. Τα παρεχόμενα extensions απομακρυσμένης παρακολούθησης χρησιμοποιούν αυθεντικοποίηση και κρυπτογράφηση για να προστατέψει τα δεδομένα π[ου διακινούνται, ακόμα και σε σημεία που δεν είναι προστατευμένα από firewalls.



Εικόνα 3: Netsaint – Status Detail Screen

Πιθανώς το σημαντικότερο χαρακτηριστικό γνώρισμα του Netsaint είναι το σύστημα χειριστών γεγονότος (event handler system). Αυτό μπορεί να χρησιμοποιηθεί για να προσπαθήσει να επανεκινήσει τις υπηρεσίες που έχουν αποτύχει χωρίς απαίτηση της ανθρώπινης επέμβασης. Συνδυασμένο με το ssh και την κατάλληλη βασική διανομή, αυτό είναι ένα εξαιρετικά ισχυρό εργαλείο. Η ιεραρχία δικτύων υποστηρίζεται για τους οικοδεσπότες (hosts), αλλά όχι για τις υπηρεσίες (services) πάνω σε εκείνους τους οικοδεσπότες.



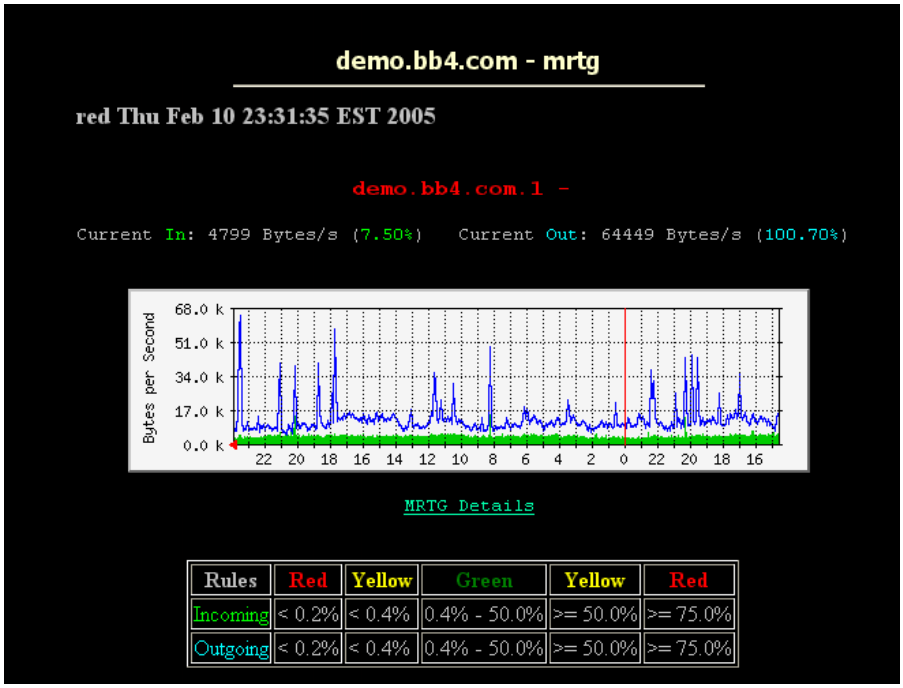
Εικόνα 4: Netsaint – Status Map Screen

6.3 Big Brother

Το Big Brother είναι η τελευταία των τριών "σημαντικών" πακέτων ελέγχου. Στηρίζεται αποκλειστικά σε web-based εμφάνιση και είναι εξαρτώμενη από γραφικό browser. Δεδομένου ότι περιέχει επίσης πολλά κινούμενα GIFs, τείνει να επιβραδύνει τους περισσότερους ξεφυλλιστές. Η παρεχόμενη σειρά των οργάνων ελέγχου είναι εύλογα καλή, καλύπτοντας τις περισσότερες από τις τυποποιημένες υπηρεσίες, εν τούτοις δεν περιλαμβάνει SNMP ή παιχνίδια. Η δοκιμή γίνεται παράλληλα, αλλά δεν υπάρχει καμία υποστήριξη ιεραρχίας και το σύστημα πρέπει να επανεκινήσει για να προσθέσει τα νέα όργανα ελέγχου.

Το remote monitoring του είναι περιεκτικό και, αντίθετα από τις περισσότερες υπόλοιπες εφαρμογές, περιλαμβάνει πελάτες για τα συστήματα NT. Εντούτοις, οι remotely-monitored πληροφορίες εκτίθενται σε καθέναν που μπορεί να συνδεθεί με το σχετικό port, δεδομένου ότι δεν υπάρχει καμία επικύρωση, κρυπτογράφηση ή IP-βασισμένη ασφάλεια. Το BB έχει ένα πλήρες σύστημα ειδοποιήσεων (notifications), συμπεριλαμβανομένης της αναγνώρισης και της κλιμάκωσης, η οποία είναι πιθανώς η καλύτερη από οποιαδήποτε άλλη εφαρμογή.

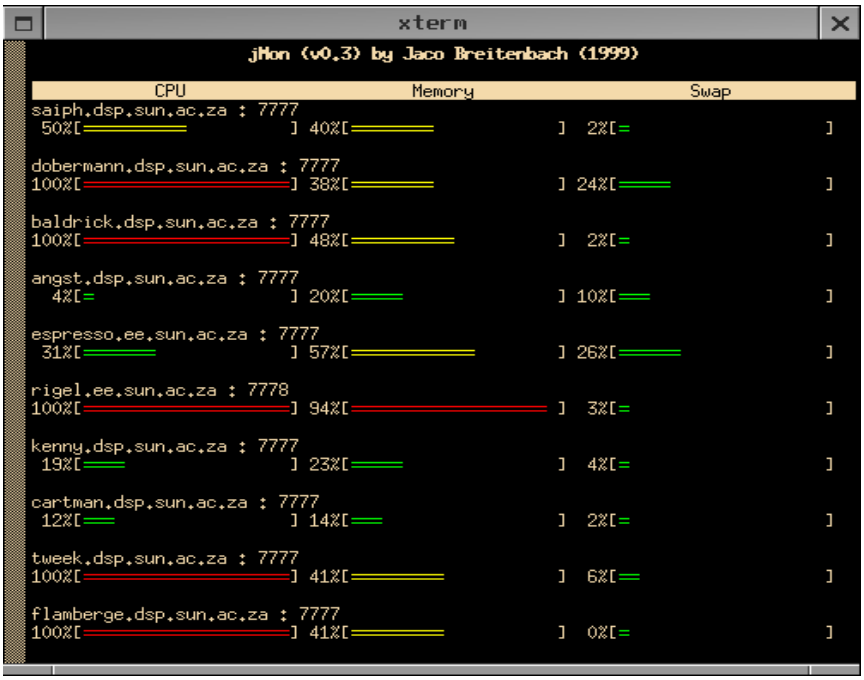
Αντίθετα από όλα τα άλλα προγράμματα που παρουσιάζονται εδώ, που είναι πραγματικά ελεύθερο λογισμικό, το BB απαιτεί μια βαριά αμοιβή αδειών για την εμπορική χρήση. Αυτό το ξεπερασμένο σχέδιο είναι πιθανώς ο κύριος λόγος που δεν είναι ευρέως διαδεδομένος.



Εικόνα 5. Big Brother

6.4 JMon

Το JMon είναι μια εφαρμογή μακρινού ελέγχου (remote monitoring) που εκθέτει την ΚΜΕ, τη μνήμη και την ανταλλαγή με τις μακρινές μηχανές. Η παραγωγή είναι μέσω της κονσόλας μόνο, και configurability είναι πολύ χαμηλό. Η ασφάλεια είναι επίσης κάπως φτωχή, χωρίς την κρυπτογράφηση να συμπεριλαμβάνεται ή να προστίθεται εύκολα.



Εικόνα 6: JMon

6.5 Συμπέρασμα

Συνολικά, το Netsaint εμφανίζεται να είναι το καλύτερο πακέτο παρακολούθησης δικτύων. Είναι εύκολο να εγκατασταθεί γρήγορα, και παρέχει ένα περιεκτικό όργανο ελέγχου. Εντούτοις, η έλλειψη παραλληλησμού στην τρέχουσα έκδοση είναι ένα πρόβλημα. Ενώ ο κώδικας ανάπτυξης είναι εύλογα σταθερός, άλλες αλλαγές κάνουν την αναβάθμιση σημαντικό στόχο. Το NOCOL είναι επίσης εύκολο να εγκατασταθεί και προσφέρει τον παράλληλο έλεγχο, αν και η σύνταξη εντολής είναι κάπως λιγότερο διαισθητική. Η Web διεπαφή φαίνεται κάπως δυσκίνητη. Τα άλλα δύο εργαλεία που παρουσιάστηκαν είναι λίγο ξεπερασμένα, παρόλο που σε ορισμένες περιπτώσεις μπορούν να βοηθήσουν σε καταστάσειςόπου δεν χρειάζονται ιδιαίτερες συνθήκες παρακολούθησης.

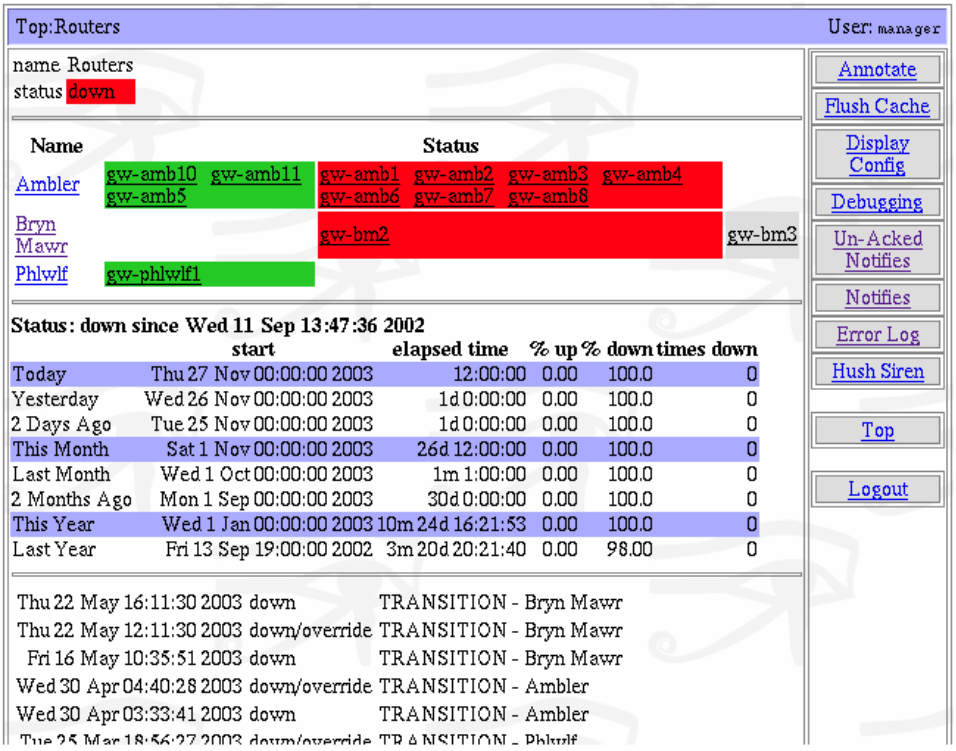
7 Εργαλεία Ανοικτού Λογισμικού για διαχείριση δικτύων

Σε αυτό το σημείο θα παρουσιαστούν μερικά ολοκληρωμένα εργαλεία διαχείρισης δικτύων.

7.1 Argus

Το Argus σχεδιάστηκε αρχικά για να παρακολουθεί servers και συνδέσεις δικτύων για ISPs (Internet Service Providers). Τώρα μπορεί να χρησιμοποιηθεί από μεγάλο μέρος επιχειρήσεων. Τα βασικά χαρακτηριστικά του είναι:

- Είναι open source και διατίθεται δωρεάν
- Έχει όμορφο web interface
- Οι ιστοσελίδες μπορούν να κατανοηθούν από άτομα χωρίς σχετική εμπειρία
- Δημιουργει γραφικά για το τι συμβαίνει
- Παρακολουθεί κίνηση δικτύων
- Μπορεί να παρακολουθεί το περιεχόμενο των web σελίδων
- Μπορεί να παρακολουθεί τα αποτελέσματα εντολών SQL
- Προειδοποιεί κάποιον για οτιδήποτε συμβαίνει
- Κρατάει ιστορικά δεδομένων
- Χρησιμοποιεί groups χρηστών
- Υποστηρίζει IPv6
- Υποστήρίζει SNMPv3
- Υποστηρίζει πολυγλωσία.



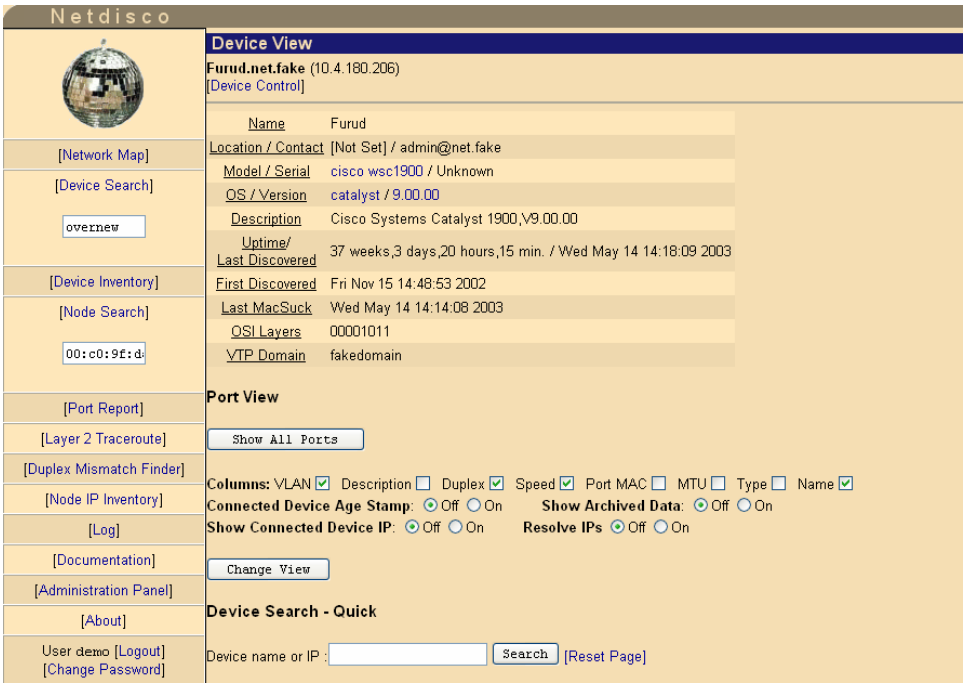
Εικόνα 7: Argus

7.2 NetDisco

Το NetDisco είναι ένα πρόγραμμα ελεύθερου λογισμικού βασισμένο στο web. Έχει σχεδιαστεί για μεσαία και μεγάλα δίκτυα και με την χρήση του SNMP συγκεντρώνει πληροφορίες σχετικά με την διάρθρωση και την δύνδεση των δεδομένων. Τα δεδομένα αποθηκεύονται σε σχεσιακή βάση δεδομένων για ευελιξία και ταχύτητα.

Χαρακτηριστικά:

- Κεντρική διαχείριση port/συσκευών
- Πλοήγηση με χρήση web
- Χρήση βάσεων δεδομένων
- Απόκρυψη πληροφοριών σε μη εξουσιοδοτημένους χρήστες
- Ασφάλεια στην διαχείριση
- Δημιουργία αναφορών
- Δημιουργία στατιστικών



Εικόνα 8: NetDisco

8. Προτάσεις για μελλοντική έρευνα

Η διαχείριση και η παρακολούθηση δικτύων αποτελεί τομέα εφαρμογών ο οποίος ήδη διανύει κάποιες δεκαετίες ζωής. Όσο περνάει, όμως, ο καιρός και με την αυξανόμενη ανάγκη για δικτύωση των υπολογιστών, η ανάγκη για ανάπτυξη νέων μεθόδων και τεχνολογιών είναι πέρα από κάθε τι άλλο ορατή. Οι τομείς στους οποίους υπάρχουν δυνατότητες βελτίωσης των διαδικασιών μέσω την εντατικής έρευνας μπορούν να προσδιοριστούν στους παρακάτω:

Διαχείριση των δικτύων μέσω απομακρυσμένης πρόσβασης με την ταυτόχρονη δημιουργία τρισδιάστατης γραφικής απεικόνισης της τοπολογίας του δικτύου.
Βελτίωση του SNMP ώστε να υποστηρίζει πολύ μεγάλα δίκτυα με μεγαλύτερη ασφάλεια.
Βελτίωση της γραφικής διεπαφής των open source εργαλείων, ώστε να μπορούν να χρησιμοποιηθούν και από άπειρους χρήστες.

Σε όλους τους παραπάνω τομείς έχουν ήδη γίνει κάποιες εργασίες για την βελτίωση τους, αλλά δεν έχουν φτάσει σε ικανοποιητικό επίπεδο. Στο μέλλον, όμως, η έρευνα αυτή αναμένεται να εντατικοποιηθεί και να παρουσιάσει τα αποτελέσματά της στις επόμενες εφαρμογές της διαχείρισης και παρακολούθησης των δικτύων.

9. Βιβλιογραφία

9.1 Web Sites

1. CIO Magazine (3/15/03) "Your Open Source Plan" http://www.cio.com/archive/031503/opensource.html InfoWorld (10/24/03) "Open Source

2. Citizenship" http://www.infoworld.com/article/03/10/24/42OPstrategic_1.html O'Reilley

3. OpenSource: http://opensource.oreilly.com/ Difference between free (GNU.org) and

4. OpenSource: http://www.oreilly.com/pub/a/oreilly/ask_tim/2003/gnusource_0703.html Gnu

5. Free Software Directory: http://www.gnu.org/directory/ Freshmeat (OSDN repository): http://freshmeat.net SourceForge (OSDN repository): http://sourceforge.net/ Dravis Group

6. Report on OSS http://www.infodev.org/symp2003/publications/OpenSourceSoftware.pdf

7. Open Source Tools in Network Management Waking a Sleeping Giant, http://www.linux.ncsu.edu/lug/lectures/opennms/

8. Network Monitoring Tools, http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html

9. Network Monitoring Management, http://www.cotse.com/tools/netman.htm

10. Network Monitoring White Papers, Webcasts and Case Studies, http://itresearch.forbes.com/rlist/term/Network-Monitoring.html

11. ITPRC – Network Management, http://www.itprc.com/nms.htm

9.2 Βιβλία - Papers

1. Evolution of Network Monitoring (2003), Interloci Network Management

2. Network Management: Open-Source Tool Options (May 2004), Michael Martone

3. Network Management Software (2003, 2004), Operative Software Products

4. Open Source Network Monitoring Software (November 2000), Roger Burton West

5. Network Performance Toolkit Using Open Source Testing Tools, Richard Blum

6. Open Source Network Administration (2004), James M Kretchmar