Πανεπιστήμιο Πειραιώς
Τμήμα Ψηφιακών Συστημάτων

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ & ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΚΑΤΕΥΘΥΝΣΗ: ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ:

Θέματα Ασφάλειας σε Σύννεφα Υπολογιστών (Cloud Computing)

Project: Μετάβαση της ολοκληρωμένης εφαρμογής Πληροφοριών (Εταιρειών - Πρωτοκόλλων - Φ.Ε.Κ. - Εκτυπώσεων) του Εθνικού Τυπογραφείου σε ασφαλές περιβάλλον Cloud Computing

ΖΑΓΟΥΡΑΣ ΠΑΝΑΓΙΩΤΗΣ ΜΤΕ1048

VMware for Linux 1.0 (1999) booting Windows 95 and Windows 98 on Red Hat Linux 5.2

Επιβλέπων: ΛΑΜΠΡΙΝΟΥΔΑΚΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ
Επίκουρος Καθηγητής

ΑΘΗΝΑ , ΟΚΤΩΒΡΙΟΣ 2012

ΑΚΑΔΗΜΑΪΚΟ ΕΤΟΣ 2011-2012

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον καθηγητή μου κ. Λαμπρινουδάκη Κωνσταντίνο για την άψογη συνεργασία που είχα μαζί του και τη δυνατότητα που μου έδωσε να μελετήσω ένα τόσο σύγχρονο και ιδιαίτερο θέμα που σχετίζεται άμεσα με το χώρο εργασίας μου.

Ευχαριστώ επίσης όλους τους ακαδημαϊκούς του συγκεκριμένου μεταπτυχιακού προγράμματος για την πολύτιμη προσφορά των γνώσεών τους –μέσα στα πλαίσια της εκπαίδευσης– ως προς το εξειδικευμένο πεδίο της ασφάλειας ψηφιακών συστημάτων.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου για την συμπαράσταση και τη στήριξη της κατά τη διάρκεια των σπουδών μου.

«Η παιδεία, καθάπερ ευδαίμων χώρα, πάντα τα αγαθά φέρει».
Σωκράτης (469-399 π.Χ.), αρχαίος Έλληνας φιλόσοφος

ΠΕΡΙΕΧΟΜΕΝΑ

Περίληψη (Abstract)

Βασικός σκοπός της παρούσας διπλωματικής είναι η αναλυτική μελέτη της σύγχρονης τεχνολογίας της επιστήμης της Πληροφορικής η οποία ονομάζεται *Cloud Computing* και των εφαρμογών της. Συγκεκριμένα θα παρουσιαστούν αναλυτικά όλα τα τεχνικά ζητήματα που εγκαθιδρύουν και τελειοποιούν την συγκεκριμένη τεχνολογία και θα διερευνηθούν συγκεκριμένα θέματα ασφάλειας, εμπιστοσύνης και προστασίας της ιδιωτικότητας στο περιβάλλον αυτό. Παράλληλα θα γίνει διεξοδική παρουσίαση των τεχνολογιών της VMware για τον ESXi Server της IBM, της Microsoft για τον SQL Server 2008 R2 για VMware εγκαταστάσεις και των δυνατοτήτων ασφάλειας του VMware vShield Framework για Cloud Computing.

Το πρακτικό μέρος της εργασίας αφορά τη μεταφορά της ολοκληρωμένης εφαρμογής των Πληροφοριών του Εθνικού Τυπογραφείου σε ασφαλές περιβάλλον Cloud Computing στα πλαίσια της ηλεκτρονικής διακυβέρνησης. Το συγκεκριμένο project θα βασιστεί στις υποδομές που διαθέτει το Εθνικό Τυπογραφείο.

Λέξεις-κλειδιά

Cloud Computing, Iaas, Saas, Paas, virtualization, VMware, vShield, ESXi Server, SQL Server 2008 R2, Εθνικό Τυπογραφείο, Ηλεκτρονική Διακυβέρνηση

Abstract

Basic purpose of this thesis is the detailed study of modern technologies of Computer Science which are called *Cloud Computing* and their applications. More specifically, all technical issues that establish and perfect the specific technology will be presented in detail, and certain safety, trust and privacy protection issues will be looked into in this environment. At the same time, there will be a full presentation of VMware for the ESXi Server of IBM, Microsoft technologies for SQL Server 2008 R2 for VMware establishment and the security capacities of VMware vShield Framework for Cloud Computing.

The practical part of this project is about the transfer of the completed application of the National Printing House Information Project in a safe Cloud Computing environment in the frame of electronic governance. This project will be based on National Printing House Infrastructure.

Keywords

Cloud Computing, Iaas, Saas, Paas, virtualization, VMware, vShield, ESXi Server, SQL Server 2008 R2, National Printing House, e-governance

1. Εισαγωγή

Το Cloud Computing αποτελεί μια νέα προσέγγιση στην επιστήμη των κατανεμημένων συστημάτων, η οποία ωστόσο χρησιμοποιεί και ορισμένες παλαιότερες τεχνολογίες. Η δύναμη του Cloud Computing είναι η παροχή υπηρεσιών πόρων όπως η υπολογιστική ισχύς και η αποθηκευτική δυνατότητα στους χρήστες του συστήματος.

Τα τελευταία χρόνια η ασφάλεια της πληροφορίας γίνεται όλο και πιο σημαντική για όλους μας. Λίγα χρόνια πριν, κυβερνητικοί οργανισμοί, ειδικοί στην ασφάλεια και διαχειριστές συστημάτων ήταν προσηλωμένοι σε θέματα όπως οι ηλεκτρονικές απειλές. Σήμερα δεν περνάει ούτε μια μέρα χωρίς να διαβάσουμε σε κάποια εφημερίδα ή σε κάποιο μπλόγκ για ένα ατύχημα ασφάλειας ή μια καινούρια τρύπα σε ένα λειτουργικό σύστημα. Ο λόγος για αυτή τη μεγάλη αλλαγή είναι η αυξανόμενη χρήση της τεχνολογίας.

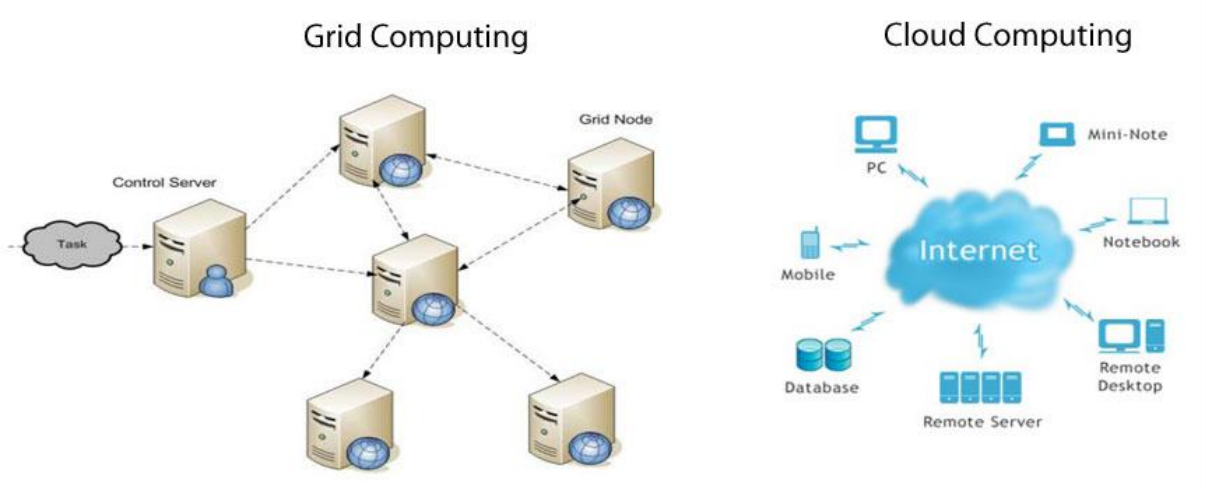
Κάθε υπολογιστής πλέον είναι συνδεδεμένος σε ένα μικρό δίκτυο, όπου απειλές όπως οι ιοί και τα σκουλήκια μπορούν να επηρεάσουν όλους τους χρήστες του δικτύου. Ακόμα και τα κινητά τηλέφωνα που είναι συνδεδεμένα στο Internet είναι ένας γνώριμος στόχος για τους εγκληματίες. Για τους λόγους αυτούς, όλο και περισσότερες εταιρείες ασφάλειας προωθούν διαφορετικές λύσεις ασφαλείας για διαφορετικές πλατφόρμες, όπως στο Cloud Computing.

2 Γενικά

Cloud Computing – για να το πούμε με απλά λόγια – σημαίνει Internet Computing [1] . Το Διαδίκτυο απεικονίζεται συνήθως σαν «σύννεφο» και ο όρος computing μεταφράζεται σε υπολογισμό που γίνεται μέσω διαδικτύου.
Με το Cloud Computing οι χρήστες μπορούν να χρησιμοποιούν πόρους βάσεων δεδομένων μέσω Internet από οπουδήποτε για όσο χρονικό διάστημα χρειάζονται, χωρίς να χρειάζεται να μεριμνούν για τη συντήρηση ή τη διαχείριση των πραγματικών πόρων. Για αυτό το λόγο οι βάσεις δεδομένων στο Cloud Computing είναι πολύ δυναμικές και εξελικτικές.
Το Cloud Computing, σε αντίθεση με το Grid Computing, έχει το χαρακτήρα του utility computing ή autonomic computing. Στην πραγματικότητα είναι μια εξαιρετικά ανεξάρτητη πλατφόρμα από άποψη υπολογισμού. Το καλύτερο παράδειγμα για Cloud Computing είναι τα Google Apps όπου οποιαδήποτε εφαρμογή μπορεί να προσεγγιστεί χρησιμοποιώντας έναν browser και μπορεί να επεκταθεί σε χιλιάδες υπολογιστές μέσω του Διαδικτύου.

2.1 Ορισμός του Cloud Computing

Το Cloud Computing παρέχει τη δυνατότητα για πρόσβαση σε κοινούς πόρους και μέσα στο Διαδίκτυο ώστε να μπορεί να εκτελέσει τις διαδικασίες που ικανοποιούν τις μεταβαλλόμενες επιχειρησιακές ανάγκες. Η θέση των φυσικών πόρων και οι συσκευές που προσεγγίζονται δεν είναι χαρακτηριστικά γνωστές στον τελικό χρήστη.
Επίσης παρέχει στους χρήστες τις απαραίτητες εγκαταστάσεις για να αναπτύξουν, να επεκτείνουν και να διαχειριστούν τις εφαρμογές τους στο cloud. Αυτό συνεπάγεται και το virtualization των πόρων που διατηρούν και ρυθμίζονται για κάθε χρήστη.



Εικόνα 2.1: Grid-Cloud Computing

Μερικά γενικά παραδείγματα περιλαμβάνουν:

- Amazon Elastic Computing Cloud (EC2): προσφέρει τις υπολογιστικές του υπηρεσίες και επιτρέπει στους χρήστες να χρησιμοποιήσουν τους κύκλους της CPU χωρίς αγορά περισσότερων υπολογιστών.
- Υπηρεσίες αποθήκευσης, όπως εκείνες που παρέχονται από την Amazon Simple Storage Service (S3).
- Επιχειρήσεις σαν την Nirvanix, που επιτρέπουν σε οργανισμούς να αποθηκεύσουν τα στοιχεία και τα έγγραφά τους χωρίς την προσθήκη ενός επιτόπιου κεντρικού υπολογιστή.
- Επιχειρήσεις SaaS, σαν την το Salesforce.com, που παρέχουν υπηρεσίες CRM. Έτσι οι χρήστες μπορούν να διαχειριστούν τη πληροφορία πελάτη χωρίς την εγκατάσταση εξειδικευμένου λογισμικού.

2.1.2 Τύποι Cloud Computing

Το Cloud Computing προσφέρει ποικίλους τρόπους στις επιχειρήσεις για να αυξήσουν την αποθηκευτική και λειτουργική ικανότητα Τεχνολογιών Πληροφορικής (ΤΠ) χωρίς να απαιτείται νέα υποδομή, προσωπικό και λογισμικό. Παρακάτω αναλύονται 6 διαφορετικοί τύποι Cloud Computing και σε σχέση με τις υπηρεσίες που παρέχουν στις επιχειρήσεις.

- **Web-based cloud services: Αυτές οι υπηρεσίες επιτρέπουν την εκμετάλλευση ορισμένων λειτουργιών υπηρεσιών Ιστού, παρά τη χρησιμοποίηση των πλήρως αναπτυγμένων εφαρμογών. Για παράδειγμα μπορεί να περιλαμβάνει ένα API για τα google maps ή μια υπηρεσία όπως μια διαδικασία πιστωτικής κάρτας.**
- **SaaS (Software as a Service): Πρόκειται για παροχή μιας δεδομένης εφαρμογής σε πολλαπλούς μισθωτές με την βοήθεια ενός browser. Οι λύσεις SaaS είναι κοινές στις πωλήσεις.**
- **Platform as a Service: Πρόκειται για μια παραλλαγή του SaaS. Η διαφορά είναι ότι τρέχουμε την εφαρμογή μας στη συγκεκριμένη υποδομή που παρέχει το cloud.**
- **Utility cloud services: Αυτές οι υπηρεσίες είναι εικονικές επιλογές αποθήκευσης και κεντρικών υπολογιστών. Έτσι οργανισμοί μπορούν να έχουν πρόσβαση κατόπιν παραγγελίας και να τους επιτρέπεται ακόμη και η δημιουργία ενός εικονικού κέντρου δεδομένων.**
- **Managed services: Αυτή είναι η παλιότερη περίπτωση χρησιμοποίησης τεχνολογίας Cloud Computing. Ουσιαστικά, στην περίπτωση αυτή το Cloud χειρίζεται μια εφαρμογή και όχι τους τελικούς χρήστες. Για παράδειγμα μπορεί να περιλαμβάνει υπηρεσίες anti-spam ή υπηρεσίες monitoring εφαρμογών.**
- **Service commerce: Οι συγκεκριμένες λύσεις Cloud είναι μια μίξη από SaaS και Managed services. Ουσιαστικά παρέχουν ένα πλήθος υπηρεσιών με τις οποίες ο χρήστης αλληλεπιδρά. Τέτοιες υπηρεσίες βρίσκουμε σε travel ordering ή virtual assistant services.**

Βρισκόμαστε όμως πραγματικά στην αρχή. Νέες ιδέες και αντιλήψεις αναδύονται διαρκώς. Δεδομένου ότι το **Cloud Computing** εξελίσσεται σε μια βιώσιμη αλλά και απαραίτητη επιλογή για πολλές επιχειρήσεις, οι τύποι υπηρεσιών που οι providers μπορούν να προσφέρουν στους πελάτες θα συνεχίσουν να αυξάνονται.

Ουσιαστικά υπάρχουν 3 είδη Cloud:

- **Public Clouds:** Οι υποδομές του συγκεκριμένου είδους είναι ανοικτές προς χρήση από το ευρύ κοινό και υπάρχουν πέρα από το firewall ενός οργανισμού. Τις υποδομές αυτές τις φιλοξενούν και τις διαχειρίζονται προμηθευτές όπως οι: Google, Amazon, Microsoft. Ακολουθούν τη λογική «Pay as you go» με το ξεκίνημα στην αρχή να είναι μικρό και όσο μεγαλώνει μετά δεν απαιτεί άλλη επένδυση στην υποδομή. Εδώ ο χρήστης δεν έχει τον έλεγχο της διαχείρισης των πόρων. Η διαχείριση είναι εξολοκλήρου στα χέρια των προμηθευτών, που είναι υπεύθυνοι για την εγκατάσταση λογισμικού (setup), τα updates και τα patches.

- **Private Clouds:** Οι υποδομές του συγκεκριμένου είδους υπάρχουν μέσα στα όρια του firewall ενός οργανισμού. Ρυθμίζονται κεντρικά από την επιχείρηση και έχουν όλα τα χαρακτηριστικά γνωρίσματα των **Public Clouds,** με τη διαφορά ότι την υποστήριξη την έχει η υφιστάμενη Διεύθυνση Πληροφορικής. Είναι ασφαλέστερη σαν τεχνολογία δεδομένου ότι βρίσκεται εσωτερικά σε έναν οργανισμό και χρησιμοποιεί τους πόρους σύμφωνα με τις επιχειρησιακές ανάγκες. Αυτές οι υποδομές είναι καταλληλότερες για εφαρμογές που απαιτούν μεγάλη ασφάλεια και ακολουθούν ορισμένες αυστηρές πολιτικές. Δεν είναι βέβαια εύκολο για έναν οργανισμό να ακολουθήσει μια τέτοια λύση, εξαιτίας της πολυπλοκότητας και της δυσκολίας διαχείρισης που παρουσιάζει. Για το λόγο αυτό, τέτοιες λύσεις επιλέγονται συνήθως από μεγάλες εταιρείες που έχουν κάνει τεράστιες επενδύσεις σε τεχνολογίες πληροφορικής και επικοινωνιών και διαθέτουν προσωπικό με ικανότητες διαχείρισης.

- **Hybrid Clouds:** Αποτελούνται από ένα συνδυασμό εξωτερικών και εσωτερικών προμηθευτών, δηλαδή πρόκειται για ένα μίγμα **Public** και **Private Clouds**. Ο οργανισμός διαχειρίζεται εσωτερικά τις εφαρμογές που είναι κομβικής σημασίας και τις εφαρμογές με μεγάλες απαιτήσεις ασφάλειας, ενώ ο εξωτερικός προμηθευτής διαχειρίζεται τις πιο απλές εφαρμογές. Δεσμεύονται με μια μοναδική ταυτότητα, χρησιμοποιούν τυποποιημένη τεχνολογία και επιτρέπουν τη φορητότητα στοιχείων και εφαρμογής. Χρησιμοποιούνται σε περιπτώσεις σαν το ***Cloud Bursting.*** *Μέσα στην επόμενη δεκαετία, στις περισσότερες χώρες θα δούμε το μεγαλύτερο μερίδιο των επενδύσεων να κατευθύνεται στα* **Hybrid Clouds***, για τον απλούστατο λόγο* ότι οι επιχειρήσεις συνήθως είναι πιο δύσπιστες ως προς την ασφάλεια του cloud και προτιμούν να ρυθμίζουν μόνοι τους τα κρίσιμα στοιχεία και να αναθέτουν στον εξωτερικό προμηθευτή τη διαχείριση των μη κρίσιμων στοιχείων. Για τους τελικούς χρήστες παρουσιάζουν μεγαλύτερο ενδιαφέρον τα **Public Clouds**. Όλοι χρησιμοποιούν υπηρεσίες **Public Cloud** όπως τα **Microsoft Office Web apps, Windows Live Mesh 2011** και **Google Docs.**

2.2 Χαρακτηριστικά Cloud Computing

Τον Οκτώβριο του 2009 μια παρουσίαση [2] με τίτλο “Effectively and Securely Using the Cloud Computing Paradigm” του Peter Mell and Tim Grance, του The National Institute of Standards and Technology (NIST) Information Technology Laboratory, όρισαν το Cloud Computing ως εξής:

> *Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable and reliable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction.*

Συγκεκριμένα το Cloud Model αποτελείται από πέντε βασικά χαρακτηριστικά, τρεις υπηρεσίες που το διαμορφώνουν και τέσσερα deployment models. Τα 5 βασικά χαρακτηριστικά είναι τα εξής:

- On-demand self-service
- Ubiquitous network access
- Resource pooling
- Location independence
- Rapid elasticity
- Measured service

Τα 3 μοντέλα υπηρεσιών είναι:

- Cloud Software as a Service (SaaS)—Use provider's applications over a network.
- Cloud Platform as a Service (PaaS)—Deploy customer-created applications to a cloud.
- Cloud Infrastructure as a Service (IaaS)—Rent processing, storage, network capacity, and other fundamental computing resources.

Τα 4 deployment models είναι:

- Private cloud—Enterprise owned or leased
- Community cloud—Shared infrastructure for specific community
- Public cloud—Sold to the public, mega-scale infrastructure
- Hybrid cloud—Composition of two or more clouds

2.2.1 Τι υπηρεσίες μπορούν να χρησιμοποιηθούν στο Cloud ;

Οι βασισμένες [3] στο Web υπηρεσίες αποστολής ηλεκτρονικών μηνυμάτων όπως το Gmail και το Hotmail αποτελούν παράδειγμα του Cloud Computing: οι χρήστες μπορούν να έχουν πρόσβαση στο ηλεκτρονικό ταχυδρομείο τους στο Cloud από οποιοδήποτε υπολογιστή με σύνδεση στο Διαδίκτυο, στον συγκεκριμένο υπολογιστή. Τα ηλεκτρονικά ταχυδρομεία φιλοξενούνται στους κεντρικούς υπολογιστές της Google και της Microsoft και δεν χρειάζεται να αποθηκευτούν τοπικά στον υπολογιστή του πελάτη.
Κατά τη διάρκεια των τελευταίων ετών, έχουμε δει την τεράστια αύξηση του Cloud Computing σε πολλές δημοφιλείς Web Applications όπως: VoIP (Skype, Google Voice), social applications (Facebook, Twitter, LinkedIn), media services (Picasa, YouTube, Flickr), content distribution (Bit Torrent), financial apps (Mint) και πολλά άλλα. Ακόμη και το παραδοσιακό λογισμικό εφαρμογών γραφείου, το Microsoft Office, κινήθηκε εν μέρει προς τον Ιστό με το Office 2010 Web Apps.

(1) SCENARIO	**On-premise application unchanged in the cloud**
CHARACTERISTICS	Multiple red legacy, Java or.NET based application
AMAZON	Threat the machine as another server in the data center and do the necessary changes to configuration
GOOGLE	Needs significant refactoring of application and data logic for existing Java application
MICROSOFT	If existing application is ASP.NET application, then re-factor data, otherwise refactoring effort can be quite significant

	depending on the complexity

(2) SCENARIO	**Scalable Web application**
CHARACTERISTICS	Moderate to high Web application with a back-end store and load balancing
AMAZON	Threat the machine instance as another server in the data center and do the necessary changes to configuration. But scalability and elasticity is manual configuration
GOOGLE	Use dynamically scalable features of AppEngine and scripting technologies to build rich applications
MICROSOFT	Build scalable Web applications using familiar.NET technologies. Scaling up/down purely driven by configuration.

(3) SCENARIO	**Parallel processing computational application**
CHARACTERISTICS	Automated long running processing with little to no user interaction.
AMAZON	Need to configure multiple machine instances depending on the scale needed and manage the environments.
GOOGLE	Platform has minimal built-in support for building compute heavy applications. Certain application scenarios, such as image manipulation, are easier to develop with built-in platform features.
MICROSOFT	With worker roles and storage features like Queues and blobs, it is easy to build a compute heavy application that can be managed and controlled for scalability and elasticity.

(4) SCENARIO	**Application in the cloud interacts with on-premise data**
CHARACTERISTICS	Cloud based applications interacting with on-premise apps for managing transactions of data
AMAZON	Applications in EC2 server cloud can easily be configured to interact with applications running on premise.
GOOGLE	No support from the platform to enable this scenario. Possible through each application using intermediary store to communicate.
MICROSOFT	From features like Service Bus to Sync platform components it is possible to build compelling integration between the two environments.

(5) SCENARIO	**Application in the cloud interacts with on-premise application**
CHARACTERISTICS	On-premise applications
AMAZON	Applications in EC2 server cloud can easily be configured to interact with applications running on premise.
GOOGLE	No support from the platform to enable this scenario. Possible through each application using intermediary store to communicate.
MICROSOFT	From features like Service Bus to Sync platform components it is possible to build compelling integration between the two environments.

Εικόνα 2.2.1: Cloud Computing Platforms and Different Scenarios

2.2.2 Ποια είναι τα οφέλη από το Cloud Computing ;

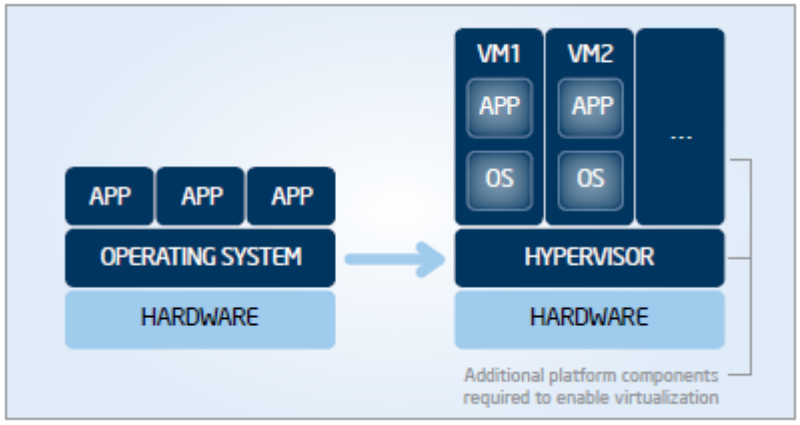
Το Cloud Computing απελευθερώνει [4] τις επιχειρήσεις και τους καταναλωτές από την ανάγκη να επενδύουν σε υλικό ή να εγκαθιστούν λογισμικό στις συσκευές τους. Μειώνουν τις ανάγκες συντήρησης υλικού και, επειδή οι λύσεις είναι όλες βασισμένες στο Web, ακόμα και οι παλιότεροι υπολογιστές μπορούν να χρησιμοποιηθούν στις υπηρεσίες Cloud Computing.
Για τους χρήστες κινητών συσκευών, το Cloud Computing παρέχει απίστευτη ευελιξία: οι επαγγελματίες μπορούν να εργαστούν από οποιαδήποτε ηλεκτρονική συσκευή οπουδήποτε, εφόσον έχουν πρόσβαση στον Ιστό. Καθιστά επίσης τη συνεργασία ευκολότερη, δεδομένου ότι οι διανεμημένες ομάδες (ή ένας συνδυασμός κινητών εργαζομένων και εσωτερικού προσωπικού) μπορούν να λειτουργήσουν στις κοινές πληροφορίες που αποθηκεύονται κεντρικά στο σύννεφο μέσω, παραδείγματος χάριν, των σε απευθείας σύνδεση εφαρμογών groupware .

2.2.3 Μερικές σκέψεις για το Cloud Computing

Υπάρχουν επίσης μερικά ζητήματα ή εμπόδια στο Cloud Computing. Μια σύνδεση στο Διαδίκτυο είναι προφανώς απαραίτητη για να εκμεταλλευθούμε πλήρως μια υπηρεσία Cloud Computing. Όταν είμαστε σε μη απευθείας σύνδεση –ή εάν υπάρχουν οποιεσδήποτε διασπάσεις με την ίδια την υπηρεσία Cloud– τα στοιχεία μπορεί να μην είναι καθόλου προσιτά. Κάποια Cloud apps (όπως το Gmail) παρέχουν τη δυνατότητα μη απευθείας σύνδεσης ενώ άλλα, όπως η Mint, απαιτούν σύνδεση στο Διαδίκτυο. Η Evernote notetaking application, προσφέρει ένα αγαθό – υβριδική λύση με τον υπολογιστή γραφείου ή το τηλεφωνικό λογισμικό, μια υπηρεσία online μέσω της οποίας οι ενημερώσεις των σημειώσεων γίνονται στο Cloud.
Ένα άλλο θέμα με το Cloud εκτός από τη διαθεσιμότητα είναι και η ασφάλεια. Είναι πιθανόν τα άτομα και οι επιχειρήσεις να μην νιώθουν άνετα αποθηκεύοντας τις πληροφορίες, ιδίως προσωπικά ή ευαίσθητα στοιχεία, στον κεντρικό υπολογιστή κάποιου άλλου στο Διαδίκτυο.
Τα ζητήματα της εμπιστοσύνης και της αξιοπιστίας θα είναι κρίσιμα για τις υπηρεσίες Cloud και θα πρέπει να επιλυθούν προτού να κινηθεί κάποιος προς το Cloud. Οι διαβεβαιώσεις των τεχνολογιών κρυπτογράφησης, της προστασίας της ιδιωτικότητας και των λύσεων για τη δυνατότητα πρόσβασης σε μη απευθείας σύνδεση πρέπει να λυθούν ολοκληρωτικά.

2.3 Τεχνολογία στο Cloud Computing

Το virtualization είναι μια από τις δομικές μονάδες βασικής τεχνολογίας που επιτρέπει το Cloud Computing. Η δυνατότητα να παγιωθούν τα εικονικά περιβάλλοντα (μηχανήματα εικονικής πραγματικότητας) σε έναν ενιαίο φυσικό κεντρικό υπολογιστή αυξάνει τη χρησιμοποίηση των πόρων των ανά βάση κεντρικού υπολογιστή και συνεπώς μειώνει το κόστος.
Εντούτοις, η εμφάνιση του virtualization έχει αλλάξει πλήρως τον παραδοσιακό σωρό πλατφορμών υπηρεσιών ΤΠ.
Με την προσθήκη του hypervisor (δηλαδή του οργάνου ελέγχου μηχανημάτων εικονικής πραγματικότητας) και του virtualized περιβάλλοντος πολυ-μισθωτών, η επιφάνεια επίθεσης εναντίον της πλατφόρμας ενισχύεται, και το επίπεδο εκλέπτυνσης της επίθεσης αυξάνεται διαρκώς.
Ουσιαστικά ο hypervisor ή αλλιώς virtual machine manager/monitor (VMM) είναι ένα computer hardware platform virtualization software που επιτρέπει σε πολλά και διαφορετικά λειτουργικά συστήματα να μοιραστούν ένα single hardware host. Καθένα από τα λειτουργικά συστήματα φαίνεται να έχει από τον host δικιά του μνήμη, επεξεργαστή και πόρους. Επίσης ο hypervisor διαχειρίζεται και τον host υπολογιστή (επεξεργαστή, μνήμη, πόρους) και εξασφαλίζει ότι τα φιλοξενούμενα λειτουργικά συστήματα δεν θα έρχονται σε επαφή.

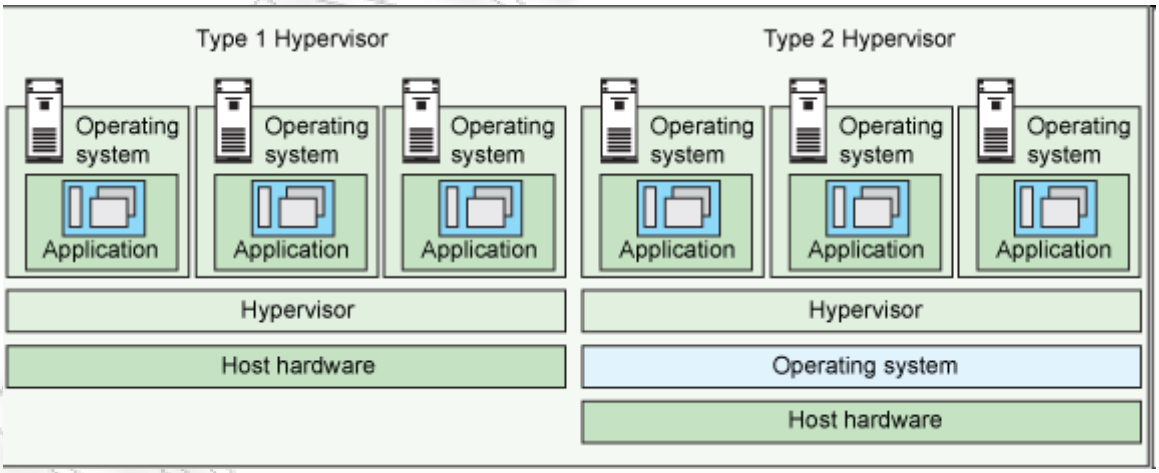


Εικόνα 2.3: Μετάβαση από μια παραδοσιακή πλατφόρμα σε μια virtualized.

2.3.1 Τεχνολογίες Hypervisor

Οι τεχνολογίες αυτές [5] χωρίζονται σε 2 βασικούς τύπους:

- ΤΥΠΟΣ 1 (native, bare metal): πρόκειται για hypervisors που «τρέχουν» κατευθείαν στο host υλικό για να διαχειριστούν το υλικό και το φιλοξενούμενο λειτουργικό σύστημα. Το φιλοξενούμενο λειτουργικό σύστημα λειτουργεί ένα επίπεδο πάνω από τον hypervisor. Τέτοιου τύπου hypervisors είναι το z/VM, XenServer, VMware ESXi, και το Microsoft Hyper-V hypervisor.
- ΤΥΠΟΣ 2 (hosted): είναι hypervisors που «τρέχουν» ένα συμβατικό λειτουργικό σύστημα. Με τον hypervisor να υπάρχει σε ένα μοναδικό δεύτερο επίπεδο, το φιλοξενούμενο λειτουργικό σύστημα βρίσκεται σε τρίτο επίπεδο πάνω από το υλικό. Τέτοιου τύπου hypervisors είναι τα KVM και VirtualBox.



Εικόνα 2.3.1.1: Τα δύο είδη των hypervisor

Οι πιο γνωστές τεχνολογίες hypervisor είναι οι εξής:

- PowerVM
- VMware ESX Server
- Xen
- KVM

Για να κατανοήσουμε καλύτερα όμως τους μηχανισμούς αυτούς και να δούμε ποιος μας ταιριάζει καλύτερα στην υπηρεσία που χρησιμοποιούμε, θα δούμε αναλυτικά ορισμένα από τα βασικά στοιχεία τους.

PowerVM

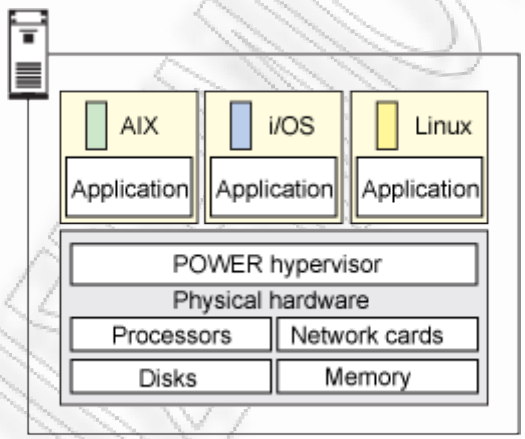
Το PowerVM είναι virtualization χωρίς όρια. Οι οργανισμοί που χρησιμοποιούν το PowerVM virtualization χρειάζονται λιγότερα συστήματα, αυξάνουν τη λειτουργικότητα του server και μειώνουν το κόστος. Το PowerVM παρέχει ασφάλεια και επεκτάσιμο virtualization περιβάλλον για AIX, IBM i και Linux εφαρμογές το οποίο βασίζεται στα χαρακτηριστικά RAS και την αρχική απόδοση της Power Systems Platform.

Εκδόσεις των λειτουργικών συστημάτων που υποστηρίζονται:

- AIX 5.3, AIX 6.1 και AIX 7
- IBM i 6.1 and IBM i 7.1
- Red Hat Enterprise Linux 5 και Red Hat Enterprise Linux 6
- SUSE Linux Enterprise Server 10 και SUSE Linux Enterprise Server 11

Πλατφόρμες hardware που υποστηρίζονται:

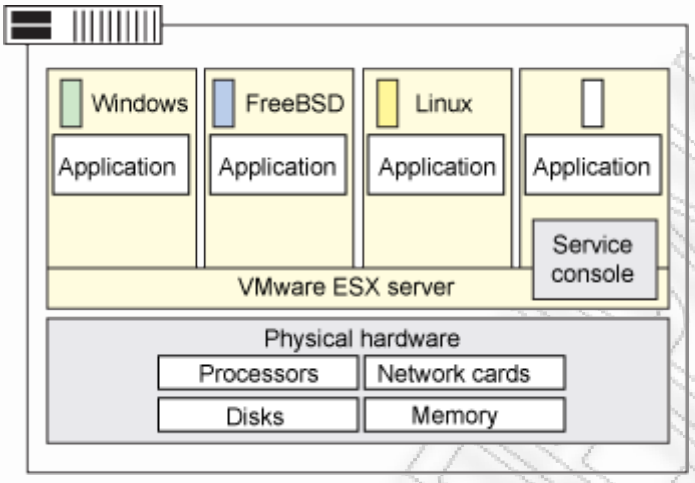
- IBM Power Systems με POWER5, POWER6 και POWER7 επεξεργαστές



Εικόνα 2.3.1.2: Αρχιτεκτονική του PowerVM hypervisor

VMware ESX Server

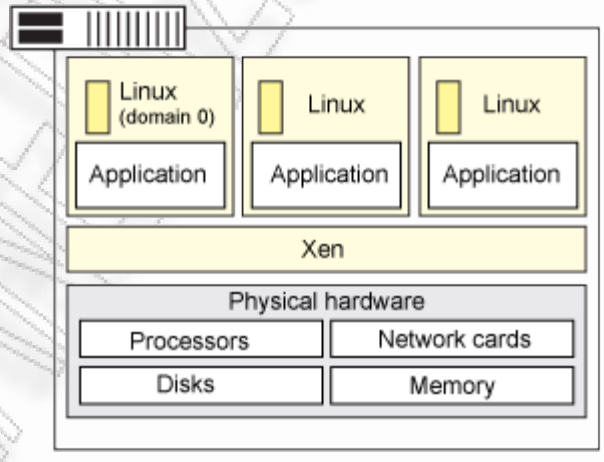
Ο ESX Server ανήκει στον πρώτο τύπο hypervisor, που είδαμε πιο πάνω, δημιουργεί logical pools από πηγές του συστήματος, με αποτέλεσμα πολλές virtual machines να μπορούν να μοιράζονται τις ίδιες φυσικές πηγές.
Ο ESX Server είναι λειτουργικό σύστημα που λειτουργεί ως hypervisor και τρέχει απευθείας σε ένα σύστημα hardware. Εισάγει ένα επίπεδο virtualization ανάμεσα στο σύστημα hardware και στις virtual machines, μετατρέποντας το σύστημα hardware σε μια δεξαμενή λογικών υπολογιστικών πηγών, που ο ESX Server μπορεί δυναμικά να διανέμει σε οποιαδήποτε λειτουργικό σύστημα ή εφαρμογή.
Η Εικόνα **2.3.1.3** απεικονίζει ένα σύστημα ESX Server που τρέχει virtual machines. Ο ESX Server τρέχει ένα virtual machine με το service console και τρεις επιπλέον virtual machines. Κάθε επιπλέον virtual machine τρέχει ένα λειτουργικό σύστημα και εφαρμογές ξεχωριστά από τα υπόλοιπα virtual machines, όμως μοιράζονται τις ίδιες φυσικές πηγές.



Εικόνα 2.3.1.3: Αρχιτεκτονική του VMware ESX Server

Xen

Ο Xen ανήκει επίσης στον πρώτο τύπο hypervisor, όπως και ο ESX Server.
Ο Xen είναι hypervisor που τρέχει απευθείας στο σύστημα hardware. Επίσης, εισάγει ένα επίπεδο virtualization ανάμεσα στο σύστημα hardware και τα virtual machines, μετατρέποντας το σύστημα hardware σε μια δεξαμενή λογικών υπολογιστικών πηγών, που ο Xen μπορεί δυναμικά να διανέμει σε οποιαδήποτε λειτουργικό σύστημα ή εφαρμογή. Η Εικόνα **2.3.1.4** απεικονίζει το σύστημα Xen που τρέχει virtual machines.

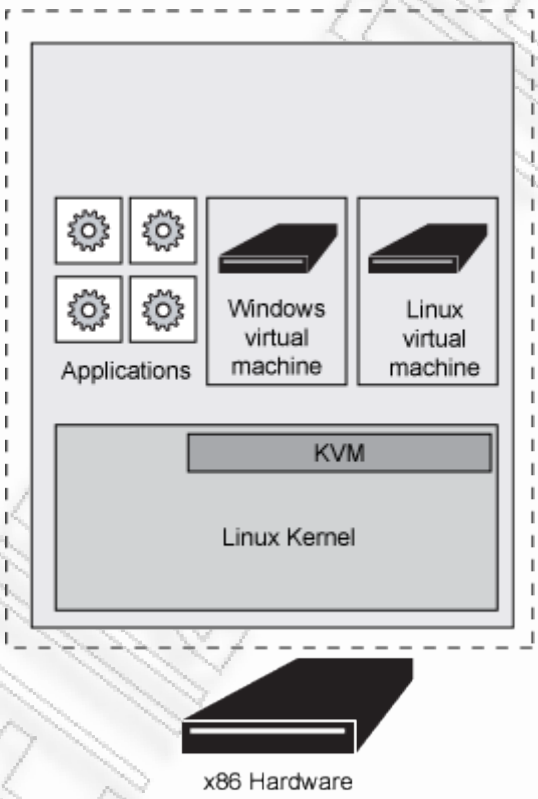


Εικόνα 2.3.1.4: Αρχιτεκτονική του Xen

Ο Xen τρέχει τρεις virtual machines. Κάθε virtual machine τρέχει ένα λειτουργικό σύστημα και εφαρμογές ξεχωριστά από τα υπόλοιπα virtual machines, όμως μοιράζονται τις ίδιες φυσικές πηγές.

KVM

Το Kernel-based Virtual Machine (KVM) είναι μια λύση full native virtualization για συστήματα Linux με αρχιτεκτονική x86 με επεκτάσεις virtualization (Intel VT ή AMD-V). Περιορισμένη υποστήριξη για paravirtualization είναι επίσης διαθέσιμη για επισκέπτες Linux και Windows guests σε ένα paravirtual δίκτυο.
Το interface του KVM είναι πρόσφατα σχεδιασμένο για kernel. Οι εκδόσεις λειτουργικών συστημάτων που υποστηρίζει περιλαμβάνουν μια μεγάλη γκάμα όπως Linux, BSD, Solaris, Windows, Haiku, ReactOS, και AROS Research Operating System. Μία ενημερωμένη έκδοση του KVM (qemu) τρέχει και σε περιβάλλον MacOS X.
Ωστόσο το KVM δεν πραγματοποιεί εξομοίωση από μόνο του, αντ' αυτού ένα πρόγραμμα user-space χρησιμοποιεί το /dev/kvm interface για τη δημιουργία χώρου διευθύνσεων στον guest virtual server, προσθέτοντας και συσκευές I/O. Η Εικόνα **2.3.1.5** απεικονίζει την αρχιτεκτονική του KVM.



Εικόνα 2.3.1.5: Αρχιτεκτονική του KVM

Στην αρχιτεκτονική KVM, η virtual machine είναι εμφυτευμένη «is implemented as regular Linux process», προγραμματισμένη σύμφωνα με το Linux. Στην πραγματικότητα, κάθε virtual CPU εμφανίζεται ως μία συνηθισμένη διεργασία Linux. Αυτό επιτρέπει στο KVM να επωφεληθεί πλήρως από τα χαρακτηριστικά του Linux kernel.

3. Ασφάλεια Cloud Computing-Hypervisor

Οι επιχειρήσεις που διεισδύουν στο Cloud Computing [6] για την επέκταση των υποδομών τους πρέπει να γνωρίζουν τα ζητήματα ασφαλείας που μπορούν να θέσουν σε κίνδυνο την ακεραιότητα και την ασφάλεια των εφαρμογών και δεδομένων τους.
Η αδυναμία στη χρήση των συστημάτων αυτών αφορά επιθέσεις στα ίδια virtual machines που βρίσκονται στον ίδιο server, με αποτέλεσμα να απαιτούνται μηχανισμοί ασφαλείας, τους οποίους θα περιγράψουμε αναλυτικά παρακάτω.
Έτσι, λοιπόν, εφαρμόζουμε μηχανισμούς ασφαλείας όπως χρήση firewall, ανίχνευση και πρόληψη εισβολών (IDS και IPS), παρακολούθηση της ακεραιότητας, παρακολούθηση των αρχείων logs και προστασία από κακόβουλο λογισμικό, καθώς είναι ορισμένες από τις πιο αποτελεσματικές μεθόδους. Μπροστά στον κίνδυνο επίθεσης και παραβίασης των συστημάτων τους οι επιχειρήσεις λαμβάνουν μέτρα, προκειμένου οι υπηρεσίες τους να είναι ασφαλείς και να αντέξουν στον ανταγωνισμό των άλλων συστημάτων Cloud Computing.

3.1 Προκλήσεις ασφαλείας στο Cloud Computing

Με την πρώτη ματιά, οι απαιτήσεις ασφάλειας για τους παρόχους φαίνεται να είναι ίδιες όπως στην περίπτωση των παραδοσιακών datacenters, αρκεί δηλαδή η εφαρμογή μιας περιμετρικής ασφάλειας του δικτύου, ώστε να κρατήσει τους κακόβουλους χρήστες απ' έξω. Ωστόσο, ο φυσικός διαχωρισμός και η τεχνολογία hardware-based ασφάλειας δεν μπορούν να προστατεύσουν από επιθέσεις εναντίον των εικονικών μηχανών του ίδιου διακομιστή. Στη συνέχεια παρουσιάζονται συνοπτικά μερικά από τα αρχικά ζητήματα τα οποία οι επιχειρήσεις πρέπει να λαμβάνουν υπόψη τους κατά το σχεδιασμό ανάπτυξης ενός Cloud Computing.

3.1.1 Εξουσιοδοτημένη πρόσβαση σε servers και εφαρμογές

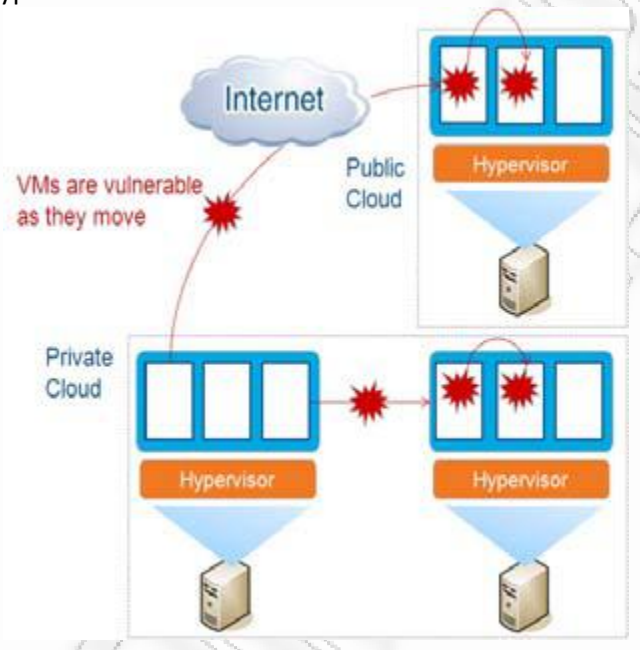
Ένα από τα πιο σημαντικά χαρακτηριστικά του Cloud Computing είναι ότι προσφέρει «self-service» πρόσβαση σε υπολογιστική ισχύ, μέσω του διαδικτύου. Στο Cloud Computing, η πρόσβαση ενός administrator πραγματοποιείται μέσω του διαδικτύου, με αποτέλεσμα να έχουμε αυξανόμενη έκθεση στους κινδύνους. Γι' αυτό είναι εξαιρετικά σημαντικό να περιορίσουμε την πρόσβαση των administrators και να ελέγχουμε αυστηρά ποιοι θα έχουν αυτό το δικαίωμα και την παρακολούθηση κατά τη διάρκεια της πρόσβασης και των αλλαγών στο σύστημα ελέγχου

3.1.2 Δυναμικά Virtual Machines

Τα virtual machines είναι δυναμικά. Μπορούν να «μεταφερθούν» γρήγορα σε προηγούμενες περιπτώσεις, να κάνουν παύση και επανεκκίνηση σχετικά εύκολα. Μπορούν επίσης να κλωνοποιηθούν εύκολα και να μετακινηθούν ομαλά μεταξύ φυσικών διακομιστών. Λόγω της δυναμικής φύσης και των δυνατοτήτων επέκτασης των VM, είναι αδύνατο να επιτευχθεί και να διατηρηθεί μια συνεπής ασφάλεια. Αδυναμίες ή τυχόν σφάλματα ρύθμισης παραμέτρων μπορεί να προκύψουν πολύ εύκολα . Επίσης, είναι δύσκολο να διατηρηθούν στοιχεία για την κατάσταση της ασφάλειας μιας εικονικής μηχανής σε κάθε δεδομένη χρονική στιγμή. Σε περιβάλλον Cloud Computing, θα πρέπει να είναι σε θέση να αποδείξουν την κατάσταση ασφαλείας του συστήματος, ανεξάρτητα από τη θέση του ή αν βρίσκεται κοντά σε άλλα και ανασφαλή virtual machines.

3.1.3 Εκμετάλλευση τρωτών σημείων και επιθέσεις VM-to-VM

Οι διακομιστές ενός hypervisor χρησιμοποιούν τα ίδια λειτουργικά συστήματα και web εφαρμογές με τα virtual machines και τους φυσικούς διακομιστές . Η δυνατότητα ενός εισβολέα ή κακόβουλου λογισμικού να εκμεταλλευτεί απομακρυσμένα τρωτά σημεία των συστημάτων αυτών και των εφαρμογών αποτελεί σημαντική απειλή. Επιπλέον, η «συστέγαση» πολλών virtual machines αυξάνει την επιφάνεια επίθεσης και τον κίνδυνο έκθεσης σε επιθέσεις VM-to-VM. Συστήματα ανίχνευσης εισβολών και πρόληψης πρέπει να είναι σε θέση να εντοπίσουν κακόβουλες δραστηριότητες στο επίπεδο του virtual machine, ανεξάρτητα από τη θέση του VM στο περιβάλλον του hypervisor.



Εικόνα 3.1.3: Ευπάθειες στα virtual machines

3.1.4 Ασφάλεια σε κατάσταση αναμονής

Σε αντίθεση με μια φυσική μηχανή, όταν ένα virtual machine είναι συνδεδεμένο, εξακολουθεί να είναι διαθέσιμο σε οποιαδήποτε εφαρμογή που μπορεί να έχει πρόσβαση στον αποθηκευτικό χώρο μέσω του δικτύου και ως εκ τούτου είναι ευπαθές σε κακόβουλο λογισμικό. Ωστόσο, όταν βρίσκεται σε κατάσταση αναμονής ή offline δεν έχει τη δυνατότητα να εκτελέσει σάρωση με τη χρήση ενός anti-malware. Virtual machines σε αναμονή μπορούν να υπάρχουν όχι μόνο σε hypervisor, αλλά μπορεί επίσης να συμπληρώσουν ή να αρχειοθετηθούν σε άλλους διακομιστές ή μέσα αποθήκευσης. Στο περιβάλλον Cloud Computing, την ευθύνη για την προστασία και τη σάρωση των αδρανών μηχανημάτων τη φέρει ο πάροχος. Οι επιχειρήσεις που χρησιμοποιούν Cloud Computing θα πρέπει να αναζητήσουν τους παρόχους υπηρεσιών που μπορούν να διασφαλίσουν τα virtual machines που βρίσκονται σε αναμονή, ώστε να διατηρηθεί η συνεκτική ασφάλεια στο σύστημα.

3.2 Προκλήσεις ασφαλείας Hypervisor

Παρακάτω θα δούμε αναλυτικά ορισμένες τεχνολογίες ασφαλείας που θα πρέπει να αναπτύξουμε σε έναν hypervisor προκειμένου να αυξήσουμε την ασφάλεια και να διατηρήσουμε την ακεραιότητα στους διακομιστές και τις εφαρμογές που βρίσκονται μέσα στο περιβάλλον του cloud.

3.2.1 Firewall

Ένα αμφίδρομο τείχος προστασίας, που έχει αναπτυχθεί σε μεμονωμένους hypervisors, μπορεί να παρέχει κεντρική διαχείριση της πολιτικής που εφαρμόζει το τείχος προστασίας του διακομιστή. Θα πρέπει όμως, να περιλαμβάνει προκαθορισμένα πρότυπα για κοινούς τύπους εταιρικών διακομιστών και να επιτρέπει τα εξής:

- Απομόνωση των hypervisor.
- Φιλτράρισμα εσωτερικών και εξωτερικών διευθύνσεων, πορτών.
- Κάλυψη όλων των IP-based πρωτοκόλλων (TCP, UDP, ICMP, κ.λπ.).
- Κάλυψη όλων των τύπων πλαισίου (IP, ARP).
- Πρόληψη επιθέσεων Denial of Service (DoS).
- Σχεδιασμό πολιτικών ανά διασύνδεση δικτύου.
- Ανίχνευση των σαρώσεων αναγνώρισης για διακομιστές στο Cloud Computing.

3.2.2 Συστήματα ανίχνευσης και πρόληψης εισβολών (IDS/IPS)

Ασπίδα κατά των ευπαθειών των λειτουργικών συστημάτων και των εφαρμογών μιας επιχείρησης έως ότου να επιδιορθωθούν, για να επιτευχθεί η έγκαιρη προστασία έναντι γνωστών και zero-day επιθέσεων.

Όπως αναφέρθηκε προηγουμένως, οι εικονικές μηχανές και οι servers στο Cloud Computing χρησιμοποιούν τα ίδια λειτουργικά συστήματα, τις επιχειρήσεις και τις web εφαρμογές όπως και οι φυσικοί διακομιστές. Η ανάπτυξη συστημάτων ανίχνευσης εισβολών και πρόληψης, όπως το λογισμικό σε hypervisors, ανακάλυψαν πρόσφατα ευπάθειες σε αυτές τις εφαρμογές και τα λειτουργικά συστήματα, που ενδέχεται να θέσουν σε κίνδυνο τα συστήματα (όπως, για παράδειγμα, ευπάθειες που παρουσιάζονται κάθε μήνα από τη Microsoft και αφορούν έναν απεριόριστο αριθμό exploits).

3.2.3 Παρακολούθηση ακεραιότητας

Παρακολούθηση αρχείων, συστημάτων και της registry για αλλαγές. Η παρακολούθηση ακεραιότητας στα κρίσιμα σημεία ενός λειτουργικού συστήματος και τα αρχεία εφαρμογών (όπως αρχεία, κατάλογοι, registry keys και τιμές, κ.λπ.) είναι απαραίτητη για την ανίχνευση κακόβουλων και απρόσμενων αλλαγών που θα μπορούσαν να σηματοδοτήσουν έκθεση πόρων του συστήματος Cloud Computing σε κινδύνους. Η ακεραιότητα λογισμικού παρακολούθησης πρέπει να εφαρμόζεται σε επίπεδο hypervisor.

Μία λύση ελέγχου ακεραιότητας πρέπει να επιτρέπει:

- Την κατ΄απαίτηση ή προγραμματισμένη ανίχνευση.
- Εκτενή έλεγχο των ιδιοτήτων αρχείων και φακέλων, συμπεριλαμβάνοντας τις μεταβλητές.
- Παρακολούθηση σε επίπεδο καταλόγου.

- Ευέλικτη πρακτική παρακολούθησης μέσω των λειτουργιών προσθήκης/αποκλεισμού.
- Αναφορές ελέγχου.

3.2.4 Καταγραφή των logs

Συλλέγουμε και αναλύουμε το λειτουργικό σύστημα και τα αρχεία καταγραφής συμβάντων των εφαρμογών για την ασφάλεια. Οι κανόνες για την καταγραφή των logs βελτιστοποιούν τον προσδιορισμό των σημαντικών γεγονότων της ασφάλειας που καταχωρούνται σε πολλαπλά log entries. Οι εκδηλώσεις αυτές μπορούν να αποστέλλονται σε ένα αυτόνομο σύστημα ασφαλείας, το οποίο συμβάλει στη μέγιστη καταγραφή και παρακολούθηση πληροφοριών και συμβάντων. Όπως και στην παρακολούθηση ακεραιότητας, οι δυνατότητες ελέγχου καταγραφής πρέπει να εφαρμόζονται σε επίπεδο hypervisor. Η καταγραφή logs σε λογισμικό επιτρέπει:

- Ανίχνευση ύποπτης συμπεριφοράς.
- Καταγραφή των πράξεων των administrators που σχετίζονται με την ασφάλεια.
- Βελτιστοποιημένη συλλογή των γεγονότων ασφαλείας από τα datacenter.

3.2.5 Προστασία από κακόβουλο λογισμικό

Η πολυεπίπεδη προστασία χρησιμοποιεί εικονικές μηχανές σάρωσης που συντονίζονται σε πραγματικό χρόνο μέσα σε κάθε hypervisor. Αυτό εξασφαλίζει ότι τα virtual machines είναι ασφαλή όταν είναι αδρανή, και έτοιμα να εγκαταστήσουν τις πρόσφατες ενημερώσεις κάθε φορά που ενεργοποιούνται. Τα μέτρα αυτά εξασφαλίζουν:

- Πρόληψη του κακόβουλου λογισμικού και των επιπτώσεων του, τόσο σε ενεργούς αλλά και αδρανείς hypervisors.
- Προστασία από επιθέσεις που αποτρέψαμε και απεγκαταστήσαμε χρησιμοποιώντας patch ασφαλείας για κακόβουλο λογισμικό.
- Αυτόματη ρύθμιση παραμέτρων ασφαλείας νέων hypervisors.

3.2.6 Κρυπτογράφηση και διατήρηση ελέγχου των δεδομένων

Εξασφαλίζει τον έλεγχο των δεδομένων σε περιβάλλον Cloud Computing. Η τοποθέτηση ευαίσθητων δεδομένων έξω από το datacenter στο δημόσιο cloud θέτει μια νέα πρόκληση για την τεχνολογία της πληροφορικής και οι επιχειρήσεις πρέπει να σχεδιάσουν να διατηρήσουν τον έλεγχο των δεδομένων αυτών. Ο έλεγχος γίνεται με μορφή του ελέγχου των δεδομένων που χρησιμοποιούνται στις cloud-based virtual machines και την επικύρωση των δεδομένων αυτών. Το cloud δημιουργεί νέες προκλήσεις για τον έλεγχο και την κρυπτογράφηση της διαχείρισης των κλειδιών, δίνοντας τη δυνατότητα να συμμορφωθεί όσο το δυνατόν καλύτερα με τις πρακτικές ασφαλείας, εσωτερικής διακυβέρνησης και της εξωτερικής ρύθμισης. Η επιχείρηση ελεγχόμενης κρυπτογράφησης και διαχείρισης κλειδιών επιτρέπει τη φορητότητα ανάμεσα σε cloud μηχανήματα, καθώς η ασφάλεια των δεδομένων δεν συνδέεται με οποιονδήποτε μοναδικό προμηθευτή Cloud Computing. Οι βέλτιστες πρακτικές ασφαλείας στο Cloud Computing θα πρέπει να περιλαμβάνουν:

- Κρυπτογράφηση ευαίσθητων δεδομένων που χρησιμοποιούνται από cloud-based virtual machines.
- Κεντρική διαχείριση του κλειδιού κρυπτογράφησης για τα δεδομένα που ελέγχονται από την επιχείρηση για να διευκολύνουν τη φορητότητα και τη διατήρηση της εξουσίας της επιχείρησης, ξεχωριστά για κάθε μηχάνημα.

- Διασφάλιση ότι τα δεδομένα είναι προσβάσιμα σύμφωνα με τις πολιτικές ασφαλείας της επιχείρησης.

4. Εισαγωγή στο Full Virtualization

Virtualization είναι η προσομοίωση του λογισμικού ή του υλικού πάνω στο οποίο τρέχει κάποιο άλλο λογισμικό. Αυτό το περιβάλλον προσομοίωσης ονομάζεται εικονική μηχανή (Virtual Machine, VM). Υπάρχουν πολλές μορφές virtualization, τα οποία διακρίνονται κυρίως από το επίπεδο της αρχιτεκτονικής υπολογιστών. Για παράδειγμα, η εφαρμογή virtualization παρέχει μια εικονική διεπαφή προγραμματισμού εφαρμογών (application programming interface, API), δίνοντας τη δυνατότητα εφαρμογές που έχουν αναπτυχθεί για μία πλατφόρμα να τρέχουν σε μία άλλη χωρίς να τροποποιηθούν οι ίδιες οι εφαρμογές. Η Java Virtual Machine (JVM) είναι ένα παράδειγμα εφαρμογής virtualization. Ενεργεί κατά κάποιο τρόπο ως μεσάζων μεταξύ του κώδικα εφαρμογής της Java και του λειτουργικού συστήματος (λειτουργικό σύστημα OS).
Μια άλλη μορφή του virtualization, γνωστή και ως λειτουργικό σύστημα το virtualization, παρέχει μια εικονική εφαρμογή της διεπαφής του λειτουργικού συστήματος που μπορεί να χρησιμοποιηθεί για να τρέξουν εφαρμογές γραμμένες για το ίδιο λειτουργικό σύστημα με τον πάροχο, με την κάθε εφαρμογή να είναι σε ξεχωριστό δοχείο VM. Η έκδοση αυτή επικεντρώνεται στη μορφή του virtualization που είναι γνωστή ως Full Virtualization. Στη μορφή Full Virtualization, ένα ή περισσότερα λειτουργικά συστήματα και οι εφαρμογές που περιέχουν τρέχουν πάνω στο εικονικό υλικό. Κάθε παράδειγμα ενός λειτουργικού συστήματος και οι εφαρμογές του, τρέχουν σε ξεχωριστό VM, το οποίο ονομάζεται φιλοξενούμενο OS. Το φιλοξενούμενο σε έναν κεντρικό υπολογιστή λειτουργικό σύστημα το διαχειρίζεται ο Hypervisor, που ονομάζεται επίσης Virtual Machine Monitor (VMM), ο οποίος ελέγχει τη ροή των εντολών μεταξύ των επισκεπτών OS και του φυσικού υλικού (hardware), όπως η CPU, οι σκληροί δίσκοι, η μνήμη και οι κάρτες διασύνδεσης δικτύου. Ο hypervisor έχει τη δυνατότητα να διαμοιράσει τους πόρους του συστήματος και να απομονώσει τον επισκέπτη ενός λειτουργικού συστήματος, έτσι ώστε ο καθένας έχει πρόσβαση μόνο σε δικούς του πόρους, καθώς και πιθανή πρόσβαση σε κοινόχρηστους πόρους, όπως τα αρχεία του host OS.
Επίσης, κάθε φιλοξενούμενο OS μπορεί να είναι εντελώς κλειστό, καθιστώντας το φορητό. Μερικοί hypervisors τρέχουν πάνω τους ένα άλλο λειτουργικό σύστημα, το οποίο είναι γνωστό ως λειτουργικό σύστημα υποδοχής, με πλήρη εικονικοποίηση του hypervisor, το οποίο παρέχει τα ίδιες δυνατότητες με τις διεπαφές υλικού, με αυτές που προβλέπονται από τη φυσική πλατφόρμα του υλικού. Αυτό σημαίνει ότι το λειτουργικό σύστημα και εφαρμογές που τρέχουν μέσα σε πλήρη εικονικοποίηση δεν χρειάζεται να τροποποιηθούν για να εκτελέσουν μια εργασία virtualization, εφόσον το λειτουργικό σύστημα και οι εφαρμογές είναι συμβατές με το υποκείμενο υλικό. Μια ενδιαφέρουσα εκδοχή της πλήρους εικονικοποίησης είναι η paravirtualization, η οποία είναι μια μέθοδος που προσφέρει διασυνδέσεις του hypervisor με το λειτουργικό σύστημα του επισκέπτη, επιτρέποντας στο φιλοξενούμενο λειτουργικό σύστημα να χρησιμοποιηθεί αντί για το κανονικό με τις διεπαφές υλικού. Ένα φιλοξενούμενο λειτουργικό σύστημα μπορεί να χρησιμοποιήσει paravirtualized διασυνδέσεις, που προσφέρουν σημαντικά ταχύτερη πρόσβαση στους πόρους, όπως σκληρούς δίσκους, και τα δίκτυα. Διαφορετικοί τύποι paravirtualization προσφέρονται από διαφορετικά συστήματα hypervisor.

4.1 Κίνητρα για χρήση του Virtualization

Η πρόσφατη αύξηση της χρήσης των προϊόντων που χρησιμοποιούν πλήρη virtualization και των υπηρεσιών τους έχει δημιουργήσει πολλά οφέλη. Μία από τις πιο συχνές αιτίες για την υιοθέτηση της πλήρους εικονικοποίησης είναι η λειτουργική αποτελεσματικότητα:
Οι οργανισμοί μπορούν να χρησιμοποιήσουν το υπάρχον υλικό τους (και τις νέες αγορές hardware) πιο αποτελεσματικά, δίνοντας μεγαλύτερη ισχύ σε κάθε υπολογιστή. Σε γενικές γραμμές, οι διακομιστές που χρησιμοποιούν την πλήρη virtualization μπορούν να αξιοποιήσουν καλύτερα την επεξεργαστική ισχύ του υπολογιστή και τους πόρους μνήμης των servers που τρέχουν ένα μόνο παράδειγμα, το λειτουργικό σύστημα και ένα ενιαίο σύνολο υπηρεσιών.
Οι πρόσφατες εξελίξεις στην αρχιτεκτονική των επεξεργαστών έχουν κάνει την πλήρη εικονικοποίηση πιο γρήγορη από ό,τι πριν από λίγα χρόνια, ενώ παρόμοια πρόοδος αναμένεται να συνεχίσει να πραγματοποιείται τόσο από τους πωλητές CPU όσο και από τους προμηθευτές λογισμικού εικονικοποίησης. Επίσης, οι αλλαγές στην αρχιτεκτονική των επεξεργαστών έχουν κάνει την πλήρη εικονικοποίηση πιο ασφαλή, με την ενίσχυση των περιορισμών του hypervisor για τους πόρους.
Μια δεύτερη κοινή χρήση της πλήρους virtualization αφορά εφαρμογές desktop virtualization, όπου, για παράδειγμα, ένα PC τρέχει περισσότερα από ένα λειτουργικά. Υπάρχουν αρκετοί λόγοι για την ανάπτυξη desktop virtualization. Μπορεί να προσφέρει υποστήριξη για εφαρμογές που τρέχουν μόνο σε ένα συγκεκριμένο λειτουργικό σύστημα. Επιτρέπει αλλαγές που πρέπει να γίνουν σε ένα λειτουργικό σύστημα και στη συνέχεια επιστροφή στην αρχική κατάσταση , αν χρειαστεί, όπως για την εξάλειψη των αλλαγών που επηρεάζουν αρνητικά την ασφάλεια. Το desktop virtualization υποστηρίζει επίσης τον καλύτερο έλεγχο των OS, προκειμένου να διασφαλίζεται ότι πληρούν τις απαιτήσεις ασφαλείας του οργανισμού. Ο έλεγχος αυτός μπορεί να υποστηριχθεί με τη δημιουργία μιας πλατφόρμας υψηλής διαβεβαίωσης που ενημερώνει συνεχώς το λειτουργικό σύστημα του επισκέπτη, ώστε να έχει τις ακριβές εκδόσεις των προγραμμάτων που είναι εξουσιοδοτημένα να έχουν και να μην υπάρχουν άλλα προγράμματα.
Μια πιο πρόσφατη χρήση του desktop virtualization είναι να καταστεί δυνατή η χρήση των εφαρμογών που τρέχουν μόνο σε μια παλαιότερη έκδοση του λειτουργικού συστήματος, όταν στην επιφάνεια εργασίας του χρήστη τρέχει μια νεότερη έκδοση. Σε μια τέτοια κατάσταση, το virtualization desktop είναι χρήσιμο. Καθώς περισσότερες εφαρμογές γίνονται web-based, το desktop virtualization μπορεί να γίνει ακόμη πιο σημαντικό: μια διαδικτυακή εφαρμογή που τρέχει μόνο σε μια παλαιότερη έκδοση ενός συγκεκριμένου προγράμματος περιήγησης μπορεί να εκτελεστεί σε ένα εικονικό σύστημα που διαθέτει την παλαιότερη έκδοση αυτού του προγράμματος περιήγησης, ενώ το κύριο περιβάλλον του χρήστη εκτελεί τη νεότερη (συνήθως πιο ασφαλή) έκδοση του προγράμματος περιήγησης. Για τις περιπτώσεις χρήσης όπως αυτή, πολλοί οργανισμοί χρησιμοποιούν τη virtualization εφαρμογή αντί για το desktop virtualization.
Η χρήση όμως της πλήρους εικονικοποίησης έχει ορισμένες αρνητικές συνέπειες για την ασφάλεια. Αυτή η έκδοση προσθέτει επιπλέον επίπεδα στην τεχνολογία, η οποία μπορεί να αυξήσει το βάρος της απαιτούμενης διαχείρισης ασφάλειας με πρόσθετους ελέγχους. Επιπλέον, ορισμένα συστήματα virtualization καθιστούν εύκολη την ανταλλαγή πληροφοριών μεταξύ των συστημάτων, με αποτέλεσμα το ενδεχόμενο μιας επίθεσης να είναι σημαντικό αν δεν ελέγχονται προσεκτικά. Σε ορισμένες περιπτώσεις, τα εικονικά περιβάλλοντα είναι αρκετά πιο δυναμικά, γεγονός που καθιστά τη δημιουργία και τη διατήρηση των απαραίτητων ορίων ασφαλείας πιο περίπλοκη.

4.2 Virtualization Security

Η μετεγκατάσταση υπολογιστικών πόρων σε ένα εικονικό περιβάλλον έχει μικρή ή καμία επίδραση στις περισσότερες από τις αδυναμίες των πόρων και τις απειλές που αντιμετωπίζουν. Για παράδειγμα, αν μια υπηρεσία έχει εξ αρχής αδυναμίες, με τη μετακίνηση της υπηρεσίας από ένα μη-virtualized διακομιστή σε έναν εικονικό διακομιστή, η υπηρεσία θα εξακολουθεί να είναι εξίσου ευάλωτη σε επιθέσεις exploitation. Ωστόσο, ενώ η χρήση του virtualization μπορεί να βοηθήσει στη μείωση των επιπτώσεων της εν λόγω επίθεσης, το virtualization μπορεί παράλληλα να ενισχύσει τέτοιου είδους επιθέσεις, αυξάνοντας έτσι την πιθανότητα επιτυχημένων επιθέσεων. Πολλές από τις λειτουργίες του virtualization προσφέρουν σημαντικά πλεονεκτήματα αλλά και μειονεκτήματα ως προς την ασφάλεια.

4.3 Απομόνωση Guest OS

Ο hypervisor είναι υπεύθυνος για τη διαχείριση της πρόσβασης επισκεπτών OS στο υλικό (hardware) (π.χ. CPU, μνήμη, σκληροί δίσκοι). Ο hypervisor διανέμει αυτούς τους πόρους έτσι ώστε κάθε φιλοξενούμενο λειτουργικό σύστημα να μπορεί να έχει πρόσβαση στους «δικούς» του και μόνο πόρους και να μην μπορεί να έχει πρόσβαση στους πόρους των άλλων επισκεπτών OS ή οι πόροι να μην διατίθενται για χρήση virtualization. Αυτό αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση σε πόρους του συστήματος και επίσης βοηθά στην προστασία ενός φιλοξενούμενου λειτουργικού από επίθεση κακόβουλου λογισμικού, που θα είχε ως αποτέλεσμα τη μόλυνση των αρχείων των επισκεπτών ή την τοποθέτηση κώδικα κακόβουλου λογισμικού στη μνήμη ενός άλλου φιλοξενούμενου OS. Από την άλλη, η στεγανοποίηση μπορεί επίσης να μειώσει την απειλή μιας επίθεσης Denial of Service που προκαλείται από την υπερβολική κατανάλωση των πόρων σε άλλους πελάτες και λειτουργικά συστήματα με τον ίδιο hypervisor.

Οι πόροι μπορούν να διαχωριστούν φυσικά ή λογικά. Στη φυσική στεγανοποίηση, ο hypervisor εκχωρεί ξεχωριστούς φυσικούς πόρους σε κάθε φιλοξενούμενο λειτουργικό σύστημα, όπως κατατμήσεις δίσκων, οδηγούς δίσκων και καρτών διασύνδεσης δικτύου. Με τον λογικό διαχωρισμό μπορούμε να χωρίσουμε τους πόρους σε μια ενιαία υποδοχή ή σε πολλούς κεντρικούς υπολογιστές, όπως σε ένα απόθεμα δυναμικού με τον ίδιο αντίκτυπο ,κατηγοριοποίηση σε επίπεδο ασφάλειας επιτρέποντας πολλαπλούς επισκέπτες να μοιράζονται τους ίδιους φυσικούς πόρους , όπως επεξεργαστές και μνήμη RAM, με τον hypervisor ως διαμεσολαβητή για την πρόσβαση σε αυτούς τους πόρους. Η φυσική στεγανοποίηση θέτει σκληρούς περιορισμούς στους πόρους για κάθε φιλοξενούμενο OS, επειδή η αχρησιμοποίητη παραγωγική ικανότητα από τη μια πηγή δεν μπορεί να προσεγγιστεί από οποιοδήποτε άλλο φιλοξενούμενο λειτουργικό σύστημα. Ωστόσο, εφαρμόζοντας τον φυσικό διαχωρισμό των πόρων μπορεί να παρέχει μεγαλύτερη ασφάλεια και καλύτερη απόδοση από ό, τι η λογική κατάτμηση. Πολλά συστήματα virtualization μπορούν να εφαρμόσουν τόσο τη φυσική όσο και τη λογική κατάτμηση. Μερικοί οργανισμοί ακολουθούν πολιτικές σύμφωνα με τις οποίες τα δεδομένα τους μπορούν να διανεμηθούν σε μονάδες δίσκου μαζί με τα δεδομένα των άλλων εφαρμογών, καθώς και οι πολιτικές αυτές πρέπει να λαμβάνουν υπόψη τη φυσική και τη λογική κατάτμηση στους hypervisors.

Οι διαφορετικές κατατμήσεις των πόρων αποτελούν σημαντικό μέρος της απομόνωσης του επισκέπτη OS. Η απομόνωση περιλαμβάνει επίσης τον περιορισμό του φιλοξενούμενου λειτουργικού συστήματος επικοινωνιών και της πρόσβασης σε κάθε φιλοξενούμενο λειτουργικό σύστημα που έχει με τους άλλους επισκέπτες OS, στο hypervisor και στον κεντρικό υπολογιστή του λειτουργικού συστήματος (αν υπάρχει). Οι hypervisors μπορούν να υποστηρίξουν θεωρητικά ένα επίπεδο λογικής απομόνωσης σχεδόν ισοδύναμης με τη φυσική απομόνωση, διευθετώντας όλες τις επικοινωνίες από κάθε φιλοξενούμενο OS, ώστε να έχουν πλήρη έλεγχο των ενεργειών κάθε επισκέπτη. Επίσης, οι hypervisors μπορούν να επιτρέπουν αλληλεπιδράσεις

μεταξύ επισκεπτών OS ανάλογα με τις ανάγκες, όπως να επιτραπεί σε δύο desktop OS να μοιράζονται ένα κοινό σύστημα αρχείων. Ακόμη, μπορούν να αλλάξουν δυναμικά την απομόνωση για κάθε λειτουργικό σύστημα επισκέπτη ανάλογα με τις ανάγκες, όπως για παράδειγμα, ενεργοποίηση και απενεργοποίηση της δικτύωσης σε συγκεκριμένες ώρες. Η έννοια της απομόνωσης παρέχει προφανή οφέλη ασφάλειας, αλλά μπορεί επίσης να αυξήσει την αξιοπιστία της με μια σειρά από δράσεις πρόληψης σε ένα φιλοξενούμενο λειτουργικό σύστημα που επηρεάζει άμεσα τα υπόλοιπα. Για παράδειγμα, εάν ένα φιλοξενούμενο λειτουργικό σύστημα κολλάει εξαιτίας ενός σφάλματος εφαρμογής ή μιας επίθεσης, το άλλο λειτουργικό σύστημα σε αυτόν τον κεντρικό υπολογιστή είναι πιθανό να μην επηρεαστεί καθόλου. Η απομόνωση κάθε λειτουργικού συστήματος επισκέπτη από τα υπόλοιπα και ο περιορισμός του ως προς τους πόρους στους οποίους μπορεί να έχει πρόσβαση και ως προς τα προνόμια που μπορεί να αποκτήσει είναι επίσης γνωστή ως Sandboxing.
Ένα άλλο κίνητρο για την απομόνωση των επισκεπτών OS από τους υπόλοιπους, είναι οι επιθέσεις που εκμεταλλεύονται τις φυσικές ιδιότητες του υλικού για να αποκαλύψουν πληροφορίες σχετικά με τα πρότυπα χρήσης για πρόσβαση στη μνήμη, χρήση της CPU και άλλους πόρους που χρησιμοποιούνται. Ένας κοινός στόχος αυτών των επιθέσεων είναι να αποκαλύψουν τα κλειδιά κρυπτογράφησης. Αυτές οι επιθέσεις θεωρούνται δύσκολες, γιατί συνήθως απαιτούν την άμεση φυσική πρόσβαση στον κεντρικό υπολογιστή.
Οι επιτιθέμενοι, όμως, μπορούν να επιχειρήσουν να επιτεθούν από ένα φιλοξενούμενο λειτουργικό σύστημα ώστε να αποκτήσουν πρόσβαση στο hypervisor, σε άλλα φιλοξενούμενα λειτουργικά συστήματα ή ακόμη και στο host OS. Εάν ένας εισβολέας κατορθώσει να ξεφύγει από έναν OS επισκέπτη και να αποκτήσει πρόσβαση στο hypervisor, μπορεί να θέσει σε κίνδυνο τον hypervisor και να πάρει υπό τον έλεγχό του το σύνολο των επισκεπτών του OS. Έτσι, ο hypervisor μπορεί να δημιουργήσει ένα σημαντικό κενό ασφαλείας, θέτοντας σε κίνδυνο όλους τους φιλοξενούμενους OS.
Οι φιλοξενούμενοι OS συχνά δεν είναι εντελώς απομονωμένοι από τους άλλους και από το λειτουργικό σύστημα υποδοχής, γιατί αυτό θα εμπόδιζε τη λειτουργικότητα. Για παράδειγμα, πολλοί που χρησιμποποιούν virtualization παρέχουν μηχανισμούς με τους οποίους ο επισκέπτης OS μπορεί να έχει πρόσβαση σε αρχεία, καταλόγους και άλλους πόρους στο κεντρικό λειτουργικό σύστημα ή άλλο φιλοξενούμενο λειτουργικό σύστημα. Όμως αυτοί οι μηχανισμοί επικοινωνίας μπορούν ακούσια να χρησιμεύσουν ως φορέας μιας επίθεσης, όπως η μετάδοση κακόβουλου λογισμικού, ή να επιτρέψουν σε έναν εισβολέα να αποκτήσει πρόσβαση σε συγκεκριμένους πόρους. Μόνο το Bare Metal Virtualization λογισμικό δεν προσφέρει τέτοιες δυνατότητες κοινής χρήσης αρχείων.

4.4 Παρακολούθηση Guest OS

Ο hypervisor έχει πλήρη επίγνωση της τρέχουσας κατάστασης του κάθε φιλοξενούμενου λειτουργικού συστήματος που ελέγχει. Ως εκ τούτου, ο hypervisor έχει τη δυνατότητα να παρακολουθεί κάθε OS επισκεπτών, όπως είναι η ενδοσκόπηση. Η ενδοσκόπηση μπορεί να παρέχει όλες τις δυνατότητες ελέγχο. Μέσω της ενδοσκόπησης παρέχεται η δυνατότητα παρακολούθησης της κυκλοφορίας του δικτύου, της μνήμης, των διαδικασιών, καθώς και άλλων στοιχείων ενός επισκέπτη OS. Για πολλά προϊόντα virtualization, ο hypervisor μπορεί να ενσωματώσει περαιτέρω λειτουργίες ασφαλείας ή διασύνδεσης με εξωτερικούς ελέγχους ασφαλείας, οι οποίοι θα παρέχουν πληροφορίες για τα στοιχεία που συγκεντρώθηκαν μέσω της ενδοσκόπησης. Τα παραδείγματα περιλαμβάνουν firewalling, ανίχνευση εισβολέων, καθώς και έλεγχο πρόσβασης.
Το δίκτυο παρακολούθησης της κυκλοφορίας είναι ιδιαίτερα σημαντικό όταν μια δικτύωση διεξάγεται μεταξύ δύο επισκεπτών OS στον κεντρικό υπολογιστή ή μεταξύ ενός επισκέπτη OS και του host OS. Σε συνηθισμένες ρυθμίσεις παραμέτρων του δικτύου, αυτή η κίνηση δεν περνά μέσα από το δίκτυο αλλά μέσω των ελέγχων ασφαλείας φιλοξενίας .

4.5 Διαχείριση εικόνας και στιγμιότυπου

Η «δημιουργία» εικόνων και στιγμιοτύπων μιας μηχανής επισκέπτη δεν επηρεάζει τα τρωτά σημεία στο εσωτερικό τους, όπως μπορούν να επηρεαστούν στον επισκέπτη OS, τις υπηρεσίες και τις εφαρμογές. Ωστόσο, οι εικόνες και τα στιγμιότυπα επηρεάζουν την ασφάλεια με πολλούς τρόπους, μερικές φορές θετικά και κάποιες άλλες αρνητικά, και επίσης μπορούν να επηρεάσουν τις λειτουργίες ενός IT.

Ένα από τα μεγαλύτερα ζητήματα ασφάλειας με εικόνες και στιγμιότυπα είναι ότι περιέχουν ευαίσθητα δεδομένα (όπως είναι οι κωδικοί πρόσβασης, δεδομένα προσωπικού χαρακτήρα, και ούτω καθεξής), ακριβώς όπως ένας φυσικός σκληρός δίσκος. Επειδή είναι πιο εύκολο για κάποιο ννα κινηθεί γύρω από μια εικόνα ή ένα στιγμιότυπο από ότι σε ένα σκληρό δίσκο, είναι πιο σημαντικό να μεριμνήσουμε για την ασφάλεια των δεδομένων σε αυτή την εικόνα ή το στιγμιότυπο. Τα στιγμιότυπα μπορεί να είναι πιο επικίνδυνα από τις εικόνες, επειδή περιέχουν τα περιεχόμενα της μνήμης RAM τη χρονική στιγμή που τραβήχτηκε το στιγμιότυπο και αυτό μπορεί να περιλαμβάνει τις ευαίσθητες πληροφορίες που δεν ήταν ακόμη αποθηκευμένες στη μονάδα δίσκου του ίδιου του συστήματος.

Ένα λειτουργικό σύστημα μαζί με τις εφαρμογές του μπορούν να εγκατασταθούν και να ρυθμιστούν ώστε να εξασφαλιστούν και να δοκιμαστούν σε μια ενιαία εικόνα, και στη συνέχεια η εικόνα αυτή να διανέμεται σε πολλούς κεντρικούς υπολογιστές. Αυτός ο τρόπος μπορεί να μας εξοικονομήσει πολύ χρόνο, ενώ παράλληλα βελτιώνει τη συνοχή και τη δύναμη της ασφάλειας σε ολόκληρο το σύστημα. Ωστόσο, επειδή οι εικόνες μπορούν να διανεμηθούν και να αποθηκευθούν εύκολα, πρέπει να προστατεύονται προσεκτικά από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση και αντικατάσταση των δεδομένων τους. Ορισμένοι οργανισμοί πρέπει να έχουν ένα μικρό αριθμό «γνωστών» εικόνων των προσκεκλημένων λειτουργικών συστημάτων που διαφέρουν, για παράδειγμα ως προς το λογισμικό εφαρμογής που έχει εγκατασταθεί.

Δεδομένου ότι η χρήση των διακομιστών και των desktop virtualization αυξάνεται μέσα σε μια οργάνωση, η διαχείριση των εικόνων μπορεί να αποτελέσει σημαντική πρόκληση. Ορισμένα προϊόντα virtualization προσφέρουν λύσεις διαχείρισης ώστε να μπορούν να εξετάζουν τις αποθηκευμένες εικόνες και να ενημερώνουν ανάλογα με τις ανάγκες, (π.χ. εφαρμόζοντας τα κατάλληλα μπαλώματα και κάνοντας αλλαγές στις ρυθμίσεις ασφαλείας), όμως υπάρχουν και άλλα προϊόντα τα οποία δεν προσφέρουν τρόπους για την εφαρμογή των ενημερώσεων ασφαλείας, εκτός από τη φόρτωση κάθε εικόνας. Για τα προϊόντα αυτά, οι επιπλέον εικόνες αποθηκεύονται χωρίς να «τρέχουν», με αποτέλεσμα τα τρωτά σημεία που πιθανόν να περιέχονται να επανενεργοποιούνται όταν φορτώνονται και πάλι. Μπορεί να είναι απαραίτητο να παρακολουθούμε όλες τις εικόνες προκειμένου να εξασφαλίσουμε ότι κάθε εικόνα ενημερώνεται περιοδικά. Η παρακολούθηση των εικόνων μπορεί επίσης να αποτελέσει σημαντικό πρόβλημα, ειδικά αν οι χρήστες και οι διαχειριστές μπορούν να δημιουργούν τις δικές τους εικόνες. Αυτές οι εικόνες μπορούν επίσης να μην εξασφαλίζονται κατάλληλα, ειδικά εάν δεν βασίζονται σε μια βάση ασφάλειας (π.χ. αυτή που παρέχεται από μία διαφορετική προ-ασφαλισμένη εικόνα). Αυτό θα μπορούσε να αυξήσει τον κίνδυνο του «συμβιβασμού».

Ένα άλλο πιθανό πρόβλημα με την αύξηση της χρήσης του virtualization, ειδικότερα, είναι η διάδοση των εικόνων, επίσης γνωστή ως εξάπλωση. Είναι εύκολο να δημιουργήσουμε μια νέα εικόνα –συχνά μπορεί να γίνει και μέσα σε λίγα λεπτά– χωρίς όμως να εξετάσουμε την ασφάλεια και πόσες περιττές εικόνες μπορεί να δημιουργήσουμε και να τρέξουν. Κάθε πρόσθετο τρέξιμο μιας εικόνας είναι ένα άλλο δυναμικό σημείο του «συμβιβασμού» για έναν εισβολέα. Επίσης, κάθε πρόσθετη εικόνα είναι μια διαφορετική εικόνα που πρέπει να έχει την ασφάλεια που ακολουθείται. Ως εκ τούτου, οι οργανισμοί θα πρέπει να ελαχιστοποιήσουν τη δημιουργία, την αποθήκευση και τη χρήση περιττών εικόνων. Επίσης, οι οργανισμοί θα πρέπει να εξετάσουν την εφαρμογή των τυπικών διαδικασιών διαχείρισης μιας εικόνας που διέπουν τη δημιουργία της εικόνας, την ασφάλεια, τη διανομή, την αποθήκευση, τη χρήση και την

καταστροφή, ειδικά για virtualization. Παρόμοια προσοχή πρέπει να δοθεί στη διαχείριση ενός στιγμιότυπου. Σε ορισμένες περιπτώσεις, οι οργανισμοί ακολουθούν πολιτικές που δεν επιτρέπουν την αποθήκευση των στιγμιότυπων, λόγω του κινδύνου των malware από τα μολυσμένα συστήματα τα οποία μπορούν να αποθηκευθούν σε στιγμιότυπα και αργότερα να επαναφορτωθούν.

Η διαχείριση των εικόνων μπορεί να προσφέρει σημαντικά οφέλη ασφαλείας και λειτουργίας σε έναν οργανισμό. Για παράδειγμα, αν είναι σε κίνδυνο το περιεχόμενο μιας εικόνας, καταστραφεί ή υποστεί άλλη βλάβη, η εικόνα μπορεί γρήγορα να αντικατασταθεί με μια γνωστή-καλή εικόνα. Επίσης, τα στιγμιότυπα μπορεί να χρησιμεύσουν ως αντίγραφα ασφαλείας, που επιτρέπουν την ταχεία ανάκτηση των πληροφοριών που προστίθενται στο φιλοξενούμενο λειτουργικό σύστημα από την αρχική εικόνα που αναπτύχθηκε. Ένα από τα μειονεκτήματα που συνδέονται με αυτό το είδος της δημιουργίας αντιγράφων ασφαλείας είναι ότι λαμβάνονται πρόσθετα ή διαφορετικά αντίγραφα ασφαλείας του συστήματος τα οποία μπορεί να μην είναι εφικτά εάν τα αντίγραφα ασφαλείας υποστηρίζονται μόνον από τον hypervisor. Εάν πραγματοποιηθεί μια τροποποίηση στο φιλοξενούμενο λειτουργικό σύστημα μετά από τη «σύλληψη» ενός στιγμιότυπου, το αρχικό στιγμιότυπο δεν θα περιλαμβάνει την τροποποίηση και ένα νέο στιγμιότυπο θα πρέπει να εφαρμοστεί. Εξαιτίας αυτού, το στιγμιότυπο της διαχείρισης θα πρέπει να θεωρηθεί ως μέρος της διαχείρισης της εικόνας.

Τα αρχεία εικόνας μπορούν να ελέγχονται για τον εντοπισμό μη εξουσιοδοτημένων αλλαγών: αυτό μπορεί να γίνει με τον υπολογισμό κρυπτογραφικών αθροισμάτων ελέγχου για κάθε αρχείο που είναι αποθηκευμένο, στη συνέχεια γίνεται εκ νέου υπολογισμός αυτών των checksums περιοδικά ώστε να ερευνούν την προέλευση τυχόν αποκλίσεων. Τα αρχεία εικόνας μπορούν επίσης να σαρωθούν για την ανίχνευση rootkits και άλλων κακόβουλων προγραμμάτων, που όταν τρέχουν, να μπορούν να αποκρύπτονται οι ίδιες από το παρόν λογισμικό ασφάλειας που υπάρχει εντός του φιλοξενούμενου λειτουργικού.

Σε μερικά συστήματα virtualization, τα guest OS μπορούν να μετακινηθούν από τον ένα υπολογιστή στον άλλο όταν απαιτείται, όπως όταν ένας host πρέπει να επανεκκινήσει ή να κλείσει για εργασίες συντήρησης, όταν εμφανιστεί σφάλμα στον κεντρικό υπολογιστή ή ανιχνευθεί μια επίθεση εναντίον του hypervisor ή OS, όταν υπάρχει υποψία για επικείμενη επίθεση. Αυτό μπορεί να μειώσει την πίεση για ταχεία εκτέλεση των αναβαθμίσεων και των αντικαταστάσεων, μειώνοντας έτσι την ταλαιπωρία στους διαχειριστές του συστήματος και παρέχοντας περισσότερο χρόνο για τη δοκιμή των αλλαγών. Για το virtualization, ο hypervisor μπορεί να είναι σε θέση να μεταφέρει έναν επισκέπτη OS σε άλλους κεντρικούς υπολογιστές αυτόματα, όμως σε μερικά συστήματα VM αυτό μπορεί να συμβεί όταν οι εικονικές μηχανές θα βρίσκονται σε εξέλιξη και δεν απαιτούν διακοπή ή αναστολή του λειτουργικού συστήματος των επισκεπτών. Για το desktop virtualization, οι ενέργειες γίνονται βάσει ενός εγχειριδίου αλλαγών. Ένα δίκτυο αποθήκευσης είναι προορισμένο να εκτελεί αυτές τις αλλαγές και το κανάλι μεταφοράς έχει τον πλήρη έλεγχο ταυτότητας και κρυπτογράφησης για να διαφυλαχθεί η ακεραιότητα του VM και να αποτραπεί η διαρροή πληροφοριών.

Για ένα virtualization που περιλαμβάνει πολλούς φυσικούς διακομιστές, το φιλοξενούμενο λειτουργικό σύστημα μετανάστευσης το οποίο υποστηρίζει την εξισορρόπηση φορτίου, επιτρέπει τον δυναμικό έλεγχο για κάθε εικονικό διακομιστή που φιλοξενεί το οποίο μπορεί να τρέχει σε κάθε χρονική στιγμή. Για παράδειγμα, αν ένα συγκεκριμένο host γίνεται «βαρύ», σχεδόν μέχρι το σημείο εξάντλησης των πόρων του, ένα ή περισσότερα φιλοξενούμενα λειτουργικά σύστηματα θα μπορούσαν να μεταφερθούν σε υπολογιστές με μειωμένη χρησιμοποίηση. Αυτό αποτρέπει την εμφάνιση Denial of Service (DOS), αλλά πιο συχνά χρησιμοποιείται για να βελτιώσει τις επιδόσεις του φιλοξενούμενου OS.

Ένα πιθανό μειονέκτημα των φιλοξενούμενων λειτουργικών συστημάτων που χρησιμοποιούν λειτουργικό σύστημα μετανάστευσης είναι ότι, εάν ένα φιλοξενούμενο λειτουργικό σύστημα έχει τεθεί σε κίνδυνο ή περιέχει κακόβουλο κώδικα, αλλά αυτή η κακόβουλη δραστηριότητα δεν έχει ανιχνευθεί, το φιλοξενούμενο λειτουργικό σύστημα μπορεί να μετεγκατασταθεί σε

άλλο υποδοχής, με αποτέλεσμα να τίθεται σε κίνδυνο και αυτό. Το ίδιο πρόβλημα παρουσιάζεται κατά τη μετατροπή ενός φυσικού συστήματος σε μια εικονική μηχανή.
Η χρήση των εικόνων μπορεί να βελτιώσει τις πρακτικές δοκιμές του λογισμικού. Ένας οργανισμός μπορεί να εξετάσει μια αίτηση σε πολλά OS χωρίς να χρειάζεται ξεχωριστό υλικό για το κάθε λειτουργικό σύστημα. Πρόσθετες φυσικές μηχανές δοκιμής μπορεί να είναι αναγκαίες για να ελέγξουμε τη συμβατότητα του υλικού. Οι οργανισμοί δεν πρέπει να εξαρτώνται αποκλειστικά από τα αποτελέσματα των δοκιμών που προβλέπονται σε ένα εικονικό περιβάλλον. Το περιβάλλον virtualization μπορεί να παρέχει κάποιες λειτουργίες ή τις λειτουργίες ασφαλείας που δεν υπάρχουν για το περιβάλλον-στόχο, με πιθανό αποτέλεσμα ανακριβή αποτελέσματα. Ειδικότερα, λόγω των γενικών εξόδων που απαιτούνται για ένα virtualization, το φορτίο δοκιμής σε ένα εικονικό περιβάλλον μπορεί να μην παρέχει τα ίδια αποτελέσματα με τον έλεγχο του φορτίου σε ένα φυσικό περιβάλλον. Εκτός από την εξασφάλιση ότι το φιλοξενούμενο OS, η δοκιμαστική εικόνα, έχει ρυθμιστεί όπως το περιβάλλον-στόχος, οι οργανισμοί θα πρέπει να εξασφαλίζουν ότι οι πρόσθετες αυτές δοκιμές πραγματοποιούνται σε φυσικό υλικό.
Οι οργανισμοί μπορούν να διατηρήσουν τα γνωστά-καλά αντίγραφα για κάθε φιλοξενούμενο λειτουργικό σύστημα σε έναν ενιαίο χώρο, επιτρέποντας στους ελεγκτές να επωφελούνται από ένα «νέο» αντίγραφο του φιλοξενούμενου λειτουργικού συστήματος για κάθε δοκιμή που μπορεί να επαναφέρει το σύστημα στην επιθυμητή κατάσταση. Αυτό επιτρέπει στους ελεγκτές να εξασφαλίσουν ότι η διαμόρφωση του περιβάλλοντος των δοκιμών συμπίπτει με εκείνη του περιβάλλοντος παραγωγής και ότι τα αποτελέσματα της εκτέλεσης μιας δοκιμής δεν θα επηρεάσουν κατά λάθος τα αποτελέσματα του επόμενου τεστ. Επίσης, μέσω του virtualization, οι δοκιμαστές μπορούν να έχουν πρόσβαση σε πολλαπλές διαμορφώσεις και πλατφόρμες για τη δοκιμή εφαρμογών, ενημερώσεων λογισμικού ή μπαλώματα, σε ένα ασφαλές περιβάλλον. Με την σωστή ρύθμιση των παραμέτρων του φιλοξενούμενου λειτουργικού, κάθε διαθέσιμη διαμόρφωση σε ένα σύστημα παραγωγής μπορεί να αναπαραχθεί. Σε όλες αυτές τις περιπτώσεις, οι εικόνες μπορούν να χρησιμοποιηθούν ώστε να επιτευχθεί ένα καλό αποτέλεσμα. Οι εικόνες που περιέχουν ένα ολόκληρο φιλοξενούμενο λειτουργικό σύστημα μπορούν να εφαρμοστούν σε κάθε νέο αντίγραφο, καθώς πολλοί οργανισμοί διατηρούν τις εικόνες τους σε κοινό χώρο αποθήκευσης, έτσι ώστε πολλές υπηρεσίες να μπορούν να έχουν πρόσβαση σε αυτές εύκολα.

4.6 Συστάσεις ασφαλείας για τα μέρη του Virtualization

Η ασφάλεια που παρέχει η πλήρης εικονικοποίηση εξαρτάται σε μεγάλο βαθμό από την ατομική ασφάλεια των συστατικών του ξεχωριστά –συμπεριλαμβανομένου του hypervisor– στον κεντρικό υπολογιστή και host OS (κατά περίπτωση), guest OS, των εφαρμογών και των σκληρών δίσκων. Οι οργανισμοί θα πρέπει να εξασφαλίσουν όλα αυτά τα στοιχεία και τη διατήρηση της ασφαλείας τους, ώστε να βασίζονται σε ορθές πρακτικές ασφαλείας, όπως ο περιορισμός της πρόσβασης σε διοικητικές διεπαφές, διατηρώντας το λογισμικό ενημερωμένο με τα μπαλώματα ασφαλείας, χρησιμοποιώντας ασφαλή διαμόρφωση βάσης, που εκτελεί την καταγραφή και την ανάλυση των κορμών σε όλα τα στρώματα της λύσης και με βάσει κεντρικού τείχους προστασίας, λογισμικό προστασίας από ιούς, ή άλλους κατάλληλους μηχανισμούς για την ανίχνευση και την αντιμετώπιση των επιθέσεων.
Ωστόσο, οι παραπάνω πρακτικές δεν είναι αρκετές για να εξασφαλίσουν μία ασφαλή λύση virtualization. Virtualization μπορεί να χρησιμοποιηθεί με πολλούς τρόπους, έτσι ώστε να διαφέρουν απο τους ενδεδειγμένους ελέγχους ασφαλείας για κάθε κατάσταση. Αυτή η ενότητα περιγράφει τις κοινές απειλές κατά των λύσεων virtualization και παρέχει συστάσεις για την αντιμετώπιση αυτών των απειλών. Με αυτές τις πληροφορίες, οι οργανισμοί θα είναι σε θέση να εφαρμόσουν το πλαίσιο διαχείρισης των κινδύνων που περιγράφονται στο «NIST SP 800 - 37 Αναθεώρηση 1, οδηγός για την εφαρμογή του πλαισίου διαχείρισης κινδύνων για

Ομοσπονδιακά Πληροφοριακά Συστήματα: “Μια Ζωή Ασφαλείας -Προσέγγιση Κύκλου” με μεγαλύτερη ακρίβεια για την αξιολόγηση των κινδύνων που συνδέονται με το virtualization.
Σε γενικές γραμμές, οι οργανισμοί πρέπει να εφαρμόζουν τους ίδιους ελέγχους ασφαλείας που ισχύουν για τα εικονικά λειτουργικά συστήματα που τρέχουν άμεσα τα ίδια λειτουργικά συστήματα με το υλικό. Το ίδιο ισχύει και για τις εφαρμογές που εκτελούνται στο φιλοξενούμενο λειτουργικό σύστημα: εάν ο φορέας ακολουθεί μια πολιτική ασφάλειας για μια εφαρμογή, θα πρέπει να εφαρμόζεται η ίδια ανεξάρτητα από το αν η εφαρμογή εκτελείται σε ένα λειτουργικό σύστημα μέσα σε ένα hypervisor ή σε ένα λειτουργικό σύστημα που εκτελείται σε hardware.

4.6.1 Περιπτώσεις ασφάλειας στο virtualization

Τα προγράμματα που ελέγχουν έναν hypervisor θα πρέπει να ασφαλίζονται με μεθόδους παρόμοιες με αυτές που χρησιμοποιούνται για την προστασία άλλων λογισμικών που τρέχουν σε συνηθισμένους υπολογιστές και servers. Η ασφάλεια ολόκληρης της εικονικής υποδομής βασίζεται στην ασφάλεια του συστήματος διαχείρισης της εικονικοποίησης που ελέγχει τον hypervisor και επιτρέπει στον χειριστή την εκκίνηση ενός φιλοξενούμενου OS, τη δημιουργία νέων επισκεπτών και την εκτέλεση όλων των ενεργειών που επιτρέπονται. Λόγω των επιπτώσεων των εν λόγω δράσεων στην ασφάλεια, η πρόσβαση στο σύστημα διαχείρισης του virtualization θα πρέπει να περιορίζεται μόνο στους εξουσιοδοτημένους διαχειριστές. Μερικά συστήματα διαχείρισης virtualization επιτρέπουν διαφορετικό επίπεδο πρόσβασης σε διαφορετικούς χρήστες, όπως η παροχή πρόσβασης σε ορισμένους χρήστες μόνο για ανάγνωση μέσω της διασύνδεσης ενός φιλοξενούμενου λειτουργικού, ενώ σε άλλους τον έλεγχο των χρηστών πάνω σε συγκεκριμένους πελάτες OS και σε άλλους χρήστες τον πλήρη έλεγχο. Οι περισσότεροι hypervisors λογισμικού προς το παρόν χρησιμοποιούν ως έλεγχο ασφαλείας μόνο τους κωδικούς πρόσβασης για τον έλεγχο πρόσβασης. Αυτή όμως είναι μία πολύ αδύναμη πολιτική ασφαλείας και έτσι ορισμένοι οργανισμοί μπορεί να απαιτούν χρήση ελέγχων αντιστάθμισης, όπως ένα ξεχωριστό σύστημα ελέγχου ταυτότητας που χρησιμοποιείται για τον περιορισμό της πρόσβασης στον κεντρικό υπολογιστή όπου βρίσκεται εγκατεστημένο το σύστημα διαχείρισης του virtualization. Υπάρχουν κάποιοι hypervisors που επιτρέπουν τη διαχείριση με πολλαπλές μεθόδους. Είναι σημαντικό, όμως, κάθε περιβάλλον διαχείρισης ενός hypervisor να παρέχει πρόσβαση τόσο τοπικά όσο και εξ αποστάσεως. Η δυνατότητα για απομακρυσμένη διαχείριση συνήθως μπορεί να ενεργοποιηθεί ή να απενεργοποιηθεί από το σύστημα διαχείρισης του virtualization. Εάν η απομακρυσμένη διαχείριση είναι ενεργοποιημένη σε ένα hypervisor, η πρόσβαση σε όλες τις απομακρυσμένες διεπαφές θα πρέπει να περιορίζεται από ένα τείχος προστασίας. Επίσης, η διαχείριση των επικοινωνιών θα πρέπει να προστατεύεται. Μια επιλογή είναι να διαθέτουν ένα ειδικό δίκτυο διαχείρισης που είναι ξεχωριστό από όλα τα άλλα δίκτυα και είναι προσβάσιμο μόνο από εξουσιοδοτημένους διαχειριστές. Οι επικοινωνίες που πραγματοποιούνται σε μη αξιόπιστα δίκτυα πρέπει να κρυπτογραφούνται με FIPS-εγκεκριμένες μεθόδους, που μπορούν να παρέχονται από το ίδιο το virtualization ή άλλες third-party services, όπως ένα εικονικό ιδιωτικό δίκτυο (VPN) που ενσωματώνει την κίνηση της διαχείρισης.
Επειδή, λόγω του επιπέδου ελέγχου πρόσβασης και τον έλεγχο του guest OS σε έναν hypervisor, ο περιορισμός της πρόσβασης είναι κρίσιμο σημείο για την ασφάλεια του όλου συστήματος. Οι περισσότεροι bare metal hypervisors ελέγχουν την πρόσβαση σε ένα σύστημα. Συνήθως, για την πρόσβαση απαιτείται μόνο το όνομα χρήστη και ο κωδικός πρόσβασης, αλλά μερικοί bare metal hypervisors προσφέρουν επιπλέον στοιχεία ελέγχου, όπως το υλικό token ελέγχου ταυτότητας που επιτρέπει την πρόσβαση στη διεπαφή διαχείρισης του hypervisor. Σε μερικά συστήματα υπάρχουν διαφορετικά επίπεδα ασφάλειας, τα οποία επιτρέπουν σε ορισμένους χρήστες να βλέπουν logs, αλλά δεν είναι σε θέση να αλλάξουν τις ρυθμίσεις ή να αλληλεπιδρούν απευθείας με τον επισκέπτη OS. Αυτά προορίζονται κυρίως μόνο για προβολή λογαριασμών χρηστών που

επιτρέπουν στους ελεγκτές και τους άλλους να έχουν επαρκή πρόσβαση για την κάλυψη των αναγκών τους, χωρίς μείωση της συνολικής ασφάλειας.
Σε αντίθεση με τη λύση bare metal που διαθέτουν διάφορα προϊόντα hosted virtualization, σπάνια εφαρμόζεται έλεγχος πρόσβασης στον hypervisor και οποιοσδήποτε μπορεί να εκκινήσει μια εφαρμογή στο λειτουργικό σύστημα υποδοχής μπορεί να τρέξει τον hypervisor. Ο μόνος έλεγχος πρόσβασης που εφαρμόζεται αφορά το αν μπορεί κάποιος να συνδεθεί στο λειτουργικό σύστημα υποδοχής. Λόγω αυτής της μεγάλης ανισότητας στον τομέα της ασφάλειας, οι οργανισμοί πρέπει να εφαρμόζουν πολιτικές ασφαλείας σχετικά με το ποια OS επισκεπτών μπορούν να εκτελεστούν από τους bare metal hypervisors . Περαιτέρω, οι οργανισμοί μπορούν να τρέξουν bare metal hypervisors, όμως θα πρέπει να ακολουθούν πολιτικές που προσδιορίζουν ποιος μπορεί ή όχι να χρησιμοποιήσει τις λειτουργίες του hypervisor.

Ακολουθούν συστάσεις ασφαλείας για έναν hypervisor:

- Εγκατάσταση όλων των ενημερώσεων στο hypervisor, όπως έχουν τεθεί από τον πωλητή. Οι περισσότεροι hypervisors έχουν χαρακτηριστικά που ελέγχουν για ενημερώσεις αυτόματα και στη συνέχεια κάνουν εγκατάσταση των ενημερώσεων αυτών, όταν βρεθούν. Επίσης, μπορούν να χρησιμοποιηθούν και patches για τη διαχείριση και την εγκατάσταση των ενημερώσεων.
- Περιορισμός της διοικητικής πρόσβασης στη διαχείριση του hypervisor. Προστασία όλων των καναλιών επικοινωνίας με τη διαχείριση ενός ειδικού δικτύου διαχείρισης ή του δικτύου διαχείρισης επικοινωνιών τα οποία πρέπει να είναι επικυρωμένα και να κρυπτογραφούνται με FIPS 140-2.
- Συγχρονισμός της υποδομής virtualization, ώστε ο διακομιστή ώρας να είναι επίσημος και αξιόπιστος.
- Αποσύνδεση του υλικού hardware που δεν χρησιμοποιούμε από το σύστημα υποδοχής. Για παράδειγμα, μια αφαιρούμενη μονάδα δίσκου μπορεί μερικές φορές να χρησιμοποιείται για την δημιουργία αντιγράφων ασφαλείας, αλλά θα πρέπει να αποσυνδέεται όταν δεν χρησιμοποιείται για τη δημιουργία αντιγράφων ασφαλείας ή για επαναφορά. Πρέπει να αποσυνδέουμε τα NIC που δεν χρησιμοποιούμε από οποιοδήποτε δίκτυο.
- Απενεργοποίηση όλων των υπηρεσιών hypervisor, όπως το πρόχειρο ή την ανταλλαγή αρχείων μεταξύ των επισκεπτών OS και του host OS, εκτός αν αυτό είναι απαραίτητο. Κάθε μια από αυτές τις υπηρεσίες μπορεί να είναι ένας πιθανός φορέας επίθεσης. Η κοινή χρήση αρχείων μπορεί επίσης να είναι φορέας μιας επίθεσης σε συστήματα όπου περισσότεροι από ένας guest OS μοιράζεται τον ίδιο φάκελο με το host OS.
- Χρησιμοποίηση της δυνατότητας ενδοσκόπησης για την παρακολούθηση της ασφάλειας σε κάθε φιλοξενούμενο OS. Εάν ένα φιλοξενούμενο λειτουργικό σύστημα βρίσκεται σε κίνδυνο, ο έλεγχος ασφαλείας του μπορεί να απενεργοποιηθεί ή να αναδιαμορφωθεί έτσι ώστε να καταστείλει οποιαδήποτε σημάδια κινδύνου. Εφαρμόζοντας υπηρεσία ασφαλείας στο hypervisor, μπορούμε να παρακολουθούμε την ασφάλεια ακόμη και όταν το φιλοξενούμενο λειτουργικό σύστημα βρίσκεται σε κίνδυνο.
- Χρησιμοποίηση της δυνατότητας ενδοσκόπησης για την παρακολούθηση της ασφάλειας των δραστηριοτήτων που πραγματοποιούνται στους επισκέπτες OS. Αυτό είναι ιδιαίτερα σημαντικό για την επικοινωνία σε ένα non-virtualized περιβάλλον, που πραγματοποιείται πάνω στα δίκτυα και παρακολουθείται από μηχανισμούς ασφάλειας δικτύου (όπως τα firewalls του δικτύου, συσκευές ασφαλείας, και το δίκτυο αισθητήρων IDP).
- Προσεκτική παρακολούθηση του ίδιου του hypervisor για σημάδια επίθεσης, καθώς και παρακολούθηση και ανάλυση, σε συνεχή βάση, των στοιχείων που καταγράφονται σε ένα hypervisor.

Φυσικά, είναι σημαντικό να παρέχουμε ελέγχους φυσικής πρόσβασης για το hardware πάνω στο οποίο τρέχει το σύστημα virtualization. Για παράδειγμα, οι hosted hypervisors συνήθως ελέγχονται από το λογισμικό διαχείρισης και μπορούν να χρησιμοποιηθούν από οποιονδήποτε έχει πρόσβαση στο πληκτρολόγιο και το ποντίκι. Ακόμα, οι bare metal hypervisors απαιτούν φυσική ασφάλεια, δηλαδή κάποιος μπορεί να επανεκκινήσει τον υπολογιστή στον οποίο τρέχει ο hypervisor ή μπορεί να αλλάξει ορισμένες από τις ρυθμίσεις ασφαλείας του hypervisor. Είναι επίσης σημαντικό να διασφαλιστούν οι εξωτερικοί πόροι που χρησιμοποιεί ο hypervisor και ιδίως τα δεδομένα που είναι αποθηκευμένα στους σκληρούς δίσκους και τις άλλες συσκευές αποθήκευσης.
Το hosted virtualization εκθέτει το σύστημα σε πιο πολλές απειλές λόγω της παρουσίας ενός host OS. Για να αυξήσουμε την ασφάλεια του host OS, ελαχιστοποιούμε τον αριθμό των εφαρμογών που τρέχουν στο σύστημα, εκτός από τον hypervisor. Όλες οι «άχρηστες» εφαρμογές θα πρέπει να αφαιρεθούν. Εκείνες που παραμένουν θα πρέπει τις περιορίσουμε όσο το δυνατόν περισσότερο για την αποφυγή εγκατάστασης κακόβουλων προγραμμάτων στο σύστημα. Για παράδειγμα, ένα πρόγραμμα περιήγησης στο Web χρησιμοποιείται συχνά για να κατεβάσουμε ενημερώσεις για τον hypervisor και επίσης για να διαβάσουμε οδηγίες και ενημερωτικά δελτία για το hypervisor. Εάν ο υπολογιστής προορίζεται να χρησιμοποιείται αποκλειστικά για την εκτέλεση του host hypervisor, το πρόγραμμα περιήγησης στο Web θα πρέπει να έχει τις ρυθμίσεις του προσαρμοσμένες στο υψηλότερο επίπεδο ασφαλείας τους.
Επειδή τα συστήματα hosted virtualization λειτουργούν κάτω από το host OS, η ασφάλεια του κάθε φιλοξενούμενου OS βασίζεται στην ασφάλεια του λειτουργικού συστήματος υποδοχής. Αυτό σημαίνει ότι θα πρέπει να υπάρχουν αυστηροί έλεγχοι πρόσβασης στο OS του κεντρικού υπολογιστή για να αποτραπεί κάποιος από το να αποκτήσει πρόσβαση μέσω του host OS στο σύστημα virtualization και ενδεχομένως να μπορέσει να προβεί στην αλλαγή των ρυθμίσεων ή την τροποποίηση του guest OS.
Υπήρξε κάποια ανησυχία στην κοινότητα ασφαλείας για το σχεδιασμό hypervisors έτσι ώστε να μην μπορούν να ανιχνευθούν από τους εισβολείς. Για να επιτευχθεί αυτό, παρέχεται ένα επιπλέον επίπεδο ασφάλειας που είναι αόρατο στον εισβολέα, αποτρέποντας έτσι μια επιτυχή επίθεση εναντίον του hypervisor και του host OS, κάτω από αυτό. Ωστόσο, οι hypervisors έχουν διάφορα χαρακτηριστικά και μηχανισμούς που επιτρέπουν στους επιτιθέμενους να ανιχνεύουν την παρουσία τους. Οι τεχνικές ανίχνευσης περιλαμβάνουν έλεγχο για αντικείμενα στις διαδικασίες, το σύστημα των αρχείων και της μνήμης, έλεγχο για συγκεκριμένες οδηγίες επεξεργαστή ή ικανότητες, και ειδικό έλεγχο για εικονικές συσκευές υλικού. Αυτές οι τεχνικές ανίχνευσης εξαρτώνται από την υλοποίηση του συστήματος που έχει επιλέξει ο οργανισμός. Παρά το γεγονός ότι η ανίχνευση του hypervisor μπορεί να ελαχιστοποιηθεί από κάποιον ειδικό, τροποποιώντας την εφαρμογή hypervisor ή προσπαθώντας να αποκρύψει τα στοιχεία του λογισμικού, όμως δεν είναι δυνατόν να κρύψει εντελώς όλα τα χαρακτηριστικά. Κατά το σχεδιασμό ασφάλειας του virtualization, οι οργανισμοί δεν θα πρέπει να υποθέτουν ότι οι επιτιθέμενοι δεν θα είναι σε θέση να ανιχνεύσουν την παρουσία ενός hypervisor ή τον τύπο του προϊόντος και την έκδοση.

4.6.2 Guest OS Security

Ένα guest OS που εκτελείται σε ένα εικονικό περιβάλλον λειτουργεί σχεδόν όμοια με το λειτουργικό σύστημα που εκτελείται στο hardware. Όλα τα ζητήματα ασφαλείας που ισχύουν για ένα OS που εκτελείται στο hardware ισχύουν και για τα OS των guest. Ωστόσο, υπάρχουν και κάποιες άλλα θέματα σχετικά με την ασφάλεια των guest OS. Για να εκτελέσουμε σε μια virtual machine ένα φιλοξενούμενο λειτουργικό σύστημα πρέπει να χρησιμοποιήσουμε όλο το hardware υλικό που είναι συμβατό με τον hypervisor, όπως η κάρτα γραφικών, η κάρτα ήχου, το πληκτρολόγιο, το ποντίκι και οι οδηγοί δικτύου. Δεν υπάρχουν ειδικά θέματα ασφαλείας για

αυτούς τους οδηγούς, εκτός εάν παρουσιάζουν σφάλματα εξ αρχής, κάτι το οποίο δεν είναι συνηθισμένο σε αυτούς τους οδηγούς.
Το πιο σημαντικό είναι ότι πολλά hosted virtualization συστήματα επιτρέπουν στους guest OS να μοιράζονται πληροφορίες με το λειτουργικό σύστημα υποδοχής μέσω κοινόχρηστων δίσκων ή φακέλων, οι οποίοι φυσικά δημιουργούνται πάνω στο δίκτυο. Σε κάθε περίπτωση, εάν κάποιο guest OS έχει παραβιαστεί από κάποιο κακόβουλο λογισμικό, αυτό μπορεί να εξαπλωθεί μέσω του κοινόχρηστου δίσκου ή φακέλου. Αυτό είναι ένα θέμα ευπάθειας της ασφαλείας που δεν υπάρχει στα «συνηθισμένα» OS, εκτός αν βρίσκονται στο ίδιο δίκτυο. Οι οργανισμοί που εφαρμόζουν πολιτικές ασφαλείας που καλύπτουν το δίκτυο του κοινού χώρου αποθήκευσης θα πρέπει να εφαρμόζουν αυτές τις πολιτικές για τους κοινόχρηστους δίσκους στα συστήματα virtualization.
Επίσης πολλά hosted virtualization συστήματα επιτρέπουν στους guest OS να μοιράζονται πληροφορίες με το λειτουργικό σύστημα υποδοχής, μέσω της ανταλλαγής δεδομένων στο clipboard. Δηλαδή, αντιγραφή πληροφοριών στο πρόχειρο του host OS, το οποίο επιτρέπει αυτές οι πληροφορίες να επικολληθούν στο guest OS και το αντίστροφο. Ομοίως, όταν κάποιος αντιγράφει πληροφορίες από το πρόχειρο σε ένα φιλοξενούμενο λειτουργικό σύστημα, οι ίδιες αυτές πληροφορίες εμφανίζονται και στο πρόχειρο των υπολοίπων guest OS που λειτουργούν στον ίδιο hypervisor. Αυτό είναι ένα πρακτικό χαρακτηριστικό για τους χρήστες, αλλά αποτελεί επίσης ένα βοήθημα για τις επιθέσεις μεταξύ των επισκεπτών OS και του host OS. Εξαιτίας αυτού, οι οργανισμοί πρέπει να εφαρμόζουν συγκεκριμένες πολιτικές σχετικά με τη χρήση των κοινών clipboards.

Ακολουθούν συστάσεις ασφαλείας για το φιλοξενούμενο λειτουργικό σύστημα (guest OS):

- Τήρηση των συνιστώμενων πρακτικών για τη διαχείριση των φυσικών OS, όπως, για παράδειγμα, συγχρονισμό του χρόνου, διαχείριση καταγραφής, ελέγχου ταυτότητας, απομακρυσμένη πρόσβαση κλπ.
- Άμεση εγκατάσταση όλων των ενημερώσεων για το λειτουργικό σύστημα επισκέπτη. Όλα τα σύγχρονα OS διαθέτουν χαρακτηριστικά που ελέγχουν αυτόματα για ενημερώσεις, τις οποίες και εγκαθιστούν.
- Δημιουργία αντιγράφων ασφαλείας των εικονικών συσκευών που χρησιμοποιούνται από το φιλοξενούμενο λειτουργικό σύστημα σε τακτική βάση, χρησιμοποιώντας για τα αντίγραφα ασφαλείας την ίδια πολιτική που χρησιμοποιείται για τους non-virtualized υπολογιστές στον οργανισμό.
- Σε κάθε φιλοξενούμενο OS πρέπει να αποσυνδέσουμε το hardware που δεν χρησιμοποιούμε. Αυτό είναι ιδιαίτερα σημαντικό για τις εικονικές συσκευές (συνήθως τη συσκευή CD και μονάδα δισκέτας) και τους άλλους προσαρμογείς δικτύου, εκτός από την κύρια διασύνδεση του δικτύου και σειριακή ή παράλληλες θύρες.
- Χρησιμοποίηση ξεχωριστών ταυτοτήτων για κάθε guest OS, εκτός εάν υπάρχει ιδιαίτερος λόγος δύο πελάτες του guest OS να μοιράζονται τα διαπιστευτήρια.
- Επιβεβαίωση ότι οι εικονικές συσκευές του guest OS σχετίζονται μόνο με τις κατάλληλες φυσικές συσκευές στο σύστημα host, όπως οι αντιστοιχίσεις μεταξύ φυσικών και εικονικών NIC.

Εάν ένα guest OS σε ένα hosted virtualization σύστημα βρίσκεται σε κίνδυνο, τότε υπάρχει μεγάλη πιθανότητα να μολύνει και τα υπόλοιπα συστήματα στον ίδιο hypervisor. Ο πιθανότερος τρόπος που μπορεί να συμβεί αυτό είναι η κοινή χρήση δίσκων ή clipboards. Εάν αυτή η κατανομή είναι ενεργοποιημένη σε δύο ή περισσότερα guest OS και ένα φιλοξενούμενο λειτουργικό σύστημα βρίσκεται σε κίνδυνο, ο διαχειριστής του συστήματος virtualization πρέπει να αποφασίσει πώς θα αντιμετωπίσει το ενδεχόμενο έκθεσης των υπολοίπων στον κίνδυνο. Δύο είναι οι στρατηγικές για την αντιμετώπιση αυτής της κατάστασης και είναι οι εξής:

- Ας υποθέσουμε ότι όλοι οι guest OS για το ίδιο υλικό έχουν παραβιαστεί. Τότε θα χρειαστεί η επαναφορά κάθε guest OS σε μια γνωστή καλή εικόνα που αποθηκεύτηκε από backup πριν από την παραβίαση.
- Διερεύνηση κάθε guest OS ξεχωριστά για παραβίαση, ακριβώς όπως θα γινόταν κατά τη διάρκεια της κανονικής σάρωσης για κακόβουλο λογισμικό. Αν βρεθεί κάποιο malware, ακολουθούμε τη συνήθη πολιτική ασφάλειας του οργανισμού.

Η πρώτη μέθοδος υποθέτει ότι το guest OS είναι διαφορετικό από το «κανονικό» σύστημα, ενώ η δεύτερη θεωρεί ότι η τρέχουσα πολιτική ασφάλειας του οργανισμού είναι επαρκής και πρέπει να εφαρμόζεται σε όλα τα συστήματα με τον ίδιο τρόπο.

4.6.3 Virtualized Infrastructure Security

Το virtualization προσφέρει προσομοίωση του hardware, όπως η αποθήκευση και το δίκτυο διασυνδέσεων. Η υποδομή αυτή είναι εξίσου σημαντική για την ασφάλεια ενός virtualized guest OS. Πραγματική υποδομή υλικού είναι ένα λειτουργικό σύστημα που εκτελείται σε ένα φυσικό υπολογιστή. Πολλά συστήματα virtualization διαθέτουν τα χαρακτηριστικά γνωρίσματα για να παρέχουν έλεγχο πρόσβασης στο εικονικό hardware, ιδιαίτερα για την αποθήκευση και τη δικτύωση. Η πρόσβαση στο εικονικό υλικό θα πρέπει να περιορίζεται αυστηρά στο guest OS που θα το χρησιμοποιήσει. Για παράδειγμα, αν δύο πελάτες μοιράζονται έναν εικονικό σκληρό δίσκο, μόνο τα δύο αυτά OS θα πρέπει να έχουν πρόσβαση σε αυτόν. Για παράδειγμα, μια εικόνα δίσκου που αντιπροσωπεύει ένα CD εγκατάστασης μπορεί να μοιραστεί μεταξύ πολλών επισκεπτών OS ακόμα και αν η πρόσβαση σε αυτήν την εικόνα θα πρέπει να είναι μόνο για ανάγνωση και καμία εικόνα των guest να μην μπορεί να το αντιγράψει και να το χρησιμοποιήσει περαιτέρω.
Στα συστήματα hypervisor που συνδέουν πολλούς πελάτες μαζί σε ένα εικονικό δίκτυο προκύπτουν ζητήματα όταν πρόκειται για οργανισμούς των οποίων οι πολιτικές απαιτούν ότι όλα τα δίκτυα πρέπει να ελέγχονται. Για παράδειγμα, ένας οργανισμός μπορεί να εφαρμόζει μια πολιτική ασφάλειας των δικτύων που ορίζει ότι όλοι οι διακόπτες του δικτύου που συνδέουν πολλούς διακομιστές, η διοίκηση και η κυκλοφορία μεταξύ των διακομιστών θα πρέπει να παρακολουθούνται για ύποπτη δραστηριότητα. Ωστόσο, οι διακόπτες του δικτύου στα περισσότερα εικονικά συστήματα δεν έχουν τέτοια δυνατότητα. Κάποιοι εικονικοί διακόπτες υποστηρίζουν εικονικό LAN (VLAN) και ικανότητες υποστήριξης firewall και παρέχουν διαχωρισμό και απομόνωση της VM κίνησης του δικτύου. Σε ορισμένα περιβάλλοντα, επιπλέον συσκευές ασφαλείας μπορούν να τοποθετηθούν για την επιθεώρηση, τον έλεγχο και την παρακολούθηση του VM δικτύου επικοινωνιών σε μια κεντρική τοποθεσία.
Οι hypervisors προσφέρουν μερικές φορές εικονικά δίκτυα αποθήκευσης και εικονικές διασυνδέσεις με τα υφιστάμενα δίκτυα αποθήκευσης υλικού. Αυτά τα χαρακτηριστικά παρουσιάζουν τα ίδια προβλήματα ασφάλειας με τα εικονικά δίκτυα, δηλαδή οι οργανισμοί των οποίων η πολιτική ασφαλείας τους απαιτεί την παρακολούθηση αυτών των συνδέσεων δεν μπορεί να χρησιμοποιήσει τις ίδιες μεθόδους για την εικονική αποθήκευση όπως για τη φυσική αποθήκευση. Χρησιμοποιώντας φυσικές διασυνδέσεις στην υπάρχουσα δικτυακή αποθήκευση μπορεί να εξαλειφθεί αυτό το πρόβλημα, αλλά μειώνει εν μέρει την ευελιξία που προσφέρουν οι hypervisors.

4.6.4 Desktop Virtualization Security

Μια σημαντική διαφορά ως προς την ασφάλεια μεταξύ server και desktop virtualization αφορά τη δυνατότητα ελέγχου των εικόνων. Σε ένα περιβάλλον server, η δυνατότητα δημιουργίας και διαχείρισης εικόνων περιορίζεται συνήθως στους διαχειριστές. Αλλά σε περιβάλλον γραφείου, οι τελικοί χρήστες έχουν συχνά τη δυνατότητα να δημιουργήσουν, να τροποποιήσουν και να διαγράψουν εικόνες. Το ίδιο το λογισμικό virtualization μπορεί επίσης να ελέγχεται πλήρως από

το χρήστη. Είναι πιθανόν ένας οργανισμός να μην μπορεί να εξασφαλίσει ότι το guest OS πληροί τις απαιτήσεις ασφάλειας του οργανισμού.
Οι οργανισμοί εξετάζουν τη χρήση του desktop virtualization και στη συνέχεια καθορίζουν τα σενάρια που απαιτούνται για την επιβολή της ασφάλειας και τη διαχείριση του virtualization, και τα σενάρια τα οποία δεν απαιτούν κεντρική διαχείριση. Για παράδειγμα, αν ένας τηλε-εργαζόμενος χρησιμοποιεί το desktop virtualization για την εκτέλεση προγραμμάτων τα οποία η πολιτική ασφάλειας θα του επιτρέψει να τρέχει, λ.χ., κάτω από μια ελαφριά προστασία του υπολογιστή στο σπίτι, τότε το σύστημα αυτό κατά πάσα πιθανότητα δεν χρειάζεται να είναι τόσο αυστηρό στη διαχείριση, σε σχέση με ένα άλλο που έχει πρόσβαση στις εσωτερικές βάσεις δεδομένων ή τις ιστοσελίδες, κάτι το οποίο θα συνεπαγόταν αυστηρότερους ελέγχους ασφαλείας. Επίσης, οι οργανισμοί συχνά διαχειρίζονται εικονικές μηχανές σαν να είναι πραγματικοί υπολογιστές. Μια άλλη επιλογή είναι να τις αντιμετωπίζουν ως συσκευές που λήγουν (ή τίθενται υποχρεωτικά εκτός λειτουργίας) μετά από ένα χρονικό διάστημα και να τις αντικαταθιστούν με πιο up-to-date συσκευές.
Το desktop virtualization μπορεί να χρησιμοποιηθεί για τη βελτίωση της ασφάλειας, παρέχοντας μία καλά προστατευμένη εικόνα guest OS για το περιβάλλον στην επιφάνειας εργασίας. Ένας αριθμός virtualization vendors παρέχει λύσεις που επιτρέπουν στους οργανισμούς να αναπτύξουν ένα διαχειριζόμενο desktop guest OS σε υπολογιστές που δεν μπορούν να διαχειριστούν. Για παράδειγμα, εργαζόμενοι εξ αποστάσεως μπορούν να εγκαταστήσουν ένα hypervisor στον υπολογιστή του σπιτιού τους και μέσω intranet να έχουν πρόσβαση στον οργανισμό μέσα από μια συγκεκριμένη εικόνα guest OS ή πρόσβαση από έναν απομακρυσμένο διακομιστή που θα μπορούσε να προσφέρει μια καθαρή εικόνα κάθε φορά που ένας χρήστης ξεκινά μια περίοδο λειτουργίας απομακρυσμένης πρόσβασης. Ορισμένες λύσεις, ακόμη, επιτρέπουν στους χρήστες να εκκινήσουν τους υπολογιστές στο σπίτι τους από ένα αφαιρούμενο μέσο (π.χ. εξωτερικός σκληρός δίσκος) το οποίο περιέχει εγκατεστημένο έναν hypervisor και μια εικόνα guest OS. Αυτό μπορεί να προσφέρει μια bare metal λύση virtualization που δεν τρέχει το λειτουργικό σύστημα του κεντρικού υπολογιστή στον υπολογιστή που χρησιμοποιεί ο χρήστης στο σπίτι. Τα guest OS ενημερώνονται συχνά, πράγμα που σημαίνει ότι θα πρέπει να καταστρέφονται τα παλιά δεδομένα που είναι μόνο για ανάγνωση των μέσων ενημέρωσης και τα νέα να δημιουργούνται και να διανέμονται. Για το λόγο αυτό, ορισμένες εταιρείες θα έμπαιναν στον πειρασμό να χρησιμοποιήσουν επανεγγράψιμα μέσα αντ' αυτού, αλλά αυτό θα μπορούσε να οδηγήσει σε μέσα ενημέρωσης που έχουν μολυνθεί με κακόβουλο λογισμικό.
Οι οργανισμοί κατά κανόνα κάνουν χρήση τέτοιων λύσεων desktop virtualization για τη μείωση των προβλημάτων ασφαλείας που σχετίζονται με τη σύνδεση μη διαχειριζόμενων συστημάτων σε εσωτερικούς πόρους, καθώς και για να μειώσουν την εξάρτηση από τη διανομή σε υπολογιστές ιδιωτών και να προσπαθήσουν να διασφαλίσουν ότι οι μη διαχειριζόμενοι υπολογιστές πληρούν τις απαιτήσεις ασφαλείας. Για τα δεδομένα και τους πόρους στα οποία ένας επισκέπτης αποκτά πρόσβαση εντός ενός λειτουργικού συστήματος, ο οργανισμός μπορεί να παρέχει κάποια προστασία από απειλές στο host OS, για παράδειγμα με τη δημιουργία ενός VPN για την οργάνωση και την κρυπτογράφηση των αποθηκευμένων δεδομένων. Ωστόσο, δεν μπορεί να παρέχει πλήρη προστασία από τις απειλές στο host OS.
Ένα άλλο πλεονέκτημα της χρήσης του desktop virtualization για τη διαχείριση των εικόνων των guest OS είναι ότι μπορούν να ενημερωθούν από τον οργανισμό ανάλογα με τις ανάγκες, χωρίς να απαιτείται η παρέμβαση του χρήστη. Ωστόσο, η διανομή της εικόνας μπορεί να είναι προβληματική, διότι μια ενιαία εικόνα ενός guest OS μπορεί να είναι πολλά gigabytes σε μέγεθος, γεγονός που καθιστά δύσκολο το κατέβασμα της. Οι οργανισμοί όμως μπορούν να επιλέξουν να μειώσουν τη συχνότητα των τακτικών ενημερώσεων από τη ρύθμιση των παραμέτρων της εικόνας, για να επιδιορθώσουν και να ενημερώσουν τα λειτουργικά συστήματα και τις εφαρμογές τους αυτόματα. Οι οργανισμοί που διαχειρίζονται τα guest OS για πολλαπλούς χρήστες πρέπει επίσης να είναι ιδιαίτερα προσεκτικοί γιατί οι αλλαγές που

γίνονται από έναν χρήστη δεν μεταδίδονται πίσω στην κύρια εικόνα και στη συνέχεια εμφανίζονται στις εικόνες που χρησιμοποιούνται από άλλους χρήστες.
Μια άλλη χρήση του desktop virtualization υποστηρίζει μια εφαρμογή που τρέχει μόνο σε κληρονομικό λειτουργικό σύστημα που δεν μπορεί να ασφαλιστεί κατάλληλα από μόνο του. Στην περίπτωση αυτή, το hypervisor ή το host OS μπορεί να είναι σε θέση να παρακολουθεί τις ενέργειες του guest OS χρησιμοποιώντας διάφορους ελέγχους αντιστάθμισης για να εντοπίσει ότι το κληρονομικό λειτουργικό σύστημα δεν μπορεί να τρέξει. Οι εφαρμογές κληρονομιάς μπορεί να έχουν τρωτά σημεία που ενδέχεται να είναι εκτεθειμένα, αν έχει χορηγηθεί πρόσβαση στο δίκτυο σε αυτές. Επίσης, οι εφαρμογές αυτές (και το OS το οποίο τρέχουν) μπορούν επίσης να είναι πιο επιρρεπείς σε προσβολή λόγω έλλειψης αυστηρών μηχανισμών ελέγχου. Θα μπορούσε να προστεθούν ένα πρόσθετο επίπεδο ταυτοποίησης και ελέγχου, όπως στο επίπεδο host OS. Το virtualization μπορεί επίσης να χρησιμοποιηθεί για την ενίσχυση της επικοινωνίας του δικτύου ως προς την κληρονομιά στις εφαρμογές-επιλογές για την πρόσβαση σε μια εφαρμογή, οι οποίες περιλαμβάνουν την πρόσβαση σε ένα αυτόνομο guest OS μέσω μιας κονσόλας, χρησιμοποιώντας ένα απομακρυσμένο πρωτόκολλο σύνδεσης με το guest OS. Στις περιπτώσεις που η αίτηση κληρονομιάς πρέπει να παρέχει πλήρη πρόσβαση στο δίκτυο, αυτό πρέπει να ληφθεί σοβαρά υπόψη προκειμένου να διασφαλιστεί ότι τα δεδομένα που λαμβάνει δεν είναι κακόβουλα, και επίσης η πολιτική θα πρέπει να προϋποθέτει ότι οι πληροφορίες κρυπτογραφούνται και υπογράφονται.

5. Ανάλυση ασφάλειας Hypervisor

Όσο το Cloud Computing [8] αυξάνει τη δημοτικότητα του σε μεγάλα και οργανωμένα δίκτυα, οι χρήστες και οι διαχειριστές κατευθύνονται προς το live migration προκειμένου να χρησιμοποιήσουν τα οφέλη του διαμοιρασμού των εργασιών και της διαχείρισης που παρέχει. Ωστόσο η ασφάλεια των live virtual machines migration πρέπει να αναλυθεί διεξοδικά.
Χάρη στην πρόσφατη πρόοδο στο virtualization, ο τομέας των Virtual Machines έχει εξελιχθεί σε ένα ευρύ πεδίο για έρευνα και ανάπτυξη.

5.1 Επιθέσεις στο Hypervisor

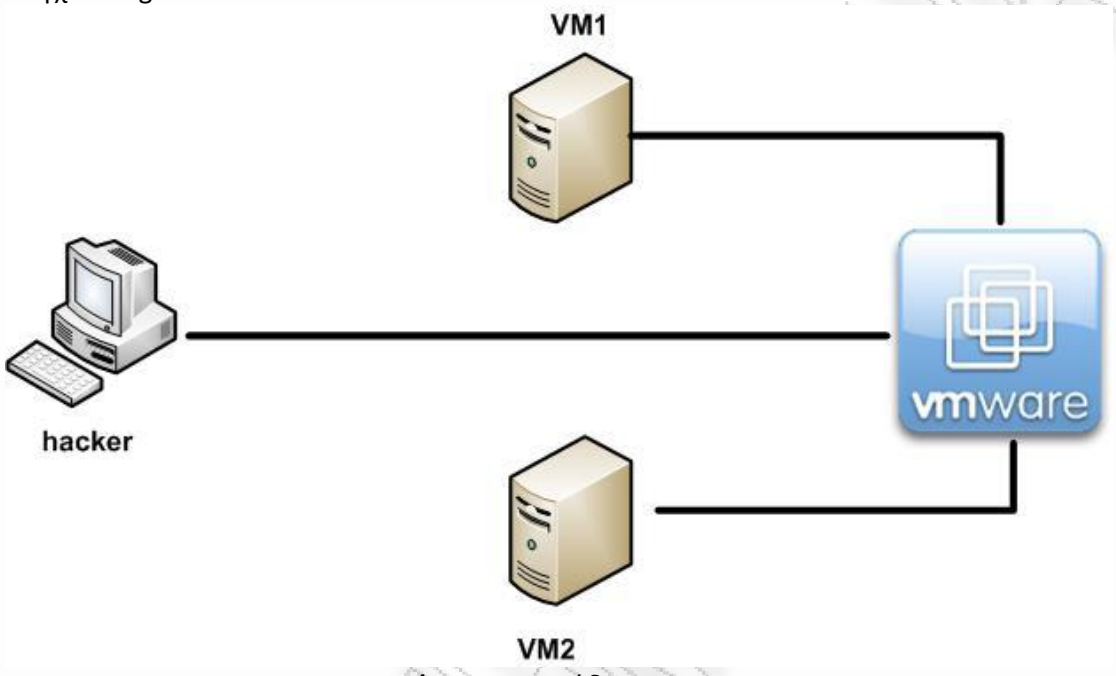
Πετυχημένες οικονομικές επιχειρήσεις όπως το Xen, το VMWare κ.ά. έχουν προωθήσει την υιοθέτηση του virtualization λογισμικού από πολλούς οργανισμούς. Σύμφωνα με στατιστικές μελέτες, ο αριθμός των virtualized servers αυξήθηκε κατά 40 % την πενταετία 2005-2010.
Το live migration των virtual machines, η διαδικασία της μεταφοράς ενός VM από ένα VMM σε ένα άλλο χωρίς καθυστέρηση του guest operating system συνήθως μεταξύ διακριτών φυσικών μηχανών έχουν δημιουργήσει νέες ευκαιρίες στον τομέα του computing. Υποστηριζόμενο από πολλά και διαφορετικά virtualization προϊόντα, το live migration μπορεί να βοηθήσει σε περιπτώσεις όπως: υπηρεσίες υψηλής διαθεσιμότητας, διαφανή φορητότητα, διαμοιρασμό εργασιών και διαχείρισης.
Όσο το virtualization και το live migration ενσωματώνουν σημαντικές νέες λειτουργίες προκύπτουν νέα θέματα ασφάλειας.
Όταν ένα VMM συνεργάζεται με μια όχι ιδιαίτερα ασφαλή live migration λειτουργία υπάρχει περίπτωση έκθεσης τόσο του guest όσο και του host. Το αποτέλεσμα της επίθεσης θα είναι η απώλεια της ακεραιότητας του συστήματος.
Εξαιτίας του μεγάλου και αυξανόμενου πεδίου αγοράς του virtualization, είναι απαραίτητο να γίνει κατανοητή η ανάγκη για ασφάλεια του virtual machine migration. Για το σκοπό αυτό, το συγκεκριμένο κομμάτι ασφάλειας πρέπει να αναλυθεί διεξοδικά. Υπάρχουν 3 περιπτώσεις απειλών για το live migration:

- **Control Plane:** Οι μηχανισμοί επικοινωνίας που διαθέτει το VMM για να διαχειρίζεται το live migration πρέπει να είναι αυθεντικοποιημένοι και ανθεκτικοί στις επιθέσεις. Ο επιτιθέμενος μπορεί να έχει τη δυνατότητα να χειριστεί το control plane ενός virtual machine, να επέμβει στο live migration και να πάρει τον έλεγχο ενός guest operating system.
- **Data Plane:** Το Data Plane μέσα στο virtual machine migration πρέπει να είναι ασφαλές και προστατευμένο από επιθέσεις snooping και tampering στο guest operating system. Πιθανές επιθέσεις στο Data Plane μπορεί να προκαλέσουν διαρροές ευαίσθητων πληροφοριών από το guest operating system και active attacks μπορούν να προκαλέσουν ολοκληρωτική αιχμαλωσία του guest operating system.
- **Migration Module:** Το κομμάτι του VMM που συνεργάζεται με τη λειτουργία του Migration πρέπει να είναι ελαστικό στις επιθέσεις.

Αν ένας επιτιθέμενος μπορεί να υπονομεύει το VMM χρησιμοποιώντας αδυναμίες του Migration Module, τότε μπορεί εύκολα να πάρει τον έλεγχο του VMM και του guest operating system.
Γενικά η τεχνολογία του VMM και του virtualization παρουσιάζουν πολλά τεχνικά και οικονομικά πλεονεκτήματα. Ωστόσο, η παραπάνω τεχνολογία δημιουργεί ένα νέο σύνολο προκλήσεων ασφάλειας.
Στην πραγματικότητα υπάρχουν πλέον νέα σενάρια στον τομέα του virtual environment, όπως η ασφάλεια μεγάλου αριθμού virtual machines, η ασφάλεια μεγάλου αριθμού διαφορετικών λειτουργικών συστημάτων καθώς και η ασφάλεια φορητών virtual machines που βρίσκονται σε διαφορετικές φυσικές θέσεις και διαφορετικά δίκτυα.
Υπάρχουν πολλοί και διαφορετικοί τρόποι με τους οποίους ένα VM μπορεί να μεταφερθεί από ένα VMM σε ένα άλλο. Αφού τα εικονικά συστήματα είναι σε συνηθισμένα αρχεία στους δίσκους, τα αρχεία που είναι συνδεδεμένα με σταματημένα συστήματα μπορούν να αντιγραφούν σε άλλο VMM από το δίκτυο ή από φορητούς δίσκους όπως τα usb.
Επιπλέον, εκτός από το migration σταματημένων συστημάτων, πολλά και δημοφιλή VMM υποστηρίζουν τη λογική του live migration, δηλαδή τη μεταφορά ενός virtual machine από ένα VMM σε ένα άλλο χωρίς το σταμάτημα του guest operating system.
Παρόλο που τα ποικίλης τεχνολογίας VMM χρησιμοποιούν διαφορετικά πρωτόκολλα στα πακέτα δικτύου (καλώδιο), οι αλγόριθμοι που λειτουργούν στο πιο χαμηλό επίπεδο είναι παρόμοιοι.
Για παράδειγμα, οι τεχνικές για live migration αρχίζουν συνήθως αντιγράφοντας σελίδες μνήμης από το VM μέσω δικτύου από το source VMM στο destination, ενώ το VM συνεχίζει να δουλεύει από το source VMM. Η διαδικασία συνεχίζεται όσο το VM επεξεργάζεται τις σελίδες. Όταν το source VMM φτάσει ένα όριο και κρίνει ότι δεν υπάρχει άλλη πρόσθετη ή σημαντική επεξεργασία, τότε στέλνει τις υπόλοιπες σελίδες μνήμης και σταματάει το VM στέλνοντας σήμα στο άλλο VMM (SOURCE) ότι μπορεί να συνεχίσει (resume) την εκτέλεση του VM. Το σημείο αυτό στο οποίο το source VMM στέλνει τις τελευταίες σελίδες και αποφασίζει να στείλει σήμα στο destination VMM είναι πολύ σημαντικό, γιατί το VMM εκείνη τη στιγμή προσπαθεί να διαχειριστεί σωστά και να μειώσει το χρόνο του migration και το downtime του VM. Σε άλλες υλοποιήσεις αναλαμβάνουν το VM κατευθείαν οι destination VMM και ζητάνε στη συνέχεια τις σελίδες μνήμης με αιτήσεις.
Σίγουρα όμως η παραπάνω διαδικασία, που γίνεται μέσω δικτύου, δεν είναι και τόσο ασφαλής. Ουσιαστικά τέτοιες διαδικασίες σε μεγάλους οργανισμούς με τεράστια και διαφορετικά δίκτυα και σε μεγάλες γεωγραφικές αποστάσεις δεν είναι ιδιαίτερα ασφαλή. Βέβαια έχουν γίνει migration σε τόσο μεγάλα δίκτυα με downtime 1-2 seconds. Το συμπέρασμα είναι ότι το live migration μπορεί να δώσει δυνατότητα σε έναν κακόβουλο χρήστη να δει (view) ή να αλλάξει (modify) δεδομένα και να επηρεάσει τις migration υπηρεσίες (services) του source ή του destination VMM.

Παράδειγμα Control Plane

INCOMING MIGRATION CONTROL: Εάν ξεκινήσει μια διαδικασία migration χωρίς εξουσιοδότηση, ο κακόβουλος χρήστης μπορεί να δημιουργήσει ένα migration ενός guest VM στον ίδιο τον υπολογιστή του και έτσι να πάρει ο συγκεκριμένος χρήστης τον ολοκληρωτικό έλεγχο του guest VM.



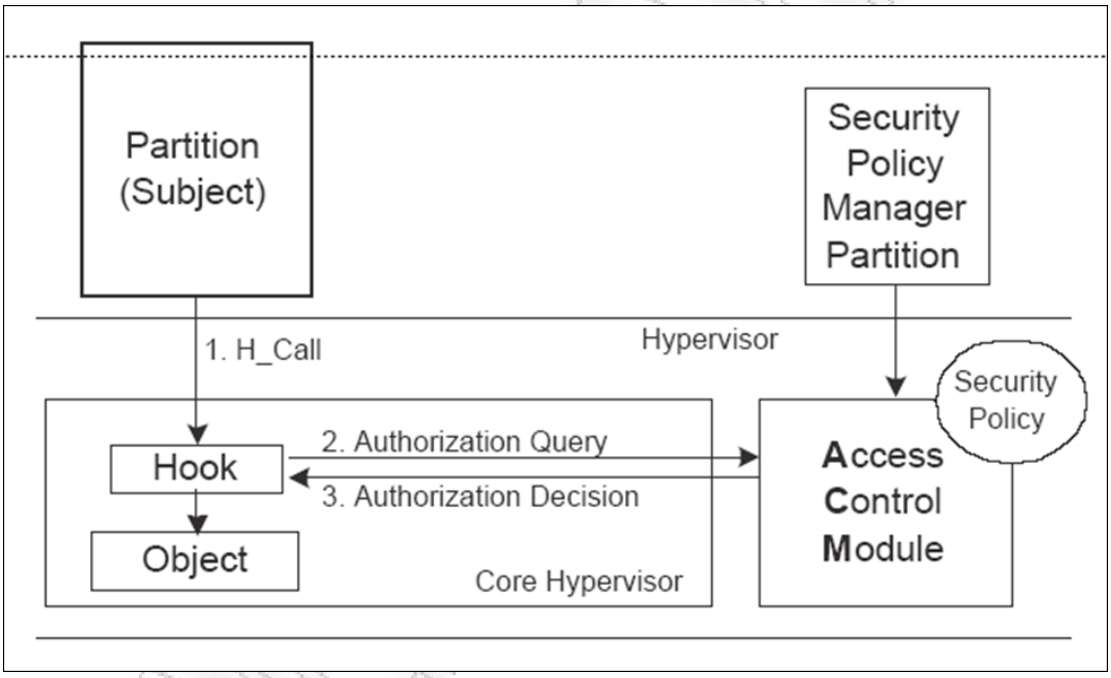
Εικόνα 5.1: Παράδειγμα incoming

OUTCOMING MIGRATION CONTROL: Με την ίδια λογική, ένας κακόβουλος χρήστης μπορεί να δημιουργήσει το migration πολλών VM και αυτό θα οδηγήσει σε διακοπές της λειτουργίας και DOS.

5.2 Η περίπτωση sHype

Η αρχιτεκτονική ασφαλείας του sHype [9] είναι αναμφισβήτητα μία από τις καλύτερες προσεγγίσεις ενός ασφαλούς hypervisor. Το sHype συνδέεται με ένα ερευνητικό πρόγραμμα της IBM και αρχικά αναπτύχθηκε για το IBM rHype, που είναι ένας hypervisor ανοικτού λογισμικού για έρευνα.
Μετά το πρώτο του release, είναι γνωστό και ως Xen [BDF+03] open-source hypervisor. Η μεγάλη επιτυχία του προγράμματος ήταν ότι άνοιξε νέους δρόμους για τη διαχείριση της πληροφορίας που μεταφέρεται μεταξύ των virtual machines. Ωστόσο είναι σημαντικό να διαπιστώσουμε ότι το πρόγραμμα sHype δεν είχε αρχικό σκοπό να διαχειριστεί όλη την πληροφορία μεταξύ των virtual machines αλλά τη ροή συγκεκριμένων πληροφοριών.
Για να διαχειριστούμε την πληροφορία μεταξύ των virtual machines που ονομάζονται logical partitions από τους διαχειριστές του sHype, το sHype χρησιμοποιεί MAC address για να ενδυναμώσει το security policy. Ουσιαστικά το sHype είναι ένα κομμάτι reference monitor, δηλαδή είναι ένα authorization control reference το οποίο διαχειρίζεται subjects και objects. Οποτεδήποτε δηλαδή ένα subject θέλει να προσπελάσει ένα object, ο sHype είναι υπεύθυνος για το deny ή το grant access σύμφωνα με την πολιτική ασφάλειας. Ουσιαστικά οριοθετεί την απόφαση η οποία παίρνεται σε άλλο σημείο του συστήματος.

Η συγκεκριμένη αρχιτεκτονική λέγεται Access Control Module (ACM) και είναι υπεύθυνη για τις αποφάσεις. Χρησιμοποιεί formal security policy με ετικέτες που είναι συνδεδεμένες με subject και object του συστήματος και τον τύπο της διαδικασίας που ένα subject θέλει να εκτελέσει Η λειτουργία αυτή λέγεται Access Control Decision (ACD). Η διαδικασία έχει ως εξής:
Η αίτηση για προσπέλαση από το subject μεταφέρεται στο reference monitor το οποίο με τη σειρά του καλεί το ACM παραθέτοντας ένα Authorization Query (AQ). Το συγκεκριμένο query περιέχει την ετικέτα του subject και του object και τη διαδικασία που το subject θέλει να εκτελέσει (read, write,…).
Σε αυτή τη διαδικασία το reference monitor χρησιμοποιεί τα Enforcement Hooks τα οποία είναι εγκατεστημένα στον hypervisor. Έτσι, όταν ένα subject προσπαθεί να προσπελάσει ένα object, ένα enforcement hook «πυροδοτείται» (triggered) και έτσι καλείται το ACM.
Από τα παραπάνω καταλαβαίνουμε ότι η αρχιτεκτονική sHype είναι πολύ ευέλικτη, εφόσον το ACM εξαρτάται από το reference monitor. Πρακτικά είναι πολύ καλό να διαχωρίζεται το separate policy enforcement από το policy management. Εάν πραγματοποιηθούν αλλαγές στο ACM, το reference monitor παραμένει το ίδιο όσο οι διεπαφές μεταξύ του ACM και του reference monitor μένουν ανέπαφες, το οποίο είναι και το πιο συνηθισμένο. Φυσικά, το ίδιο συμβαίνει και στο ACM εάν το reference monitor αλλάξει.



Εικόνα 5.2: sHype αρχιτεκτονική

Το sHype ορίζει ένα subject σαν ένα Partition (VM), ενώ ένα object είναι μία virtual πηγή, σαν ένας εικονικός δίσκος. Αυτό έχει ως επακόλουθο ότι το sHype ελέγχει μόνο την πρόσβαση των VMs στις εικονικές πηγές. Επίσης, το sHype δεν μπορεί να ελέγξει ποιο πρόγραμμα μέσα σε ένα VM προσπαθεί να αποκτήσει πρόσβαση σε ένα αντικείμενο. Αυτό έχει ως αποτέλεσμα ότι μόνο συγκεκριμένα προγράμματα ή διεργασίες επιτρέπεται να έχουν πρόσβαση σε ένα object, και από μόνο του το VM έχει το δικαίωμα να αλλάξει τους κανόνες.
Για να οριοθετήσουμε και να διαχειριστούμε το πρότυπο πολιτικής ασφάλειας που χρησιμοποιείται από το ACM, οι δημιουργοί του sHype πρότειναν ένα ιδιωτικό virtual machine που λέγεται Security Policy Manager Partition. Η ιδιότητα του συγκεκριμένου virtual machine είναι ότι μπορεί να διαχειριστεί ευκολότερα τις πολιτικές ασφαλείας για τον διαχειριστή και να αποφύγει τα λάθη. Αυτό για παράδειγμα μπορεί να είναι ένα πρόγραμμα που παρέχει στον administrator μία έτοιμη φόρμα-μάσκα που θα του δίνει τη δυνατότητα να δημιουργεί

πολιτικές ασφάλειας εύκολα και γρήγορα. Στη συνέχεια τα συγκεκριμένα policies θα μπορούν αυτόματα να αναγνωρίζονται και να μεταφέρονται στο ACM.
Αφού το sHype έχει τη δυνατότητα να δημιουργεί και να χρησιμοποιεί formal πολιτικές ασφάλειας μπορεί να υποστηρίξει οποιοδήποτε μοντέλο ασφάλειας. Ήδη η αρχιτεκτονική sHype υποστηρίζει πολλά formal security μοντέλα όπως τα Bell-La Padula, Biba, και Chinese Wall.
Ωστόσο, η συγκεκριμένη αρχιτεκτονική παρουσιάζει ακόμα προβλήματα, τα οποία είναι ωστόσο μακριά από το συγκεκριμένο σκοπό του sHype project.

6. Εφαρμογή πληροφοριών στο Εθνικό Τυπογραφείο

Το Εθνικό Τυπογραφείο [10] λειτουργεί με τη νομική μορφή του ενιαίου διοικητικού τομέα του Υπουργείου Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης, του οποίου προΐσταται μετακλητός Ειδικός Γραμματέας, και υπάγεται απευθείας στις αρμοδιότητες του Υπουργού.

6.1 Αρμοδιότητες

Το Εθνικό Τυπογραφείο είναι τεχνική παραγωγική μονάδα γραφικών τεχνών και η γενική του αρμοδιότητα συνίσταται στην έκδοση και κυκλοφορία της Εφημερίδας της Κυβερνήσεως καθώς και στην κάλυψη των εκτυπωτικών αναγκών των Δημοσίων Υπηρεσιών. Ειδικότερα είναι αρμόδιο για:

- Την παραγωγή και κυκλοφορία της Εφημερίδας της Κυβερνήσεως.
- Την παραγωγή των κειμένων της νομοθετικής λειτουργίας.
- Την εκτύπωση γενικού τύπου εντύπων που χρησιμοποιούνται από τις Δημόσιες Υπηρεσίες.
- Την παραγωγή εντύπων και εκδόσεων που ζητούνται από τους αρμόδιους Υπουργούς για την εξυπηρέτηση των αναγκών των Υπουργείων ή Υπηρεσιών που εποπτεύουν.
- Την εκτύπωση και βιβλιοδεσία του Διαρκούς Κώδικα Νομοθεσίας.
- Την παραγωγή εκδόσεων διδακτικού ή εκπαιδευτικού χαρακτήρα.
- Την επιμέλεια και παραγωγή εκδόσεων που κρίνεται ότι εξυπηρετούν εθνικούς σκοπούς ή κοινωνικούς σκοπούς.
- Την παραγωγή εκδόσεων που καθορίζονται σύμφωνα με τις διατάξεις του άρθρου 13 του Ν. 1943/1991.
- Τη διάθεση ΦΕΚ στις Νομαρχίες σε εφαρμογή του Ν. 2225/1994 και 2266/1994.

6.2 Τμήμα Πληροφοριών Εθνικού Τυπογραφείου

Από το Τμήμα Πληροφοριών του Εθνικού Τυπογραφείου οι πολίτες μπορούν να πάρουν πληροφορίες για τα δημοσιεύματα όλων των Φ.Ε.Κ. Συγκεκριμένα μπορούν μέσω τηλεφωνικού κέντρου ή από το γκισέ του τμήματος (Καποδιστρίου 34, Ισόγειο, Γραφείο 3) να ενημερωθούν για οποιοδήποτε δημοσίευμα τους ενδιαφέρει μέσω του ολοκληρωμένου Πληροφοριακού Συστήματος ή μέσω της συγκεκριμένης εφαρμογής πληροφοριών που θα αναλύσουμε παρακάτω.

6.3 Εφαρμογή Πληροφοριών Εθνικού Τυπογραφείου

Η συγκεκριμένη εφαρμογή είχε αναπτυχθεί αρχικά σε περιβάλλον Microsoft Visual Studio 2005, στη συνέχεια σε Microsoft Visual Studio 2008 και τώρα υποστηρίζεται σε περιβάλλον Microsoft Visual Studio Ultimate 2010.

Η εφαρμογή περιλαμβάνει εξειδικευμένες φόρμες αναζητήσεων εταιρειών, πρωτοκόλλων, Φ.Ε.Κ., Νόμων – Προεδρικών Διαταγμάτων, Φορέων και ειδικές αναζητήσεις. Συνδέεται δυναμικά με την κεντρική βάση δεδομένων του Εθνικού Τυπογραφείου που υποστηρίζεται από την πλατφόρμα Microsoft SQLServer 2000 Enterprise Edition. Τα εκτυπωτικά της εφαρμογής γίνονται κατευθείαν από τις φόρμες της εφαρμογής χωρίς την ανάγκη χρήσης reporting services.
Το performance της εφαρμογής έχει προσεχθεί ιδιαίτερα, με ειδικά indexes για τα queries και σωστή παραμετροποίηση των switches του δικτύου για την επικοινωνία των servers που εμπλέκονται. Γενικά, όλες οι απαιτήσεις της εφαρμογής έχουν απόκριση σε σωστό και γρήγορο χρόνο.

6.4 Υλικό υλοποίησης της εφαρμογής σε Cloud Computing

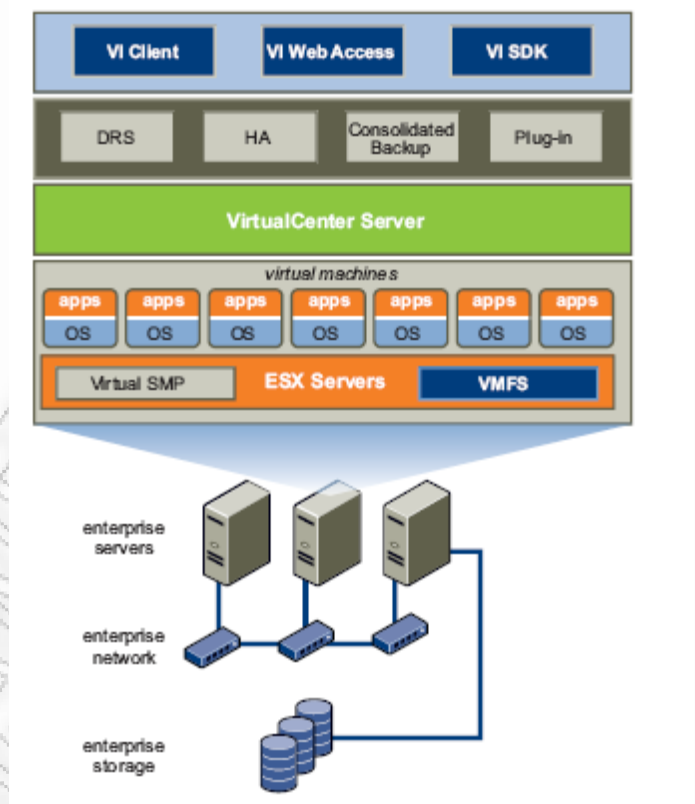
Το Εθνικό Τυπογραφείο διαθέτει στις εγκαταστάσεις του μια συστοιχία IBM Blade Center v και χρησιμοποιεί πλατφόρμα VMWARE ESXi 4.1.0.
Σε ένα server τις συγκεκριμένης συστοιχίας έχει γίνει εγκατάσταση WINDOWS SERVER 2008 R2 Standard και MSSQLSERVER 2008 Express Edition σε ένα Virtual Machine με όνομα VMSQL, και στον ίδιο SERVER σε άλλο Virtual Machine εγκατάσταση WINDOWS SERVER 2008 R2 Standard με όνομα VMPDF για file service (τα pdf των Φ.Ε.Κ.).
Σε αυτά τα δύο Virtual Machines θα «τρέξει» η εφαρμογή των Πληροφοριών με διαφορετικές υλοποιήσεις σε κομμάτια κώδικα, ρόλων και ασφάλειας της εφαρμογής στο νέο Internal Cloud Computing περιβάλλον.

7. VMware ESXi υποδομή

Η υποδομή VMware [11] είναι μια πλήρης virtualization ακολουθία υποδομής που παρέχει περιεκτικό virtualization για τη διαχείριση και τη βελτιστοποίηση των πόρων, τη διαθεσιμότητα εφαρμογής και τις λειτουργικές ικανότητες αυτοματοποίησης σε ένα πλήρες πακέτο.
Η υποδομή VMware εικονικοποιεί και αθροίζει όλους τους ελλοχεύοντες φυσικούς πόρους υλικού μέσα σε πολλαπλά συστήματα και παρέχει τις δεξαμενές των εικονικών πόρων στο datacenter μέσα στο εικονικό περιβάλλον.
Η υποδομή VMware επιφέρει ένα σύνολο διανεμημένων υπηρεσιών που επιτρέπει την κατανομή των πολιτικών προσανατολισμένη προς την υψηλή διαθεσιμότητα τον πόρων, fine-grain αρχιτεκτονικές, και ολοκληρωτικά παγιωμένο backup που θα είναι το θεμέλιο όλου του εικονικού datacenter.
Αυτές οι διανεμημένες υπηρεσίες επιτρέπουν σε εταιρείες – οργανισμούς να συνάψουν και να ολοκληρώσουν συμφωνίες παραγωγής με πελάτες κατά τρόπο οικονομικώς αποδοτικό.

7.1 Αναλυτική παρουσίαση της υποδομής VMware

Οι σχέσεις μεταξύ των διάφορων συστατικών της υποδομής VMware παρουσιάζονται στο παρακάτω σχήμα:



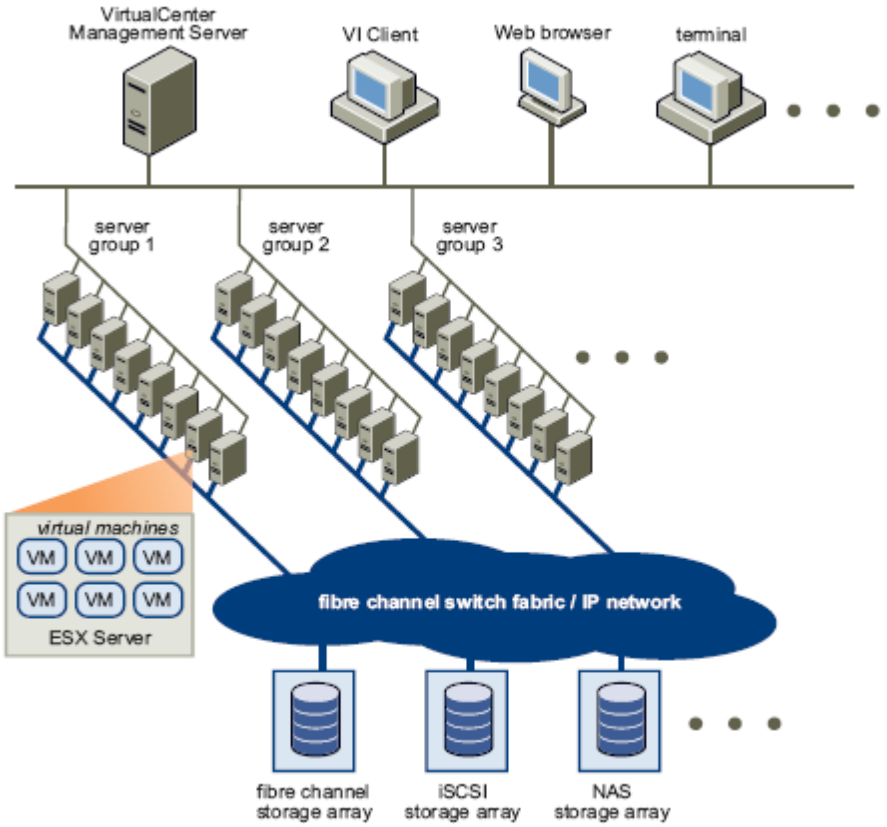
Εικόνα 7.1: Υποδομή VMware

- VMware ESX Server: Πρόκειται για ένα ανθεκτικό virtualization στρώμα παραγωγής που εκτελείται επάνω σε φυσικούς κεντρικούς υπολογιστές και αφηρημένα διαμοιράζει τον επεξεργαστή, τη μνήμη, την αποθήκευση, και τους πόρους δικτύωσης στα διαφορετικά μηχανήματα εικονικής πραγματικότητας.
- VirtualCenter Server: Το κεντρικό σημείο για τη διαμόρφωση, την παραμετροποίηση και τη διαχείριση των virtualized μηχανών.

- VMware Infrastructure Client (VI Client): Μια διεπαφή που επιτρέπει στους χρήστες να συνδέονται απομακρυσμένα με τον κεντρικό υπολογιστή VirtualCenter ή τους μεμονωμένους κεντρικούς υπολογιστές ESX από οποιοδήποτε PC με Windows.
- VMware Infrastructure Web Access (VI Web Access): Μια διεπαφή Ιστού που επιτρέπει τη διαχείριση και την πρόσβαση μηχανημάτων εικονικής πραγματικότητας στις απομακρυσμένες κονσόλες.
- VMware Virtual Machine File System (VMFS): Ένα υψηλής απόδοσης σύστημα cluster file για τα ESX Server virtual machines.
- VMware Virtual Symmetric Multi-Processing (SMP): Ένα χαρακτηριστικό γνώρισμα που επιτρέπει στο ενιαίο μηχάνημα εικονικής πραγματικότητας να χρησιμοποιήσει τους πολλαπλούς φυσικούς επεξεργαστές ταυτόχρονα.
- VMware VMotion and VMware Storage VMotion: Το VMware VMotion επιτρέπει το live migration των μηχανημάτων εικονικής πραγματικότητας από έναν φυσικό κεντρικό υπολογιστή σε έναν άλλο σε μηδέν χρόνο, με συνεχή διαθεσιμότητα υπηρεσιών και πλήρη ακεραιότητα συναλλαγής.
- VMware High Availability (HA): Ένα χαρακτηριστικό γνώρισμα που παρέχει εύκολη στη χρήση, χαμηλού κόστους υψηλή διαθεσιμότητα για τις εφαρμογές που τρέχουν στα μηχανήματα εικονικής πραγματικότητας. Σε περίπτωση αποτυχίας κεντρικών υπολογιστών, τα μηχανήματα εικονικής πραγματικότητας που έχουν επηρεαστεί ξαναξεκινούν αυτόματα σε άλλους εφεδρικούς κεντρικούς υπολογιστές παραγωγής.
- VMware Distributed Resource Scheduler (DRS): Συγκεντρώνει και ισορροπεί δυναμικά την ικανότητα υπολογισμού μεταξύ συλλογών από Hardware Resources σε virtual machines. Αυτό το χαρακτηριστικό γνώρισμα περιλαμβάνει τη διανεμημένη διαχείριση της ισχύος, ικανότητα που επιτρέπει σε ένα datacenter να μειώσει σημαντικά την κατανάλωση ισχύος.
- VMware Consolidated Backup (Consolidated Backup): Χαρακτηριστικό γνώρισμα που παρέχει ευκολία στη χρήση και δυνατότητα για free agent backup των μηχανημάτων εικονικής πραγματικότητας. Απλοποιεί το backup administration και μειώνει το φορτίο στους κεντρικούς υπολογιστές ESX.
- VMware Infrastructure SDK: Χαρακτηριστικό γνώρισμα που παρέχει μια τυποποιημένη διεπαφή για VMware και third-party solutions για να έχει πρόσβαση στην υποδομή VMware.

7.2 Φυσική τοπολογία ενός VI DataCenter

Στο παρακάτω σχήμα φαίνεται μια χαρακτηριστική υποδομή VMware datacenter. Αποτελείται από βασικές φυσικές δομικές μονάδες, όπως τους x86 κεντρικούς υπολογιστές υπολογισμού, τα δίκτυα και τις σειρές αποθήκευσης, τα δίκτυα IP, έναν διοικητικό κεντρικό υπολογιστή και τους πελάτες υπολογιστών γραφείου.



Εικόνα 7.2: VI DataCenter

7.3 Περιγραφή ενός VI DataCenter

Κάθε στοιχείο ενός VI DataCenter αναλύεται διεξοδικά στις παρακάτω παραγράφους.

7.3.1 Κεντρικοί υπολογιστές υπολογισμού

Οι κεντρικοί υπολογιστές υπολογισμού είναι υπολογιστές x86 τεχνολογίας που τρέχουν τον κεντρικό υπολογιστή VMware ESX σε bare metal. Το ESX Server software παρέχει τους πόρους και «τρέχει» τα virtual machines.
Κάθε κεντρικός υπολογιστής υπολογισμού αναφέρεται ως standalone host στο εικονικό περιβάλλον. Διάφοροι ομοίως διαμορφωμένοι x86 κεντρικοί υπολογιστές μπορούν να ομαδοποιηθούν μαζί με τις συνδέσεις στα ίδια υποσυστήματα δικτύων και αποθήκευση,ς για να παρέχουν ένα εννιαίο σύνολο πόρων στο εικονικό περιβάλλον, αποκαλούμενο συστάδα (cluster).

7.3.2 Storage Networks and Arrays

Οι Fiber Channel SAN arrays, iSCSI SAN arrays, και NAS arrays είναι πλατιά διαδεδομένες τεχνολογίες storage που υποστηρίζονται από το VMware Infrastructure για να μπορεί να υποστηρίζει διαφορετικές ανάγκες datacenter storage. Διαμοιράζοντας τα storage arrays μεταξύ ομάδων servers μέσω storage area networks συγκεντρώνει τα storage resources και παρέχει μεγαλύτερη ευελιξία για τη συνεργασία τους με τα virtual machines.

7.3.3 IP Networks

Κάθε computing server διαθέτει πολλαπλά Ethernet network interface cards (NICs), για να μπορεί να παρέχει μεγάλο bandwidth και αξιόπιστο networking σε ολόκληρο το datacenter.

7.3.4 VirtualCenter Server

Ο κεντρικός υπολογιστής VirtualCenter παρέχει ένα κατάλληλο ενιαίο σημείο ελέγχου στο datacenter. Παρέχει πολλές ουσιαστικές υπηρεσίες datacenter, όπως έλεγχο προσπέλασης, έλεγχο της απόδοσης και διαμόρφωση. Ενοποιεί τους πόρους των μεμονωμένων κεντρικών υπολογιστών υπολογισμού τους οποίους μοιράζονται τα μηχανήματα εικονικής πραγματικότητας σε ολόκληρο datacenter. Αυτό ολοκληρώνεται με τη διαχείριση της ανάθεσης των μηχανημάτων εικονικής πραγματικότητας στους κεντρικούς υπολογιστές υπολογισμού και της ανάθεσης των πόρων στα μηχανήματα εικονικής πραγματικότητας μέσα σε έναν δεδομένο κεντρικό υπολογιστή υπολογισμού βασισμένο στις πολιτικές που τίθενται από τον administrator.
Οι κεντρικοί υπολογιστές υπολογισμού θα συνεχίσουν να λειτουργούν ακόμη και στο απίθανο ενδεχόμενο που ο κεντρικός υπολογιστής VirtualCenter γίνει απρόσιτος (παραδείγματος χάριν, το δίκτυο χωρίζεται). Αφού ο κεντρικός υπολογιστής VirtualCenter γίνει προσιτός, μπορεί να διαχειριστεί το datacenter συνολικά και πάλι.

7.3.5 Desktop Clients

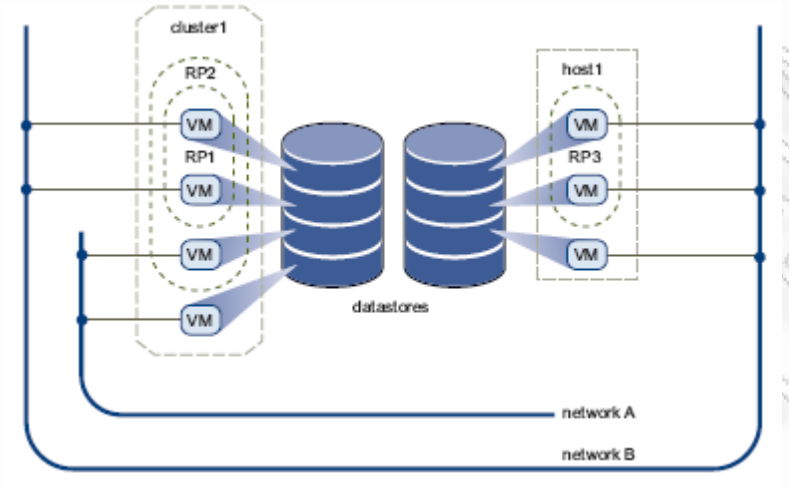
Η υποδομή VMware παρέχει τη δυνατότητα επιλογής των διεπαφών για τη διαχείριση datacenter και την πρόσβαση μηχανημάτων εικονικής πραγματικότητας. Οι χρήστες μπορούν να επιλέξουν τη διεπαφή που ικανοποιεί καλύτερα τις ανάγκες τους:
Πελάτης υποδομής VMware (VI πελάτης), πρόσβαση Ιστού μέσω μιας μηχανής αναζήτησης Ιστού ή των τελικών υπηρεσιών (όπως οι τελικές υπηρεσίες windows).

7.3.6 Virtual Datacenter Architecture

Η υποδομή VMware «εικονικοποιεί» ολόκληρη την υποδομή Τεχνολογιών Πληροφορικής συμπεριλαμβανομένων των κεντρικών υπολογιστών, της αποθήκευσης και των δικτύων. Αθροίζει αυτούς τους ετερογενείς πόρους και παρουσιάζει ένα απλό και ομοιόμορφο σύνολο στοιχείων στο εικονικό περιβάλλον. Με την υποδομή VMware, μπορούμε να διαχειριστούμε τους πόρους Τεχνολογιών Πληροφορικής σαν ένα δυναμικό shared utility στις διαφορετικές εμπορικές μονάδες και τα προγράμματα χωρίς να ανησυχούμε για τις ελλοχεύουσες διαφορές και τους περιορισμούς υλικού.
Το παρακάτω σχήμα δείχνει τα βασικά σημεία ενός virtual datacenter. Μπορούμε να δούμε, να ρυθμίσουμε και να διαχειριστούμε αυτά τα στοιχεία χρησιμοποιώντας τον VirtualCenter Server. Αυτά τα βασικά στοιχεία περιλαμβάνουν:

- Computing and memory resources called hosts, clusters, and resource pools
- Storage resources called datastores
- Networking resources called networks
- Virtual machines

Virtual Datacenter Αρχιτεκτονική:



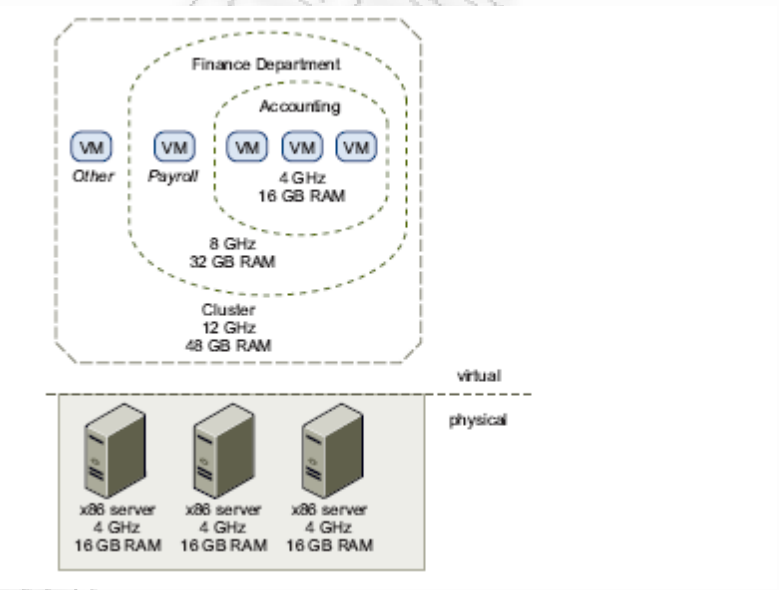
Εικόνα 7.3.6: Virtual datacenter

Ένας host είναι ουσιαστικά η εικονική αναπαράσταση των πόρων CPU και μνήμης μιας φυσικής μηχανής που τρέχει τον κεντρικό υπολογιστή ESX. Όταν μια ή περισσότερες φυσικές μηχανές συγκεντρώνονται για να λειτουργήσουν και να ρυθμιστούν συνολικά, οι συνολικοί πόροι υπολογισμού και μνήμης διαμορφώνουν μια συστάδα (cluster).
Οι μηχανές μπορούν να προστεθούν και να αφαιρεθούν δυναμικά από μια συστάδα (cluster). Οι πόροι CPU και μνήμης από τους οικοδεσπότες και τις συστάδες μπορούν να χωριστούν σε μια ιεραρχία από resource pools.
Τα datastores είναι ουσιαστικά εικονικές αναπαραστάσεις των συνδυασμών των φυσικών πόρων αποθήκευσης στο datacenter. Αυτοί οι φυσικοί πόροι αποθήκευσης μπορούν να προέλθουν από τους τοπικούς δίσκους SCSI, SAS ή SATA του κεντρικού υπολογιστή, τις σειρές δίσκων καναλιών SAN και σειρές δίσκων iSCSI SAN ή συνημμένες στο δίκτυο σειρές αποθήκευσης (NAS).
Τα δίκτυα στο εικονικό περιβάλλον συνδέουν τα μηχανήματα εικονικής πραγματικότητας το ένα με το άλλο ή με το φυσικό δίκτυο έξω από το εικονικό datacenter.
Τα virtual machines σχεδιάζονται για ένα συγκεκριμένο host, cluster ή resource pool και datastore όταν δημιουργούνται. Το virtual machine συμπεριφέρεται σαν μια κανονική ηλεκτρική συσκευή που καταναλώνει ρεύμα.
Αφού τροφοδοτηθούν με ενέργεια καταναλώνουν τους πόρους δυναμικά, αυξάνοντάς τους όταν μεγαλώνει το workload και μειώνοντάς τους όταν το workload μειώνεται.
Η παροχή virtual machines είναι πολύ γρηγορότερη και ευκολότερη από τις φυσικές μηχανές.
Τα νέα virtual machines μπορούν να δημιουργηθούν σε δευτερόλεπτα.
Όταν ένα virtual machine είναι “on power”, το λειτουργικό σύστημα και οι εφαρμογές μπορούν να εγκατασταθούν χωρίς καμία αλλαγή για να υποστηρίξουν ένα συγκεκριμένο φόρτο εργασίας σαν να ήταν εγκατεστημένα σε ένα κανονικό φυσικό μηχάνημα. Επίσης υπάρχει η δυνατότητα κατά την παροχή το λειτουργικό σύστημα και οι εφαρμογές να είναι ήδη εγκατεστημένες και παραμετροποιημένες.
Οι πόροι στα virtual machines είναι βασισμένοι στις πολιτικές που τίθενται από τον administrator που κατέχει τους πόρους. Οι πολιτικές μπορούν να διατηρήσουν ένα σύνολο πόρων για ένα συγκεκριμένο virtual machine και να εγγυηθούν για την απόδοσή του. Οι πολιτικές μπορούν επίσης να δώσουν προτεραιότητα και να θέσουν μια μεταβλητή μερίδα των συνολικών πόρων σε κάθε virtual machine.

Σε ένα virtual machine θα αποτραπεί να γίνει power-on εάν υπάρχουν συγκεκριμένες πολιτικές ενέργειας.

7.3.7 Hosts, Clusters, and Resource Pools

Οι hosts, τα clusters και τα resource pools παρέχουν ευέλικτους και δυναμικούς τρόπους για την οργάνωση των συνολικών πόρων CPU και μνήμης στο εικονικό περιβάλλον και για τη σύνδεσή τους με τους φυσικούς πόρους. Ένας host αντιπροσωπεύει τους συνολικούς πόρους CPU και μνήμης ενός φυσικού x86 κεντρικού υπολογιστή. Για παράδειγμα εάν ο φυσικός x86 κεντρικός υπολογιστής έχει τέσσερα διπλοπυρήνα CPU που τρέχουν στα 4 gigahertz και 32 gigabytes μνήμης, οι host θα έχουν 32 gigahertz CPU και 32 gigabytes μνήμης διαθέσιμων για τα virtual machines. Ένα cluster συμπεριφέρεται και το διαχειριζόμαστε σαν ένα host. Αντιπροσωπεύει το σύνολο των πόρων CPU και μνήμης μιας ομάδας φυσικών x86 κεντρικών υπολογιστών που μοιράζεται τις ίδιες σειρές δικτύων και αποθήκευσης. Παραδείγματος χάριν, εάν η ομάδα περιέχει οκτώ κεντρικούς υπολογιστές, κάθε κεντρικός υπολογιστής έχει τέσσερα διπλοπύρηνα CPU που τρέχουν στα 4 gigahertz και σε 32 gigabytes μνήμης.
Για παράδειγμα: Έστω ότι ένα group περιέχει οκτώ κεντρικούς υπολογιστές. Καθένας κεντρικός υπολογιστής έχει τέσσερα διπλοπύρηνα CPU που τρέχουν στα 4 gigahertz και σε 32 gigabytes μνήμης. Το cluster θα έχει έπειτα 256 gigahertz CPU και 256 gigabytes της μνήμης διαθέσιμων για τα virtual machines που θα δώσει.
Τα resource pools είναι partitions από CPU και memory resources από ένα host ή ένα cluster. Οποιοδήποτε resource pool μπορεί να χωριστεί σε μικρότερα resource pools για μεγαλύτερη υποδιαίρεση και να οριστούν resources σε διαφορετικά groups για διαφορετικούς λόγους. Με άλλα λόγια τα resource pools μπορούν να είναι τοποθετημένα ιεραρχικά.
Ένα σχήμα από resource pools φαίνεται παρακάτω:



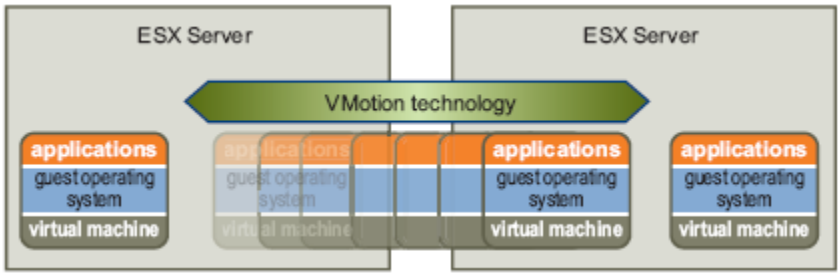
Εικόνα 7.3.7: Resource Pools

Στο παραπάνω σχήμα παρουσιάζεται η χρησιμότητα των resource pools. Τρείς κεντρικοί υπολογιστές x86 με 4GHZ CPU και 16GB RAM δημιουργούν ένα cluster με 48 GB RAM και 12 GHZ CPU.

Ένα A resource pool («Finance Department») χρησιμοποιεί 8 gigahertz από τη δύναμη της CPU και 32 gigabytes από τη μνήμη του cluster αφήνοντας 4 gigahertz CPU και 16 gigabytes μνήμη (reserved) για το virtual machine «Others».
Τα resources που είναι δεσμευμένα μπορούν να αλλάξουν δυναμικά. Για παράδειγμα, αν ένα χρόνο αργότερα το «Accounting» περιβάλλον εργασίας αυξάνεται και θέλουμε να αυξήσουμε το resource pool «Accounting» από τη δέσμευση 4 gigahertz της CPU σε 6 gigahertz , μπορούμε να κάνουμε αυτή την αλλαγή στο resource pool δυναμικά χωρίς να χρειαστεί να σβήσουμε κάποιο από τα δεσμευμένα virtual machines. Τα resources που δεσμεύονται για resource pool ή για virtual machine δεν γίνονται αστραπιαία. Γίνονται ανάλογα με τη ζήτηση δυναμικά.
Δηλαδή αν τα 4 gigahertz από CPU που είναι δεσμευμένα για το «Accounting» δεν χρησιμοποιούνται, το virtual machine «Payroll» μπορεί να χρησιμοποιήσει αυτά τα gigahertz κατά τη διάρκεια μεγάλης ανάγκης του. Όταν το «Accounting» τα χρειαστεί ξανά τότε το «Payroll» θα τα δώσει πίσω δυναμικά. Το αποτέλεσμα είναι ότι resources τα οποία έχουν δεσμευτεί σε διαφορετικά resource pools δεν χάνονται αλλά σπαταλούνται αλλού αν δεν τα χρησιμοποιεί ο ιδιοκτήτης τους.
Το τελικό συμπέρασμα είναι ότι τα resource pools μπορούν να οργανωθούν ιεραρχικά και να παραμετροποιηθούν εκ νέου δυναμικά έτσι ώστε το ηλεκτρονικό περιβάλλον να είναι περίπου ίδιο με την οργάνωση της εταιρείας. Μεμονωμένες μονάδες εργασίας μπορούν να χρησιμοποιούν συγκεκριμένες υποδομές, ενώ παράλληλα απολαμβάνουν τα οφέλη της αποδοτικότητας από τη συγκέντρωση των πόρων.

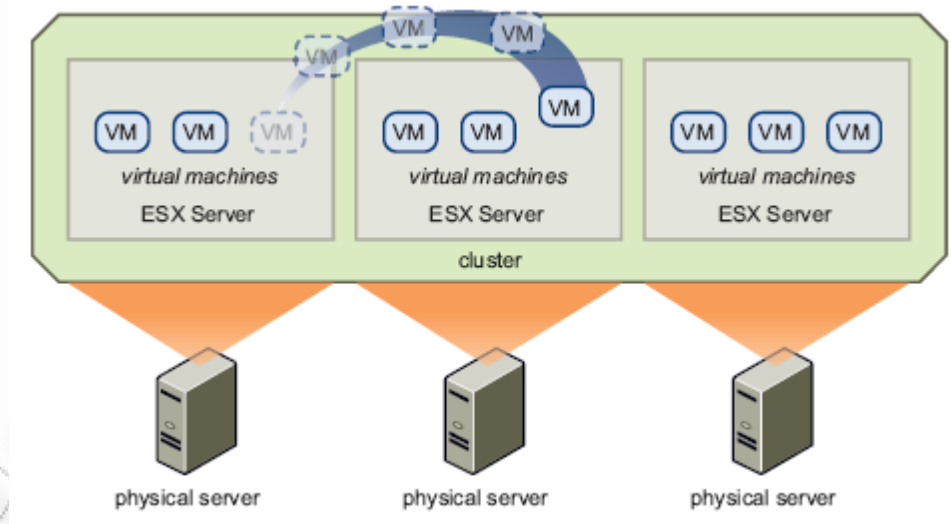
7.3.8 VMware Infrastructure Distributed Services

Τα VMware VMotion, VMware Storage VMotion, VMware DRS, and VMware HA είναι διανεμημένες υπηρεσίες που επιτρέπουν την αποδοτική και αυτοματοποιημένη διαχείριση των πόρων και την υψηλή διαθεσιμότητα των virtual machines.
Τα virtual machines τρέχουν και καταναλώνουν τους πόρους του κεντρικού υπολογιστή ESX. Το VMotion επιτρέπει τη μετανάστευση του τρεξίματος των virtual machines από έναν φυσικό κεντρικό υπολογιστή σε έναν άλλον χωρίς διακοπή υπηρεσιών, όπως φαίνεται στο παρακάτω σχήμα. Αυτό επιτρέπει στα virtual machines να κινηθούν από έναν βαριά φορτωμένο κεντρικό υπολογιστή προς έναν ελαφρά φορτωμένο. Το αποτέλεσμα είναι η αποδοτικότερη ανάθεση των πόρων. Με το VMotion, οι πόροι μπορούν να αναδιανεμηθούν δυναμικά στα virtual machines και στους φυσικούς κεντρικούς υπολογιστές.
Η αποθήκευση με το VMotion επιτρέπει τη μετανάστευση των virtual machines από ένα datastore σε ένα άλλο χωρίς διακοπή υπηρεσιών. Αυτό επιτρέπει στους administrators να μεταφέρουν off-load virtual machines από ένα storage array σε ένα άλλο για συντήρηση, παραμετροποίηση των LUNs, και αναβάθμιση των VMFS volumes. Οι administrators μπορούν έτσι να βελτιστοποιήσουν το περιβάλλον αποθήκευσης, να παρέχουν βελτιωμένη απόδοση και να μεταναστεύσουν εύκολα και αυτόματα virtual machines. Η τεχνολογία VMotion φαίνεται στο παρακάτω σχήμα.



Εικόνα 7.3.8.1: Τεχνολογία VMotion

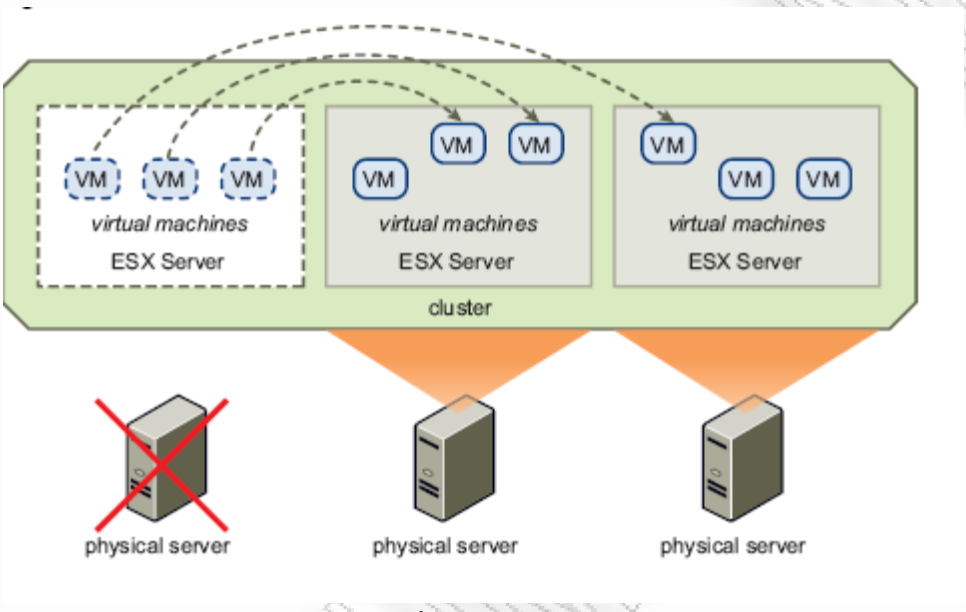
Το VMware DRS ενισχύσει τον έλεγχο των πόρων και την ικανότητα διαχείρισης στο εικονικό datacenter. Ένα cluster μπορεί να αντιμετωπισθεί ως ένα σύνολο από την CPU και την μνήμη των hosts συνολικά σε ένα single pool. Τα virtual machines μπορούν να οριστούν σε αυτό το συγκεκριμένο single pool. Τα DRS monitors ελέγχουν το φόρτο εργασίας των virtual machines καθώς και τη χρησιμοποίηση των πόρων των hosts .
Χρησιμοποιώντας το VMotion και έναν ευφυή scheduler των πόρων, τα DRS VMware αυτοματοποιούν τα virtual machines με τους κεντρικούς υπολογιστές μέσα στο cluster για να χρησιμοποιήσουν τους πόρους CPU και μνήμης συγκεκριμένου κεντρικού υπολογιστή όπως φαίνεται στο σχήμα. Τα DRS κάνουν τον υπολογισμό και αυτοματοποιούν την ένωση.
Εάν διατεθεί ένας νέος φυσικός κεντρικός υπολογιστής, τα DRS ανακατανέμουν αυτόματα τα virtual machines χρησιμοποιώντας VMotion για να εξισορροπήσουν το φόρτο εργασίας. Εάν ένας φυσικός κεντρικός υπολογιστής πρέπει να κλείσει για οποιοδήποτε λόγο, τα DRS επανεκχωρούν αυτόματα τα virtual machines του σε άλλους κεντρικούς υπολογιστές.
Όταν το DPM επιτρέπεται, το σύστημα συγκρίνει το cluster – και την ικανότητα επιπέδων των hosts – με τις απαιτήσεις των virtual machines που τρέχουν στο cluster. Εάν ένας host βρεθεί να έχει αρκετή πλεονάζουσα ικανότητα να απορροφήσει τα virtual machines ενός άλλου host, τότε τα virtual machines μεταφέρονται και ο άλλος host γίνεται stand-by.
Κατά αυτόν τον τρόπο, το DPM βελτιστοποιεί την κατανάλωση ισχύος του cluster. Τα DRS μπορούν να διαμορφωθούν ώστε να εφαρμόζουν αυτόματα τις ενέργειες εξισορρόπησης φορτίων και διαχείρισης ισχύος .



Εικόνα 7.3.8.2: DRS

Το VMware HA προσφέρει μια απλή , χαμηλού κόστους εναλλακτική λύση διαθεσιμότητας .Επιτρέπει ταχύτατη αυτόματη νέα εκκίνηση των virtual machines σε έναν διαφορετικό φυσικό κεντρικό υπολογιστή μέσα σε ένα cluster, εάν ο host κεντρικός υπολογιστής αποτύχει. Όλες οι εφαρμογές μέσα στα μηχανήματα εικονικής πραγματικότητας απολαμβάνουν το υψηλό όφελος διαθεσιμότητας (μέσω application clustering).

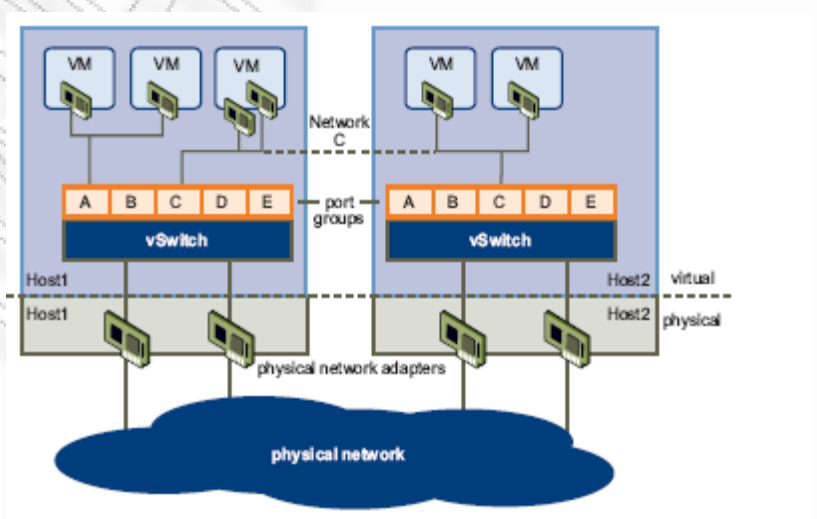
Το HA ελέγχει όλους τους hosts σε ένα cluster και ανιχνεύει τις αποτυχίες τους. Ένας agent που τοποθετείται σε κάθε host διατηρεί heartbeat με τους άλλους hosts στο cluster, και η απώλεια ενός heartbeat κινεί τη διαδικασία σε όλα τα επηρεασθέντα virtual machines ώστε να πάνε σε άλλους hosts.
Το HA εξασφαλίζει ότι ικανοποιητικοί πόροι είναι διαθέσιμοι από το cluster για να ξαναξεκινήσει τα virtual machines σε διαφορετικούς hosts . Αυτό φαίνεται στο παρακάτω σχήμα :



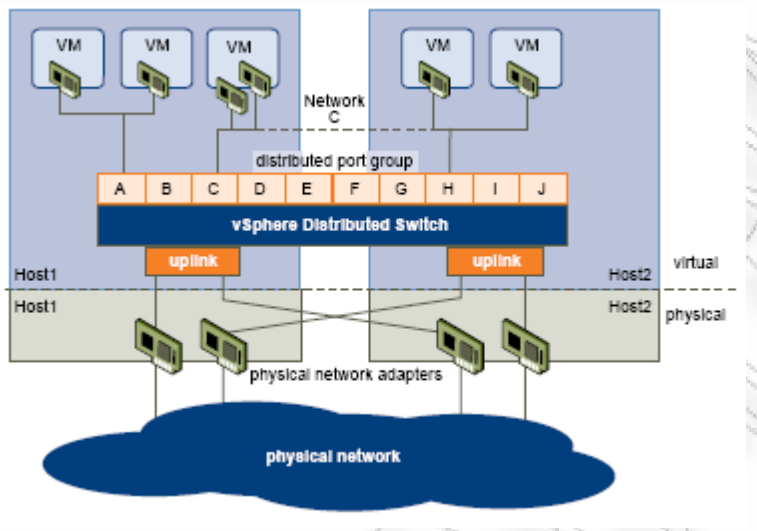
Εικόνα 7.3.8.3: HA

7.4 Network Architecture

Η υποδομή VMware είναι μια λύση που προσφέρει ένα πλούσιο σύνολο από virtual networking elements που κάνουν τη δικτύωση των virtual machines σε ένα datacenter πολύ εύκολη και απλή όσο και στο φυσικό περιβάλλον. Επιπλέον, επιτρέπει ένα νέο σύνολο ικανοτήτων που είναι αδύνατες σε φυσικό περιβάλλον, καθώς πολλοί από τους περιορισμούς του φυσικού κόσμου δεν ισχύουν εδώ.



Εικόνα 7.4.1: Network



Εικόνα 7.4.2: Distributed Network

Τα παραπάνω σχήματα παρουσιάζουν τη σχέση μεταξύ των δικτύων μέσα και έξω από το εικονικό περιβάλλον. Το εικονικό περιβάλλον παρέχει παρόμοια στοιχεία δικτύωσης με το φυσικό κόσμο. Πρόκειται για εικονικές κάρτες διεπαφών δικτύων (vNIC), εικονικούς διακόπτες (vSwitch) και port groups. Όπως μια φυσική μηχανή, έτσι κάθε virtual machine διαθέτει το δικό της vNIC. Το λειτουργικό σύστημα και οι εφαρμογές μιλούν στο vNIC μέσω ενός τυποποιημένου οδηγού συσκευών ή ενός βελτιστοποιημένου VMware οδηγού συσκευών ακριβώς σαν το vNIC, που είναι ένα φυσικό NIC.

Στον φυσικό κόσμο, το vNIC έχει τη διεύθυνση της MAC του και μια ή περισσότερες διευθύνσεις IP. Αποκρίνεται στο τυποποιημένο πρωτόκολλο Ethernet ακριβώς όπως ένα φυσικό NIC. Στην πραγματικότητα, ένας εξωτερικός πράκτορας δεν ξέρει ότι επικοινωνεί με ένα virtual machine.

Ένα virtual switch λειτουργεί όπως ένα physical switch στο στρώμα 2. Κάθε κεντρικός υπολογιστής διαθέτει τα δικά του virtual switch. Στη μια πλευρά του virtual switch βρίσκονται τα group port που συνδέονται με τα virtual machines. Στην άλλη πλευρά βρίσκονται οι uplink συνδέσεις με φυσικούς adapters Ethernet στον κεντρικό υπολογιστή, όπου το virtual switch «ζει». Τα virtual switches συνδέονται με τον εξωτερικό κόσμο μέσω των φυσικών adapters Ethernet που συνδέονται με τα virtual switch uplinks.

Ένα virtual switch μπορεί να συνδέσει στα δικά του uplinks περισσότερους από έναν physical Ethernet adapters και έτσι να ενεργοποιήσει το NIC teaming. Με το NIC teaming δύο ή περισσότεροι physical adapters μπορούν να χρησιμοποιηθούν για να μοιραστούν όλο το δικτυακό φορτίο κυκλοφορίας ή να παρέχουν ένα παθητικό failover σε περίπτωση αστοχίας υλικού ή διακοπής λειτουργίας των δικτύων.

Το port group αποτελεί μια μοναδική σύλληψη στο εικονικό περιβάλλον. Το port group είναι ένας μηχανισμός για τις πολιτικές που διαχειρίζονται το δίκτυο που συνδέεται με αυτό. Ένα vSwitch μπορεί να έχει πολλά group port.

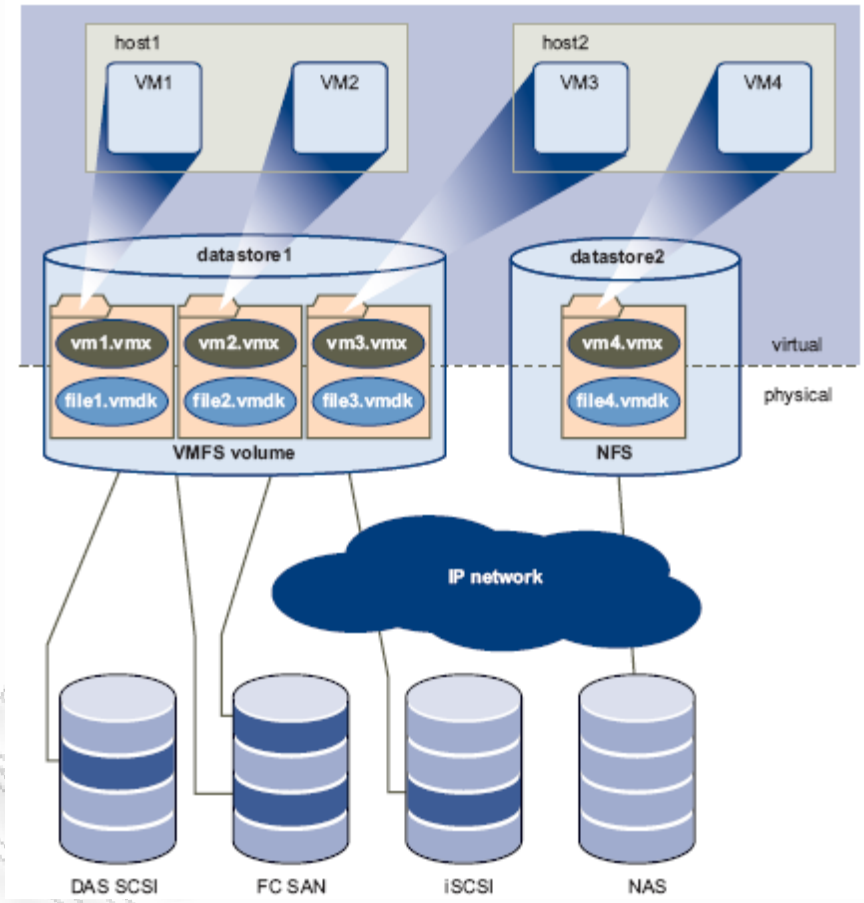
Αντί να συνδέουμε μια συγκεκριμένη πόρτα σε ένα vSwitch, ένα virtual machine συνδέει το vNIC του με ένα group port. Όλα τα virtual machines που συνδέονται με το ίδιο group port ανήκουν στο ίδιο δίκτυο μέσα στο εικονικό περιβάλλον, ακόμα κι αν βρίσκονται σε διαφορετικούς φυσικούς κεντρικούς υπολογιστές.

Τα group ports μπορούν να διαμορφωθούν για να επιβάλουν διάφορες πολιτικές που παρέχουν ενισχυμένη ασφάλεια δικτύωσης, κατάτμηση δικτύων, καλύτερη απόδοση, υψηλότερη διαθεσιμότητα και διαχείριση κυκλοφορίας:

Layer 2 security options – Επιβάλλει το τι μπορεί να κάνει το vNic σε ένα virtual machine, όπως controlling promiscuous mode, MAC address change, forged transmits.
VLAN support – Επιτρέπει σε virtual networks να συνδεθούν με VLANs και να υποστηρίξουν QOS policies
Traffic shaping – Ορίζουν τα average bandwidth, peak bandwidth και burst size. Τέτοια policies ορίζονται για να βελτιώσουν το traffic management.
NIC teaming – Ορίζοντας NIC teaming policies για ένα individual port group ή δίκτυο μπορούμε να μοιράζουμε το δικτυακό φορτίο κυκλοφορίας ή να παρέχουμε ένα παθητικό failover σε περίπτωση αστοχίας υλικού ή διακοπής λειτουργίας των δικτύων.

7.5 Storage Architecture

Η αρχιτεκτονική αποθήκευσης υποδομής VMware, που παρουσιάζεται στο παρακάτω σχήμα, αποτελείται από τα στρώματα της αφαίρεσης που κρύβουν και διαχειρίζονται την πολυπλοκότητα και τις διαφορές μεταξύ των φυσικών υποσυστημάτων αποθήκευσης.



Εικόνα 7.5: Storage architecture

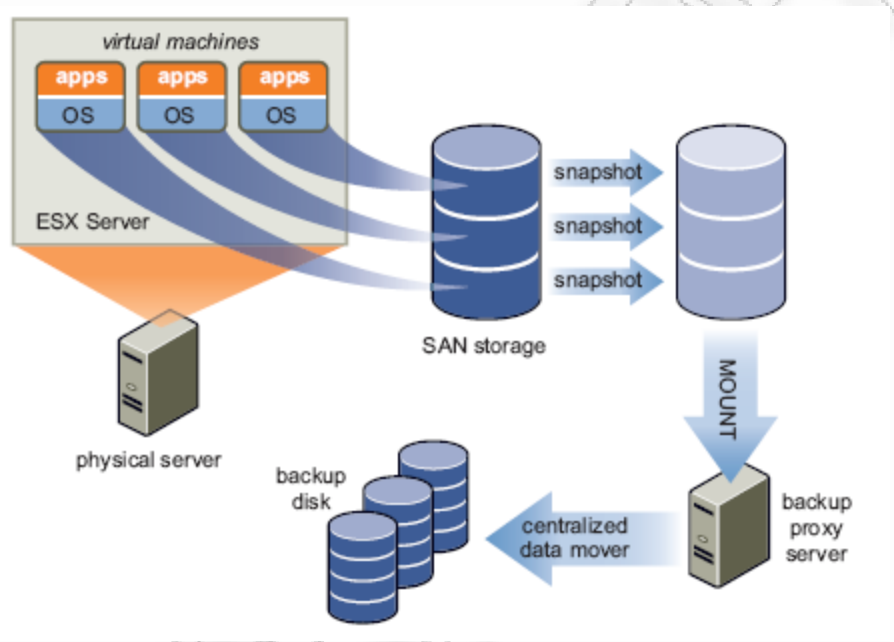
Στις εφαρμογές και τα λειτουργικά συστήματα μέσα σε κάθε virtual machine το υποσύστημα αποθήκευσης είναι ένας απλός εικονικός virtual Bus Logic ή LSI SCSI host bus adapter που συνδέεται με έναν ή περισσότερους εικονικούς δίσκους SCSI, όπως παρουσιάζεται στο παραπάνω σχήμα.

Οι εικονικοί δίσκοι SCSI είναι από τα στοιχεία datastore που παρέχονται στο datacenter. Ένα datastore λειτουργεί σαν μια συσκευή αποθήκευσης που παρέχει χώρο αποθήκευσης σε πολλά virtual machines πέρα από τους πολλαπλούς φυσικούς hosts.
Το datastore εφαρμόζει ένα απλό μοντέλο για να διαθέσει το χώρο αποθήκευσης στα μεμονωμένα μηχανήματα εικονικής πραγματικότητας χωρίς να τα εκθέτει στην πολυπλοκότητα της ποικιλίας των φυσικών τεχνολογιών αποθήκευσης που είναι διαθέσιμες, όπως το κανάλι ινών SAN, iSCSI SAN, ή η άμεση συνημμένη αποθήκευση και το NAS.
Ένα virtual machine αποθηκεύεται ως ένα σύνολο αρχείων σε έναν κατάλογο στο datastore. Ένας εικονικός δίσκος μέσα σε κάθε μηχάνημα εικονικής πραγματικότητας είναι ένα ή περισσότερα αρχεία στον κατάλογο. Κατά συνέπεια, μπορούμε να αναπτύξουμε δραστηριότητες σε εικονικό δίσκο (αντίγραφο, κίνηση, υποστήριξη) ακριβώς όπως σε ένα αρχείο. Οι νέοι εικονικοί δίσκοι μπορούν να είναι «hot-added» σε ένα virtual machine χωρίς να το κλείσουν. Σε αυτή την περίπτωση, ένα εικονικό αρχείο δίσκων (.vmdk) δημιουργείται σε ένα VMFS αρχείο για να παρέχει τη νέα αποθήκευση για τον «hot-added» εικονικό δίσκο ή ένα υπάρχον εικονικό αρχείο δίσκων συνδέεται με ένα virtual machine. Κάθε datastore είναι φυσικά ένας όγκος VMFS (ή για NAS datastores, ένας όγκος NFS με τα χαρακτηριστικά VMFS) σε μια συσκευή αποθήκευσης. Το datastore μπορεί να επεκταθεί σε πολλαπλά φυσικά υποσυστήματα αποθήκευσης. Όπως φαίνεται στο σχήμα, ένας ενιαίος όγκος VMFS μπορεί να περιέχει ένα ή περισσότερα LUNs από μια τοπική σειρά δίσκων SCSI σε έναν φυσικό host, μια φάρμα δίσκων καναλιών SAN ινών ή iSCSI φάρμα δίσκων SAN. Νέα LUNs που προστίθενται σε οποιοδήποτε υποσύστημα φυσικής αποθήκευσης ανακαλύπτονται αυτόματα και τίθενται στην διάθεση όλων των υπαρχόντων ή νέων datastores. Η μεγάλη χωρητικότητα σε έναν προηγουμένως δημιουργημένο όγκο VMFS (datastore) μπορεί να επεκταθεί (hot-extended) χωρίς τη διακοπή τροφοδοσίας σε physical host ή στα υποσυστήματα αποθήκευσης, με την προσθήκη ενός νέου φυσικού LUN από οποιοδήποτε από τα υποσυστήματα αποθήκευσης που είναι ορατά σε αυτό. Αντίθετα, εάν οποιοδήποτε από τα LUNs μέσα σε έναν όγκο VMFS (datastore) αποτυγχάνει ή γίνεται μη διαθέσιμο, μόνο εκείνα τα virtual machines που αγγίζουν το συγκεκριμένο LUN επηρεάζονται. Όλα τα άλλα virtual machines με τους εικονικούς δίσκους που υπάρχουν σε άλλο LUN συνεχίζουν να λειτουργούν κανονικά. Το VMFS είναι ένα clustered σύστημα αρχείων που δίνει την δυνατότητα σε ένα shared storage να επιτρέπει σε πολλούς φυσικούς hosts να διαβάσουν και να γράψουν στο ίδιο storage ταυτόχρονα. Το VMFS παρέχει τη δυνατότητα κλειδώματος των δίσκων εξασφαλίζοντας ότι το ίδιο virtual machine δεν γίνεται συγχρόνως powered on από πολλαπλούς κεντρικούς υπολογιστές. Εάν ένας physical host αποτύχει στο κλείδωμα δίσκου για κάθε virtual machine, απελευθερώνεται και έτσι κάθε virtual machine μπορεί να γίνει restart σε άλλον φυσικό host. Το VMFS επίσης χαρακτηρίζεται από enterprise-class μηχανισμούς συνέπειας και αποκατάστασης συντριβής όπως: distributed journaling, crash consistent virtual machine I/O path, και machine state snapshots. Αυτοί οι μηχανισμοί μπορούν να βοηθήσουν το φυσικό host σε μια quick root-cause and recovery κατάσταση στο μηχάνημα εικονικής πραγματικότητας, και στις αποτυχίες των υποσυστημάτων αποθήκευσης.

7.6 VMware Consolidated Backup

Η αρχιτεκτονική αποθήκευσης VMware επιτρέπει μια απλή εφεδρική λύση μηχανημάτων εικονικής πραγματικότητας: το VMware Consolidated Backup. Το VMware Consolidated Backup προσφέρει μια συγκεντρωμένη δυνατότητα για ένα LAN-free backup των virtual machines.
Όπως φαίνεται στο παρακάτω σχήμα το Consolidated Backup δουλεύει από κοινού με έναν third-party backup agent που τρέχει σε έναν εφεδρικό κεντρικό υπολογιστή proxy (όχι στον κεντρικό υπολογιστή που τρέχει τον κεντρικό υπολογιστή ESX), αλλά δεν απαιτεί έναν agent μέσα στα virtual machines.

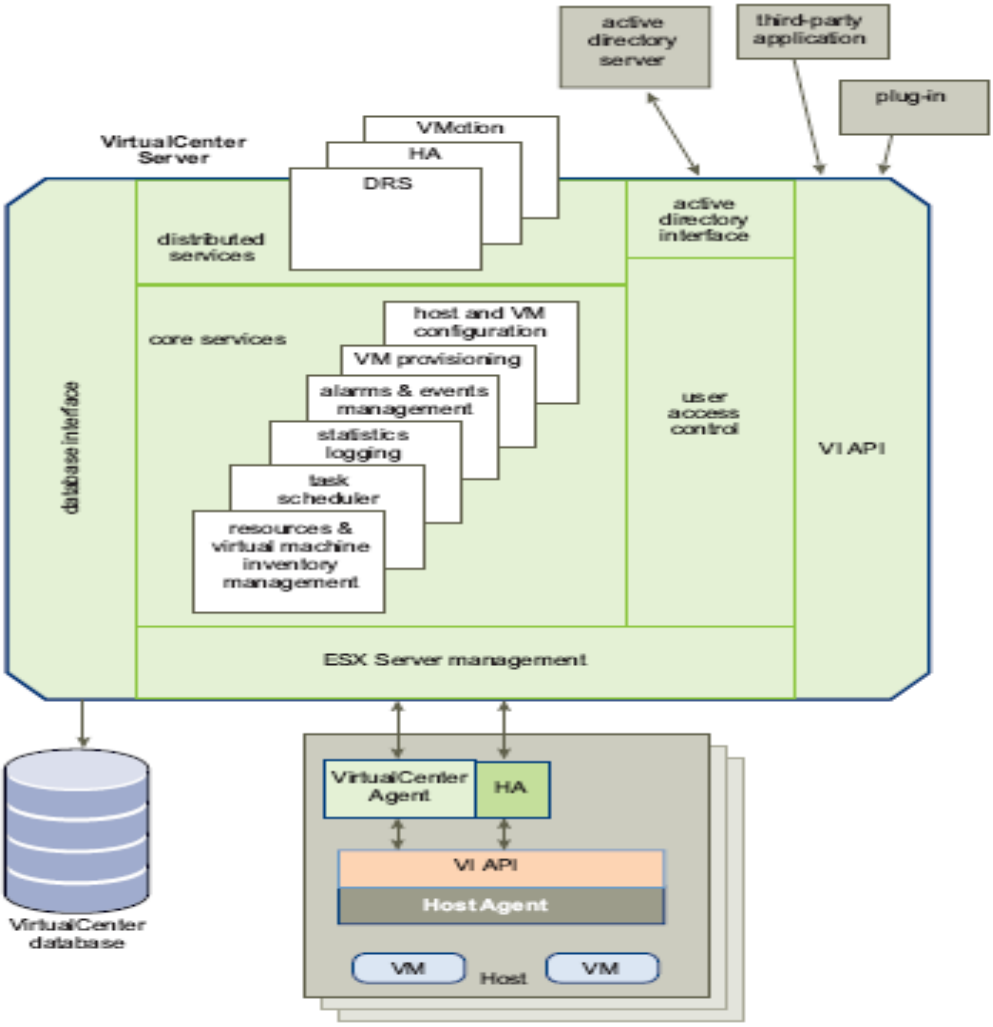
Ο third-party backup διαχειρίζεται το backup schedule. Ξεκινά το Consolidated Backup όταν είναι η ώρα να γίνει το backup. Όταν αρχίζει το Consolidated Backup τρέχει κάποια pre-backup scripts για να ακινητοποιηθούν τα virtual disks και να πάρουν το δικό τους snapshot. Στην συνέχεια τρέχει ένα σετ από post-thaw scripts για να επαναφέρει τα virtual machines στην κανονική τους διαδικασία. Την ίδια χρονική στιγμή γίνεται mount το disk snapshot στον backup proxy server. Στο τέλος ο third-party backup agent παίρνει backup τα αρχεία στο mounted snapshot στους δικούς του backup προορισμούς. Δημιουργώντας snapshots από virtual disks και backups από αυτά σε ξεχωριστό proxy server, το Consolidated Backup παρέχει απλή, λιγότερο παρεισφρητική, με χαμηλό overhead backup λύση για το εικονικό περιβάλλον.



Εικόνα 7.6: VMware Consolidated Backup

7.7 VirtualCenter Server

Το VirtualCenter Server προσφέρει συγκεντρωμένη διαχείριση για τα datacenters. Αθροίζει τους φυσικούς πόρους από τους πολλαπλούς κεντρικούς υπολογιστές ESX και παρουσιάζει μια κεντρική συλλογή των απλών και εύκαμπτων πόρων στον administrator των συστημάτων, ώστε να μπορεί να παρέχει τα virtual machines στο εικονικό περιβάλλον.
Τα components του VirtualCenter Server είναι ο έλεγχος προσπέλασης χρηστών, οι υπηρεσίες πυρήνων, οι διανεμημένες υπηρεσίες, τα plug-ins και διάφορες διεπαφές.



Εικόνα 7.7: VirtualCenter Server Components

Το παραπάνω σχήμα δείχνει τα στοιχεία του VirtualCenter Server.

Το User Access Control επιτρέπει στον system administrator να δημιουργεί και να διαχειρίζεται διαφορετικά επίπεδα προσπέλασης στο VirtualCenter από διαφορετικούς χρήστες.
Για παράδειγμα, μπορεί να υπάρχει ένας user που θα μπορεί να παραμετροποιεί τους φυσικούς server στο datacenter, όπως επίσης μπορεί να υπάρχει και ένας διαφορετικός χρήστης που θα διαχειρίζεται μόνο τα virtual resources από ένα συγκεκριμένο resource pool.
Οι υπηρεσίες πυρήνα είναι βασικές υπηρεσίες διαχείρισης για ένα virtual datacenter. Περιέχουν υπηρεσίες όπως:

VM Provisioning – Οδηγοί και αυτοματοποιημένες διαδικασίες παροχής virtual machines.

Host and VM Configuration – Επιτρέπει την παραμετροποίηση των hosts και των virtual machines.

Resources and Virtual Machine Inventory Management – Οργάνωση των virtual machines και των resources του εικονικού περιβάλλοντος. Εγκατάσταση της διαχείρισης τους.

Statistics and Logging – Αναλυτικές στατιστικές αναφορές και logs για το performance και resource από τα στοιχεία του datacenter όπως virtual machines, hosts, και clusters.

Alarms and Event Management – Παρακολουθεί και προειδοποιεί τους χρήστες για κάποιο πιθανό πρόβλημα, γεγονός ή κατάσταση.

Task Scheduler – Χρονοπρογραμματισμός ενεργειών όπως το VMotion που γίνεται σε συγκεκριμένο χρόνο.

Consolidation – Αναλύει την ικανότητα και τη χρησιμοποίηση φυσικών πόρων του datacenter. Προβαίνει σε συστάσεις για τη βελτίωση του utilization με την ανακάλυψη των φυσικών συστημάτων που μπορούν να μετατραπούν στα μηχανήματα εικονικής πραγματικότητας και να παγιωθούν επάνω στους κεντρικούς υπολογιστές ESX. Αυτοματοποιεί τη διαδικασία σταθεροποίησης αλλά και παρέχει την ευελιξία χρηστών στη ρύθμιση των παραμέτρων σταθεροποίησης.

Οι διανεμημένες υπηρεσίες είναι λύσεις που επεκτείνουν τις ικανότητες του VMware Infrastructure's στο επόμενο επίπεδο όπως VMware DRS VMware HA, και VMware VMotion. Οι διανεμημένες υπηρεσίες επιτρέπουν τη διαμόρφωση και τη διαχείριση αυτών των λύσεων κεντρικά από τον κεντρικό υπολογιστή VirtualCenter. Τα plug-ins είναι εφαρμογές που μπορούν να εγκατασταθούν πάνω από το VirtualCenter και που προσθέτουν επιπλέον χαρακτηριστικά, γνωρίσματα και λειτουργίες. Τα plug-ins περιλαμβάνουν:

VMware Converter Enterprise for VirtualCenter – Δίνει τη δυνατότητα στον user να μετατρέψει μια φυσική μηχανή ή ένα virtual machine οποιουδήποτε είδους σε ένα ESX Server virtual machine. Τα συστήματα που έχουν μετατραπεί μπορούν να εισαχθούν σε οποιοδήποτε σημείο (location) του VirtualCenter inventory.

VMware Update Manager – Δίνει τη δυνατότητα στον administrator να ενισχύσει τις ρυθμίσεις ασφάλειας σε όλο το μήκος των ESX Server hosts και να διαχειριστεί τα virtual machines. Το συγκεκριμένο plug-in παρέχει τη δυνατότητα να δημιουργούμε user-defined security baselines που θα παρουσιάζουν ένα σύνολο από security standards. Οι Security administrators μπορούν να συγκρίνουν τους hosts και τα virtual machines με τα συγκεκριμένα security baselines για να ανακαλύψουν και να διορθώσουν όσα virtual machines δεν είναι συμμορφωμένα.

Το VirtualCenter Server διαθέτει 4 key interfaces:

ESX Server management – Πρόκειται για interfaces μαζί με τον VirtualCenter agent για τη διαχείριση κάθε φυσικού server στο datacenter.

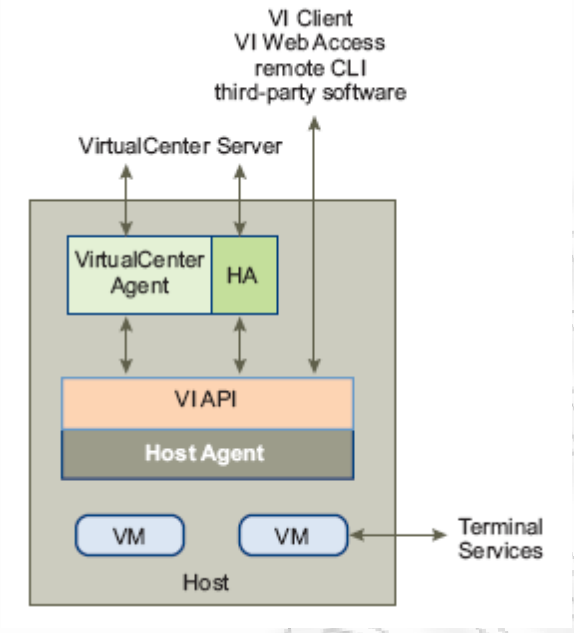
VMware Infrastructure API – Πρόκειται για interfaces μαζί με τα VMware management clients και από third-party λύσεις.

Database interface – Παρέχει τη δυνατότητα σύνδεσης με Oracle ή Microsoft SQL Server για την αποθήκευση πληροφορίας όπως virtual machine configurations, host configurations, resources και virtual machine inventory, performance statistics, events, alarms, user permissions και roles.

Active Directory interface – Παρέχει τη δυνατότητα σύνδεσης με το to Active Directory για λήψη των user access control information.

7.8 Επικοινωνία μεταξύ VirtualCenter και ESX Server

Το VirtualCenter επικοινωνεί με τον host agent του ESX Server μέσω του VMware Infrastructure API (VI API). Όταν ένας host προστίθεται στο VirtualCenter τότε το VirtualCenter στέλνει έναν VirtualCenter agent να τρέχει στον host. Αυτός ο agent επικοινωνεί με τον host agent.



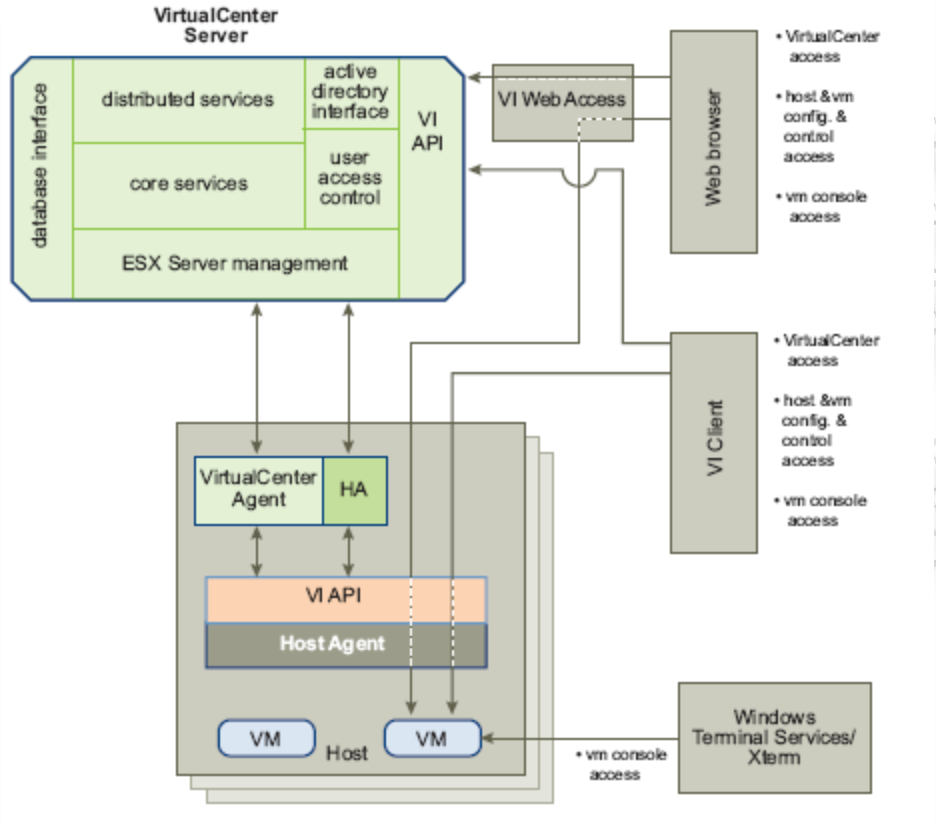
Εικόνα 7.8: Επικοινωνία μεταξύ VirtualCenter και ESX Server

Το VirtualCenter agent ενεργεί σαν ένας μικρός VirtualCenter Server για να εκτελέσει τις ακόλουθες λειτουργίες:

- Αναμεταδίδει και επιβάλλει τις αποφάσεις κατανομής των πόρων που λαμβάνονται στο VirtualCenter, συμπεριλαμβανομένων και εκείνων που στέλνονται από DRS engine.
- Μεταφέρει στο virtual machine όλες τις εντολές αλλαγής που γίνονται στο host agent.
- Μεταφέρει host configuration αλλαγές στο host agent.
- Συλλέγει τις στατιστικές απόδοσης, τους συναγερμούς και τις καταστάσεις λάθους από τον host agent, και τα στέλνει στον κεντρικό υπολογιστή VirtualCenter.

7.9 Accessing the Virtual Datacenter

Οι χρήστες μπορούν να διαχειριστούν την υποδομή VMware datacenter ή να έχουν πρόσβαση στην κονσόλα των virtual machines με τρεις διαφορετικούς τρόπους: μέσω του VI client, με την πρόσβαση Ιστού μέσω μιας μηχανής αναζήτησης Ιστού ή μέσω terminal services (με τα Windows Terminal Services), όπως φαίνεται στο παρακάτω σχήμα.
Η πρόσβαση σε hosts μπορεί να γίνει μόνο από τους administrators των φυσικών hosts. Όλη η σχετική λειτουργία που μπορεί να γίνει στον host μπορεί επίσης να γίνει στον κεντρικό υπολογιστή VirtualCenter.



Εικόνα 7.9: VMware Infrastructure Access and Control

Ο VI Client αποκτά προσπέλαση στο VirtualCenter μέσω του VMware API. Αφού ο χρήστης αυθεντικοποιηθεί, ένα session ξεκινά στο VirtualCenter και ο user βλέπει τα resources και τα virtual machines που του έχουν αντιστοιχηθεί. Για την προσπέλαση μιας κονσόλας virtual machine ο VI Client πρώτα βρίσκει την τοποθεσία του virtual machine από το VirtualCenter μέσω του VMware API. Στη συνέχεια συνδέεται στον κατάλληλο host και του παρέχεται προσπέλαση στην κονσόλα του virtual machine.

8.0 MS SQL Server 2008 R2 σε VMware

8.1 Γενικά

Ο Microsoft SQL Server [12] είναι μια από τις ευρύτατα διαδεδομένες πλατφόρμες βάσεων δεδομένων στον κόσμο, με πολλούς οργανισμούς που έχουν εκατοντάδες ή ακόμα και χιλιάδες εγκαταστάσεις στα περιβάλλοντά τους. Η ευελιξία της κεντρικής μηχανής SQL σε συνάρτηση με τις πλούσιες δυνατότητες εφαρμογής που προσφέρει δίνουν άμεσα ευελιξία σε κάθε είδους εφαρμογή, με αποτέλεσμα οι χρήστες να επωφελούνται από τα πιο χρήσιμα χαρακτηριστικά γνωρίσματα της εφαρμογής. Έτσι έχουμε βελτίωση της παραγωγικότητας.
Ωστόσο, η ευελιξία εφαρμογής συνεπάγεται ανάλογο κόστος στις διαδικασίες. Δεδομένου ότι ο αριθμός εφαρμογών σε μια επιχείρηση αυξάνεται διαρκώς, ένας αυξανόμενος αριθμός κεντρικών υπολογιστών SQL δημιουργείται κάτω από τη διαχείριση του κύκλου ζωής. Κάθε εφαρμογή έχει ένα σύνολο απαιτήσεών για το στρώμα των βάσεων δεδομένων, με συνέπεια τις πολλαπλάσιες εκδόσεις, τα πολλά patch-levels και τις διαδικασίες συντήρησης.
Δεδομένου ότι ο φόρτος εργασίας μιας εφαρμογής ποικίλλει ευρέως, σε πολλούς από τους κεντρικούς υπολογιστές SQL δίνεται περισσότερο υλικό από χρειάζονται, ενώ σε άλλους που το χρειάζονται πραγματικά δεν δίνεται.
Η πρόκληση για τον administrator είναι να παράσχει τις βασικές υπηρεσίες βάσεων δεδομένων στους χρήστες της εφαρμογής την ευελιξία και την αυτονομία που αναμένουν κρατώντας την υποδομή όσο το δυνατόν πιο απλή και οικονομική. Το παραδοσιακό database consolidation είναι ένα εξαιρετικά σύνθετο εγχείρημα, που απαιτεί σε βάθος επανόρθωση της εφαρμογής και αυστηρή προσοχή στις λειτουργικές διαδικασίες που εφαρμόζονται για τον έλεγχο της έκδοσης και τη συνεχή συμβατότητα της εφαρμογής.
Δημιουργώντας «virtualizing» Microsoft SQL Servers με VMware vSphere μπορούμε να πετύχουμε το καλύτερο ανάμεσα σε δύο κόσμους. Θα βελτιστοποιήσουμε και θα σταθεροποιήσουμε την ανάγκη για πόρους διατηρώντας παράλληλα την ευελιξία της εφαρμογής μέσω της απομόνωσης του ρόλου (role isolation).
Οι Microsoft SQL Servers μπορούν να μεταναστεύσουν στη τρέχουσα κατάσταση χωρίς κόστος, χωρίς μεγάλα και σημαντικά λάθη στην εφαρμογή και χωρίς τη μεταβαλλόμενη έκδοση λειτουργικών συστημάτων ή εφαρμογής ή patch-level.
Για βάσεις δεδομένων υψηλής επίδοσης, το VMware παρέχει, μέσω του vSphere, τη δυνατότητα να τρέχουν οι πιο απαιτητικοί φόρτοι εργασίας κεντρικών υπολογιστών SQL. Για μικρότερες και πιο εξειδικευμένες βάσεις δεδομένων, το vSphere προσφέρει υψηλές αναλογίες σταθεροποίησης, σχεδιάζοντας τα χαρακτηριστικά γνωρίσματα που δίνουν στους χρήστες της εφαρμογής την ευελιξία και την απόδοση που χρειάζονται, απλοποιώντας και χαμηλώνοντας παράλληλα τις δαπάνες για την επιχείρηση.

8.2 Εκτιμήσεις απόδοσης κεντρικών υπολογιστών με Microsoft SQL Server

Το VMWARE vSphere4 προσφέρει πολλαπλές δυνατότητες στον τομέα της απόδοσης, κάνοντας εξαιρετικά εύκολη την «εικονικοποίηση» μιας βαριάς βάσης δεδομένων με ελάχιστες επιπτώσεις στην απόδοση.
Οι βελτιωμένες διαχειριστικές ικανότητες των πόρων στο vSphere διευκολύνουν την αποτελεσματικότερη σταθεροποίηση των πολλαπλών virtual machines κεντρικών υπολογιστών SQL (VM) σε έναν ενιαίο host χωρίς μείωση της απόδοσης ή της εξελιξιμότητας. Η μεγάλη σταθεροποίηση μπορεί να μειώσει σημαντικά το κόστος της φυσικής υποδομής και της χορήγησης αδειών του κεντρικού υπολογιστή SQL, ακόμη και σε μικρότερα περιβάλλοντα.

Το 2009 η VMware εκτέλεσε μια διαδικασία ανάλυσης της απόδοσης του Microsoft SQL Server 2008 σε πλατφόρμα vSphere. Το τεστ απόδοσης έγινε με σημαντικό φόρτο στη CPU, στη μνήμη, στο storage και στο δίκτυο. Τα αποτελέσματα έδειξαν μια ιδιαίτερα εξελικτική και άριστη απόδοση για μια enterprise επιχειρηματική βάση δεδομένων που τρέχει σε μια virtual πλατφόρμα.

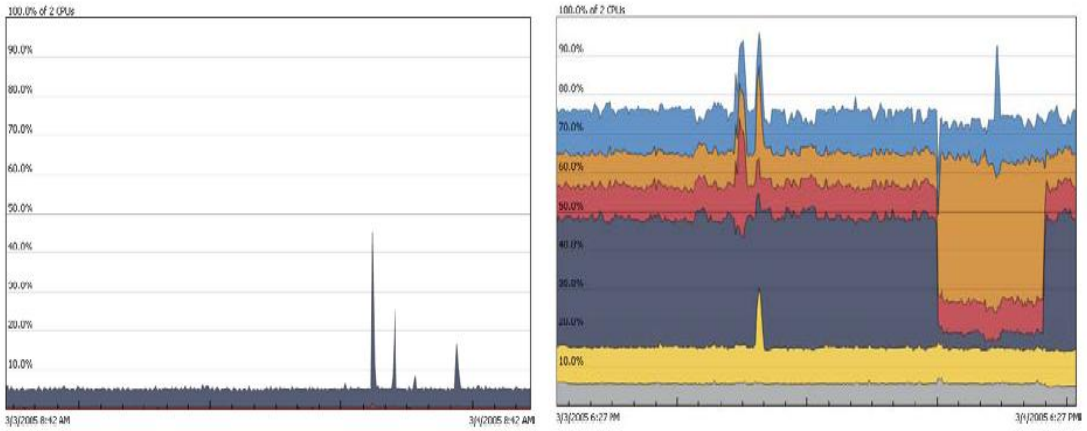
8.3 Πλεονεκτήματα για το virtualizing του Microsoft SQL Server

Η σταθεροποίηση των κεντρικών υπολογιστών παρέχει σημαντικά οφέλη στους «virtualized» SQL Servers:

- Αξιοποίηση όλων των πυρήνων των επεξεργαστών των κεντρικών υπολογιστών.
- Σταθεροποίηση όλων των κεντρικών υπολογιστών με ελάχιστες επιπτώσεις στις εφαρμογές.
- Σταθεροποίηση των αδειών χρήσης του Microsoft SQL Server στους κεντρικούς υπολογιστές.

8.3.1 Αξιοποίηση όλων των πυρήνων των επεξεργαστών των κεντρικών υπολογιστών

Ενώ οι μεγάλοι multi-core κεντρικοί υπολογιστές αποτελούν πλέον τον κανόνα, οι περισσότερες εφαρμογές δεν μπορούν να αξιοποιήσουν όλους τους πυρήνες των επεξεργαστών σε έναν φυσικό κεντρικό υπολογιστή.
Αν και τα vSphere virtual machines μπορούν να κλιμακοποιήσουν ένα CPU με 8 πυρήνες –εάν είναι απαραίτητο– για το φόρτο εργασίας, τα μικρότερα virtual machines προσφέρουν ευελιξία στην τοποθέτηση και μπορούν να βοηθήσουν στην αύξηση των αναλογιών σταθεροποίησης και να βελτιώσουν την απόδοση.
Οι σημερινοί νέοι εξηντατετράμπιτοι (64 bit) κεντρικοί υπολογιστές διαθέτουν μεγάλο αριθμό multi-core CPU, αυξανόμενα όρια μνήμης και φυσικής RAM. Σε πολλούς οργανισμούς, ιδιαίτερα σε εκείνους που δεν χρησιμοποιούν virtualization, είναι απίθανο ένας ενιαίος κεντρικός υπολογιστής SQL να χρησιμοποιήσει την πλήρη ισχύ υπολογισμού αυτών των συστημάτων.
Εντούτοις, σε πολλές περιπτώσεις το κόστος του γεμίσματος όλων των διαθέσιμων slots για CPU σε ένα νέο 64 bit server μπορεί να μην έχει το επιθυμητό αποτέλεσμα, παρά την αύξηση του κόστους. Ωστόσο με το vSphere αυτή η παραπάνω CPU μπορεί να αξιοποιηθεί σωστά.
Για παράδειγμα, οι μικρότερες εγκαταστάσεις κεντρικών υπολογιστών SQL μπορούν να ωφεληθούν από τη σταθεροποίηση των κεντρικών υπολογιστών και τη εύκολη συντήρηση των βάσεων δεδομένων. Τα μεγαλύτερα περιβάλλοντα μπορούν να τρέξουν σε πολύ μεγάλα virtual machines κεντρικών υπολογιστών SQL με μέχρι 255GB RAM, και να επωφεληθούν από την αυξανόμενη ευελιξία που παρέχει το vSphere.
Ουσιαστικά το τρέξιμο πολλών virtual machines σε αυτά τα εξηντατετράμπιτα συστήματα είναι ένας άριστος τρόπος να μεγιστοποιηθεί η αξία που μπορεί να δώσει αυτό το ισχυρό υλικό.

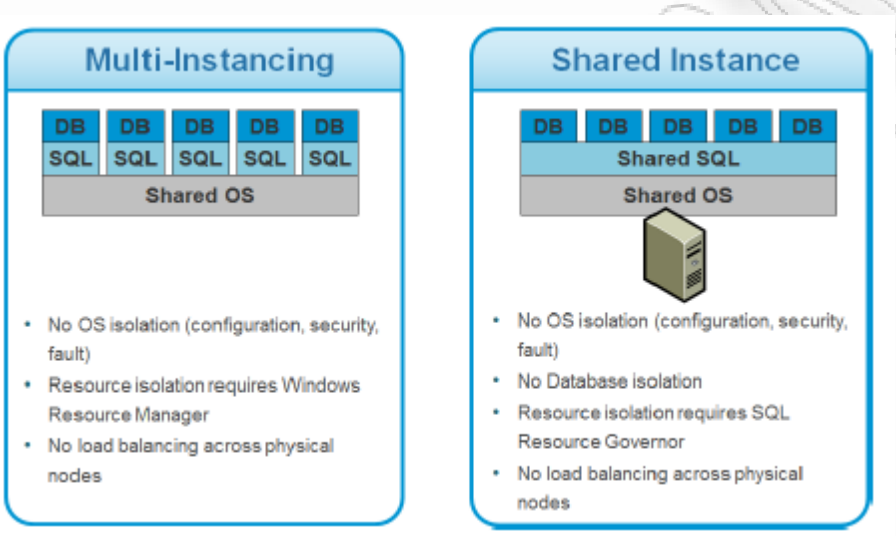


Εικόνα 8.3.1: Αξιοποίηση όλων των πυρήνων των επεξεργαστών

8.3.2 Εγκατάσταση των κεντρικών SQL Servers σε VMware, με τον ελάχιστο αντίκτυπο στις εφαρμογές των υπολογιστών

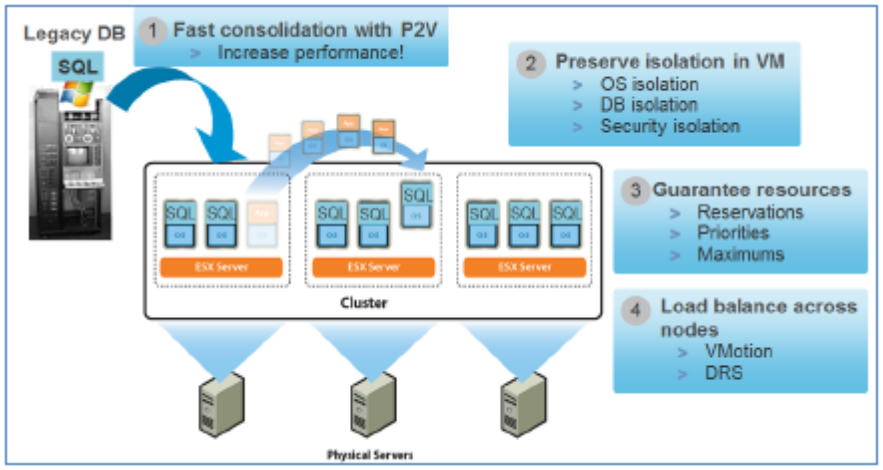
Η σταθεροποίηση των βάσεων δεδομένων μπορεί να είναι δύσκολο να επιτευχθεί, απαιτώντας σε βάθος επανόρθωση εφαρμογής αλλά και αλλαγές στις υπάρχουσες επιχειρησιακές διαδικασίες. Κάθε εφαρμογή έχει τις απαιτήσεις της για το στρώμα βάσεων δεδομένων (εκδόσεις κεντρικών υπολογιστών OS και SQL, patches, κ.λπ.), τεχνικά ζητήματα αλλά και ζητήματα σχετικά με την παραβίαση των συμφωνιών υποστήριξης ISV.
Όταν γίνεται εγκατάσταση κεντρικού υπολογιστή SQL με χρήση vSphere, δίνεται η δυνατότητα να χρησιμοποιηθούν υπάρχουσες διαμορφώσεις κεντρικών υπολογιστών SQL. Απλά γίνεται μετανάστευση φυσικών κεντρικών υπολογιστών SQL χρησιμοποιώντας P2V ή LUNs στους δίσκους RDM που συνδέονται με τα νέα virtual machines. Καμία αλλαγή δεν απαιτείται στις εκδόσεις κεντρικών υπολογιστών OS ή SQL και καμία επανόρθωση εφαρμογής. Ακόμη και η διεύθυνση IP και το όνομα υπολογιστή παραμένουν αμετάβλητες.
Τα προγράμματα σταθεροποίησης των βάσεων δεδομένων είναι πάρα πολύ δύσκολα στην ανάπτυξη και στην παραμετροποίηση.
Οι κεντρικοί υπολογιστές SQL υποστηρίζουν ποικίλους φόρτους εργασίας εφαρμογής και κάθε εφαρμογή έχει τις δικές της απαιτήσεις ως προς την απόδοση, την εξελιξιμότητα, τη διαμόρφωση και την υποστήριξη. Οι εμπορικές εφαρμογές μπορεί να διέπονται από σημαντικούς κανόνες για τη διαμόρφωση ή και ακριβή πολιτική υποστήριξης.
Οι custom εφαρμογές που γράφονται υπόκεινται σε ένα σύνολο ζητημάτων, όπως η χρήση παλιών λειτουργιών βάσεων δεδομένων που αποτρέπουν το update ή τον άσχημο κώδικα καθώς επίσης και το hard code ονομάτων των κεντρικών υπολογιστών ή των διευθύνσεων IP.
Η σταθεροποίηση των βάσεων δεδομένων στους φυσικούς κεντρικούς υπολογιστές λαμβάνει συνήθως μία από τις εξής δύο μορφές: multi-instance ή shared-instance. Στην πρώτη περίπτωση πολλαπλοί κεντρικοί υπολογιστές SQL εγκαθίστανται σε έναν ενιαίο που τρέχει μία ή περισσότερες βάσεις δεδομένων. Αυτό παρέχει τη διαφοροποίηση στο επίπεδο εφαρμογής των βάσεων δεδομένων. Έτσι μπορούμε να χάσουμε ένα instance χωρίς να επηρεάζονται οι άλλες βάσεις δεδομένων. Επίσης έχουμε μεγάλη ευελιξία με τις εκδόσεις κεντρικών υπολογιστών SQL. Δυστυχώς όμως, με αυτή τη διαμόρφωση, το OS είναι το ενιαίο σημείο της αποτυχίας για όλες

τις περιπτώσεις και δεν υπάρχει κανένας τρόπος να ελεγχθεί η κατανάλωση των πόρων της κάθε περίπτωσης χωρίς τη χρησιμοποίηση του Windows Resource Manager.
Στη δεύτερη περίπτωση, ένας κεντρικός υπολογιστής SQL χρησιμοποιείται για να τρέξει πολλές βάσεις δεδομένων. Αυτή η διαμόρφωση όχι μόνο απαιτεί την τυποποίηση σε μια ιδιαίτερη έκδοση κεντρικών υπολογιστών SQL, αλλά και εκθέτει τη μηχανή κεντρικών υπολογιστών SQL ως ενιαίο σημείο αποτυχίας (εκτός από το OS). Η κατανάλωση των πόρων στη μέθοδο αυτή απαιτεί τη χρήση SQL Resource Governor.



Εικόνα 8.3.2.1: Εγκατάσταση των κεντρικών SQL servers **σε VMware**

Η σταθεροποίηση των βάσεων δεδομένων μέσα σε μια εικονική υποδομή παρέχει τα οφέλη της φυσικής σταθεροποίησης βάσεων δεδομένων μειώνοντας σημαντικά τις αναμενόμενες προκλήσεις της εφαρμογής. Πολλοί πελάτες προσεγγίζουν την εικονική σταθεροποίηση των βάσεων δεδομένων κάνοντας μια φυσική σε εικονική (P2V) μετατροπή σε κάθε έναν από τους φυσικούς κεντρικούς υπολογιστές τους. Αξίζει να σημειωθεί ότι το νέο virtual machine περιέχει ολόκληρο και απομονωμένο το σωρό του λογισμικού που βρισκόταν στο φυσικό κεντρικό υπολογιστή. Έτσι δεν υπάρχει καμία μείωση της απομόνωσης των πόρων από Windows ή SQL Server perspective.
Δεν υπάρχει καμία ανάγκη για επανασχεδιασμό των πρότυπων ασφάλειας μέσα στο νέο guest φιλοξενούμενο λειτουργικό σύστημα. Το vSphere παρέχει τη δυνατότητα να παρουσιαστούν οι πόροι (KME, μνήμη και αποθήκευση) στο VM και δεδομένου ότι απαιτείται να εγγυηθεί για τις εφαρμογές που το απαιτούν.
Αυτές οι δυνατότητες μειώνουν την ανάγκη για υπερπρομήθεια πόρων. Έτσι τα VM μπορούν να χειριστούν τους μέγιστους φόρτους εργασίας. Τα VM δημιουργούν αυξανόμενα επίπεδα εξυπηρέτησης χρησιμοποιώντας τα VMware High Availability, Fault Tolerance και vMotion.



Εικόνα 8.3.2.2: Σταθεροποίηση των βάσεων δεδομένων

8.4 Λειτουργικά (operational) πλεονεκτήματα

8.4.1 Αυτόματη αντίδραση στην αλλαγή απαιτήσεων πόρων

Χρησιμοποιώντας τη μηχανή του SQLServer μπορούμε να χρησιμοποιήσουμε όλα τα λειτουργικά πλεονεκτήματα που παρέχει το συγκεκριμένο λογισμικό. Δηλαδή:

1) Γρήγορη παροχή SQL server μέσω των virtual machines templates.

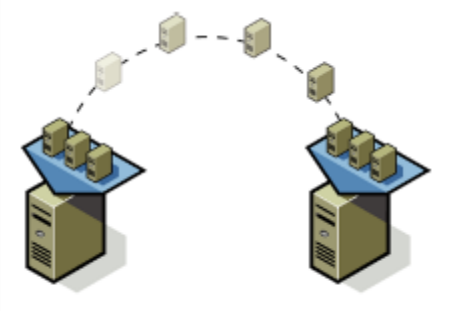
Τα πρότυπα μηχανημάτων εικονικής πραγματικότητας μπορούν να επιταχύνουν τους χρόνους επέκτασης με την εξάλειψη της επαναλαμβανόμενης εγκατάστασης του OS και της εγκατάστασης των patches. Τα νέα virtual machines μπορούν να επεκτείνουν τη διαμόρφωση των πυρήνων τους σε λίγα λεπτά, να επιτρέψουν τη γρήγορη εισαγωγή των εφαρμογών στην παραγωγή και να μειώσουν τη χειρωνακτική εργασία που απαιτείται κατά τη διάρκεια της επέκτασής τους. Επιπλέον, τα προϊόντα όπως το VMware vCenter Lab Manager και το VMware PowerCLI μπορούν να επιταχύνουν και να αυτοματοποιήσουν περαιτέρω τη διαδικασία στα δοκιμασμένα virtual machines των κεντρικών υπολογιστών SQL.

Η ανάπτυξη ενός νέου κεντρικού υπολογιστή SQL μπορεί να πάρει πολλές ώρες ώσπου να διαμορφωθεί το υλικό, η αποθήκευση, η εγκατάσταση του λειτουργικού συστήματος και των patches καθώς και οι σχετικές εφαρμογές και οι αναπροσαρμογές τους. Αυτή η διαδικασία πρέπει να επαναληφθεί για κάθε κεντρικό υπολογιστή και αυτό μπορεί να οδηγήσει σε μεγάλη επιμήκυνση του χρόνου επέκτασης, ειδικά για τις μεγάλες, σύνθετες αρχιτεκτονικές.

Εναλλακτικά, ένα πρότυπο virtual machines μπορεί να διαμορφωθεί και να αποθηκευτεί μια φορά για κάθε τύπο κεντρικού υπολογιστή στο συγκεκριμένο περιβάλλον, επιτρέποντας έτσι στους διαχειριστές κεντρικών υπολογιστών SQL να διατηρούν μια εικονική βιβλιοθήκη όλων των εικόνων των κεντρικών υπολογιστών. Αυτό μπορεί να εξοικονομήσει αμέτρητες ώρες κατά την ανάπτυξη των νέων συστημάτων, ιδιαίτερα για τις μεγαλύτερες επεκτάσεις κεντρικών υπολογιστών SQL που μπορεί να πρέπει να επεκτείνουν τις εκατοντάδες των νέων κεντρικών υπολογιστών για να υποστηρίξουν τις απαιτήσεις εφαρμογής μιας οργάνωσης.

Προκειμένου να κερδίσουμε χρόνο και να μειωθούν οι διακοπές λειτουργίας στα σενάρια ανίχνευσης μηχανικών βλαβών λογισμικού, η συγκεκριμένη πλατφόρμα μπορεί σε μερικές περιπτώσεις να επεκτείνει ταχύτατα ένα νέο μηχάνημα εικονικής πραγματικότητας από ένα

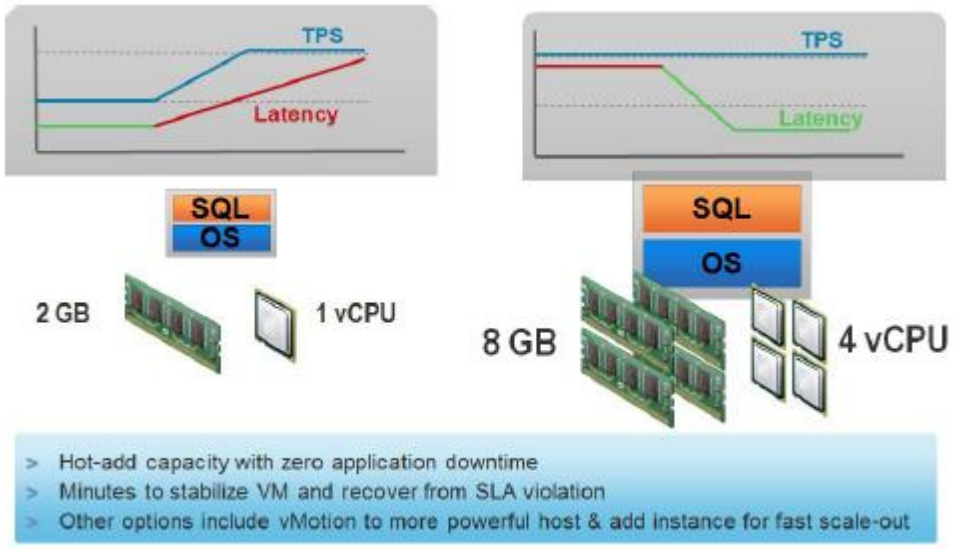
πρότυπο, να διαμορφώσει τον κεντρικό υπολογιστή SQL, και να το συνδέσει έπειτα στις υπάρχουσες βάσεις δεδομένων με το νέο virtual machine.
Μόλις συνδεθούν οι βάσεις δεδομένων με το νέο virtual machine, η υπηρεσία εφαρμογής χρηστών αποκαθίσταται και το παλαιό μηχάνημα εικονικής πραγματικότητας ελευθερώνεται για άλλους στόχους, όπως η προηγμένη εκτέλεση της ανίχνευσης μηχανικών βλαβών και των διαγνωστικών. Εναλλακτικά, το παλαιό virtual machine μπορεί απλά να παροπλιστεί.
Το PowerCLI είναι ένα ισχυρό εργαλείο με γραμμή εντολών που δίνει τη δυνατότητα να αυτοματοποιηθούν όλες οι πτυχές διαχείρισης του vSphere, συμπεριλαμβανομένου του δικτύου, της αποθήκευσης, του VM, του φιλοξενουμένου OS και πολλών άλλων. Το PowerCLI παρέχεται σαν Windows Power Shell Snap In και διαθέτει αναλυτικές οδηγίες και παραδείγματα.



Εικόνα 8.4.1.1: Virtual Machine Templates

2) Εύκολη προσθήκη CPU και μνήμης.

Πολλές εφαρμογές είναι πολύπλοκες στον προσδιορισμό του μεγέθους της βάσης δεδομένων. Οι administrators αναγκάζονται συχνά να προβλέψουν τις απαιτήσεις των μεγεθών για 3-5 έτη στο μέλλον και έπειτα να «μεταφράσουν» αυτή την εκτίμηση σε προδιαγραφές συστημάτων (ΚΜΕ, μνήμη, αποθήκευση). Εάν η εκτίμησή τους αποδειχτεί λανθασμένη, η εφαρμογή πρέπει να είναι επαναπροσδιοριστεί, προκαλώντας έτσι χρόνο διακοπής και σημαντική διάσπαση στην εφαρμογή.
Με τη vSphere Hot-add δυνατότητα οι εφαρμογές μπορούν να είναι κατά κάποιο τρόπο «μελλοντικά ασφαλείς». Δεδομένου ότι οι εφαρμογές αυξάνονται με την πάροδο του χρόνου και απαιτούν περισσότερους πόρους (επεξεργαστή, μνήμη, δίκτυο, δίσκους) οι administrators μπορούν να εισάγουν πόρους στα virtual machines δυναμικά και κατά τη διάρκεια λειτουργίας, χωρίς να αναστατώσουν την εφαρμογή και χωρίς κάποια σύνθετη επανεγκατάσταση.



Εικόνα 8.4.1.2: vSphere Hot-add

Στο παραπάνω σχήμα το transaction rate TPS αυξάνει με αποτέλεσμα η καθυστέρηση να αυξάνεται πέρα από τα SLA όρια. Ο administrator μπορεί να δώσει λύση σε αυτό το πρόβλημα προσθέτοντας χωρητικότητα στο virtual machine και αυτόματα ο SQL server θα αντιληφθεί και θα χρησιμοποιήσει τη νέα χωρητικότητα. Μέσα σε λίγα λεπτά, ο SQL server διαχειρίζεται τη νέα χωρητικότητα και, χωρίς διακοπή του συστήματος, η καθυστέρηση μειώνεται σύμφωνα με τις SLA απαιτήσεις.

3) Ενίσχυση της δοκιμής και της αντιμετώπισης προβλημάτων μέσω των κλωνοποιημένων virtual machines.
   Τα snapshots και οι κλώνοι αποτελούν ισχυρά εργαλεία για τη δοκιμή και την ανίχνευση μηχανικών βλαβών οποιουδήποτε virtual machine. Στα σύνθετα περιβάλλοντα εφαρμογής που υποστηρίζονται από τον κεντρικό υπολογιστή SQL, αυτή η ικανότητα είναι ιδιαίτερα πολύτιμη. Με το VMware η ανίχνευση μηχανικών βλαβών μπορεί να βοηθήσει και να μειώσει ουσιαστικά το χρόνο λύσης κάποιων κρίσιμων ζητημάτων και να μειώσει το γενικό αντίκτυπό τους στο περιβάλλον παραγωγής.
   Τα virtual machines snapshots αποτελούν ένα πολύ δυνατό εργαλείο παρακολούθησης και ανίχνευσης λαθών. Τα live snapshots σε virtual machine του VMware μπορούν να χρησιμοποιηθούν για να επιστρέψουμε σε ένα σωστό configuration.
   Η κλωνοποίηση ενός virtual machine δίνει τη δυνατότητα στους administrators να έχουν ένα ακριβές και ανεξάρτητο από το περιβάλλον αντίγραφο οποιουδήποτε virtual machine. Το αντίγραφο μπορεί να εγκατασταθεί σε ένα δοκιμαστικό περιβάλλον για ελέγχους.

8.5 Υψηλή διαθεσιμότητα με τη μικρότερη πολυπλοκότητα

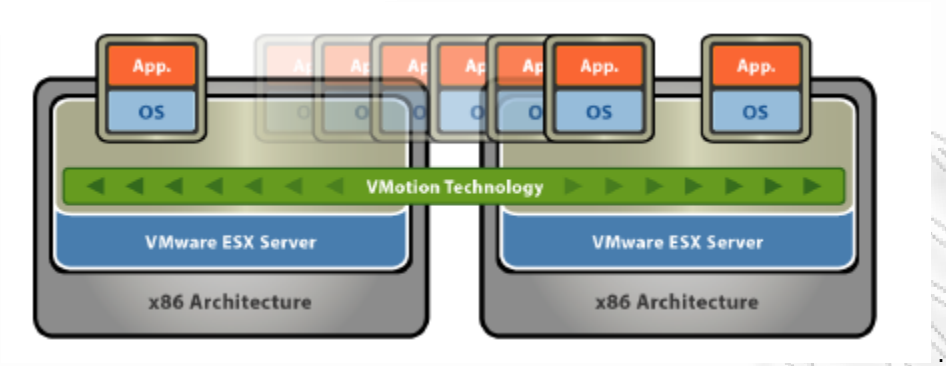
Η πλατφόρμα vSphere έχει τη δυνατότητα να παρέχει ένα μεγάλο εύρος από επιλογές για τη διαθεσιμότητα του συστήματος. Η τεχνολογία VMware HA παρέχει προστασία από βλάβες υλικού του server και είναι ανεξάρτητες από το λειτουργικό σύστημα ή τις εφαρμογές και αυτή η τεχνολογία δουλεύει για κάθε virtual machine που είναι σε πλατφόρμα vSphere.
Για να βοηθήσουν στο δυναμικό load balancing των SQL servers virtual machines, τα VMware DRS μπορούν να διαχειριστούν τους φόρτους εργασίας και να τους ισορροπήσουν αυτόματα. Βασικές λύσεις που στηρίζονται σε VMware HA και DRS μπορούν να επεκταθούν με τις ελάχιστες αλλαγές διαμόρφωσης και να παρέχουν μια γερή λύση διαθεσιμότητας. Αυτές οι

λύσεις μπορούν επίσης να ενισχυθούν για να παρέχουν τα πιο υψηλά επίπεδα διαθεσιμότητας σε συνδυασμό με τις παραδοσιακότερες τεχνολογίες clustering και replication.
Με τα εγγενή οφέλη μιας virtualization βασισμένης πλατφόρμας η επέκταση των κεντρικών υπολογιστών SQL που χρησιμοποιεί το vSphere προσφέρει ποικίλες επιλογές διαθεσιμότητας. Κάθε μια από αυτές τις επιλογές παρέχει διαφορετικά επίπεδα προστασίας και κόστους, ικανοποιώντας μοναδικές υψηλές απαιτήσεις διαθεσιμότητας οποιουδήποτε περιβάλλοντος κεντρικού υπολογιστή SQL. Διάφορα εργαλεία είναι διαθέσιμα από προμηθευτές όπως η VMware και η Microsoft. Επίσης λογισμικό και υλικό τρίτων κατασκευαστών μπορούν να χρησιμοποιηθούν για να διευκολύνουν τις μακρινές διαθεσιμότητες και την αποκατάσταση περιοχών.
Η πλατφόρμα vSphere διαθέτει δύο ισχυρά χαρακτηριστικά: το VMware HA και το DRS.
Επίσης μπορεί να μειώσει τον downtime χρόνο λόγω ενημερώσεων υλικού ή BIOS, με το VMware vMotion σαν βάση για τη δημιουργία λύσεων υψηλών προδιαγραφών και διαθεσιμότητας. Με τις επιλογές διαθεσιμότητας που παρέχει το vSphere εξασφαλίζουμε:

- **Μείωση του downtime χρόνου στις ενημερώσεις (updates) υλικού και BIOS από το VMware vMotion**

  Τα virtual machines αποσυνδέουν το λειτουργικό σύστημα και τις εφαρμογές από τη βάση του υλικού και έτσι επιτρέπουν στην υποδομή να αυξάνεται και να αλλάζει γρήγορα. Το vMotion επιτρέπει σε οποιοδήποτε virtual machine να μεταφερθεί μέσα στους φυσικούς κεντρικούς υπολογιστές, ακόμη και αν οι κεντρικοί υπολογιστές είναι από διαφορετικούς προμηθευτές και με διαφορετικές διαμορφώσεις υλικού. Ο προγραμματισμένος χρόνος διακοπής μπορεί να ελαχιστοποιηθεί και με μια πιο ευέλικτη υποδομή, και έτσι το περιβάλλον κεντρικών υπολογιστών SQL server γίνεται πιο ελαστικό. Σε ένα περιβάλλον χωρίς virtualization δεν μπορεί να υπάρξει τέτοιο επίπεδο ευελιξίας.
  Αφότου μια εφαρμογή επεκταθεί στην παραγωγή, η επέκταση τείνει να γίνει σχετικά στατική, σημαίνοντας ότι ο φόρτος της εργασίας της είναι πιο στενά συνδεδεμένος με την πλατφόρμα υλικού στην οποία τρέχει. Κατά συνέπεια, οι βελτιώσεις υλικού στην υποδομή εφαρμογής αντιστοιχούν άμεσα στην απελευθέρωση και στην αναβάθμιση της ίδιας της εφαρμογής.

Με τις συχνές αλλαγές που απαιτούνται μερικές φορές στον επιχειρησιακό κόσμο, η στατική φύση της υποδομής της εφαρμογής μπορεί να περιορίσει τη δυνατότητα να ικανοποιηθούν οι μεταβαλλόμενες απαιτήσεις στο περιβάλλον οργάνωσης. Για παράδειγμα, μια μαζική είσοδος των χρηστών μιας νέας εφαρμογής μπορεί να απαιτήσει πρόσθετο υλικό και επανασχεδίαση κάποιων συστημάτων για υποστήριξη.
Σε αντίθεση με την παραπάνω στατική και φυσική επέκταση κεντρικών υπολογιστών το VMware αποσυνδέει το OS και τις σχετικές εφαρμογές από το υπάρχων υλικό των κεντρικών υπολογιστών. Με το vMotion VMware, οποιοδήποτε virtual machine μπορεί να είναι μεταναστευμένο μεταξύ των κεντρικών υπολογιστών ESX χωρίς τη διακοπή στην υπηρεσία (σχήμα 7). Το vMotion επιτρέπει στους administrators να μεταφέρουν το φόρτο εργασίας των κεντρικών υπολογιστών SQL προς το ισχυρότερο υλικό χωρίς διακοπές λειτουργίας ή δαπανηρή επανασχεδίαση συστημάτων. Αυτή η πρόσθετη ευκινησία επιτρέπει στο περιβάλλον εφαρμογής να αλλάζει καθώς αλλάζει το περιβάλλον της επιχείρησης. Οι προγραμματισμένες διακοπές μπορούν να μειωθούν, αφού τα SQL server virtual machines μπορούν να μεταφερθούν σε άλλους hosts κατά τη διάρκεια των προγραμματισμένων διαδικασιών.



Εικόνα 8.5.1: Migrating Virtual Machines Across ESX Hosts with vMotion

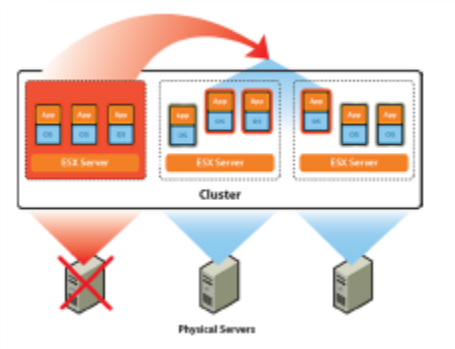
- **Μείωση του downtime χρόνου εξαιτίας αποτυχιών ή περιορισμών των πόρων**

  Η πλατφόρμα vSphere μπορεί να παρέχει μια μεγάλη σειρά επιλογών διαθεσιμότητας. Το VMware HA παρέχει προστασία από την αποτυχία υλικού κεντρικών υπολογιστών, που είναι ανεξάρτητη από το λειτουργικό σύστημα ή τις εφαρμογές και λειτουργεί για κάθε virtual machine που τρέχει σε VSphere.
  Για να βοηθήσει το δυναμικό load balancing των SQL server virtual machines το VMware DRS μπορεί να χρησιμοποιηθεί για να ισορροπεί αυτόματα τους φόρτους εργασίας. Οι βασικές λύσεις που στηρίζονται σε VMware HA και DRS μπορούν να επεκταθούν με ελάχιστες αλλαγές στη διαμόρφωση και να παρέχουν μια γερή λύση διαθεσιμότητας.

Για να βοηθήσουν στο δυναμικό φορτίο την εξισορρόπηση των μηχανημάτων εικονικής πραγματικότητας κεντρικών υπολογιστών SQL, οι DRS VMware μπορούν να χρησιμοποιηθούν στους φόρτους εργασίας ισορροπίας αυτόματα. Οι λύσεις βάσεων που στηρίζονται στη συγκεκριμένη τεχνολογία μπορούν να επεκταθούν με τις ελάχιστες αλλαγές διαμόρφωσης και να παρέχουν μια γερή λύση διαθεσιμότητας. Αυτές οι λύσεις μπορούν επίσης να ενισχυθούν για να παρέχουν τα πιο υψηλά επίπεδα διαθεσιμότητας σε συνδυασμό με τις παραδοσιακότερες τεχνολογίες clustering και replication.

- **VMware High-Availability (HA)**

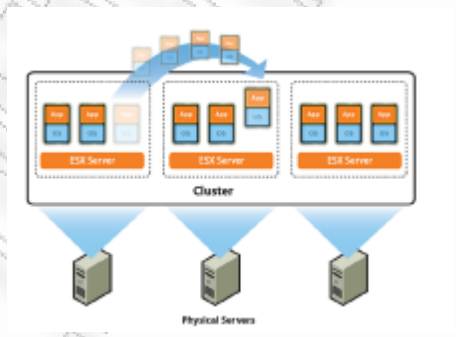
  Παρέχει απλή και χαμηλού κόστους προστασία για κάθε virtual machine, προστατεύοντας τα από κάθε φυσική αποτυχία των hosts. Σε περίπτωση διακοπής λειτουργίας του υλικού των κεντρικών υπολογιστών, το VMware HA θα ξαναξεκινήσει αυτόματα όλα τα virtual machine σε έναν άλλο host ESX (βλ. σχήμα 7), ελαχιστοποιώντας τη διάσπαση στο περιβάλλον των κεντρικών υπολογιστών SQL. Το VMware HA είναι απλό στην οργάνωση και προστατεύει κάθε virtual machine χωρίς να απαιτεί σύνθετο συγκεντρωμένο λογισμικό.



Εικόνα 8.5.2: VMware HA Managing an ESX Host Hardware Failure

- **VMware Distributed Resource Scheduler (DRS)**

  Με το VMware DRS, μπορούμε να διαχειριστούμε δυναμικά τα virtual machines μέσα σε μια ολόκληρη ομάδα (pool) πόρων των κεντρικών υπολογιστών. Τα DRS συλλέγουν τις πληροφορίες χρήσης των πόρων για όλους τους hosts και τα virtual machines και παράγουν τις συστάσεις για την τοποθέτηση των virtual machines. Αυτές οι συστάσεις μπορούν να εφαρμοστούν χειροκίνητα ή αυτόματα. Τα DRS μπορούν να διαχειριστούν δυναμικά την ισορροπία σε όλα τα virtual machines στο περιβάλλον με τη μετατόπιση των φόρτων εργασίας σε ολόκληρη την ομάδα hosts ESX (σχήμα 8.5.3). Αυτή η δυνατότητα εξασφαλίζει ότι τα virtual machines που τρέχουν SQL server θα έχουν πάντα την επεξεργαστική ισχύ και τη μνήμη που χρειάζονται για να ολοκληρώσουν δύσκολες διαδικασίες απόδοσης.



Εικόνα 8.5.3: VMware DRS Dynamic Load Balancing

Οι λύσεις που χρησιμοποιούν VMware HA και VMware DRS παρέχουν out-of-the-box υψηλή διαθεσιμότητα για ολόκληρο το περιβάλλον του SQL server χωρίς την ανάγκη λογισμικού clustering (Microsoft ή άλλου κατασκευαστή). Για SQL servers που είναι ανεπτυγμένοι σε vSphere οι λύσεις VMware HA και VMware DRS αποτελούν τη νέα εναλλακτική λύση, συνδυάζοντας την απλότητα των αυτόνομων μηχανημάτων με την εικονική πραγματικότητα και δίνοντας μεγάλο πλεόνασμα υλικού κεντρικών υπολογιστών για κάθε virtual machine και όχι μόνο για τα clustered.
Το VMware HA είναι επικεντρωμένο σε πτώση υλικού και όχι σε πτώση λειτουργικού συστήματος ή λογισμικού. Για παραπάνω προστασία και ασφάλεια διαθεσιμότητας του SQL Server η διαχείριση τέτοιων καταστάσεων γίνεται με παραδοσιακές λύσεις cluster όπως το

MSCS. Μερικά παραδείγματα που είναι πέρα από τη λύση VMware HA/DRS παρουσιάζονται παρακάτω:

- **Database Mirroring**

Οι καθρέπτες (mirrors) μιας SQL Server βάσης δεδομένων λειτουργούν χρησιμοποιώντας μια μη κοινόχρηστη διαθέσιμη λύση αποθήκευσης που είναι ενσωματωμένη στην τεχνολογία SQL Server replication, ικανή να δημιουργεί και να διαχειρίζεται ένα ή περισσότερα αντίγραφα μιας βάσης δεδομένων από ένα άλλο περιβάλλον SQL Server. Οι καθρέπτες (mirrors) μιας SQL Server βάσης δεδομένων παρέχουν υψηλή διαθεσιμότητα εφαρμογών, και το κομμάτι του χώρου στο δίσκο κάνει το VMware μια εύκολη και φιλική λύση, διευκολύνοντας τη χρήση των τεχνολογιών vMotion, DRS, και HA.

- **Log Shipping**

Η συγκεκριμένη τεχνολογία είναι άρρηκτα συνδεδεμένη με σενάρια αποκατάστασης καταστροφής. Το Log Shipping καθυστερεί το commit των log files στο αντίγραφο μιας βάσης δεδομένων, σύμφωνα με συγκεκριμένο χρόνο καθυστέρησης ορισμένο από τον administrator. Επαναλαμβανόμενες καθυστερημένες επαναλήψεις παρέχουν προστασία ενάντια στο λογικό σφάλμα μιας βάσης δεδομένων, δίνοντας τη δυνατότητα να γυρίσουμε πίσω στο προηγούμενο αντίγραφο και συγκεκριμένο log file ή σε ένα ειδικό σημείο –specific point-in-time (PIT)– με τη δυνατότητα του χειρισμού των log files.

- **Microsoft Failover Clustering (MSCS)**

Τα Microsoft failover clusters χρησιμοποιούν μια κοινή λύση διαθεσιμότητας αποθήκευσης, χρησιμοποιώντας το Microsoft Clustering Service για να αντιμετωπίσουν περιπτώσεις αποτυχίας κάποιου service μιας εφαρμογής στο ενεργό κλαδί (node) του cluster. Το Microsoft failover clusters provide application δίνει στην εφαρμογή μεγάλη υπόσχεση διαθεσιμότητας, προσφέροντας μικρό σφάλμα στο storage του συστήματος. Εξαιτίας αυτού του συγκεκριμένου χώρου στο δίσκο, το Microsoft failover clusters δεν μπορεί να χρησιμοποιήσει δυνατότητες του VMware όπως τα vMotion, DRS και HA.

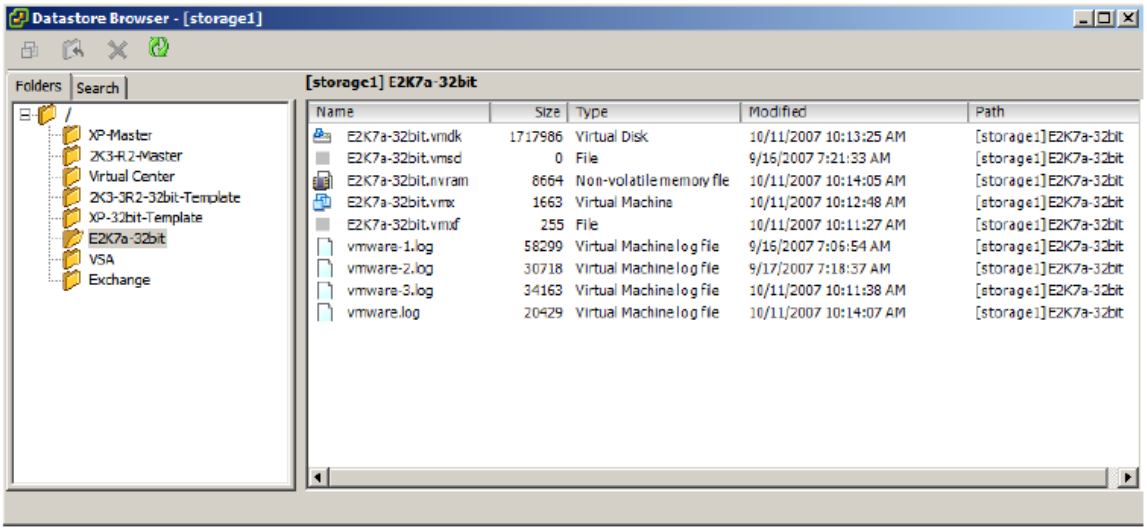
- **Δημιουργία απλών και αξιόπιστων disaster recovery plans για SQL Server 2008 εγκαταστάσεις**

Το vSphere απλοποιεί την αποκατάσταση μετά από καταστροφή κεντρικών υπολογιστών SQL (disaster recovery DR) με τη μείωση των περιορισμών συμβατότητας υλικού και με τη μείωση μέσω της σταθεροποίησης του αριθμού κεντρικών υπολογιστών που απαιτείται στην DR περιοχή. Η τεχνολογία αυτή συνδυασμένη με το SQL server mirroring ή το log shipping, μπορεί να αποκαταστήσει την αποτυχία υλικού και λογισμικού πού γρήγορα, μειώνοντας το χρόνο αποκατάστασης ουσιαστικών υπηρεσιών στους τελικούς χρήστες.

Ένα σημαντικό πλεονέκτημα του virtualization είναι η ανεξαρτησία του λειτουργικού συστήματος και των εφαρμογών από το υλικό του φυσικού server. Αυτό το γεγονός είναι πολύ χρήσιμο σε σενάρια disaster recovery, γιατί αποβάλλει την ανάγκη της παραδοσιακής απαίτησης του ίδιου φυσικού server στη DR περιοχή. Οποιοδήποτε virtual machine μπορεί να έρθει on line από οποιονδήποτε ESX host, χωρίς να απαιτείται συμβατότητα υλικού ή λογισμικού.

Η δυνατότητα λειτουργίας πολλών virtual machines σε ένα συγκεκριμένο server μειώνει το κόστος μιας DR λύσης, αφού τα SQL Server components και τα services θα χρειαζόντουσαν κάποιους φυσικούς servers. Εκτός αυτού, έχοντας όλα τα applications του SQL server καθώς και όλα τα components της υλοποίησης σε συγκεκριμένα virtual machines της DR περιοχής, χρειαζόμαστε λίγο υλικό που θα βοηθήσει σε μια γρήγορη disaster recovery κατάσταση.

Σε αντίθεση με τη λογική και το μοντέλο των φυσικών μηχανημάτων, τα virtual machines σε παραγωγή φέρνουν on line οποιοδήποτε VMware ESX host στη DR περιοχή.
Όταν χρησιμοποιούμε το vSphere, η φορητότητα μιας βάσης δεδομένων SQL Server δημιουργεί επιλογές για disaster recovery. Virtual machines που βρίσκονται σε ετοιμότητα μπορούν να εισαχθούν και να ετοιμαστούν και σε περιβάλλον παραγωγής αλλά και σε περιβάλλον DR. Αυτά τα virtual machines μπορο εύκολα να συνδεθούν με μια βάση δεδομένων SQL Server κατά τη διάρκεια ενός recovery.
Η έννοια "virtual machine encapsulation " σημαίνει ότι μια ολόκληρη εγκατάσταση SQL Server μπορεί να περιέχεται σε ένα μικρό σύνολο από files, που σημαίνει ότι μπορεί εύκολα να γίνει DR.
Η μεταφορά ενός ολόκληρου virtual machine μπορεί να γίνει με ένα απλό copy αρχείων.



Εικόνα 8.5.4: Virtual Machine Encapsulated into a Small Set of Files

8.6 Εναλλακτικές λύσεις επέκτασης

Η εικονικοποίηση του SQL Server σε vSphere παρέχει πολλά πλεονεκτήματα.

Υπάρχουν πολλές μέθοδοι εικονικοποίησης που μπορούμε να ακολουθήσουμε για να επωφεληθούμε από όλα αυτά τα πλεονεκτήματα σε μια εγκατάσταση SQL Server σήμερα. Μερικά τέτοια σενάρια παρουσιάζονται παρακάτω:

- **Εικονικοποίηση SQL Server σε περιβάλλοντα δοκιμής και ανάπτυξης**
  Η εικονικοποίηση προσφέρει έναν απλό και φτηνό τρόπο λειτουργίας του SQL Server σε περιβάλλον δοκιμής ή προ- παραγωγής (staging) με το ελάχιστο δυνατό υλικό. Οι δοκιμές των virtual machines είναι ένας άριστος τρόπος για να αναπαράγουμε σενάρια εφαρμογών και μεταναστεύσεων σε ένα διαχειριστικό περιβάλλον προτού ολοκληρώσουμε τις νέες αλλαγές σε περιβάλλον παραγωγής.

- **Εικονικοποίηση passive SQL Server Mirrors ή Cluster Nodes**
  Τα virtual machines μπορούν να χρησιμοποιηθούν σαν «passive» κόμβοι, είτε χρησιμοποιούμε Microsoft failover clustering είτε SQL database mirroring. Η χρησιμοποίηση

των virtual machines σαν passive κόμβων μπορεί να μειώσει την ποσότητα του υλικού που χρειάζεται για διαθεσιμότητα, ενώ παράλληλα παρέχεται ασφάλεια σε επίπεδο εφαρμογής.

- **Virtualizing SQL Server Disaster Recovery servers**
  Στον πραγματικό κόσμο η διαδικασία αποκατάστασης καταστροφής (disaster recovery) διπλασιάζει το κόστος παραγωγής του υλικού. Κάθε φυσικός server παραγωγής απαιτεί ένα ακριβές αντίγραφο με τον ίδιο εξοπλισμό στην περιοχή αποκατάστασης καταστροφής. Επιπλέον, οι διαδικασίες αποκατάστασης καταστροφής βασισμένες σε φυσικό server είναι πολύπλοκες και προκαλούν πολλά λάθη κατά τη διάρκεια της αποκατάστασης. Με την εικονικοποίηση της περιοχής αποκατάστασης καταστροφής πετυχαίνουμε τη μείωση του κόστους και της πολυπλοκότητας.
  Αρχικά δεν είμαστε υποχρεωμένοι να ακολουθήσουμε την αναλογία 1:1 για το υλικό που χρειάζεται στην περιοχή παραγωγής και στην περιοχή αποκατάστασης καταστροφής. Μπορούμε να εκτελούμε όσα virtual machines θέλουμε σε έναν φυσικό host σε συνάρτηση με την απόδοση. Επίσης μπορούμε να χρησιμοποιούμε οποιοδήποτε υλικό θέλουμε χωρίς να πρέπει οι DR servers να είναι ίδιοι. Η σχεδίαση και ο έλεγχος του SQL Server disaster recovery μπορεί ολοκληρωτικά να αυτοματοποιηθεί χρησιμοποιώντας τον VMware vCenter Site Recovery Manager.

- **Πλήρης εικονικοποίηση όλων των SQL Servers**
  Με τον SQL Server 2005 και 2008 η απόδοση ενός virtual machine είναι συγκρίσιμη με την απόδοση ενός φυσικού server, στοιχείο που αναδεικνύει τον SQL Servers σε ιδανικό υποψήφιο για να πραγματοποιήσει τα οφέλη του virtualization.
  Η απόφαση για το ποια στοιχεία θα εικονικοποιηθούν σε ένα περιβάλλον παραγωγής εξαρτάται από πολλούς παράγοντες. Τέτοιοι παράγοντες είναι η εμπειρία του administrator στον SQL Server και στο vSphere, οι συμφωνίες υποστήριξης με την Microsoft και την VMware καθώς και με τους προμηθευτές υλικού.

8.7 Συμπεράσματα για τον SQL Server σε VMware

Οποιαδήποτε πλατφόρμα επιλεχθεί για να υποστηρίζει μια εφαρμογή και τις εργασίες μιας βάσης δεδομένων πρέπει να είναι αξιόπιστη και αποδεδειγμένα λειτουργική όπως η παραδοσιακή λύση των φυσικών server. Περισσότεροι από 100.000 πελάτες σε όλο τον κόσμο χρησιμοποιούν προϊόντα VMware. Περισσότεροι από το 50% των πελατών της VMware που δουλεύουν με SQL Server έχουν εικονικοποιήσει το περιβάλλον παραγωγής. Η πλατφόρμα vSphere έχει την ωριμότητα, τη σταθερότητα, την απόδοση και τη λειτουργικότητα να υποστηρίζει σημαντικές υποδομές SQL Server.
Για να ικανοποιηθούν οι μεταβαλλόμενες ανάγκες του επιχειρησιακού τοπίου, οι σημερινές εφαρμογές και τα περιβάλλοντα των βάσεων δεδομένων πρέπει να είναι ιδιαίτερα διαθέσιμα, εύκαμπτα, αποδοτικά και με χαμηλού κόστος. Η προτίμηση του vSphere ως πλατφόρμας για τον κεντρικό υπολογιστή SQL μπορεί να βοηθήσει ώστε να ευθυγραμμιστεί καλύτερα το περιβάλλον εφαρμογής στους επιχειρησιακούς στόχους.
Δυνατότητες σαν τα VMware HA και DRS μπορούν να μειώσουν τους νεκρούς χρόνους (downtime) που συνδέονται με πτώσεις υλικού, παρέχοντας τη δυνατότητα για πιο γρήγορη ανάνηψη των υπηρεσιών μηνυμάτων. Τα snapshots και οι κλώνοι των Virtual machines βοηθάνε στη επίλυση προβλημάτων και άλλων ζητημάτων εγκατάστασης.
Με την αποδέσμευση του OS και των σχετικών εφαρμογών από το υλικό, το vMotion VMware ενισχύει πολύ την ανθεκτικότητα και την ευκινησία, επιτρέποντας αντικαταστάσεις και

βελτιώσεις υλικού σε πραγματικό χρόνο, δίνοντας τη δυνατότητα γρήγορης διαχίρισης μεταβαλλόμενων φόρτων εργασίας. Τέλος, το vSphere βοηθά να διατηρηθεί ένα οικονομικά αποδοτικό περιβάλλον κεντρικών υπολογιστών SQL με μεγιστοποίηση της χρήσης της υπολογιστικής ισχύος μέσω της διαχείρισης. Το δυνατό σύνολο των χαρακτηριστικών γνωρισμάτων του vSphere μπορεί να μειώσει τις διοικητικές δαπάνες ελευθερώνοντας τους administrators για άλλες προκλήσεις που είναι στρατηγικά σημαντικές στην επιχείρηση.

9.0 VMware Server Security – Access, Roles, Permissions

Ενώ τα πλεονεκτήματα [13] που προσφέρουν οι λύσεις virtualization όπως ο κεντρικός υπολογιστής VMware έχουν αναλυθεί σε βάθος, μόνο σχετικά πρόσφατα δόθηκε προσοχή στα πιθανά σενάρια ασφάλειας (security risks) που συνδέονται με την ανάπτυξη τέτοιας τεχνολογίας.
Ενώ τα λειτουργικά συστήματα των φιλοξενουμένων που τρέχουν στα μηχανήματα εικονικής πραγματικότητας είναι αμφισβητήσιμα και εξίσου τρωτά με εκείνα που τρέχουν στο φυσικό υλικό (εκτός αν το ίδιο το ελλοχεύον hypervisor συμβιβάζεται με κάποιο τρόπο), η αναρμόδια πρόσβαση στη virtualization διαχείριση επιτρέπει σε έναν πιθανό εισβολέα να σβήσει τα μηχανήματα ή ακόμα και να διαγράψει μόνιμα κρίσιμα συστήματα και δεδομένα.

9.1 VMware Server 2.0 Access Controls

Οι ιδιότητες ασφάλειας του κεντρικού υπολογιστή VMware έχουν σχεδιαστεί για να ελέγχουν την πρόσβαση στο VI Web Access management interface και για να περιορίζουν τις δραστηριότητες που μπορούν να εκτελεσθούν μόλις συνδεθεί επιτυχώς ένας χρήστης.
Η πρόσβαση στο VI Web Access management interface ελέγχεται από την οθόνη σύνδεσης που εμφανίζεται όταν συνδέεται ένας web browser με το σύστημα κεντρικών υπολογιστών VMware. Αντί να αναπαραχθεί διπλά η λειτουργία, ο κεντρικός υπολογιστής VMware παρουσιάζει τον μηχανισμό σύνδεσης και κωδικού πρόσβασης που προσφέρεται από το λειτουργικό σύστημα οικοδεσποτών. Αυτό το επίπεδο ασφάλειας λειτουργεί κάτω από συγκεκριμένους ρόλους και άδειες στους κεντρικούς υπολογιστές VMware, που καθορίζονται από έναν διαχειριστή. Οι ρόλοι αυτοί και οι άδειες ορίζουν τις επιτρεπόμενες ενέργειες μόλις συνδεθεί ο χρήστης.
Έτσι, ένας χρήστης μπορεί να συνδεθεί σε ένα VI Web Access management interface εάν έχει έγκυρους κωδικούς σύνδεσης και πρόσβασης στο σύστημα που φιλοξενεί τον κεντρικό υπολογιστή VMware 2.0. Επιπλέον, στο χρήστη πρέπει να έχουν δοθεί οι κατάλληλες άδειες σύνδεσης από έναν διαχειριστή κεντρικών υπολογιστών VMware (εξ ορισμού, όλοι οι χρήστες στο σύστημα οικοδεσποτών ρυθμίζονται να μην έχουν καμία πρόσβαση). Ο πρώτος διαχειριστής δημιουργείται κατά τη διάρκεια της διαδικασίας εγκαταστάσεων κεντρικών υπολογιστών VMware 2.0, αν μπορούν να δοθούν διοικητικά προνόμια και σε άλλους χρήστες μέσω του VI Web.

9.2 Privileges Roles and Permissions

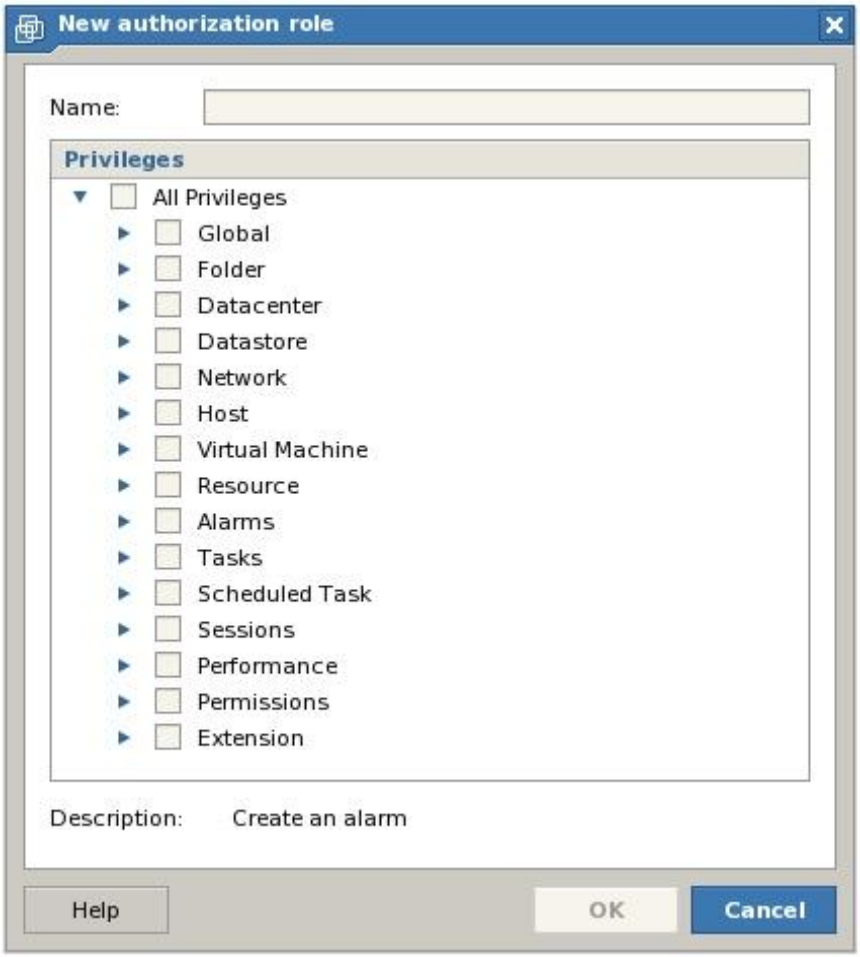
Όταν ένας χρήστης εισέλθει επιτυχώς στο VI Web Access interface το επόμενο επίπεδο ασφάλειας περιλαμβάνει την χρήση των privileges, roles και permissions. Τα στοιχεία αυτά μας δίνουν τη δυνατότητα να διαχειριστούμε τις ενέργειες (actions) που μπορεί να εκτελέσει ένας χρήστης και την πληροφορία για το πού επιτρέπεται η πρόσβαση.

Το «privilege» παρέχει το δικαίωμα εκτέλεσης ενός ιδιαίτερου task από ένα συγκεκριμένο object του VMware Server που ανήκει σε κάποια κατηγορία.
Τα «Roles» είναι ουσιαστικά ένας αριθμός από «privileges» σε group, με συγκεκριμένο όνομα, που μπορούν να οριστούν σε users και groups με συγκεκριμένα objects και κατηγορίες.
Για παράδειγμα, ένα group από privileges μπορεί να συγκεντρωθεί σε ένα ρόλο για εκπαιδευόμενους διαχειριστές, ο οποίος τους δίνει τη δυνατότητα να ξεκινούν και να σβήνουν virtual machines αλλά όχι να τα μεταφέρουν από τον κατάλογο τους (inventory). Ο VMware Server παρέχεται με τρεις προκαθορισμένους ρόλους:

- **No Access** – Είναι ο default ρόλος για τους χρήστες και διαφορετικός απο τον διαχειριστή. Απαγορεύει την πρόσβαση στο VI Web Access interface. Προσπάθειες για είσοδο στο σύστημα θα αντιμετωπίσουν μήνυμα από τον κεντρικό υπολογιστή ότι δεν έχουν δικαίωμα για είσοδο στο σύστημα.
- **Read Only** – Δίνει τη δυνατότητα στο χρήστη να εισέλθει στο σύστημα και να κάνει view. Δεν μπορεί να αλλάξει ρυθμίσεις συστήματος και να μεταβάλλει virtual machine. Επίσης δεν επιτρέπει την πρόσβαση σε virtual machine consoles.
- **Administrator** – Παρέχει πλήρη προνόμια σε όλες τις πτυχές του VMware Server 2.0, συμπεριλαμβανομένης της δυνατότητας ρύθμισης των roles, permissions και privileges για όλους τους χρήστες και τα groups.

9.3 Creating, Modifying and Removing Roles

Ο ρόλος είναι μια συλλογή από privileges συγκεντρωμένα σε ένα group με συγκεκριμένο όνομα. Σε αντίθεση με τους τρεις προκαθορισμένους ρόλους του συστήματος, δίνεται η δυνατότητα να κατασκευάσουμε custom ρόλους μέσα από ένα μεγάλο εύρος από privileges. Η φόρμα που μας δίνει τη δυνατότητα να κατασκευάσουμε custom ρόλους φαίνεται παρακάτω:



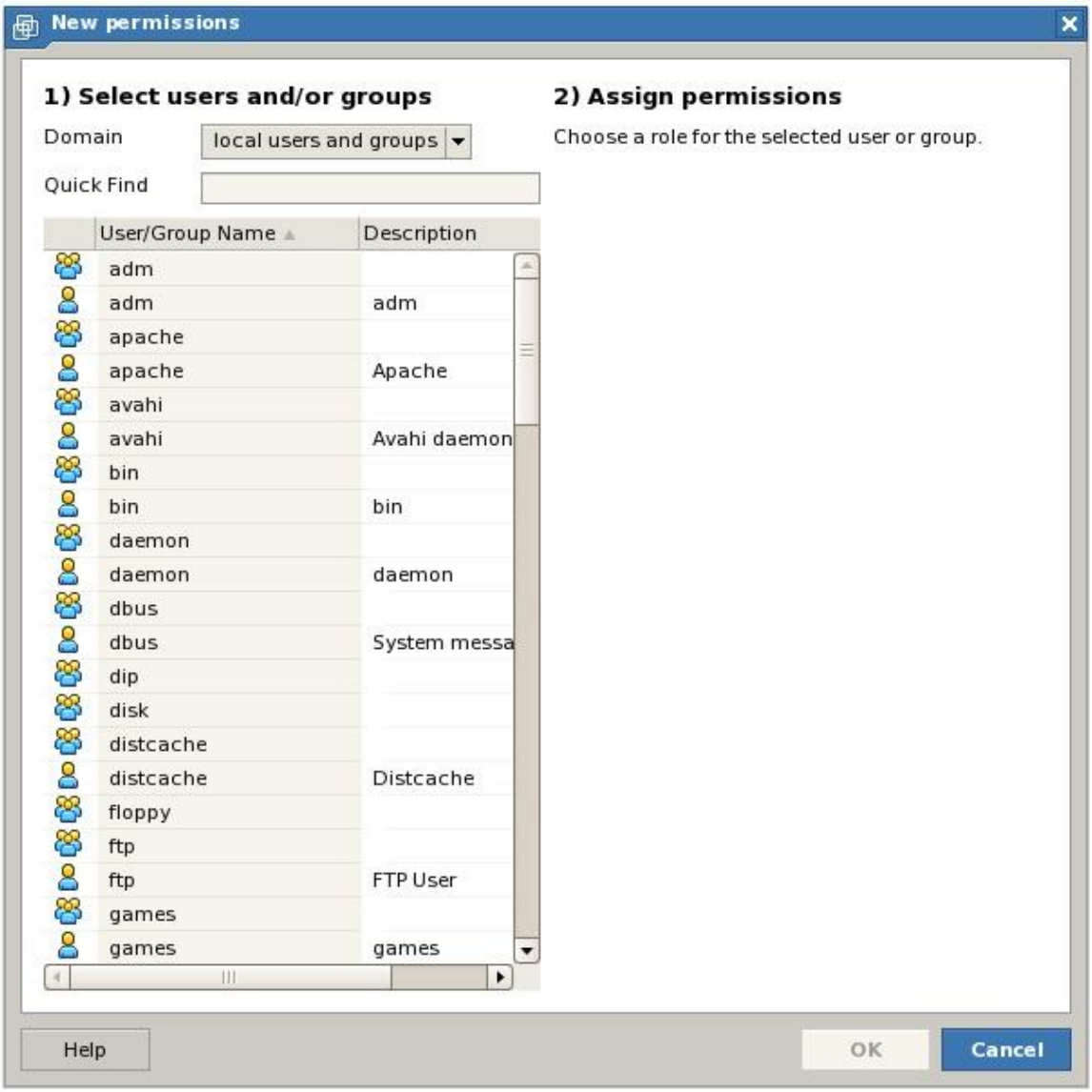
Εικόνα 9.3: New authorization role

9.4 Creating, Modifying and Removing Permissions

Το permission είναι ένας συνδυασμός από ρόλο και χρήστη ή group που είναι ορισμένο σε ένα object του VMware Server. Για παράδειγμα, ένας custom ρόλος που ονομάζεται *Training* εφαρμοσμένος σε κάποιον χρήστη και ορισμένος σε ένα virtual machine είναι ένα permission, δηλαδή ο συγκεκριμένος χρήστης έχει άδεια προσπέλασης στο συγκεκριμένο virtual machine.

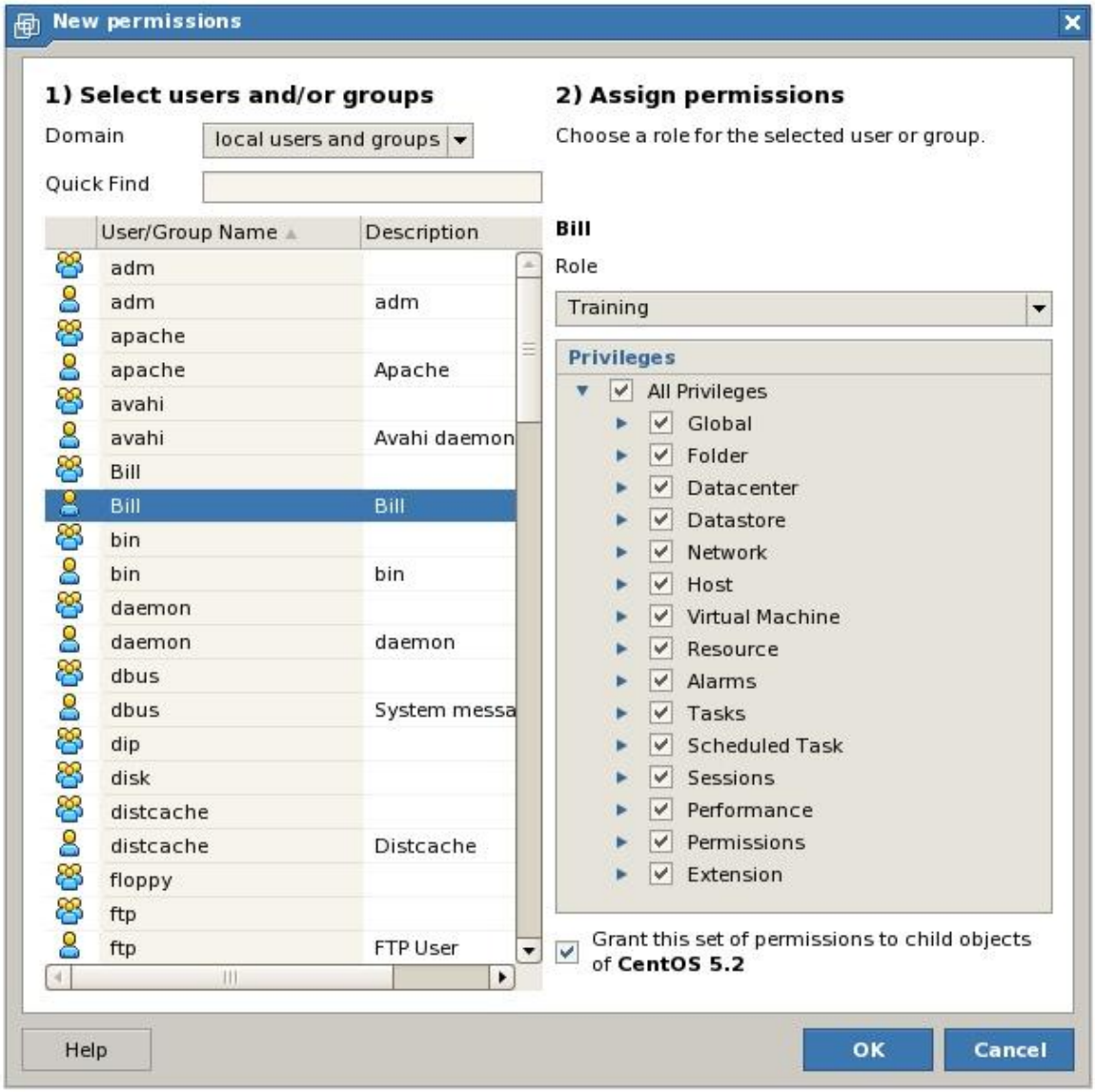
Τα permissions στον VMware Server τα διαχειρίζεται το VI Web Access interface. Όταν ένας χρήστης εισέρχεται στο σύστημα με τα κατάλληλα διοικητικά προνόμια (administrative privileges) επιλέγει τον host ή το virtual machine στο οποίο προορίζεται να συνδεθεί το νέο permission από τον κεντρικό κατάλογο.

Η διαδικασία δημιουργίας νέου permission φαίνεται στο παρακάτω σχήμα:



Εικόνα 9.4.1: Users/Groups and Permissions

Πολλές από τις επιλογές μπορούν να χρησιμοποιηθούν για να ρυθμίσουν τα access privileges για κάποιο permission. Αυτό φαίνεται στο παρακάτω σχήμα:



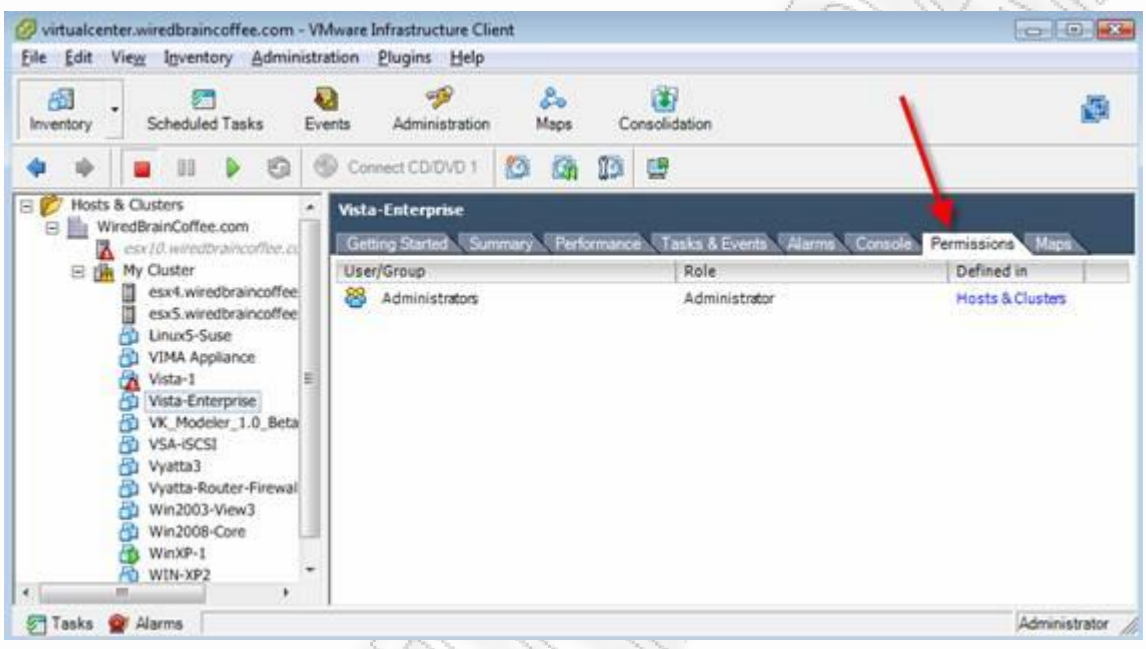
Εικόνα 9.4.2: Assign Permissions

Στα παραπάνω σχήματα βλέπουμε ότι έχουμε τη δυνατότητα να δημιουργήσουμε, να αλλάξουμε και να διαγράψουμε permissions.

9.5 Using Roles to secure your VMware ESX Infrastructure

Όλα τα [14] σύγχρονα λειτουργικά συστήματα όπως τα Windows και το Linux έχουν συγκεκριμένα security roles. Στα Windows, για παράδειγμα, μπορεί να υπάρχει ένας print server operator, ένας server administrator ή ένας backup operator. Αυτοί είναι κάποιοι έτοιμοι (built-in) ρόλοι που τα Windows ονομάζουν «built-in groups» που έχουν οριστεί ειδικά windows δικαιώματα για να εκτελούν κάποια actions. Το VMware δεν είναι διαφορετικό από αυτά τα λειτουργικά συστήματα, από την άποψη ότι έχει και αυτό τους δικούς του ενσωματωμένους (built-in) ρόλους ασφάλειας όπως επίσης παρέχει και τη δυνατότητα για δημιουργία νέων ρόλων ασφάλειας.

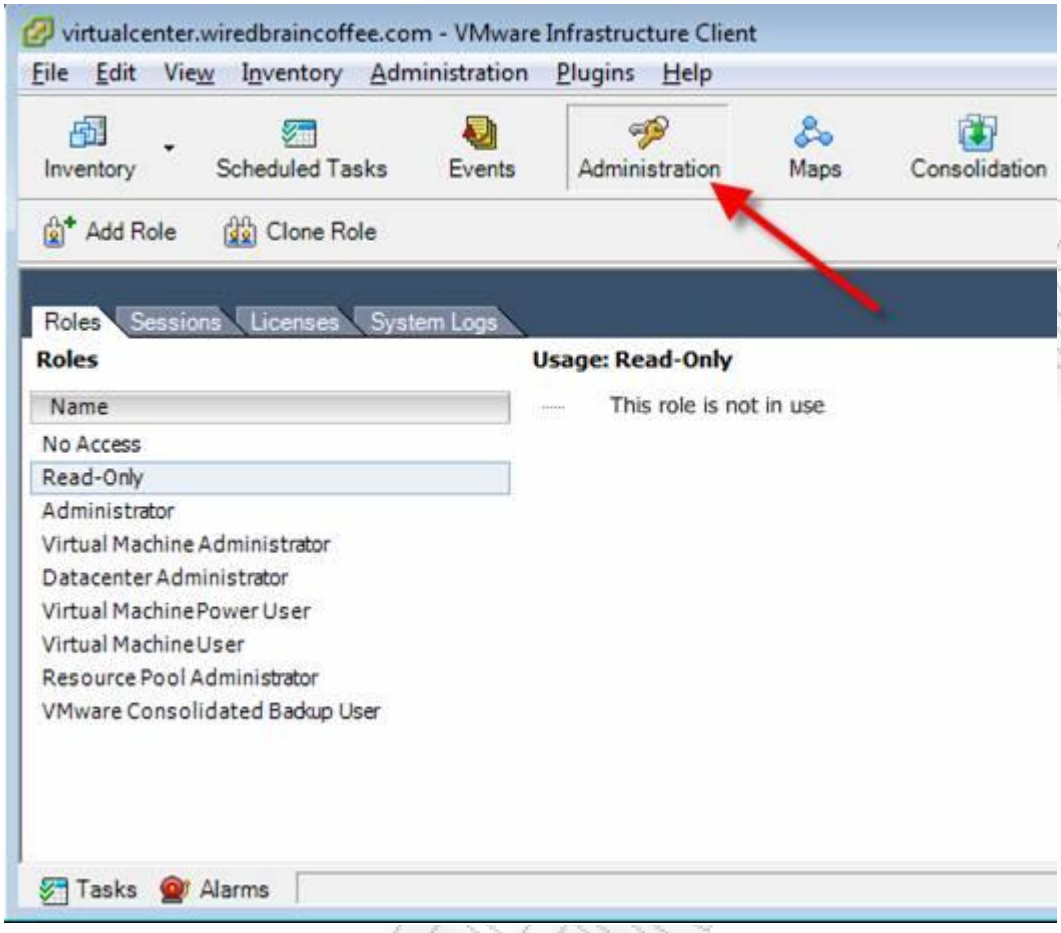
Στο VMware ESX & Virtual Infrastructure η ασφάλεια ρυθμίζεται σε πολλά επίπεδα με χρήση permissions. Τα permissions είναι ο πυρήνας της ασφάλειας του VMware infrastructure. Αυτά τα permissions είναι ένας συνδυασμός από user/group και ρόλους ασφαλείας που είναι ορισμένοι σε κάποια επίπεδα του VMware Infrastructure.
Αν χρησιμοποιούμε VMware ESX ή ESXi χωρίς το vCenter, τα permissions είναι ορισμένα στον ESX host και στο επίπεδο του VM guest. Με το vCenter έχουμε περισσότερα επίπεδα ασφάλειας όπου μπορούν να οριστούν permissions.



Εικόνα 9.5.1: Permissions

Από το παραπάνω σχήμα φαίνεται πως το permission tab δείχνει το user/group και τους ρόλους μέσα από τα permissions που έχουν οριστεί σε αυτό το VM Guest. Από αυτό το tab επίσης φαίνεται πού έχουν οριστεί τα permissions.
Από το παραπάνω σενάριο φαίνεται ότι το permission δεν είναι ουσιαστικά ορισμένο στο επίπεδο του VM Guest. Το permission είναι ορισμένο στο Hosts & Clusters επίπεδο (το μεγαλύτερο επίπεδο του VMware Infrastructure Inventory).
Οι ρόλοι φαίνονται και είναι ορισμένοι στο Administration View.
Η συγκεκριμένη όψη περιλαμβάνει:

- Ρόλους
- Sessions – Ποιος είναι μέσα στο vCenter
- Licenses – Τι είδους άδειες χρησιμοποιούμε, τι τύπου, σε ποιους servers και πόσοι υπολείπονται
- System Logs – VMware ESX & vCenter system logs



Εικόνα 9.5.2: Administration

Στην προβολή των ρόλων μπορούμε να δούμε τους ρόλους ασφάλειας που είναι ήδη έτοιμοι στο VMware Infrastructure. Μερικοί από τους ήδη έτοιμους ρόλους του VMware Infrastructure είναι:

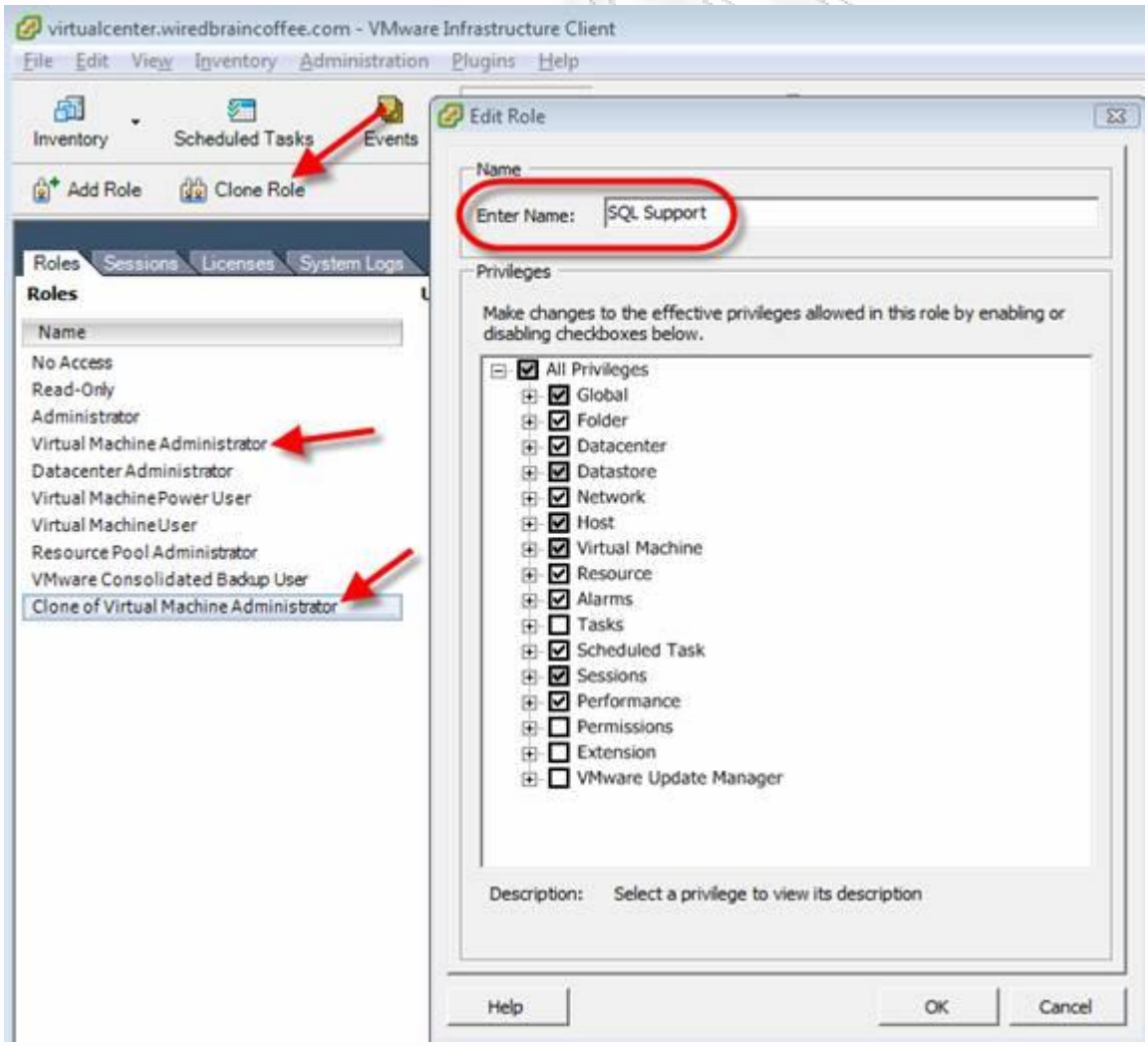
- **Read-Only**: Το security group που είναι συνδεδεμένο με αυτό το ρόλο θα έχει μόνο τη δυνατότητα να βλέπει την κατάσταση αυτού του object. Για παράδειγμα, μπορεί το IT Support Help Desk group να έχει read-only access σε όλα τα VMs για να μπορούν να βλέπουν αν ένα VM είναι ανοικτό ή κλειστό.
- **Administrator:** Ο παντοδύναμος ρόλος που έχει ο administrator user σε ολόκληρη την υποδομή. Δεν πρέπει να ορίζουμε αυτόν τον ρόλο σε κάθε χρήστη και σε κάθε group, αλλά να είμαστε πιο επιλεκτικοί. Ουσιαστικά πρέπει να λειτουργούμε με τη λογική του «principle of least privilege» και να ορίζουμε τα λιγότερα privileges που χρειάζονται για να κάνει ένας χρήστης τη δουλειά του. Για παράδειγμα, αν ένας χρήστης χρειάζεται πρόσβαση για να διαχειριστεί ένα single virtual guest machine, πρέπει να του οριστεί ο ρόλος του *virtual machine administrator* που αναλύεται παρακάτω.
- **Virtual Machine Administrator:** Ο ιδεατός ρόλος για να ορίσουμε ένα user ή group που πρέπει να διαχειρίζεται ένα virtual machine ή group από VMs που είναι συγκεκριμένα στην περιοχή τους. Για παράδειγμα, αυτό το σενάριο έχει εφαρμογή σε administrator (DBA) που διαχειρίζεται SQL Server VMs. Πρέπει να αντιστοιχήσουμε στον DBA (ή στο DBA group) αυτόν το ρόλο σε αυτά τα VMs. Ακόμη καλύτερα μπορούμε να δημιουργήσουμε έναν κατάλογο στο virtual infrastructure, να τοποθετήσουμε τους SQL servers και να ορίσουμε στο DBA group τον ρόλο Virtual Machine Administrator σε όλο το φάκελο.

- **Data Center Administrator:** Σε μεγάλες virtual υποδομές μπορεί να έχουμε πολλά datacenters που τα διαχειρίζονται πολλαπλά group από administrators. Για να ασφαλίσουμε σωστά και να σχεδιάσουμε αυτό το vCenter, θα δημιουργήσουμε virtual data centers, θα μεταφέρουμε τους αντίστοιχους ESX hosts και VM guests σε αυτά και θα ορίσουμε στο data center τον administrator ρόλο.

Αυτοί οι ρόλοι μπορούν να οριστούν και ως εξής:

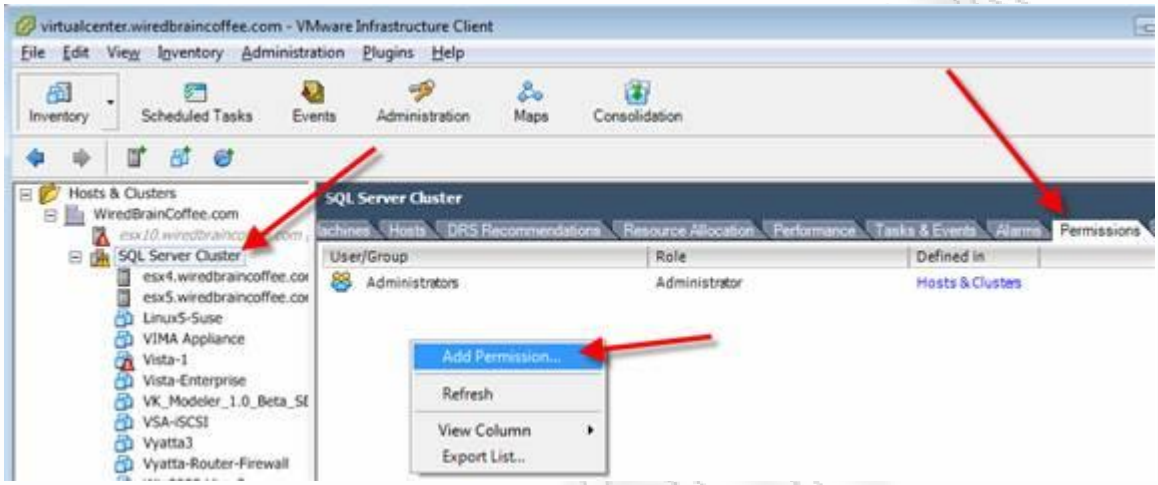
- **Administrator**: Ο ρόλος αυτός μπορεί να ανατεθεί στο Windows Administrators security group.
- **Read only:** Ο ρόλος αυτός μπορεί να ανατεθεί στο help desk group.

Σίγουρα οι default ρόλοι είναι πολύ χρήσιμοι, ωστόσο η δημιουργία custom roles είναι πάντα αναγκαία.
Για παράδειγμα, για να δημιουργήσουμε έναν SQL Server DBA Support Role μπορούμε να κλωνοποιήσουμε έναν ήδη υπάρχοντα ρόλο. Επιλέγοντας τον **Virtual Machine Administrator Role** δημιουργούμε έναν **Clone Role.** Έτσι ο νέος ρόλος θα λέγεται **Clone of Virtual Machine Administrator.** Επιλέγοντας rename τον ονομάζουμε **SQL Support.**
Η διαδικασία αυτή φαίνεται στο παρακάτω σχήμα:



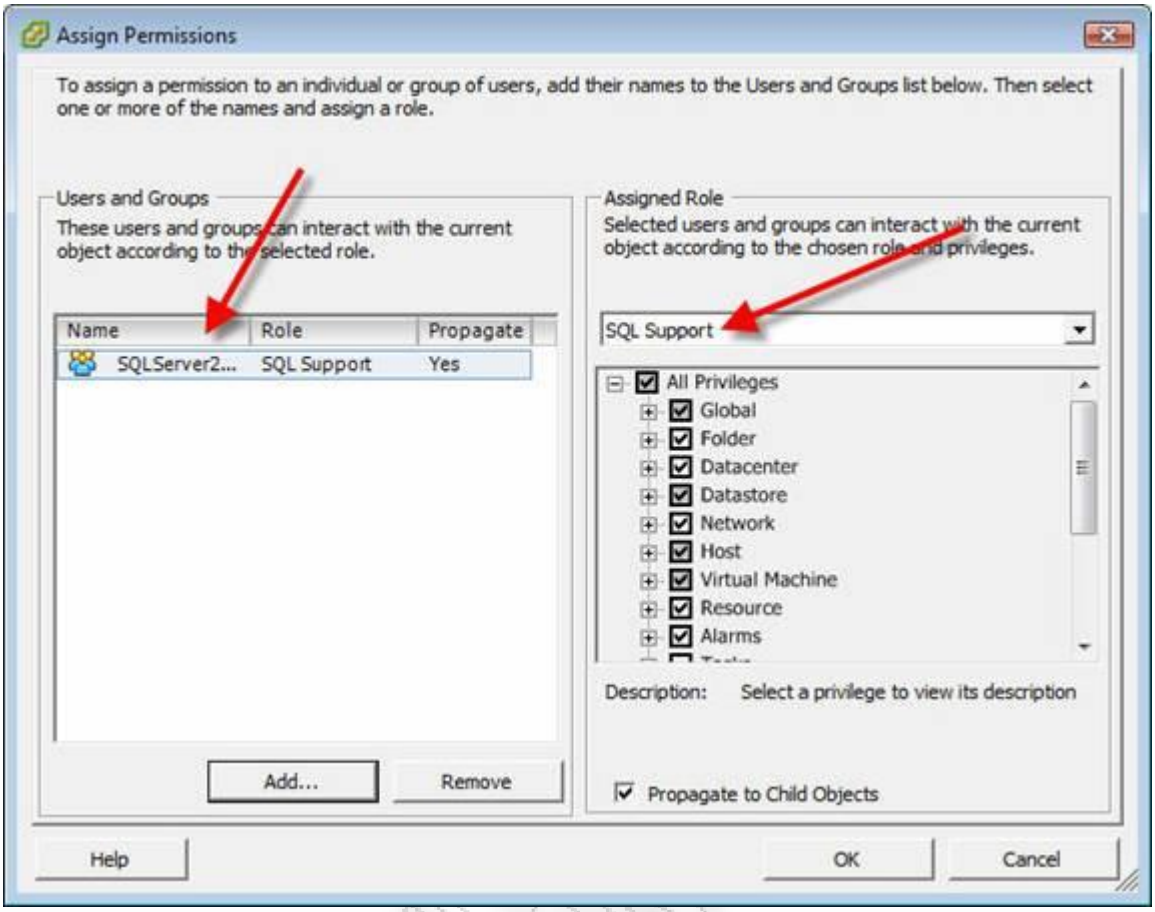
Εικόνα 9.5.3: Roles

Αφού δημιουργήσουμε το νέο ρόλο χρειάζεται να αντιστοιχήσουμε μερικά VMs, ένα φάκελο ή cluster στην virtual υποδομή μας. Για παράδειγμα, έστω ότι έχουμε ένα DRS/HA Cluster που λέγεται SQL Server Cluster. Στο συγκεκριμένο λοιπόν cluster στο permission tab μπορούμε να εισάγουμε permissions. Η δυνατότητα αυτή φαίνεται στο παρακάτω σχήμα:



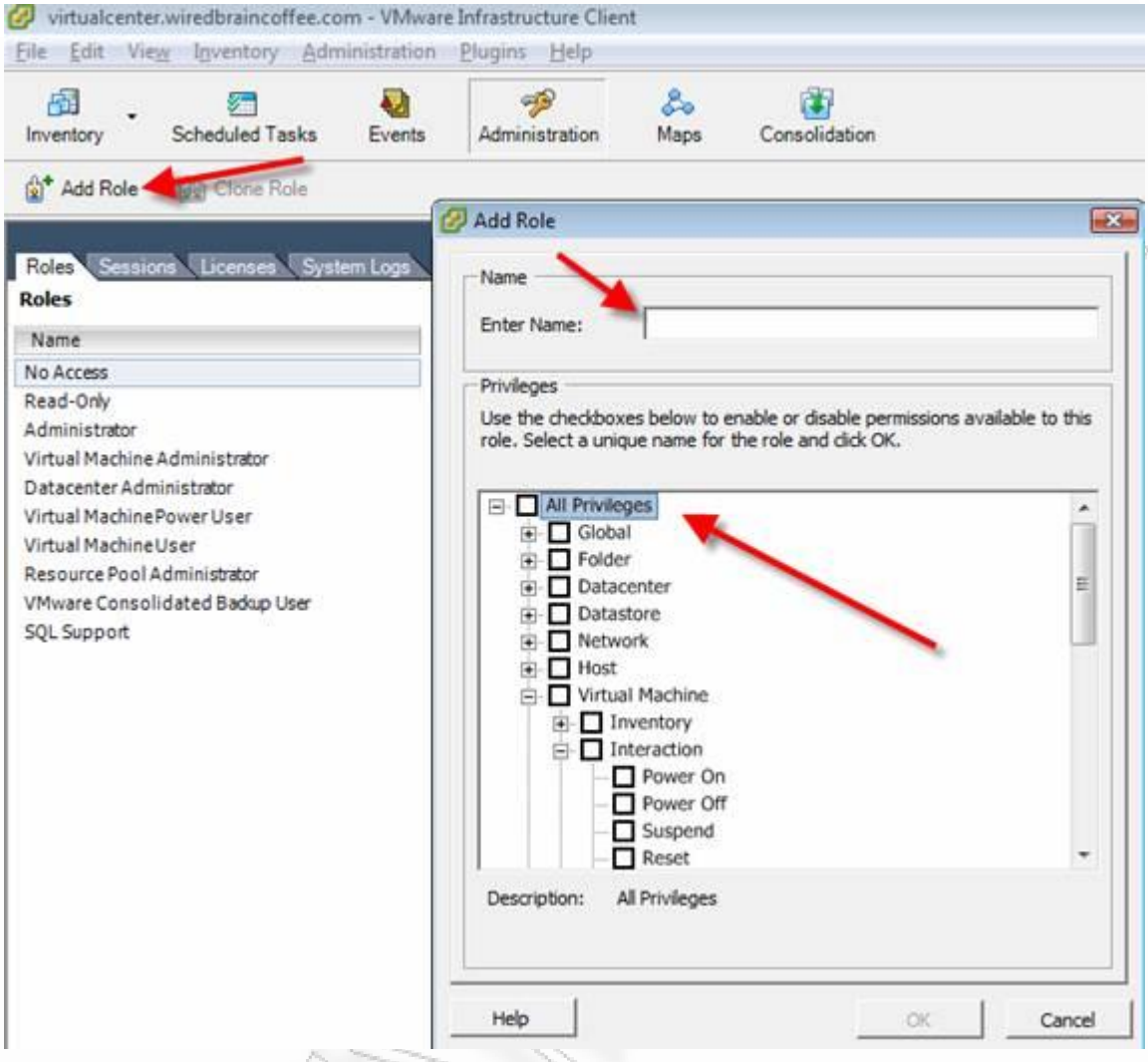
Εικόνα 9.5.4: Add Permissions

Στον καινούργιο ρόλο που έχουμε δημιουργήσει μπορούμε να εισάγουμε έναν νέο χρήστη ή group. Στη συγκεκριμένη περίπτωση μπορούμε να επιλέξουμε το SQLServer2005AdminGroup που έχουμε ήδη δημιουργήσει. Έτσι έχουμε έναν νέο custom ρόλο σε ολόκληρο το cluster. Επειδή έχουμε κάνει copy τον virtual machine administrator ρόλο αυτό, το group των SQLAdmins θα έχει τη δυνατότητα να διαχειρίζεται μόνο guest virtual machines στο cluster και όχι το ίδιο το cluster ή τον ESX server στο cluster. Η διαδικασία αυτή φαίνεται στο παρακάτω σχήμα:



Εικόνα 9.5.5: Assign Permissions

Αντί να χρησιμοποιήσουμε έναν υπάρχοντα ρόλο μπορούμε να δημιουργήσουμε έναν νέο. Αυτή η διαδικασία φαίνεται στο παρακάτω σχήμα:



Εικόνα 9.5.6: Add Role

Παρακάτω δίνονται δύο παραδείγματα άλλων τρόπων με τους οποίους μπορούν να χρησιμοποιηθούν οι custom ρόλοι:

- Virtual Machines Power Off/On: Αυτός ο συγκεκριμένος ρόλος μπορεί να οριστεί σε έναν admin για ένα συγκεκριμένο application ενός virtual machine.
- Console Interaction: Αυτός ο ρόλος συνδέεται με το δικαίωμα του virtual machine power off/on. Αυτό το δικαίωμα επιτρέπει σε ένα χρήστη να εκτελέσει ένα VM guest console remote control.

10. VMware vShield Framework

Για πολλούς οργανισμούς που αποσκοπούν στο να χρησιμοποιήσουν τα οφέλη του Cloud Computing χωρίς να θυσιάσουν την ασφάλεια και τον έλεγχο, η οικογένεια λύσεων ασφάλειας VMware vShield [15] εξασφαλίζει ευρεία προστασία για εικονικά datacenters και συνθήκες cloud. Το vShield επιτρέπει στους οργανισμούς να ενισχύσουν τις εφαρμογές και την ασφάλεια των δεδομένων παρέχοντας προστασία απέναντι στους εισβολείς του δικτύου, βελτιώνοντας την απόδοση σε ιούς, προστατεύοντας από κακόβουλα προγράμματα, βελτιώνοντας τον έλεγχο των ευαίσθητων δεδομένων και επιτυγχάνοντας τη συμμόρφωση μέσα στην εταιρεία-επιχείρηση.

10.1 Cloud Security Challenges

Αρκετοί οργανισμοί επιλέγουν μια Cloud Computing προσέγγιση για να αυξήσουν την ευστροφία και να μειώσουν τα κόστη. Παρ' όλα αυτά, πρόσφατες μελέτες καταναλωτών τοποθετούν την ασφάλεια και τον έλεγχο ως τα πρωτεύοντα ενδιαφέροντα.
Συνεπώς, οι οργανισμοί ψάχνουν να βρουν τρόπους για να λύσουν αυτά τα θέματα, έτσι ώστε να χρησιμοποιήσουν το Cloud Computing χωρίς συμβιβασμούς ως προς την ασφάλεια και τον έλεγχο.

ΠΡΟΚΛΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΟ CLOUD

Application and Data Security: • Σύγχρονες λύσεις του cloud δεν παρέχουν στις επιχειρήσεις τα εξελιγμένα εργαλεία που χρειάζονται ώστε να διασφαλίσουν τις εφαρμογές ή να εμποδίσουν την απώλεια και τη διαρροή δεδομένων
Visibility and Control: • Σύγχρονες λύσεις του cloud δεν παρέχουν στους διαχειριστές ασφαλείας την ορατότητα που χρειάζονται για να ελέγχουν τις τακτικές ασφάλειας κατά τη διάρκεια του κύκλου ζωής από τον ορισμό, στην εφαρμογή, την επιβολή και τον έλεγχο
Compliance Management: • Οι περισσότερες επιχειρήσεις διαθέτουν ήδη εργαλεία, τεχνολογίες και διαδικασίες για να διαχειρίζονται τις ρυθμίσεις του ελέγχου, και χρειάζονται λύσεις cloud που δε θα παρακωλύουν τη δυνατότητα να έχουν γρήγορα τον έλεγχο

10.2 Ασφάλεια στο Cloud με VMware vShield

Όσο το virtualization είναι απαραίτητο για να μεταφέρει τις εφαρμογές στη νέα υποδομή cloud, η vShield είναι ένα κλειδί ασφαλείας για το περιβάλλον Cloud Computing. Η VMware παρέχει ασφάλεια και αξιόπιστες λύσεις για το virtualization για παραπάνω από μια δεκαετία. Σήμερα η VMware βοηθάει να απελευθερωθούν τα οφέλη του Cloud Computing με τη νέα οικογένεια προϊόντων ασφαλείας VMware vShield για virtual datacenters και cloud περιβάλλοντα.

Τα προϊόντα αυτά βοηθούν την επιχείρηση να υιοθετήσει ένα μοντέλο cloud που ανταποκρίνεται στις ανάγκες της επιχείρησης και να μπορέσει να διεκπεραιώσει το πιο σημαντικό cloud με ασφάλεια.

10.3 Οφέλη από το VMware vShield

- Πίσω από τους περιορισμούς της φυσικής ασφάλειας

Οι λύσεις VMware vShield παρέχουν προσαρμοστική ασφάλεια που μεταφέρεται με virtual machines καθώς μεταναστεύουν από host σε host, ώστε οι επιχειρήσεις να μπορέσουν με ασφάλεια να υποστηρίξουν τα virtual machines σε δυναμικά περιβάλλοντα Cloud Computing. Αυτή η προσέγγιση βοηθάει επίσης να διασφαλιστεί ότι οι εφαρμογές τρέχουν αποτελεσματικά στο περιβάλλον Cloud Computing, ενώ παράλληλα διατηρούν τον μερισμό των χρηστών και των ευαίσθητων δεδομένων.

- Βελτίωση και απλοποίηση της εφαρμογής ασφάλειας σε εννιαίο πλαίσιο

Μέσα σε ένα εννιαίο και περιεκτικό πλαίσιο, η VMware vShield διασφαλίζει virtual datacenters και περιβάλλοντα cloud σε όλα τα επίπεδα: φιλοξενία, δίκτυο, εφαρμογή, δεδομένα και endpoint. Βοηθάει επίσης να διασφαλιστεί ότι η σωστή/ορθή κατάτμηση και οι ζώνες εμπιστοσύνης επιβάλλονται σε όλα τα application deployments που είναι σε βασική υλοποίηση VMware Cloud. Η vShield μαζί με τις δυνατότητες ενδοσκόπησης της πλατφόρμας VMware παρέχουν μια ολοκληρωμένη σειρά δυνατοτήτων για να προστατεύσουν τους hosts και τα virtual machines. Αυτά τα χαρακτηριστικά μαζί με τις αξιόπιστες λύσεις από τους συνεργάτες της VMware οδηγούν στο συμπέρασμα ότι τα cloud της VMware παρέχουν μια άριστη και ασφαλή προστασία για τις εφαρμογές και τα δεδομένα.

- Μείωση της πολυπλοκότητας και εξάλειψη των antivirus storms

Η vShield βοηθάει στη μείωση της πολυπλοκότητας της ασφάλειας του virtualization επιτρέποντας στις επιχειρήσεις να σταθεροποιούν τις υποδομές ασφάλειας και να εξαλείφουν την αταξία που συνδέεται με software agents, πολιτική ασφαλείας, εφαρμογές ασφαλείας και κενές λύσεις. Η vShield εμποδίζει τα antivirus storms που συνδέονται με τα endpoints security agents εξαλείφοντας την ανάγκη εγκατάστασης λογισμικού antivirus σε μεμονωμένες μονάδες (virtual machines).

- Προστασία των εφαρμογών και επιτάχυνση της συμμόρφωσης του IT

Η vShield προστατεύει τις εφαρμογές στο virtual datacenter από τις επιθέσεις που προέρχονται από το δίκτυο. Οι επιχειρήσεις κερδίζουν ορατότητα και έλεγχο στις επικοινωνίες του δικτύου ανάμεσα στα virtual machines. Η εφαρμογή της πολιτικής είναι ευκίνητη εφόσον βασίζεται σε λογικές δομές συμπεριλαμβάνοντας την μίξη της VMware vCenter και την ασφάλεια της VShield και όχι μόνο τις φυσικές δομές όπως η IP address. Η vShield ανιχνεύει για ευαίσθητα δεδομένα όπως αριθμούς πιστωτικής κάρτας μέσω εικονικών πηγών. Εξαπατήσεις της πολιτικής αναφέρονται αναλυτικά δίνοντας τη δυνατότητα στους οργανωτές του IT να

επαναπροσδιορίσουν την κατάσταση του ελέγχου με διεθνείς ρυθμίσεις και κανονισμούς ασφαλείας από όλον τον κόσμο.

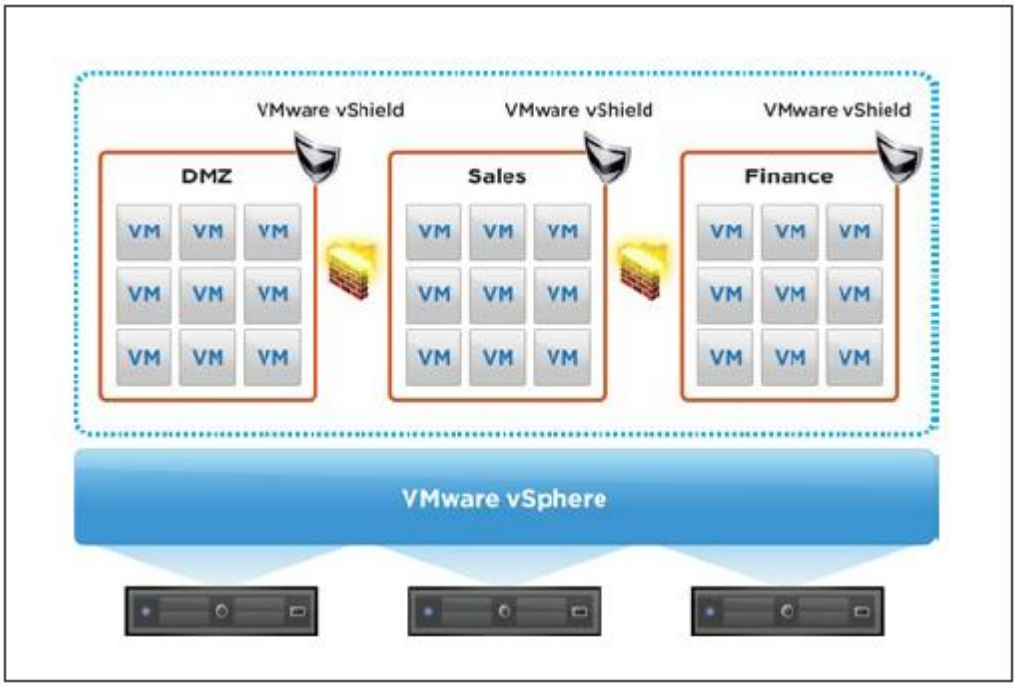
- Επιρροή των υπαρχόντων λύσεων ασφαλείας

Η vShield είναι σχεδιασμένη να εργάζεται απρόσκοπτα με τις υπάρχουσες λύσεις ασφαλείας του IT μέσω της Representational State Transfer (REST) APIs, η οποία επιτρέπει λύσεις για την ολοκληρωμένη ενσωμάτωση των δυνατοτήτων της vShield σε εξωτερικές λύσεις ασφαλείας. Επιπροσθέτως η vShield συμπεριλαμβάνει ένα τερματικό (endpoint) ασφαλείας API, το οποίο ισχυροποιεί την ενσωμάτωση με τις ήδη υπάρχουσες antivirus και anti-malware λύσεις, καθώς επίσης αντικατοπτρίζει σε ευρύτερες λύσεις ασφάλειας για την ασφάλεια των πληροφοριών, των εφαρμογών, την προστασία διαρροής των πληροφοριών, την αλλαγή και διαμόρφωση του ελέγχου.

10.4 Χρησιμοποιώντας την VMware vShield

Ασφάλεια στην εργασία – Σημαντικές εφαρμογές
Οι λύσεις που δίνει η vShield διευκολύνουν τους πελάτες να υποστηρίξουν τις εφαρμογές που ανήκουν σε διαφορετικά επίπεδα αξιοπιστίας (trust) από το ίδιο το virtual datacenter.
Το hypervisor firewall επίπεδο της vShield διασφαλίζει ότι ο σωστός μερισμός και οι ζώνες αξιοπιστίας επιβάλλονται για όλες τις εφαρμογές ανάπτυξης.

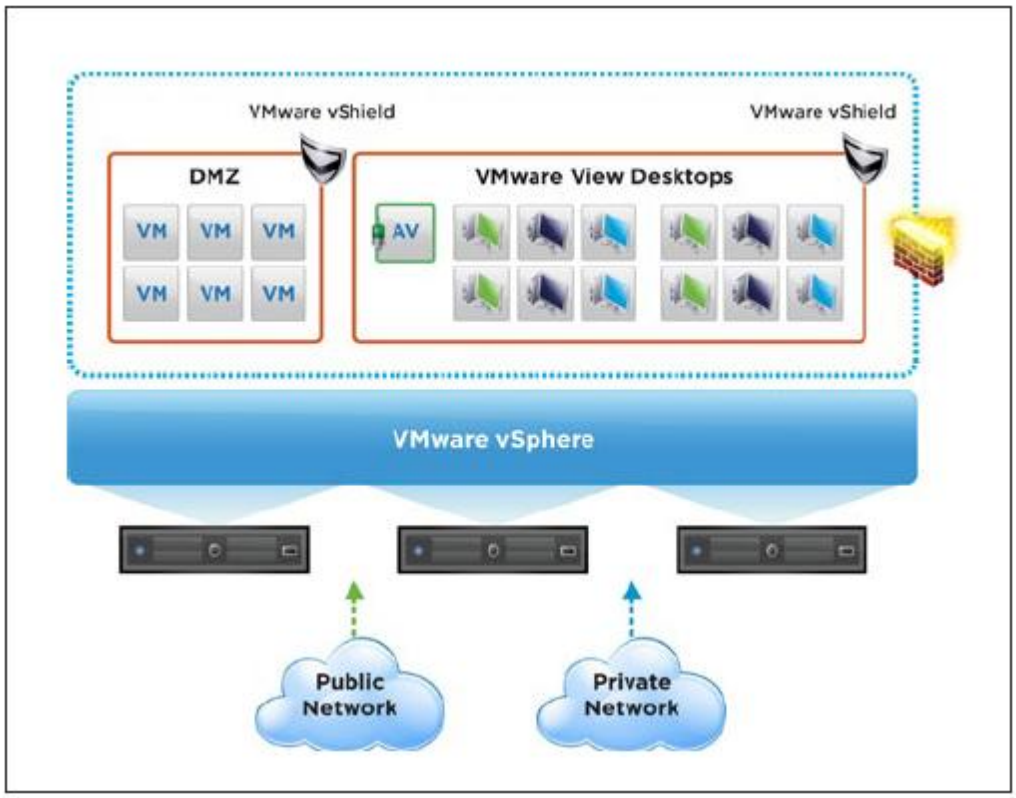
Ασφαλείς virtual εφαρμογές ανάπτυξης του desktop
Μέσω της συγχώνευσης με το VMware View η vShield δίνει την δυνατότητα να αναπτυχθούν πιο αποτελεσματικά antivirus και anti-malware για τα virtual endpoints και τις εφαρμογές. Αυτό γίνεται απαλλάσσοντας ειδικά antivirus και anti-malware functions από τα μεμονωμένα virtual machines και μεταφέροντάς τα σε μια πιο ασφαλή εικονική εφαρμογή η οποία προστατεύει τον host και όλα τα virtual machines που είναι πάνω σε αυτήν την εφαρμογή. Αυτή η προσέγγιση εκσυγχρονίζει την εφαρμογή της ασφάλειας και παρέχει επιπρόσθετη προστασία ενάντια στα antivirus «storms», botnet απόδοσης και botnet επίθεσης.
Η δυνατότητα αυτή φαίνεται στο παρακάτω σχήμα:



Εικόνα 10.4.1: vShield

Η vShield επίσης βοηθάει τις επιχειρήσεις να δημιουργήσουν λογικά μέτρα ασφαλείας σε virtual desktop υποδομές μέσω ολικής απομόνωσης του δικτύου και μιας συστάδας εξόδων δικτύου όπως είναι τα firewalls, τα VPN's και τα DHCP.

Μείωση του κινδύνου μη συμμόρφωσης με την ανακάλυψη των ευαίσθητων δεδομένων
Οι επιχειρήσεις μπορούν να χρησιμοποιήσουν τις εφαρμογές της vShield για την ασφάλεια των δεδομένων ώστε να ανακαλύψουν με ακρίβεια και να αναφέρουν ευαίσθητα δεδομένα σε μη δομημένα αρχεία. Με περισσότερα από 80 προκαθορισμένα templates που δίνονται με ακριβείς οδηγίες για τη χώρα και την βιομηχανία που θα χρησιμοποιηθούν , γρήγορα ταυτίζεται και αναφέρει έκθεση ευαίσθητων δεδομένων. Επιπροσθέτως, βελτιώνει την απόδοση μεταφέροντας λειτουργίες δεδομένων σε μια πιο virtual εφαρμογή / παραλλαγή.
Οι δυνατότητες αυτές φαίνονται στο παρακάτω σχήμα:



Εικόνα 10.4.2: vShield Public/Private Network

Ασφαλή multi-tenant περιβάλλοντα

Οι λύσεις της vShield διευκολύνουν τις επιχειρήσεις και την υπηρεσία του Cloud Computing να υποστηρίξουν γειτονικά IT περιβάλλοντα (multi-tenant IT environments) να μοιράζουν με ασφάλεια τις πηγές του δικτύου δημιουργώντας λογικές ζώνες ασφαλείας και να παρέχουν ολοκληρωμένη απομόνωση του δικτύου για τα εικονικά datacenters. Η vShield επίσης παρέχει έλεγχο και ορατότητα στην κίνηση της εξόδου (gateway) του τερματικού του δικτύου, σε συνδυασμό με τις παροχές VPN, ώστε να προστατεύσει την εχεμύθεια και την ακεραιότητα των επικοινωνιών ανάμεσα στα εικονικά datacenters.

10.5 Οι λύσεις της vShield

- vShield Edge

Η vShieldEdge είναι μια λύση εξόδου του δικτύου η οποία προστατεύει τα edges του εικονικού datacenter με την DHCP, το Network Address Translation (NAT), το firewalling, το load balancing, το site to site VPN, το port group isolation και άλλες δυνατότητες που βοηθούν τις επιχειρήσεις να διατηρήσουν την ανάλογη κατάτμηση / μερισμό ανάμεσα σε διαφορετικές μονάδες οργάνωσης.

- Για την ασφάλεια των δεδομένων

Η vShieldApp μαζί με το data security προστατεύει τις εφαρμογές και τα δεδομένα στο virtual datacenter από απειλές που βασίζονται στο δίκτυο. Δίνει τη δυνατότητα στις επιχειρήσεις να δημιουργήσουν και να εφαρμόσουν πολιτικές που συνδέονται με την επιχείρηση, οι οποίες συνδέονται με δυναμικά cloud environments. Επίσης παρέχει βαθιά ορατότητα στις επικοινωνίες του δικτύου, ανάμεσα στα virtual machines μέσω του δικτύου ασφαλείας. Επίσης περιλαμβάνει την ανακάλυψη μη κρυπτογραφημένων ευαίσθητων δεδομένων, όπως οι πιστωτικές κάρτες, τα οποία φυλάσσονται σε υπάρχοντα αρχεία στις εικονικές μηχανές. Με αυτές τις λύσεις, οι διαχειριστές έχουν τη δυνατότητα να ελέγχουν διεξοδικά τα datacenters, τα clusters ή τα resource pools για την παρουσία ευαίσθητων δεδομένων. Οι διαχειριστές μπορούν να χρησιμοποιήσουν τα REST APIs ώστε να βάλλουν σε καραντίνα τα μολυσμένα αρχεία.

- vShield Endpoint

Η vShield Endpoint ενισχύει την ασφάλεια στις εικονικές μηχανές και παράλληλα βελτιώνει την απόδοση για την προστασία των endpoints σε σημεία με μεγάλη σπουδαιότητας. Η vShield Endpoint μεταφέρει antivirus και anti-malware agent processing σε μια αφοσιωμένη και ασφαλή εικονική εφαρμογή, η οποία παρέχεται από την VMware. Η λύση είναι σχεδιασμένη ώστε να επηρεάζει ήδη υπάρχουσες επενδύσεις για εικονικά περιβάλλοντα με την ίδια επιφάνεια εφαρμογής που χρησιμοποιούν για να ασφαλίσουν τα φυσικά περιβάλλοντα.

- vShield Bundle

Η vShield Bundle περιλαμβάνει τα ακόλουθα προϊόντα από την οικογένεια vShield: vShield Edge, vShield App με Data Security, vShield Endpoint και vShield Manager.

- vShield Manager

Συμπεριλαμβανομένων όλων των προϊόντων της vShield, η vShield Manager παρέχει ένα κεντρικό σημείο ελέγχου για την εφαρμογή, την αναφορά, την είσοδο και την ενσωμάτωση εξωτερικής κατασκευής υπηρεσιών ασφαλείας. Σε συνδυασμό με τον vCenter Server, η vShield Manager επιτρέπει την πρόσβαση για έλεγχο , για **role based access control** και διαχωρισμό καθηκόντων σαν ένα μέρος ενός ενοποιημένου πλαισίου για την εφαρμογή της εικονικής ασφάλειας.

- vShield Zones

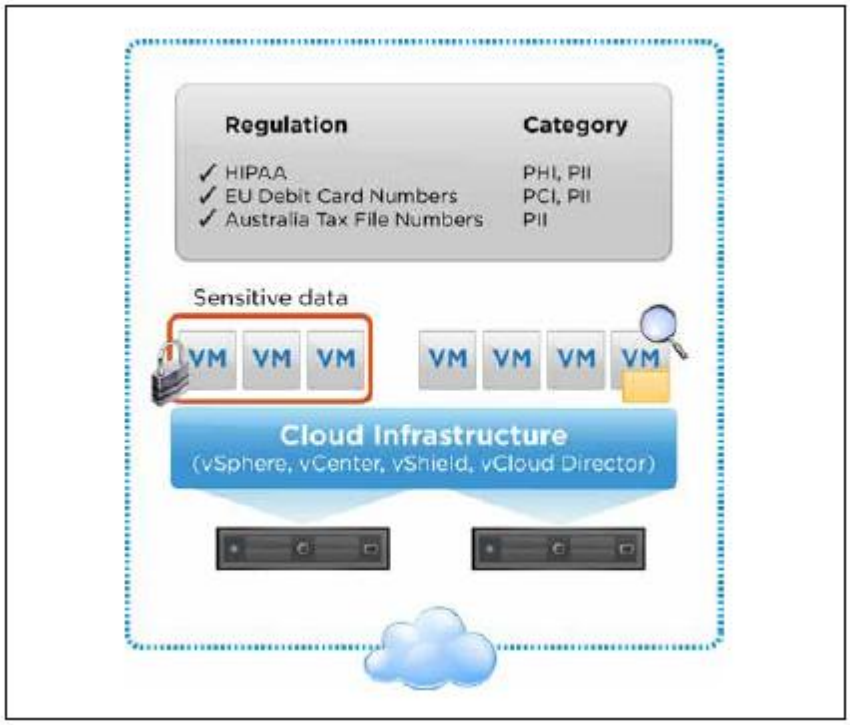
Τα vShield Zones μαζί με το vSphere παρέχουν βασική προστασία από απειλές που βασίζονται στο δίκτυο των εικονικών datacenters. Υπάρχουν εφαρμογές firewalling και εφαρμοσμένη πολιτική ασφάλειας βασισμένα σε ζώνες που καθορίζονται από τους διαχειριστές χρησιμοποιώντας τη βασική κίνηση της πληροφορίας, όπως η IP Address και η πόρτα κατεύθυνσης.

10.6 VMware vShield App with Data Security

Η VMware vShield App with DataSecurity [16] ανήκει στην οικογένεια των προϊόντων εικονικής ασφάλειας της VMware vShield που προστατεύει τις εφαρμογές και τα δεδομένα στο εικονικό Datacenter από τις επιθέσεις δικτύου. Οι επιχειρήσεις κερδίζουν ορατότητα και έλεγχο στις επικοινωνίες του δικτύου ανάμεσα στις εικονικές μηχανές. Το προϊόν επίσης σκανάρει μέσω virtualized workloads για ευαίσθητα δεδομένα, όπως οι πιστωτικές κάρτες, και αναφέρει

παραβιάσεις των κανονισμών (όπως το PCI-DSS), παρέχοντας διευκόλυνση των οργανώσεων ΤΟ, για να αξιολογήσει γρήγορα την κατάσταση της συμμόρφωσης με τους κανονισμούς σε όλο τον κόσμο.
Με την VMware vShield App with DataSecurity μας δίνεται η δυνατότητα να έχουμε:

- Αυξημένη ορατότητα και έλεγχο στις επικοινωνίες του δικτύου ανάμεσα στις εικονικές μηχανές.
- Μείωση του κίνδυνου μη συμμόρφωσης/έλεγχου μέσω της ορατότητας στα ευαίσθητα δεδομένα που είναι αποθηκευμένα στις εικονικές μηχανές.
- Μείωση της ανάγκης για αφοσιωμένο λογισμικό (hardware) και VLANs, ώστε οι ομάδες ασφάλειας να ξεχωρίσουν μεταξύ τους.
- Βελτιστοποίηση της πηγής χρήσης του λογισμικού (hardware), διατηρώντας παράλληλα ισχυρή ασφάλεια.
- Απλοποίηση του έλεγχου με τη λεπτομερή καταγραφή του δικτύου των δραστηριοτήτων όλων των εικονικών μηχανημάτων.



Εικόνα 10.6: vShield App with Data Security

Αυτό το προϊόν συνδέεται άμεσα με την VMware vSphere ώστε να προστατεύει ενάντια στις εσωτερικές απειλές του δικτύου και να μειώνει τον κίνδυνο των παραβιάσεων μέσα στην περίμετρο της ασφάλειας. Για να το κατορθώσει αυτό, το προϊόν χρησιμοποιεί application – aware firewalling με βαθιά ενδοσκόπηση και σύνδεση έλεγχου βασιζόμενη στο source και το destination IP address.
Επίσης, απλοποιεί την πολιτική της ασφάλειας με το να παρέχει στο IT γρήγορη δημιουργία ομάδων ασφάλειας που συνδέονται με την επιχείρηση, καθώς η ροή του έλεγχου βοηθά το IT να αναλύσει το virtual machine network traffic και να ενδυναμώσει δυναμικά την ασφάλεια στην πολιτική των ομάδων. Οι διαχειριστές μπορούν να ελέγξουν κεντρικά την vShield App με Data Security διά μέσου της κονσόλας της vShield Manager, η όποια ενσωματώνεται με τον VMware vCenter Server ώστε να διευκολύνει την ενοποιημένη ασφάλεια για τα virtual datacenters.

Επιπλέον, διαθέτει μια διαχειριστική κονσόλα για να ελέγχει τα ευαίσθητα δεδομένα. Οι διαχειριστές ακολουθούν μια λογική , επιλέγοντας ρυθμίσεις οι οποίες μπορούν να εφαρμοστούν ώστε να σκανάρουν τον στόχο μέσα στα containers των εικονικών μηχανημάτων-datacenters, clusters and resource pools. Τα αρχεία που πρόκειται να σκαναριστούν μπορούν να φιλτραριστούν από το extension του αρχείου, το μέγεθος ή την τροποποιημένη ημερομηνία. Scan output μπορεί να αναγνωρίσει τα datacenters, τα clusters, τα virtual machine και τα filenames που δεν είναι συμβατά με την επιλεγμένη πολιτική. Οι διαχειριστές μπορούν να χρησιμοποιήσουν το Representational State Transfer (REST) APIs για να επανορθώσουν μη συμβατά αρχεία.
Η vShield App με την Data Security εγκαθίσταται σε κάθε host της vSphere και ελέγχει όλη την κίνηση του δικτύου στο host, ακόμα και για τα πακέτα που δεν περνάνε σε physical network interface card (NIC). Επιπλέον, παρέχει ένα κεντρικό interface που επηρεάζει το vCenter Server ώστε να εφαρμόζει αυτές τις πολιτικές σε διαφόρους sphere hosts στο virtual datacenter.
Πως χρησιμοποιείται η vShield App με την Data Security:

- Χρησιμοποιώντας τα REST APIs, οι διαχειριστές έχουν τη δυνατότητα, χειροκίνητα ή προγραμματιστικά (αυτόματα), να σκανάρουν αρχεία ώστε να αξιολογήσουν τον έλεγχο με τις επιλεγμένες πολιτικές.
- Supplied templates επιλέγονται από τον διαχειριστή για να δημιουργήσουν μια πολιτική η όποια έπειτα εφαρμόζεται ενάντια σε συγκεκριμένες εικονικές πήγες .
- Output από τον διεξοδικό έλεγχο των ευαίσθητων δεδομένων τοποθετούνται σε μια αναφορά που χρησιμοποιείται για να αναγνωρίσει και να βάλει σε καραντίνα μη-ελεγχόμενες εικονικές μηχανές.
- Παροχή της application aware protection – Οι διαχειριστές μπορούν να προσδιορίσουν και να ενισχύσουν αυξανόμενες πολιτικές για όλη την κίνηση του δικτύου που διασχίζει ένα εικονικό NIC, αυξάνοντας την ορατότητα μέσα στο εσωτερικό virtual datacenter traffic.
- Διατήρηση της Change-aware protection – Η προστασία των firewall είναι συνεχόμενη καθώς οι εικονικές μηχανές μεταναστεύουν από host σε host, εξασφαλίζοντας ότι οι τυπολογικές αλλαγές του δικτύου δεν έχουν αντίκτυπο στην εφαρμογή της ασφάλειας.
- Αποδοτική εφαρμογή των δυναμικών πολιτικών – Οι διαχειριστές έχουν ένα πλούσιο περιεχόμενο για να προσδιορίζουν και να επαναπροσδιορίζουν τις εσωτερικές πολιτικές των firewall .
- Μείωση των botnet risks – Οι διαχειριστές ασφάλειας έχουν τη δυνατότητα να παρέχουν προστασία από τα botnets και άλλες επιθέσεις αναθέτοντας δυναμικά ports σε αξιόπιστες εφαρμογές.
- Πρόσβαση έλεγχου σε μοιρασμένες πήγες – Οι διαχειριστές ασφάλειας μπορούν να απαγορεύσουν την πρόσβαση σε κοινές υπηρεσίες όπως είναι η αποθήκευση και υποστήριξη εφεδρικών αρχείων στα sphere hosts συμφώνα με την IP address.
- Επιτάχυνση της IT compliance – Η ορατότητα και ο έλεγχος της ασφάλειας του δικτύου στα εικονικά μηχανήματα αυξάνεται και τα logging και auditing controls βοηθούν τις επιχειρήσεις να επιδείξουν συμμόρφωση/υποταγή με τις εσωτερικές πολιτικές και με τις εξωτερικές ρυθμιστικές προϋποθέσεις.

ΒΑΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ:

Ανακάλυψη ευαίσθητων δεδομένων

- Policy Management console επιτρέπει στους διαχειριστές να διαλέξουν τους κανονισμούς που θα χρησιμοποιηθούν στα σκαναρίσματα συμμόρφωσης.

- Οι οργανισμοί έχουν τη δυνατότητα να επιλέξουν ανάμεσα σε περισσότερα από 80 templates κανονισμών, όπως το PII (Personally Identifiable Information), το PCI-DSS cardholder data και το PHI (Protected Health Information), από όλο τον κόσμο (Βόρεια Αμερική, EMEA, Ασία-Ειρηνικός).
- Η αναφορά του output αναγνωρίζει ποιες σκαναρισμένες πήγες περιλαμβάνουν δεδομένα που παραβιάζουν επιλεγμένες οδηγίες συμμόρφωσης.
- Η λειτουργικότητα μπορεί να προγραμματιστεί χρησιμοποιώντας το REST APIs ή την κονσόλα λειτουργίας.
- Τα μολυσμένα εικονικά μηχανήματα μπαίνουν σε κατάσταση καραντίνας και επαναπροσδιορίζονται με το VMware vCenter Configuration Manager.

Firewalls

- Το hypervisor-level firewall παρέχει εσωτερική και εξωτερική σύνδεση έλεγχου, η όποια επιβάλλεται στο εικονικό NIC επίπεδο μέσω επιθεώρησης του hypervisor, υποστηρίζοντας πολλαπλά multihued εικονικά μηχανήματα.
- Το layer 2 firewall (άλλοτε γνωστό ως transparent firewall) προστατεύει εναντίον πολλών τύπων επιθέσεων, όπως το password sniffing, το DHCP snooping, και το top Address Resolution Protocol (ARP) spoofing ή από μολυσμένες επιθέσεις. Επίσης, παρέχει ολοκληρωμένη απομόνωση από τα SNMP traffic.
- Η προστασία είναι δυνατόν να επιβληθεί ανάλογα με το δίκτυο, τη θύρα της εφαρμογής, τον τύπο του πρωτόκολλου (TCP, UDP), και τον τύπο της εφαρμογής.
- Η προστασία είναι δυναμικ,ή καθώς τα εικονικά μηχανήματα μεταναστεύουν/κινούνται.
- Το IP-based tasteful firewall και το application gateway υποστηρίζουν ένα ευρύ φάσμα πρωτοκόλλων, συμπεριλαμβανόμενων της Oracle, του Sun Remote Procedure Call (RPC), του Microsoft RPC, του LDAP και του SMTP. Η έξοδος/τερματικό (gateway) βελτιώνει την ασφάλεια ανοίγοντας sessions (ports) μόνο όταν χρειάζεται.

Flow Monitoring

- Οι διαχειριστές είναι σε θέση να παρατηρήσουν την δραστηριότητα του δικτύου ανάμεσα στα εικονικά μηχανήματα για να καθορίσουν και να επαναπροσδιορίσουν την πολιτική των firewall, να αναγνωρίσουν τα botnets, και να ασφαλίσουν τις διαδικασίες της επιχείρησης μέσω λεπτομερών αναφορών της εφαρμογής της κίνησης του δικτύου (application traffic) .

Ομάδες ασφάλειας

- Οι διαχειριστές μπορούν να προσδιορίσουν τις ομάδες που σχετίζονται με την επιχείρηση οποιωνδήποτε εικονικών μηχανημάτων από τα εικονικά NICs.

Εφαρμογή Πολιτικής

- Η vShield Manager παρέχει έλεγχο των χαρακτηριστικών του προϊόντος, πολλά από τα όποια είναι προστασία από το vCenter Server interface.
- Οι διαχειριστές είναι σε θέση να επιβάλλουν την πολιτική στις ομάδες ασφάλειας και στις ομάδες της vCenter Server Η REST APIs παρέχει μια προγραμματιζόμενη επιφάνεια (programmable interface) για την επιβολή της εφαρμογής και της πολιτικής.
- Το προϊόν υποστηρίζει την ενσωμάτωση με τα εργαλεία της εφαρμογής της ασφάλειας της επιχείρησης.

IP Addressing

- Το ευέλικτο IP addressing περιλαμβάνει την ικανότητα να χρησιμοποιηθεί το ίδιο IP address σε διαφορετικά tenant zones, ώστε να απλοποιηθεί ο εφοδιασμός.

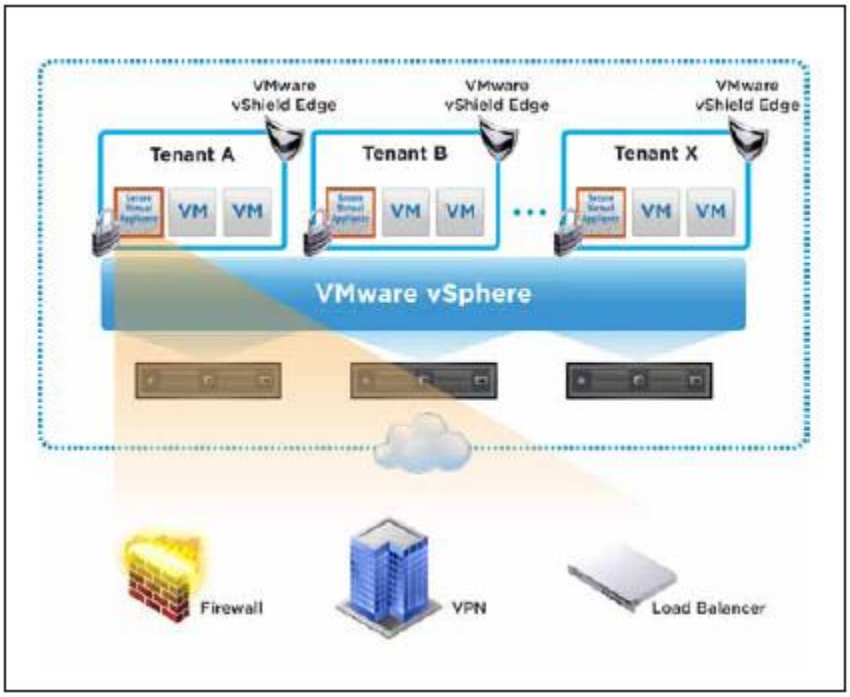
Logging and Auditing

- Το logging βασίζεται στο industry-standard syslog format.
- Η REST APIs και η shield Manager παρέχουν πρόσβαση στα εργαλεία του logging και του auditing.
- Ο διαχειριστής καθορίζει την είσοδο ή έξοδο (logging on and off) για τα firewalls σε επίπεδο κανόνα.

10.7 VMware vShield Edge

Η VMware vShield Edge [17] , μέλος της οικογένειας της VMware vShield, παρέχει μια ευρεία δικτυακή περίμετρο ασφάλειας για τα εικονικά datacenters. Η vShield Edge συνδυάζεται με την VMware vSphere και περιλαμβάνει υπηρεσίες δικτύου εξόδου (network gateway) τις οποίες χρησιμοποιούν οι οργανισμοί ώστε να αυξήσουν με ασφάλεια και με ταχύτητα τις κατασκευές του cloud.
Με την VMware vShield Edge μας δίνεται η δυνατότητα να έχουμε:

- Μείωση του κόστους και της πολυπλοκότητας ελαχιστοποιώντας πολλαπλά μέσα για συγκεκριμένο σκοπό και παρέχοντας με ταχύτητα υπηρεσίες network gateway.
- Διαβεβαίωση για την επιβολή της ασφάλειας με built-in edge ασφάλεια δικτύου και υπηρεσίες.
- Αύξηση της κλίμακας ανόδου και παρουσίασης με ένα edge per organization or tenant.
- Απλοποίηση της συμμόρφωσης του IT με λεπτομερές logging.
- Αποδοτική/εκσυγχρονισμένη οργάνωση της εφαρμογής με τη χρήση μιας επιφάνειας με όλα τα χαρακτηριστικά που συνδυάζεται με την VMware vCenter Server και οδηγεί σε λύσεις ασφάλειας για την επιχείρηση.



Εικόνα 10.7: vShield Edge

Η vshield Edge είναι μια λύση ασφάλειας που παρέχει κεντρικές δυνατότητες ασφάλειας, όπως network security gateway services και web load balancing για την απόδοση και την διαθεσιμότητα. Η λύση συνδέεται άμεσα με την vSphere και επηρεάζει τα ενσωματωμένα χαρακτηριστικά (built-in features) όπως είναι η fault tolerance και η υψηλή διαθεσιμότητα.
Οι διαχειριστές έχουν την δυνατότητα να διαχειρίζονται/ελέγχουν κεντρικά το shield Edge μέσω της κονσόλας που συμπεριλαμβάνεται στο shield Manager, το όποιο ενσωματώνεται με το vCenter Server, ώστε να διευκολύνει την εφαρμογή ενοποιημένης ασφάλειας των virtual datacenters. Η shield Edge, επίσης, εργάζεται σε συμφωνία με την VMware Cloud Director, ώστε να αυτοματοποιήσει και να επιταχύνει την ασφαλή παροχή των virtual datacenters σε multitenant cloud infrastructures.
Αναπτυσσομένη σαν μια εικονική επιρροή, η shield Edge παρέχει firewall, VPN, Web load Balancer, network address translation (NAT) και DHCP υπηρεσίες για να παρακολουθεί packet headers για source και destination IP addresses. Συμφώνα με την πολιτική, είναι πιθανόν να αρνηθεί ή να επιτρέψει συνδέσεις, να εισαγάγει και να τερματίσει VPN sessions, να εκτελέσει network address translation ή να παρακολουθήσει data by source ή destination port και protocol type (TCP ή UDP).

Επίσης η vShield Edge έχει τη δυνατότητα για:

- Γρήγορη και ασφαλή παροχή των περιμέτρων των virtual datacenter – Η vShield επιτρέπει στους οργανισμούς να δημιουργήσουν ασφαλείς, λογικές και ανεξάρτητες από το υλικό περιμέτρους στα εικονικά περιβάλλοντα των datacenter.
- Προστασία της εχεμύθειας των δεδομένων στα κοινά δίκτυα – Η vShield Edge παρέχει site-to-site VPN με 256-bit encryption, ώστε να προστατεύει την εχεμύθεια όλων των δεδομένων που μεταδίδονται μέσα στα virtual datacenter perimeters.
- Διαβεβαίωση της απόδοσης και διαθεσιμότητα των υπηρεσιών του δικτύου – Η vShield Edge καταφέρνει αποτελεσματικά το inbound web traffic μέσα στα clusters των εικονικών μηχανημάτων και περιλαμβάνει web load balancing capabilities, ώστε οι πελάτες να μπορούν να αναπτύξουν διαδικασίες με ή χωρίς την ασφάλεια της edge.

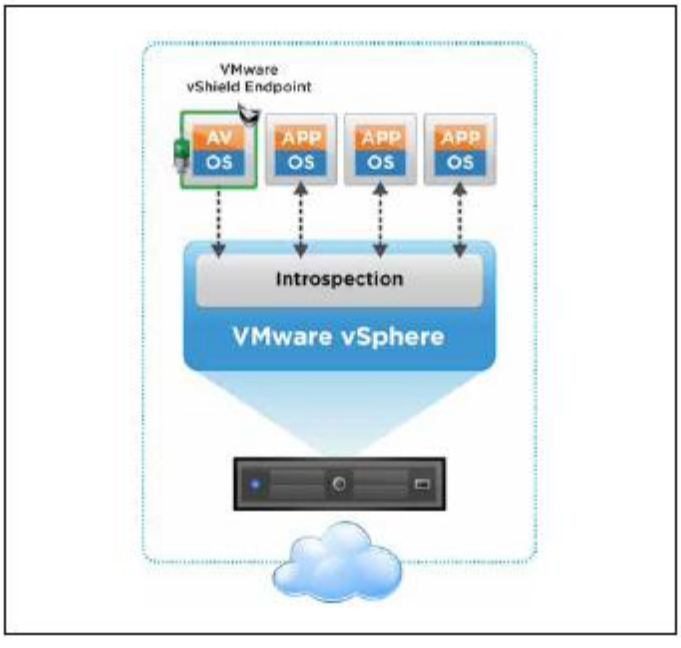
- Διευκόλυνση της εφαρμογής του ελέγχου – Η vShield παρέχει τον απαιτούμενο έλεγχο, όπως είναι το detailed event logging and flow statistics.

10.8 VMware vShield EndPoint

Η VMware vShield Endpoint [18] ενισχύει την ασφάλεια των εικονικών μηχανημάτων, καθώς βελτιώνει την απόδοση για προστασία στα endpoints . Η vShield Endpoint μεταφέρει δικτυακά antivirus και anti-malware agent processing σε μια ασφαλή εικονική παροχή την οποία διαθέτει η VMware. Η λύση είναι σχεδιασμένη ώστε να επηρεάσει τις ήδη υπάρχουσες επενδύσεις επιτρέποντας στους πελάτες να εφαρμόζουν πολιτικές για τα antivirus και τα anti-malware για εικονικά περιβάλλοντα με τα ίδια interfaces που χρησιμοποιούν για να ασφαλίσουν τα φυσικά περιβάλλοντα.

Με την VMware vShield EndPoint μας δίνεται η δυνατότητα να έχουμε:

- Βελτίωση της σταθεροποίησης των ratios και της απόδοσης με την ελαχιστοποίηση των antivirus agents από τα guest virtual machines.
- Αποδοτική οργάνωση για την ανάπτυξη των antivirus και των anti-malware και έλεγχο στα περιβάλλοντα της VMware.
- Βελτίωση της ασφάλειας με τη σταθεροποίηση των antivirus software agents, ώστε να μειώνεται το attack surface.
- Ικανοποίηση της συμμόρφωσης και των audits requirements μέσω του logging of antivirus και anti-malware activities.



Εικόνα 10.8: vShield Endpoint

Η vShield Endpoint καινοτομεί στον τομέα της προστασίας των guest virtual machines από τους ιούς και τα malware. Η λύση που εφαρμόζει η VMware vSphere και η VMware View παρέχει ασφάλεια ενάντια στους ιούς.
Η vShield Endpoint βελτιώνει την απόδοση μεταφέροντας virus-scanning activities από κάθε εικονικό μηχάνημα σε μια πιο ασφαλή εφαρμογή/παροχή, η οποία διαθέτει μια μηχανή για να ανιχνεύει τους ιούς, καθώς επίσης και τα stored antivirus signatures. Για τις λειτουργίες των antivirus και των antimalware, το vShield Endpoint ελαχιστοποιεί τα software agent footprint στα guest virtual machines, ελευθερώνει τις πηγές του συστήματος, βελτιώνει την απόδοση και μειώνει την απειλή των antivirus «storms» (υπερχειλισμένες πηγές που δημιουργούνται κατά τη διάρκεια προγραμματισμένων scans και signature updates). Χάρη στην ασφαλή εικονική παροχή η οποία –σε αντίθεση με ένα guest virtual machine– δεν βγαίνει εκτός δικτύου, μπορεί να ενημερώνει διαρκώς τις antivirus signatures, παρέχοντας συνεχή ασφάλεια στα εικονικά μηχανήματα στον host. Επιπλέον, καινούργιες εικονικές μηχανές (ή υπάρχουσες που είναι εκτός δικτύου) διασφαλίζονται αυτόματα με τις πιο σύγχρονες antivirus signatures όταν εισέρχονται στο δίκτυο.
Η vShield Endpoint ενισχύει την ασφάλεια με μια ασφαλή εικονική παροχή (η οποία παρέχεται από την VMware), χρησιμοποιώντας την εύρωστη και ασφαλή ενδοσκόπηση της vSphere, μειώνοντας την ευπάθεια των antivirus και των antimalware.
Η vShield Endpoint παρέχει, επίσης, interfaces, καθώς επίσης μνήμη και process scanning. Οι επιχειρήσεις έχουν τη δυνατότητα να χρησιμοποιήσουν στιγμιαία πολλαπλές λύσεις ασφάλειας, όπως για παράδειγμα τη χρησιμοποίηση ευαίσθητων δεδομένων από μια ασφαλή εικονική παροχή, χρησιμοποιώντας ένα antivirus solution σε μια διαφορετική εικονική παροχή.
Οι οργανισμοί μπορούν να επιδείξουν συμμόρφωση και να ικανοποιήσουν τις απαιτήσεις του ελέγχου, μέσα από λεπτομερείς δραστηριότητες logging μέσα από την υπηρεσία του antivirus και antimalware.
Οι διαχειριστές είναι δυνατό να ελέγξουν κεντρικά το vShield Endpoint μέσα από την κονσόλα της vShield Manager, η οποία ενσωματώνεται με την VMware vCenter Server, ώστε να διευκολύνει την εφαρμογή της ασφάλειας για τα virtual datacenters.

Η vShield Endpoint συνδέεται άμεσα με την vSphere και περιλαμβάνει τρία συστατικά:

- Σκληραγωγημένες ασφαλείς εικονικές παροχές, που παρέχονται από την VMware.
- Λεπτομερείς πράκτορες για εικονικά μηχανήματα, ώστε να απαλλάσσει παροχές ασφάλειας (συμπεριλαμβανομένων των εργαλείων της VMware).
- Οι VMware Endpoint ESX hypervisor είναι σε θέση να παρέχουν επικοινωνία ανάμεσα στα δύο πρώτα συστατικά στο hypervisor layer.
-

Για παράδειγμα, στην περίπτωση ενός antivirus solution, η vShield Endpoint παρακολουθεί τα file events των εικονικών μηχανημάτων και προειδοποιεί το antivirus engine, το οποίο ανιχνεύει και επιστρέφει τη διάταξη/διαρρύθμιση/εξουσία. Η λύση υποστηρίζει και τα on access και τα on demand (προγραμματισμένα) σκαναρίσματα αρχείων που είχαν ενεργοποιηθεί από τη μηχανή των antivirus σε μια ασφαλή εικονική παροχή.
Όταν η διόρθωση είναι αναγκαία, οι διαχειριστές είναι σε θέση να προσδιορίσουν επανορθωτικές λύσεις χρησιμοποιώντας τα ήδη υπάρχοντα εργαλεία antivirus και anti-malware, ενώ με αυτόν τον τρόπο η vShield Endpoint μπορεί να εφαρμόσει επανορθωτική/διορθωτική πολιτική μέσα στα μολυσμένα εικονικά μηχανήματα.
Η κονσόλα εφαρμογής που παρέχεται από την VMware, χρησιμοποιείται ώστε να διαμορφώσει και να ελέγξει το λογισμικό της VMware που φιλοξενείται στην ασφαλή εικονική παροχή. Η VMware είναι σε θέση να παρέχει ένα interface στον χρήστη, καθιστώντας την εμπειρία της εφαρμογής όμοια με την εφαρμογή του λογισμικού που φιλοξενείται σε ένα φυσικό περιβάλλον ασφάλειας.
Οι διαχειριστές της εικονικής υποδομής επιδεικνύουν μικρή προσπάθεια, επειδή τα εικονικά μηχανήματα δεν ελέγχουν τα antivirus agents. Αντίθετα, η κονσόλα εφαρμογής χρησιμοποιείται

για να ελέγξει την εικονική ασφαλή παροχή. Αυτή η προσέγγιση μειώνει , επίσης, την ανάγκη συχνής αναβάθμισης σε κάθε εικονικό μηχάνημα. Όσον αφορά την ανάπτυξη, η VMware Tools περιλαμβάνει το thin agent και το ESX module που παρέχει hypervisor ενδοσκόπηση.
Οι διαχειριστές της εικονικής υποδομής έχουν τη δυνατότητα να ελέγξουν την ανάπτυξη, ώστε να καθορίσουν, για παράδειγμα, εάν ένα antivirus solution δουλεύει ορθά.

Δυνατότητες

- Βελτίωση της απόδοσης, χρησιμοποιώντας το εγχείρημα vShield Endpoint ESX, ώστε να μεταφέρει δραστηριότητες από την ανίχνευση των ιών σε ένα πιο ασφαλές περιβάλλοντα χώρο, όπου η ανίχνευση των ιών επιβάλλεται.
- Καθήκοντα όπως, τα αρχεία, η μνήμη και η ανίχνευση μεταφέρονται από τις εικονικές μηχανές σε μια πιο ασφαλή εικονική εφαρμογή/παροχή μέσω ενός thin client agent και ενός partner ESX module.
- Η vShield Endpoint EPSEC επιτρέπει την επικοινωνία ανάμεσα στα εικονικά μηχανήματα και την ασφαλή εικονική παροχή, χρησιμοποιώντας ενδοσκόπηση στο hypervisor layer.
- Τα antivirus engine and signature files ενημερώνονται μόνο μέσα από την εικονική παροχή, αλλά οι πολιτικές μπορούν να εφαρμοστούν σε όλες τις εικονικές μηχανές σε έναν οικοδεσπότη της vSphere.

Επανόρθωση/Διορθωτική

- Η vShield Endpoint επιβάλλει antivirus policies, οι οποίες υπαγορεύουν εάν ένα μολυσμένο αρχείο πρέπει να διαγραφεί ή να μπει σε κατάσταση καραντίνας ή να τροποποιηθεί με άλλο τρόπο.
- Το thin agent διορθώνει κάποιο αρχείο μέσα στο εικονικό μηχάνημα.

Ενσωματώσεις της vShield

- Η EPSEC API δίνει τη δυνατότητα στους VMware anti-virus partners να ενσωματωθούν με την vShield Endpoint παρέχοντας ενδοσκόπηση στη δραστηριότητα των αρχείων μέσα στο hypervisor. Σημαντικές λειτουργίες των antivirus υποστηρίζονται μέσα από αυτήν την API.

VShield Manager, Policy Management και Automation

- Η vShield Manager παρέχει πλήρη ανάπτυξη χαρακτηριστικών και διαμόρφωση της vShield Endpoint.
- Η Representational State Transfer (REST) APIs επιτρέπει υποστηριζόμενη, αυτόματη ενσωμάτωση των δυνατοτήτων της vShield Endpoint που οδηγούν σε λύσεις.
- Επίσης, παρέχονται ελεγκτικές αναφορές.
- Η vShield Manager είναι δυνατόν να επηρεαστεί σαν ένα vCenter plug-in.

Logging and Auditing

- Το Event logging βασίζεται σε μια βιομηχανοποιημένη φόρμα syslog.

10.9 VMware vShield Bundle

Η VMware vShield Bundle [19] αποτελεί ιδανική λύση για μια διαπιστευμένη υποδομή του Cloud Computing. Η vShield Bundle παρέχει υπηρεσίες ασφάλειας και έλεγχου που προστατεύουν τα virtual datacenters και τα περιβάλλοντα cloud σε όλα τα επίπεδα – όπως είναι το network edge, δεδομένα και endpoints. Η vShield Bundle συνεργάζεται με τη VMware vSphere, τη VMware vCenter Server και τη VMware vCloud Director.

Με τη VMware vShield Bundle μας δίνεται η δυνατότητα να έχουμε:

- Ασφαλή εικονικά datacenters και cloud environments σε όλα τα επίπεδα – όπως είναι το network edge, δεδομένα και endpoints.
- Μείωση του κόστους και της πολυπλοκότητας.
- Ελαχιστοποίηση των antivirus and anti-malware «storms» διαμέσου ανάπτυξης χωρίς agents (agentless).
- Μείωση του κινδύνου της μη-συμμόρφωσης/έλεγχου και της επικινδυνότητας με την ανακάλυψη των ευαίσθητων δεδομένων.
- Αξιόπιστες ζώνες για τη δημιουργία εφαρμογών και δεδομένων που έχουν σαν κοινό την ασφάλεια και την πρόσβαση.

Η vShield Bundle προσφέρει περισσότερα από τη φυσική ασφάλεια για τα virtualized datacenters. Συνδυάζει τις προηγμένες δυνατότητες τεσσάρων προϊόντων της vShield, ώστε να παράγει ενσωματωμένες προσαρμοστικές και cost-effective υπηρεσίες ασφάλειας, που προστατεύουν τα virtual datacenters και cloud environments από τα network edge στις εφαρμογές και στα δεδομένα, καταλήγοντας στα endpoints.

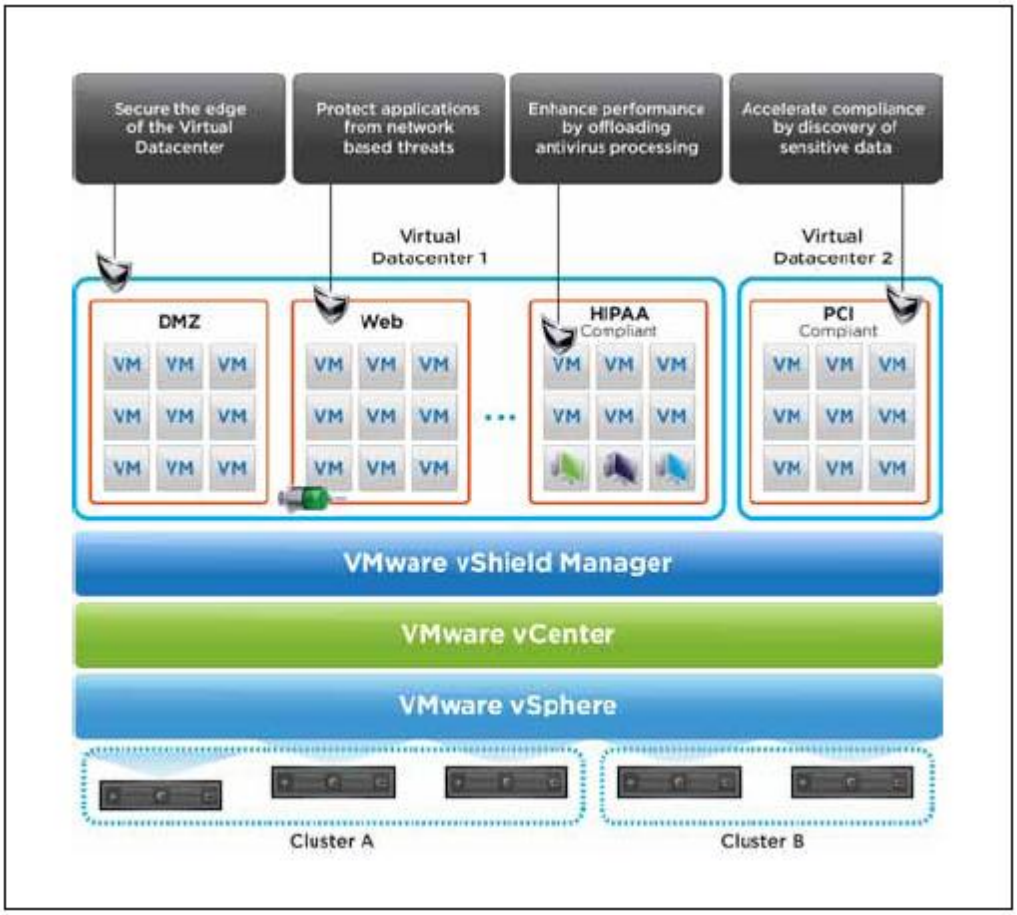
Network Edge

Με την Edge ή Network Edge λύση ασφάλειας για να προστατέψει την περίμετρο των εικονικών datacenters, η vShield Bundle παρέχει κεντρικές δυνατότητες ασφάλειας, όπως είναι οι network security gateway services και το Web load balancing για την απόδοση και τη διαθεσιμότητα. Η λύση συνδέεται άμεσα με την VMware vSphere και επηρεάζει χαρακτηριστικά που ήδη υπάρχουν, συμπεριλαμβανομένων της ψευδούς ανοχής και της υψηλής διαθεσιμότητας .
Η vShield Bundle, επίσης, δρα σε συνδιασμό με την VMware vCloud Director, ώστε να αυτοματοποιήσει και να επιταχύνει τον ασφαλή ερχομό των εικονικών datacenters σε multitenant cloud κατασκευές. Οι διαχειριστές περιορίζουν την πρόσβαση μόνο σε διακεκριμένες πηγές.
Η vShield Bundle παρέχει network security gateway functions όπως είναι το firewall, το virtual private network (VPN), το Web load balancer, το network address translation (NAT) και τις dynamic host configuration protocol (DHCP) services για να ελέγχει τα packet headers για source και destination IP addresses. Σε άμεση συνάφεια με την πολιτική, είναι δυνατόν να αρνηθεί ή να επιτρέψει συνδέσεις, να εισαγάγει και να τερματίσει συνεδρίες, να παρουσιάσει μετάφραση στη διεύθυνση του δικτύου ή να επιθεωρήσει δεδομένα by source destination port and protocol type (transmission control protocol [TCP] or user datagram protocol [UDP]).

Εφαρμογές και δεδομένα

Η vShield Bundle παρέχει ένα hypervisor-based, application aware firewall solution για τα εικονικά datacenters, όπως είναι το network edge, applications , δεδομένα, και endpoints. Επιτρέπει τη δυναμική ανακάλυψη των ευαίσθητων δεδομένων, όπως τα δεδομένα της πιστωτικής κάρτας, που είναι δυνατόν να αποθηκεύονται σε μη δομημένα αρχεία δεδομένων που διαμένουν στα εικονικά μηχανήματα. Οι διαχειριστές είναι σε θέση να ελέγχουν, χρησιμοποιώντας το συγκεκριμένο συνδυασμό προϊόντων για να σκανάρουν τα datacenters, τα clusters ή τα resource pools, όσον αφορά την παρουσίαση των ευαίσθητων δεδομένων.

Το προϊόν συνδέεται άμεσα με την vSphere για να προστατέψει απέναντι στις εσωτερικές απειλές του δικτύου και μειώνει την απειλή των παραβιάσεων της πολιτικής μέσα στην ενσωματωμένη περίμετρο ασφάλειας. Το τελευταίο συμβαίνει καθώς χρησιμοποιείται το application-aware firewalling με ένα πακέτο ενδοσκόπησης και έλεγχου που βασίζεται στο source and destination IP addresses. Απλοποιεί, επίσης, την πολιτική του ελέγχου παρέχοντας στους διαχειριστές τη δυνατότητα να δημιουργήσουν άμεσα ομάδες ασφάλειας που σχετίζονται με την επιχείρηση. Η vShield Bundle δημιουργεί και ενισχύει πολιτικές που βασίζονται στον διαχειριστή και στις ομάδες ασφάλειας που σχετίζονται με την επιχείρηση. Περιλαμβάνει τον έλεγχο ροής για να αναλύσει την κυκλοφορία δικτύων μηχανημάτων εικονικής πραγματικότητας και να επιβάλλει δυναμικά την πολιτική ομάδας ασφάλειας.
Η vShield Bundle παρέχει στον διαχειριστή μια κονσόλα για την πολιτική της εφαρμογής των ευαίσθητων δεδομένων. Η «πολιτική» δημιουργείται με την επιλογή των εφαρμόσιμων κανονισμών, ώστε να ανιχνεύσει αυτά που εμπεριέχουν τα εικονικά μηχανήματα, όπως είναι τα datacenters, οι συστάδες και τα resource pools. Τα αρχεία που ανιχνεύουν μπορούν να φιλτραριστούν περαιτέρω με βάση την επέκταση του αρχείου, το μέγεθος ή την ημερομηνία τροποποίησης. Τα αποτελέσματα ανίχνευσης περιλαμβάνουν τον προσδιορισμό των ονομάτων datacenter, συστάδων, μηχανημάτων εικονικής πραγματικότητας και αρχείων που δεν συμμορφώνονται με τις επιλεγμένες πολιτικές. Οι διαχειριστές μπορούν να χρησιμοποιήσουν το Representational State Transfer (REST) APIs, ώστε να διορθώσουν τα μη-συμμορφωμένα αρχεία.



Εικόνα 10.9: VMware vShield enables granular policy enforcement using security groups.

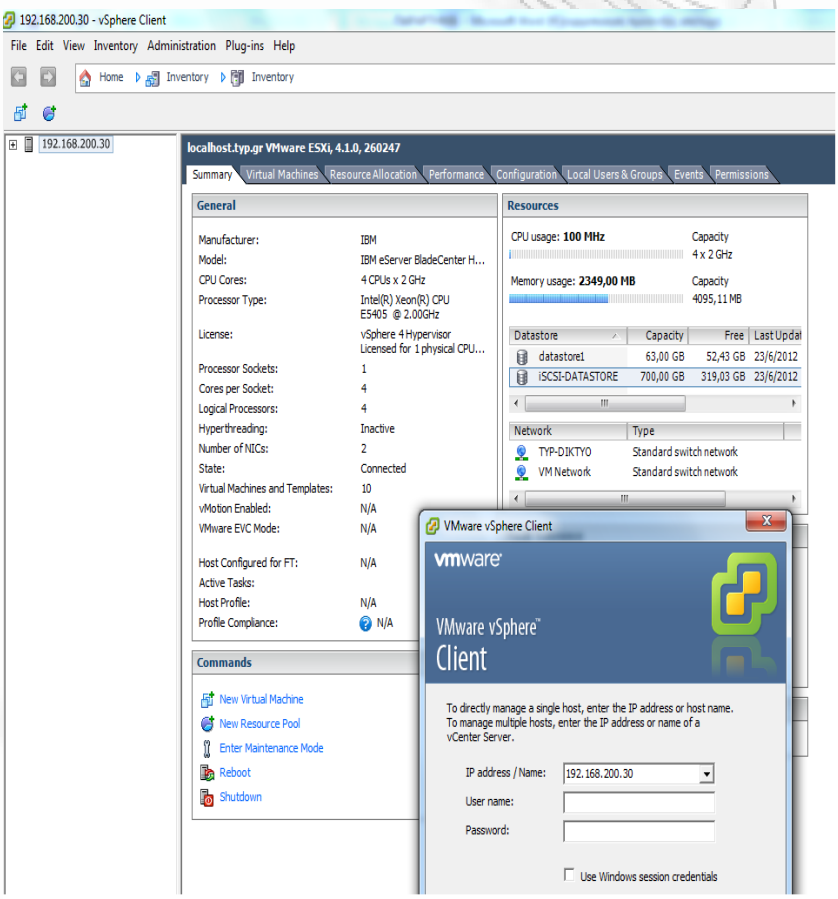
11.0 Παράρτημα (Παρουσίαση Εφαρμογής)

Για την συγκεκριμένη εφαρμογή χρησιμοποιήθηκαν πολλά και διαφορετικά εργαλεία για την ολοκλήρωση της μετάβασης της σε VMware 4.1.0 περιβάλλον . Θα παρουσιαστούν ενδεικτικά κάποια κομμάτια κώδικα καθώς και λεπτομέρειες τεχνολογιών που χρησιμοποιήθηκαν για αυτό το project.

- **Σύνδεση client**

Το vSphere client είναι μια εφαρμογή που επιτρέπει τη διαχείριση μιας εγκατάστασης vSphere . Ένας client vSphere μπορεί να αναπτύξει δραστηριότητες σε συσκευές τόσο διαφορετικές όσο ένα iPad ή ένας προσωπικός υπολογιστής γραφείου με Windows. Ο client vSphere παρέχει σε έναν διαχειριστή την πρόσβαση στις βασικές λειτουργίες του vSphere χωρίς την ανάγκη να προσεγγιστεί ένας κεντρικός υπολογιστής vSphere άμεσα.

Στην συγκεκριμένη εφαρμογή χρησιμοποιήθηκε ο vSphere client 4.1.0 που μας δίνει δυνατότητες διαχείρισης του ESXi 4.1.0 Server.Η φόρμα εισόδου και ολόκληρη η κονσόλα φαίνεται στο παρακάτω σχήμα :



Εικόνα 11.1: Φόρμα εισόδου και περιβάλλον vSphere client

Με το συγκεκριμένο εργαλείο έγινε δημιουργία των δύο νέων virtual machines SQLVM και VMPDF . Στη συνέχεια έγινε η εγκατάσταση του λειτουργικού συστήματος WINDOWS 2008 R2 SERVER και στα δύο virtual machines .

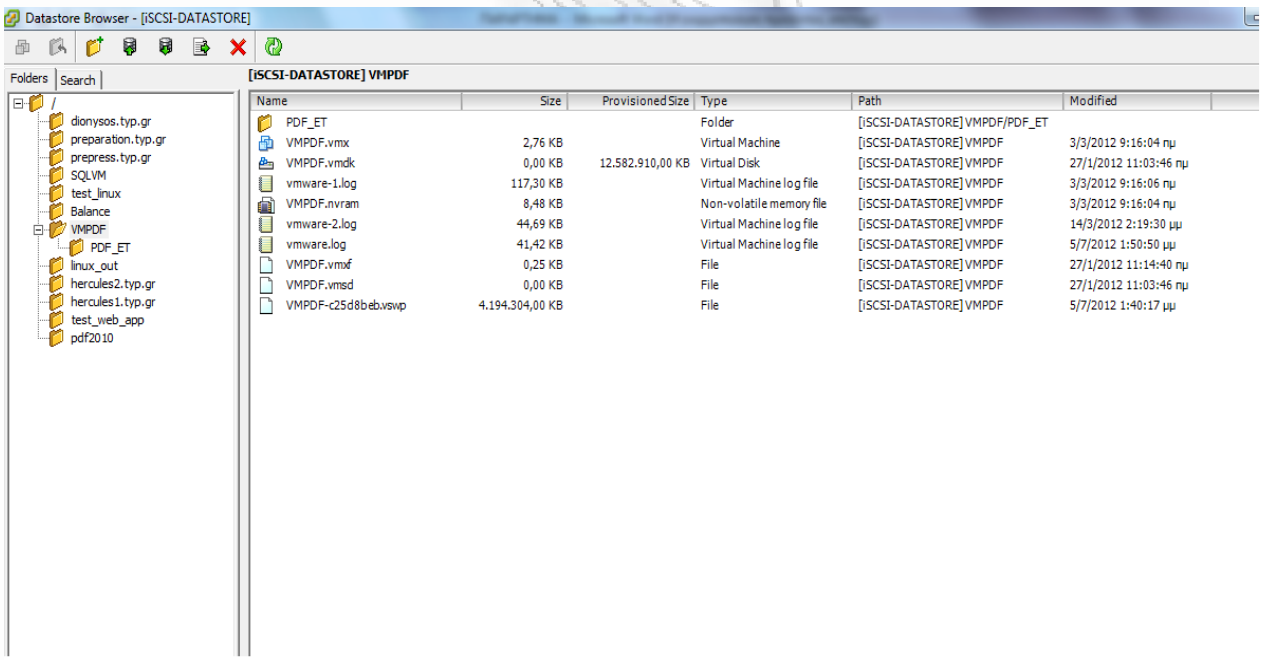
Στο virtual machine SQLVM έγινε η εγκατάσταση του SQLSERVER 2008 R2 και η παραμετροποίηση για τη βάση δεδομένων της εφαρμογής.

- **Αρχεία**

Τα δεδομένα της βάσης δεδομένων μεταφέρθηκαν από τον κεντρικό SERVER του Εθνικού Τυπογραφείου στο συγκεκριμένο VM και έγιναν RESTORE .Έτσι δημιουργήθηκε ένα πιστό αντίγραφο της κεντρικής βάσης δεδομένων του Εθνικού Τυπογραφείου σε περιβάλλον Cloud Computing.

Τα DATAFILES της βάσης δεδομένων δημιουργήθηκαν σε ειδικό χώρο του iSCSI δίσκου του ESXi για το συγκεκριμένο VM και έγινα rebuild τα indexes.

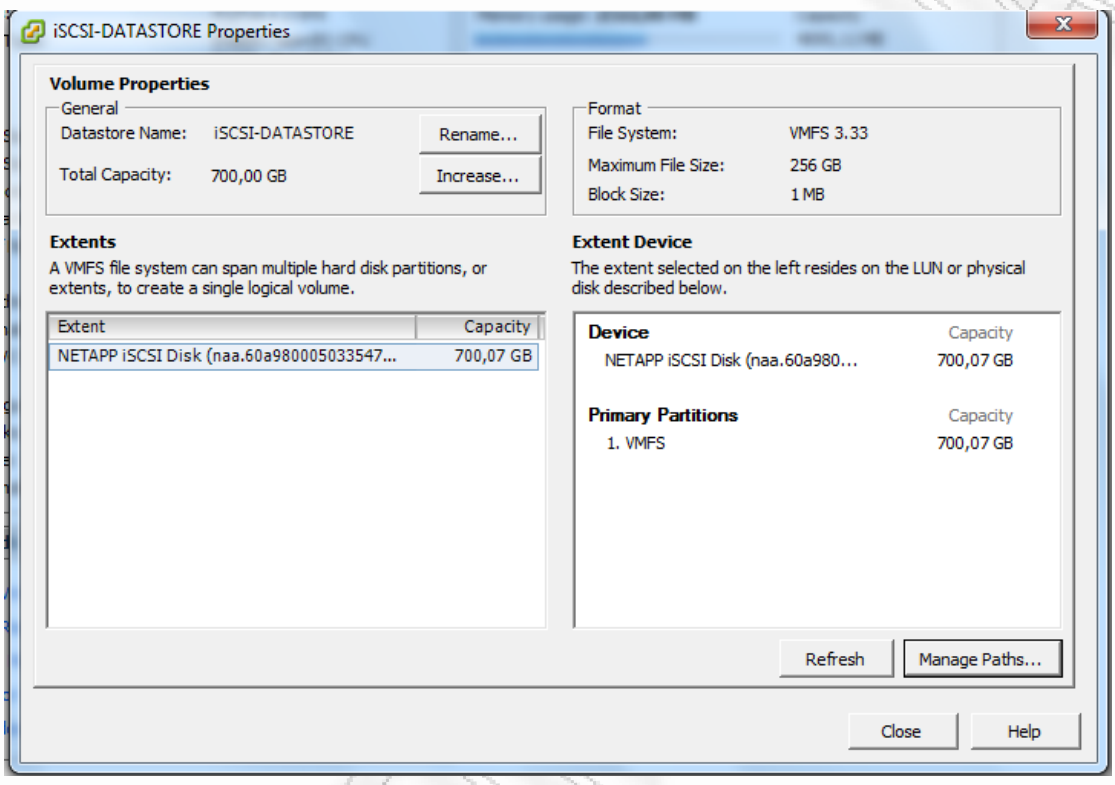
Επειδή η εφαρμογή έχει την δυνατότητα να ανοίγει πατώντας το πλήκτρο ‘ο’ ή ‘Ο’ από τα αποτελέσματα αναζήτησης των ΦΕΚ και των πρωτοκόλλων έγιναν ‘UPLOAD ’ files στο datastore του VMPDF και συγκεκριμένα στον folder PDF_ET.Η διαδικασία αυτή φαίνεται στο παρακάτω screenshot :



Εικόνα 11.2: Αρχεία στο iSCSI – Datastore του VMDPF

Σε αυτό το screenshot φαίνονται καθαρά όλα τα αρχεία του συγκεκριμένου VM.

Ολόκληρο το **iSCSI** -datastore του συγκεκριμένου ESX i φαίνεται αναλυτικά παρακάτω:



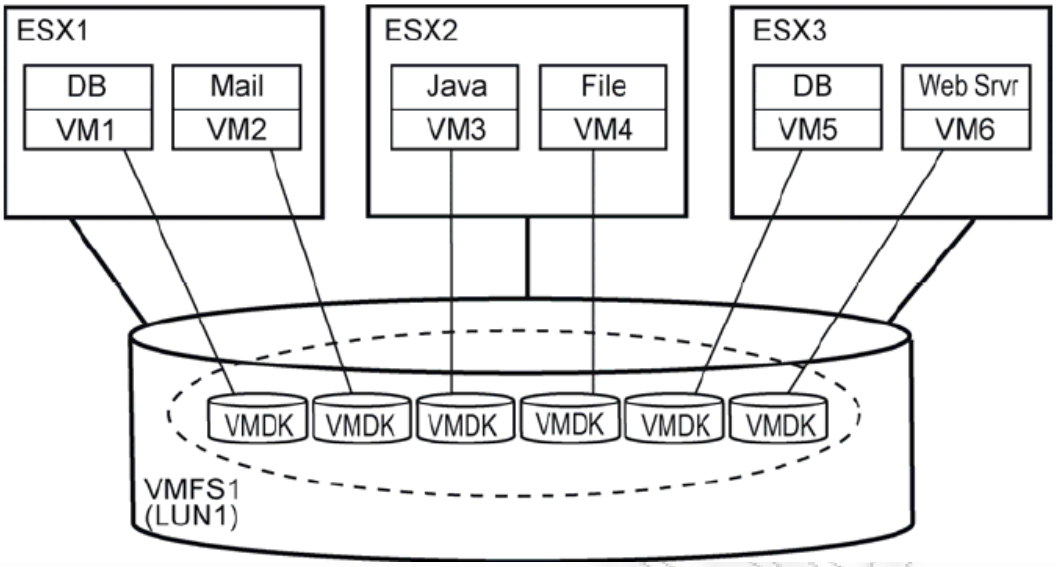
Εικόνα 11.3: Ρυθμίσεις στο iSCSI – Datastore του ESXi

Το σύστημα αρχείων που χρησιμοποιεί η συγκεκριμένη τεχνολογία λέγεται VMFS.

Το VMFS δηλαδή το «VMware Virtual Machine File System» είναι ένα υψηλής απόδοσης cluster σύστημα αρχείων που επιτρέπει virtualization πέρα από τα όρια ενός ενιαίου συστήματος.

Σχεδιασμένο, κατασκευασμένο, και βελτιστοποιημένο για τον εικονικό περιβάλλον ,το VMFS αυξάνει τη χρησιμοποίηση των πόρων παρέχοντας σε πολλαπλά μηχανημάτα εικονικής πραγματικότητας την κοινή πρόσβαση σε μια παγιωμένη ομάδα της συγκεντρωμένης αποθήκευσης.

Το παρακάτω σχήμα δείχνει πώς οι πολλαπλοί κεντρικοί υπολογιστές ESX με τα μηχανήματα εικονικής πραγματικότητας που τρέχουν μπορούν να χρησιμοποιήσουν VMFS για να μοιραστούν μια κοινή συγκεντρωμένη ομάδα αποθήκευσης.



Εικόνα 11.4: Το VMS επιτρέπει σε πολλούς ESX severs να μοιράζονται το storage

Με την συγκεκριμένη τεχνολογία θα είναι πιο εύκολη και γρήγορη η αναζήτηση και η εμφάνιση των αρχείων των ΦΕΚ στο συγκεκριμένο μέσο αποθήκευσης. Επίσης projects που μπορεί να αναπτυχθούν στο μέλλον θα έχουν τη δυνατότητα πλέον να χρησιμοποιούν τη συγκεκριμένη τεχνολογία.

- **Εισαγωγή στο σύστημα**

Για την ασφάλεια των χρηστών στο νέο περιβάλλον δημιουργήθηκε ένας νέος πίνακας στη βάση δεδομένων με όνομα cloud_users.

Ο πίνακας αυτός έχει τις εξής στήλες :

User_name “Το όνομα του χρήστη”

Password “Ο κρυφός κωδικός του”

Hashed_password “Κρυπτογραφημένος κωδικός μαζί με το όνομα δικτύου του PC”

IsAdmin “Αν είναι διαχειριστής”

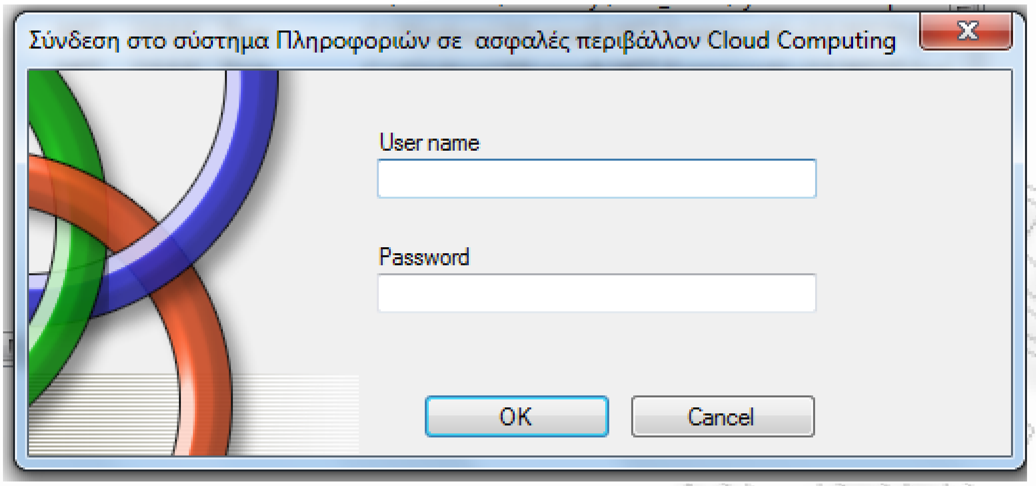
Ο πίνακας αυτός έγινε για να υπάρχει ξεχωριστή ασφάλεια στους χρήστες που χρησιμοποιούν την εφαρμογή (στο Cloud) από τους χρήστες στο domain του Εθνικού Τυπογραφείου.

Η εφαρμογή χρησιμοποιεί configuration αρχείο app.config για να μπορούμε εύκολα να αλλάζουμε παραμέτρους στο πρόγραμμα. Συγκεκριμένα για την αλλαγή της βάσης δεδομένων που θα λειτουργεί για το πρόγραμμα προστέθηκε στο section : `<appSettings>`

Η γραμμή : <add key="con1" value="Network Library=DBMSSOCN;Data Source=……..;Initial Catalog=……;User ID=……;Password=…….; "/>

Το DataSource είναι το δικτυακό όνομα του SQLSERVER 2008 R2 στο VM SQLVM , το InitialCatalog είναι το όνομα της βάσης των ΦΕΚ και username και password είναι ο χρήστης που έχει δημιουργηθεί στο συγκεκριμένο VM με δικαιώματα db_reader και ικανότητα εκτέλεσης μόνο select στους πίνακες της βάσης .

Η κεντρική φόρμα της εισαγωγής στο σύστημα φαίνεται στο παρακάτω screenshot :



Εικόνα 11.5: Εισαγωγή στην εφαρμογή

Ο κώδικας vb.net της παραπάνω φόρμας φαίνεται παρακάτω :

```
Imports System.Security.Cryptography
Imports System
Imports System.Drawing
Imports System.Collections
Imports System.ComponentModel
Imports System.Windows.Forms
Imports System.Data
Imports System.GC
Imports System.Drawing.Printing
Imports System.Diagnostics
Imports System.IO
Imports System.Text
Imports System.Threading
Imports System.Configuration
Imports System.Configuration.ConfigurationSettings
Imports System.Web.Services.Configuration
Imports System.Data.SqlClient
Imports System.Security

Public Class LoginForm1
Public appl As New AppSettingsReader()
Public genconnection As String = appl.GetValue("con1",
GetType(String))
Private Sub OK_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles OK.Click
Dim password, uname As String
Dim securePwd As New SecureString()
uname = txtusername.Text
password = txtpassword.Text
txtpassword.Text = Nothing
txtpassword.Text   =   "YOU   WILL   NOT   FIND   MY   PASSWORD
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!"
```

```
For Each c As Char In password
securePwd.AppendChar(c)

Next

securePwd.MakeReadOnly()

password = Nothing
password     =     "YOU     WILL     NOT     FIND     MY     PASSWORD
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!"

Dim strHostName As String
Dim sCn As String = genconnection
Dim cn As SqlConnection
Dim dsfirst As New DataSet()
dsfirst = New DataSet
Dim dafirst As SqlDataAdapter
dafirst = New SqlDataAdapter
Dim sqlfirst As String
strHostName = System.Net.Dns.GetHostName()
cn = New SqlConnection(sCn)
cn.Open()



Dim ptr As IntPtr
ptr                                                                    =
System.Runtime.InteropServices.Marshal.SecureStringToBSTR(secureP
wd)
Dim decryptstring As String = Nothing
decryptstring =
System.Runtime.InteropServices.Marshal.PtrToStringUni(ptr)

sbfirst.Append("SELECT  user_name,password,hashed_password,IsAdmin from
cloud_users ")
sbfirst.Append(" WHERE user_name='" & uname & "' and password='" &
System.Runtime.InteropServices.Marshal.PtrToStringUni(ptr) & "' AND
hashed_password ='" & passwordEncryptSHA(System.Net.Dns.GetHostName() &
"crypto_password __ _ $$!09%   " & decryptstring.ToString) & "' ")

securePwd.Dispose()
System.Runtime.InteropServices.Marshal.ZeroFreeBSTR(ptr)

sqlfirst = sbfirst.ToString()
Dim cmdfirst As SqlCommand
cmdfirst = New SqlCommand(sqlfirst, cn)
sqlfirst = Nothing
dafirst = New SqlDataAdapter(cmdfirst)
dafirst.Fill(dsfirst, "cloudusers")

If dsfirst.Tables(0).Rows.Count = 0 Then
MsgBox("Λάθος username ή password! Ξαναπροσπαθήστε")
txtusername.Text = ""
txtpassword.Text = ""
End If
```

```
If dsfirst.Tables(0).Rows.Count = 1 Then
txtusername.Text = ""
txtpassword.Text = ""
Me.Hide()
Form2.Show()

End If

If dsfirst.Tables(0).Rows.Count >= 2 Then
MsgBox("Πρόβλημα στην βάση δεδομένων επικοινωνήστε με τον διαχειριστή !")
txtusername.Text = ""
txtpassword.Text = ""
Exit Sub
End If
SqlConnection.ClearPool(cn)
cn.Close()
End Sub
```

Ασφάλεια με την κλάση SecureString Class

Στον παραπάνω κώδικα έχει χρησιμοποιηθεί το namespace System.Security με assembly mscorlib.dll που περιέχει την κλάση SecureString Class η οποία δεν μπορεί να κληρονομηθεί.
Η κλάση αυτή μας επιτρέπει να δημιουργήσουμε encrypted strings και να τα διαγράψουμε από τη μνήμη όταν δεν τα χρειαζόμαστε. Ακόμα μπορούμε να τα ορίσουμε ώστε να συμπεριφέρονται σαν read-only strings ώστε να αποφύγουμε αντίγραφα . Μπορούμε να τα διαγράψουμε από τη μνήμη με την εντολή Dispose() και `System.Runtime.InteropServices.Marshal.ZeroFreeBSTR(ptr).`
Αφού πληκτρολογήσει ο χρήστης το username και το password τότε η μεταβλητή password παίρνει την τιμή από το textbox του password. Στην συνέχεια το txtpassword.text αφού «καθαριστεί» δέχεται άλλα δεδομένα.

Με τις εντολές :
```
For Each c As Char In password
    securePwd.AppendChar(c)

Next

securePwd.MakeReadOnly()


password = Nothing
password = "YOU WILL NOT FIND MY PASSWORD !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!"
```

Αρχικά γίνεται εισαγωγή της τιμής του password στην μεταβλητή securePwd της κλάσης SecureString Class. Ακολούθως η μεταβλητή αυτή γίνεται readonly που σημαίνει ότι δεν μπορεί να αλλαχθεί και να γίνει copy και η μεταβλητή password αφού «καθαριστεί» δέχεται άλλα δεδομένα.

Το τελικό query που θα τρέξει η εφαρμογή θα έχει στο "where" μια μεταβλητή readonly για το password που θα έχει γίνει decrypt (μέσα στην εντολή του query και όχι σε άλλο

σημείο ή σε άλλη μεταβλητή) και ένα μεγάλο string για το hashed password αποτέλεσμα της κρυπτογράφησης του ονόματος δικτύου του PC , κάποιου string και του secure password.
*Για κάποιον που θα μπορέσει να «αντιληφθεί» το query δηλαδή τη μεταβλητή «`sqlfirst`» με κάποιο τρόπο , περιέχει τεράστια αλφαρηθμητικά από κρυπτογράφηση SHA1 στην τελευταία συνθήκη του **where** .*

Ενδεικτικά μια τιμή για την κάθε μεταβλητή σε runtime :

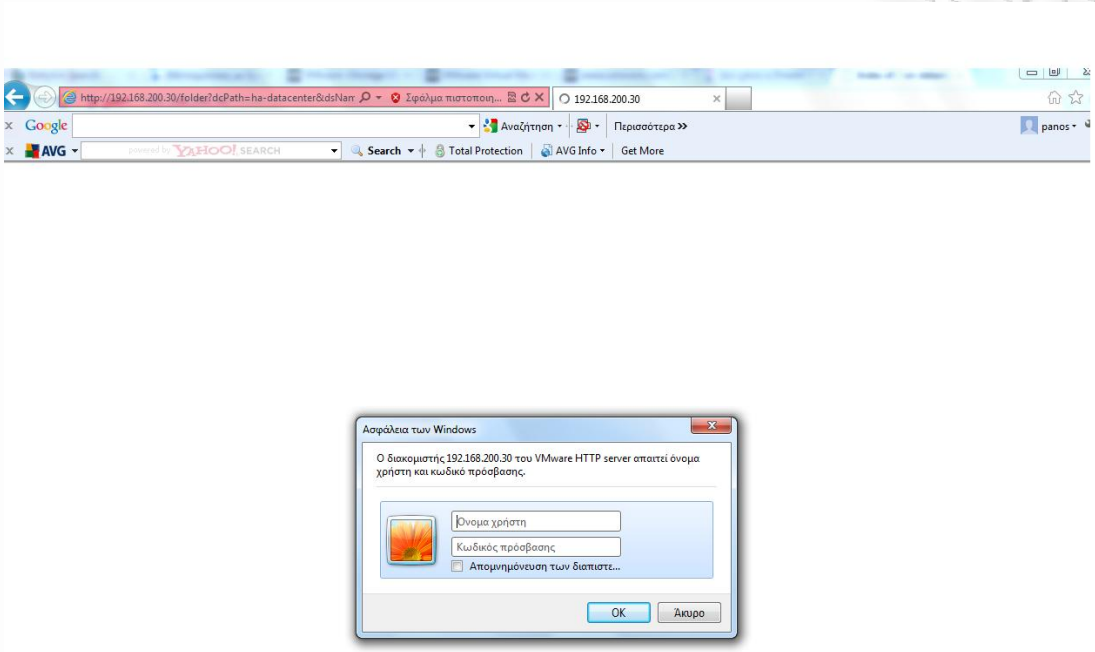
Query : SELECT user_name,password,hashed_password,IsAdmin from cloud_users WHERE user_name='panos' and password='123456' AND hashed_password ='ff10017d67b2e5fc079a9e3eae34b4425e83bba3'
Η μεταβλητή telikostring παίρνει κατευθείαν κρυπτογραφημένη μορφή χωρίς να ξέρουμε τη λογική της. Έτσι είναι δύσκολο να βρεθεί η συγκεκριμένη τιμή.

```
Private Sub Cancel_Click(ByVal sender As System.Object, ByVal e
As System.EventArgs) Handles Cancel.Click
Me.Close()
End Sub
Private Sub UsernameTextBox_TextChanged(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
txtusername.TextChanged
End Sub

End Sub
Public Function passwordEncryptSHA(ByVal password As String) As
String
Dim hashedpas As String = ""
Dim passwordhash As New
Security.Cryptography.SHA1CryptoServiceProvider
Dim bToHash() As Byte =
System.Text.Encoding.UTF8.GetBytes(password)
bToHash = passwordhash.ComputeHash(bToHash)
For Each bytepas As Byte In bToHash
hashedpas += bytepas.ToString("x2")
Next
Return hashedpas
End Function
Private Sub LoginForm1_Load(ByVal sender As System.Object, ByVal
e As System.EventArgs) Handles MyBase.Load
End Sub
End Class
```

Έχει δημιουργηθεί ειδική φόρμα για τον administrator της εφαρμογής που δημιουργεί χρήστες παράγοντας αυτόματα το hashed_password , χρησιμοποιώντας το password του χρήστη , το ειδικό string και το δικτυακό όνομα του υπολογιστή. Έτσι τα τέσσερα στοιχεία username,password , hashed_password , IsAdmin γίνονται insert στη βάση δεδομένων και συγκεκριμένα στον πίνακα cloud_users.

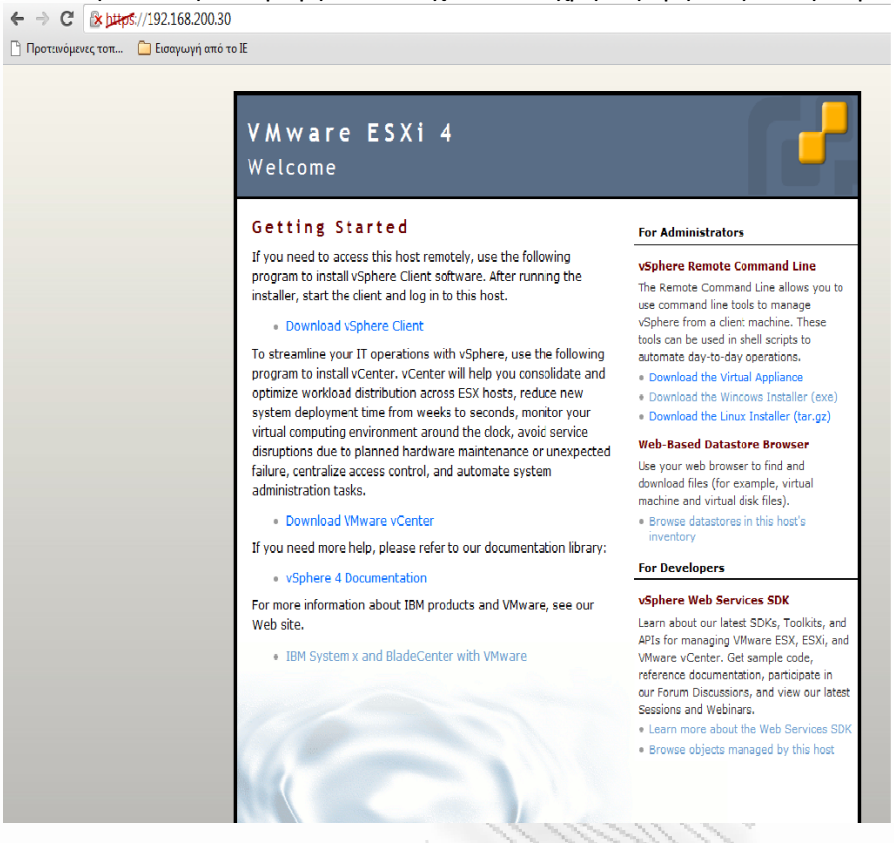
- **Αναζήτηση εμφάνιση αρχείων**

Για την εμφάνιση των αρχείων θα χρησιμοποιήσουμε το πρωτόκολλό **http** του ESX i με sessions για την συγκεκριμένη τεχνολογία . Η διαδικασία αυτή φαίνεται παρακάτω :



Εικόνα 11.6.1: Εισαγωγή στον ESXi με http πρωτόκολλο

Μετά την σωστή εισαγωγή των στοιχείων του χρήστη εμφανίζεται η παρακάτω φόρμα :



Εικόνα 11.6.2: Επιτυχής εισαγωγή στον ESXi με http πρωτόκολλο

Με τον συγκεκριμένο χρήστη και τον default browser έχει πλέον δημιουργηθεί session από τον ESX i και μπορούμε να ανοίγουμε γρήγορα και με ασφάλεια pdf αρχεία.

Έχει δημιουργηθεί ήδη χρήστης για το συγκεκριμένο σημείο του datastore που το χειρίζεται το VM “VMPDF”.

Ο κώδικας VB.NET που παράγει το path του datastore και ανοίγει το pdf παρουσιάζεται παρακάτω :

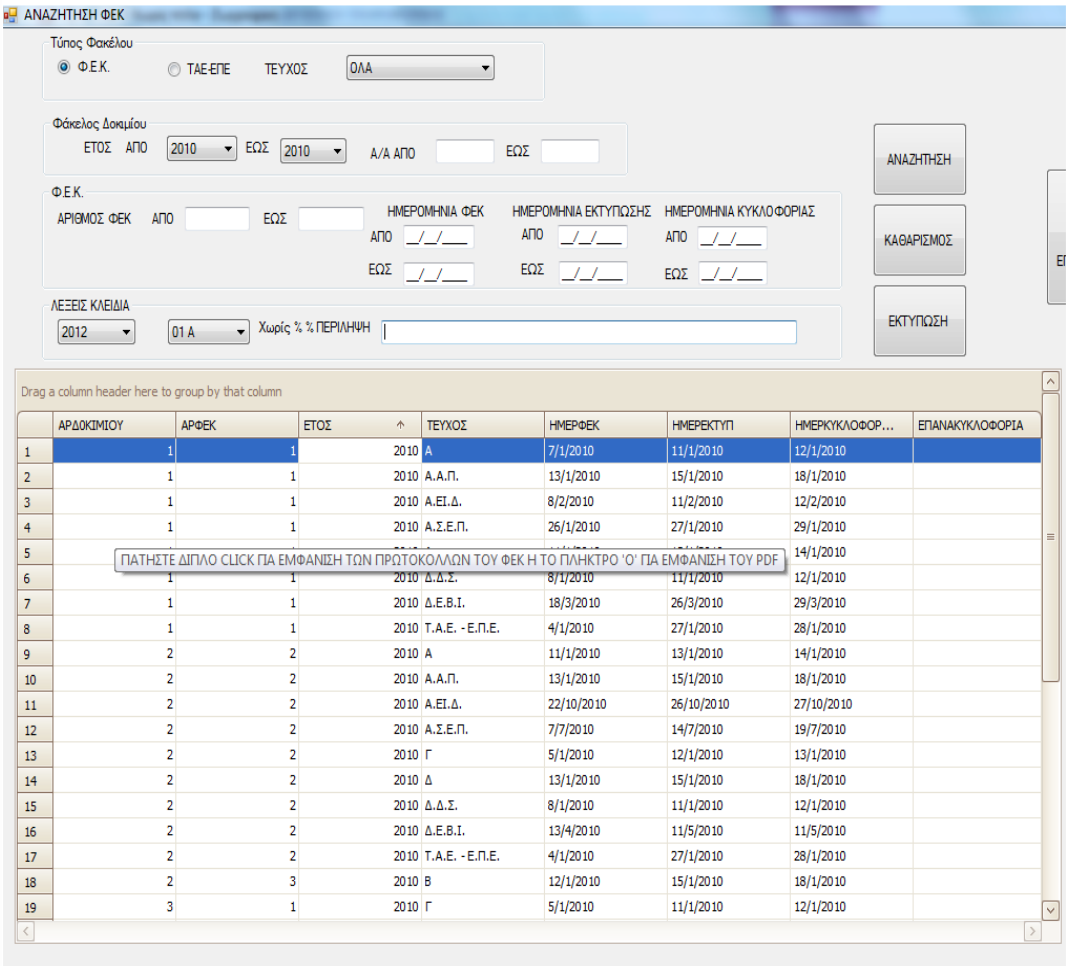
```
Imports System
Imports System.Drawing
Imports System.Collections
Imports System.ComponentModel
Imports System.Windows.Forms
Imports System.Data
Imports DevExpress.XtraPrinting
Imports DevExpress.XtraGrid
Imports System.Drawing.Printing
Imports System.Diagnostics
Imports System.IO
Imports System.Text
Imports System.Threading
Imports DevExpress.XtraPrintingLinks
Imports System.Data.OleDb
Imports System.Data.SqlClient

Private Sub Gridfek_KeyPress(ByVal sender As Object, ByVal e As
System.Windows.Forms.KeyPressEventArgs) Handles Gridfek.KeyPress
Dim PATHFEK As String = Nothing
Dim teyxos As String = Nothing
```

```
Dim teyxostr As String = Nothing
Dim etos As String = Nothing
Dim arith As String = Nothing
Dim telikofilename As String = Nothing
Dim telikocloudpath As String = Nothing
Dim myProcess As New System.Diagnostics.Process
If e.KeyChar = "ο" Or e.KeyChar = "Ο" Or e.KeyChar = "Ο" Or e.KeyChar =
"ο" Then
arith    =    CStr((GridView1.GetRowCellValue(GridView1.FocusedRowHandle,
"ΑΡΦΕΚ")))
etos    =    Trim(((GridView1.GetRowCellValue(GridView1.FocusedRowHandle,
"ΕΤΟΣ"))))
teyxostr    =    ((GridView1.GetRowCellValue(GridView1.FocusedRowHandle,
"ΤΕΥΧΟΣ")))
If teyxostr = "Α" Then
          teyxos = "01"
End If
If teyxostr = "Β" Then
          teyxos = "02"
End If
If teyxostr = "Γ" Then
          teyxos = "03"
End If
If teyxostr = "Δ" Then
          teyxos = "04"
End If
If teyxostr = "Ν.Π.Δ.Δ." Then
          teyxos = "05"
End If
If teyxostr = "Α.Π.Σ." Then
          teyxos = "06"
End If
If teyxostr = "ΠΑΡΑΡΤΗΜΑ" Then
          teyxos = "07"
End If
If teyxostr = "Δ.Ε.Β.Ι." Then
          teyxos = "08"
End If
If teyxostr = "Α.ΕΙ.Δ." Then
          teyxos = "09"
End If
If teyxostr = "Α.Σ.Ε.Π." Then
          teyxos = "10"
End If
If teyxostr = "ΑΕ-ΕΠΕ" Then
          teyxos = "11"
End If
If teyxostr = "Δ.Δ.Σ." Then
           teyxos = "12"
End If
If teyxostr = "Ο.Π.Κ." Then
           teyxos = "13"
End If
If teyxostr = "Υ.Ο.Δ.Δ." Then
           teyxos = "14"
End If
If teyxostr = "Α.Α.Π." Then
           teyxos = "15"
End If
```

```
telikofilename = "……."

telikocloudpath    =    "http://192.168.200.30/folder/vmpdf/pdf_et/"    &
telikofilename   &   ".pdf"   &   "?dcPath=ha-datacenter   &   dsName=iSCSI-
DATASTORE"

            myProcess.StartInfo.UseShellExecute = False

            myProcess.StartInfo.FileName = (telikocloudpath)
            myProcess.StartInfo.Verb = "open"
            myProcess.StartInfo.CreateNoWindow = True

            myProcess.Start()


    End Sub
```

Το τελικο cloudpath έγινε στο folder που θα περιέχει πλέον όλα τα pdf (ΦΕΚ) «pdf_et» χωρίς sub directory χρησιμοποιώντας την δυνατότητα του VMFS για γρήγορο indexing , ασφάλεια , ανάκτηση .

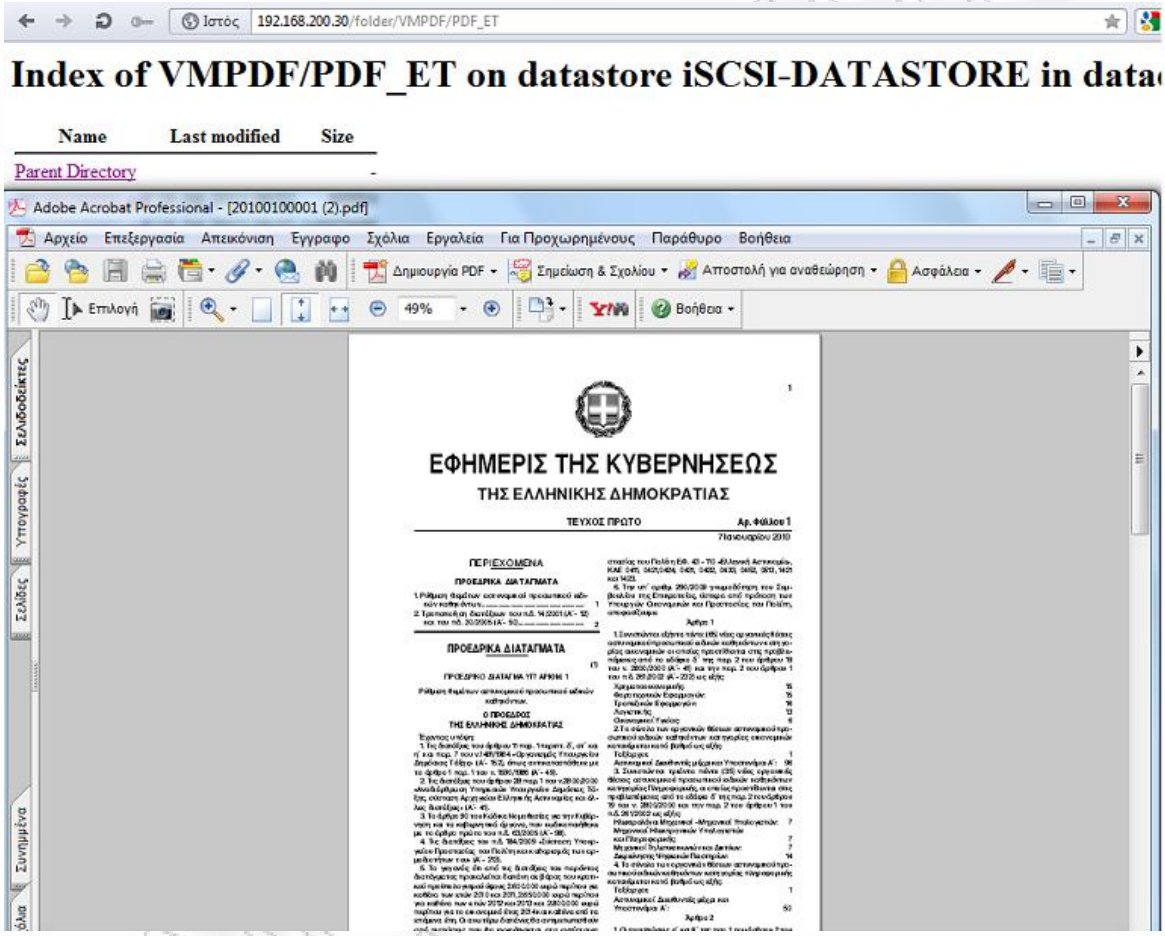
Ο παραπάνω κώδικας είναι για την συγκεκριμένη φόρμα :



Εικόνα 11.7: Αναλυτική φόρμα ΦΕΚ

Με αυτή τη δυνατότητα μπορεί ο χρήστης της εφαρμογής να ανοίγει οποιοδήποτε ΦΕΚ θέλει μέσα από περιβάλλον Cloud Computing χωρίς να επηρεάζει το εσωτερικό σύστημα παραγωγής ΦΕΚ με μεγαλύτερη ασφάλεια , ευκολία και ταχύτητα.

Πατώντας ο χρήστης το πλήκτρο ‘ο’ ή ‘Ο’ η εφαρμογή ανοίγει δυναμικά μέσω του VMPDF το ΦΕΚ που επιλέξαμε. Η δυνατότητα αυτή φαίνεται στο παρακάτω screenshot :

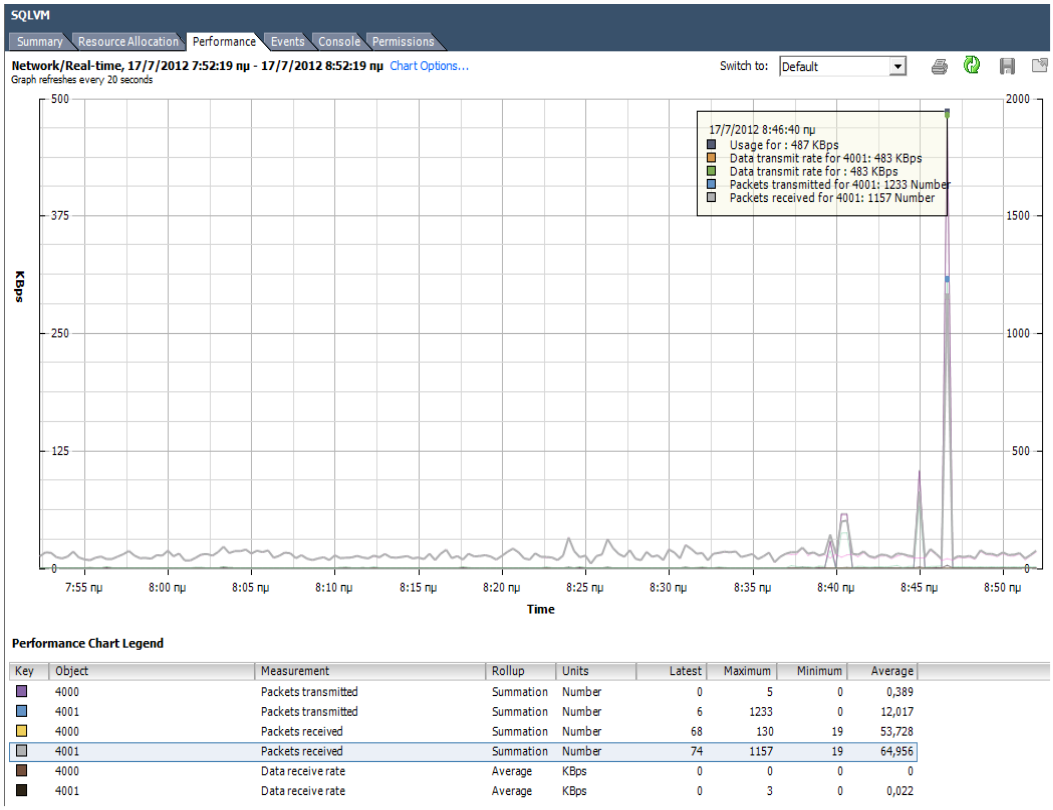


Εικόνα 11.8: Ανάκτηση ΦΕΚ με http

- **Απόδοση συστήματος**

Την απόδοση της εφαρμογής μπορούμε πλέον με τα εργαλεία του vSphere client να την παρακολουθούμε διεξοδικά. Με αυτόν τον τρόπο αλλάζοντας παραμέτρους - που έχουμε δυνατότητα - μπορούμε να οδηγήσουμε την απόδοση της εφαρμογής σε υψηλότερα επίπεδα.

Το vSphere client μας δίνει την δυνατότητα να βλέπουμε στατιστικά για την απόδοση της εφαρμογής μέσω του tab performance. Για παράδειγμα , για ένα μεγάλο query που εκτελείτε στην εφαρμογή το performance του δικτύου φαίνεται στο παρακάτω screenshot:



Key	Object	Measurement	Rollup	Units	Latest	Maximum	Minimum	Average
	4000	Packets transmitted	Summation	Number	0	5	0	0,389
	4001	Packets transmitted	Summation	Number	6	1233	0	12,017
	4000	Packets received	Summation	Number	68	130	19	53,728
	4001	Packets received	Summation	Number	74	1157	19	64,956
	4000	Data receive rate	Average	KBps	0	0	0	0
	4001	Data receive rate	Average	KBps	0	3	0	0,022

Εικόνα 11.9: Απόδοση δικτύου

Τα object «4000» και «4001» είναι ουσιαστικά οι διαφορετικοί virtual adapters δικτύου στο VM “SQLVM”. Συγκεκριμένα το ethernet0 είναι ο «4000» και το ethernet1 ο «4001». Με αυτό το εργαλείο μπορούμε να έχουμε μια δυναμική όψη της κατάστασης του δικτύου αυτής της εικονικής μηχανής που λειτουργεί η βάση δεδομένων της εφαρμογής. Επίσης τέτοια ολοκληρωμένα views μπορούμε να έχουμε για την μνήμη , το δίσκο , τον επεξεργαστή , το datastore , το σύστημα , το virtual disk και το power.

Ακόμα έχουμε τη δυνατότητα να κάνουμε export όλο το performance της μηχανής σε αρχείο Excel (.xls) όπως επίσης και αναλυτικά τα στοιχεία του ESXi server σε web σελίδα (html) .

- **Αποτελέσματα**

Η μεταφορά της συγκεκριμένης εφαρμογής σε VMware ESXi 4.1.0 δημιουργεί βαθύτερη γνώση σε αυτό το περιβάλλον και δίνει άπειρες δυνατότητες για το μέλλον.

Η εγκατάσταση νέων virtual machines , η παραμετροποίηση της νέας πλατφόρμας της βάσης δεδομένων , η εισαγωγή των αρχείων στο νέο datastorage και η σύνδεση της κονσόλας προγραμματισμού με το νέο περιβάλλον ήταν πραγματικά μια πολύ ευχάριστη εμπειρία.

Το αποτέλεσμα , είναι μια πολύ πιο γρήγορη εφαρμογή , με μεγαλύτερη ασφάλεια που χρησιμοποιεί νέες τεχνολογίες και κάνει τη χρήση της πιο ευχάριστη.

12.0 Επίλογος

Σίγουρα το Cloud Computing θα αποτελέσει βασικό θεμέλιο της ηλεκτρονικής διακυβέρνησης τα επόμενα χρόνια. Το ελληνικό κράτος έχει ήδη αρχίσει να επενδύει στις συγκεκριμένες τεχνολογίες και να πραγματοποιεί διαρθρωτικές αλλαγές σε ολοκληρωμένα πληροφοριακά συστήματα. Ωστόσο, κάποια σοβαρά θέματα ασφάλειας, εμπιστοσύνης και ιδιωτικότητας δεν έχουν αποσαφηνιστεί ακόμα επαρκώς. Επίσης, το επίπεδο της εκπαίδευσης στη συγκεκριμένη τεχνολογία στο δημόσιο τομέα είναι ακόμα περιορισμένο . Μόνο κάποιες συγκεκριμένες υπηρεσίες έχουν τεχνογνωσία και υποδομές για Cloud Computing.
Ουσιαστικά βρισκόμαστε στην ανατολή μιας νέας enterprise υπηρεσίας βασισμένη στο internet. Cloud applications θα δημιουργούνται πλέον με γεωμετρική πρόοδο, ωστόσο επειδή βρισκόμαστε ακόμα στην αρχή θα υπάρχουν πολλά κενά και αδυναμίες που θα δημιουργήσουν μεγάλα προβλήματα σε αυτή τη νέα εικονική πραγματικότητα. Θα χρειαστούν εξελιγμένες υπηρεσίες και εφαρμογές στο κομμάτι της ασφάλειας.
Κλείνοντας θα ήθελα να ευχηθώ η επιστήμη της πληροφορικής και το ερευνητικό της κομμάτι ειδικά στην Ελλάδα να έχει τη δύναμη να βοηθήσει ώστε η συγκεκριμένη τεχνολογία να ολοκληρωθεί επιστημονικά και να έχει την καλύτερη δυνατή εφαρμογή στην ηλεκτρονική διακυβέρνηση.

REFERENCES :

1) Cloud Computing: An Overview. Srinivasa Rao, Nageswara Rao ,Kusuma Kumari. Journal of Theoretical and Applied Information Technology

2) Effectively and Securely Using the Cloud Computing Paradigm. Peter Mell, Tim Grance NIST, Information Technology Laboratory .

3) Computing Platforms and Different Scenarios Which Platform is Right for You?. www.cumulux.com.

4) White Paper Intel Trusted Execution Technology Healthcare Secure Healthcare Cloud: Start Now

5) IBM http://www.ibm.com/developerworks/cloud/library/cl-hypervisorcompare/

6) Cloud Computing Security –Making Virtual Machines Cloud-Ready A Trend Micro White Paper, May 2010

7) NIST : Guide for security for full virtualization technology. KarenScarfone ,MurugiahSouppaya ,PaulHoffman January 2011

8) Empirical Exploitation of Live Virtual Machine Migration. Jon Oberheide, Evan Cooke, Farnam Jahanian. Electrical Engineering and Computer Science Department, University of Michigan 2009

9) Secure Hypervisors Sebastian Vogl University of Munchen

10) Εθνικό Τυπογραφείο http://www.et.gr

11) VMware http://www.vmware.com/pdf/vi3_35/esx_3/r35/vi3_35_25_intro_vi.pdf

12) VMware http://www.vmware.com/files/pdf/sql_server_use_cases.pdf

13) VMware server
http://www.virtuatopia.com/index.php/VMware_Server_2.0_Security_-_Access,_Roles_and_Permissions

14) VMware - ESXi
http://www.virtualizationadmin.com/articles-tutorials/vmware-esx-and-vsphere-articles/general/using-roles-ecure-vmware-esx-infrastructure.html

15) VMware
http://www.vmware.com/files/pdf/products/vShield/VMware-vShield5-Brochure.pdf

16) VMware
http://www.vmware.com/files/pdf/products/vShield/VMware-vShield5-App-with-Data-Security-Datasheet.pdf

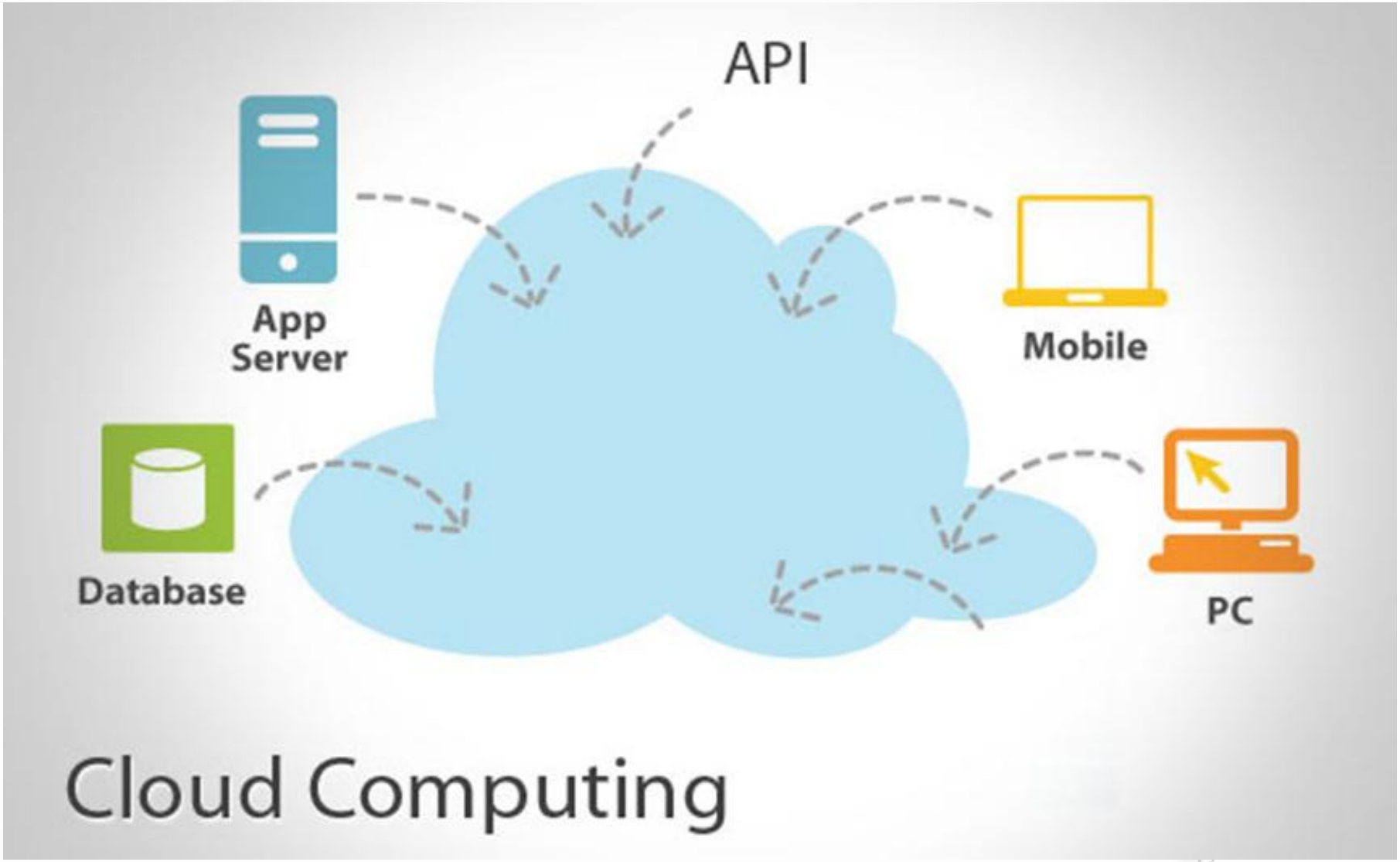
17) VMware
http://www.vmware.com/files/pdf/products/vShield/VMware-vShield5-Edge-Datasheet.pdf

18) VMware
http://www.vmware.com/files/pdf/products/vShield/VMware-vShield5-Endpoint-Datasheet.pdf

19) VMware
http://www.vmware.com/files/pdf/products/vShield/VMware-vShield5-Bundle-Datasheet.pdf

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ :

CPU	Central Processing Unit
CRM	Customer Relationship Management
DOS	Denial-of-service
DRS	Distributed Resource Scheduler
EC2	Amazon Elastic Compute Cloud
FIPS 104-2	Federal Information Processing Standards
HA	High Availability
Iaas	Infrastructure as a Service
IDS	Intrusion detection system
IP	Internet Protocol address
IPS	Intrusion prevention system
IT	Information technology
LAN	Local area network
LUNs	Logical Unit Numbers
NAS	Network-attached storage
NIC	Network interface controller
NIST	National Institute of Standards and Technology
OS	Operating system
PCI -DSS	Payment Card Industry - *Data Security Standards*
P2V	Physical-to-Virtual
Paas	Platform as a service
QoS	Quality of service
S3	Amazon Simple Storage Service
Saas	Software as a service
SAN	Storage area network
SDK	Software development kit
SMP	Symmetric Multi-Processing
SQL	Structured Query Language
TPS	Transaction Rate Per Second
VI Client	Vmware Infrastructure Client
VI Web Access	Vmware Infrastructure Web Access
VLAN	Virtual Local area network
VM	Virtual Machine
VMFS	Vmware Virtual Machine File System
VMM	Virtual Machine Monitor
Vnic	Virtual Network interface controller
VoiP	Voice over IP
Vswitch	Virtual switch
WEB	World Wide Web


API
App
Server
Mobile
Database
PC
Cloud Computing