Σκλήρυνση Μηχανής Δοχείων και Λειτουργικού Συστήματος σε Περιβάλλοντα Linux

Κωνσταντίνος Χωλίδης

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Επίβλεψη: **Δρ. Κρητικός Κυριάκος**

Μέλη εξεταστικής επιτροπής:

Δρ. Σκούτας Δημήτριος **Δρ. Σκιάνης Χαράλαμπος**

Μάρτιος 2024

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Επισκόπηση

- Στόχος
- Εισαγωγικές έννοιες
- Χρήση IaaS σήμερα
- Ασφάλεια στο νέφος
- Σχετικές εργασίες
- Προτεινόμενη λύση

Επισκόπηση

- Αποτίμηση εργαλείου
- Προτάσεις βελτίωσης
- Κλείσιμο

Στόχος της Εργασίας

Ανάπτυξη εργαλείου, το οποίο θα διευκολύνει έναν οργανισμό στην εγκατάσταση και διαμόρφωση με αυτοματοποιημένο τρόπο, ενός ασφαλούς, κατανεμημένου περιβάλλοντος (φιλοξενίας και λειτουργίας) για την εγκατάσταση και λειτουργία μιας εφαρμογής μικρο-υπηρεσιών.

Στόχος της Εργασίας

Ανάπτυξη εργαλείου, το οποίο θα διευκολύνει έναν οργανισμό στην εγκατάσταση και διαμόρφωση με αυτοματοποιημένο τρόπο, ενός ασφαλούς, κατανεμημένου περιβάλλοντος (φιλοξενίας και λειτουργίας) για την εγκατάσταση και λειτουργία μιας εφαρμογής μικρο-υπηρεσιών.

Κύριες Λειτουργίες:

Στόχος της Εργασίας

Ανάπτυξη εργαλείου, το οποίο θα διευκολύνει έναν οργανισμό στην εγκατάσταση και διαμόρφωση με αυτοματοποιημένο τρόπο, ενός ασφαλούς, κατανεμημένου περιβάλλοντος (φιλοξενίας και λειτουργίας) για την εγκατάσταση και λειτουργία μιας εφαρμογής μικρο-υπηρεσιών.

Κύριες Λειτουργίες:

- Δημιουργία εικονικών μηχανών

Στόχος της Εργασίας

Ανάπτυξη εργαλείου, το οποίο θα διευκολύνει έναν οργανισμό στην εγκατάσταση και διαμόρφωση με αυτοματοποιημένο τρόπο, ενός ασφαλούς, κατανεμημένου περιβάλλοντος (φιλοξενίας και λειτουργίας) για την εγκατάσταση και λειτουργία μιας εφαρμογής μικρο-υπηρεσιών.

Κύριες Λειτουργίες:

- Δημιουργία εικονικών μηχανών
- Σκλήρυνση των εικονικών μηχανών

Στόχος της Εργασίας

Ανάπτυξη εργαλείου, το οποίο θα διευκολύνει έναν οργανισμό στην εγκατάσταση και διαμόρφωση με αυτοματοποιημένο τρόπο, ενός ασφαλούς, κατανεμημένου περιβάλλοντος (φιλοξενίας και λειτουργίας) για την εγκατάσταση και λειτουργία μιας εφαρμογής μικρο-υπηρεσιών.

Κύριες Λειτουργίες:

- Δημιουργία εικονικών μηχανών
- Σκλήρυνση των εικονικών μηχανών
- Εγκατάσταση/Σκλήρυνση του Docker

Εισαγωγικές Έννοιες

Λίγα λόγια για:

Λίγα λόγια για:

- Νεφο-υπολογιστική

Λίγα λόγια για:

- Νεφο-υπολογιστική
- Εικονικοποίηση

Λίγα λόγια για:

- Νεφο-υπολογιστική
- Εικονικοποίηση
- Υπερ-επόπτες

Λίγα λόγια για:

- Νεφο-υπολογιστική
- Εικονικοποίηση
- Υπερ-επόπτες
- Docker

Νεφο-υπολογιστική

Νεφο-υπολογιστική

Ορισμός
Ένα μοντέλο, το οποίο επιτρέπει την ανά πάσα στιγμή πρόσβαση σε υπολογιστικούς πόρους, μέσω του διαδικτύου.

Νεφο-υπολογιστική

Ορισμός

Ένα μοντέλο, το οποίο επιτρέπει την ανά πάσα στιγμή πρόσβαση σε υπολογιστικούς πόρους, μέσω του διαδικτύου.

Χαρακτηριστικά

Νεφο-υπολογιστική

Ορισμός

Ένα μοντέλο, το οποίο επιτρέπει την ανά πάσα στιγμή πρόσβαση σε υπολογιστικούς πόρους, μέσω του διαδικτύου.

Χαρακτηριστικά

- Αυτοεξυπηρέτηση κατά παραγγελία (On-demand Self-service)

Νεφο-υπολογιστική

Ορισμός

Ένα μοντέλο, το οποίο επιτρέπει την ανά πάσα στιγμή πρόσβαση σε υπολογιστικούς πόρους, μέσω του διαδικτύου.

Χαρακτηριστικά

- Αυτοεξυπηρέτηση κατά παραγγελία (On-demand Self-service)
- Πανταχού παρούσα πρόσβαση (Ubiquitous Access)

Νεφο-υπολογιστική

Ορισμός

Ένα μοντέλο, το οποίο επιτρέπει την ανά πάσα στιγμή πρόσβαση σε υπολογιστικούς πόρους, μέσω του διαδικτύου.

Χαρακτηριστικά

- Αυτοεξυπηρέτηση κατά παραγγελία (On-demand Self-service)
- Πανταχού παρούσα πρόσβαση (Ubiquitous Access)
- Πολλαπλή Μίσθωση (Multi-Tenancy)

Νεφο-υπολογιστική

Ορισμός

Ένα μοντέλο, το οποίο επιτρέπει την ανά πάσα στιγμή πρόσβαση σε υπολογιστικούς πόρους, μέσω του διαδικτύου.

Χαρακτηριστικά

- Αυτοεξυπηρέτηση κατά παραγγελία (On-demand Self-service)
- Πανταχού παρούσα πρόσβαση (Ubiquitous Access)
- Πολλαπλή Μίσθωση (Multi-Tenancy)
- Ελαστικότητα (Elasticity)

Νεφο-υπολογιστική

Ορισμός

Ένα μοντέλο, το οποίο επιτρέπει την ανά πάσα στιγμή πρόσβαση σε υπολογιστικούς πόρους, μέσω του διαδικτύου.

Χαρακτηριστικά

- Αυτοεξυπηρέτηση κατά παραγγελία (On-demand Self-service)
- Πανταχού παρούσα πρόσβαση (Ubiquitous Access)
- Πολλαπλή Μίσθωση (Multi-Tenancy)
- Ελαστικότητα (Elasticity)
- Μετρούμενη υπηρεσία (Measured Service)

Μοντέλα Παράδοσης

Μοντέλα Παράδοσης

- Software as a Service (SaaS) (Λογισμικό ως Υπηρεσία)

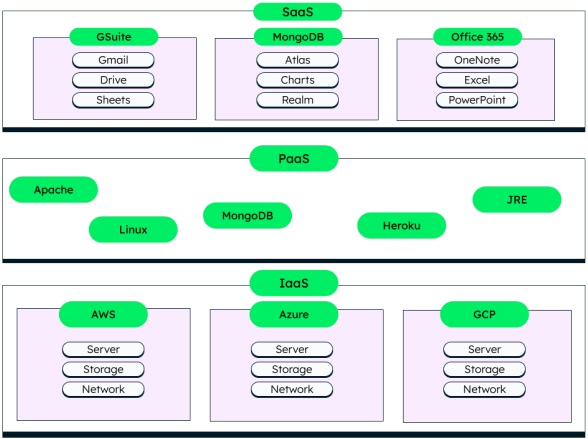
Μοντέλα Παράδοσης

- Software as a Service (SaaS) (Λογισμικό ως Υπηρεσία)
- Platform as a Service (PaaS) (Πλατφόρμα ως Υπηρεσία)

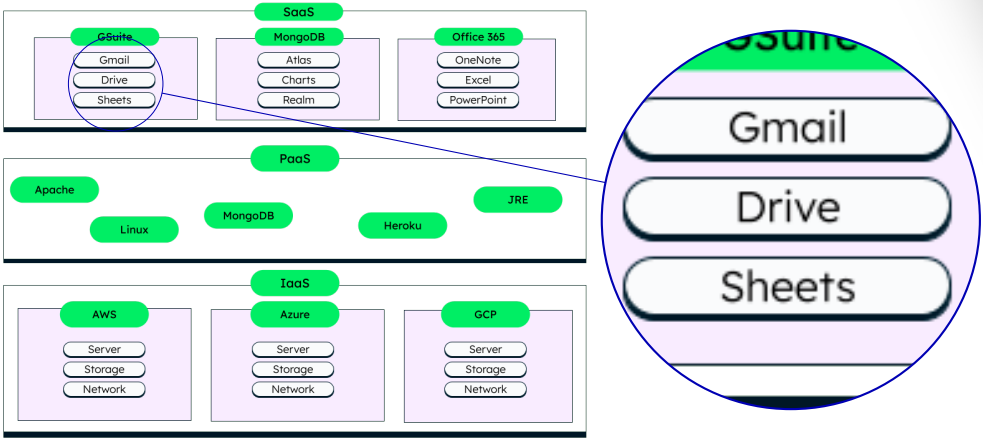
Μοντέλα Παράδοσης

- Software as a Service (SaaS) (Λογισμικό ως Υπηρεσία)
- Platform as a Service (PaaS) (Πλατφόρμα ως Υπηρεσία)
- Infrastructure as a Service (IaaS) (Υποδομή ως Υπηρεσία)

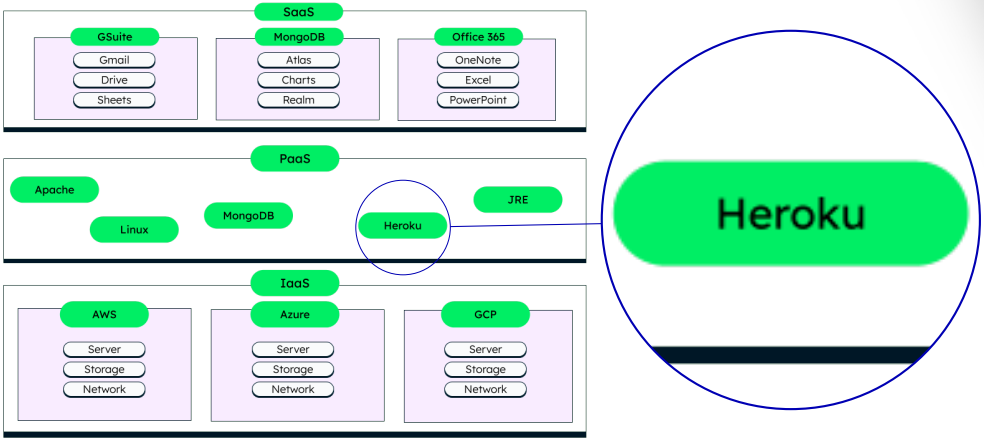
Διαχωρισμός Εννοιών



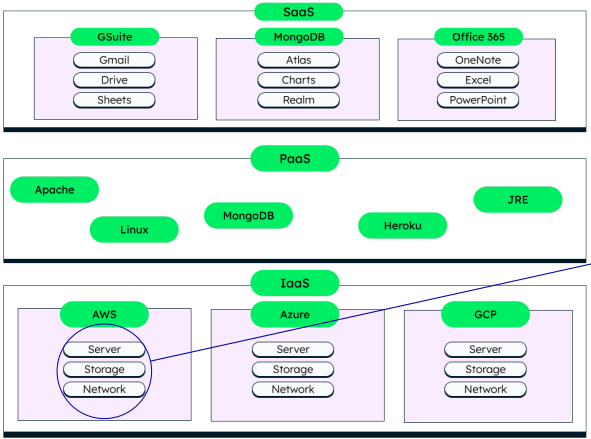
Διαχωρισμός Εννοιών

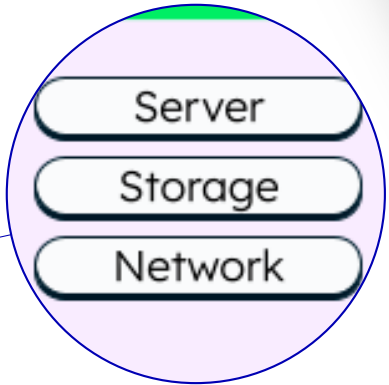


Διαχωρισμός Εννοιών

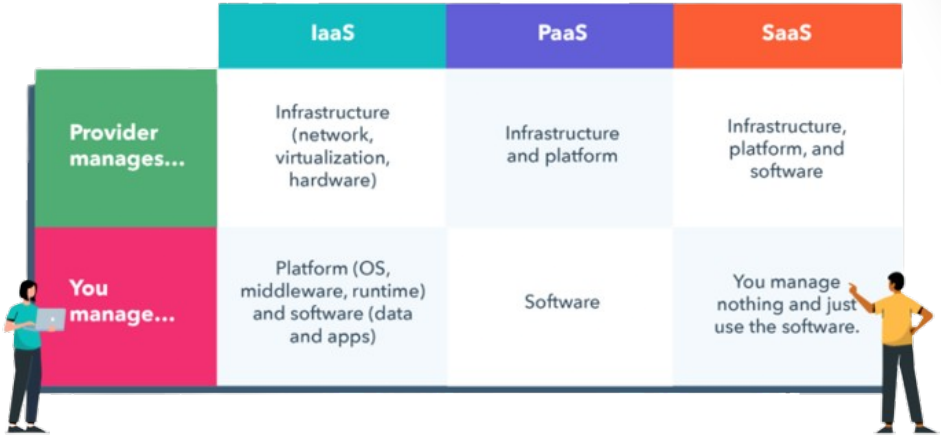


Διαχωρισμός Εννοιών



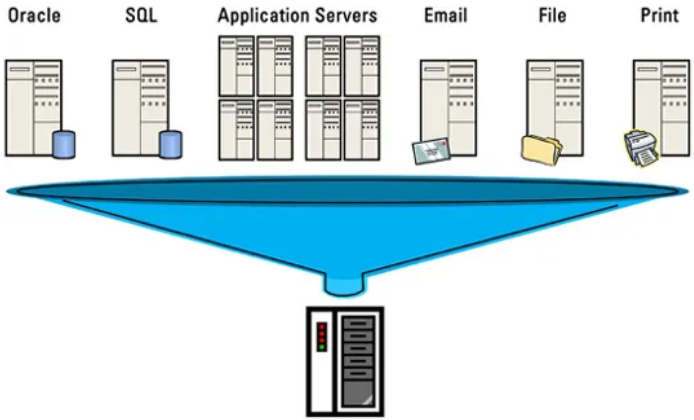


Εμβέλεια ελέγχου



	IaaS	PaaS	SaaS
Provider manages...	Infrastructure (network, virtualization, hardware)	Infrastructure and platform	Infrastructure, platform, and software
You manage...	Platform (OS, middleware, runtime) and software (data and apps)	Software	You manage nothing and just use the software.

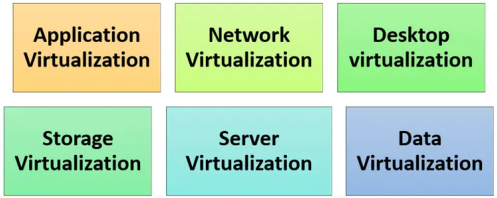
Εικονικοποίηση



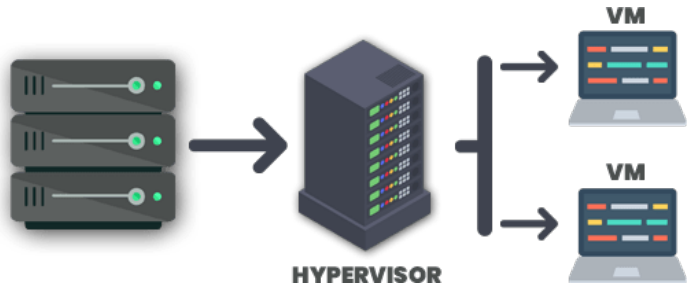
Εικονικοποίηση

Ορισμός
Η αναπαράσταση υπολογιστικών πόρων σε εικονική μορφή με σκοπό την αναδιαμόρφωσή τους προς ικανοποίηση των αναγκών ενός συστήματος.

- **Είδη**:

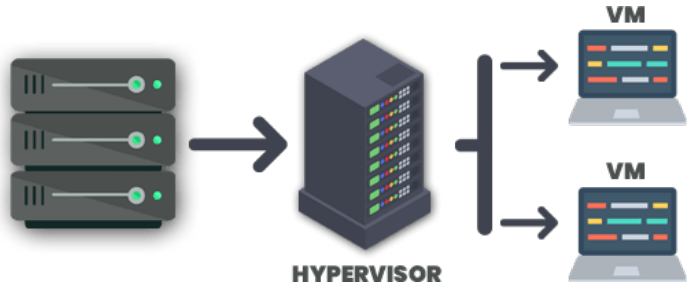


Εικονικοποίηση διακομιστών



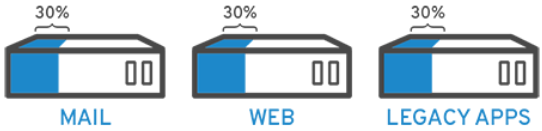
Εικονικοποίηση διακομιστών

Πως λειτουργεί;
Ένας υπερ-επόπτης είναι υπεύθυνος για την κατάτμηση των φυσικών πόρων σε εικονικούς, καθώς και για την ανάθεση αυτών στις εικονικές μηχανές.



Χωρίς εικονικοποίηση

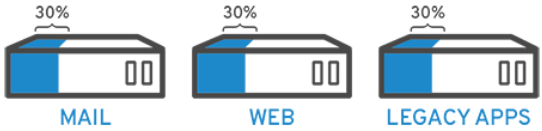
Υποχρησιμοποίηση



Χωρίς εικονικοποίηση

Υποχρησιμοποίηση

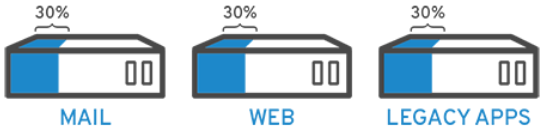
- Αποθηκευτικού χώρου



Χωρίς εικονικοποίηση

Υποχρησιμοποίηση

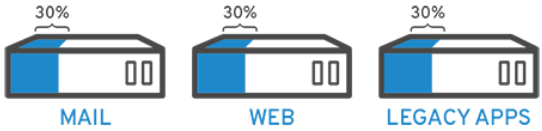
- Αποθηκευτικού χώρου
- Μνήμης



Χωρίς εικονικοποίηση

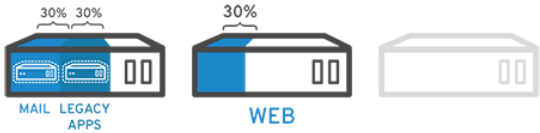
Υποχρησιμοποίηση

- Αποθηκευτικού χώρου
- Μνήμης
- Επεξεργαστικής ισχύος



Με Εικονικοποίηση

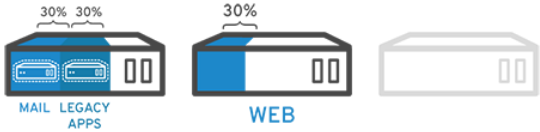
Διαφορές



Με Εικονικοποίηση

Διαφορές

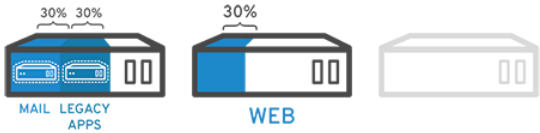
- Καλύτερη αξιοποίηση πόρων



Με Εικονικοποίηση

Διαφορές

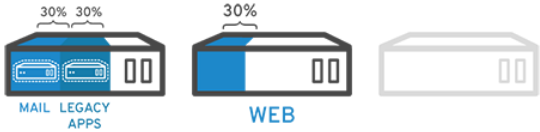
- Καλύτερη αξιοποίηση πόρων
- Εξοικονόμηση κόστους



Με Εικονικοποίηση

Διαφορές

- Καλύτερη αξιοποίηση πόρων
- Εξοικονόμηση κόστους
- Ευκολότερη διαχείριση



Επιπρόσθετα Πλεονεκτήματα

Προσφέρει

Επιπρόσθετα Πλεονεκτήματα

Προσφέρει

- Ταχύτερη παροχή

Επιπρόσθετα Πλεονεκτήματα

Προσφέρει

- Ταχύτερη παροχή
- Ελάχιστος χρόνος διακοπής λειτουργίας

Επιπρόσθετα Πλεονεκτήματα

Προσφέρει

- Ταχύτερη παροχή
- Ελάχιστος χρόνος διακοπής λειτουργίας
- Καμία ανάγκη για επιπλέον υλικό

Υπερ-επόπτες

Ορισμός
Ένα λογισμικό, το οποίο διαχειρίζεται τους φυσικούς πόρους ενός διακομιστή, απομονώνοντάς τους σε διακριτά υποσύνολα αυτών.

Υπερ-επόπτες

Ορισμός
Ένα λογισμικό, το οποίο διαχειρίζεται τους φυσικούς πόρους ενός διακομιστή, απομονώνοντάς τους σε διακριτά υποσύνολα αυτών.

Είδη

Υπερ-επόπτες

Ορισμός
Ένα λογισμικό, το οποίο διαχειρίζεται τους φυσικούς πόρους ενός διακομιστή, απομονώνοντάς τους σε διακριτά υποσύνολα αυτών.

Είδη

- Υπερ-επόπτης Τύπου 1 (Bare Metal)

Υπερ-επόπτες

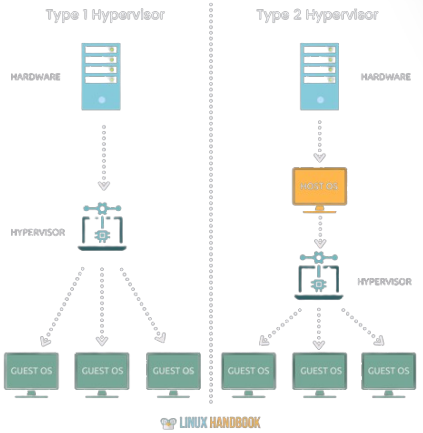
Ορισμός
Ένα λογισμικό, το οποίο διαχειρίζεται τους φυσικούς πόρους ενός διακομιστή, απομονώνοντάς τους σε διακριτά υποσύνολα αυτών.

Είδη

- Υπερ-επόπτης Τύπου 1 (Bare Metal)
- Υπερ-επόπτης Τύπου 2 (Hosted)

Διαφορές υπερ-επόπτη Τύπου 1 και 2

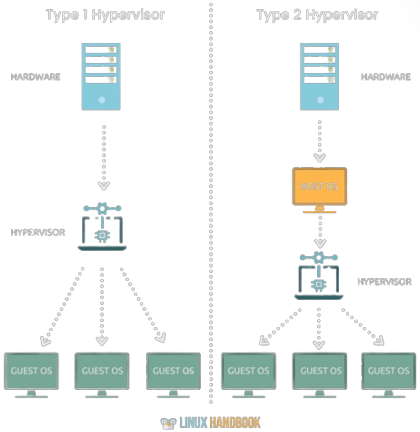
Οι υπερ-επόπτες τύπου 1:



Διαφορές υπερ-επόπτη Τύπου 1 και 2

Οι υπερ-επόπτες τύπου 1:

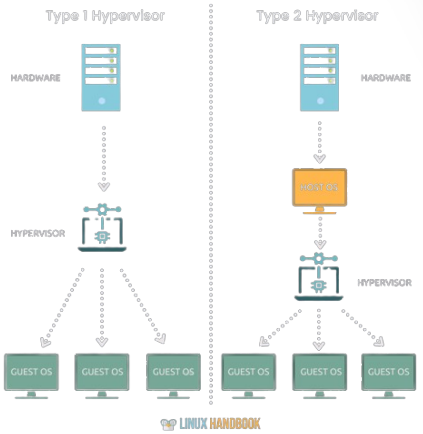
- Είναι πιο αποδοτικοί



Διαφορές υπερ-επόπτη Τύπου 1 και 2

Οι υπερ-επόπτες τύπου 1:

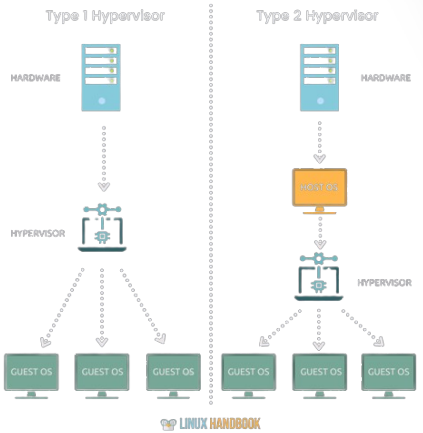
- Είναι πιο αποδοτικοί
- Αντικαθιστούν το λειτουργικό σύστημα



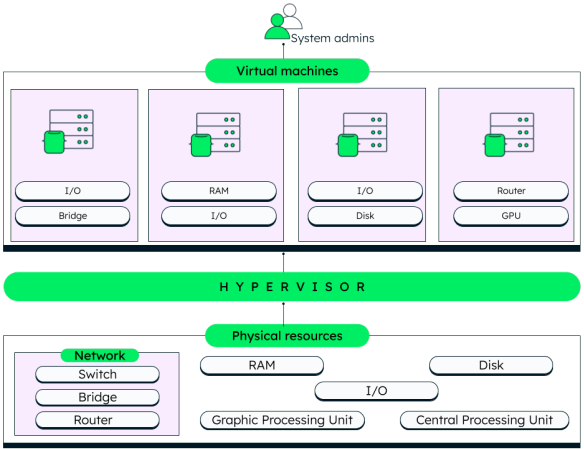
Διαφορές υπερ-επόπτη Τύπου 1 και 2

Οι υπερ-επόπτες τύπου 1:

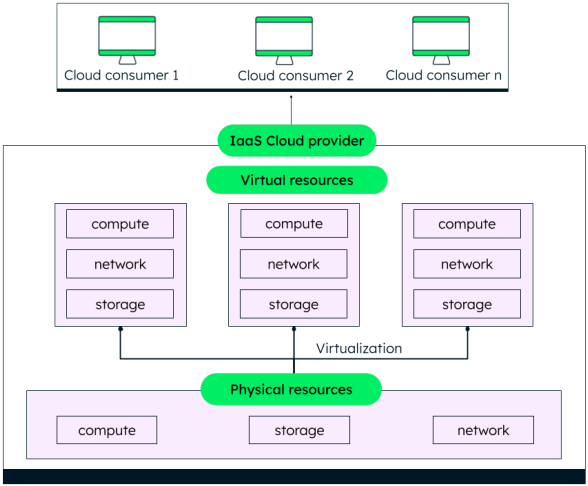
- Είναι πιο αποδοτικοί
- Αντικαθιστούν το λειτουργικό σύστημα
- Χρησιμοποιούνται σε περιβάλλοντα παραγωγής



Αλληλεξάρτηση τεχνολογιών



Αλληλεξάρτηση τεχνολογιών



Docker

Ορισμός
Μηχανή δοχείων, η οποία επιτρέπει την εκτέλεση εφαρμογών σε μορφή δοχείων.

Docker

Ορισμός
Μηχανή δοχείων, η οποία επιτρέπει την εκτέλεση εφαρμογών σε μορφή δοχείων.

Χαρακτηρίζεται από

Docker

Ορισμός
Μηχανή δοχείων, η οποία επιτρέπει την εκτέλεση εφαρμογών σε μορφή δοχείων.

Χαρακτηρίζεται από

- Μεταφερσιμότητα

Docker

Ορισμός
Μηχανή δοχείων, η οποία επιτρέπει την εκτέλεση εφαρμογών σε μορφή δοχείων.

Χαρακτηρίζεται από

- Μεταφερσιμότητα
- Ταχύτητα

Docker

Ορισμός
Μηχανή δοχείων, η οποία επιτρέπει την εκτέλεση εφαρμογών σε μορφή δοχείων.

Χαρακτηρίζεται από

- Μεταφερσιμότητα
- Ταχύτητα
- Μέγιστη χρηστικότητα πόρων

Docker

Ορισμός
Μηχανή δοχείων, η οποία επιτρέπει την εκτέλεση εφαρμογών σε μορφή δοχείων.

Χαρακτηρίζεται από

- Μεταφερσιμότητα
- Ταχύτητα
- Μέγιστη χρηστικότητα πόρων
- Ευκολία διαχείρισης

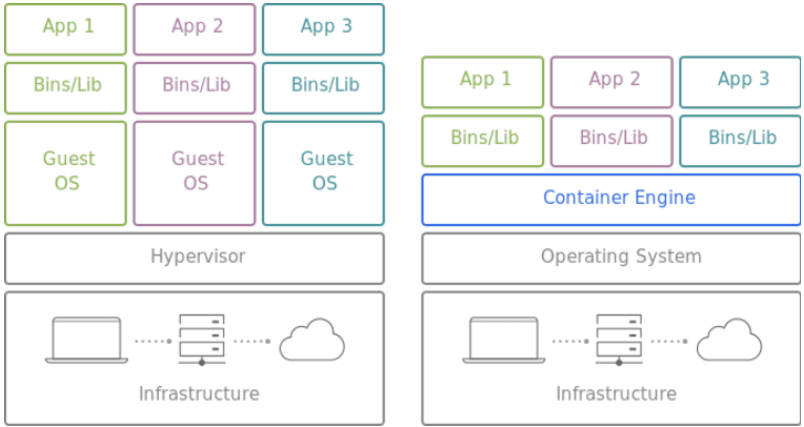
Docker

Ορισμός
Μηχανή δοχείων, η οποία επιτρέπει την εκτέλεση εφαρμογών σε μορφή δοχείων.

Χαρακτηρίζεται από

- Μεταφερσιμότητα
- Ταχύτητα
- Μέγιστη χρηστικότητα πόρων
- Ευκολία διαχείρισης
- Ασφάλεια

Εικονικές μηχανές και δοχεία



Χρήση IaaS Σήμερα

Χειροκίνητα Βήματα

Βήματα:

- Επιλογή παρόχου υπηρεσίας

Χειροκίνητα Βήματα

Βήματα:

- Επιλογή παρόχου υπηρεσίας
- Εισαγωγή στο διαδικτυακό διαχειριστικό πάνελ

Χειροκίνητα Βήματα

Βήματα:

- Επιλογή παρόχου υπηρεσίας
- Εισαγωγή στο διαδικτυακό διαχειριστικό πάνελ
- Επιλογή προδιαγραφών εικονικής μηχανής

Χειροκίνητα Βήματα

Βήματα:

- Επιλογή παρόχου υπηρεσίας
- Εισαγωγή στο διαδικτυακό διαχειριστικό πάνελ
- Επιλογή προδιαγραφών εικονικής μηχανής
- Εφαρμογή επιλογών

Το πρόβλημα ανεξαρτήτως παρόχου

- Χρονοβόρα διαδικασία

Το πρόβλημα ανεξαρτήτως παρόχου

- Χρονοβόρα διαδικασία
- Πιθανότητα λάθους

Το πρόβλημα ανεξαρτήτως παρόχου

- Χρονοβόρα διαδικασία
- Πιθανότητα λάθους
- Εγκλωβισμός σε έναν πάροχο

Το πρόβλημα ανεξαρτήτως παρόχου

- Χρονοβόρα διαδικασία
- Πιθανότητα λάθους
- Εγκλωβισμός σε έναν πάροχο
- Ανάγκη για επαναλαμβανόμενες διαδικασίες

Το πρόβλημα ανεξαρτήτως παρόχου

- Χρονοβόρα διαδικασία
- Πιθανότητα λάθους
- Εγκλωβισμός σε έναν πάροχο
- Ανάγκη για επαναλαμβανόμενες διαδικασίες
- Χειροκίνητη σκλήρυνση

Γιατί επιλέγεται το IaaS;

- Ευελιξία

Γιατί επιλέγεται το IaaS;

- Ευελιξία
- Αποδοτικότητα

Γιατί επιλέγεται το IaaS;

- Ευελιξία
- Αποδοτικότητα
- Ασφάλεια

Γιατί επιλέγεται το IaaS;

- Ευελιξία
- Αποδοτικότητα
- Ασφάλεια
- Αξιοπιστία

Γιατί επιλέγεται το IaaS;

- Ευελιξία
- Αποδοτικότητα
- Ασφάλεια
- Αξιοπιστία
- Εξοικονόμηση χρόνου

Γιατί επιλέγεται το IaaS;

- Ευελιξία
- Αποδοτικότητα
- Ασφάλεια
- Αξιοπιστία
- Εξοικονόμηση χρόνου
- Εξοικονόμηση κόστους

Θέματα Ασφαλείας

Προβλήματα που μπορεί να προκύψουν

- Απαιτείται εμπιστοσύνη προς τον πάροχο

Προβλήματα που μπορεί να προκύψουν

- Απαιτείται εμπιστοσύνη προς τον πάροχο
- Χαμηλού επιπέδου προκαθορισμένες ρυθμίσεις ασφαλείας

Προβλήματα που μπορεί να προκύψουν

- Απαιτείται εμπιστοσύνη προς τον πάροχο
- Χαμηλού επιπέδου προκαθορισμένες ρυθμίσεις ασφαλείας
- Πλήρη εξάρτηση από τον πάροχο

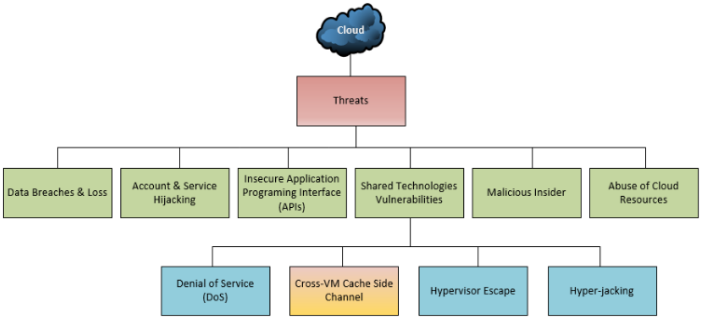
Προβλήματα που μπορεί να προκύψουν

- Απαιτείται εμπιστοσύνη προς τον πάροχο
- Χαμηλού επιπέδου προκαθορισμένες ρυθμίσεις ασφαλείας
- Πλήρη εξάρτηση από τον πάροχο
- Επιθέσεις στο νέφος

Προβλήματα που μπορεί να προκύψουν

- Απαιτείται εμπιστοσύνη προς τον πάροχο
- Χαμηλού επιπέδου προκαθορισμένες ρυθμίσεις ασφαλείας
- Πλήρη εξάρτηση από τον πάροχο
- Επιθέσεις στο νέφος
- Επιθέσεις στα δοχεία

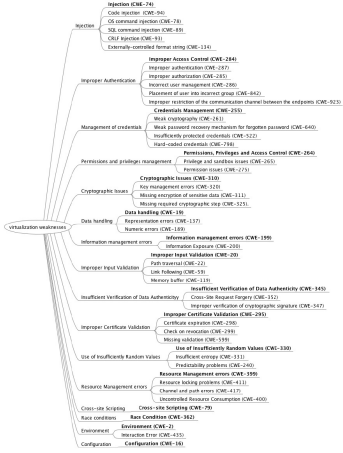
Απειλές στο Νέφος



Σημεία αδυναμίας

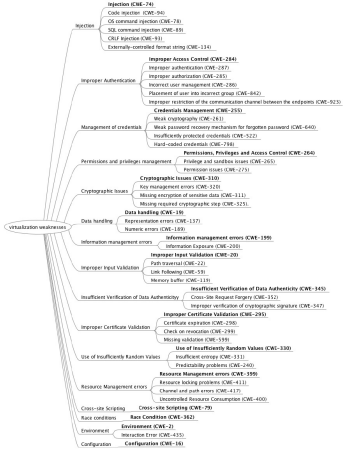
- Παρατηρήσεις

Σημεία αδυναμίας



- Παρατηρήσεις
  - 16 group απειλών

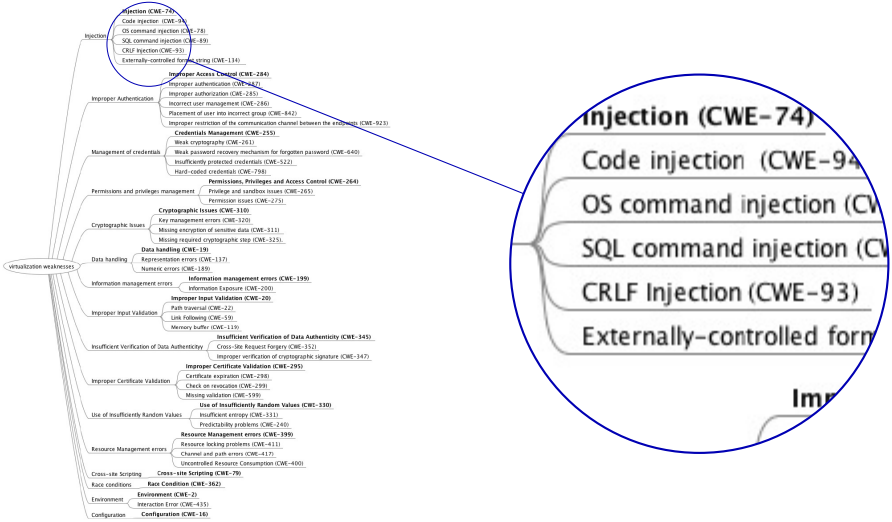
Σημεία αδυναμίας



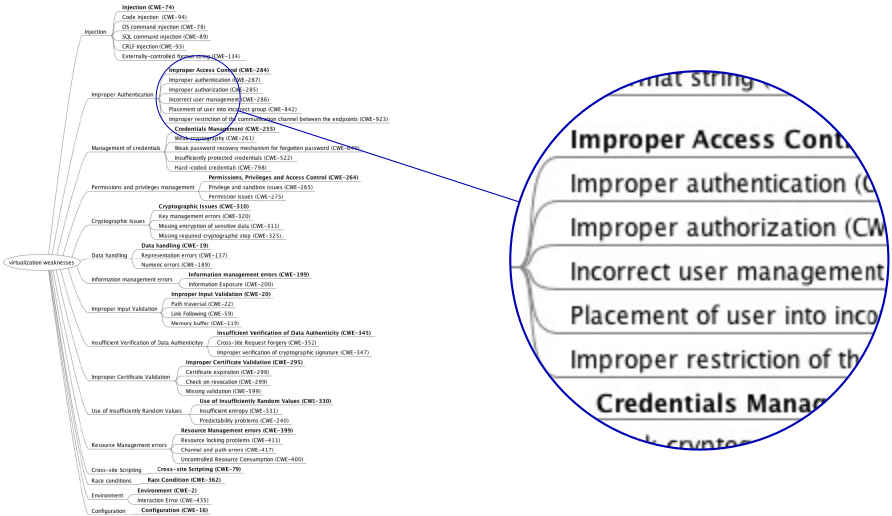
- Παρατηρήσεις
  - 16 group απειλών
  - 39 ξεχωριστά CWEs

Σημεία αδυναμίας

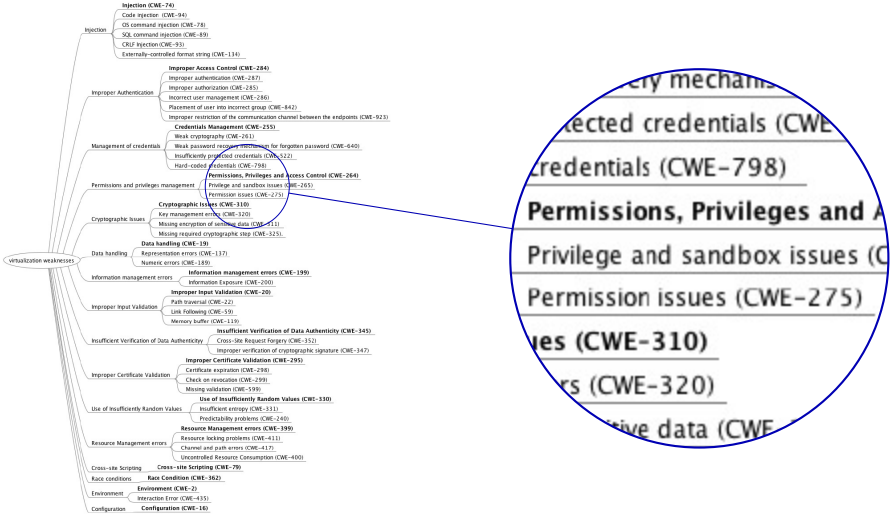
Σημεία αδυναμίας



Σημεία αδυναμίας



Σημεία αδυναμίας



Συχνές επιθέσεις στο Docker

Κίνδυνος από

Συχνές επιθέσεις στο Docker

Κίνδυνος από

- Εκμεταλλεύσεις πυρήνα (Kernel Exploits)

Συχνές επιθέσεις στο Docker

Κίνδυνος από

- Εκμεταλλεύσεις πυρήνα (Kernel Exploits)
- Άρνηση υπηρεσίας

Συχνές επιθέσεις στο Docker

Κίνδυνος από

- Εκμεταλλεύσεις πυρήνα (Kernel Exploits)
- Άρνηση υπηρεσίας
- Αποδράσεις Δοχείων (Container Breakouts)

Συχνές επιθέσεις στο Docker

Κίνδυνος από

- Εκμεταλλεύσεις πυρήνα (Kernel Exploits)
- Άρνηση υπηρεσίας
- Αποδράσεις Δοχείων (Container Breakouts)
- Δηλητηριασμένες εικόνες δοχείων

Συχνές επιθέσεις στο Docker

Κίνδυνος από

- Εκμεταλλεύσεις πυρήνα (Kernel Exploits)
- Άρνηση υπηρεσίας
- Αποδράσεις Δοχείων (Container Breakouts)
- Δηλητηριασμένες εικόνες δοχείων
- Απόκτηση μυστικών κωδικών/κλειδιών

Συχνές επιθέσεις στο Docker

Κίνδυνος από

- Εκμεταλλεύσεις πυρήνα (Kernel Exploits)
- Άρνηση υπηρεσίας
- Αποδράσεις Δοχείων (Container Breakouts)
- Δηλητηριασμένες εικόνες δοχείων
- Απόκτηση μυστικών κωδικών/κλειδιών
- Ενδιάμεσου (Man-in-the-Middle - MitM)

Συχνές επιθέσεις στο Docker

Κίνδυνος από

- Εκμεταλλεύσεις πυρήνα (Kernel Exploits)
- Άρνηση υπηρεσίας
- Αποδράσεις Δοχείων (Container Breakouts)
- Δηλητηριασμένες εικόνες δοχείων
- Απόκτηση μυστικών κωδικών/κλειδιών
- Ενδιάμεσου (Man-in-the-Middle - MitM)
- Πλαστογράφηση ARP (ARP spoofing)

Η τριάδα της ασφάλειας

- Εμπιστευτικότητα
- Ακεραιότητα
- Διαθεσιμότητα

Η τριάδα της ασφάλειας

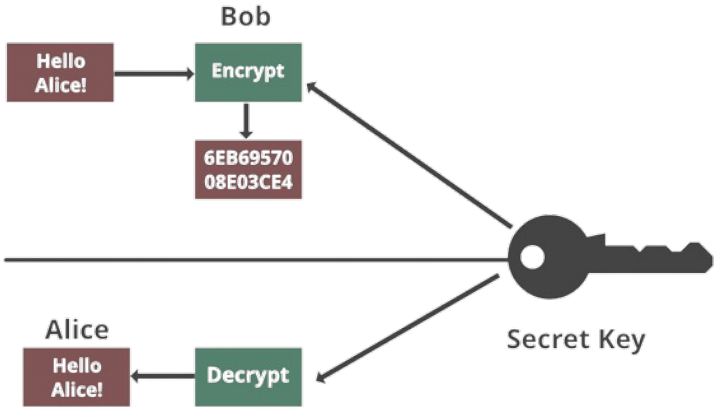
- Εμπιστευτικότητα
  - Προστασία από αποκάλυψη
- Ακεραιότητα
- Διαθεσιμότητα

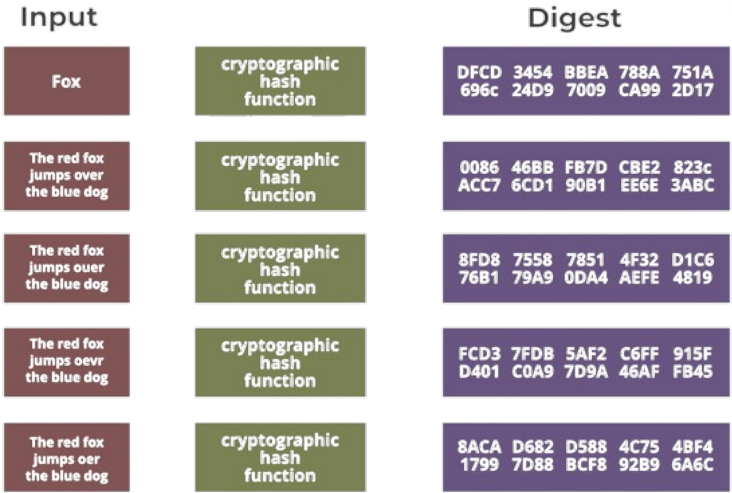
Η τριάδα της ασφάλειας

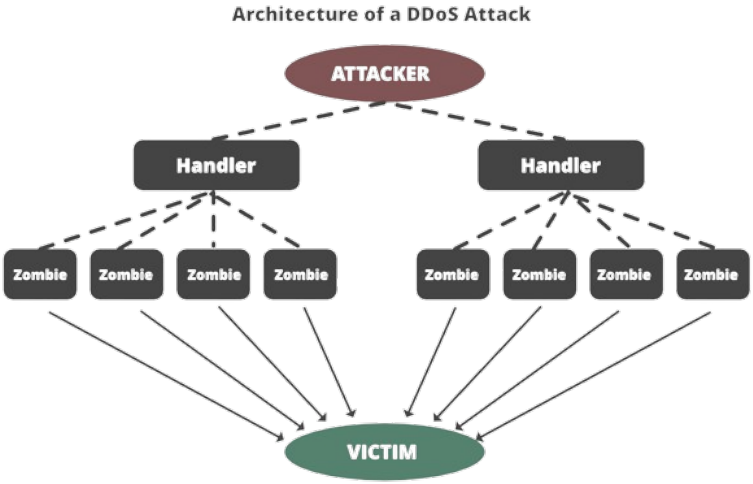
- Εμπιστευτικότητα
  - Προστασία από αποκάλυψη
- Ακεραιότητα
  - Προστασία από αλλοίωση
- Διαθεσιμότητα

Η τριάδα της ασφάλειας

- Εμπιστευτικότητα
  - Προστασία από αποκάλυψη
- Ακεραιότητα
  - Προστασία από αλλοίωση
- Διαθεσιμότητα
  - Προστασία από απώλεια


Bob
Hello Alice!
Encrypt
6EB69570 08E03CE4
Secret Key
Alice
Hello Alice!
Decrypt


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696c 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823c ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C


Architecture of a DDoS Attack
ATTACKER
Handler
Handler
Zombie
Zombie
Zombie
Zombie
Zombie
Zombie
Zombie
Zombie
VICTIM

Ορθές πρακτικές στην εικονικοποίηση

Ορθές πρακτικές στην εικονικοποίηση

- Συχνή ενημέρωση του υπερ-επόπτη

Ορθές πρακτικές στην εικονικοποίηση

- Συχνή ενημέρωση του υπερ-επόπτη
- Περιορισμός πρόσβασης στο διαχειριστικό πάνελ του υπερ-επόπτη

Ορθές πρακτικές στην εικονικοποίηση

- Συχνή ενημέρωση του υπερ-επόπτη
- Περιορισμός πρόσβασης στο διαχειριστικό πάνελ του υπερ-επόπτη
- Έλεγχος των μηχανημάτων που έχουν πρόσβαση στον υπερ-επόπτη

Ορθές πρακτικές στην εικονικοποίηση

- Συχνή ενημέρωση του υπερ-επόπτη
- Περιορισμός πρόσβασης στο διαχειριστικό πάνελ του υπερ-επόπτη
- Έλεγχος των μηχανημάτων που έχουν πρόσβαση στον υπερ-επόπτη
- Περιορισμός δικτυακής πρόσβασης στο διαχειριστικό πάνελ του υπερ-επόπτη

Ορθές πρακτικές στην εικονικοποίηση

- Συχνή ενημέρωση του υπερ-επόπτη
- Περιορισμός πρόσβασης στο διαχειριστικό πάνελ του υπερ-επόπτη
- Έλεγχος των μηχανημάτων που έχουν πρόσβαση στον υπερ-επόπτη
- Περιορισμός δικτυακής πρόσβασης στο διαχειριστικό πάνελ του υπερ-επόπτη
- Χρήση κρυπτογράφησης εικονικών μηχανών

Ορθές πρακτικές στην εικονικοποίηση

- Συχνή ενημέρωση του υπερ-επόπτη
- Περιορισμός πρόσβασης στο διαχειριστικό πάνελ του υπερ-επόπτη
- Έλεγχος των μηχανημάτων που έχουν πρόσβαση στον υπερ-επόπτη
- Περιορισμός δικτυακής πρόσβασης στο διαχειριστικό πάνελ του υπερ-επόπτη
- Χρήση κρυπτογράφησης εικονικών μηχανών
- Απομόνωση των εικονικών μηχανών μεταξύ τους

Ορθές πρακτικές στην εικονικοποίηση

- Συχνή ενημέρωση του υπερ-επόπτη
- Περιορισμός πρόσβασης στο διαχειριστικό πάνελ του υπερ-επόπτη
- Έλεγχος των μηχανημάτων που έχουν πρόσβαση στον υπερ-επόπτη
- Περιορισμός δικτυακής πρόσβασης στο διαχειριστικό πάνελ του υπερ-επόπτη
- Χρήση κρυπτογράφησης εικονικών μηχανών
- Απομόνωση των εικονικών μηχανών μεταξύ τους
- Παρακολούθηση των πόρων

Ορθές πρακτικές στην εικονικοποίηση

- Συχνή ενημέρωση του υπερ-επόπτη
- Περιορισμός πρόσβασης στο διαχειριστικό πάνελ του υπερ-επόπτη
- Έλεγχος των μηχανημάτων που έχουν πρόσβαση στον υπερ-επόπτη
- Περιορισμός δικτυακής πρόσβασης στο διαχειριστικό πάνελ του υπερ-επόπτη
- Χρήση κρυπτογράφησης εικονικών μηχανών
- Απομόνωση των εικονικών μηχανών μεταξύ τους
- Παρακολούθηση των πόρων
- Ορθή διαχείριση στιγμιοτύπων εικονικών μηχανών

Ορθές πρακτικές στην εικονικοποίηση

- Συχνή ενημέρωση του υπερ-επόπτη
- Περιορισμός πρόσβασης στο διαχειριστικό πάνελ του υπερ-επόπτη
- Έλεγχος των μηχανημάτων που έχουν πρόσβαση στον υπερ-επόπτη
- Περιορισμός δικτυακής πρόσβασης στο διαχειριστικό πάνελ του υπερ-επόπτη
- Χρήση κρυπτογράφησης εικονικών μηχανών
- Απομόνωση των εικονικών μηχανών μεταξύ τους
- Παρακολούθηση των πόρων
- Ορθή διαχείριση στιγμιοτύπων εικονικών μηχανών
- Ασφάλιση του μηχανήματος φιλοξενίας

Ορθές πρακτικές στην εικονικοποίηση

- Συχνή ενημέρωση του υπερ-επόπτη
- Περιορισμός πρόσβασης στο διαχειριστικό πάνελ του υπερ-επόπτη
- Έλεγχος των μηχανημάτων που έχουν πρόσβαση στον υπερ-επόπτη
- Περιορισμός δικτυακής πρόσβασης στο διαχειριστικό πάνελ του υπερ-επόπτη
- Χρήση κρυπτογράφησης εικονικών μηχανών
- Απομόνωση των εικονικών μηχανών μεταξύ τους
- Παρακολούθηση των πόρων
- Ορθή διαχείριση στιγμιοτύπων εικονικών μηχανών
- Ασφάλιση του μηχανήματος φιλοξενίας
- Σκλήρυνση των εικονικών μηχανών

Ορθές πρακτικές το Docker

Ορθές πρακτικές το Docker

- Χρήση ελάχιστων δικαιωμάτων

Ορθές πρακτικές το Docker

- Χρήση ελάχιστων δικαιωμάτων
- Χρήση read-only

Ορθές πρακτικές το Docker

- Χρήση ελάχιστων δικαιωμάτων
- Χρήση read-only
- Περιορισμός πόρων

Ορθές πρακτικές το Docker

- Χρήση ελάχιστων δικαιωμάτων
- Χρήση read-only
- Περιορισμός πόρων
- Αποφυγή privileged

Ορθές πρακτικές το Docker

- Χρήση ελάχιστων δικαιωμάτων
- Χρήση read-only
- Περιορισμός πόρων
- Αποφυγή privileged
- Εικόνες δοχείων από έμπιστες πηγές

Ορθές πρακτικές το Docker

- Χρήση ελάχιστων δικαιωμάτων
- Χρήση read-only
- Περιορισμός πόρων
- Αποφυγή privileged
- Εικόνες δοχείων από έμπιστες πηγές
- Αποφυγή επικοινωνίας δοχείων μεταξύ τους

Ορθές πρακτικές το Docker

- Χρήση ελάχιστων δικαιωμάτων
- Χρήση read-only
- Περιορισμός πόρων
- Αποφυγή privileged
- Εικόνες δοχείων από έμπιστες πηγές
- Αποφυγή επικοινωνίας δοχείων μεταξύ τους
- Χρήση Kernel Capabilities

Ορθές πρακτικές το Docker

- Χρήση ελάχιστων δικαιωμάτων
- Χρήση read-only
- Περιορισμός πόρων
- Αποφυγή privileged
- Εικόνες δοχείων από έμπιστες πηγές
- Αποφυγή επικοινωνίας δοχείων μεταξύ τους
- Χρήση Kernel Capabilities
- Χρήση Kernel Security Modules

Ορθές πρακτικές το Docker

- Χρήση ελάχιστων δικαιωμάτων
- Χρήση read-only
- Περιορισμός πόρων
- Αποφυγή privileged
- Εικόνες δοχείων από έμπιστες πηγές
- Αποφυγή επικοινωνίας δοχείων μεταξύ τους
- Χρήση Kernel Capabilities
- Χρήση Kernel Security Modules
- Χρήση χώρων ονομάτων

Απαίτηση αυτοματοποίησης

Απαίτηση αυτοματοποίησης

- Δημιουργία εικονικών μηχανών

Απαίτηση αυτοματοποίησης

- Δημιουργία εικονικών μηχανών
- Σκλήρυνση εικονικών μηχανών

Απαίτηση αυτοματοποίησης

- Δημιουργία εικονικών μηχανών
- Σκλήρυνση εικονικών μηχανών
- Σκλήρυνση Docker

Σχετικές Εργασίες

Υπάρχουσες λύσεις εργαλείων

- Για δημιουργία εικονικών μηχανών
- Για σκλήρυνση εικονικών μηχανών
- Για σκλήρυνση Docker

Υπάρχουσες λύσεις εργαλείων

- Για δημιουργία εικονικών μηχανών
  - Terraform
- Για σκλήρυνση εικονικών μηχανών
- Για σκλήρυνση Docker

Υπάρχουσες λύσεις εργαλείων

- Για δημιουργία εικονικών μηχανών
  - Terraform
  - Libcloud CLI
- Για σκλήρυνση εικονικών μηχανών

- Για σκλήρυνση Docker

Υπάρχουσες λύσεις εργαλείων

- Για δημιουργία εικονικών μηχανών
  - Terraform
  - Libcloud CLI
- Για σκλήρυνση εικονικών μηχανών
  - JShielder
- Για σκλήρυνση Docker

Υπάρχουσες λύσεις εργαλείων

- Για δημιουργία εικονικών μηχανών
  - Terraform
  - Libcloud CLI
- Για σκλήρυνση εικονικών μηχανών
  - JShielder
  - nixarmor
- Για σκλήρυνση Docker

Υπάρχουσες λύσεις εργαλείων

- Για δημιουργία εικονικών μηχανών
  - Terraform
  - Libcloud CLI
- Για σκλήρυνση εικονικών μηχανών
  - JShielder
  - nixarmor
- Για σκλήρυνση Docker
  - docker-rootless-setup

Υπάρχουσες λύσεις εργαλείων

- Για δημιουργία εικονικών μηχανών
  - Terraform
  - Libcloud CLI
- Για σκλήρυνση εικονικών μηχανών
  - JShielder
  - nixarmor
- Για σκλήρυνση Docker
  - docker-rootless-setup
  - docksec

Σύγκριση με group 1 (Δημιουργία VM)

Κριτήρια	Terraform	Libcloud CLI	SecDep
Ευελιξία κατά την χρήση	Όλες οι προδιαγραφές δηλώνονται σε αρχείο κειμένου.	Επιλογή παραμέτρων κατά την σύνταξη.	Επιλογή παραμέτρων κατά την σύνταξη.
Ευκολία χρήσης	Κάθε αλλαγή απαιτεί τροποποίηση του αρχείου προδιαγραφών.	Οι παράμετροι είναι εύκολες στην κατανόηση και την χρήση.	Οι παράμετροι είναι εύκολες στην κατανόηση και την χρήση.
Εύρος υποστήριξης παρόχων	Όλοι οι μεγάλοι και μικροί πάροχοι υποστηρίζονται.	Μονάχα ένας πάροχος υποστηρίζεται.	Υποστηρίζονται όλοι οι μεγάλοι πάροχοι.
Επεκτασιμότητα	Λόγω της αρχιτεκτονικής του είναι δυσκολότερη η επέκτασή του.	Επεκτείνεται εύκολα με τροποποίηση του εκτελέσιμου αρχείου.	Επεκτείνεται εύκολα με τροποποίηση του εκτελέσιμου αρχείου.

Σύγκριση με group 2 (Σκλήρυνση VM)

Κριτήρια	JShielder	nixarmor	SecDep
Εύρος υποστήριξης διανομών	Υποστηρίζεται μια διανομή με δύο εκδόσεις.	Υποστηρίζονται 4 διανομές.	Υποστηρίζονται 6 διανομές με πολλαπλές εκδόσεις τους.
Ευκολία χρήσης	Αρκεί η εκτέλεσή του με διαχειριστικά δικαιώματα.	Αρκεί η εκτέλεση ενός εκτελέσιμου αρχείου του με διαχειριστικά δικαιώματα.	Αρκεί η εκτέλεσή του με διαχειριστικά δικαιώματα.
Εύρος σκλήρυνσης	Ικανοποιητικό εύρος σκλήρυνσης.	Μικρότερο συγκριτικά με τα υπόλοιπα.	Επιτυγχάνεται σε ικανοποιητικό βαθμό.
Υποστήριξη διαρκούς σκλήρυνσης	Διαρκής ενημέρωση πακέτων.	Διαρκείς ενημερώσεις ασφαλείας σε μια διανομή.	Διαρκείς ενημερώσεις ασφαλείας και πακέτων, κλείσιμο αχρησιμοποίητων θυρών.

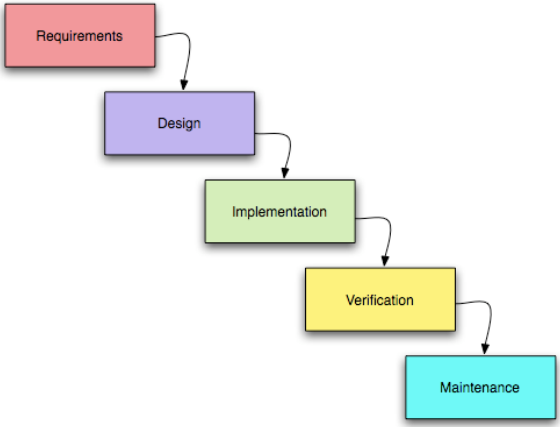
Σύγκριση με group 3 (Σκλήρυνση Docker)

Κριτήρια	docker-rootless-setup	docksec	SecDep
Ευκολία χρήσης	Αρκεί η εκτέλεσή του με διαχειριστικά δικαιώματα.	Αρκεί να εκτελεστεί με διαχειριστικά δικαιώματα.	Αρκεί η εκτέλεσή του με διαχειριστικά δικαιώματα.
Εύρος σκλήρυνσης	Μονάχα εγκατάσταση του Rootless Docker.	Μονάχα καλύτερη ρύθμιση του δαίμονα.	Καλύτερη ρύθμιση του δαίμονα, εγκατάσταση του Rootless Docker, αντικατάσταση προκαθορισμένου Container Runtime.
Υποστήριξη διαρκούς σκλήρυνσης	Όχι.	Όχι.	Εγκατάσταση του watchtower.
Επεκτασιμότητα	Αρκεί η προσθήκη νέων λειτουργιών στο εκτελέσιμο αρχείο του.	Αρκεί η προσθήκη νέων λειτουργιών στο εκτελέσιμο αρχείο του.	Αρκεί η προσθήκη νέων λειτουργιών στο εκτελέσιμο αρχείο του.

Προτεινόμενη Λύση

Ανάπτυξη του SecDep

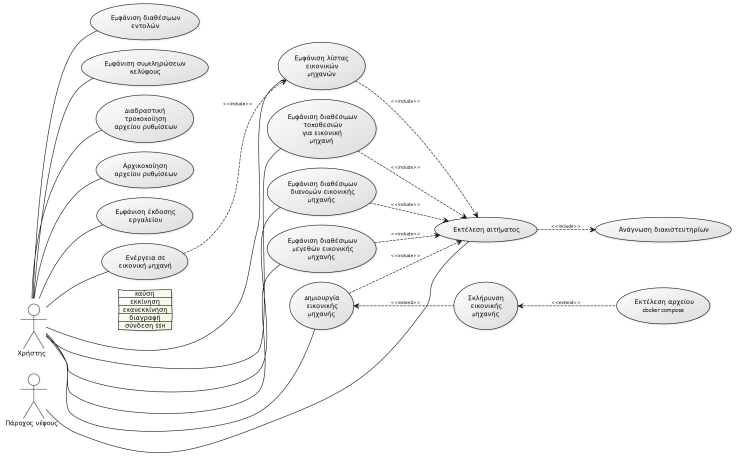
Μοντέλο Ανάπτυξης



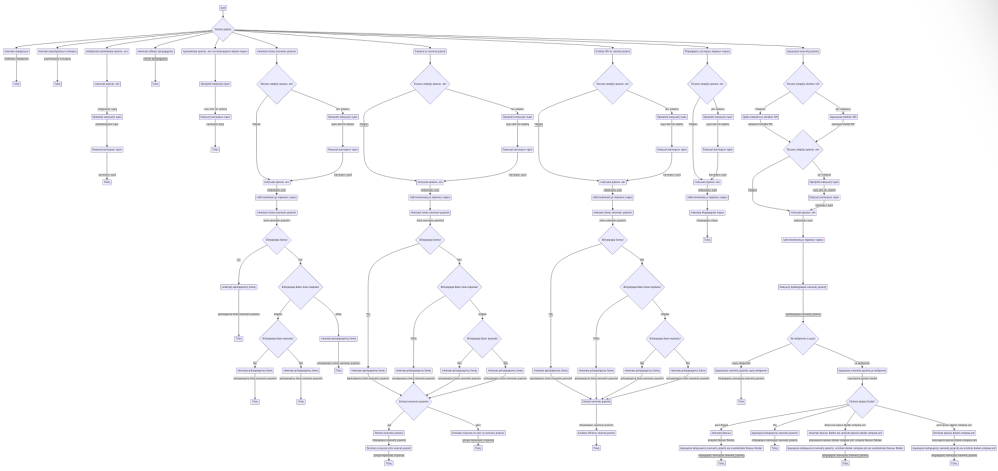
Απαιτήσεις Συστήματος

- Λειτουργικές απαιτήσεις
  - Εμφάνιση μεγεθών, τοποθεσιών και διανομών εικονικών μηχανών
  - Προτροπή για ελλειπή παράμετρο
  - Έλεγχος εγκυρότητας των παραμέτρων
  - Δημιουργία εικονικής μηχανής
  - Παύση, εκκίνηση, επανεκκίνηση και διαγραφή εικονικής μηχανής
  - Σύνδεση με SSH
  - Εμφάνιση εικονικών μηχανών
  - Εμφάνιση σφαλμάτων
  - Διαδραστική διαμόρφωση αρχείου ρυθμίσεων
  - Σκλήρυνση εικονικών μηχανών
  - Εγκατάσταση/Σκλήρυνση του Docker
  - Περιοδική ενημέρωση πακέτων
  - Κλείσιμο αχρησιμοποίητων θυρών
  - Εγκατάσταση δοχείων
  - Εκτέλεση docker-compose.yml
  - Εμφάνιση διαθέσιμων εντολών, συμπληρώσεων κελύφους και έκδοσης προγράμματος
  - Παράμετρος προσπέρασης επιβεβαίωσης
  - Ύπαρξη μηχανισμού συγκεκριμενοποίησης περιοχής της AWS
  - Ύπαρξη μηχανισμού επιλογής θύρας SSH συνδέσεων
  - Ύπαρξη μηχανισμού αρχικοποίησης ρυθμίσεων ενός μόνο παρόχου
- Μη λειτουργικές απαιτήσεις
  - Υποστήριξη νεφών από Amazon, Google, Microsoft
  - Υποστήριξη των διανομών Debian, Ubuntu, Red Hat Enterprise Linux, Fedora, CentOS, openSUSE Leap
  - Λειτουργία μέσω της γραμμής εντολών
  - Ευκολία στην χρήση
  - Αξιοπιστία
  - Δημιουργία αρχείου ρυθμίσεων
  - Δημιουργία αρχείου με τις IP διευθύνσεις των εικονικών μηχανών
  - Δημιουργία κλειδιών SSH
  - Εγκατάσταση των watchtower και portainer

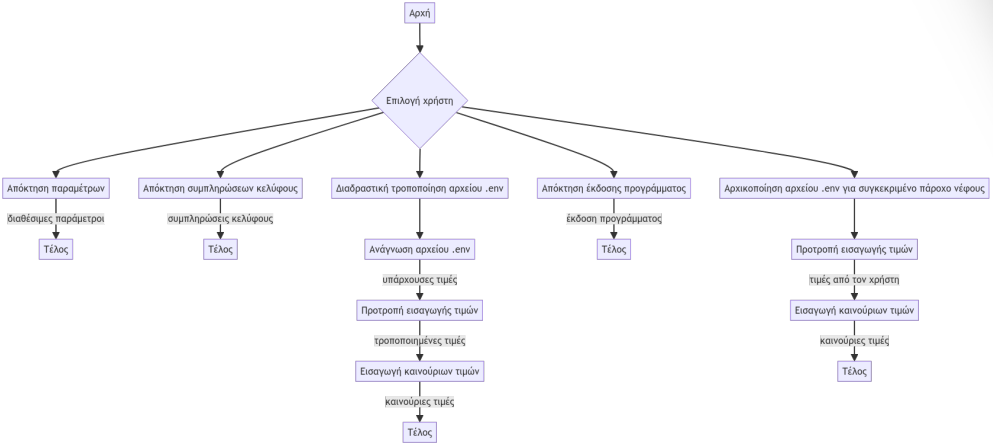
Διάγραμμα περιπτώσεων χρήσης



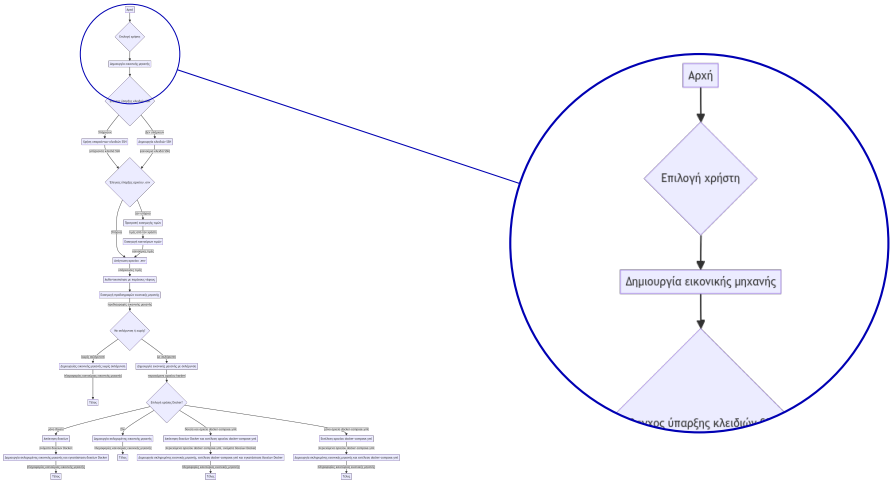
Διάγραμμα ροών



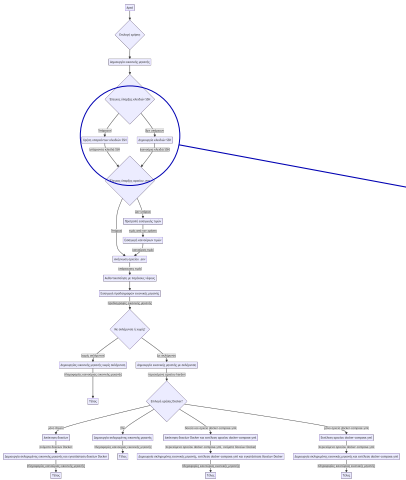
Ροές απλών λειτουργιών

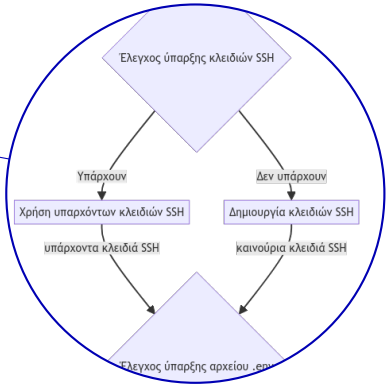


Ροή - Δημιουργία εικονικής μηχανής

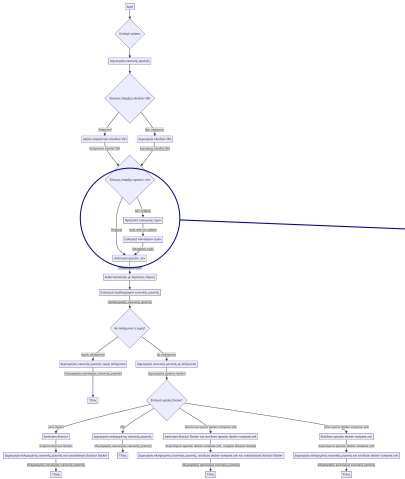


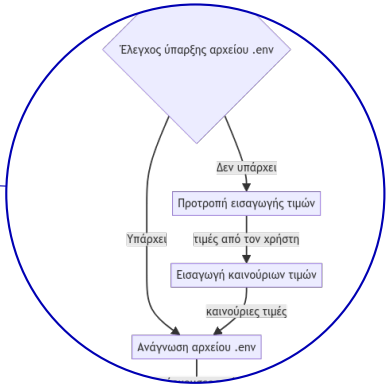
Ροή - Δημιουργία εικονικής μηχανής



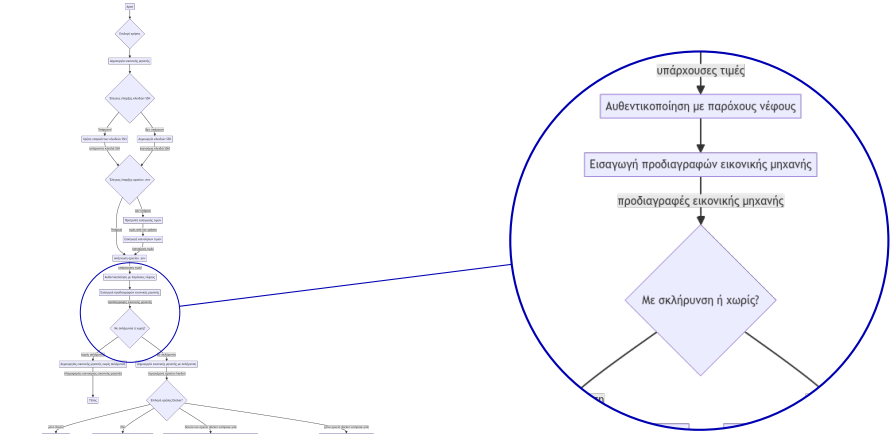


Ροή - Δημιουργία εικονικής μηχανής

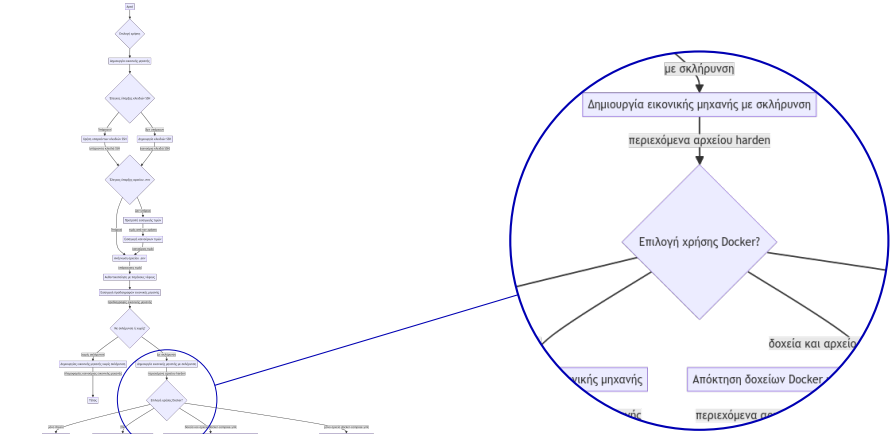




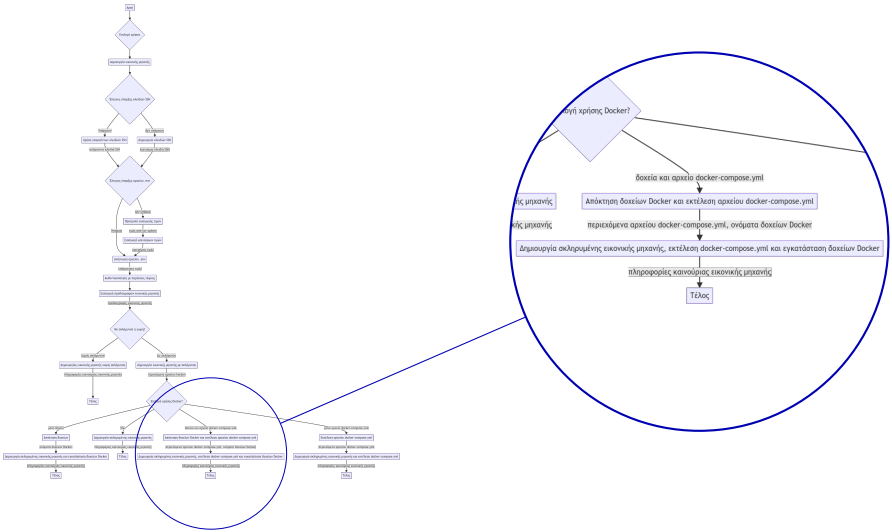
Ροή - Δημιουργία εικονικής μηχανής



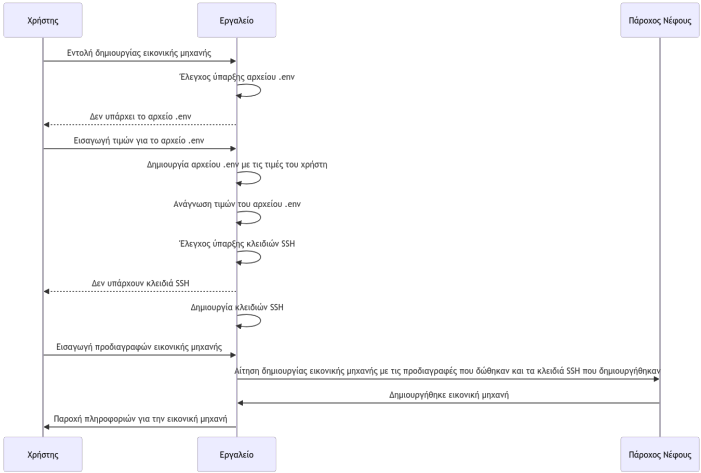
Ροή - Δημιουργία εικονικής μηχανής



Ροή - Δημιουργία εικονικής μηχανής



Διάγραμμα ακολουθίας



Υποστηριζόμενες εκδόσεις διανομών

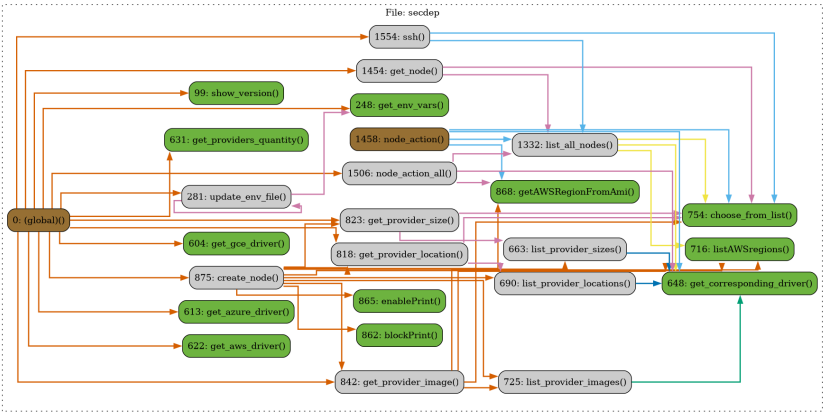
		Πάροχοι		
		AWS	Azure	GCE
Διανομές	Ubuntu	22.04, 22.10	22.04, 22.10	Όλες
	Debian	10, 11	10, 11	Όλες
	CentOS	7, 8, 9	8.4, 8.5	Όλες
	Fedora	37	36, 37	Όλες
	Red Hat Enterprise Linux	7.9, 8.6, 9	8.6, 9.1	Όλες
	openSUSE Leap	15.3, 15.4	15.3, 15.4	Όλες

Σημαντικές συναρτήσεις του SecDep

- create_node
  - provider
  - name
  - location
  - size
  - image
  - confirm
  - deploy
- node_action
  - start
  - stop
  - reboot
  - delete
- list_all_nodes
  - provider
  - filterIn
  - awsRegion

- hardenSSH
- dockerInit
- kernelSecurityModuleInit
- configureFail2ban

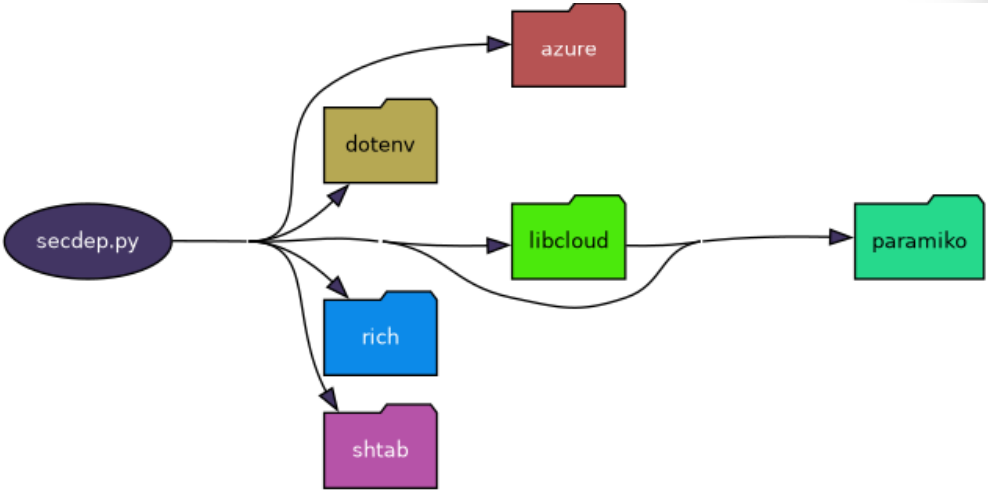
Σχέσεις συναρτήσεων του secdep.py



Code2flow Legend	
Regular function	
Trunk function (nothing calls this)	
Leaf function (this calls nothing else)	
Function call	→

Σχέσεις συναρτήσεων του harden

Εξαρτήσεις του SecDep



Εγκατάσταση και επίδειξη

Προαπαιτούμενα

Θα χρειαστούμε

Προαπαιτούμενα

Θα χρειαστούμε

- Python 3.7+

Προαπαιτούμενα

Θα χρειαστούμε

- Python 3.7+
- pip

Προαπαιτούμενα

Θα χρειαστούμε

- Python 3.7+
- pip
- git ή φυλλομετρητής

Εντολές εγκατάστασης

```
git clone https://git.konsthol.eu/konsthol/SecDep.git
```

```
cd SecDep
```

```
pip install -r requirements.txt [--break-system-packages]
```

Ρύθμιση για AWS

Απαιτείται

Ρύθμιση για AWS

Απαιτείται

- Λογαριασμός AWS

Ρύθμιση για AWS

Απαιτείται

- Λογαριασμός AWS
- Όνομα κλειδιού πρόσβασης

Ρύθμιση για AWS

Απαιτείται

- Λογαριασμός AWS
- Όνομα κλειδιού πρόσβασης
- Περιεχόμενο κλειδιού

Αντιστοιχίες τιμών

Μεταβλητή του SecDep	Αντιστοιχία
SECDEP_AWS_ACCESS_KEY	Αναγνωριστικό κλειδιού
SECDEP_AWS_SECRET_KEY	Περιεχόμενο κλειδιού

```
python3 secdep.py --init aws
```

Παραδείγματα εντολών I

- Επεξεργασία αρχείου ρυθμίσεων

```
python3 secdep.py --edit
```

- Δημιουργία απλής εικονικής μηχανής

```
python3 secdep.py --provider aws --create --name test-node --size
↪ t3.micro --image ami-08869bacfa1188ec9 --yes
```

- Δημιουργία εικονικής μηχανής με σκλήρυνση, δοχεία και εκτέλεση docker-compose.yml

```
python3 secdep.py --provider aws --create --name test-node --size
↪ t3.micro --image ami-08869bacfa1188ec9 --yes --docker_compose
↪ --deploy node mysql
```

Παραδείγματα εντολών II

- Επιλογή εικονικής μηχανής της AWS για σύνδεση SSH

```
python3 secdep.py --provider aws --ssh
```

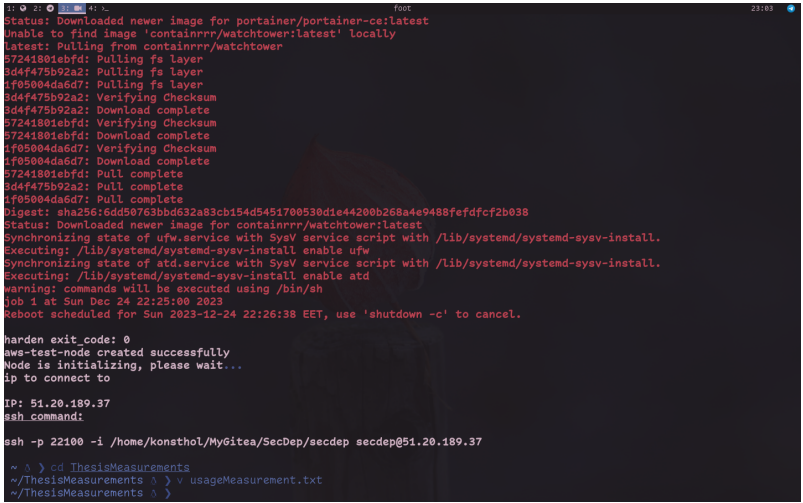
- Εμφάνιση εικονικών μηχανών συγκεκριμένης περιοχής της AWS

```
python3 secdep.py --provider aws --awsregion us-east-2 --list
```

- Επιλογή εικονικής μηχανής για διαγραφή

```
python3 secdep.py --provider aws --action delete --awsregion eu-north-1
```

Οθόνη εκτέλεσης - Δημιουργία με --deploy



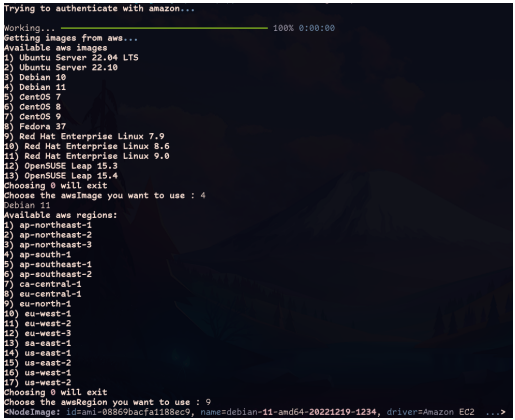
Οθόνη εκτέλεσης - Λίστα VM

Επιλογή πόρου

```
python3 secdep.py --provider aws --listimages
↪  --print
```

Αποτέλεσμα της μορφής

```
<NodeImage: id=ami-0eb2c4104acb437b2,
↪  name=debian-10-amd64-20221224-1239,
↪  driver=Amazon EC2  ...>
```



SECDEP

Αξιολόγηση

Εργαλεία Αξιολόγησης

Εργαλεία Αξιολόγησης

Χρησιμοποιήθηκαν τα:

Εργαλεία Αξιολόγησης

Χρησιμοποιήθηκαν τα:

- Lynis

Εργαλεία Αξιολόγησης

Χρησιμοποιήθηκαν τα:

- Lynis
- Lunar

Εργαλεία Αξιολόγησης

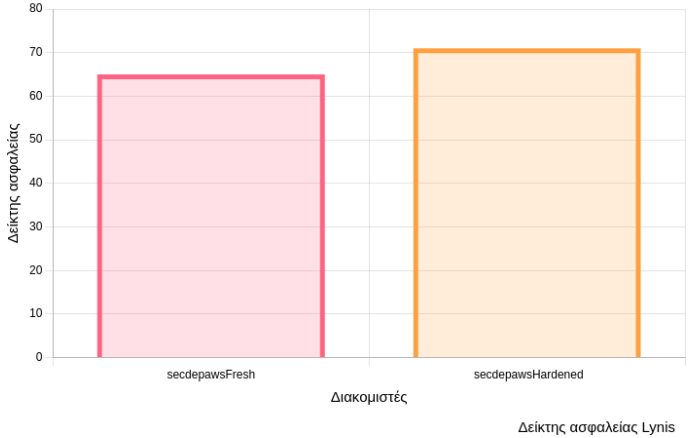
Χρησιμοποιήθηκαν τα:

- Lynis
- Lunar
- Vuls

Αποτελέσματα μέσω του Lynis

Διακομιστής	Δείκτης Ασφαλείας
Προ σκλήρυνσης	65
Μετά σκλήρυνσης	71

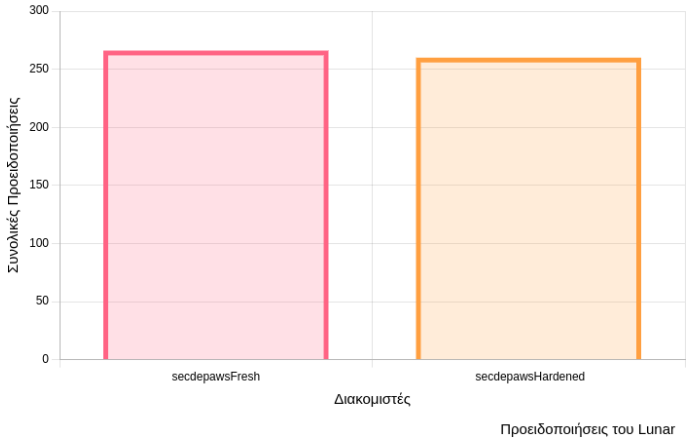
Αποτελέσματα μέσω του Lynis



Αποτελέσματα μέσω του LUNAR

Διακομιστής	Αριθμός Προειδοποιήσεων
Προ σκλήρυνσης	266
Μετά σκλήρυνσης	260

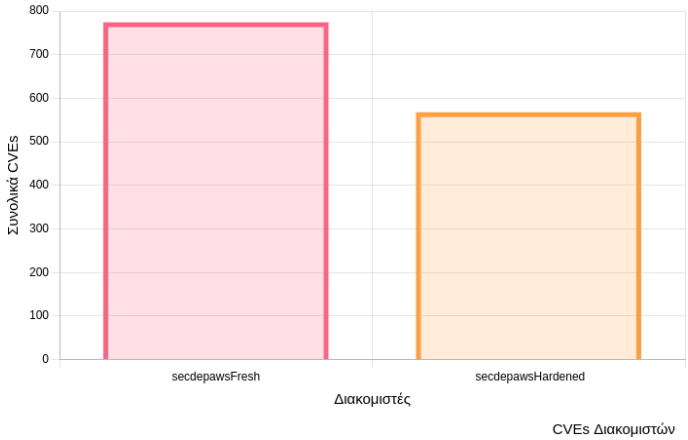
Αποτελέσματα μέσω του LUNAR



Αποτελέσματα μέσω του Vuls

Διακομιστής	Καθαρός αριθμός CVE
Προ σκλήρυνσης	774
Μετά σκλήρυνσης	568

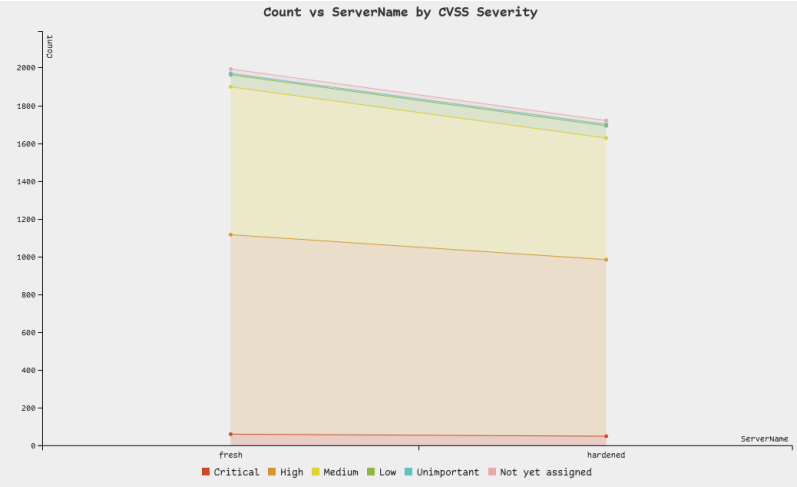
Αποτελέσματα μέσω του Vuls



Vuls - CVEs ανά κατηγορία σοβαρότητας

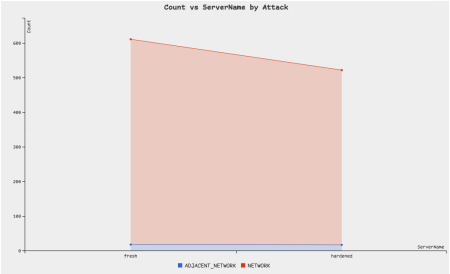
CVSS Severity \ ServerName	fresh	hardened	Totals
Critical	61	50	**111**
High	1,055	934	**1,989**
Medium	782	643	**1,425**
Low	64	65	**129**
Unimportant	7	8	**15**
Not yet assigned	23	20	**43**
Totals	**1,992**	**1,720**	**3,712**

Vuls - CVEs ανά κατηγορία σοβαρότητας



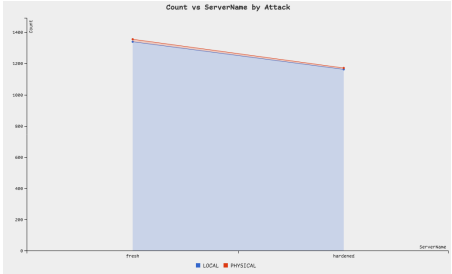
Vuls - CVEs δικτύου

Attack \ ServerName	fresh	hardened	Totals
ADJACENT_NETWORK	18	17	35
NETWORK	593	505	1,098
Totals	611	522	1,133



Vuls - Φυσικά CVEs

Attack \ ServerName	fresh	hardened	Totals
LOCAL	1,339	1,162	2,501
PHYSICAL	16	9	25
Totals	1,355	1,171	2,526



Αποτελέσματα

Με την χρήση του SecDep καταφέραμε να ασφαλίσουμε τους διακομιστές σε ικανοποιητικό βαθμό.

Αποτελέσματα

Με την χρήση του SecDep καταφέραμε να ασφαλίσουμε τους διακομιστές σε ικανοποιητικό βαθμό.

Αύξηση ασφάλειας

Αποτελέσματα

Με την χρήση του SecDep καταφέραμε να ασφαλίσουμε τους διακομιστές σε ικανοποιητικό βαθμό.

Αύξηση ασφάλειας

- Vuls 26.62%

Αποτελέσματα

Με την χρήση του SecDep καταφέραμε να ασφαλίσουμε τους διακομιστές σε ικανοποιητικό βαθμό.

Αύξηση ασφάλειας

- Vuls 26.62%
  - Ευπάθειες δικτύου 14.57%

Αποτελέσματα

Με την χρήση του SecDep καταφέραμε να ασφαλίσουμε τους διακομιστές σε ικανοποιητικό βαθμό.

Αύξηση ασφάλειας

- Vuls 26.62%
  - Ευπάθειες δικτύου 14.57%
  - Φυσικές ευπάθειες 13.58%

Αποτελέσματα

Με την χρήση του SecDep καταφέραμε να ασφαλίσουμε τους διακομιστές σε ικανοποιητικό βαθμό.

Αύξηση ασφάλειας

- Vuls 26.62%
  - Ευπάθειες δικτύου 14.57%
  - Φυσικές ευπάθειες 13.58%
- Lynis 9.23%

Αποτελέσματα

Με την χρήση του SecDep καταφέραμε να ασφαλίσουμε τους διακομιστές σε ικανοποιητικό βαθμό.

Αύξηση ασφάλειας

- Vuls 26.62%
  - Ευπάθειες δικτύου 14.57%
  - Φυσικές ευπάθειες 13.58%
- Lynis 9.23%
- Lunar 2.26%

Αποτελέσματα

Με την χρήση του SecDep καταφέραμε να ασφαλίσουμε τους διακομιστές σε ικανοποιητικό βαθμό.

Αύξηση ασφάλειας

- Vuls 26.62%
  - Ευπάθειες δικτύου 14.57%
  - Φυσικές ευπάθειες 13.58%
- Lynis 9.23%
- Lunar 2.26%

Προτάσεις βελτίωσης

1. Περαιτέρω σκλήρυνση του SSH
2. Επιπρόσθετοι περιορισμοί πυρήνα
3. Αυστηρότερες άδειες πρόσβασης σε αρχεία και φακέλους
4. Ρύθμιση ημερομηνίας λήξης λογαριασμών χρηστών
5. Ρύθμιση ελάχιστης και μέγιστης ηλικίας κωδικών πρόσβασης
6. Εγκατάσταση/ρύθμιση προγράμματος ελέγχου ακεραιότητας ευαίσθητων αρχείων
7. Εγκατάσταση προγράμματος σάρωσης κακόβουλου λογισμικού

Ευχαριστώ πολύ για τον χρόνο σας!

Ερωτήσεις;

konsthol@proton.me