Перелік посилань

1. Юдін О. К. Аналіз стеганографічних методів приховування інформаційних потоків у контейнери різних форматів / О. К. Юдін, Р. В. Зюбіна, О. В. Фролов // Радиоэлектроника и информатика. — Х. : НХНУРЕ, 2015. — № 3. — С. 24-31.

2. Steganography and Digital Watermarking: a global view [Електроний ресурс] - Режим доступу до ресурсу: http://lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti00/fortini/proiect.pdf.

3. LSB стеганография [Електроний ресурс]. - 2019. - Режим доступу до ресурсу: https://habr.eom/ru/post/112976

4. Рейда О.В. Аналіз та дослідження форматних стеганоалгоритмів на основі графічних контейнерів / Рейда О.В., Джулій В.М. // Тези доповідей Всеукраїнської науково-практичної конференції "Інтелектуальний потенціал – 2018". – 2018 – С. 86-90.

5. Cristi Cuturicu, JPEG - Алгоритм стиснення, Code Net [Електронний ресурс] / Формати файлів, - Режим доступу: http://www.codenet.ru/progr/forrnt/jpeg_00.php

Метод створення віртуальних полігонів на основі технологій хмарних обчислень системи управління базами даних

Джулій В.М., Лукін В.С., Чешун В.М.
Хмельницький національний університет

При виконанні дослідження було поставлено наступні задачі:

– дослідження і вибір існуючих систем, придатних для реалізації цілей і задач цієї роботи;

– проектування апаратно-програмного комплексу, включаючи дослідження і побудову всіх його підсистем;

– створення працюючого прототипу апаратно-програмного комплексу;

– визначення ефективності прототипу.

В рамках поставлених завдань розроблені наступні підсистеми апаратно-програмного комплексу та забезпечено їх взаємодію для виконання цілей цієї роботи:

– обчислювальна підсистема (система віртуалізації);

– мережева підсистема;

– система зберігання даних;

– система автоматизації надання послуг та забезпечення універсального доступу.

Для вирішення поставлених завдань розроблена архітектура інфраструктури віртуальних полігонів.

Робочі сервери віртуалізації [1,2] з встановленим гіпервізором є обчислювальним ядром інфраструктури, що забезпечує створення і управління роботою віртуальних машин, диспетчеризацію розподілу ресурсів між віртуальними машинами. Робочі сервери об'єднуються в ресурсний пул для забезпечення еластичності інфраструктури, можливості масштабувати інфраструктуру прозоро для користувачів. У ресурсному пулі виділяється керуючий master-сервер, за допомогою якого здійснюється централізоване адміністрування як всією обчислювальною системою, так і управління системою зберігання даних і мережевий підсистемою. Так само, master-сервер є центральним інтерфейсом управління всією системою за допомогою наданого їм API.

Обчислювальна підсистема забезпечує наступну функціональність: забезпечення продуктивності всіх компонентів віртуальних машин на рівні продуктивності пристроїв фізичних серверів;

– можливість створення готових шаблонів віртуальних машин з попередніми налаштованими пакетами програмного забезпечення;

– об'єднання фізичних серверів в ресурсні пули для динамічного розподілу віртуальних машин між фізичними серверами;

– можливість динамічної міграції віртуальних машин між серверами;

– підтримка режиму паравіртуалізації для найбільш ефективного використання обчислювальних та інших ресурсів операційними системами сімейства Linux.

Оскільки обчислювальна система є ядром всієї інфраструктури віртуальних полігонів, деякі вимоги до інших підсистем продиктовані функціональними можливостями обраного рішення віртуалізації.

Додавання нових серверів, а також штатне або аварійне вимкнення наявних серверів, відбувається прозоро для адміністратора системи і головне - для користувачів. Операція не вимагає переналаштовування системи і будь-яких додаткових дій з боку людини, не призводить до втрати інформації і збоїв в роботі інфраструктури. При цих діях користувач або взагалі не помічає змін, що відбулися, або перерви в роботі сервісів мінімальні.

Така можливість є суттєвою з точки зору хмарної моделі надання послуг, тому що забезпечує об'єднання ресурсів в ресурсні пули для динамічного перерозподілу потужностей між користувачами в умовах постійної зміни попиту на потужності, функції динамічної міграції віртуальних машин при проведенні технічного обслуговування окремих серверів, балансування навантаження між робочими серверами.

В архітектурі системи дана вимога виражається в необхідності використання зовнішнього сховища даних для зберігання файлів віртуальних машин, шаблонів віртуальних машин, віртуальних жорстких дисків користувачів. Гіпервізор повинен підтримувати роботу не тільки з локальною

системою зберігання даних робочого сервера, але і з зовнішніми системами зберігання даних.

Мережева підсистема забезпечує створення довільних топологій мережевої інфраструктури віртуальних машин, мережеву зв'язаність віртуальних машин як в межах внутрішніх віртуальних мереж між віртуальними машинами, так і відносно зовнішніх до системи мереж і пристроїв, нормальне функціонування віртуальних машин з точки зору мережевих протоколів.

Віртуальні машини, розгорнуті на різних фізичних серверах, мають можливість бути об'єднаними в єдиний віртуальний домен комутації на рівні L2. Для забезпечення вимоги до високої еластичності інфраструктури при реалізації мережевої підсистеми максимально використовуються програмні мережеві рішення – вбудовані можливості гіпервізора і стандартних мережевих засобів операційної системи Linux. З апаратних рішень використовується тільки фізичний комутатор рівня L2 для підключення серверів до локальної обчислювальної мережі.

Технічне управління і адміністрування системою в режимі нормальної експлуатації здійснюється з окремої програми з графічним інтерфейсом користувача, встановленої на керуючому сервері адміністратора системи. Адміністраторів системи може бути будь-яка кількість, так само можливо наділяти користувачів розширеними правами на управління частинами віртуальної інфраструктури. У цій програмі існує можливість створювати всі типові настройки, шаблони віртуальних машин, управляти життєвим циклом віртуальних машин, здійснювати адміністрування віртуальних машин, в тому числі в режимі консолі.

Конфігурація робочих серверів віртуалізації так само має здійснюватися підключенням до них безпосередньо по SSH через інтерфейс командного рядка (CLI). Звичайні користувачі отримують параметри доступу до віртуальних машин, а так доступ до консолі віртуальної машини через веб-сервер (портал) управління. Портал доступний як всередині локальної мережі організації, так і через мережу Інтернет.

Веб-сервер написаний на мові програмування Java і релизована на стандартній платформі, контйнері сервлетів, що підтримує функціонал віддалених процедур XML-RPC. Необхідний фунцонал веб-сервера забезпечується з допомогою APImaster-сервера.

Стосовно запропонованих рішень проведене дослідження підсистем інфраструктури віртуальних полігонів і їх взаємодії для того, щоб прийти до найбільш оптимальної схеми побудови всієї системи.

Проведені дослідження стали основою для створення віртуальних полігонів на основі технологій хмарних обчислень системи управління базами даних.

Перелік посилань
1. Michelle Bailey. The Economics of Virtualization: Moving Toward an Application- Based Cost Model. IDC.URL: http://www.vmware.com/files/pdf/Virtualization-
2. Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing. NIST Special Publication 800-145. URL: http://csrc.nist.gov/publications/nistpubs/800- 145/SP800-145.pdf

Метод захисту від загрозливих програм, заснований на реалізації контролю доступу до файлових об'єктів

Казіміров В.О., Мостовий С.В., Нагребецький О.В., Орленко В.С.
Хмельницький національний університет

Використання сучасних систем інформаційної безпеки вимагає, з одного боку, відстеження швидких змін в інформаційних технологіях та нових загроз, а з іншого - з урахуванням реальних характеристик апаратного та програмного забезпечення корпоративних мереж та систем. Процедура придбання пристроїв захисту інформації проста. Набагато складніше вирішити проблему - як захистити і які заходи безпеки застосовувати, мінімізуючи витрати. Впроваджуючи різні засоби захисту, необхідно визначити баланс між можливим збитком від несанкціонованого витоку інформації та обсягом інвестицій, які витрачаються на забезпечення безпеки інформаційних ресурсів. З метою підвищення ефективності захисту інформаційних ресурсів необхідно дослідити підходи до оцінки рівня їх захисту та систем захисту. Ця оцінка для кожного випадку індивідуальна і залежить від багатьох факторів (вартості інформації, статусу організації, важливості інформації, рівня технічного та програмного забезпечення тощо).

В роботі здійснено дослідження основних типів загрозливих програм, та запропоновано класифікацію шкідливого програмного забезпеченні (ШПЗ) за способом їх виконання. Враховуючи аналіз існуючої статистики зроблено висновок, що найбільш актуальними для захисту є виконувані двійкові і файли сценаріїв.

Можна виділити два найбільш поширених способи зараження: соціальна інженерія; технічні прийоми впровадження ШПЗ, що заражається без відома користувачf [1].

Ці види ШПЗ передбачають обов'язкове збереження файлу на вінчестері перед виконанням.

Тому можна зробити висновок що застосування розмежувальної політики доступу до виконуваних об'єктів, дозволяє мінімізувати загрози.

Проведено дослідження існуючих підходів до оцінки ефективності методів і засобів захисту від загрозливих програм, в результаті якого зроблені