



DOI: 10.31388/2220-8674-2023-2-42

УДК 004

А. В. Антоненко, к.т.н., доц.

ORCID: 0000-0001-9397-1209

О. О. Сорочинський

ORCID: 0009-0001-5894-1554

Державний університет телекомунікацій

e-mail: artem.v.antonenko@gmail.com, тел.: 063-263-33-03

МОДЕЛЮВАННЯ ПРИВАТНОГО МЕРЕЖЕВО-СЕРВЕРНОГО СЕРЕДОВИЩА З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ OPENNEBULA

Анотація. Використання приватних хмарних середовищ для побудови та керування мережево-серверною інфраструктурою привернуло значну увагу в останні роки. OpenNebula є платформою хмарних обчислень з відкритим вихідним кодом, яка здатна створювати віртуалізовані центри обробки даних та керувати ними. Це комплексне рішення для проектування та розгортання хмарних середовищ, шляхом автоматизації та управління віртуальними машинами, сховищами даних та мережевими ресурсами. OpenNebula має модульну архітектуру, що дозволяє користувачам налаштовувати та розширювати платформу відповідно до своїх конкретних потреб. Однією з ключових особливостей OpenNebula є підтримка декількох гіпервізорів, включаючи KVM, VMware та LXD, забезпечуючи управління віртуальними машинами на різних платформах віртуалізації з єдиного інтерфейсу. OpenNebula ставить основний акцент на простоту та зручність використання. Платформа має веб-інтерфейс, за допомогою якого легко керувати своєю хмарною інфраструктурою з будь-якого пристрою, що підключений до мережі Інтернет. Також платформа включає набір інструментів командного рядка (CLI), які дозволяють досвідченим користувачам автоматизувати платформу та керувати ресурсами програмно. Ще однією ключовою особливістю OpenNebula є її масштабованість. Платформа розроблена для підтримки широкого спектру сценаріїв розгортання, від невеликих приватних хмар до великомасштабних публічних хмар, що дозволяє легко та швидко масштабувати свою інфраструктуру в залежності від потреб, не вимагаючи значних змін у базовій архітектурі. OpenNebula має велику та активну спільноту користувачів та розробників, які вносять свій внесок у постійний розвиток та вдосконалення платформи. Програмне забезпечення випускається під ліцензією Apache, що робить його вільним та відкритим для використання, модифікації та



розповсюдження, без будь-яких ліцензійних платежів.

Ключові слова: OpenNebula, сховище, мережеві ресурси, масштабованість, приватні хмари, публічні хмари.

Постановка проблеми. У сучасному цифровому світі організації все більше покладаються на приватні мережі для зберігання та керування критично важливими даними та програмами. Приватне мережево-серверне середовище забезпечує покращену безпеку, контроль і масштабованість порівняно з загальнодоступними мережами, що робить його привабливим вибором для багатьох компаній. Однак проектування та моделювання такого середовища може бути складним, вимагаючи ретельного дослідження різних факторів, таких як архітектура, розподіл ресурсів, технологія віртуалізації та інструменти керування. [1]

Однією з популярних технологій для побудови та керування приватними мережево-серверними середовищами є OpenNebula. OpenNebula - це платформа для хмарних обчислень, яка вирішує завдання управління та направлення віртуалізованих ресурсів у центрах обробки даних та гібридних хмарних середовищах. Зокрема, це комплексне та гнучке рішення для розгортання, управління та масштабування віртуальних машин та контейнерів, на базі різних технологій віртуалізації. Пропонує широкий спектр функцій, включаючи керування віртуальними машинами, керування мережею та сховищами, керування користувачами та групами, а також моніторинг і звітування [2].

Однією з ключових проблем у розробці з використанням OpenNebula є вибір відповідної архітектури. Архітектура повинна бути ретельно спланована, щоб забезпечити ефективний розподіл ресурсів, високу доступність і масштабованість. У статті обговорюватимуться різні варіанти архітектури, такі як одновузлова, багатовузлова та гібридна архітектури, а також їхні переваги та недоліки. У статті також буде розглянуто фактори, які необхідно враховувати при виборі відповідної архітектури, наприклад, розмір організації, типи додатків і робочих навантажень, а також бажаний рівень продуктивності та доступності [3].

Іншою проблемою при розробці середовища є розподіл ресурсів процесора, пам'яті та зберігання даних, між віртуальними машинами. Ефективний розподіл ресурсів має вирішальне значення для забезпечення оптимальної продуктивності. У статті обговорюватимуться різні методи розподілу, такі як статичний, динамічний та гібридний розподіл, а також їхні переваги та недоліки. У статті також досліджуватимуться фактори, які необхідно враховувати під час визначення відповідної стратегії розподілу



ресурсів, такі як характеристики робочого навантаження, вимоги до продуктивності додатків і обмеження вартості.

Формулювання проблеми при проектуванні та моделюванні приватного середовища з використанням технології OpenNebula передбачає вирішення різних проблем, пов'язаних з архітектурою, розподілом ресурсів, технологією віртуалізації, управлінням, безпекою, масштабованістю, сумісністю та економічною ефективністю. Ретельно аналізуючи та вирішуючи ці завдання, організації можуть створити ефективне приватне мережево-серверне середовище, яке відповідає їхнім цілям продуктивності, безпеки та вартості. У наступних розділах статті детальніше буде розглянуто кожен з цих проблем, надаючи розуміння та рекомендації щодо проектування та моделювання такого середовища. [4]

Аналіз останніх досліджень. В останні роки було опубліковано значну кількість досліджень і літератури на тему моделювання та проектування приватних мережево-серверних середовищ за допомогою технології OpenNebula. У цьому розділі статті буде надано аналіз останніх джерел, у тому числі наукових робіт, статей і публікацій, щоб висвітлити поточний стан галузі та визначити ключові тенденції та висновки [1-11].

Однією помітною тенденцією в останній літературі є наголос на важливості безпеки при проектуванні та моделюванні приватних хмар. Зі зростанням поширення кіберзагроз і витоку даних організації надають пріоритет заходам безпеки для захисту своїх конфіденційних даних і програм. Автори рекомендують застосовувати найкращі методи безпеки, такі як регулярні аудити безпеки, керування виправленнями та сегментацію мережі, щоб мінімізувати ризик порушення безпеки.

Оскільки організації ростуть і їхні вимоги змінюються, таке середовище має бути масштабованим, щоб відповідати сучасним вимогам. Організаціям часто потрібно інтегрувати свою інформаційну інфраструктуру з іншими системами та технологіями, які забезпечують бездоганну взаємодію. Це включає підтримку кількох гіпервізорів, інтеграцію із зовнішніми системами зберігання та сумісність із різними мережевими конфігураціями.

Іншою ключовою тенденцією, виявленою в літературних джерелах, є необхідність комплексного управління та моніторингу приватної хмари, а також обговорюється важливість розгляду аспекту енергоефективності. Ефективне управління, моніторинг та оптимізації споживання енергії у своїй IT-інфраструктурі, є критично важливими для забезпечення продуктивності, доступності та надійності.

Загалом аналіз останніх джерел підкреслює важливість цілісного підходу до проектування та моделювання приватних мережевих серверних середовищ за допомогою технології OpenNebula. Це



включає в себе розгляд заходів безпеки для захисту від кіберзагроз, забезпечення масштабованості для адаптації до змінних вимог, досягнення сумісності з іншими системами та технологіями, оптимізацію витрат для узгодження з організаційними бюджетами, прийняття OpenNebula як гнучкого та масштабованого рішення, впровадження ефективних стратегій управління та моніторингу, і розгляд практики енергоефективності для екологічної стійкості. Включаючи ці фактори в процес проектування та моделювання, організації можуть створити надійне, безпечне, масштабоване та ефективне рішення, яке відповідає вимогам їх бізнесу та відповідає їх ІТ-цілям.

Формулювання мети статті. Мета дослідження - моделювання та проектування приватного мережево-серверного середовища з використанням технології OpenNebula.

Об'єкт дослідження - приватне мережево-серверне середовище, що складається з комп'ютерів, мережевих пристроїв та серверів, а також технології OpenNebula.

Предмет дослідження - процес моделювання та проектування приватного мережево-серверного середовища з використанням технології OpenNebula, включаючи в себе визначення вимог до системи, вибір необхідного обладнання та налаштування програмного забезпечення.

Основна частина. OpenNebula - це рішення для хмарних обчислень з відкритим вихідним кодом, яке повністю підтримує приватні, публічні та гібридні хмарні платформи. Технологія розроблена для легкої адаптації до будь-якої інфраструктури та легкого розширення новими компонентами. Результатом є модульна система, яка може реалізувати різноманітні хмарні архітектури та може взаємодіяти з кількома службами центру обробки даних. Внутрішніми компонентами OpenNebula є основний модуль, набір підключених драйверів та кілька інструментів. Віртуальні ресурси, такі як віртуальні машини, віртуальні мережі, віртуальні сховища та шаблони, управляються і контролюються основним модулем. Крім того, він обробляє запити від клієнтів і викликає відповідні драйвери для керування ресурсами, які потрібно використовувати. Драйвери - це адаптери, які взаємодіють з проміжним програмним забезпеченням. За допомогою низки інструментів та API, кінцеві користувачі можуть отримати доступ до ключових функціональних можливостей.

Основні складові OpenNebula:

- Керуючий вузол (frontend node) - центральний вузол, який відповідає за управління всіма іншими вузлами хмари. Він включає в себе веб-інтерфейс, API та базу даних.

- Вузли хмари (cloud nodes) - обчислювальні вузли, на яких



запускаються віртуальні машини. Вони можуть бути розташовані на різних фізичних серверах і мати різну конфігурацію обладнання.

- Хмарні образи (cloud images) - образи віртуальних машин, які можна використовувати для запуску нових віртуальних машин на вузлах хмари.

- Хмарні шаблони (cloud templates) - конфігурації для створення віртуальних машин, включаючи параметри вузлів, образи, мережі та інші параметри.

- Хмарні мережі (cloud networks) - віртуальні мережі, на яких працюють віртуальні машини.

Компонентами установки OpenNebula є:

OpenNebula Daemon (oned): OpenNebula Daemon є основною службою платформи. Він керує вузлами кластера, віртуальними мережами та сховищами, групами, користувачами та їхніми віртуальними машинами, а також надає API XML-RPC іншим службам і кінцевим користувачам.

База даних: OpenNebula зберігає стан хмари у вибраній базі даних SQL. Це ключовий компонент, який слід контролювати та налаштовувати для найкращої продуктивності, дотримуючись найкращих практик конкретного продукту бази даних.

Планувальник: планувальник OpenNebula відповідає за планування віртуальних машин, на доступних вузлах гіпервізора. Це спеціальний демон, встановлений разом із OpenNebula Daemon, його також можна розгорнути окремо на іншій машині.

Edge Cluster Provision: цей компонент створює повнофункціональні кластери OpenNebula у загальнодоступній хмарі. Модуль Provision інтегрує Edge Clusters у вашу хмару OpenNebula, використовуючи три основні технології: Terraform, Ansible і OpenNebula Services.

Моніторинг: підсистема моніторингу представлена спеціальним демоном, що працює як частина демона OpenNebula. Він збирає інформацію, що стосується хостів і віртуальних машин, основними показниками є продуктивність, статус віртуальної машини та споживання ресурсів.

OneFlow: OneFlow керує службами кількох віртуальних машин у цілому, визначаючи залежності та політики автоматичного масштабування для компонентів програми, взаємодіє з демоном OpenNebula для керування віртуальними машинами (запуск, зупинка), ним також можна керувати через графічний інтерфейс Sunstone або через CLI.

OneGate: сервер OneGate дозволяє забезпечити зв'язок між віртуальними машинами та вузлами OpenNebula. Завдяки OneGate

користувачі можуть легко взаємодіяти зі своїми віртуальними машинами ззовні хмари, що значно полегшує їх роботу з хмарними ресурсами.

OneGate/Proху: служба OneGate/Proху — це просте рішення TCP-проксі, яке можна використовувати для покращення безпеки кінцевої точки OneGate. Користувачі можуть увімкнути його на вузлах гіпервізора, тоді стане набагато простіше захищати трафік OneGate за допомогою рішення VPN [10].

OpenNebula є високомасштабованою архітектурною системою (Рис. 1). Інтерфейси працюють на основі REST API (наприклад, EC2-Query API), OpenNebula Cloud API (OCA) та власних API драйверів (Рис. 2). Також є підтримка підключення до AWS.

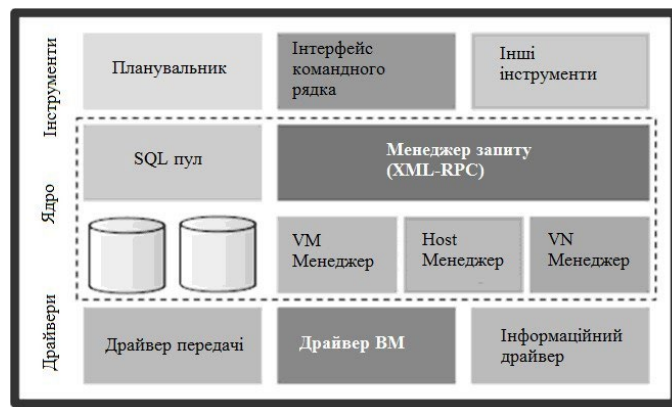


Рисунок 1. Внутрішня архітектура OpenNebula

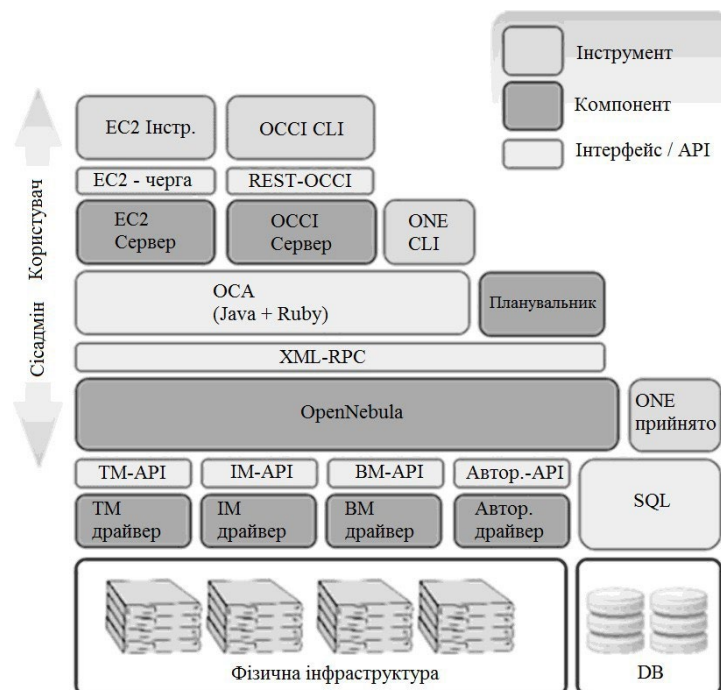


Рисунок 2. Інтерфейси



Рішення OpenNebula спеціально розроблене для адаптації до будь-якої інфраструктури і може бути легко розширене за допомогою інших компонентів. Результатом є модульна система, яка дозволяє створювати необмежену кількість хмарних архітектур. Крім того, вона може бути інтегрована з центрами обробки даних.

Хмарний інтерфейс потрібен нам для управління віртуальними машинами, мережами та зображеннями за допомогою REST API. Він обмежує потребу в додаткових знаннях про хмару для того, щоб кінцеві користувачі могли їх освоїти. OpenNebula реалізує два типи інтерфейсів:

EC2-запит API: OpenNebula реалізує функції, що надаються EC2 API від Amazon, які пов'язані з управлінням віртуальними машинами. Тому при доступі до хмари OpenNebula можна використовувати будь-який інструмент EC2-запитів [4].

OSSI-OGF: цей веб-сервіс дозволяє запускати віртуальні машини в OpenNebula та керувати ними, використовуючи останню версію проекту OSSI API.

Інтерфейс XML-RPC є основним інтерфейсом OpenNebula і надає всі функції для взаємодії з програмним рішенням OpenNebula. За допомогою інтерфейсу XML-RPC ви можете контролювати і керувати будь-якими ресурсами OpenNebula, включаючи віртуальні машини, мережі, образи, користувачів, хости і кластери. Інтерфейс XML-RPC рекомендується використовувати при розробці спеціальних бібліотек для хмарних додатків або коли потрібен низькорівневий інтерфейс до ядра OpenNebula.

OpenNebula Cloud API надають простий і зручний спосіб взаємодії з ядром OpenNebula. Ці API надають ту ж функціональність, що і XML RPC інтерфейси. API підтримують дві мови, Ruby та Java. Якщо ви розробляєте просунутий IaaS-інструмент і вам потрібен повний доступ до функціональності OpenNebula, найкраще використовувати інтерфейс OCA.

Внутрішні дані, стан OpenNebula та призначена інформація зберігається в постійній базі даних. Можуть використовуватися бази даних такі як MySQL або SQLite, що дозволяє легко взаємодіяти з будь-якими інструментами для роботи з базами даних.

Залежно від налаштування віртуальної мережі, віртуальна машина OpenNebula підключає свій мережевий інтерфейс (визначений в опції NIC) до фізичних пристроїв гіпервізора. Таким чином, віртуальна машина може отримати доступ як до публічних, так і до приватних мереж [3,11].

OpenNebula надає потужну та гнучку платформу, що дозволяє організаціям віртуалізувати свої обчислювальні ресурси, сховище даних та мережу для створення масштабованої та гнучкої



інфраструктури. Використовуючи функції та можливості OpenNebula, організації можуть створити середовище, яке відповідає їхнім конкретним вимогам, чи то для невеликих масштабів, чи для великих центрів обробки даних. Це дозволяє їм визначати детальний контроль доступу та політики безпеки для обмеження несанкціонованого використання, що гарантує, що лише авторизовані користувачі та процеси мають доступ до ваших ІТ-ресурсів та даних.

Інтеграція з інструментами та службами безпеки: OpenNebula підтримує взаємодію із зовнішніми інструментами та сервісами безпеки, такими як брандмауери, системи виявлення та запобігання вторгнень та антивірусне програмне забезпечення. Це дозволяє використовувати переваги цих інструментів і сервісів для посилення захисту інфраструктури вцілому [7].

Відповідність та сертифікація: OpenNebula може допомогти вам задовольнити вимоги безпеки та відповідності вашої організації або галузі, надаючи такі функції як: шифрування та безпечні комунікації. OpenNebula також сертифікована на відповідність стандартам безпеки, таким як ISO/IEC 27001:2013, що може допомогти вам продемонструвати безпеку та надійність вашої хмарної інфраструктури.

Безпечний зв'язок: OpenNebula підтримує безпечні протоколи зв'язку, такі як SSL/TLS, щоб гарантувати безпечну передачу даних між компонентами вашої віртуалізованої інфраструктури. Це допомагає запобігти підслуховуванню або фальсифікації даних під час передачі, що може становити значну загрозу безпеці.

Аварійне відновлення: OpenNebula надає функції для аварійного відновлення, такі як резервне копіювання та відновлення, реплікація та висока доступність. Ці функції можуть допомогти вам підтримувати безперервність бізнесу в разі інциденту з безпекою або збою системи, гарантуючи, що ваші дані та додатки будуть доступні та відновлені [2,11].

Сегментація віртуальної мережі: OpenNebula дозволяє створювати віртуальні мережі та сегменти мережі, ізольовані один від одного, що може допомогти запобігти латеральному переміщенню зловмисників у вашій віртуалізованій інфраструктурі. Це зменшує вплив інцидентів безпеки і допомагає стримувати потенційні порушення безпеки.

Безперервний моніторинг безпеки: OpenNebula підтримує безперервний моніторинг безпеки, який передбачає регулярне тестування та оцінку безпеки вашої віртуалізованої інфраструктури за допомогою автоматизованих інструментів і методів. Це може допомогти вам виявити та усунути вразливості та слабкі місця безпеки на випередження, перш ніж ними зможуть скористатися зловмисники.

В цілому, OpenNebula може надати широкий спектр функцій і



можливостей безпеки, які допоможуть вам побудувати безпечну і відмовостійку хмарну інфраструктуру. Однак важливо відзначити, що безпека - це безперервний процес, і що потрібно стежити за регулярними оновленнями для усунення ризиків і загроз безпеці у вашому хмарному середовищі.

Висновки. У цій статті ми дослідили моделювання та проектування приватного мережево-серверного середовища за допомогою технології OpenNebula. Ми обговорили архітектурні компоненти, міркування щодо конфігурації та найкращі методи створення надійного рішення. Підсумовуючи усе вище наведене, можна сказати, що OpenNebula пропонує організаціям потужну та гнучку платформу для віртуалізації їхніх обчислювальних ресурсів, сховищ та мереж. Ретельно враховуючи архітектурні компоненти, параметри конфігурації та найкращі практики, організації можуть створити приватне мережево-серверне середовище, яке адаптоване до їхніх вимог, забезпечуючи підвищене використання ресурсів, покращену масштабованість, підвищену безпеку та спрощену роботу. Завдяки належному плануванню, оптимізації ресурсів, заходам безпеки, регулярному моніторингу та технічному обслуговуванню, а також тестуванню, організації можуть використовувати OpenNebula для створення ефективного, безпечного та високодоступного приватного мережево-серверного середовища, що дозволить їм задовольняти свої обчислювальні потреби та досягнення своїх ІТ-цілей.

Список використаних джерел

1. OpenNebula Beginner's Guide. Giovanni Toraldo. Packt Publishing. 2012, P. 215–303.
2. Mastering OpenNebula 3. Andres Lucas Arrivillaga and Ruben S. Montero. Packt Publishing. 2013. P. 107–122.
3. OpenNebula 5.8: Cloud Computing. Omar A. Mendoza. Packt Publishing. 2019. P. 350–400.
4. Cloud Storage Security: A Practical Guide. Aaron Wheeler and Michael Winburn. Apress. 2016. P. 153–200.
5. Зайцев Є. О. Smart засоби визначення аварійних станів у розподільних електричних мережах міст. Таврійський науковий вісник. Серія: Технічні науки (5), 2022.
6. Цвик О. С. Аналіз і особливості програмного забезпечення для контролю трафіку. Вісник Хмельницького національного університету. Серія: Технічні науки (1), 2023.
7. Балвак А. А., Новіченко Є. О. Актуальні засади створення алгоритмів обробки інформації для логістичних центрів. Таврійський науковий вісник. Серія: Технічні науки (1), 2023.
8. Твердохліб А. О., Коротін Д. С. Ефективність функціонування



комп'ютерних систем при використанні технології блокчейн і баз даних. Таврійський науковий вісник. Серія: Технічні науки (6), 2022.

9. Cloud Computing with OpenNebula 3. Helion Ventures. Helion Ventures. 2012. P. 50–62.

10. Data Center Handbook. Hwaiyu Geng. Wiley. 2015. P. 704–768.

11. OpenNebula 3 Cloud Computing: Leverage the Power of Cloud Computing Using OpenNebula 3. Giovanni Toraldo. Packt Publishing, 2012.

Стаття надійшла до редакції 12.04.2023 р.

A. Antonenko, O. Sorochynskyi
State University of Telecommunications

MODELING OF A PRIVATE NETWORK-SERVER ENVIRONMENT USING OPENNEBULA TECHNOLOGY

Summary

The use of private cloud environments to build and manage network and server infrastructure has attracted considerable attention in recent years. OpenNebula is an open source cloud computing platform capable of creating and managing virtualized data centers. It is a comprehensive solution for designing and deploying cloud environments by automating and managing virtual machines, data storage and network resources. OpenNebula has a modular architecture that allows users to customize and extend the platform according to their specific needs. One of the key features of OpenNebula is its support for multiple hypervisors, including KVM, VMware and LXD, providing management of virtual machines on different virtualization platforms from a single interface. OpenNebula puts the main emphasis on simplicity and ease of use. The platform has a web interface that makes it easy to manage your cloud infrastructure from any device connected to the Internet. The platform also includes a set of command-line tools (CLI) that allow advanced users to automate the platform and manage resources programmatically. Another key feature of OpenNebula is its scalability. The platform is designed to support a wide range of deployment scenarios, from small private clouds to large-scale public clouds, allowing you to easily and quickly scale your infrastructure based on needs without requiring significant changes to the underlying architecture. OpenNebula has a large and active community of users and developers who contribute to the continuous development and improvement of the platform. The software is released under the Apache license, which makes it free and open to use, modify and distribute, without any license fees.

Key words: OpenNebula, storage, network resources, scalability, private clouds, public clouds.