ISSN 1998-7927(print) ISSN 2664-6498 (online)

DOI: https://doi.org/10.33216/1998-7927-2026-301-3-14-24

УДК 004.45: 004.38

АВТОМАТИЗАЦІЯ ПРОЦЕДУР КАСКАДНОГО КЕРУВАННЯ ЖИВЛЕННЯМ СЕРВЕРІВ VMWARE VSPHERE ЗАСОБАМИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

Могильний Г.А., Семенов М.А., Донченко В.Ю., Швець І.М., Донченко С.М.

AUTOMATING CASCADING POWER MANAGEMENT PROCEDURES FOR VMWARE VSPHERE SERVERS USING NETWORK INFRASTRUCTURE

Mohylnyi H.A., Semenov M.A., Donchenko V.U., Shvets I.M., Donchenko S.M.

У статті досліджено актуальну проблему забезпечення стійкості інформаційних систем в умовах енергетичного кризису. Обґрунтовано необхідність захисту віртуалізованих середовищ VMware vSphere, де раптові вимкнення живлення без попереднього керованого завершення роботи призводять до незворотних пошкоджень файлових систем віртуальних дисків, порушення цілісності баз даних та метаданих на рівні сховищ.

Аналіз існуючих рішень показав, що існуючі системи безперебійного живлення (ДБЖ) з мережевими картами керування (NMC) мають високу вартість та обмежену програмну гнучкість, що робить їх використання економічно неефективним для сегментів малих та середніх кластерів.

Метою роботи є розробка гнучкої автоматизованої системи каскадного керування живленням на базі доступної мережевої інфраструктури, зокрема роутерів MikroTik, та побутових зарядних станцій великої потужності. У межах дослідження проведено класифікацію віртуальних ресурсів та запропоновано розподілити усі ресурси на декілька рівнів обслуговування, наприклад: мінімальний (vCenter, сервери AD, Web-сервер), базовий (файлові сервери, RDP) та повний (VMware Horizon, UAG). Автори навели опис основних етапів створення дотичної системи: розподіл віртуального середовища, дослідження використання електричної потужності, налаштування віртуального середовища, а також розробка процедур (скриптів) для керування запуском/завершенням роботи віртуального середовища VMware vSphere.

На основі експериментальних даних запропоновано часові затримки для каскадного запуску та завершення роботи, що забезпечує коректну синхронізацію системних компонентів. Описано технічну реалізацію системи, яка включає налаштування BIOS серверів для автоматичного відновлення живлення та підтримки Wake-on-LAN. Запропоновано схему розподілу енергоспоживання через два блоки живлення, що дозволяє оптимізувати заряджання станцій без зупинки роботи серверів. Також розглянуто методи оптимізації середовища VMware Horizon через керування параметром ParentVMs для зменшення кількості активних службових віртуальних машин та особливості розробки процедур керування запуском/завершенням роботи на прикладі роутеру MikroTik

Практична значущість результатів, апробованих у лабораторії «Центр ІТ-рішень» ЛНУ імені Тараса Шевченка, полягає у створенні бюджетного та надійного інструменту захисту інфраструктури, що імітує функціонал корпоративних NMC-систем. Використання протоколу SSH із сертифікатами для автоматизації команд на хостах ESXi забезпечує високий рівень автономності та безпеки процесу керування без необхідності ручного втручання адміністратора.

***Ключові слова**: UPS, VMware by Broadcom, VMware vSphere, VMware Horizon, ESXi, SSH, віртуальні ресурси, роутер MikroTik.*

Вступ. Сучасний етап розвитку інформаційних технологій в Україні та світі характеризується критичною залежністю бізнес-процесів, освітніх платформ та державних сервісів від безперебійної роботи окремих

серверів та центрів обробки даних. Проте, у сучасних реаліях повномасштабної збройної агресії російської федерації проти України, питання забезпечення стабільного функціонування інформаційно-комунікаційних систем трансформувалося з суто технічної площини у фундаментальний аспект національної та кібернетичної стійкості. Цілеспрямований енергетичний терор, що супроводжується масованими ракетними та дроновими атаками на об'єкти критичної інфраструктури, створив безпрецедентні виклики для підтримки складних віртуалізованих середовищ, таких як VMware vSphere [1], які є основою для багатьох наукових, освітніх та державних сервісів. В умовах частих, непередбачуваних та екстрених відключень електроенергії традиційні методи керування електроживленням виявляються недостатніми.

Особлива небезпека полягає у специфіці архітектури платформи віртуалізації, де раптове зникнення живлення без попереднього «м'якого» завершення роботи неминуче призводить до критичних пошкоджень файлових систем віртуальних дисків, порушення цілісності баз даних та метаданих на рівні сховищ. Для навчальних лабораторій, де розгорнуто складні моделі, зберігаються данні студентів, викладачів та результати експериментів, такі інциденти означають не лише технічні помилки, а й безповоротну втрату напрацювань та дороговартісного обладнання, заміна якого в умовах війни є вкрай ускладненою через фінансові обмеження.

У цьому контексті автоматизація за допомогою спеціалізованих процедур керування живленням стає критичним запобіжником, що дозволяє реалізувати гнучкий алгоритм виходу системи з ладу з мінімальними втратами. Традиційні системи джерел безперебійного живлення (ДБЖ) [2, 3] мають обмеження у програмному забезпеченні, ресурсі акумуляторів, а також мають велику вартість. У ситуації, коли період відключення перевищує час автономності ДБЖ, постає критична потреба не просто у вимкненні обладнання, а у керованому завершенні роботи та поетапному старті, які гарантують цілісність даних.

Такий підхід до забезпечення життєздатності інформаційних систем безпосередньо впливає на стабільність цифрового простору України та є життєво необхідною адаптацією вітчизняної ІТ-галузі до умов постійного деструктивного зовнішнього впливу, що дозволяє надійно зберігати різноманітні данні та забезпечувати безперервність освітнього процесу навіть у найскладніші періоди енергетичного дефіциту.

Аналіз останніх досліджень і публікацій. Попередні дослідження авторів вже успішно вирішували завдання організації систем з віддаленим доступом до інформаційних ресурсів та навчальних комп'ютерних лабораторій [4], а також розгортання надійного корпоративного середовища [5]. Проте досвід експлуатації таких систем в умовах воєнного стану та енергетичного терору виявив нову критичну проблему – вразливість побудованої інфраструктури до раптових багаторазових знеструмлень, що вимагає переходу від класичних методів адміністрування до автоматизованого каскадного керування на рівні гіпервізорів.

Загалом, сучасні дослідження у сфері забезпечення безперервності функціонування інформаційних систем зосереджені на поєднанні технологій віртуалізації, енергетичної ефективності та відмовостійкості. Базові принципи управління обчислювальними ресурсами у середовищах VMware vSphere висвітлені у фундаментальних працях. Зокрема, у дослідженні A. Gulati та співавторів [6] описано механізми Distributed Resource Scheduler та Distributed Power Management, які дозволяють автоматично балансувати навантаження та оптимізувати енергоспоживання кластерів. Проблематика переведення серверів у режими зниженого енергоспоживання також досліджувалася C. Isci та ін. [7], де запропоновано підходи до динамічного керування станами живлення серверів.

Значна кількість робіт присвячена енергетично ефективному управлінню ресурсами дата-центрів. Зокрема, у дослідженнях Q. Zhang та A. Beloglazov [8, 9] розглядаються алгоритми оптимізації розміщення віртуальних машин, їх міграції та консолідації з метою зниження енергоспоживання. Однак такі підходи орієнтовані переважно на планову оптимізацію роботи систем у штатних умовах і не враховують сценаріїв аварійного вимкнення живлення та необхідності коректного завершення роботи віртуальних середовищ.

Окремий напрям досліджень пов'язаний із використанням програмно-визначених сховищ, таких як VMware vSAN [10], а також

інфраструктурі віртуальних робочих столів на базі VMware Horizon [11]. У роботі [12] запропоновано використання VMware vCenter в якості віртуального освітнього середовища, де здобувачі освіти мають можливість самостійно запускати та зупиняти окремі віртуальні машини. Однак, у такому випадку раптове відключення живлення може привести до повного пошкодження файлових систем віртуальних машин. Аналогічна ситуація складається у інформаційних систем на базі VMware vSphere з використанням VMware Horizon, у яких королювати кількість активних віртуальних ресурсів вкрай складно. У цих системах особливо критичним є забезпечення узгодженості даних, оскільки раптове відключення електроживлення без коректного завершення транзакцій може призвести до пошкодження файлових систем та втрати даних. Водночас існуючі рішення не забезпечують достатньої адаптивності до багаторазових циклів зникнення та відновлення електроживлення.

Важливу роль у забезпеченні відмовостійкості відіграють джерел безперебійного живлення (ДБЖ), які підтримують різні режими роботи: offline, line-interactive та online [2, 3]. У практичних реалізаціях для середовищ VMware використовуються Smart-UPS або Online-UPS із вбудованими мережевими платами управління (NMC), що підтримують протоколи моніторингу та взаємодії з інфраструктурою. Такі системи дозволяють ініціювати завершення роботи серверів через централізовані механізми, однак їх функціональність зазвичай обмежується подачею сигналу на вимкнення без урахування складних логічних залежностей між сервісами.

З іншого боку, автоматичне включення серверів після відновлення електроживлення реалізується через апаратні механізми (зокрема налаштування BIOS "Restore on AC Power Loss"), проте цей підхід є негнучким, оскільки не враховує стан мережі, готовність сервісів та необхідну послідовність запуску компонентів системи.

Стандартизаційні підходи, зокрема ISO/IEC 27001 [13] та IEEE 446 [14], визначають загальні вимоги до забезпечення безперервності бізнес-процесів та надійності енергоживлення, однак не регламентують конкретні механізми каскадного керування віртуалізованими середовищами.

У контексті мережевої автоматизації важливе значення мають можливості різноманітних роутерів. Поверхневий огляд та порівняння їх можливостей наведено у [15]. Однак особливо виділяються роутери з вбудованими операційними системами, зокрема MikroTik RouterOS [16], які підтримують інструменти моніторингу доступності вузлів (Netwatch) та виконання сценаріїв автоматичного реагування. Для віддаленого управління серверною інфраструктурою використовується протокол SSH [17], що забезпечує захищене виконання команд і сценаріїв адміністрування. Проте в існуючих дослідженнях такі інструменти розглядаються переважно як допоміжні засоби і не інтегруються у єдину систему автоматизованого керування електроживленням.

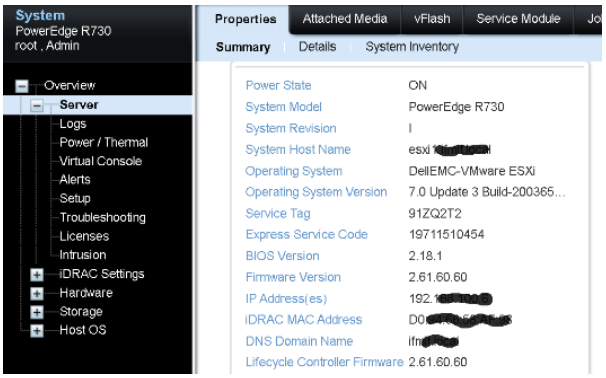
Таким чином, проведений аналіз показує, що існуючі наукові та практичні підходи охоплюють окремі аспекти проблеми: віртуалізацію ресурсів, енергетичну ефективність, використання ДБЖ та мережевих протоколів управління. Проте відсутні комплексні рішення, які б поєднували ці компоненти для реалізації поетапної (каскадної) черговості процесів вимкнення та запуску серверів у віртуалізованому середовищі без використання дорогих промислових ДБЖ. Це обумовлює актуальність розробки гнучких підходів до керування електроживленням із використанням засобів мережевої інфраструктури, що і визначає напрям даного дослідження.

Мета статті. На засадах комплексного аналізу розробити гнучку автоматизовану систему керування живленням серверів VMware vSphere з використанням мережевих роутерів.

Виклад основного матеріалу дослідження. Дослідження, налаштування та впровадження виконувались у лабораторії «Центр ІТ-рішень» (https://mitc.luguniv.edu.ua/) навчально-наукового інституту математики та інформаційних технологій (https://imit.luguniv.edu.ua/) ДЗ «Луганський національний університет імені Тараса Шевченка» (https://luguniv.edu.ua/).

До складу інформаційної системи входить декілька комп’ютерних класів, різноманітне мережеве обладнання та два сервери: сервер

DELL та сервер SUPERMICRO. Загальну характеристику серверів наведено на рисунку 1.



а

б

Рис. 1. Загальна характеристика серверів:
а – сервер DELL; б – сервер SUPERMICRO

До складу мережевої інфраструктури (рис.2), яка входить до предмету дослідження, належать: пороговий роутер MikroTik RB750Gr3 з RouterOS 6.49 [16] (рис.3), який під'єднаний до мережі Інтернет та двох окремих мереж: гостьової та основної, в кожній з яких є проміжні комутатори. Два сервери (DELL та SUPERMICRO) приєднані до обох мереж, та з'єднані між собою адаптерами (10 Гбіт) для швидкого трафіку vSAN та vMotion.

Таким чином, структура VMware vSphere (рис. 4) складається з одного датацентру, одного кластеру, до яких входять два хости, додатково працює vSAN [10] та VMware Horizon [11].

В цілому, у віртуальному середовищі працює (рис.5):

- vCenter з ОС Photon OS для керування процесами віртуалізації;
- два сервери (по одному на кожному хості) з ОС Windows Server 2016 з підтримкою служб MS AD та сервер політики мережі для інтеграції з клієнтами Radius, підтримка VPN-з'єднань;

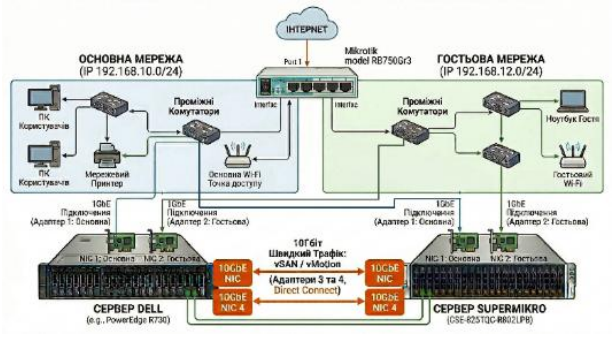


Рис. 2. Структура мережі

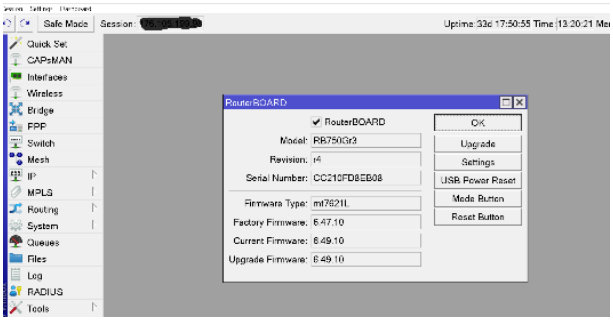


Рис. 3. Характеристика MikroTik

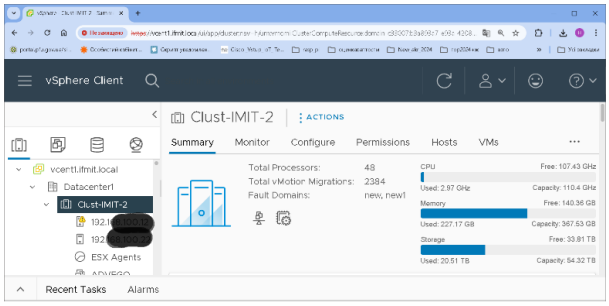


Рис. 4. Структура VMware

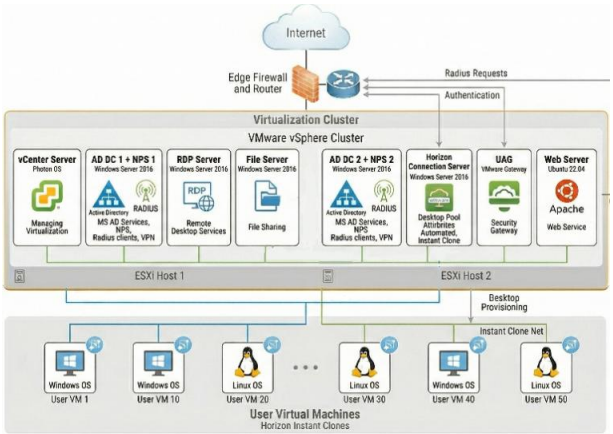


Рис. 5. Віртуальне середовище

- Web-сервер (Apache) з ОС Ubuntu 22.04;
- файловий сервер з ОС Windows Server 2016;
- сервер з ОС Windows Server 2016 з підтримкою служби віддалених робочих столів (RDP);
- сервер з ОС Windows Server 2016 та додатковим програмним забезпеченням VMware Horizon Connection Server;
- сервер з ОС Photon OS з програмним забезпеченням VMware Unified Access Gateway (UAG)
- інші віртуальні машини (ОЗУ 4-16 ГБ, віртуальні накоричувачі 48-128 ГБ) користувачів (в середньому від 10 до 50), створені на засадах використання VMware Horizon за допомогою Desktop Pool Attributes Automated, Instant Clone.

За таких умов назви віртуальних машин та їх загальна кількість, що одночасно працюють у віртуальному середовищі, невідомі та постійно змінюється залежно від кількості та потреб активних користувачів. Встановлено, що загальний час старту та синхронізації всього віртуального середовища на цьому апаратному забезпеченні становить 30-40 хвилин. За цей час, в умовах постійних перебоїв з електроживленням, напруга може зникати та з'являтися декілька разів. Крім того, складно спланувати частину (відсоток) використання ємності заряду ДБЖ та налаштувати час підтримки електроживлення.

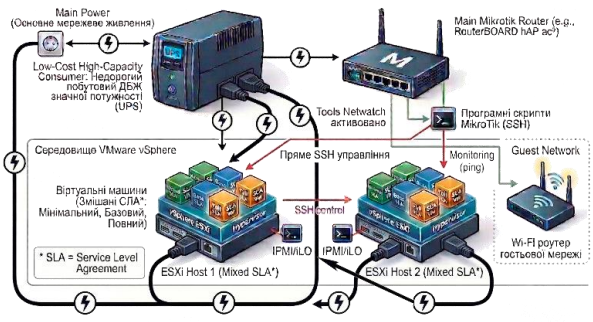


Рис. 6. Структура керування електроживленням

У результаті комплексного аналізу запропоновано створити автоматизовану систему керування електроживленням (рис. 6) шляхом використання мережевих роутерів, наприклад MikroTik з підтримкою Netwatch, та недорогих побутових приладів резервного живлення значної потужності, яка буде поетапно вмикати/вимикати віртуальні ресурси. Така система дозволить імітувати потужну UPS з підтримкою NMC, але буде значно дешевшою та володіти більш потужним програмним забезпеченням, яке дозволить створити кероване каскадне увімкненням/вимкненням серверів.

У процесі комплексного аналізу запропоновано, що основні етапи та завдання створення системи керування живленням можна звести до таких кроків:

1. Провести розподіл віртуального середовища на рівні обслуговування, наприклад, мінімальний, базовий та повний рівень.

2. Дослідити споживання електричної потужності, час її відновлення та періоди затримки між стартами компонентів віртуального середовища.

3. Налаштувати віртуальне середовище та окремі ресурси на зменшення кількості активних віртуальних машин та створити можливість керування хостами за допомогою протоколу SSH.

4. Розробити процедури (скрипти) для роутера (MikroTik), які дозволять керувати поетапним (каскадним) стартом та завершенням роботи активних віртуальних машин.

Розглянемо основні складові цих етапів.

У першу чергу потрібно виділити рівні обслуговування, складові підтримки працездатності інформаційної системи. В кожному окремому випадку, залежно від особливостей спрямованості інформаційної системи, можна виділити декілька груп сервісів. В інформаційній системі, що розглядається, було виділено три рівні:

- Мінімальний – сервер vCenter, сервери з підтримкою MS AD та Web-сервер.
- Базовий – охоплює мінімальний та додатково файловий сервер та сервер RDP.
- Повний – включає базовий та додатково сервер VMware Horizon Connection Server та сервер VMware Unified Access Gateway.

Таким чином, при старті (завантаженні), в першу чергу стартує vCenter, сервери з підтримкою Ms AD та Web-сервер, потім файловий сервер та сервер RDP, а на останньому етапі VMware Horizon Connection Server та VMware Unified Access Gateway.

При завершенні (у разі припинення електроживлення) робимо у зворотному порядку, але додаємо етап завершення всіх

активних віртуальних машин, які були завантажені користувачами за допомогою VMware Horizon.

Для впорядкування цього етапу було запропоновано переналаштувати автозавантаження віртуальних машин у середовищі vCenter (для об'єктів хост: меню: Configure -> Virtual Machines -> VM Startup/Shutdown->Edit) та залишити автозавантаження/завершення тільки машин, що входять до мінімального рівня обслуговування (рис. 7).

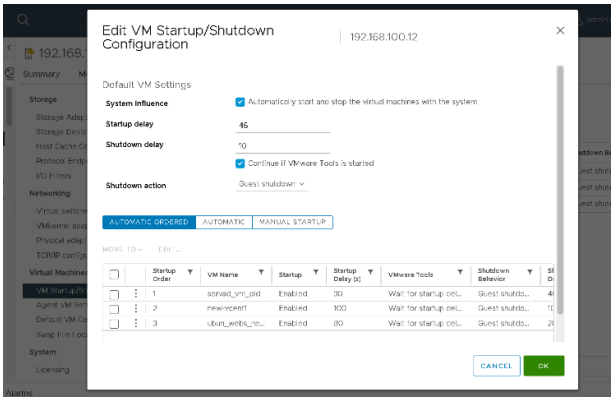


Рис. 7. Зміна налаштувань автозавантаження ВМ

Наступним кроком буде дослідження електричної потужності та певних часових затримок при старті/завершенні всіх серверів. Безумовно, цей аналіз необхідно виконувати з урахуванням особливостей певної ДБЖ та переліку інформаційних ресурсів та серверів. Для дослідження, було задіяно побутову зарядну станцію Bluetti потужністю 2000 W.

Експериментально встановлено певні особливості використання цієї зарядної станції. Потужність зарядки складає приблизно 500 W, але споживана потужність двох серверів становить 400-800 W залежно від навантаження. Таким чином, у випадку повного підключення серверів до цієї зарядної станції, ємність батареї не відновлюється та вона поступово розряджається. Вирішення цього питання було знайдено за рахунок того, що у кожному сервері по два блоки живлення. Один блок живлення кожного серверу було підключено до зарядної станції, а другий безпосередньо, напряму у розетку 220 V. За рахунок такого підключення споживана потужність на зарядній станції під час присутності електроживлення складає приблизно 270-400 W, а час повного відновлення – 4 години. У випадку відсутності електроживлення вся споживча потужність серверів йде через зарядну станцію, та період розрядки внутрішньої батареї складає 35 %/год. Ці характеристики дозволяють спланувати час підтримки роботи серверів у випадку відсутності електроживлення.

Для планування часових затримок поетапного (каскадного) старту/завершення роботи серверів необхідно провести експериментальний аналіз часу завантаження віртуальних машин для кожного рівня обслуговування. Безумовно, у кожній інформаційній системі цей час буде різнитися залежно від кількості рівнів обслуговування, особливостей серверів (хостів) та віртуальних машин. В інформаційній системі, яка досліджується, встановлено, що мінімальний рівень завантажується за 6-8 хвилин, базовий – 3-5 хвилин, а повний – 5 хвилин. Потім процес синхронізації всіх ресурсів протягом 5-10 хвилин.

При зворотному процесі – завершенні роботи встановлено, що віртуальні ресурси повного рівня обслуговування завершуються протягом 1 хвилини, базового рівня – 1,5-2 хвилин, а мінімального – 1,5 хвилини. Однак слід врахувати додаткові етапи завершення. Це завершення активних віртуальних машин, які завантажені у середовищі VMware Horizon Connection Server – приблизно 1,5-2 хвилини, та зупинка хостів ESXi – приблизно 4 хвилини.

Ці затримки слід враховувати при програмуванні завершення/старту віртуального середовища на роутері MikroTik (команда :delay XXs).

Наступним кроком рекомендується переглянути кількість віртуальних машин (за можливістю) зменшити період обслуговування, наприклад, певні сервіси перевести на обслуговування з 24/7 на 12/7.

В інформаційній системі, що досліджувалась, було прийнято рішення уповільнити роботу сервісів Desktop Pool Automated, Instant Clone у VMware Horizon. Встановлено, що VMware Horizon використовує службові віртуальні машини у спеціальних теках (папках з назвою ClonePrep….) середовища vCenter (рис. 8), які мають спеціальний атрибут та не можуть бути завершені автоматично. Для цього у консолі керування VMware Horizon було відключено параметр ParentVMs у меню Setting->Server->vCenter Servers (рис. 9). Відключення цього параметра призвело до вивантаження службових віртуальних машин, але уповільнило розгортання клонів машин для користувачів.

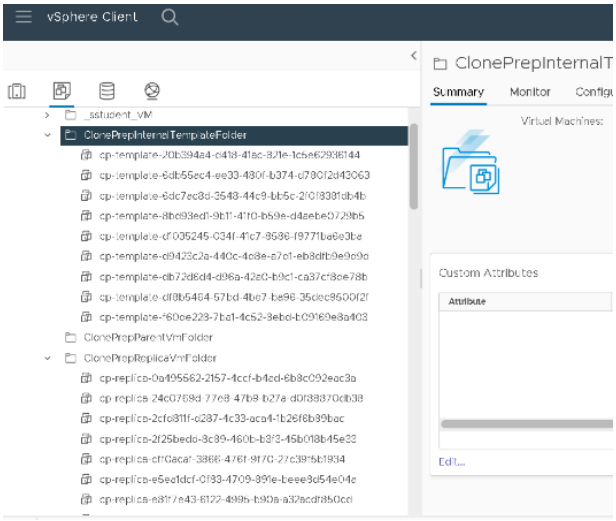


Рис. 8. Службові теки VMware Horizon у vCenter

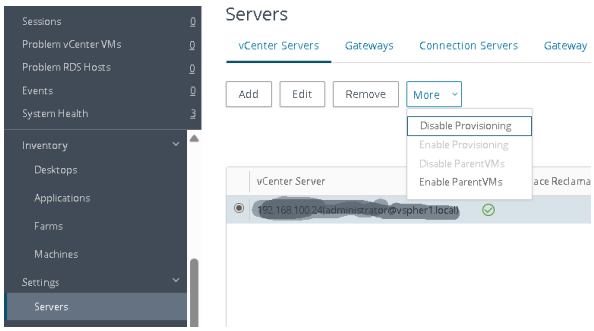


Рис. 9. Відключення параметра ParentVMs у VMware Horizon

Для автоматизації старту хостів ESXi та автоматичного відновлення живлення було проведено переналаштування BIOS. У BIOS було встановлено автоматичне відновлення живлення та підтримку пакетів WOL з метою подачі команди від роутера MikroTik. Слід відзначити, що у багатьох серверів, залежно від виробника та моделі сервера ці налаштування розташовані у різних меню BIOS.

Для створення умов керування хостами ESXi за допомогою MikroTik необхідно дозволити підтримку SSH. Існує декілька варіантів, але один зі шляхів – через консоль хоста в меню Troubleshoot Option->Enable SSH. На рис. 10 показано стан меню у випадку, коли SSH вже активовано.

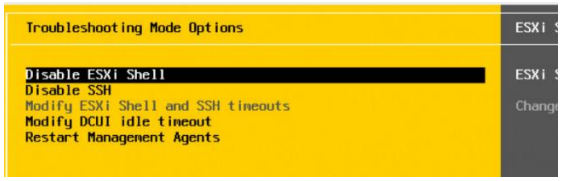


Рис. 10. Включення SSH на хосту ESX

Встановлено, що при віддаленому підключенні з роутера MikroTik з RouterOS 6.49 неможливо автоматично (у скрипті) підключитися до віддаленого хосту (ESXi) за допомогою пароля. Для автоматичного, програмованого підключення треба використовувати тільки сертифікати. Таким чином, потрібно додатково налаштувати службу SSH на кожному хосту у файлі /etc/ssh/sshd_config:

- дозволити підключатися користувачу root – параметр PermitRootLogin yes
- заборонити підключатися з використанням паролів – встановити параметр PasswordAuthentication no
- встановити відповідний сертифікат для користувача root на кожен хост ESXi у каталозі /etc/ssh/keys-root/ , де створити, або відредагувати файл authorized_keys, у якому кожен окремий рядок.

Слід відзначити, що сертифікати ESXi та MikroTik з ОС RouterOS 6.49 не сумісні між собою. ESXi використовує більш сучасні сертифікати типу OpenSSH (RFC 4716), а MikroTik з ОС RouterOS 6.49 – сертифікати RSA PEM. Одним зі шляхів вирішення цього питання є відключення (у файлі /etc/ssh/sshd_config) параметра FipsMode no. Однак це збільшує ризики безпеки. В цілому питання сумісності сертифікатів вирішено у RouterOS v7.12. Однак за певних обставин існує можливість згенерувати сумісний сертифікат і для RouterOS v6.49. У межах цієї статті розглянемо тільки основні етапи:

- Згенерувати сертифікат у будь-якій ОС.
- Встановити на MikroTik підтримку сучасних алгоритмів шифрування за допомогою команди у терміналі: /ip ssh set strong-crypto=yes host-key-size=2048 .
- Імпортувати сертифікати користувачу (admin) MikroTik, від імені якого будуть запускатися скрипти за допомогою команди: /user ssh-keys private import private-key-file=file public-key-file=file.pub .

Останнім кроком у створенні системи керування живленням є розробка процедур (скриптів) для роутера (MikroTik), які дозволять керувати поетапним (каскадним) запуском та завершенням активних віртуальних машин. У межах цієї статті розглянемо лише основні

складові цього процесу. Слід відзначити, що створення складних скриптів у MikroTik RouterOS v6.49 – це окреме завдання. Тому зупинимось лише на деяких особливостях цього процесу.

1. Для визначення подій увімкнення/вимкнення живлення достатньо скористатися утилітою Netwatch та налаштувати її на відстеження одного з пристроїв гостьової мережі (неважливий прилад), що не підтримується резервним живлення. Для цього скористаємося командою /tool netwatch add host=<IP_addr_guest_net> timeout=<sec> interval=<sec> , або меню tools->Netwatch. У результаті такого налаштування роутер буде визначати події включення живлення (скрипт Up) та зникнення живлення (скрипт Down).

2. Netwatch скрипти мають обмеження у розмірі та розглядаються як один рядок. Тому створюйте окремі скрипти (підскрипти) та обов'язково завершуйте команду символом «;» Для запуску скрипта (підскрипта) у фоновому режимі скористайтесь командою – :execute <name_script>;

3. При створенні додаткових скриптів (підскриптів) врахуйте певні привілеї (Policy) скриптів. Їх повинно бути чотири: read, reboot, write, test. Будь-які інші комбінації Policy недопустимі.

4. У скриптах, для підключення до хостів ESXi та виконання певної команди на хості використовуйте команду скрипта /system ssh-exec user=<user_ESXi> address=<IP_addr_ESXi> command="Command_ESX" ;

5. У скриптах для запуску ESXi (перший рівень обслуговування) скористайтесь командою /tool wol mac=<MAC_ADDR_ESXi> interface=<Name_interf_connect_ESXi>;

6. Скрипти не мають параметрів. Для передавання параметрів скористайтесь Address Lists. Таким чином, для передавання параметрів додайте інформацію у Address Lists з певним ім'ям, у скрипті зчитайте інформацію з Address Lists та за необхідністю видаляйте Address Lists. Наприклад, для роботи з Address Lists з ім'ям powerDOWN:

- отримання IP адреси /ip firewall address-list get [find list="powerDOWN"] address;
- знищення – /ip firewall address-list remove [find where list="powerDOWN"];
- додавання /ip firewall address-list add list="powerDOWN" address=127.0.0.1;

Існує ще велика кількість особливостей створення скриптів у MikroTik для автоматичного програмування процесів каскадного запуску/завершення роботи серверів ESXi, які будуть викладені у межах іншої статті.

Загалом було створено 6 скриптів для старту та 8 для завершення.

Висновки. У результаті проведеного дослідження вирішено актуальне науково-практичне завдання щодо забезпечення відмовостійкості та безперервності роботи віртуалізованих центрів обробки даних (на базі VMware vSphere) в умовах критичної енергетичної нестабільності. На основі комплексного аналізу недоліків традиційних промислових ДБЖ розроблено та впроваджено гнучку автоматизовану систему каскадного керування живленням серверів VMware vSphere, що базується на використанні існуючої мережевої інфраструктури та побутових зарядних станцій.

Впровадження цієї системи забезпечує високий рівень кібернетичної стійкості інформаційних систем в умовах нестабільного енергопостачання, мінімізуючи ризики пошкодження файлових систем віртуальних дисків та втрати критичних даних через раптові відключення. Запропонована методика логічного сегментування віртуального середовища на рівні обслуговування, наприклад — мінімальний, базовий та повний, що дозволило оптимізувати черговість запуску та зупинки сервісів з урахуванням їхньої логічної взаємозалежності.

На основі експериментальних даних визначено часові затримки для каскадного запуску та поетапного завершення роботи, що гарантує синхронізацію всіх компонентів інформаційної системи. Технічна реалізація системи за допомогою роутерів MikroTik, протоколу SSH із сертифікатами та службою Netwatch дозволила автоматизувати процеси керування без потреби у дороговартісних промислових ДБЖ з картаою мережевого керування (NMC). Вагомим результатом роботи є розробка та впровадження етапів створення автоматизованого каскадного керування електроживленням віртуалізованих середовищ, що інтегрує алгоритми пріоритезації ресурсів та спеціальні сценарії завершення й відновлення роботи системних сервісів на базі мережевої інфраструктури – програмованих роутерів MikroTik та побутових систем електроживлення. Це дозволяє імітувати функціонал складних корпоративних систем

моніторингу за допомогою програмно-визначених сценаріїв, забезпечуючи гнучкість налаштувань під потреби малих та середніх кластерів.

Практична значущість дослідження полягає у створенні бюджетного та надійного інструменту захисту інфраструктури, який успішно апробовано в лабораторії «Центр ІТ-рішень» ЛНУ імені Тараса Шевченка. Отримані результати дозволяють підтримувати безперервність освітнього процесу та наукових експериментів навіть у періоди тривалих енергетичних дефіцитів, спричинених зовнішніми деструктивними впливами.

Подальші дослідження у цьому напрямі можуть бути спрямовані на розширення можливостей системи моніторингу електроживлення, впровадження більш гнучких інтелектуальних алгоритмів спрямованих на прогнозування тривалості підтримка роботи серверів від батареї ДБЖ та інтеграцію гібридних хмарних рішень у загальний алгоритм каскадного керування.

Література

1. VMware vSphere 7.0 [Електронний ресурс] URL: https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/7-0.html (дата звернення: 08.01.2026).
2. Системи UPS пояснення: типи, особливості та переваги [Електронний ресурс] URL: https://www.wthdne.com/uk/blog/ups-systems-explained-types-features-and-benefits (дата звернення: 08.04.2026).
3. Типи системи безперебійного живлення [Електронний ресурс] URL: https://www.svcpower.com/uk/types-of-uninterruptible-power-system.html (дата звернення: 08.04.2026).
4. Могильний Г., Семенов М., Кірєєв І. Впровадження системи віддаленого доступу до інформаційних ресурсів комп'ютерних лабораторій. *Вісник Східноукраїнського національного університету імені Володимира Даля.* 2022. № 2 (272). С. 7–14. URL: https://doi.org/10.33216/1998-7927-2022-272-2-7-14 .
5. Могильний Г., Донченко В., Донченко С. Огляд та аналіз інструментів створення корпоративного середовища. *Інформаційні технології та суспільство*. 2024. № 4 (15). С. 99–107. URL: https://doi.org/10.32689/maup.it.2024.4.16.
6. VMware distributed resource management: Design, implementation, and lessons learned. VMware / A. Gulati et al. *Technical Journal.* 2012. Vol. 1, No. 1. P. 45–64. URL: https://www.waldspurger.org/carl/papers/drs-vmtj-mar12.pdf. (дата звернення: 08.01.2026).
7. Agile, efficient virtualization power management with low-latency server power states. / C. Isci et al. *ACM SIGARCH Computer Architecture News.* 2013. Vol. 41, no. 3. P. 96–107. URL: https://doi.org/10.1145/2485922.2485931 .
8. Beloglazov A., Buyya R. Energy efficient resource management in virtualized cloud data centers. *IEEE Transactions on Cloud Computing.* 2013. Vol. 1, No. 1. P. 14–28. URL: https://doi.org/10.1109/CCGRID.2010.46 .
9. Zhang Q., Cheng L., Boutaba R. Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications. 2010. Vol. 1, No. 1. P. 7–18. URL: https://doi.org/10.1007/s13174-010-0007-6 .
10. VMware vSAN 7.0 [Електронний ресурс] URL: https://techdocs.broadcom.com/us/en/vmware-cis/vsan/vsan/7-0.html (дата звернення: 08.04.2026).
11. Horizon Overview and Deployment Planning [Електронний ресурс] URL: https://docs.omnissa.com/bundle/HorizonOverviewDeployment/page/HorizonOverviewandDeploymentPlanning.html (дата звернення: 08.01.2026).
12. Могильний Г., Переяславська С., Донченко В., Швець І., Донченко С., Самотіс С. Створення віртуального навчального середовища на засадах VMware Vcenter. *Вісник Східноукраїнського національного університету імені Володимира Даля.* 2026. № 1(299). С. 5–15. URL: https://doi.org/10.33216/1998-7927-2026-299-1-5-15 .
13. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva : ISO, 2022. 26 p.
14. IEEE 446-1995. IEEE Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications (IEEE Orange Book). New York : IEEE, 1996. 320 p.
15. Могильний Г. Аналіз програмно-апаратних засобів створення системи з віддаленим доступом до навчальних комп'ютерних лабораторій закладів середньої освіти. *Вісник Східноукраїнського національного університету імені Володимира Даля.* 2023. № 1(277). С. 5–19. URL: https://doi.org/10.33216/1998-7927-2019-256-8-5-19.
16. RouterOS Documentation [Електронний ресурс] URL: https://help.mikrotik.com/docs/spaces/ROS/pages/328059/RouterOS (дата звернення: 08.01.2026).
17. Using ESXi Shell in vSphere [Електронний ресурс] URL: https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0/vsphere-security-8-0/securing-esxi-hosts/using-esxi-shell-in-vsphere.html (дата звернення: 08.01.2026).

R e f e r e n c e s

1. VMware vSphere 7.0 [Elektronnyi resurs] URL: https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/7-0.html (accessed: 08.01.2026).
2. Systemy UPS poiasnennia: typy, osoblyvosti ta perevahy [Elektronnyi resurs] URL: https://www.wthdne.com/uk/blog/ups-systems-explained-types-features-and-benefits (accessed: 08.04.2026).
3. Typy systemy bezperebiinoho zhyvlennia [Elektronnyi resurs] URL: https://www.svcpower.com/uk/types-of-uninterruptible-power-system.html (accessed: 08.04.2026).
4. Mohylnyi H., Semenov M., Kirieiev I. Vprovadzhennia systemy viddalenoho dostupu do informatsiinykh resursiv kompiuternykh laboratorii. Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia. 2022. № 2 (272). S. 7–14. URL: https://doi.org/10.33216/1998-7927-2022-272-2-7-14 .
5. Mohylnyi H., Donchenko V., Donchenko S. Ohliad ta analiz instrumentiv stvorennia korporatyvnoho seredovyshcha. Informatsiini tekhnolohii ta suspilstvo. 2024. № 4 (15). S. 99–107. URL: https://doi.org/10.32689/maup.it.2024.4.16.
6. VMware distributed resource management: Design, implementation, and lessons learned. VMware / A. Gulati et al. Technical Journal. 2012. Vol. 1, No. 1. P. 45–64. URL: https://www.waldspurger.org/carl/papers/drs-vmtj-mar12.pdf (accessed: 08.01.2026).
7. Agile, efficient virtualization power management with low-latency server power states. / C. Isci et al. ACM SIGARCH Computer Architecture News. 2013. Vol. 41, no. 3. P. 96–107. URL: https://doi.org/10.1145/2485922.2485931 .
8. Beloglazov A., Buyya R. Energy efficient resource management in virtualized cloud data centers. IEEE Transactions on Cloud Computing. 2013. Vol. 1, No. 1. P. 14–28. URL: https://doi.org/10.1109/CCGRID.2010.46 .
9. Zhang Q., Cheng L., Boutaba R. Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications. 2010. Vol. 1, No. 1. P. 7–18. URL: https://doi.org/10.1007/s13174-010-0007-6 .
10. VMware vSAN 7.0 [Elektronnyi resurs] URL: https://techdocs.broadcom.com/us/en/vmware-cis/vsan/vsan/7-0.html (accessed: 08.04.2026).
11. Horizon Overview and Deployment Planning [Elektronnyi resurs] URL: https://docs.omnissa.com/bundle/HorizonOverviewDeployment/page/HorizonOverviewandDeploymentPlanning.html (accessed: 08.01.2026).
12. Mohylnyi H., Pereiaslavska S., Donchenko V., Shvets I., Donchenko S., Samotis S. Stvorennia virtualnoho navchalnoho seredovyshcha na zasadakh VMware Vcenter. Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia. 2026. № 1(299). S. 5–15. URL: https://doi.org/10.33216/1998-7927-2026-299-1-5-15 .
13. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva : ISO, 2022. 26 p.
14. IEEE 446-1995. IEEE Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications (IEEE Orange Book). New York : IEEE, 1996. 320 p.
15. Mohylnyi H. Analiz prohramno-aparatnykh zasobiv stvorennia systemy z viddalenym dostupom do navchalnykh kompiuternykh laboratorii zakladiv serednoi osvity. Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia. 2023. № 1(277). S. 5–19. URL: https://doi.org/10.33216/1998-7927-2019-256-8-5-19 .
16. RouterOS Documentation [Elektronnyi resurs] URL: https://help.mikrotik.com/docs/spaces/ROS/pages/328059/RouterOS (accessed:: 08.01.2026).
17. Using ESXi Shell in vSphere [Elektronnyi resurs] URL: https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0/vsphere-security-8-0/securing-esxi-hosts/using-esxi-shell-in-vsphere.html (accessed: 08.01.2026).

Mohylnyi H.A., Semenov M.A., Donchenko V.U., Shvets I. M., Donchenko S.M Automating cascading power management procedures for VMware vSphere servers using network infrastructure

The article investigates the current problem of ensuring the stability of information systems in the conditions of an energy crisis. The need to protect VMware vSphere virtualized environments is substantiated, where sudden power outages without prior controlled shutdown lead to irreversible damage to virtual disk file systems, violation of database integrity and metadata at the storage level.

Analysis of existing solutions has shown that industrial uninterruptible power supply systems (UPS) with network management cards (NMC) have a high cost and limited software flexibility, which makes their use economically inefficient for small and medium-sized cluster segments.

The aim of the work is to develop a flexible automated cascade power management system based on available network infrastructure, in particular MikroTik routers, and high-power household charging stations. Within the framework of the study, a classification of virtual resources was carried out and it was proposed to distribute all resources into several service levels, for example: minimal (vCenter, AD servers, Web server), basic (file servers, RDP) and full (VMware Horizon, UAG). The authors described the main stages of creating

the relevant system: distribution of the virtual environment, study of electrical power consumption, configuration of the virtual environment, as well as development of procedures (scripts) for controlling the start/shutdown of the VMware vSphere virtual environment. Based on experimental data, time delays for cascading start and shutdown are proposed, which ensures correct synchronization of system components. The technical implementation of the system is described, which includes setting the server BIOS for automatic power recovery and supporting Wake-on-LAN. A scheme for distributing power consumption through two power supplies is proposed, which allows optimizing charging of stations without stopping the servers. Also considered are methods for optimizing the VMware Horizon environment through the ParentVMs parameter control to reduce the number of active service virtual machines and the features of developing start/stop control procedures using the example of a MikroTik router.

The practical significance of the results tested in the laboratory "IT Solutions Center" of Taras Shevchenko National University of Lviv is the creation of a budget and reliable infrastructure protection tool that simulates the functionality of corporate NMC systems. The use of the SSH protocol with certificates for command automation on ESXi hosts provides a high level of autonomy and security of the management process without the need for manual administrator intervention.

***Key words**: UPS, VMware by Broadcom, VMware vSphere, VMware Horizon, ESXi, SSH, virtual resources, MikroTik router.*

Могильний Геннадій Анатолійович – к. т. н., доцент, директор Навчально-наукового інституту математики та інформаційних технологій Луганського національного університету імені Тараса Шевченка,
ORCID: 0000-0001-5317-2795
g.mogilniy@gmail.com
Семенов Микола Анатолійович – к.п.н., доцент кафедри інформаційних технологій та систем Навчально-наукового інституту математики та інформаційних технологій Луганського національного університету імені Тараса Шевченка,
ORCID: 0000-0003-4989-8109
nasemenov@gmail.com
Донченко Володимир Юрійович – старший викладач кафедри інформаційних технологій та систем Навчально-наукового інституту математики та інформаційних технологій Луганського національного університету імені Тараса Шевченка,
ORCID: 0000-0003-0359-3051
ifmit.s.2014@gmail.com
Швець Ірина Михайлівна – асистент кафедри математики та інформатики Навчально-наукового інституту математики та інформаційних технологій Луганського національного університету імені Тараса Шевченка,
ORCID: 0009-0000-2767-8821
irinachipenkooo@gmail.com
Донченко Світлана Миколаївна – асистент кафедри інформаційних технологій та систем Навчально-наукового інституту математики та інформаційних технологій Луганського національного університету імені Тараса Шевченка,
ORCID: 0000-0002-2374-2109
donchenko.lana77@gmail.com

Дата першого надходження статті 13.02.2026.
Дата прийняття статті до друку після рецензування 25.03.2026.
Дата публікації 11.05.2026.