

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ЦЕНТРАЛІЗОВАНОГО СХОВИЩА КОНФІГУРАЦІЙ ДЛЯ БЕЗПЕЧНОГО КЕРУВАННЯ ІНФРАСТРУКТУРОЮ ХМАРНИХ СЕРВІСІВ

Є. В. Марценюк

Національний університет “Львівська політехніка”,
кафедра захисту інформації

E-mail: yevhenii.v.martseniuk@lpnu.ua

© Марценюк Є. В., 2025

У сучасних умовах широкого впровадження хмарних технологій, таких як AWS, GCP та Azure, організації стикаються з викликами централізованого управління хмарними ресурсами, які передбачають забезпечення стандартів безпеки, моніторинг метрик сервісів, оптимізацію витрат і управління конфігураціями. Основна проблема полягає у відмінностях архітектури сервісів різних хмарних провайдерів, що ускладнює інтеграцію та стандартизацію процесів в мультихмарних середовищах.

Ця стаття присвячена аналізу проблематики централізованого управління конфігураціями за допомогою бази даних управління конфігураціями (CMDB) як єдиного джерела правди. Досліджено методи організації та управління CMDB у публічних хмарних середовищах із акцентом на управління доступом, організаційними структурами, підписками та інвентаризацією хмарних ресурсів. Особливу увагу приділено розробленню рекомендацій для оптимізації процесів управління з метою підвищення загальної ефективності та безпеки.

Практична частина дослідження представлена інтеграцією системи Cherwell як CMDB із автоматизованим збором даних через Prisma API. Ця інтеграція дає змогу автоматизувати інвентаризацію ресурсів, зменшити ризик людських помилок, підвищити точність даних та забезпечити відповідність стандартам безпеки. Крім того, завдяки централізації даних та їх аналізу у Power BI дослідження продемонструвало ефективність підходу в контексті мультихмарного середовища.

Проведено детальний аналіз проблематики управління хмарними конфігураціями, особливостей сервісів основних хмарних провайдерів та їх інтеграції в єдину інформаційну модель. Основний акцент зроблено на розробленні рекомендацій щодо побудови ефективної системи управління конфігураціями, яка враховує мультихмарність, вимоги безпеки та специфіку операційних процесів. Практичний аспект дослідження ґрунтується на інтеграції системи Cherwell як CMDB із використанням Prisma API для автоматизації збору даних у мультихмарному середовищі. Інтеграція продемонструвала значні переваги, зокрема підвищення точності даних, зменшення ручної роботи, підвищення безпеки інформації та оптимізацію управлінських процесів.

Ключові слова: публічні хмарні середовища, управління конфігураціями, автоматизація, інтеграція.

Вступ

База даних управління конфігураціями, або CMDB, є важливим елементом сучасних систем управління IT-послугами. Вона забезпечує централізоване зберігання даних про IT-активи, їх конфігурації та взаємозв'язки. У хмарній інфраструктурі, де ресурси є динамічними та розподіленими, ефективне управління CMDB стає критично важливим для досягнення стабільності операцій, підтримання відповідності стандартам та забезпечення безпеки даних.

Метою цього дослідження є розроблення та вдосконалення підходів до управління конфігураціями у публічних хмарних середовищах. Для цього проведено аналіз сучасних методів, вивчено наявні інструменти та розроблено рекомендації щодо централізованого управління ресурсами за допомогою CMDB. Увага приділяється дослідженню інтеграційних можливостей CMDB для відображення змін у хмарній інфраструктурі, автоматизації обліку ресурсів та аналізу їх ефективності.

Дослідження також охоплює управління доступом і ресурсами, особливості організаційних структур, автоматизацію збору даних за допомогою Prisma API та інтеграцію з інструментами моніторингу та безпеки, такими як Splunk, Tenable і Power BI. Ці аспекти дають змогу створити єдине джерело правди для управління IT-інфраструктурою.

Практична частина дослідження зосереджена на інтеграції Cherwell із Prisma API для автоматизованого збору даних у мультихмарних середовищах. Цей підхід дає змогу мінімізувати ризики людських помилок, підвищити точність даних і сприяти дотриманню стандартів безпеки.

Ця стаття надає рекомендації та практичні рішення для організацій, які прагнуть забезпечити ефективність, безпеку та прозорість у своїй хмарній інфраструктурі, використовуючи CMDB як центральний інструмент управління.

Основні функції CMDB полягають у такому:

- **збереження детальної інформації:** підтримка комплексних даних про кожен елемент конфігурації (CI), включаючи його атрибути, стан і взаємозв'язки з іншими CI;
- **відстеження змін:** фіксація та управління змінами у конфігураціях для забезпечення контрольованого розвитку IT-інфраструктури;
- **сприяння аналізу впливу:** надання інформації про те, як зміни одного CI можуть вплинути на інші, що допомагає в аналізі впливу та прийнятті рішень;
- **підтримка управління IT-послугами:** покращення практик управління IT-послугами шляхом надання точної та актуальної інформації про IT-середовище.

Ці функції CMDB забезпечують ефективне управління IT-інфраструктурою, особливо в умовах складності та динаміки публічних хмарних середовищ.

Огляд літературних джерел

Наукові дослідження вказують, що основні функції CMDB полягають у збереженні детальної інформації про елементи конфігурації (CI), відстеженні змін, аналізі впливу змін і підтримці практик управління IT-послугами. Наприклад автори [1] підкреслюють, що інтеграція CMDB із сучасними хмарними платформами значно спрощує управління складними робочими навантаженнями. Автори [2] досліджують, як правильно спроектовані моделі даних CMDB можуть зменшити складність управління IT-інфраструктурою, водночас забезпечуючи її функціональність. У [3] акцентується увага на важливості оцінки та вдосконалення існуючих CMDB для покращення операційної ефективності.

У публічних хмарних середовищах CMDB відіграє ключову роль завдяки динамічному та масштабованому характеру хмарних ресурсів, які постійно змінюються залежно від потреб організацій. Наприклад, у публікації [4] акцентують увагу на важливості впровадження найкращих практик під час розгортання CMDB для ефективного управління великими середовищами. Автори наголошують, що правильна структура CMDB дає змогу забезпечити інтеграцію різнорідних джерел

даних, таких як сервіси різних хмарних провайдерів або ресурси, що розташовані в різних географічних регіонах. Це своєю чергою створює цілісне уявлення про інфраструктуру організації, що полегшує управління та забезпечує прозорість процесів.

Автор у праці [5] пропонує інноваційний підхід до забезпечення доступності ресурсів за допомогою реєр-to-реєр архітектури. Це рішення дає змогу швидко реагувати на запити користувачів навіть у разі тимчасової недоступності деяких ресурсів хмари. Такий підхід значно підвищує надійність хмарної інфраструктури та покращує функціонування CMDB, особливо в умовах мультихмарних або розподілених середовищ.

Крім того, роль CMDB у хмарній інфраструктурі охоплює автоматизацію процесів управління ресурсами. Як зазначають автори [1], інтеграція CMDB із автоматизованими системами управління дає змогу суттєво скоротити ручну роботу, мінімізувати людський фактор і забезпечити точність даних. Автоматизація також сприяє більш швидкому реагуванню на зміни в конфігураціях та забезпечує відповідність нормативним вимогам.

Постановка задачі

У процесі побудови та експлуатації хмарної інфраструктури організації стикаються з численними викликами, пов'язаними із забезпеченням прозорості, керованості та відповідності вимогам безпеки. Зокрема, в умовах мультихмарних середовищ виникає потреба в уніфікованому підході до управління конфігураціями, відстеження змін і реагування на інциденти, що потребує наявності ефективної системи обліку та контролю ресурсів.

Традиційні методи управління часто не забезпечують достатнього рівня автоматизації, інтеграції та масштабованості, що призводить до фрагментації даних, зниження точності конфігураційної інформації та підвищення операційних ризиків. У цьому контексті виникає необхідність формалізації процесів управління конфігураціями через впровадження централізованої CMDB-системи, здатної взаємодіяти з хмарними платформами та системами моніторингу в режимі реального часу.

З огляду на це актуальним є дослідження підходів до побудови автоматизованої архітектури управління конфігураціями, що забезпечує цілісність даних, відповідність політикам безпеки та ефективність у мультихмарному середовищі. Визначимо основні вимоги, обмеження та цілі, що лягли в основу формулювання задачі дослідження.

Виклики в управлінні CMDB у хмарних середовищах

Управління CMDB у публічних хмарних середовищах стикається з низкою викликів, зумовлених складністю та динамічністю таких систем. Однією з ключових проблем є різноманітність хмарних сервісів і їх конфігурацій. Автори [2] зазначають, що через велику кількість постачальників послуг, які використовують власні стандарти та архітектури, підтримка комплексної бази даних управління конфігураціями стає надзвичайно складною. Це створює бар'єри для інтеграції даних і ускладнює створення цілісної моделі інфраструктури.

Проблеми видимості ресурсів і їх взаємозв'язків особливо загострюються в мультихмарних середовищах, де організаціям доводиться працювати з декількома провайдерами одночасно. Як зазначають автори [6], інтеграція високодоступних баз даних у віртуалізовані хмарні платформи є важливим кроком для забезпечення надійності системи. Однак це потребує значних технічних зусиль та ретельного планування, щоб уникнути проблем із продуктивністю або несумісністю між різними платформами.

Автори [1] також підкреслюють необхідність автоматизації процесів для підтримання точності та актуальності даних у CMDB. Постійні зміни в хмарних ресурсах та швидкий темп їх оновлення ускладнюють ручне управління базою даних. Автоматизація не лише спрощує ці процеси, а й дає змогу інтегрувати CMDB із іншими інструментами ІТ-управління, знижуючи ризики втрати даних або порушення нормативних вимог.

Ще одним викликом є забезпечення безпеки даних у хмарних середовищах. Зростаючі вимоги до відповідності нормативам вимагають від CMDB не лише забезпечення точності конфігурацій, а й захисту інформації від потенційних загроз. Це потребує застосування сучасних засобів моніторингу та аналізу, які мають бути інтегровані безпосередньо в інфраструктуру CMDB.

Доступ як елемент конфігурації в CMDB

У публічних хмарних середовищах доступ до ресурсів є не лише операційним завданням, а й важливим конфігураційним елементом, який має бути врахований у цілісній системі управління конфігураціями (CMDB). Оскільки конфігурації доступу прямо впливають на безпеку та цілісність хмарної інфраструктури, інтеграція даних про доступ у CMDB є критично важливою для забезпечення комплексного підходу до кібербезпеки.

Ідентифікація доступу через IAM: Системи управління ідентифікацією та доступом (IAM) є ключовим джерелом інформації про політики доступу, призначення ролей користувачам і рівні дозволів. Інтеграція цих даних у базу даних управління конфігураціями (CMDB) у вигляді конфігураційних елементів (CI) дає змогу досягти значно більшої прозорості в управлінні доступом у хмарній інфраструктурі [7].

Зокрема, така інтеграція дає змогу фіксувати всі зміни в політиках доступу, забезпечуючи повну історичну простежуваність. Завдяки цьому можна вчасно виявляти потенційні конфлікти або помилки у налаштуваннях дозволів, які можуть виникати внаслідок неправильного призначення ролей чи порушення внутрішніх політик. Крім того, відображення IAM-даних у CMDB дає змогу проводити постійну перевірку відповідності принципу найменших привілеїв, що є базовою вимогою інформаційної безпеки. Отже, CMDB є не лише як репозиторій конфігураційної інформації, а і як контрольна точка для валідації та посилення політик доступу.

Ролі та атрибути доступу як конфігураційні параметри. Управління доступом у хмарних середовищах на основі ролей (RBAC) і атрибутів (ABAC) доцільно реалізовувати через включення відповідних параметрів до конфігураційної моделі в межах CMDB. Це дає змогу формалізувати зв'язки між користувачами, ролями та ресурсами, створюючи логічне відображення структури доступу в організації. Зокрема, включення ролей до CMDB дає змогу точно визначати, які користувачі мають доступ до яких ресурсів, у якому обсязі та з якими обмеженнями [8].

Крім того, застосування атрибутивної моделі дає змогу створювати умовні політики безпеки, що враховують контекст доступу, зокрема географічне розташування користувача, час доби або тип пристрою. Такі політики можуть адаптуватися в реальному часі, змінюючи правила доступу відповідно до динаміки середовища. Інтеграція цих механізмів у CMDB створює цілісну систему контролю доступу, яка є масштабованою, керованою та узгодженою з вимогами інформаційної безпеки.

Цілісність даних доступу. Забезпечення цілісності та актуальності даних про доступ у CMDB є критично важливим для підтримання ефективної системи контролю в хмарній інфраструктурі. Інформація про доступ має постійно синхронізуватися з фактичним станом прав і ролей у системах, які забезпечують автентифікацію та авторизацію. Для цього доцільно застосовувати автоматизовані механізми збору даних із таких джерел, як хмарні платформи (наприклад, AWS IAM, Azure Active Directory, Google Cloud IAM) та сторонні системи керування доступом, зокрема Okta, CyberArk.

Автоматизація дає змогу уникнути затримок у відображенні змін політик доступу, що знижує ймовірність виникнення розривів у системі безпеки. Крім того, своєчасне оновлення допомагає оперативно виявляти порушення чи відхилення від затверджених політик ще на ранніх етапах. У такий спосіб CMDB стає не лише інформаційною платформою, а й інструментом забезпечення безперервного контролю й відповідності вимогам безпеки.

Роль доступів в цілісній картині кібербезпеки. У хмарній інфраструктурі конфігурації доступу відіграють ключову роль у забезпеченні цілісної системи кібербезпеки. Вони визначають, хто і на яких умовах може взаємодіяти з ресурсами, впливаючи безпосередньо як на технічний захист,

так і на відповідність нормативним вимогам. Якщо організація не інтегрує управління доступом до єдиної конфігураційної бази знань, зокрема до CMDB, це може призвести до серйозних наслідків. Серед них - виникнення “сліпих зон”, коли певні дозволи або політики доступу залишаються непоміченими чи неузгодженими між різними хмарними провайдерами. Така фрагментація підвищує ризик порушення політик безпеки та невиконання вимог регуляторів [9].

Однак реалізація повноцінної інтеграції доступу в CMDB супроводжується низкою викликів. Одним із них є складність масштабування: великі організації працюють з тисячами користувачів, ролей і дозволів, що потребує обробки значних обсягів конфігураційних даних. Без належної автоматизації це створює надмірне навантаження на процеси підтримки CMDB в актуальному стані. Ще одним суттєвим аспектом є необхідність автоматичного оновлення - без регулярної синхронізації з ІАМ-системами конфігурації швидко втрачають актуальність, що знижує ефективність контролю доступу. Окрему проблему становить контекстуальність даних: права доступу часто залежать від умов використання, таких як місце, час, пристрій або рівень ризику. Це ускладнює їх стандартизоване подання в межах єдиної моделі даних CMDB.

Отже, включення інформації про доступ у CMDB є необхідним кроком для побудови послідовної та керованої системи кібербезпеки в хмарному середовищі. Проте ця інтеграція потребує продуманої архітектури, автоматизованих процесів і врахування контексту доступу як змінної частини конфігурації.

Огляд пропозицій CMDB на ринку хмарних рішень

Конфігураційна база даних управління (CMDB) є ключовим компонентом для організацій, що використовують хмарні платформи. Вона дає змогу централізовано зберігати дані про ресурси, їх конфігурації та взаємозв'язки, забезпечуючи прозорість управління інфраструктурою. AWS, Azure і GCP пропонують унікальні можливості для інтеграції з CMDB, автоматизації обліку ресурсів та їх подальшого управління, проте кожна платформа має свої особливості, які впливають на процеси організації.

Особливості обліку ресурсів на AWS

Amazon Web Services (AWS) надає інструменти для обліку та управління ресурсами, які характеризуються високим рівнем автоматизації та інтеграції з іншими сервісами екосистеми AWS. Одним із ключових рішень є AWS Config, який забезпечує створення повного інвентаря хмарних ресурсів, їх змін та відповідності організаційним політикам безпеки. Завдяки цьому сервісу організації можуть отримувати повну картину стану ресурсів і контролювати їх відповідність згідно з нормативними стандартами. Ще одним важливим інструментом є AWS Systems Manager, який спрощує централізоване управління конфігураціями. Завдяки цьому сервісу дані про ресурси можуть бути легко інтегровані з CMDB для забезпечення точності й актуальності інформації. Переваги AWS - глибока інтеграція всередині екосистеми, що дає змогу автоматизувати більшість процесів обліку та управління ресурсами [10]. Крім того, API AWS пропонують потужні можливості для інтеграції із зовнішніми системами CMDB, що розширює функціональність і спрощує роботу з конфігураціями. Однак важливим обмеженням є орієнтація на власну екосистему, що може створювати труднощі для організацій, які використовують мультихмарні середовища, де потрібна гнучка інтеграція з іншими платформами [11].

Особливості обліку ресурсів на Azure

Платформа Microsoft Azure забезпечує централізоване управління ресурсами через такі інструменти, як Azure Resource Manager (ARM). ARM дає змогу використовувати шаблони для опису інфраструктури та інтеграції з CMDB, що спрощує впровадження стандартів у процеси управління конфігураціями. Для моніторингу стану ресурсів і забезпечення відповідності організаційним стандартам Azure пропонує Azure Monitor та Azure Policy. Ці сервіси допомагають виявляти та

виправляти порушення конфігурацій, гарантуючи, що всі ресурси відповідають встановленим політикам. Основною перевагою Azure є тісна інтеграція з іншими корпоративними рішеннями Microsoft, такими як Active Directory. Це забезпечує безшовну роботу організацій, які використовують гібридні середовища, поєднуючи хмарні та локальні ресурси. Однак, порівняно з AWS та GCP, Azure має менш розвинені можливості для мультихмарного управління, що може обмежувати його використання в більш складних інфраструктурах [12].

Особливості обліку ресурсів на GCP

Google Cloud Platform (GCP) вирізняється своїм акцентом на аналітику та інструменти для детального моніторингу ресурсів. Основним інструментом є Google Cloud Asset Inventory, який дає змогу вести повний інвентар ресурсів із можливістю інтеграції з CMDB. Цей сервіс забезпечує точне відображення конфігурацій, змін і залежностей між ресурсами. Для більш глибокого аналізу та моніторингу GCP пропонує Google Cloud Operations Suite (раніше відомий як Stackdriver), який надає інструменти для моніторингу продуктивності, аналізу логів та діагностики проблем. Перевагами GCP є його орієнтація на аналітику, що дозволяє ефективно прогнозувати використання ресурсів і виявляти потенційні проблеми. Крім того, GCP активно підтримує мультихмарні середовища через сервіси, такі як Anthos, які забезпечують уніфіковане управління ресурсами в різних хмарах. Однак інтеграція інструментів GCP з традиційними CMDB-системами може бути складною через відмінності у підходах до моделювання даних і конфігурацій [13].

Порівняння CMDB рішень від постачальників хмарних послуг

Грунтуючись на цьому, можна зробити загальні висновки.

AWS, Azure та GCP мають унікальні особливості в управлінні ресурсами, які підходять для різних сценаріїв використання. AWS надає потужні інструменти для інтеграції з CMDB, але обмежує гнучкість у мультихмарних середовищах [14]. Azure ідеально підходить для організацій із гібридною інфраструктурою, завдяки інтеграції з іншими корпоративними рішеннями Microsoft. GCP виділяється аналітичними можливостями та підтримкою мультихмарності, але може потребувати додаткових зусиль для інтеграції з традиційними CMDB-системами (табл. 1). Вибір платформи залежить від конкретних потреб організації, її інфраструктури та стратегічних цілей.

Таблиця 1

Порівняння підходів інтеграції з CMDB

Хмарна платформа	Інструменти для обліку ресурсів	Інтеграція з CMDB	Особливості
AWS	AWS Config, Systems Manager	Потужні API	Глибока інтеграція в екосистему AWS
Azure	ARM, Azure Monitor, Azure Policy	Інтеграція через Active Directory	Зручність для гібридних середовищ
GCP	Cloud Asset Inventory, Operations Suite	Підтримка мультихмарності	Орієнтація на аналітику

Що пропонує ринок для вирішення задачі інтеграції CMDB та обліку ресурсів?

Сучасний ринок пропонує низку інструментів, які спрощують інтеграцію CMDB із хмарними платформами та автоматизують облік і управління ресурсами. Ці рішення забезпечують не лише збереження даних про конфігурації, а й автоматичний збір, моніторинг і аналіз інформації з хмарних середовищ, таких як AWS, Azure, та GCP. Нижче наведено ключові платформи, які пропонують комплексний підхід до цієї задачі [15].

ServiceNow ITOM є одним із провідних рішень для управління CMDB у хмарних середовищах. Воно забезпечує глибоку інтеграцію з основними хмарними платформами, такими як AWS, Azure, та GCP, через API. Це дає змогу автоматично збирати дані про ресурси, відстежувати їх зміни та зберігати інформацію у CMDB. Окрім цього, ServiceNow ITOM пропонує аналітичні інструменти для оцінки впливу змін на інфраструктуру, що дозволяє організаціям швидше реагувати на динамічні зміни у хмарних середовищах.

Cherwell ITSM також є популярним вибором для управління CMDB. Завдяки інтеграції з Prisma API цей інструмент забезпечує автоматизований збір даних про хмарні ресурси та їхню актуалізацію. Cherwell характеризується гнучкістю в конфігурації моделей даних, що робить його зручним для організацій із нестандартними або складними інфраструктурами. Додатковою перевагою є можливість налаштування робочих процесів для автоматизації рутинних завдань.

HashiCorp Terraform пропонує унікальний підхід до управління конфігураціями завдяки своїй орієнтації на принцип Infrastructure as Code (IaC). Це дає змогу синхронізувати конфігурації з CMDB та забезпечує автоматизоване управління змінами у хмарній інфраструктурі. Terraform також характеризується мультихмарною підтримкою, що робить його ідеальним для організацій із різноманітними хмарними середовищами.

BMC Helix Discovery спеціалізується на автоматичному виявленні хмарних ресурсів і їхньої інтеграції з CMDB. Інструмент дає змогу швидко ідентифікувати нові активи та зберігати їх у централізованій базі даних. Підтримка мультихмарності забезпечує BMC Helix Discovery гнучкість у роботі з різними платформами, дозволяючи організаціям отримувати єдине уявлення про всі свої ресурси.

CloudHealth by VMware спрямований на облік ресурсів, управління витратами та інтеграцію цих даних із CMDB. Інструмент дає змогу організаціям оптимізувати свої витрати, аналізуючи використання ресурсів, а також забезпечує автоматизацію збору даних для збереження актуальності інформації.

Рішення для інтеграції CMDB із хмарними платформами, такими як ServiceNow ITOM, Cherwell ITSM, HashiCorp Terraform, BMC Helix Discovery, і CloudHealth by VMware, відіграють ключову роль у сучасному управлінні хмарною інфраструктурою. Кожне з цих рішень пропонує унікальні підходи до інтеграції, автоматизації та управління конфігураціями, що дає змогу організаціям обирати інструмент відповідно до своїх потреб.

ServiceNow ITOM є потужним рішенням, яке забезпечує глибоку інтеграцію з основними хмарними платформами (AWS, Azure, GCP) та пропонує аналітичні можливості для управління змінами. Однак його підтримка мультихмарних середовищ залишається на середньому рівні, що може обмежувати його ефективність у складних інфраструктурах.

Cherwell ITSM вирізняється своєю гнучкістю та здатністю інтегруватися з великою кількістю API. Інструмент забезпечує зручне налаштування моделей даних і автоматизацію робочих процесів, що робить його ідеальним для організацій із складними та мультихмарними середовищами. Cherwell також інтегрує сервісний підхід у систему, що забезпечує не лише облік ресурсів, а й управління сервісами, змінами та інцидентами.

HashiCorp Terraform орієнтований на підхід Infrastructure as Code (IaC), що робить його ідеальним для автоматизації конфігурацій у мультихмарних середовищах. Однак його функціонал більше сфокусований на технічних аспектах управління ресурсами, а не на сервісному управлінні.

BMC Helix Discovery пропонує ефективний інструмент для автоматичного виявлення активів у хмарних середовищах та їх інтеграції з CMDB. Завдяки підтримці мультихмарності та швидкому виявленню нових ресурсів це рішення забезпечує ефективний облік, хоча його функціонал обмежений аналітичними та сервісними можливостями.

CloudHealth by VMware фокусується на управлінні витратами та оптимізації використання ресурсів, забезпечуючи інтеграцію даних із CMDB. Однак його можливості з управління конфігураціями менш розвинені порівняно з іншими інструментами.

Ключові аспекти вибору системи

1. Для організацій, які потребують глибокої інтеграції з хмарними платформами та аналітичними інструментами, ServiceNow ITOM буде ефективним рішенням.
2. Якщо потрібна гнучкість, автоматизація та інтеграція з великою кількістю сервісів, Cherwell ITSM є найкращим вибором.
3. HashiCorp Terraform буде оптимальним для організацій, що впроваджують IaC і працюють у мультихмарних середовищах.
4. BMC Helix Discovery підходить для швидкого виявлення ресурсів та інтеграції з CMDB у мультихмарних середовищах.
5. CloudHealth by VMware буде корисним компаніям, які фокусуються на оптимізації витрат і моніторингу ресурсів.

Таблиця 2

Порівняння основних рішень для інтеграції з CMDB

Рішення	Основні можливості	Особливості	Підтримка мультихмарності
ServiceNow ITOM	Автоматичний збір даних через API, аналітика змін	Глибока інтеграція з AWS, Azure, GCP	Середня
Cherwell ITSM	Автоматичний збір даних через API, інтеграція з великою кількістю API, аналітика змін, налаштування моделей даних, інтегрований сервісний підхід	Зручність конфігурації, автоматизація робочих процесів, гнучкість у налаштуванні	Висока
HashiCorp Terraform	Управління конфігураціями через IaC, синхронізація з CMDB	Орієнтація на мультихмарність, автоматизація змін	Висока
BMC Helix Discovery	Автоматичне виявлення ресурсів, інтеграція з CMDB	Швидке виявлення нових активів, підтримка мультихмарності	Висока
CloudHealth by VMware	Облік ресурсів, управління витратами, інтеграція з CMDB	Оптимізація витрат, аналіз використання ресурсів	Середня

Кожна система пропонує унікальний набір функцій, орієнтованих на різні аспекти інтеграції та управління CMDB. Вибір найкращого рішення залежить від конкретних потреб організації, таких як масштаб інфраструктури, вимоги до автоматизації, підтримка мультихмарності та пріоритетність сервісних або аналітичних функцій. Загалом Cherwell ITSM пропонує найбільш збалансований підхід, поєднуючи гнучкість, зручність конфігурації та потужну інтеграцію, що робить його лідером серед представлених рішень [16].

Серед поданих рішень Cherwell ITSM вирізняється своєю універсальністю та гнучкістю, що робить його оптимальним вибором для організацій, які прагнуть ефективно інтегрувати CMDB з хмарними платформами. Cherwell забезпечує автоматичний збір даних через API, пропонує інтеграцію з великою кількістю сервісів та API, а також дає змогу легко налаштовувати моделі даних під специфічні потреби організації. Крім того, інтегрований сервісний підхід робить Cherwell зручним для автоматизації складних робочих процесів, що забезпечує високу ефективність у мультихмарних середовищах.

На відміну від інших рішень (табл. 2.), таких як ServiceNow ITOM чи CloudHealth by VMware, Cherwell ITSM пропонує більшу гнучкість у налаштуванні та підтримує високий рівень мультихмарності. Порівняно з HashiCorp Terraform, яке орієнтоване на Infrastructure as Code, Cherwell забезпечує ширший функціонал для управління як ресурсами, так і сервісами, включаючи інтеграцію змін та інцидентів. Це робить Cherwell ITSM не лише універсальним інструментом, а й стратегічним рішенням для організацій, які прагнуть отримати максимальну вигоду від своєї CMDB [17].

Організаційні структури та управління підписками: роль CMDB у забезпеченні ефективності

Ефективне управління ресурсами в публічних хмарних середовищах потребує чітко визначеної організаційної структури та стратегії управління підписками. CMDB, як централізоване сховище інформації про конфігурації, відіграє ключову роль у забезпеченні прозорості, узгодженості та оптимізації цих процесів. У цьому розділі розглянемо, як організаційні структури та управління підписками інтегруються з CMDB для досягнення вищої ефективності управління хмарними ресурсами.

Організаційні структури

Великі організації, що використовують хмарні платформи, часто стикаються з необхідністю управління великою кількістю облікових записів (тенантів), які розподіляються між різними проєктами, відділами чи середовищами, такими як розробка, тестування та продакшн. Тенант у цьому контексті визначається як логічно ізольована одиниця, що надається користувачам або групам користувачів у межах спільної хмарної платформи чи сервісу. В основі концепції тенанта лежить забезпечення ізоляції даних, конфігурацій, користувачів і ресурсів одного клієнта від інших, що використовують ту саму хмарну платформу [18].

Ізоляція, яку забезпечують тенанти, дає змогу організаціям створювати сегментовані середовища для різних бізнес-потреб, наприклад, тестування нових функцій без ризику впливу на продуктивні системи. Це також сприяє дотриманню політик безпеки та спрощує управління ресурсами в масштабних інфраструктурах.

Використання CMDB для управління тенантами

Конфігураційна база даних управління (CMDB) може бути ключовим інструментом для інтеграції й управління тенантами. У CMDB кожен тенант можна відобразити як конфігураційний елемент (Configuration Item, CI), що дає змогу ефективно структурувати дані про всі облікові записи організації. Це створює основу для впровадження структурованого підходу до управління обліковими записами через такі ключові механізми:

- **сегментація облікових записів:** CMDB дає змогу організувати облікові записи за логічними групами відповідно до організаційної структури, проєктів або середовищ. Така сегментація полегшує управління доступом, ресурсами й витратами, дозволяючи надавати точні дані про використання ресурсів у кожній групі;
- **централізоване управління:** інтеграція тенантів у CMDB дає змогу впроваджувати уніфіковані політики безпеки та відповідності для всіх облікових записів. Наприклад, автоматизація моніторингу дозволяє постійно перевіряти відповідність конфігурацій кожного тенанта встановленим стандартам і політикам [19].

Тегування та категоризація як інструменти організації ресурсів

Окрім управління обліковими записами, CMDB підтримує функції **тегування** та **категоризації**, які є потужними інструментами для організації й аналізу хмарних ресурсів.

- **Тегування** дає змогу додавати метадані до ресурсів, наприклад, визначати їх власника, проєкт, середовище чи інші атрибути. Це спрощує процеси пошуку та групування ресурсів, а також полегшує аналіз їх використання. Наприклад, тег “Розробка” допомагає відстежувати витрати на певному етапі проєкту.
- **Категоризація** дає змогу логічно групувати ресурси за типом програми, середовищем або іншими атрибутами. Це створює структуроване уявлення про ресурси, що значно спрощує звітність, управління витратами та моніторинг продуктивності.

Інтеграція тенантів у CMDB, доповнена функціями тегування та категоризації, дає змогу створити єдину систему управління, яка відповідає сучасним вимогам до масштабованості та безпеки

хмарної інфраструктури. Такий підхід є особливо важливим для великих організацій, які працюють у мультихмарних середовищах, де важливо не лише контролювати ресурси, а й забезпечувати їхнє відповідне використання з точки зору витрат, продуктивності й відповідності стандартам [20].

Завдяки описаним механізмам CMDB стає не просто сховищем даних про конфігурації, а стратегічним інструментом, що сприяє ефективному управлінню всією хмарною інфраструктурою.

Управління підписками

Управління підписками в хмарних середовищах є важливим аспектом забезпечення прозорості витрат і ефективного використання ресурсів. У цьому контексті конфігураційна база даних управління (CMDB) є потужним інструментом для інтеграції даних про підписки, відстеження витрат і прогнозування бюджету. Завдяки можливостям централізації та аналітики CMDB дає змогу організаціям підвищити контроль над своїми хмарними інвестиціями [20].

Контроль витрат через інтеграцію CMDB

Інтеграція даних про підписки з CMDB забезпечує організаціям можливість більш глибокого аналізу витрат. CMDB дозволяє об'єднати інформацію про витрати на рівні окремих облікових записів, проєктів чи відділів, створюючи прозору картину розподілу ресурсів. Наприклад, організація може відстежувати, який проєкт чи підрозділ споживає найбільше хмарних ресурсів, що дає змогу виявляти області для оптимізації.

Завдяки інтеграції з CMDB організації також можуть ідентифікувати можливості для зниження витрат. Аналіз використання ресурсів дає змогу визначити недовикористовувані або зайві підписки, а також рекомендувати перехід на економічніші моделі, такі як резервовані інстанси. Це забезпечує не лише економію, а й дає змогу ефективніше планувати розподіл ресурсів у майбутньому [21].

Формування бюджетів та прогнозування витрат

CMDB може відігравати ключову роль у бюджетуванні та прогнозуванні хмарних витрат. Інтеграція даних про підписки дає змогу формувати точні бюджети для проєктів чи підрозділів, ґрунтуючись на історичних даних про використання ресурсів. Наприклад, якщо підрозділ постійно перевищує свій бюджет, CMDB може допомогти ідентифікувати основні причини цього та надати рекомендації для зменшення витрат.

Прогнозування майбутніх витрат також значно полегшується завдяки аналітичним можливостям CMDB. Враховуючи заплановані зміни у конфігурації ресурсів або обсягах їх використання, CMDB може передбачати потенційні витрати. Це дає змогу організаціям завчасно коригувати бюджети та уникати непередбачених витрат. Наприклад, якщо планується масштабування певного сервісу, CMDB може допомогти оцінити, як це вплине на загальні витрати організації [22].

Контроль доступу (IAM) у контексті управління підписками

CMDB може бути використана для інтеграції з інструментами управління ідентифікацією та доступом (IAM), забезпечуючи централізований контроль над політиками доступу до хмарних ресурсів. Це передбачає:

- **аналіз та оптимізація ролей:** CMDB інтегрується з IAM-системами (наприклад, AWS IAM, Azure AD), даючи змогу відстежувати, хто має доступ до яких ресурсів, та виявляти надмірні привілеї;
- **автоматизація управління доступом:** завдяки автоматичному виявленню змін у привілеях доступу CMDB може сигналізувати про порушення політик безпеки або аномальні дії, які потребують уваги;
- **відповідність політикам безпеки:** CMDB зберігає інформацію про IAM-конфігурації, що дає змогу проводити регулярні аудити та забезпечувати відповідність нормативним вимогам [23].

Інтеграція з інструментами безпеки

CMDB ефективно працює у поєднанні з сучасними інструментами безпеки, такими як Splunk, Prisma Cloud та Tenable, для забезпечення комплексного підходу до управління ризиками та безпекою в хмарних середовищах:

- **Splunk:** використання CMDB для інтеграції з Splunk дає змогу централізувати дані про конфігурації та події безпеки, створюючи єдине джерело правди для аналізу загроз та моніторингу аномалій;
- **Prisma Cloud:** інтеграція з Prisma забезпечує автоматичний збір даних про конфігурації хмарних ресурсів, порівняння їх із політиками безпеки та виявлення вразливостей. CMDB дає змогу зберігати цю інформацію та забезпечувати історичний аналіз для підвищення відповідності стандартам.
- **Tenable:** використовуючи дані з CMDB, Tenable може проводити сканування вразливостей із контекстом конфігурацій, що дає змогу пріоритизувати виправлення найбільш критичних загроз.

Значення інтеграції CMDB у процес управління підписками

Інтеграція CMDB з процесами управління підписками, контролем доступу (IAM) та безпековими інструментами, такими як Splunk, Prisma Cloud і Tenable, відкриває нові можливості для оптимізації витрат і посилення захисту хмарної інфраструктури. Завдяки поєднанню даних про підписки, ролі доступу та безпекові події CMDB стає універсальним інструментом, що дозволяє організаціям забезпечувати прозорість, автоматизацію та відповідність у всіх аспектах управління хмарними ресурсами [24].

Розширені можливості CMDB дають змогу не лише відстежувати витрати на рівні проєктів чи підрозділів, а й прогнозувати бюджет, виявляти можливості для економії та оптимізувати використання підписок. Інтеграція з IAM забезпечує централізований контроль доступу, усуває надмірні привілеї та підвищує рівень безпеки завдяки регулярному аудиту конфігурацій. Водночас використання сучасних інструментів безпеки, таких як Prisma Cloud і Tenable, забезпечує проактивний моніторинг вразливостей і дає змогу ефективніше пріоритизувати ризики.

Такий комплексний підхід до управління підписками та безпекою не лише сприяє економії та оптимізації ресурсів, а й створює надійну основу для захисту даних та конфігурацій у хмарних середовищах. У швидко змінюваному світі хмарних технологій інтеграція CMDB із системами управління доступом та безпекою стає стратегічним елементом, що дає змогу організаціям досягати операційної досконалості та знижувати ризики, зберігаючи високий рівень продуктивності та відповідності стандартам [25].

Використання CMDB у контексті управління хмарними платформами

Управління хмарними платформами є складним завданням, яке потребує інтеграції різноманітних підходів до конфігурації, безпеки, моніторингу та оптимізації ресурсів. Конфігураційна база даних управління (CMDB) є центральним інструментом, що забезпечує узгодженість і прозорість усіх аспектів управління хмарними середовищами. Описано способи використання CMDB для автоматизації процесів, підтримки відповідності нормативам, оптимізації витрат і підвищення безпеки [26].

Організаційні структури та управління підписками інтегруються з CMDB через автоматизовані інструменти збору даних, такі як API хмарних провайдерів або спеціалізовані рішення для управління конфігураціями. Це забезпечує:

- **єдине джерело правди:** усі дані про облікові записи, підписки та ресурси доступні у єдиній системі;

- **миттєве оновлення:** дані оновлюються в реальному часі, даючи змогу знизити ризики через несвоєчасне оновлення;
- **гнучкість і масштабованість:** CMDB легко адаптується до змін у структурі організації чи обсягах хмарних ресурсів.

Інтеграція організаційних структур і підписок у CMDB дає змогу створити єдину платформу для централізованого управління, яка підтримує прозорість, ефективність і відповідність нормативним вимогам. Це є основою для побудови ефективного процесу управління ресурсами у сучасних хмарних середовищах [27].

Автоматизація управління конфігураціями є однією з ключових функцій CMDB. Інтеграція з інструментами Infrastructure as Code (IaC), такими як Terraform або Ansible, дає змогу автоматизувати створення, налаштування та управління хмарними ресурсами. CMDB зберігає дані про поточні конфігурації, що синхронізуються з автоматизованими процесами розгортання. Це знижує ризик людських помилок і прискорює впровадження змін. У випадках інцидентів CMDB надає необхідну інформацію для автоматичного відновлення інфраструктури до стабільного стану, зберігаючи дані про попередні конфігурації [28].

Управління залежностями між ресурсами - ще одна важлива функція CMDB. Вона дає змогу створювати моделі залежностей між компонентами, такими як бази даних, додатки або мережеві інтерфейси. Це спрощує аналіз впливу змін, забезпечуючи зменшення ризиків конфліктів і несумісностей конфігурацій. Наприклад, під час оновлення серверного середовища можна швидко оцінити вплив змін на пов'язані сервіси.

CMDB сприяє оптимізації продуктивності завдяки інтеграції з інструментами моніторингу, такими як AWS CloudWatch чи Datadog. Це дозволяє відстежувати продуктивність ресурсів, визначати вузькі місця та пропонувати рішення для їх усунення, наприклад, масштабування чи зміну конфігурації. Дані з CMDB використовуються для аналізу ефективності використання ресурсів, що допомагає уникати перевантажень або неефективного розподілу потужностей [29].

Для відповідності нормативним вимогам CMDB зберігає інформацію про політики доступу, конфігурації шифрування та інші аспекти безпеки. Інструменти автоматизованої звітності дають змогу організаціям проводити регулярні аудити та демонструвати відповідність стандартам, таким як GDPR, HIPAA чи PCI DSS. Це особливо важливо для організацій, які працюють із конфіденційними даними або регульованими галузями.

Інтеграція CMDB із системами управління змінами (Change Management) дає змогу аналізувати вплив запропонованих змін на інші ресурси та сервіси. Це забезпечує пріоритетність змін, сприяє їх ефективному плануванню та знижує ризик порушення стабільності системи.

З точки зору безпеки CMDB забезпечує аналіз політик доступу та допомагає відстежувати дотримання принципу мінімальних привілеїв. Інформація з CMDB дає змогу ідентифікувати вразливі конфігурації та автоматично виправляти їх. Це підвищує рівень захисту хмарної інфраструктури та мінімізує ризики порушення безпеки [30].

Підтримка мультихмарних середовищ стає дедалі актуальнішою. CMDB дає змогу інтегрувати дані з різних платформ, таких як AWS, Azure чи GCP, забезпечуючи єдину точку доступу до інформації про конфігурації. Це значно полегшує управління складними мультихмарними середовищами.

Інтеграція CMDB з DevOps процесами, зокрема CI/CD, дає змогу забезпечити відповідність стандартам конфігурації на всіх етапах розробки та розгортання. Використання CMDB у DevSecOps допомагає враховувати безпекові аспекти від початку життєвого циклу ресурсу.

CMDB є невід'ємною частиною управління хмарними платформами. Її використання дає змогу організаціям автоматизувати конфігурації, підвищити безпеку, оптимізувати витрати та забезпечити відповідність нормативам. Це робить CMDB важливим інструментом для підтримки ефективності та надійності сучасної хмарної інфраструктури [31].

Результати дослідження.

Підвищення ефективності управління CMDB у хмарній інфраструктурі

Сучасне управління CMDB у хмарних середовищах потребує високого рівня автоматизації, інтеграції та гнучкості. Платформа Cherwell, відома своєю функціональністю та зручністю, пропонує інструменти для ефективного управління CMDB, а інтеграція з Prisma API розширює її можливості для автоматизації збору даних про хмарні ресурси. У нашій корпоративній інфраструктурі впровадження Cherwell з Prisma API дало змогу досягти значного підвищення ефективності, точності та безпеки управління хмарними ресурсами.

Основні функції Cherwell для управління CMDB

Платформа Cherwell є одним із провідних інструментів для управління конфігураційними базами даних (CMDB), яка забезпечує централізоване управління ресурсами, автоматизацію процесів та підтримку мультихмарних середовищ. Її функціональні можливості розроблені для забезпечення ефективності, гнучкості та безпеки в умовах динамічної хмарної інфраструктури [32].

Гнучкі можливості CMDB

Cherwell пропонує широкий набір інструментів для відстеження активів і конфігурацій. Централізоване управління дає змогу організаціям зберігати інформацію про сервери, додатки, мережеві пристрої та їх взаємозв'язки. Це особливо важливо для аналізу впливу змін у хмарній інфраструктурі, що допомагає уникнути помилок і забезпечує стабільність роботи системи.

Додатково платформа підтримує налаштування моделей даних відповідно до специфічних потреб організацій. Це забезпечує гнучкість у створенні унікальних схем управління конфігураціями, що є критичним для підприємств, які працюють у динамічних і складних середовищах.

Управління доступом

Cherwell реалізує контроль доступу на основі ролей (RBAC), що дає змогу гнучко налаштувати доступ до даних CMDB залежно від ролей користувачів. Це забезпечує високий рівень безпеки, дотримуючись принципу мінімальних привілеїв.

Крім того, платформа підтримує журнали змін, які фіксують усі дії з даними CMDB. Це не лише забезпечує прозорість процесів, а й дає змогу організаціям відповідати нормативним вимогам, пов'язаним із безпекою даних [33].

Управління змінами та інцидентами

Cherwell інтегрує процеси управління змінами та інцидентами, що дає змогу організаціям ефективно реагувати на зміни в хмарній інфраструктурі. Управління змінами включає планування, затвердження та впровадження змін із мінімізацією ризиків. Платформа надає чіткі робочі процеси для координації цих етапів.

Управління інцидентами забезпечує швидке реагування на проблеми, що виникають у хмарних середовищах. Cherwell підтримує автоматизацію цього процесу, даючи змогу командам зосереджуватися на вирішенні складних задач.

Сервісний каталог та автоматизація

Cherwell пропонує сервісний каталог, який слугує централізованим інтерфейсом для запитів хмарних послуг. Це спрощує процеси замовлення та надання ресурсів, роблячи їх доступними для кінцевих користувачів.

Автоматизація робочих процесів є ще однією ключовою перевагою платформи. Завдяки цьому знижується ризик людських помилок і мінімізується ручна праця. Наприклад, платформа дає змогу автоматично оновлювати записи про активи або здійснювати моніторинг змін, що підвищує ефективність управління ресурсами [34].

Корпоративне впровадження: Автоматизація з Prisma API

Наведене рішення побудовано на інтеграції платформи Cherwell як центрального інструменту для управління конфігураційною базою даних (CMDB) із Prisma API, а також іншими системами моніторингу, аналітики та безпеки. Ця архітектура забезпечує вирішення ключових задач, пов'язаних із централізованим управлінням хмарними ресурсами, автоматизацією процесів та підвищенням рівня кібербезпеки (рис.).

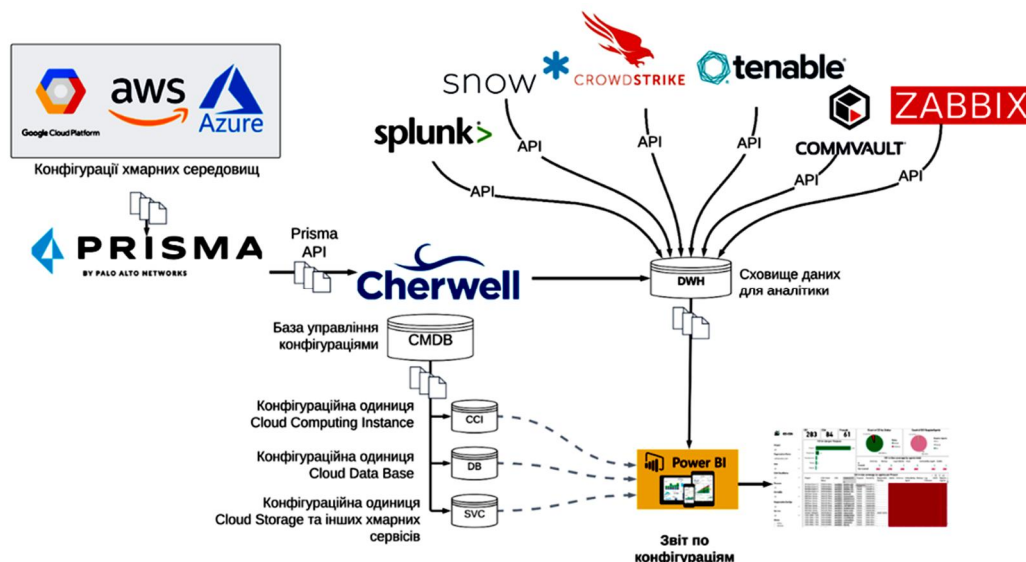


Рис. Архітектура інтеграції хмарних сервісів та системи аналітики

Однією з найбільших переваг є централізація управління, яку забезпечує Cherwell. Завдяки формуванню єдиного джерела правди (single source of truth) про всі хмарні ресурси організації платформа сприяє створенню прозорої та структурованої моделі управління, що полегшує облік активів і відстеження змін у мультихмарному середовищі [35].

Автоматизація процесів відіграє ключову роль у мінімізації ризиків людських помилок. Завдяки Prisma API дані про ресурси збираються автоматично, зокрема інформація про конфігурації, обчислювальні інстанси, бази даних і сервіси. Такий підхід забезпечує актуальність інформації в реальному часі, що критично важливо для ефективного управління динамічними хмарними середовищами.

Інтеграція з аналітичними та звітними інструментами, такими як Power BI та Splunk, дає змогу організаціям проводити детальний аналіз використання ресурсів, виявляти аномалії та формувати звіти для прийняття обґрунтованих рішень. Це сприяє оптимізації витрат, а також підвищує ефективність управлінських процесів, надаючи командам чіткі індикатори продуктивності.

Платформа також забезпечує підвищення рівня безпеки завдяки інтеграції з інструментами, такими як Prisma Cloud, Tenable та CrowdStrike. Використання цих систем дає змогу виявляти та усувати вразливості, моніторити події безпеки та зберігати відповідність нормативним вимогам. Отже, архітектура відповідає сучасним стандартам захисту даних і забезпечує стабільність роботи хмарної інфраструктури.

Підтримка мультихмарності є ще однією значною перевагою цього рішення. Завдяки інтеграції з AWS, Azure і GCP організації отримують уніфіковану модель управління ресурсами, що значно спрощує координацію та адміністрування навіть у складних мультихмарних середовищах [36].

Висновки

Інтеграція платформи Cherwell із Prisma API та іншими аналітичними й безпековими інструментами демонструє ефективний і комплексний підхід до управління хмарною інфраструктурою. Використання Cherwell як центрального елемента управління забезпечує організаціям централізоване сховище даних про всі ресурси, що слугує надійною основою для аналізу, оптимізації

та підтримання безперервності бізнес-процесів. Це рішення дає змогу підвищити точність даних, автоматизувати рутинні процеси та забезпечити відповідність сучасним вимогам безпеки.

Завдяки автоматизованому збору даних через Prisma API інтеграція значно знижує операційні витрати, мінімізує людський фактор та забезпечує актуальність конфігурацій у реальному часі. Додатково інтеграція з такими інструментами, як Power BI, Splunk та Tenable, розширює функціональність CMDB, дозволяючи поєднати управління витратами, моніторинг ресурсів та забезпечення безпеки. Це створює єдине джерело правди для хмарної інфраструктури, яке сприяє прийняттю обґрунтованих рішень і формуванню стратегій ефективного використання ресурсів.

Рішення підкреслює важливість мультихмарної підтримки, що забезпечує інтеграцію даних із різних провайдерів, таких як AWS, Azure та GCP. Це значно спрощує адміністрування складних інфраструктур, створюючи єдине інформаційне середовище для управління ресурсами та їхньої координації між платформами.

Запропонована архітектура пропонує:

1. Автоматизацію управління конфігураціями, що підвищує точність і релевантність даних.
2. Поєднання управління витратами та забезпечення безпеки завдяки використанню інтеграцій з аналітичними та моніторинговими інструментами.
3. Централізацію даних через CMDB, що забезпечує прозорість і ефективність адміністрування в мультихмарних середовищах.
4. Підвищення рівня кібербезпеки та мінімізацію ризиків завдяки інтеграції з інструментами моніторингу й захисту.

Отже, інтеграція CMDB із сучасними інструментами моніторингу, аналітики та безпеки є ключовим елементом для забезпечення високої операційної ефективності, зниження ризиків і підвищення продуктивності в хмарних середовищах.

Це комплексне рішення надає організаціям можливість адаптуватися до викликів цифрової трансформації, забезпечуючи прозорість управління, оптимізацію витрат та відповідність стандартам безпеки. Завдяки централізації даних, автоматизації рутинних процесів і мультихмарній підтримці, такий підхід створює надійну основу для довгострокового розвитку та посилення конкурентоспроможності, сприяючи ефективному використанню ресурсів і реалізації стратегічних цілей організацій.

Список літератури

1. Ellison M., Calinescu R., Paige R. Evaluating cloud database migration options using workload models. *Journal of Cloud Computing*. 2018. 7. 1–18. Doi: <https://doi.org/10.1186/s13677-018-0108-5>.
2. Brenner M., Gillmeister M. Designing CMDB data models with good utility and limited complexity. 2014 *IEEE Network Operations and Management Symposium (NOMS)*, 2014. 1–15. Doi: <https://doi.org/10.1109/NOMS.2014.6838375>.
3. Herrick D. CMDB Assessment and Remediation. *Proceedings of the 2023 ACM SIGUCCS Annual Conference*. 2023. Doi: <https://doi.org/10.1145/3539811.3579551>.
4. Keller A., Subramanian S. Best practices for deploying a CMDB in large-scale environments. 2009 *IFIP/IEEE International Symposium on Integrated Network Management*. 2009. 732–745. Doi: <https://doi.org/10.1109/INM.2009.5188880>.
5. Yaici M. P2P-based Solution for the Cloud Availability: The paper is about using a peer-to-peer configuration of the cloud users in order to respond quickly to a particular user request in case of the unavailability of the cloud. *Proceedings of the 2022 6th International Conference on Cloud and Big Data Computing*. 2022. Doi: <https://doi.org/10.1145/3555962.3555963>.
6. Yen-Jen C., Chen W. Implementation of a High Available Database on Virtualizing Cloud Platform. 2023 *5th International Conference on Computer Communication and the Internet (ICCCI)*, 2023. 229–235. Doi: <https://doi.org/10.1109/ICCCI59363.2023.10210178>.
7. Tasiran A. J., Barbosa S., Barthe M. et al. A Machine-Checked Proof of Security for AWS Key Management Service. 2019. 63–78. Doi: <https://doi.org/10.1145/3319535.3354228>.
8. Banakh R., Piskozub A., Stefinko Y. External elements of honeypot for wireless network. 2016 *13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*. Lviv, Ukraine, 2016. Pp. 480–482. Doi: <https://doi.org/10.1109/TCSET.2016.7452093>.

9. Martseniuk Y., Partyka A., Harasymchuk O., Nyemkova E., Karpinski M. Shadow IT risk analysis in public cloud infrastructure. *CEUR Workshop Proceedings*. 2024. Pp. 22- 31. 3800.
10. Muppa Kaushik Reddy. Advancing Cloud Security with AI-Enhanced AWS Identity and Access Management. *International research journal of engineering & applied sciences*. 2022. 25- 28. Doi: <https://doi.org/10.55083/irjeas.2022.v10i01005>.
11. Vakhula O., Opirskyy I., Mykhaylova O. Research on Security Challenges in Cloud Environments and Solutions based on the “security-as-Code” Approach *CEUR Workshop Proceedings*. 2023. 3550. Pp. 55–69.
12. Horpenyuk A., Opirskyy I., Vorobets P. Analysis of problems and prospects of implementation of post-quantum cryptographic algorithms. *CEUR Workshop Proceedings*. 2023. Vol. 3504 : Workshop on classic, quantum, and post-quantum cryptography, CQPC’2023. Pp. 39–49.
13. Martseniuk Y., Partyka A., Harasymchuk O., Shevchenko S. Universal centralized secret data management for automated public cloud provisioning *CEUR Workshop Proceedings*. 2024. 3826. Pp. 72- 81.
14. Raj Pritish. Continuous Integration for New Service Deployment and Service Validation Script for Vault. *Interantional journal of scientific research in engineering and management*. 2024. 08. 1- 5. Doi: <https://doi.org/10.55041/IJSREM35565>.
15. Drogseth Dennis, Sturm Rick, Twing Dan. CMDB System Deployment Stages. 2015. Doi: <https://doi.org/10.1016/B978-0-12-801265-9.00004-4>.
16. Wang Jiangning, Yang Lilong, Zheng Wei, Zhang Jun. Study on Comparative Performance of CL-20/RDX-based CMDB Propellants. *Propellants, Explosives, Pyrotechnics*. 2019. 44. Doi: <https://doi.org/10.1002/prep.201900029>.
17. Sun Shixiong, Zhao Benbo, Zhang Guangpu, Yunjun Luo. Applying Mechanically Activated Al/PTFE in CMDB Propellant. *Propellants, Explosives, Pyrotechnics*. 2018. 43. Doi: <https://doi.org/10.1002/prep.201800143>.
18. Keller A., Subramanian S. Best Practices for Deploying a CMDB in large-scale Environments. 2009. 732- 745. Doi: <https://doi.org/10.1109/INM.2009.5188880>.
19. Enunnnl Sravani. Ai and CMDB: pioneering a new era in it management author. 2024.
20. Enunnnl Sravani. Leveraging Artificial Intelligence for Configuration Management Database (CMDB) Optimization: A Comprehensive Analysis. 2024.
21. Niewiadomski Szymon, Mzyk Grzegorz. ML Support for Conformity Checks in CMDB-Like Databases. 2023. Doi: https://doi.org/10.1007/978-3-031-42508-0_33.
22. Maes Stephane. CMDB best practices: how to successfully implement CMDB in your organization. *IFS Blog*. 2023.
23. Enunnnl Sravani Harnessing the Synergy: Exploring the Benefits of Artificial Intelligence and Configuration Management Database (CMDB). 2024.
24. Martseniuk Y., Partyka A., Harasymchuk O., Korshun N. Automated Conformity Verification Concept for Cloud Security. *CEUR Workshop Proceedings*. 2024. 3654. Pp. 25- 37.
25. Yin Jianping, Li Meng, Du Wenxuan, He Xuanfu, Song Jun, Hu Bowen, Huang Meng, Li Yang, Miao Yinggang. Mechanical behaviors and failure mechanisms of CMDB propellant under wide strain rate tension loading. *Journal of Physics: Conference Series*. 2023. 2535. 012010. Doi: <https://doi.org/10.1088/17426596/2535/1/012010>.
26. Wei Huanan, Li Tianpeng, Yao Kai, Xuan Zhaolong. ReaxFF molecular dynamics simulations on thermal decomposition of RDX-based CMDB propellants. *Journal of Molecular Modeling*. 2022. 28. 388. Doi: <https://doi.org/10.1007/s00894-022-05377-4>.
27. Zheng Jian, Wang W.-Q, Cheng X.. Xu J.-S, Zhou Cunshan. Effects of loading rate and microstructure on dynamic fracture toughness of CMDB propellant. *Journal of Propulsion Technology*. 2015. 36. 940- 946. Doi: <https://doi.org/10.13675/j.cnki.tjjs.2015.06.019>.
28. Wang Tao, Duan Jingjing, Zhai Jiaqi, Zhao Jing, Gao Yulong, Gao Feng, Zhang Longlong, Zhao Yifei. Research on a cloud model intelligent computing platform for water resource management. *Journal of Hydroinformatics*. 2024. 26. Doi: <https://doi.org/10.2166/hydro.2024.223>.
29. Narayanan Pavan. Engineering Data Pipelines Using Google Cloud Platform, 2024. Doi: https://doi.org/10.1007/979-8-8688-0602-5_16.
30. Gulati Samridhi, Tyagi Ayushi, Goel Pawan. Security Automation and Orchestration in the Cloud, 2024. Doi: <https://doi.org/10.4018/979-8-3693-3249-8.ch002>
31. Nayyar Kshitiz. Best practices for seamless integration of Robotic Process Automation (RPA) and cloud technologies. *International Journal of Science and Research Archive*. 2024. 13. 3337- 3345. Doi: <https://doi.org/10.30574/ijrsra.2024.13.2.2560>.
32. Bolu Toluwani, Ade Martins. Leveraging AI and Automation in Cloud Security for Vulnerability Management, 2024.

33. Bishukarma Ramesh. *Optimising Cloud Security in Multi-Cloud Environments: A Study of Best Practices*. *Technix International Journal for Engineering Research*. 2024. 11. a590-a598.
34. Sreerangapuri Ashok. *Blockchain-Enabled AI Governance for Scalable Cloud Security Automation*. *International journal of computer engineering & technology*. 2024. 15. 947- 959. Doi: [https://doi.org/ 10.5281/zenodo.13962366](https://doi.org/10.5281/zenodo.13962366).
35. Thokala Vasudhar Sai. *Scalable Cloud Deployment and Automation for E-Commerce Platforms Using AWS, Heroku, and Ruby on Rails*. *International Journal of Advanced Research in Science, Communication and Technology*. 2023. 349- 362. Doi: <https://doi.org/10.48175/IJARSCT-13555A>.
36. Suram Kiran. *Innovations in Infrastructure Automation: Advancing IAM in Cloud Security*. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. 2025. 11. 255- 263. Doi: <https://doi.org/10.32628/CSEIT25111223>.

EXPLORING THE EFFECTIVENESS OF USING CENTRALIZED CONFIGURATION STORAGE TO SECURELY MANAGE CLOUD SERVICES INFRASTRUCTURE

Y. V. Matseniuk

Lviv Polytechnic National University,
Department of Information Protection

© Martseniuk Y. V., 2025

In the current context of widespread adoption of cloud technologies such as AWS, GCP, and Azure, organizations face challenges in centralized management of cloud resources, including ensuring security standards, monitoring service metrics, optimizing costs, and managing configurations. The main issue lies in the differences in the architecture of services provided by various cloud vendors, which complicates the integration and standardization of processes in multi-cloud environments.

This article focuses on analyzing the issues of centralized configuration management using the Configuration Management Database (CMDB) as a single source of truth. The study examines methods of organizing and managing CMDB in public cloud environments, with an emphasis on access management, organizational structures, subscriptions, and cloud resource inventory. Particular attention is paid to developing recommendations for optimizing management processes to improve overall efficiency and security.

The practical part of the study involves the integration of the Cherwell system as a CMDB with automated data collection through the Prisma API. This integration allows for the automation of resource inventory, reducing the risk of human errors, improving data accuracy, and ensuring compliance with security standards. Additionally, by centralizing data and analyzing it in Power BI, the study demonstrated the effectiveness of the approach in the context of a multi-cloud environment.

The purpose of this study is to develop a scientifically grounded approach to centralized configuration management of cloud infrastructure based on the use of a single data repository for configurations (CMDB). The study includes a detailed analysis of the challenges of cloud configuration management, the features of major cloud providers' services, and their integration into a unified informational model. The primary focus is on developing recommendations for building an efficient configuration management system that considers multi-cloud environments, security requirements, and operational processes.

The practical aspect of the study is based on the integration of the Cherwell system as a CMDB with Prisma API to automate data collection in a multi-cloud environment. This integration demonstrated significant advantages, including improved data accuracy, reduced manual work, enhanced information security, and optimized management processes.

Thus, the aim of the study is not only to provide a theoretical justification of centralized management methods for cloud resources but also to develop practical recommendations to improve the efficiency and security of configuration management in multi-cloud environments.

Keywords: Public cloud environments, configuration management, automation, integration.