Research of the Centralized Configuration Repository Efficiency for Secure Cloud Service Infrastructure Management*

Yevhenii Martseniuk[1,†], Andrii Partyka[1,†], Oleh Harasymchuk[1,†], Vyacheslav Cherevyk[2,*,†] and Nadiia Dovzhenko[2,†]

[1] *Lviv Polytechnic National University, 12 Stepan Bandera str., 79000 Lviv, Ukraine*
[2] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine*

Abstract

With the development of cloud services on public cloud infrastructures such as AWS, GCP, or Azure, organizations sooner or later face the challenge of centralized cloud resource management. This management encompasses security standards, service metrics, and various operational indicators. The issue lies in the fact that each vendor has a unique structure for their services, which are often not interchangeable. This paper aims to analyze the challenges of configuration management using a single centralized data repository based on the study of cloud provider services and to develop recommendations and approaches for managing cloud infrastructure through a unified configuration management methodology. The paper also explores methods for organizing and managing Configuration Management Databases (CMDB) in a public cloud infrastructure environment. Particular attention is given to access management, organizational structures, subscriptions, and cloud resource inventory, aiming to optimize processes to improve overall efficiency and security. The paper presents a practical implementation of integrating the Cherwell system as a CMDB with automated data collection through the Prisma API for a commercial organization, which significantly improves data accuracy and ensures security.

Keywords

cloud infrastructure, configuration management, CMDB, security compliance, security standard

1. Introduction

The Configuration Management Database (CMDB) is a key component in IT service management, providing a centralized repository of information about IT assets and their configurations. In the context of public cloud infrastructure, where resources and configurations are dynamic and distributed, effective CMDB management is crucial for maintaining operational efficiency and ensuring security. The purpose of this paper is to optimize configuration and resource management in public cloud environments by exploring existing methods and providing practical recommendations [1, 2]. Managing Configuration Management Databases (CMDB) is a critical aspect of IT management, as it ensures a centralized repository of information about IT assets and their configurations. In the dynamic and distributed nature of public cloud infrastructure, effective CMDB management is essential to maintaining operational efficiency and security.

The main functions of a CMDB are as follows:

- **Storing detailed information:** Maintaining comprehensive data about each Configuration Item (CI), including its attributes, status, and relationships with other CIs.
- **Tracking changes:** Recording and managing configuration changes to ensure controlled IT infrastructure development.

* *CPITS 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2025, Kyiv, Ukraine*
* Corresponding author.
† These authors contributed equally.
yevhenii.v.martseniuk@lpnu.ua (Y. Martseniuk); andrii.i.partyka@lpnu.ua (A. Partyka); garasymchuk@ukr.net (O. Harasymchuk); v.cherevyk@kubg.edu.ua (V. Cherevyk); n.dovzhenko@kubg.edu.ua (N. Dovzhenko)
0009-0009-2289-0968 (Y. Martseniuk); 0000-0003-3037-8373 (A. Partyka); 0000-0002-8742-8872 (O. Harasymchuk); 0000-0002-2735-5341 (V. Cherevyk); 0000-0003-4164-0066 (N. Dovzhenko)

- **Facilitating impact analysis:** Providing information on how changes to one CI may affect others, aiding in impact analysis and decision-making.
- **Supporting IT service management:** Enhancing IT service management practices by providing accurate and up-to-date information about the IT environment.

These CMDB functions enable effective IT infrastructure management, especially in the complex and dynamic nature of public cloud environments.

Scientific studies indicate that the core functions of a CMDB include storing detailed information about Configuration Items (CIs), tracking changes, analyzing the impact of changes, and supporting IT service management practices. For example, Ellison et al. (2018) [3] emphasize that integrating a CMDB with modern cloud platforms significantly simplifies the management of complex workloads. Brenner and Gillmeister (2014) [4] explore how well-designed CMDB data models can reduce the complexity of IT infrastructure management while ensuring its functionality. Herrick (2023) [5] highlights the importance of assessing and improving existing CMDBs to enhance operational efficiency.

1.1. The role of CMDB in public cloud infrastructure

In public cloud environments, the CMDB plays a key role due to the dynamic and scalable nature of cloud resources, which continuously evolve based on organizational needs. For example, Keller and Subramanian (2009) [6] emphasize the importance of adopting best practices when deploying a CMDB for efficient management of large environments. They highlight that a well-structured CMDB enables the integration of heterogeneous data sources, such as services from different cloud providers or resources located in various geographic regions. This, in turn, provides a holistic view of an organization's infrastructure, simplifying management and ensuring process transparency.

Yaici (2022) [7] proposes an innovative approach to resource availability using a peer-to-peer architecture. This solution enables quick responses to user requests even during the temporary unavailability of certain cloud resources. Such an approach significantly enhances the reliability of cloud infrastructure and improves CMDB functionality, particularly in multi-cloud or distributed environments.

Additionally, the role of CMDB in cloud infrastructure extends to automating resource management processes. As noted by Ellison et al. (2018) [3], integrating a CMDB with automated management systems can substantially reduce manual work, minimize human error, and ensure data accuracy. Automation also enables faster responses to configuration changes and ensures compliance with regulatory requirements.

1.2. Challenges in managing CMDB in cloud environments

Managing a CMDB in public cloud environments faces several challenges due to the complexity and dynamic nature of such systems. One of the key issues is the diversity of cloud services and their configurations. Brenner and Gillmeister (2014) [4] point out that the large number of service providers, each using their standards and architectures, makes maintaining a comprehensive configuration management database extremely challenging. This creates barriers to data integration and complicates the development of a cohesive infrastructure model.

Visibility issues regarding resources and their interrelationships are particularly pronounced in multi-cloud environments, where organizations work with multiple providers simultaneously. As Yen-Jen and Chen (2023) [8] note, integrating highly available databases into virtualized cloud platforms is a critical step toward ensuring system reliability. However, this requires significant technical effort and careful planning to avoid performance issues or incompatibility between different platforms.

Ellison et al. (2018) [3] also emphasize the necessity of automating processes to maintain the accuracy and relevance of data in the CMDB. Constant changes in cloud resources and the rapid pace of updates make manual database management increasingly difficult. Automation not only

simplifies these processes but also enables the integration of CMDB with other IT management tools, reducing the risks of data loss or non-compliance with regulatory requirements.
Another significant challenge is ensuring data security in cloud environments. Growing regulatory compliance demands require CMDBs to not only maintain configuration accuracy but also protect information from potential threats. This necessitates the use of modern monitoring and analytics tools that should be directly integrated into the CMDB infrastructure.

1.3. Access as a configuration Item in CMDB

In public cloud environments, access to resources is not only an operational task but also a critical configuration element that must be accounted for in a comprehensive configuration management system (CMDB). Since access configurations directly impact the security and integrity of cloud infrastructure, integrating access data into the CMDB is essential for ensuring a holistic approach to cybersecurity.

Access Identification via IAM: Identity and Access Management (IAM) systems are the primary source of data on access policies, user roles, and permissions. These data should be integrated into the CMDB as Configuration Items (CIs) [9] enabling the following:

1. Tracking changes to access policies with a history of modifications.
2. Detecting potential conflicts or errors in permissions.
3. Ensuring compliance with the principle of least privilege.

Roles and Access Attributes as Configuration Parameters: Role-based access control (RBAC) and attribute-based access control (ABAC) should be represented as configuration parameters in the CMDB. This enables the following:

1. Establishing relationships between roles, resources, and users that reflect real dependencies in the cloud infrastructure [10].
2. Leveraging access attributes to create conditional security policies that automatically adapt based on context (e.g., geographic location or time of access).

Access Data Integrity: Access information in the CMDB must be accurate and complete [11]. Automating the collection of access data from sources such as cloud platforms (AWS IAM, Azure AD, Google Cloud IAM) or third-party tools (Okta, CyberArk) helps achieve the following:

- Preventing security policy gaps due to delayed updates.
- Identifying potential access policy violations at early stages.

The Role of Access in the Holistic Picture of Cybersecurity: Access configurations are an integral part of the cybersecurity of cloud infrastructure. The lack of a unified approach to access management through the CMDB can lead to:

- The emergence of “blind spots” where permissions or access policies remain inconsistent across different cloud environments [12].
- The risk of non-compliance with regulatory requirements due to failure to adhere to security compliance principles.

Integrating access into the CMDB also faces the following challenges:

- A**Scalability issues:** The large number of users, roles, and access rules in large organizations generates substantial amounts of data that require processing.
- **Updates automation:** Ensuring data accuracy requires the implementation of automated synchronization mechanisms between the CMDB and IAM systems.

- **Contextual nature of data:** Access data is often context-dependent, which complicates its standardization for integration into the CMDB.

2. Overview of CMDB offerings in the cloud solutions market

A Configuration Management Database (CMDB) is a critical component for organizations utilizing cloud platforms. It enables centralized storage of data about resources, their configurations, and relationships, ensuring transparency in infrastructure management [13, 14]. AWS, Azure, and GCP offer unique capabilities for integration with CMDBs, automating resource inventory and management. However, each platform has distinct features that influence organizational processes.

2.1. Resource inventory features on AWS

Amazon Web Services (AWS) provides tools for resource inventory and management, characterized by a high level of automation and integration with other AWS ecosystem services. A key solution is **AWS Config**, which creates a comprehensive inventory of cloud resources, tracks changes, and ensures compliance with organizational security policies. This service enables organizations to gain a complete view of resource status and monitor adherence to regulatory standards.

Another significant tool is **AWS Systems Manager**, which simplifies centralized configuration management. This service allows resource data to be seamlessly integrated into the CMDB, ensuring accuracy and up-to-date information. AWS's main advantages include deep integration within its ecosystem, which automates most resource inventory and management processes [15]. Additionally, AWS APIs provide robust capabilities for integrating with external CMDB systems, enhancing functionality, and simplifying configuration management. However, a key limitation is AWS's strong focus on its ecosystem, which can pose challenges for organizations operating in multi-cloud environments that require flexible integration with other platforms [16].

2.2. Resource inventory features on Azure

Microsoft Azure provides centralized resource management through tools like **Azure Resource Manager (ARM)**. ARM enables the use of templates to describe infrastructure and integrate with CMDB, simplifying the implementation of configuration management standards. To monitor resource status and ensure compliance with organizational standards, Azure offers **Azure Monitor** and **Azure Policy**. These services help detect and correct configuration violations, ensuring all resources adhere to established policies. A key advantage of Azure is its close integration with other Microsoft enterprise solutions, such as **Active Directory**. This seamless integration supports organizations utilizing hybrid environments that combine cloud and on-premises resources. However, compared to AWS and GCP, Azure's capabilities for multi-cloud management are less developed, which may limit its use in more complex infrastructures [17].

2.3. Resource inventory features on GCP

Google Cloud Platform (GCP) stands out for its focus on analytics and tools for detailed resource monitoring. The primary tool is Google Cloud Asset Inventory, which enables comprehensive resource inventory management with integration capabilities for CMDB. This service ensures a precise representation of configurations, changes, and dependencies among resources. For deeper analysis and monitoring, GCP offers the Google Cloud Operations Suite (formerly Stackdriver), which provides tools for performance monitoring, log analysis, and issue diagnostics. GCP's strengths lie in its analytical orientation, allowing for effective resource usage forecasting and early problem detection. Additionally, GCP actively supports multi-cloud environments through services like Anthos, which ensures unified resource management across multiple clouds. However, integrating GCP tools with traditional CMDB systems can be challenging due to differences in data modeling and configuration approaches [18].

2.4. Comparison of CMDB solutions from cloud service providers

Based on the above, the following conclusions can be drawn:

- AWS, Azure, and GCP each offer unique features for resource management suitable for different use cases.
- AWS provides robust tools for CMDB integration but limits flexibility in multi-cloud environments [19].
- Azure is ideal for organizations with hybrid infrastructures due to its integration with other Microsoft enterprise solutions.
- GCP excels in analytics and multi-cloud support but may require additional effort to integrate with traditional CMDB systems.

Table 1 highlights the specific strengths and limitations of each platform. The choice of platform depends on an organization's specific needs, infrastructure, and strategic goals.

Table 1
Comparison of CMDB integration approaches

Cloud Platform	Resources Inventory Tools	CMDB Integration	Peculiarities
AWS	AWS Config, Systems Manager	Powerful API	Deep AWS ecosystem integration.
Azure	ARM, Azure Monitor, Azure Policy	Integration through Active Directory	Convenience for hybrid environments
GCP	Cloud Asset Inventory, Operations Suite	Multi-cloud support	Analytics orientation.

2.5. What does the market offer for CMDB integration and resource inventory management?

The modern market provides a range of tools that simplify CMDB integration with cloud platforms and automate resource inventory and management. These solutions not only maintain configuration data but also automate the collection, monitoring, and analysis of information from cloud environments such as AWS, Azure, and GCP. Below are key platforms that offer a comprehensive approach to addressing this challenge [20].

ServiceNow ITOM is a leading solution for CMDB management in cloud environments. It offers deep integration with major cloud platforms, including AWS, Azure, and GCP, through APIs. This enables automatic resource data collection, tracking of changes, and storing this information in the CMDB. Additionally, ServiceNow ITOM provides analytical tools to evaluate the impact of changes on the infrastructure, allowing organizations to respond quickly to dynamic changes in cloud environments.

Cherwell ITSM is another popular choice for CMDB management. With integration via the Prisma API, this tool ensures automated data collection on cloud resources and keeps it up to date. Cherwell is known for its flexibility in configuring data models, making it suitable for organizations with unique or complex infrastructures. An added benefit is the ability to configure workflows to automate routine tasks.

HashiCorp Terraform takes a unique approach to configuration management by focusing on the Infrastructure as Code (IaC) principle. It allows for synchronizing configurations with CMDB and ensures automated management of changes in cloud infrastructure. Terraform is also

distinguished by its multi-cloud support, making it ideal for organizations with diverse cloud environments.

BMC Helix Discovery specializes in the automatic discovery of cloud resources and their integration with CMDB. The tool allows for rapid identification of new assets and storing them in a centralized database. Multi-cloud support provides BMC Helix Discovery with the flexibility to work with various platforms, enabling organizations to achieve a unified view of all their resources.

CloudHealth by VMware focuses on resource inventory, cost management, and integrating this data with CMDB. The tool allows organizations to optimize their costs by analyzing resource usage while automating data collection to keep information up to date.

Solutions for integrating CMDB with cloud platforms, such as **ServiceNow ITOM**, **Cherwell ITSM**, **HashiCorp Terraform**, **BMC Helix Discovery**, and **CloudHealth by VMware**, play a crucial role in modern cloud infrastructure management. Each of these tools offers unique approaches to integration, automation, and configuration management, enabling organizations to choose a solution that fits their specific needs.

ServiceNow ITOM is a powerful solution offering deep integration with major cloud platforms (AWS, Azure, GCP) and providing analytical capabilities for change management. However, its multi-cloud support is moderate, which may limit its effectiveness in complex infrastructures.

Cherwell ITSM stands out for its flexibility and ability to integrate with numerous APIs. The tool offers convenient customization of data models and workflow automation, making it ideal for organizations with complex and multi-cloud environments. Cherwell also integrates a service-oriented approach, covering not only resource inventory but also service management, change management, and incident handling.

HashiCorp Terraform focuses on the Infrastructure as Code (IaC) approach, making it ideal for configuration automation in multi-cloud environments. However, its functionality is more focused on the technical aspects of resource management rather than service management.

BMC Helix Discovery provides an efficient tool for automatically discovering cloud assets and integrating them with CMDB. With multi-cloud support and rapid detection of new resources, this solution ensures effective inventory management. However, its functionality is limited in terms of analytics and service management capabilities.

CloudHealth by VMware focuses on cost management and resource usage optimization while integrating this data with CMDB. However, its configuration management capabilities are less advanced compared to other tools.

2.6. Key aspects of choosing a system

- ServiceNow ITOM is an effective solution for organizations requiring deep integration with cloud platforms and advanced analytical tools.
- Cherwell ITSM is the best choice when flexibility, automation, and integration with a wide range of services are priorities.
- HashiCorp Terraform is optimal for organizations adopting Infrastructure as Code (IaC) and operating in multi-cloud environments.
- BMC Helix Discovery is suitable for rapid resource discovery and CMDB integration in multi-cloud environments.
- CloudHealth by VMware is ideal for companies focused on cost optimization and resource monitoring.

Each system offers a unique set of features tailored to different aspects of CMDB integration and management. Choosing the best solution depends on the organization's specific needs, such as infrastructure scale, automation requirements, multi-cloud support, and the prioritization of service or analytical capabilities [21].

Table 2
Comparing main solutions for CMDB integration

Solution	Main possibilities	Peculiarities	Multi-cloud support
ServiceNow ITOM	Automatic data collection through API changes analytics	Deep integration with AWS, Azure, GCP	Medium
Cherwell ITSM	Automatic data collection through API, integration with a big amount of API, changes analytics, data models setup, integrated service approach	Comfortable configuration, work process automation, setup flexibility	High
HashiCorp Terraform	Configuration management through IaC, synchronization with CMDB	Multi-cloud orientation, change automation	High
BMC Helix Discovery	Automatic resources discovery, integration with CMDB	Quick detection of new assets, multi-cloud support	High
CloudHealth by VMware	Resources inventory, expenses management, integration with CMDB	Expenses optimization, resource usage analysis	Medium

Overall, **Cherwell ITSM** provides the most balanced approach, combining flexibility, ease of configuration, and robust integration capabilities, making it a standout leader among the presented solutions. Its versatility and adaptability make it an optimal choice for organizations aiming to integrate CMDB effectively with cloud platforms. Cherwell enables automatic data collection via APIs, integrates with a wide range of services, and allows data models to be easily customized to meet specific organizational needs. Additionally, its integrated service-oriented approach facilitates the automation of complex workflows, ensuring high efficiency in multi-cloud environments.

Compared to other solutions such as **ServiceNow ITOM** or **CloudHealth by VMware**, **Cherwell ITSM** offers greater flexibility in customization and provides superior multi-cloud support. Unlike **HashiCorp Terraform**, which focuses on Infrastructure as Code, **Cherwell ITSM** delivers a broader range of functionalities, managing both resources and services, including change and incident integration. This makes **Cherwell ITSM** not only a versatile tool but also a strategic solution for organizations aiming to maximize the value of their CMDB [22].

Table 2 highlights **Cherwell ITSM**'s advantages over its competitors, making it the most comprehensive option for effective cloud platform integration.

3. Organizational structures and subscription management: The role of CMDB in ensuring efficiency

Effective resource management in public cloud environments requires a well-defined organizational structure and subscription management strategy. CMDB, as a centralized repository of configuration information, plays a key role in ensuring transparency, consistency, and optimization of these processes. This section examines how organizational structures and subscription management integrate with CMDB to achieve greater efficiency in managing cloud resources.

3.1. Organizational structures

Large organizations using cloud platforms often face the need to manage a large number of accounts (tenants) distributed across various projects, departments, or environments such as development, testing, and production. In this context, **a tenant** is defined as a logically isolated unit provided to users or user groups within a shared cloud platform or service. The core concept of a tenant is to ensure the isolation of data, configurations, users, and resources of one client from others using the same cloud platform [23].

The isolation provided by tenants allows organizations to create segmented environments for different business needs, such as testing new features without the risk of impacting production systems. It also supports compliance with security policies and simplifies resource management in large-scale infrastructures.

3.1.1. Using CMDB for tenant management

A Configuration Management Database (CMDB) can serve as a key tool for integrating and managing tenants. In the CMDB, each tenant can be represented as a **Configuration Item (CI)**, enabling the efficient structuring of data about all organizational accounts. This creates a foundation for implementing a structured approach to account management through the following key mechanisms:

- **Account Segmentation:** CMDB enables the organization of accounts into logical groups according to organizational structure, projects, or environments. This segmentation simplifies access management, resource allocation, and cost control, providing precise data on resource usage within each group.
- **Centralized Management:** Integrating tenants into the CMDB allows for the implementation of unified security and compliance policies across all accounts. For example, automated monitoring can continuously verify that each tenant's configurations adhere to established standards and policies [24].

3.1.2. Tagging and categorization as resource organization tools

In addition to account management, the CMDB supports **tagging and categorization** functions, which are powerful tools for organizing and analyzing cloud resources.

- **Tagging** enables the addition of metadata to resources, such as identifying their owner, project, environment, or other attributes. This simplifies resource search and grouping processes and facilitates usage analysis. For instance, the tag "Development" helps track expenses during a specific project phase.
- **Categorization** allows resources to be logically grouped by application type, environment, or other attributes. This creates a structured view of resources, significantly simplifying reporting, cost management, and performance monitoring.

The integration of tenants into the CMDB, complemented by tagging and categorization functions, creates a unified management system that meets modern scalability and security requirements for cloud infrastructure. This approach is particularly important for large organizations operating in multi-cloud environments, where it is critical not only to control resources but also to ensure their optimal use in terms of cost, performance, and compliance with standards [25].

Through these mechanisms, the CMDB becomes more than just a repository of configuration data—it evolves into a strategic tool that supports the effective management of the entire cloud infrastructure.

3.2. Subscription management

Subscription management in cloud environments is a critical aspect of ensuring cost transparency and efficient resource utilization. In this context, the **Configuration Management Database (CMDB)** serves as a powerful tool for integrating subscription data, tracking expenses, and forecasting budgets. Through its centralization and analytics capabilities, the CMDB allows organizations to gain greater control over their cloud investments [26].

3.2.1. Cost control through CMDB integration

Integrating subscription data with the CMDB enables organizations to perform a deeper analysis of costs. The CMDB consolidates information on expenses at the level of individual accounts, projects, or departments, creating a clear picture of resource allocation. For instance, an organization can track which project or department consumes the most cloud resources, enabling the identification of areas for optimization.

By integrating with the CMDB, organizations can also identify opportunities for cost reduction. Resource usage analysis helps detect underutilized or redundant subscriptions and recommends transitions to more cost-effective models, such as **reserved instances**. This not only leads to savings but also allows for more effective future resource planning [27].

3.2.2. Budgeting and expense forecasting

The CMDB plays a key role in budgeting and forecasting cloud expenses. Subscription data integration allows for the creation of accurate budgets for projects or departments based on historical resource usage data. For example, if a department consistently exceeds its budget, the CMDB can help identify the root causes and provide recommendations for reducing expenses.

Forecasting future expenses is also significantly simplified by the CMDB's analytical capabilities. Considering planned changes in resource configurations or usage volumes, the CMDB can predict potential costs. This allows organizations to adjust budgets in advance and avoid unexpected expenses. For instance, if scaling a specific service is planned, the CMDB can estimate its impact on the organization's overall expenses [28].

3.2.3. Access Control in the Context of Subscription Management

The CMDB can be integrated with Identity and Access Management (**IAM**) tools to provide centralized control over access policies for cloud resources. This includes:

- **Role Analysis and Optimization:** The CMDB integrates with IAM systems (e.g., AWS IAM, Azure AD), enabling the tracking of who has access to which resources and identifying excessive privileges.
- **Access Management Automation:** Through the automatic detection of changes in access privileges, the CMDB can alert organizations to security policy violations or anomalous actions requiring attention.
- **Compliance with Security Policies:** The CMDB stores information about IAM configurations, facilitating regular audits and ensuring compliance with regulatory requirements [29].

3.2.4. Integration with security tools

The CMDB works effectively in conjunction with modern security tools like **Splunk**, **Prisma Cloud**, and **Tenable** to ensure a comprehensive approach to risk management and security in cloud environments:

- **Splunk:** Integrating the CMDB with Splunk centralizes data on configurations and security events, creating a single source of truth for threat analysis and anomaly monitoring.

- **Prisma Cloud:** Integration with Prisma enables the automatic collection of data on cloud resource configurations, comparison with security policies, and detection of vulnerabilities. The CMDB stores this information and facilitates historical analysis to enhance compliance with standards.
- **Tenable:** By leveraging CMDB data, Tenable can perform vulnerability scans with configuration context, allowing organizations to prioritize the remediation of the most critical threats.

3.2.5. The importance of CMDB Integration in subscription management processes

Integrating CMDB with subscription management, access control (IAM), and security tools like Splunk, Prisma Cloud, and Tenable unlocks new opportunities for optimizing costs and strengthening cloud infrastructure security. By combining data on subscriptions, access roles, and security events, CMDB becomes a versatile tool that enables organizations to achieve transparency, automation, and compliance across all aspects of cloud resource management [30].

The advanced capabilities of CMDB not only allow for tracking costs at the project or departmental level but also facilitate budget forecasting, identifying opportunities for savings, and optimizing subscription usage. Integration with IAM ensures centralized access control, eliminates excessive privileges, and enhances security through regular configuration audits. At the same time, the use of modern security tools like Prisma Cloud and Tenable enables proactive vulnerability monitoring and more effective risk prioritization.

This comprehensive approach to subscription and security management not only promotes cost savings and resource optimization but also provides a robust foundation for protecting data and configurations in cloud environments. In the rapidly evolving world of cloud technologies, CMDB integration with access management and security systems becomes a strategic element that allows organizations to achieve operational excellence and mitigate risks while maintaining high standards of performance and compliance [31].

3.3. Using CMDB in cloud platform management

Managing cloud platforms is a complex task requiring the integration of diverse approaches to configuration, security, monitoring, and resource optimization. The Configuration Management Database (CMDB) serves as a central tool, ensuring consistency and transparency across all aspects of cloud environment management. This section explores how CMDB can be leveraged to automate processes, ensure regulatory compliance, optimize costs, and enhance security [32].

Organizational structures and subscription management are integrated with CMDB through automated data collection tools, such as cloud provider APIs or specialized configuration management solutions. This integration ensures:

- **A single source of truth**: All data about accounts, subscriptions, and resources is accessible in one unified system.
- **Real-time updates**: Data is refreshed instantly, reducing risks associated with outdated information.
- **Flexibility and scalability**: CMDB easily adapts to changes in organizational structure or cloud resource volume [33].

Integrating organizational structures and subscriptions into CMDB creates a centralized management platform that supports transparency, efficiency, and compliance with regulatory requirements. This forms the foundation for effective resource management in modern cloud environments [34].

One of the key functions of CMDB is the automation of configuration management. Integration with Infrastructure as Code (IaC) tools such as Terraform or Ansible enables the automated creation, configuration, and management of cloud resources. CMDB stores data on current

configurations, synchronizing with automated deployment processes. This reduces the risk of human error and accelerates the implementation of changes. In incident scenarios, CMDB provides the necessary data for automatically restoring the infrastructure to a stable state while retaining information on previous configurations [35].

CMDB enables the modeling of dependencies between resources, such as databases, applications, or network interfaces. This simplifies impact analysis for changes, reducing the risk of conflicts and configuration incompatibilities. For instance, when updating a server environment, CMDB can quickly assess the impact of changes on related services.

CMDB contributes to performance optimization through integration with monitoring tools such as AWS CloudWatch or Datadog. This allows organizations to monitor resource performance, identify bottlenecks, and propose solutions, such as scaling or reconfiguring resources. CMDB data is used to analyze resource utilization efficiency, helping to prevent overloads or inefficient capacity distribution [36].

To meet regulatory requirements, CMDB stores information about access policies, encryption configurations, and other security aspects. Automated reporting tools enable organizations to conduct regular audits and demonstrate compliance with standards such as GDPR, HIPAA, or PCI DSS. This is particularly crucial for organizations handling sensitive data or operating in regulated industries.

CMDB integration with change management systems allows for analyzing the impact of proposed changes on other resources and services. This ensures proper prioritization of changes, supports efficient planning, and minimizes the risk of system stability disruptions.

From a security perspective, CMDB facilitates the analysis of access policies and helps ensure adherence to the principle of least privilege. CMDB data can identify vulnerable configurations and enable their automatic remediation [37]. This improves the security level of cloud infrastructure and minimizes the risk of security breaches.

Support for multi-cloud environments is becoming increasingly relevant. A CMDB enables the integration of data from various platforms, such as AWS, Azure, or GCP, providing a single point of access to configuration information. This greatly simplifies the management of complex multi-cloud environments.

The integration of CMDB with DevOps processes, particularly CI/CD, ensures compliance with configuration standards at all stages of development and deployment. Leveraging CMDB within DevSecOps allows security considerations to be addressed from the very beginning of a resource's lifecycle.

CMDB is an integral part of cloud platform management. Its use enables organizations to automate configurations, enhance security, optimize costs, and ensure regulatory compliance. This makes CMDB a critical tool for maintaining the efficiency and reliability of modern cloud infrastructure [38].

4. Cherwell and Prisma API: Enhancing CMDB management efficiency in cloud infrastructure

Modern CMDB management in cloud environments requires a high level of automation, integration, and flexibility. The **Cherwell** platform, known for its functionality and user-friendliness, offers tools for efficient CMDB management, while integration with the **Prisma API** extends its capabilities for automating cloud resource data collection. In our corporate infrastructure, implementing Cherwell with Prisma API has resulted in significant improvements in efficiency, accuracy, and security for cloud resource management.

4.1. Key features of Cherwell for CMDB management

The Cherwell platform is one of the leading tools for managing configuration management databases (CMDB), providing centralized resource management, process automation, and support for multi-cloud environments. Its features are designed to ensure efficiency, flexibility, and security in the context of dynamic cloud infrastructure [39].

4.1.1. Flexible CMDB capabilities

Cherwell offers a wide range of tools for tracking assets and configurations. Centralized management enables organizations to store information about servers, applications, network devices, and their interdependencies. This is especially important for analyzing the impact of changes in cloud infrastructure, helping to avoid errors, and ensuring system stability.

Additionally, the platform supports the customization of data models to meet specific organizational needs. This ensures flexibility in creating unique configuration management schemes, which is critical for enterprises operating in dynamic and complex environments.

4.1.2. Access management

Cherwell implements **role-based access control (RBAC)**, allowing flexible configuration of CMDB data access based on user roles. This ensures a high level of security while adhering to the principle of least privilege.

Additionally, the platform supports **change logs** that record all actions involving CMDB data. This not only ensures process transparency but also enables organizations to comply with data security regulatory requirements [40].

4.1.3. Change and incident management

Cherwell integrates change and incident management processes, enabling organizations to respond effectively to changes in cloud infrastructure. Change management includes planning, approval, and implementation of changes while minimizing risks. The platform provides clear workflows for coordinating these stages.

Incident management ensures a rapid response to issues that arise in cloud environments. Cherwell supports automation of this process, allowing teams to focus on resolving complex tasks.

4.1.4. Service catalog and automation

Cherwell offers a **service catalog** that serves as a centralized interface for cloud service requests. This simplifies the processes of ordering and provisioning resources, making them more accessible to end users.

Workflow automation is another key advantage of the platform. This reduces the risk of human error and minimizes manual labor. For example, the platform can automatically update asset records or monitor changes, enhancing the efficiency of resource management [41].

4.2. Corporate implementation: Automation with Prisma API

The presented solution is built on the integration of the Cherwell platform as a central tool for managing the configuration management database (CMDB) with Prisma API, as well as other monitoring, analytics, and security systems. This architecture addresses key tasks related to centralized management of cloud resources, process automation, and enhancement of cybersecurity levels (Fig. 1).

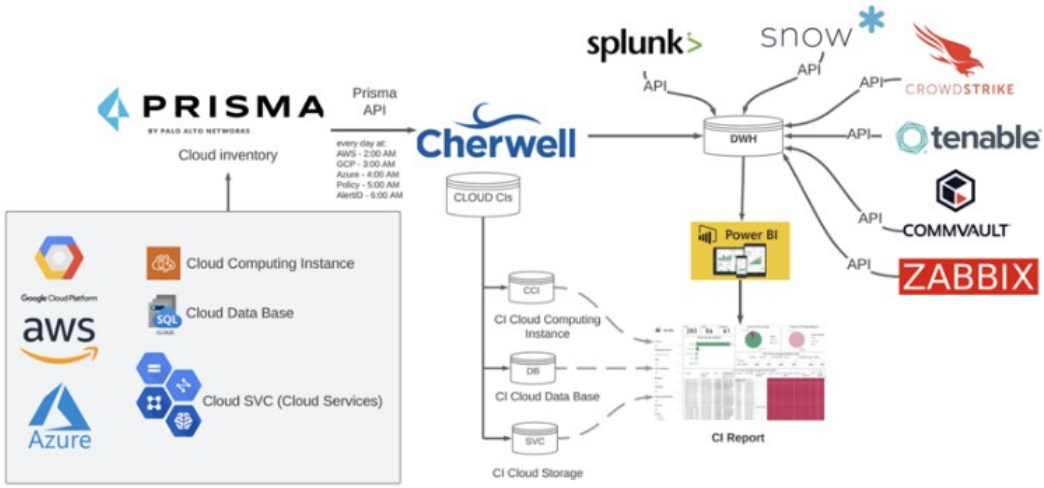

Figure 1: Integration Architecture of Cloud Services and Analytics Systems

One of the greatest advantages provided by Cherwell is **centralized management**. By establishing a single source of truth for all organizational cloud resources, the platform facilitates the creation of a transparent and structured management model, simplifying asset accounting and tracking changes in a multi-cloud environment [42].

Process automation plays a key role in minimizing the risks of human error. Through Prisma API, data about resources—such as configurations, compute instances, databases, and services—is collected automatically. This approach ensures real-time data accuracy, which is critical for effectively managing dynamic cloud environments.

Integration with **analytical and reporting tools** like Power BI and Splunk enables organizations to perform detailed analyses of resource usage, detect anomalies, and generate reports to support informed decision-making. This fosters cost optimization and enhances management efficiency by providing teams with clear performance indicators.

The platform also **enhances security levels** through integration with tools like Prisma Cloud, Tenable, and CrowdStrike. These systems help identify and mitigate vulnerabilities, monitor security events, and maintain compliance with regulatory requirements. Thus, the architecture meets modern data protection standards and ensures the stability of cloud infrastructure operations.

Another significant advantage of this solution is its **support for multi-cloud environments**. By integrating with AWS, Azure, and GCP, organizations gain a unified resource management model that greatly simplifies coordination and administration, even in complex multi-cloud environments [43].

Conclusions

The proposed architecture integrating Cherwell with Prisma API and other analytical and security tools demonstrates a highly effective and comprehensive approach to managing cloud infrastructures. Using Cherwell as the central element of the solution allows organizations to centralize all resource data, creating a powerful tool for analysis, optimization, and management.

Additionally, the automation of data collection through Prisma API and integration with systems like Power BI, Splunk, and Tenable significantly enhance the platform's functionality. These integrations not only optimize costs and improve efficiency but also strengthen data protection and compliance with security standards.

Thus, this solution serves as a reliable foundation for achieving operational efficiency, minimizing risks, and reducing costs in complex multi-cloud environments. Its implementation enables organizations to adapt their cloud strategies to modern demands and enhance competitiveness through an innovative approach to infrastructure management.

One of the key advantages of this approach is the **centralization of data** in the CMDB, creating a single source of truth for asset management. This allows organizations to track resources, analyze their usage, and optimize costs. Additionally, integration with analytical tools like Power BI enables data visualization and the creation of informative reports, supporting well-informed managerial decisions.

In the realm of security, the use of Prisma Cloud, Splunk, and Tenable ensures the detection and elimination of vulnerabilities, anomaly monitoring, and compliance with regulatory standards. These tools expand the functionality of the CMDB, transforming it into a strategic element for protecting cloud infrastructure.

The proposed architecture also highlights the importance of **multi-cloud support**, enabling the integration of data from platforms like AWS, Azure, and GCP into a unified environment. This significantly simplifies the management of complex infrastructures and facilitates effective coordination among different cloud providers.

1. The integration of Cherwell with Prisma API automates configuration management, enhancing the accuracy and real-time relevance of data.
2. Utilizing analytical and security tools like Power BI, Splunk, and Tenable combines cost management with data protection in cloud environments.
3. Multi-cloud support and data centralization through CMDB ensure transparency and ease of administration, which is critical for large and complex infrastructures.
4. This solution minimizes risks, enhances cybersecurity, and optimizes resources, enabling organizations to meet modern demands for efficiency and security.

In conclusion, the integration of CMDB with modern monitoring, security, and analytics tools is a strategically important solution for organizations aiming to achieve high operational efficiency in their cloud environments. This research offers a reliable approach that allows organizations not only to adapt to current challenges but also to build a sustainable competitive advantage.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] V. Shapoval, et al., Automation of data management processes in cloud storage, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 410–418.

[2] A. Ilyenko, et al., Practical aspects of using fully homomorphic encryption systems to protect cloud computing, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 226–233.

[3] M. Ellison, R. Calinescu, R. Paige, Evaluating cloud database migration options using workload models, J. Cloud Comput. 7 (2018) 1–18. doi:10.1186/s13677-018-0108-5

[4] M. Brenner, M. Gillmeister, Designing CMDB data models with good utility and limited complexity, in: 2014 IEEE Network Operations and Management Symposium (NOMS), 2014, 1–15. doi:10.1109/NOMS.2014.6838375

[5] D. Herrick, CMDB Assessment and remediation, in: 2023 ACM SIGUCCS Annual Conference, 2023. doi:10.1145/3539811.3579551

[6] A. Keller, S. Subramanian, Best practices for deploying a CMDB in large-scale environments, 2009 IFIP/IEEE International Symposium on Integrated Network Management, 2009, 732–745. doi:10.1109/INM.2009.5188880

[7] M. Yaici, P2P-based Solution for the cloud availability, in: 2022 6th International Conference on Cloud and Big Data Computing, 2022. doi:10.1145/3555962.3555963
[8] C. Yen-Jen, W. Chen, Implementation of a high available database on virtualizing cloud platform, in: 2023 5th International Conference on Computer Communication and the Internet (ICCCI), 2023, 229–235. doi:10.1109/ICCCI59363.2023.10210178
[9] J. Almeida, et al., A Machine-Checked Proof of Security for AWS Key Management Service, in: 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019, 63–78. doi:10.1145/3319535.3354228
[10] R. Banakh, A. Piskozub, Y. Stefinko, External elements of honeypot for wireless network, in: 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science, 2016, 480–482, doi:10.1109/TCSET.2016.7452093
[11] O. Deineka, et al., Information classification framework according to SOC 2 type II, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3826, 2024, 182–189.
[12] Y. Martseniuk, et al., Shadow IT risk analysis in public cloud infrastructure, in: Cyber Security and Data Protection, vol. 3800, 2024, 22–31.
[13] O. Mykhaylova, et al., Mobile application as a critical infrastructure cyberattack surface, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II, vol. 3550 (2023) 29–43.
[14] S. Gnatyuk, et al., Method for managing IT incidents in critical information infrastructure facilities, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3826 (2024) 326–333.
[15] K. R. Muppa, Advancing cloud security with AI-enhanced AWS identity and access management, Int. Res. J. Eng. Appl. Sci. 10(1) (2022) 25–28. doi:10.55083/irjeas.2022.v10i01005
[16] O. Mykhaylova, M. Korol, R. Kyrychok, Research and analysis of issues and challenges in ensuring cyber security in cloud computing, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3826, 2024, 30–39.
[17] A. Horpenyuk, I. Opirskyy, P. Vorobets, Analysis of problems and prospects of implementation of post-quantum cryptographic algorithms, in: Classic, Quantum, and Post-Quantum Cryptography, vol. 3504, 2023, 39–49.
[18] Y. Martseniuk, et al., Universal centralized secret data management for automated public cloud provisioning, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3826, 2024, 72–81.
[19] P. Raj, Continuous integration for new service deployment and service validation script for vault, Inte. J. Sci. Res. Eng. Manag. 08 (2024) 1–5. doi:10.55041/IJSREM35565
[20] D. Drogseth, R. Sturm, D. Twing, Chapter 4. CMDB system deployment stages: An eight-step ladder to success, CMDB System Deployment Stages, 2015, 53–78. doi:10.1016/B978-0-12-801265-9.00004-4
[21] J. Wang, et al., Study on comparative performance of CL-20/RDX-based CMDB propellants, Propellants, Explosives, Pyrotechnics 44(9) (2019) 1175–1182. doi:10.1002/prep.201900029
[22] V. Petrivskyi, et al., Development of a modification of the method for constructing energy-efficient sensor networks using static and dynamic sensors, Eastern-European J. Enterp. Technol. 1.9(115) (2022) 15–23. doi:10.15587/1729-4061.2022.252988
[23] A. Keller, S. Subramanian, Best Practices for Deploying a CMDB in large-scale Environments, in: 2009 IFIP/IEEE International Symposium on Integrated Network Management, 2009, 732–745. doi:10.1109/INM.2009.5188880
[24] S. Vasylyshyn, et al., A model of decoy system based on dynamic attributes for cybercrime investigation, Eastern-European J. Enterp. Technol. 1.9 (121) (2023) 6–20. doi:10.15587/1729-4061.2023.273363
[25] S. Enunnl, Leveraging artificial intelligence for configuration management database (CMDB) Optimization: A Comprehensive Analysis, 2024.

[26] S. Niewiadomski, G. Mzyk, ML support for conformity checks in CMDB-like databases, in: Artificial Intelligence and Soft Computing, ICAISC 2023, Lecture Notes in Computer Science, vol. 14126, 2023. doi:10.1007/978-3-031-42508-0_33
[27] S. Maes, CMDB best practices: How to successfully implement CMDB in your organization, Ifs Blog, 2023.
[28] S. Enunnl, Harnessing the synergy: Exploring the benefits of artificial intelligence and configuration management database (CMDB), 2024.
[29] Y. Martseniuk, et al., Automated conformity verification concept for cloud security, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654, 2024, 25–37.
[30] J. Yin, et al., Mechanical behaviors and failure mechanisms of CMDB propellant under wide strain rate tension loading, Phys.: Conf. Ser. 2535 (2023) 012010. doi:10.1088/1742-6596/2535/1/012010
[31] H. Wei, et al., ReaxFF molecular dynamics simulations on thermal decomposition of RDX-based CMDB propellants, J. Mol. Modeling 28 (2022). doi:10.1007/s00894-022-05377-4
[32] J. Zheng, et al., Effects of loading rate and microstructure on dynamic fracture toughness of CMDB propellant, Tuijin Jishu/J. Propuls. Technol. 36 (2015) 940–946. doi:10.13675/j.cnki.tjjs.2015.06.019
[33] O. Vakhula, I. Opirskyy, Research on security as code approach for cloud-native applications based on Kubernetes clusters, in: Cyber Security and Data Protection, vol. 3800, 2024, 58–69.
[34] T. Wang, et al., Research on a cloud model intelligent computing platform for water resource management, J. Hydroinform. 26 (2024). doi:10.2166/hydro.2024.223
[35] P. Narayanan, Engineering data pipelines using Google cloud platform, in: Data Engineering for Machine Learning Pipelines, 2024. doi:10.1007/979-8-8688-0602-5_16
[36] S. Gulati, A. Tyagi, P. Goel, Security automation and orchestration in the cloud, 2024. doi:10.4018/979-8-3693-3249-8.ch002
[37] O. Mykhaylova, T. Fedynyshyn, A. Platonenko, Hardcoded credentials in Android apps: Service exposure and category-based vulnerability analysis, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3826, 2024, 206–211.
[38] R. Bishukarma, Optimising cloud security in multi-cloud environments: A study of best practices, Technix Int. J. Eng. Res. 11 (2024) a590–a598.
[39] A. Sreerangapuri, Blockchain-enabled AI governance for scalable cloud security automation. Int. J. Comput. Eng. Technol. 15 (2024) 947–959. doi:10.5281/zenodo.13962366
[40] V. S. Thokala, Scalable cloud deployment and automation for e-commerce platforms using AWS, Heroku, and Ruby on Rails, Int. J. Adv. Res. Sci. Commun. Technol. (2023) 349–362. doi:10.48175/IJARSCT-13555A
[41] D. Soldatenko, Study of efficiency of using it-infrastructure-as-a-service for cloud computing, Syst. Technol. 2 (2022) 68–76. doi:10.34185/1562-9945-2-139-2022-07
[42] K. Suram, Innovations in infrastructure automation: Advancing IAM in cloud security, Int. J. Sci. Res. Comput. Sci. Eng. Inform. Tech. 11 (2025) 255–263. doi:10.32628/CSEIT25111223
[43] D. Narayanasamy, Transforming healthcare with secure cloud infrastructure, Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. 11 (2025) 633–644. doi:10.32628/CSEIT25111271