bmc

Thought Leadership White Paper

Unlock the Benefits of a Configuration Management Database (CMDB)

Architect an optimal CMDB to drive efficiency and service quality

Table of Contents

1 EXECUTIVE SUMMARY

2 SIX CRITERIA FOR AN EFFECTIVE CMDB

Support for Federation

Flexible Information Model Definition

Standards Compliance

Support for Built-in Policies

Auto-discovery

Strong Access Controls

4 CONCLUSION

Executive Summary

At the heart of many successful companies' IT architectures lies the configuration management database (CMDB). Acting as the index for IT services, infrastructure, and the relationships that form the complex digital enterprise that all companies are rapidly becoming, **the CMDB allows organizations to have a unified and consistent view into what makes up their IT.** The CMDB knows what services are provided to customers and what services are consumed by employees and allows IT to rapidly respond to situations that could, if not handled correctly and in a timely manner, impact their operations.

Benefits of an effective CMDB include:

- **Improving transparency** and understanding of complex IT infrastructures
- **Enabling closer collaboration** and workflows across groups
- **Allowing automation** of end-to-end processes
- **Improving service quality** and management
- **Achieving continuous compliance**

To provide high levels of integration and automation, companies need a CMDB built on an architecture that meets six important criteria:

1. Support for federation
2. Flexible information model definition
3. Standards compliance
4. Support for built-in policies
5. Auto-discovery
6. Strong access controls

This white paper provides details on these criteria so that businesses can optimize their use of a CMDB.

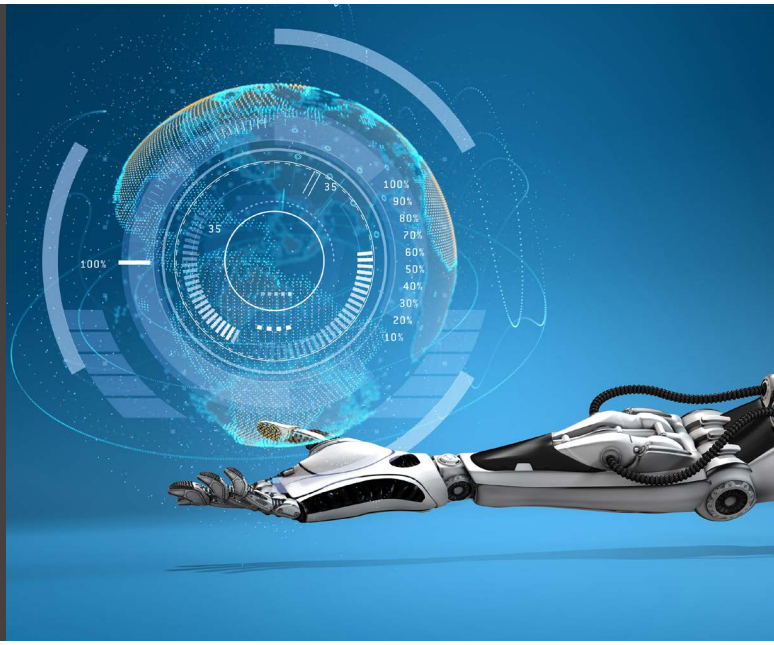
SIX CRITERIA FOR AN EFFECTIVE CMDB

A well-architected configuration management database (CMDB) provides a strong foundation for management of digital enterprises by empowering enterprise IT organizations with visibility, accountability, and control over their services infrastructure. By integrating and automating processes within and across IT service support, IT operations, and IT asset management, a well-architected CMDB can improve service quality and support compliance efforts. To achieve the highest levels of integration and automation, a CMDB's architecture should meet six criteria.

1. Support for Federation

As the central repository for data describing the IT infrastructure, the CMDB serves as a single source of reference about the IT environment. But consolidating all infrastructure information in a single database is just not feasible: there are too many infrastructure types, elements, types of management data, and varying granularity levels per data type.

The CMDB enables integration and automation of processes within and across IT service support, IT operations, and IT asset management.



The most practical solution is to unite a collection of CMDBs and other data stores into what ITIL® refers to as a configuration management system (CMS). Individual CMDB instances—that is, data stores that specialize in management functions along various boundaries of IT infrastructure and operations management—collectively contribute to an enterprise CMDB.

The ability to unite several data stores requires a federated approach that must be designed into the enterprise CMDB architecture. It cannot be added as an afterthought. A CMDB built on a federated architecture provides access to a wide range of information without the need to move all the data to the CMDB or replicate it. For this approach to work, the data stores must segment their contributory slices of the enterprise CMDB along well-defined lines. These lines of delineation must satisfy requirements for data exchange, data integrity, and data access.

For example, at a retailer of women's apparel, the CMDB stores fundamental information about the IT environment and provides pointers to other essential and more-detailed information in other data stores. Configuration item (CI) relationship and management information allows the staff to tie assets to incidents and problems, correlate incidents, and perform root cause analysis. Through federation, the CMDB provides access to information the staff needs to manage asset lifecycles more effectively, helping to ensure that the company ceases paying for support and maintenance on assets that have been retired.

A critical requirement for federation is a strong data reconciliation capability. By ensuring that data aggregated from multiple sources is accurate and consistent, data reconciliation eliminates duplicates so that there is only one configuration item for each entity. It also ensures that data aggregated from multiple sources is attached to the correct configuration item.

2. Flexible Information Model Definition

Information models for a CMDB can be based on two distinct approaches. The top-down approach takes a desired view of an organization and implements a metadata model for that view in the CMDB. It follows up by ensuring that all management applications comply with the metadata model. The bottom-up approach relies on normalizing lower-level data sets to develop a metadata model.

Most IT organizations opt for the bottom-up approach because it allows existing management data sets to be rolled up into metadata models easily, reducing implementation effort and speeding time to value. The resulting metadata models are agnostic regarding management function and application. Consequently, they are easier to manipulate than actual lower-level data sets that are tied to specific management functions driven by specific applications. The bottom-up approach also has the advantage of easier acceptance because it can be implemented without the disruptive organizational and cultural changes required for top-down approaches. However, **a well-architected CMDB supports both approaches, giving IT flexibility to implement a CMDB that best matches its requirements.**

> Gartner has seen an increase of successful CMDB implementations in up to 40% of midsize enterprises and more than 75% of large enterprises.
>
> Source: IT Market Clock for ITSM 2.0, 2015, 21 August 2015

3. Standards Compliance

Federation implies multiple CMDB instances and, therefore, multiple data segments. Interoperability among instances and segments is a must. Interoperability requires standardized data exchange mechanisms to ensure data integrity, protection, and controlled access. Consequently, **the CMDB architecture must support open standards** such as XML and service-oriented architecture principles for web services. Compliance with standards allows disparate data stores to interoperate, while ensuring data sets do not violate the overall integrity of the metadata definitions that the IT organization has developed for its enterprise CMDB.

4. Support for Built-in Policies

A well-architected CMDB maintains policies that document the standards used to build, update, enforce, and track continuous compliance for a given service and its supporting components. A service might encompass an application, middleware, system utilities, databases, network devices, and an operating system. Supporting infrastructure components might include web servers, database servers, application servers, network devices, and clients.

Standards must include details on data sets, such as configuration, installation, performance, and uptime. Policies may change depending upon factors such as time, number of users, and service level agreements (SLAs).

A well-architected CMDB also maintains process models. Because the IT environment typically changes over time, these process models must be dynamic and adapt automatically to those changes.

Because it maintains policies and process models, **the CMDB plays a pivotal role in policy-based process automation.** This automation greatly speeds process execution while enforcing the use of process best practices. For example, an infrastructure services provider focused on card-based payment transaction services, electronic payment systems, and international financial information credits its CMDB with enabling IT to execute all active and proactive processes—such as release, change, and SLA management—at an extremely high level of quality in a very short timeframe and with exceptional performance.

The CMDB acts as a consolidated store of auto-discovered data to provide more transparent understanding of infrastructure, components, and the services they support

5. Auto-discovery

For successful implementation, a CMDB must support the ability to be not only populated by auto-discovery tools but also manage the data within it in a way that allows for handling of multiple discovery sources. Simply allowing a tool to populate data is not sufficient as the underlying management architecture must support population, normalization, and reconciliation of data before publishing and consumption of it within day to day operations. **The ever increasing complexity, scale, and agility of today's IT infrastructure means that manual data population and maintenance is simply impractical and can damage IT's ability to respond to impacting situations.**

For example, CARFAX, the leading provider of vehicle history information, relies on automated tools to discover configuration items in the IT environment and feed them into the CMDB. The tools also capture the logical dependency mapping of components, identifying which IT components comprise enterprise applications.

Traditionally, IT has used auto-discovery to rapidly populate inventories with information. The latest generation of auto-discovery solutions also periodically scans the IT environment to provide live configuration insight into a given component at different time points. Live discovery combined with time series snapshots are vital to any analysis performed on components and the services they support.

6. Strong Access Controls

In the IT world, unauthorized or undesired access and system changes can result in service disruptions or downtime. Consequently, security and access controls play an essential role in CMDB design and implementation. Access policies can be used to create profiles and access controls for users and groups.

A CMDB must conform to security standards to prevent implementation of any unauthorized changes to its data set. These standards can be documented through directories to identify who has access to specific data sets and who is authorized to perform actions on different data sets. A CMDB with built-in, role-based access control supports user authentication through directories to claim access rights.

CONCLUSION

A well-architected CMDB can empower IT organizations with visibility, accountability, and control over their services infrastructure. When combined with discovery and decision-support applications, the CMDB provides the foundation for a holistic platform that automates the configuration management of services while ensuring continuous compliance with corporate policies, government regulations, and industry standards and best practices.

FOR MORE INFORMATION

To learn more about the attributes and benefits of a well-architected CMDB, visit **bmc.com/cmdb**

BMC is a global leader in software solutions that help IT transform traditional businesses into digital enterprises for the ultimate competitive advantage. Our Digital Enterprise Management set of IT solutions is designed to make digital business fast, seamless, and optimized. From mainframe to mobile to cloud and beyond, we pair high-speed digital innovation with robust IT industrialization—allowing our customers to provide intuitive user experiences with optimized performance, cost, compliance, and productivity. BMC solutions serve more than 15,000 customers worldwide including 82 percent of the Fortune 500®.

BMC – Bring IT to Life

bmc

471574