ENHANCE BUSINESS AGILITY AND COMPETITIVENESS WITH A HEALTHY CONFIGURATION MANAGEMENT DATABASE

Abstract

With IT and business being constantly aligned, organizations need to be conscious of how IT components operate. For instance, the configuration management database (CMDB) stores information about an organization's key infrastructure components that are also known as configuration items (CIs). This CMDB has strong relationships with ITSM processes like incident management, problem management, change management, and service request management. Since CMDB is at the heart of all IT operational activities, it is vital for businesses to ensure that the CMDB always contains updated, accurate and complete data. This paper examines the importance of a healthy CMDB and the factors that determine CMDB health. It also explains how CMDB health can be monitored and tracked using ServiceNow along with the salient benefits arising from a healthy CMDB.

Infosys®
Navigate your next

Introduction

The configuration management database (CMDB) is a database that stores information about all the configuration items (CIs) and the relationship between various CIs. CIs refer to all the infrastructure elements and service components that are vital for an organization's business operations like servers, network devices, software applications, business services, etc. The CMDB is governed by the configuration management process. Together, configuration management and the CMDB act as the foundation of integrated IT service management (ITSM) processes.

The first step to maximize the effectiveness of a CMDB is to populate it with data that is as complete and accurate as possible. This can be done using automated or manual methods or a combination of both. Automated data population is done by integrating the CMDB with discovery tools or data sources. Manual methods involve gathering the configuration item (CI) data maintained in spreadsheets, databases, etc., and loading this into the CMDB in the correct format. Accurately populating the details of all CIs and their relationships enhances the ability of the CMDB to support multiple IT-related processes like ITSM, IT operations management, IT asset management, and IT security management as well as non-IT processes like HR service management.

Configuration managers and key stakeholders should understand that ongoing efforts are needed to ensure that the CMDB remains relevant. However, populating the CMDB with complete and accurate data is merely the first step. In today's dynamic IT environment, where infrastructure changes occur frequently, it is critical to ensure that CI data and relationships are updated in sync with these changes. Without this, organizations will be unable to fully realize the benefits of the CMDB. Some examples of issues that can diminish these benefits are the presence of duplicate CIs, outdated CI relationships, retired CIs still marked as active in the CMDB, etc. Thus, regular monitoring and tracking of the health of the CMDB is critical to ensure that the data contained in the CMDB is precise and relevant. This will ensure that IT and other departments can use it more effectively to perform their tasks.

Business challenges affecting CMDB health

The biggest roadblock for an organization's CMDB program is the lack of executive support. Since the CMDB needs to capture data for different types of infrastructure items and business services, cooperation from different stakeholders is vital for smooth implementation and maintenance of the CMDB. Stakeholders who manage different processes or types of configuration items typically belong to various departments and locations. Each stakeholder will also have different expectations from the CMDB implementation. Hence, executive buy-in is necessary to get all these stakeholders to cooperate effectively on an ongoing basis. Consequently, this also ensures that the primary goals of a CMDB program aligns with the organization's overall strategic goals.

Maintaining CMDB data and keeping it updated and relevant is another challenge. In most large organizations, the volume of data to be captured in the CMDB is huge. With increasingly frequent infrastructure changes in the IT environment, significant effort is needed to accurately maintain these voluminous CMDB datasets. Some of the other challenges faced by configuration managers include identifying and capturing unknown CIs, tackling poor quality data and zeroing in on the actions required to rectify poorly defined CI relationships.

Large data volumes and constant infrastructure changes increase the probability of outdated and redundant CIs in the CMDB. This compromises the effectiveness of the CMDB and leads to loss of trust among the user community. Considering the importance of accurate and faster updates, an automated solution is the need of the hour to address the above challenges. Such a solution should be able to track and monitor the CMDB health in a manner such that any CI data or relationship-related issue is clearly identified and speedily rectified.

Measuring, monitoring and tracking CMDB health

The first step is to set up a CMDB health dashboard. This will help gain a single view of CI data quality and relationships. Infosys recommends ServiceNow as the CMDB tool due to the platform's strong ITSM capabilities and its ability to manage several IT and non-IT processes like IT operations management, IT business management, IT asset management, customer service management, HR service management, and more. Further, ServiceNow Discovery automates the discovery of configuration items. Although the CMDB health dashboard feature is available even without purchasing ServiceNow Discovery, its implementation enhances the CMDB and its health dashboard functionalities.

ServiceNow's CMDB health dashboard facilitates continuous monitoring and tracking of CMDB data. The dashboard is accessible through the 'CMDB view' menu on the ServiceNow CMDB dashboard module. The dashboard consists of three tabs named 'CMDB health', 'Relationship health' and 'CMDB health dashboard jobs'.

CMDB health tab

This contains a scorecard that depicts the CMDB health based on three parameters – completeness, compliance and correctness. These are further described below:

1. CMDB completeness scorecard

This displays the percentage of data completeness as well as the number of CIs where recommended and required attributes are missing. Required attributes are those that are considered mandatory for a CI class (like host name and server IP address). Though recommended attributes are not mandatory, having such data available helps IT operational teams be better equipped to handle an incident, change or any activity related to a CI. For instance, some recommended attributes that are not mandatory but good to have in an organization might include the operating system details of a server,

location of a printer or a network device, the number of users of an application, etc. The completeness score is calculated as a combination of 'recommended' and 'required' sub-metrics after considering the weightage assigned to each sub-metric.

An important point to note is that the numbers mentioned against recommended and required attributes are only based on the number of CIs that are missing those attributes. It is not the sum of the total number of recommended and required attributes missing across all the CIs. For example, if one CI has 5 missing required attributes, another CI has 3 missing required attributes and yet another CI has only 1 missing required attribute, the number displayed against the required attributes will be 3. The completeness percentage helps identify key gaps in CI attributes so that configuration managers can take appropriate actions to close the gaps and make the CI data more complete.

2. CMDB compliance scorecard

This displays the CMDB audit status after comparing the CIs against pre-defined audit parameters. It displays information like the list of audit failures as well as the trends of failed and compliant CIs. Say an organization has defined an audit parameter whereby antivirus software must be present on all computers. After running the audit, the list of CIs with audit failures in the compliance scorecard will include all the computers lacking an antivirus. Similarly, this list will also display all the CIs that do not meet the criteria for the defined audit parameters.

The definition of suitable audit criteria as per the organization's requirements and the periodic monitoring of compliance scorecard will help configuration managers take necessary actions to improve the compliance of CIs. This, in turn, will reduce the risk of compliance and its associated impact like security, financial, business continuity, and legal risks.

3. CMDB correctness scorecard

This scorecard indicates the correctness of the CI data by displaying the percentage of CIs that meet the correctness criteria. There are three types of CIs that adversely impact the correctness score. These are:

- **Duplicate CIs:** Since CMDB data is typically imported from multiple sources, sometimes manually, there is always a high possibility of duplicate CIs. This can happen due to various reasons like differences in naming conventions used by multiple discovery sources, manual errors during data import, etc.

- **Orphan CIs:** A CI is flagged as an orphan CI when it does not have a desired relationship with another CI. The orphan rule can be set based on the CI class. All the CIs in that class that meet the criteria specified by the rule are considered as orphans. For example, a rule can be set for an application CI to be considered as an orphan if it does not have a relationship with server CIs. However, within a particular CI class, criteria can be set to override the rules in certain scenarios. It is important to note that there are no baseline orphan rules.

- **Stale CIs:** These are CIs that are suspected to no longer be part of the infrastructure even though they are still present in the CMDB. As per the baseline staleness rule applied to the CMDB base table, all CIs that have not had any updates over the past 60 days are considered stale. Configuration managers can create their own staleness rule by defining an appropriate effective duration after which a CI is considered stale. Multiple staleness rules can be created with different durations for different CI classes.

The total correctness percentage is calculated based on the numbers of duplicate, orphan and stale CIs and the weightage assigned to each of these CIs. The CMDB correctness data enables configuration managers to take actions to improve the CI data quality and accuracy. This will result in availability of more trustworthy data for service desk agents, IT service managers, IT operation managers, etc.

Relationship health tab

This tab indicates the health status for CMDB relationships and displays the details of duplicate, orphan and stale relationships. Orphan relationships are those that are missing a parent or a child CI. Duplicate relationships are those that have an identical parent, child and relationship type CI. Stale relationships are those that include a stale CI. Any relationship that consists of one or more stale CIs will be considered as a stale relationship. By monitoring and tracking CI relationship health, configuration managers can quickly resolve CI relationship data issues. This makes CI relationship mapping more reliable and useful for key IT operational activities like impact analysis during incident management and problem management.

CMDB health dashboard jobs tab

This consists of jobs that validate the CMDB data against metrics defined in the system to calculate the CMDB health status. The dashboard consists of the following 5 jobs.

- CMDB health dashboard - Correctness score calculation

- CMDB health dashboard - Completeness score calculation

- CMDB health dashboard - Compliance score calculation

- CMDB health dashboard - Relationship score calculation

- CMDB health dashboard - Relationship compliance processor

These five jobs must be activated for the health scores to be properly displayed and updated in the dashboard. Each of these jobs can be marked as active from the CMDB health dashboard jobs tab. For each job, there is an option to specify the frequency of running the job (daily, weekly, monthly, etc.) and the time at which the job must be run. A best practice is to schedule all these jobs to run just after the discovery job so that it validates the CMDB health based on the latest data.

Infosys recommends scheduling the CMDB health dashboard jobs to run a few hours after midnight. Say the discovery job is scheduled to run daily at midnight. These jobs also have a 'conditional' checkbox. If this checkbox is selected, a text box will appear where one can specify a scripted condition. The job will run only if the condition is met. It is also possible to manually execute these jobs if there is a need to check the latest CMDB health status on an ad hoc basis.

Configuring the CMDB health metrics

1. Configuring scope of health tracking

As the volume of data in the CMDB is usually very high, it may not be possible to always monitor the health of every single CI. Organizations with large CMDBs should ideally limit health tracking to the most critical CIs or to those CIs that are expected to undergo changes frequently. Similarly, health tracking can be limited to certain types of health metrics, if required.

The CI class manager module in ServiceNow contains a section called health inclusion rules. This specifies the list of CI classes for which health metrics must be tracked, list of health metrics that are applicable to a CI class and the criteria that CIs must meet to be considered for calculation of the health metrics.

2. Configuring metric criteria and thresholds

The CI class manager has provisions to configure the criteria and thresholds for the metrics. These metrics and thresholds can be configured globally for the whole CMDB or separately for specific CI classes. Some examples of what can be configured are given below.

- Select the list of fields that need to be considered as the recommended fields for a CI class as part of determining the completeness health metric score

- Define the criteria for a CI to be considered as an orphan CI or stale CI. This is needed for the correctness health metric score

- Define the audit criteria to be used as part of the compliance health metric calculation

- Set the threshold values at which the health score of various metrics/sub-metrics will be considered as 'best', 'at risk' and 'critical'.

3. Configuring CMDB health metrics aggregation preferences

The CMDB health score is calculated based on the aggregation scores of completeness, correctness and compliance KPIs. The correctness score is based on the percentage values of orphan, stale and duplicate CIs. Completeness is based on the percentage of required and recommended CIs. The compliance score is based on actual audit results. The weightage of each KPI involved in these calculations can be defined manually using the 'Health Preference' module in ServiceNow.

For example, the weighted average values for completeness, compliance and correctness metrics can be modified based on the preferred weightage given for each metric during the calculation of overall health score. For the completeness metric, there are options to modify the weighted average values for recommended and required sub-metrics as per the organization's requirement. Similarly, for the correctness metric, the weighted average values for duplicate, orphan and staleness sub-metrics can be modified. The 'select metric' field also provides an option to activate or deactivate metrics.

For all sub-metrics (recommended, duplicate, etc.), there is option to set a failure threshold. When the number of CIs that fail the tests for a sub-metric is equal to the value of the failure threshold for that metric, the CMDB health tab will cease processing values for that sub-metric in the current cycle. This means that there will be no aggregated health score for that particular metric. Further, the processing status of the parent metric will be marked as 'incomplete' and processing will be attempted again in the next cycle.

For example, if the failure threshold is set as 1000 for duplicate CIs, then the CMDB health calculation job will stop processing for duplicate CIs if there are more than 1000 CIs which are identified as duplicate. As a result, the health calculation for correctness score (the parent metric) will also be marked as incomplete.

Benefits of a healthy CMDB

The presence of a mature CMDB helps users and IT stakeholders view all the key attributes of a configuration item like serial numbers, location, allocated users, IP addresses, etc. It also denotes how a configuration item is related to other configuration items in the organization's environment. This information can enhance the efficiency of ITSM processes like incident and change management by enabling detailed impact analysis of the particular CI. Thus, change managers can plan their changes better with minimal disruption while incident management teams can minimize damage and troubleshoot the root cause of an issue faster.

The ServiceNow Service Mapping tool maps the discovered configuration items to their related business services. This helps identify those business areas that will be affected by any event. Such visibility into the details of the technology that

underpins various business services will drive strategic business decision-making based on technology investments.

In the case of IT operations management, a robust and healthy CMDB can facilitate easier identification of anomalies as well as business services that are impacted by events. The CMDB also acts as a foundation for the IT asset management process by synchronizing asset status based on configuration changes made to a particular asset. Data consistency provided by a mature CMDB will lead to improved compliance and reduced penalties. CMDB can even provide invaluable supporting data for non-IT functions like HR service management and customer service management.

Monitoring, tracking and maintaining an accurate and complete CMDB is critical to maximizing the benefits. A well-defined CMDB health dashboard can help achieve

this. The CMDB health dashboard also displays whether the CMDB health is improving or worsening. Such trends aid in identifying whether the organization is going in the right direction with their CMDB efforts. It also helps uncover what improvements are needed in CMDB operational activities and configuration management processes. Another key benefit of tracking and managing CMDB health using the dashboard is increased employee productivity. This is brought on through reduced man hours spent by IT staff to resolve incidents, manage changes, etc. as well as reduced effort spent to manage the CMDB on an ongoing basis.

In short, the presence of a healthy CMDB enables organizations to focus better on their core business operational activities. It helps them become agile at managing any events in their infrastructure and frees up resources to focus on strategic activities.

Conclusion

While a healthy and accurate CMDB is essential for business and IT operations, this typically involves significant manual effort and time owing to large data volumes. Automated solutions like ServiceNow are a fitting choice to minimize errors, effort and negative impact of incomplete, outdated and inaccurate CMDBs. ServiceNow provides discovery and service mapping tools to uncover configuration items and map these to the relevant business services. This ensures that CMDB data is current and updated. ServiceNow also includes a CMDB health dashboard and scorecards with various metrics that provide ongoing visibility into the comprehensive CMDB health. This helps configuration managers easily pinpoint issues and resolve these to maintain the health of the CMDB. A well-maintained CMDB boosts stakeholder trust in the quality of CMDB data and the accuracy of relationships of CIs with other CIs and underlying business services. It also promotes informed business decision-making regarding infrastructure upgrades, acquisitions, staffing, etc. Continuous efforts in tracking and maintaining CMDB health can assist organizations in becoming more agile and productive while focusing on core business activities.

About the Authors

John Daley
Principal Consultant, Infosys

John Daley is an IT Professional who has managed IT Operations and Service Delivery for over 25 years. He has deployed ServiceNow a dozen times, including for a fortune 5 financial audit company.

Ashok Sasidharan
Consultant, Infosys

Ashok Sasidharan is an IT consultant with 9+ years of IT experience and is specialized in the areas of Configuration Management and IT Asset Management. He has successfully carried out end to end implementations of CMDB and asset management (both hardware & software) on ServiceNow.

For more information, contact askus@infosys.com

Infosys®
Navigate your next

Infosys.com | NYSE: INFY

Stay Connected