Configuration management processes can mitigate risks and enable operational agility. IT operations leaders must standardize configuration management processes across all domains, choose the right configuration management tools, and improve alignment with change management and other processes.

**Key Challenges**

- Gartner believes that more than 80% of all mission-critical IT service outages result from people and process errors and failures, and of those outages, more than 50% result from a lack of coordination between change, release and configuration management processes.
- Most IT organizations are using a variety of configuration management tools to address pain points in different domains or for different problems, which creates room for risk.
- Without standardized configuration management processes, IT operations will not be able to achieve compliance or enable agility.

**Recommendations**

IT operations leaders should:

- Assess the current state of the configuration management processes.
- Assess configuration management tools across all IT operations domains.
- Document the configuration management processes and complexity.
- Look for appropriate opportunities to automate configuration management.
- Repeat this review annually to uncover new opportunities for standardization, consolidation and optimization.
Strategic Planning Assumption(s)

Through 2018, 75% of IT organizations will fail in their configuration management efforts due to lack of standardization.

Through 2018, 90% of IT organizations will be forced to deploy multiple, overlapping configuration management tools.

Introduction

Configuration management processes support the successful execution of other IT operations processes. These processes mitigate the risk of disruption and service outages such as change, release and incident management (see Note 1). But like any process, poor design or mismanagement introduces risk. Gartner believes that more than 80% of all mission-critical IT service outages result from people and process errors and failures, and of those outages, more than 50% result from a lack of coordination between change, release and configuration management processes. In environments with virtualization and cloud technology, configuration management has a direct impact on additional processes, including performance management (see "Configuration and Performance Management Useful for Virtualization, Required for Cloud").
Most IT organizations use a variety of configuration management tools and processes that have been implemented to address pain points in different domains or for different problems even within one domain. Using multiple tools increases costs, which creates room for risk. Variations in maturity of use of the tools or the ability to use them accurately can make configuration management processes fall out of step with other critical IT operations processes.

Analysis

Step 1: Assign a Configuration Manager

The first step in ensuring you have a focus on configuration management (both process and tools) is to assign a dedicated resource for configuration management with goals (e.g., long-term direction) and SMART objectives (tactical execution; see "Improving Service with SMART Objectives in I&O"). This role may be dedicated or may be a shared role with a change manager. A configuration manager will need to facilitate cross-organizational alignment and establish process definition. This person often takes a leadership role for the follow-up configuration management database (CMDB) initiative as well.

The configuration manager must have:

- A solid understanding of the business and IT operations
- Strong communication skills
- Background in one or more configuration management domains
- Process skills
- Credibility with management and the technical community

The configuration manager will need to work with a virtual team of people from different domains who may not work well together. Typically, the configuration manager is a peer of the change manager and will often assume responsibility for release management, especially for Web application support. Ideally, the configuration manager and change manager will report to the IT operations group, which is often a part of the IT service and support. In larger IT organizations, there are often dedicated resources for process ownership, but in small and midsize organizations the configuration manager and other process owners are frequently assigned to an established manager, often a server team manager.

Recommendation:

Dedicate a resource to configuration management or establish a shared role with the change manager. A newly assigned configuration manager should start small with a pilot project. However, because configuration management reaches across IT domains, it is necessary to include stakeholders from each domain and business unit to participate in and buy into all process
discussions, especially defining requirements for the CMDB — even if the CMDB project starts narrower and doesn’t include every domain.

Step 2: Enforce Standards With Configuration Management to Gain Efficiencies and Reduce Cost

Standardization is the most important precursor to successful, cost-effective automation, but particularly critical to configuration automation. Tools are efficient and effective if used with an infrastructure based on standards and policies. Without the necessary focus on building standards throughout your infrastructure, configuration management tools will not provide the payback they promise.

Likely the enterprise architecture team has established a set of systems and application design standards. Over time, drift occurs. It is critical to understand the gaps and re-evaluate the standards. By putting architectural infrastructure and application standards in place, you also improve the ability to keep pace with the high rate of change that so many IT organizations are experiencing. With standards, deployment and maintenance of infrastructure components and IT services are more reliable and repeatable.

Configuration management tools do not create standards, but they can enable the tracking and enforcing of standards. If used correctly, configuration management tools can often help to reduce the costs associated with "touching every system for every change."

Without standards, configuration management tools can’t deliver the payback or efficiencies that come from leveraging common tasks across similar systems. Likewise, standards without a means of enforcement and auditability will not return business value; therefore, standards require governance and executive sponsorship. However, creating standards does not imply one of anything or everything. Managing diversity requires planning and an understanding of system and application providers, as well as internal development strategies. Reducing complexity through standards and policies will be an evolution, and will require configuration change and release tools and processes to enforce the policies and address changing business needs (see "Best Practices for Implementing Automation in Data Centers With Cloud and Virtualized Environments").

Recommendations:

Work with the enterprise architecture team to assess current standards and gaps in what "should be" to what is deployed and configured. (Re) establish system and application standards. Look for ways that configuration processes and tools can be used to enable and enforce standard configurations.


First, assess the currently active approaches to configuration management (both manual and automated) in all of the domains of the IT operations organization. As you complete this step, be aware of the following issues that you may encounter along the way. For example, you may find that many of the configuration management processes are not formalized or documented; take steps to
uncover tribal knowledge. You may find processes that are running with scripts, as well as by brute force (people only) or efficiently with tools. Each domain is likely to have a different level of process maturity and, even within a given domain, there may be multiple tools with different levels of process maturity associated with them and different levels of successful adoption. This can occur because of individual platform focus or because of decentralization of tool adoption. Document your findings so you can take them into consideration as you build a plan.

Gartner outlines key steps for creating a basic configuration management process (see Note 2). As you review each domain, gather context about how these steps were addressed.

**Step 3a: Document Your Processes**

Some organizations use ITIL as a framework for configuration management, though most organizations customize the guidelines to meet their own needs (see Note 3). Don't assume that a domain is following ITIL guidelines to the letter; be sure to review the real-world practices.

The configuration manager should document processes in all IT domains, rationalizing each process to establish common process steps. Each domain will have unique process requirements, but an overall understanding is critical to determine change windows and discovery updates that impact the CMDB. Without a centralized configuration process owner, duplication, variation and inefficiencies will remain. Although tools do not map directly to processes (and are often "gap fillers"), once defined, the process can be used to ensure that tools are being used efficiently or that they meet process requirements. The configuration manager should define standard configuration management processes and tailor them for domain-specific requirements while still being consistent about how they might support a CMDB.

During this time, configuration stakeholders can discuss how each domain can contribute to the configuration process as a part of the CMDB initiative. At this time, they should map configuration item (CI) semantics to an IT or a business service for the CMDB and for reconciliation (see "Seven Steps to Select Configuration Item Data and Develop a CMDB Project That Delivers Business Value"). This will help determine which CIs are most relevant for their areas, and which would be critical for an IT service view.

*Recommendation:*

Discover, document and record all configuration processes throughout various domains, but recognize that there will be great variability in maturity, use of automation and rigor and documentation.

**Step 3b: Assess Current Configuration Management Tools**

Many IT organizations have purchased a wide variety of configuration management tools to address specific pain points (e.g., patching tools for a failed audit) across the entire configuration life cycle. The primary life cycle functions are listed below, although depending on the domain and the tool, some tools have additional capabilities (e.g., client management tools often also include support for PC remote control):
Maturity plays a significant role in the adoption and success of configuration management tools. Less mature organizations address configuration management manually (e.g., having people touch the systems to make configuration changes). As maturity increases, organizations begin to automate various configuration management functions, often with homegrown tools leveraging scripts, where mature organizations marry process controls with configuration management tools that address two or more functions within a single tool.

Assess your tool portfolios to determine the continued value and opportunities for tool consolidation without too much trade-off in functionality. Having a best-of-breed tool without the appropriate process definition and staffing maturity will result in a failed implementation.

No single vendor offers a single, integrated, comprehensive (life cycle) configuration management tool for all domains (e.g., server, client, network) and all functional needs. Most vendors have acquired their configuration management tools over time, and thus have separate tools for each domain, making it impossible to use one configuration automation tool to address all domain needs.

While many consider a CMDB to be a configuration management tool, it is not. It is not an active configuration management tool; it is a repository with specialized functionality to centralize and consolidate configuration management data that comes from other sources to establish a trusted source for IT service views.

Recommendations:

Inventory the tools that are being used currently and assess the value that they are delivering. Keep track of all tools being used and the functions that they should be addressing. Look for opportunities for consolidation. Reassess yearly or as new projects arise. Once new processes and goals are established, it will be critical to ensure that tools currently being used will deliver value going forward as well.

Step 4: Choose the Right Types of Configuration Automation Tools for the Job

The configuration management process includes the tasks of identification and maintenance of various infrastructure components. For these tasks, configuration management tools provide the capability to discover and track changes against policies, baselines or models. This is the most common feature across all configuration management tools, and for some platforms (e.g., Windows) a single tool is used across multiple domains (e.g., desktops, laptops and servers). However, the full range of some configuration management tools can extend much more broadly and address the full life cycle (as described above).
As you consider automation tools for your configuration management processes, you must account for variables that affect their implementation and performance. These variables include:

- Tools that address one or two functions in the life cycle are typically best-of-breed, but cannot be extended to address the complete life cycle.
- Conversely, tools that address the complete life cycle but only for one platform (e.g., Windows) typically do not have parity of functionality for other platforms (e.g., Mac, Linux, Unix).
- Because some projects will require cross-domain configuration automation (e.g., data center or cloud environments), recognize that no one vendor can provide a single tool for all requirements. If they offer one tool, it is most likely the combination or culmination of multiple tools from their portfolio tied together through integration or IT process automation functionality (see "Know the IT Process Automation Vendor Landscape to Shortlist the Best Vendors for Your Organization").

In some scenarios, tools (and the buyer requirements) span several domains (e.g., network, server, storage). This is sometimes referred to as data center automation or, for cloud environments, cloud automation. Although automating across multiple domains is definitely a goal for IT organizations as they become IT service-aligned, no tools can automate configuration both across the infrastructure (server, network, storage and network) horizontally, as well as throughout the entire stack vertically (e.g., application, middleware, database). There are tools that can do this essentially for a single function (e.g., spanning multiple domains from a configuration perspective for compliance dashboarding, repurposing a shared infrastructure and dynamically adding capacity, such as cloud implementations; see Note 4).

Large IT operation management vendors (e.g., BMC Software, CA, HP and IBM) offer configuration management tools for each domain, but there is little or no integration among the domain-specific tools, because each was acquired and has its own architecture and graphical user interface. More importantly, each domain has different configuration management requirements (see Figure 1).
Through 2018, 90% of IT organizations will be forced to deploy multiple, overlapping configuration management tools. Based on our client interactions for the last five years, most organizations that do not build a comprehensive requirements list of current and future configuration management needs will end up with a minimum of two tools and as many as four tools to address multiple platforms and functions across the complete life cycle.

The large majority of IT organizations initially evaluate one to two functions in the scope of the configuration life cycle (e.g., patch and configuration or provisioning and configuration). Often, within 6 to 12 months, additional functionality is required. This leads to adding tools, unless a more comprehensive tool evaluation is done upfront to ensure that the tool can address the complete life cycle. One exception to this practice is client management, which is a mature discipline and there is an expectation and understanding that tool acquisition is intended to address the complete life cycle.

Note: The vendors listed represent a sampling, which is not intended to be an exhaustive listing.

Source: Gartner (October 2013)
Recommendation:

Plan for the complete configuration management life cycle and, even if immediate requirements or projects are narrowly scoped, include broader requirements in vendor evaluations. Some projects will require cross-domain configuration automation. Bring stakeholders and requirements together to develop comprehensive RFPs and proof-of-concept scenarios. Recognize that no one vendor offers a single tool to automate the entire configuration life cycle across all domains.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Cloud Management Platform Vendor Landscape"

"Magic Quadrant for Client Management Tools"

"Best Practices for Implementing Automation in Data Centers with Cloud and Virtualized Environments"

"Midsize Enterprises Should Use These Considerations to Select Server Provisioning and Configuration Tools"

"Cool Vendors in DevOps, 2013"

"Take a Four-Step Network Configuration and Change Management Approach to Stem Disasters"

Evidence

This research draws on 10 years of over 7,000 client interactions (inquiries and conference surveys) on the topic of configuration management, between 2003 to 2013.

Note 1 The Relationship Between Configuration Management and Change Management

As a starting point, we recommend closely engineering configuration management processes and change management.

- Change management is the process for governing changes in the production environment by defining who, when and what can be changed.

- Configuration management is the process for maintaining a complete and accurate picture of all of the elements of the IT infrastructure, including networking, storage, software, applications and systems.

- Configuration is the active process of executing the required type of change, such as discover, patch, provision or audit.
Configuration without change (or vice versa) solves only half of the problem. Without governance provided by change management, the integrity and accuracy of the data will suffer. For instance, improving the accuracy of patching, without the approvals of who should be doing the patching — or, even more importantly, to what systems and when — often causes outages. In this example, configuration tools and processes would improve the accuracy of patch deployment and installation.

**Note 2 Configuration Management Basics**

We have outlined how to begin your configuration process. Key steps include:

- Assign a configuration manager
- Form a configuration management team
- Define goals and milestones
- Define the process (including governance and policies)
- Set metrics and measure progress
- Ensure continuous improvement
- Start a CMDB project

**Note 3 Using ITIL in Configuration Management**

ITIL offers the following definition of v.3 Service Asset and Configuration: Identify, control, record, report, audit and verify service assets and configuration items, including versions, baselines, constituent components, their attributes, and relationships

Many IT organizations have leveraged the IT Infrastructure Library (ITIL) for their process re-engineering efforts. However, although ITIL provides some process guidance, it often is not a perfect match with an enterprise’s specific or unique requirements, especially for configuration management. ITIL has offered definitions of the configuration management process and has adjusted them during the past 10 years. Some organizations will combine ITIL with other frameworks, such as Capability Maturity Model Integration others will use it as a base guideline, and add their own process controls and definitions.

Although some vendors claim ITIL alignment or certification, ITIL is a process framework and is not prescriptive for how to automate processes.

**Note 4 Configuration Management Functional Categories for Domains Used in Gartner Research**

Server provisioning and configuration management includes:

- Initial provisioning and configuration management
- Application provisioning and configuration management (including patch management)
- Configuration modeling, audit and compliance, and remediation
- Repurposing servers (the orchestration of tasks necessary for server reprovisioning)

Client management includes:

- Inventory
- Software distribution
- OS deployment
- Patch
- Application virtualization
- License management

Network configuration and change management; includes:

- Capturing network device configuration files
- Detecting and auditing configuration changes
- Making configuration changes to network devices

Some vendors provide the initial provisioning of a network device (that is, a bare metal install), an automation wizard to guide the user through changes to network devices and to automatically generate the resulting configuration commands, compare network device configurations to the policy or "gold standard" for that device, automatically remediate devices back to policy compliance, and provide out-of-the-box compliance reporting.

Virtual configuration management includes:

- Provision
- Image
- Discovery
- Audit
- Patch
- Snapshotting
- Reclamation

Cloud management platforms include:

- Service catalog
- Self-service request portal
- Service provisioning and configuration management
Depending on the vendor, other functions are also included, such as orchestration, capacity management, chargeback, etc.
GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp