Top Seven Considerations for Configuration Management for Virtual and Cloud Infrastructures

Gartner RAS Core Research Note G00208328, Ronni J. Colville, George Spafford, 27 October 2010, RA6 05012011

Configuration management is a key process for any IT endeavor - including legacy IT systems, as well as private and public clouds or any combination thereof. Without visibility to the configuration of the relevant IT service, IT will not be able to manage the multisourced cloud infrastructure and software.

Key Findings

- Cloud implementations have demonstrated that establishing standards to support improved quality of service is crucial for success.
- Configuration management is the process that provides information and mechanisms for provisioning, discovering and maintaining IT services.
- As the number of providers/stakeholders increases, the need to exchange accurate timely information increases.

Recommendations

- Organizations adopting virtualization and cloud delivery services need to review their configuration management processes to ensure that they are optimized to support these services.
- A review of the configuration management process should focus on, and alter as required, the process design, including inputs and outputs, workflows, controls, roles and responsibilities, data models, reporting and opportunities for process automation.

STRATEGIC PLANNING ASSUMPTION(S)

Through 2015, 80% of outages impacting mission-critical services will be caused by people and process issues, and more than 50% of those outages will be caused by change/configuration/release integration and hand-off issues.

ANALYSIS

At its heart, configuration management is about visibility through accurate and timely information. The configuration management process tracks the current and historical states of all IT services, and provides this information to authorized internal and external stakeholders. This visibility is key to the effective and efficient planning and implementation of changes, which will reduce the risks to the business relating to impaired availability, security and performance.

Without establishing a process for provisioning, discovering and maintaining configuration changes to an IT service, no architecture will be able to "automagically" deliver it with sufficient integrity, given the logical service and virtual device configurations possible that tend to foil discovery tools. The need for timely and accurate information is magnified by the need to better manage human error through the change management process.

Through 2015, 80% of outages impacting mission-critical services will be caused by people and process issues, and more than 50% of those outages will be caused by change/configuration/release integration and hand-off issues. As IT adopts technologies such as virtualization and cloud services, new dynamics will be introduced (e.g., mobility and offline/online), as well as opening its doors to external providers (e.g., infrastructure as a service [IaaS]). This complexity will require IT to add more rigor (not less) to their configuration management process. As the number of internal and external service providers increases, the need for timely, accurate and secure information flows also increases. With any delivery method, configuration plays a vital role in providing logical views of IT services, including changes to configurations.

Rightsizing Your Configuration Process

Many IT organizations have not formalized their configuration management processes and have varying maturity across their domains (e.g., network, server and applications) in how configuration management is done. Yet, every domain has configuration processes. They may not be documented or formalized, or even complete for all activities; but if changes are made to systems and software, then configuration management is being done (even if not done effectively).

Many IT organizations are asking how much configuration management is "needed" for virtual and cloud infrastructures. How you define configuration requirements will be determined by two main factors: how standard your environment is and the level of risks associated with changes. Today, most standards are typically static for several years. In addition, early cloud implementations are not focused on business-critical systems, but that trend is changing with the increasing adoption of virtual infrastructures. As IT becomes more proactive, trending and predictive analysis will require a historical perspective, not of a virtual machine (VM), but of the IT service and all changes that were relative to its availability.

If you have infrastructure and software standards and a change management process that properly manages risks so that there are minimal disruptions to IT services, then your configuration processes may only need to be adjusted for the new rapid dynamics of virtualization or cloud architectures.

Consider the following questions and responses to rightsize your configuration management process for virtual and cloud infrastructures:

1. How well are standards defined and followed? Standard implementations bring predictability and speed in deployment, but the mobility of virtualization adds unpredictability in performance, because changes can be done in real time without an impact assessment. Add a shared infrastructure (e.g., multiple VMs per host and cluster) and what was standard and predictable for one IT service will potentially be affected by other IT services. These new dynamics will affect how standards are assessed and maintained, and will require closer inspection of how dynamic (versus standard and static) the IT service blueprint should be. Standards will need to be reassessed on an ongoing basis to ensure scalability and predictable availability.

2. How well are IT services documented or tracked in systems such as the configuration management database (CMDB)/configuration management system (CMS)? The CMDB/CMS will maintain a trusted view using integration and federation to bring in configuration data from a wide variety of sources. Some discovery sources can take triggers from virtual infrastructures and become closer to a "real-time view." This view, coupled with a runtime view for application performance, will enable better predictive planning. Because having visibility to public cloud infrastructures can be limited with today's discovery tools, it is critical for IT organizations to understand the service or application, and how it is manifested (internally and externally).

3. How well is automation used to discover and execute changes? While IT resources are often experts, they are still prone to human errors. Using automation to discover and better target changes will significantly reduce outages. Automating provisioning without understanding the impact of the single change to a system or software on the broader IT service

or application may have a negative effect (e.g., outage) systemwide. In addition, with the frequency of changes to the virtual and cloud infrastructures, coupled with new agile development and deployment, automation will improve the speed of changes and reduce the errors to which humans cannot scale, to accommodate the increase in changes without an increase in errors.

4. How well are audit requirements for contractual and regulatory compliance addressed? Enterprises can no longer exist without mechanisms that prove sufficient control is in place. Virtualization enables the swift and real-time movement of servers and applications from one place to another. Due to this type of movement, organizations could fail to comply with restrictions, which could subject the enterprise to significant consequences. This applies not just to country- or industry-specific regulations (e.g., payment card industry) or security-based regulations (e.g., Center for Internet Security[CIS]), but broader regulations (e.g., the USA Patriot Act) that will impact or support global enterprises.

5. How well are software licenses tracked and are they accurate? Virtual infrastructures add mobility and offline dynamics that can present a challenge for tracking application and software usage. IT organizations will have to be prepared with documentation and discovery methods that can prove license instantiation.

6. How well does IT already manage multisourced or multivendor operating environments? The public cloud is not necessarily new; in many respects, it's another flavor of outsourcing or software as a service (SaaS). IT organizations are still responsible for their data, their application availability, etc., but now there is a middleman. IT organizations that have best practices in place for multisourced or SaaS infrastructures likely will have less of a challenge adapting their configuration strategies to the public cloud. IT should seek out lessons learned from traditional outsourcing vendors and incorporate them for the broader use cases in the public cloud.

7. What is the degree of business risk that IT organizations will tolerate, associated with specific types of changes (e.g., to business-critical systems, preapproved changes, emergency changes, etc.)? Today, changes are controlled within the IT infrastructure, but cloud infrastructures will take change-impact assessment beyond the corporate firewall into more "opaque" environments (public clouds). As the scope of control alters with public cloud scenarios, business risk factors will need to be re-examined, and existing policies will need to change to enable a 90% success rate or better.

Bottom Line

No process is static. All processes should undergo evergreening on an ongoing basis. Some organizations conduct a complete review yearly, whereas others review only metrics. Some organizations modify processes, terms of the overall process, subprocesses and controls. With the adoption of cloud architectures (private and public), IT organizations will need to rightsize (assess, modify and adapt) their configuration management processes to address the dynamics discussed in this research. For some IT organizations, priorities for specific services may be the focus of the adjustments to the configuration management process.

By assessing its change management policy, an organization can modify what changes are "pre-approved" for virtual infrastructure. Likewise, the level of configuration management rigor should be based on the criticality of the service. Controls are measures in processes used to mitigate risks. All things being equal, a critical IT service will warrant additional controls to safeguard the value it delivers to the business. New technologies may alter the risk landscape and thus require a change in configuration-related controls, which may then require a change to the overall configuration processes. IT needs to strike a balance between controls that reduce risk unnecessarily and the need for speed and agility.

Even with new technologies, such as virtualization and cloud services, IT still needs configuration management to assist with the planning and operations of IT services. Opportunities for process improvement and automation must be investigated to ensure the process provides the necessary support and doesn't unintentionally become a constraint and limit the potential value of the new delivery methods.

This research is part of a set of related research pieces. See "Private Cloud Computing: Clearing the Air" for an overview.