BEST-PRACTICE RECOMMENDATIONS
CONFIGURATION MANAGEMENT

Sun Services
White Paper
May 2007

Abstract

Modern IT organizations can have hundreds or thousands of servers supporting business users around the world. These systems and networks become the lifeblood of an organization as the integration of technology and process create competitive advantages for businesses. As a result, managing and controlling IT resources becomes an ever more important task. At the core of controlling these corporate resources is understanding and managing the configuration of IT assets. Optimized configuration management allows organizations to control and protect the deployment of their IT resources. This paper outlines several best practices to help organizations implement and optimize their configuration management programs.

Contents

Three simple rules for configuration management

Rule 1 – Stay in control
You have to stay in control of configuration items and the ways they change. If you lose control, your process is worthless.

Rule 2 – Use technology
Manual configuration management may prove to be impossible. You need to use technology to help discover, record, and maintain configuration information.

Rule 3 – Configuration management makes other things happen
Implementing configuration management by itself is a waste of time. Your configuration management program must enable your change, incident, problem, and release management programs if you want to see a return.

Why is configuration management important?

Today's IT operations are a collection of integrated computing networks that possess mind-boggling complexity and sophistication. Even the simplest environment, supporting only a few business applications, requires attention to configurations to keep applications and hardware running smoothly. But why is that? Why is managing the overall configuration of your IT system important?

Enterprise Management Associates has noted that 60 percent of service impacts are due to configuration problems[1]. Beyond the personal frustration associated with having to resolve configuration-related incidents, there are also serious business-related impacts resulting from poor configuration management.

At the most obvious level, configuration problems can cause system-related failures. Key systems or services can simply stop working, or their performance can noticeably degrade, causing the productivity of business workers to fall or even come to a complete halt. When operating systems and applications are not kept current with key releases and patches, they can become vulnerable to security breaches and expose your organization to hackers and other internal or external mischief makers.

On a less obvious level, if systems are kept in a stable but non-current state for too long they may effectively become impossible to update. This can greatly affect an organization's business agility. Old systems will need to be forklift-replaced, costing valuable budget dollars and potentially years of time. These dated systems can also keep you from taking advantage of new software and hardware features to improve your business operations.

What is configuration management?

For the purposes of this paper, configuration management means the *process of providing a logic view of the IT infrastructure or services by identifying, maintaining, and verifying the versions and status of configuration items in existence.* Within this definition, a Configuration Item (CI) is *any component of the IT infrastructure that falls under the control of, and is monitored by, the configuration management process.*

It's important to note that configuration management builds on the basics of asset management but adds a very important element. configuration management understands and tracks the relationship between CIs to build its logical view. To use a chemistry analogy, not only does configuration management know what's in this beaker and that flask, but also it knows that they are connected by means of a glass rod and two pieces of surgical tubing. It's this understanding of relationships in the network that gives configuration management its value as an IT service.

While the Information Technology Information Library (ITIL)[2] and the International Standards Organization (ISO 20000)[3] have written extensively on best practices for configuration management, we believe there are three critical best practices for you to be aware of:

- **Maintaining control** – For configuration management to have any sort of useful life in your IT operations, the process must maintain control over its CIs and be continually updated. Once your configuration management process becomes stale, it's worthless.
- **Tracking the right CIs** – When you look at your IT infrastructure you may be awe-struck by all the things you could track. If you try to track them all, you'll be likely to fail. It's critical to pick the CIs that you need to track and can track.
- **Create a repository** – To make all the wonders of configuration management work for you, you must have a repository for CI information. Without it, your program will not be sustainable. ITIL defines a very comprehensive repository approach called the configuration management Database, or CMDB[4]. Regardless of what approach you take to the idea of a configuration repository, you need one.

What makes configuration management difficult?

We're not sure anyone really believes that implementing configuration management is easy. In fact, many people believe the task is downright daunting. Beyond the initial difficulties with program scope and organizational support, there are some other inherent attributes of today's IT systems that really complicate matters.

- **Integrated systems** – As systems become more integrated, a whole new set of CIs develop. Middleware software becomes a critical element to facilitate proper transaction execution. Poor configuration management at this level can cause significant issues.
- **Service-oriented architectures (SOAs)** – The reason an SOA works well is that it consolidates a set of functions common to many applications into a single service. If an SOA service configuration and its relationships are not managed well, many portions of the IT infrastructure can be impacted.
- **Bad configurations** – Many times IT shops deploy bad or unstable configurations. Bad configurations can have ripple effects that extend to many other systems in the connected IT world. Many vendors, including Sun, can help you define and test known good configurations.
- **Separate domains of IT** – There are many different disciplines within IT these days. Each domain (server, network, application, telephony) will have separate requirements for configuration management and unique CIs to manage, creating challenges for a central program.

How to get started with configuration management

Generally speaking, configuration management is an advanced but critical step in effectively managing your IT operations. Effective configuration management will allow you to react to events like security patches, firmware updates, and application version changes in a rational and efficient manner — no more running around and checking the OS levels of every server at 2:00 a.m. A few key items to consider in implementing your configuration management program are:

- **Planning and scope** – Implementing a configuration management program can be an arduous task. So it's critical to set a realistic project timeline and to start with the basics. If you try to do too much, you'll never get the program off the ground. Starting in a reasonable, limited fashion allows you to gain control in certain areas and build on established success thereafter.

- **Establish a repository** – Many vendors have very capable CMDB products that could fit your needs. Regardless of the route you choose, you must have a repository for accurate configuration information. One of the outputs from your planning and scope development should be the requirement set for a repository. Use these requirements to help you select the right pieces of repository technology. You may find that an individual CMDB product may not work for your needs. Don't be afraid to add other components to create the right technology mix for your organization.
- **Defining the right CIs** – There are literally thousands of CIs that you could track—but trying to track them all would be a waste of your time and resources. We suggest that you look at each layer of your IT infrastructure (applications, operating systems, hardware, and services) to determine the most appropriate set of CIs and relationships to track and monitor. Once you have determined the CIs you want to track, certain vendors can help gather initial CI information.

Optimizing your IT process with configuration management

Once you have the basics of configuration management up and running, there are some interesting ways to leverage your configuration management program. It's important to remember that each organization will have to decide for itself how important configuration management is and how far to go with it in optimizing overall IT infrastructure management. Some areas to consider include:

- **The use of configuration management by other IT services** – Functions like incident management, change management, release management, problem management, and asset management can all make use of key information tracked by configuration management. As other services leverage configuration management, they'll be able to respond more efficiently or implement changes faster. This integration allows for optimization of IT in its overall delivery of services to the business.
- **Federating disparate configuration information** – Most likely you won't implement one single CMDB or repository but rather have several domain-specific repositories for configuration information (one for the network, one for MVS, one for the Solaris™ Operating System, one for storage, etc.). In order to harness the true power of this information, we see a compelling reason for configuration management programs to federate these independent domains. Doing so will give you a more comprehensive view of your IT environment.
- **Policy-directed automation** – Automated discovery of assets and configuration management can go a long way in maintaining the stability of your configuration management program. Automation can potentially go farther than mere discovery; to the extent that you can base policy and rules on configuration information, a host of other automation can occur in the datacenter. This begins the creation of a self-aware, self-directing technology platform.

Conclusion

While configuration management may not be the easiest or the first function you implement in controlling your IT environment, it can be a very powerful step in ensuring proper control of your IT resources. configuration management allows you to understand the IT resources you have and how they relate to one another. This information allows you to make informed decisions on maintaining and upgrading your IT environment. Implementation of a configuration management program is a critical step to take in optimizing the management of your IT world.

Endnotes
1   Enterprise Management Associates. "Configuresoft, Inc.'s Enterprise Configuration Manager: A Continuous
    Compliance Approach to Configuration Management," 2006.
2   Best Practices for Service Support, ITIL - Office of Government Commerce, The Stationary Office, London, United
    Kingdom, 2000.
3   "Information Technology – Service Management Parts 1 &2, ISO 20000," International Standards Organization,
    Geneva, Switzerland, 2005.
4   Best Practices for Service Support, ITIL - Office of Government Commerce, The Stationary Office, London, United
    Kingdom, page 124, 2000.