CA Configuration Automation is designed to help reduce costs and improve IT efficiency by automating configuration management tasks associated with datacenter and private cloud provisioning. The product helps to ensure continuous compliance with internal IT configuration policies and industry security configuration benchmarks and supports best practice configuration change management process to improve IT service availability and reduce outages caused by configuration errors.

Overview
Managing and tracking IT resource configurations in an increasingly complex IT environment which is defined by rapidly changing and highly dynamic virtual and private cloud components is one of the toughest challenges facing IT operations today. This complexity is against a backdrop of an expanding list of regulatory compliance mandates with legal and financial implications for the business as well as for IT operations and IT security teams with converging responsibilities for implementing compliance programs and supporting audit readiness. In spite of these needs around configuration compliance, the traditional role of configuration management solutions for enabling best practice change management systems for faster incident and problem resolution is still as important as ever.

CA Configuration Automation addresses these challenges with an integrated solution for configuration change and configuration compliance management. It helps to reduce expensive head counts required to implement best-in-class compliance programs in physical and virtual IT infrastructures by automating labor-intensive configuration management tasks which are usually tedious, time-consuming and error-prone.

Benefits
CA Configuration Automation can help you:

- Maintain accurate configuration data for servers, applications, and services as part of a multivendor change management system (CMS)
- Improve service availability with intuitive visual maps of the relationships and dependencies between IT services and discovered components for service impact and root-cause analysis
• Define standardized configurations for provisioning infrastructure resources to enable repeatable and reusable IT services in private cloud and data center automation

• Enforce compliance with internal IT configuration policies or external compliance mandates such as PCI, SOX and HIPPA using policy-based contents built on industry-standard security configuration benchmarks

• Perform regular audit scans with reports to demonstrate compliance with security configuration policies

• Automatically detect and remediate changes from configuration or security baselines that could result in unplanned outages or violation of compliance requirements in critical service components such as ERP, Web and financial applications servers

• Provide various reports, dashboards and alerts on the configuration compliance status of your infrastructure components and business services

CA Configuration Automation—an integrated solution for continuous configuration compliance in private cloud

Policy-driven configuration compliance management for a new IT delivery model

A key economic promise of private cloud computing is predicated on IT’s ability to support predefined and repeatable business services, which are underpinned by infrastructure resources from shared assets. The resources should be deployed on-demand based on end-user service requests, with minimal intervention by IT staff. Successfully automating the complex tasks involved requires IT to minimize variations in the service request fulfillment processes by deploying components with standardized configurations that meet minimal internal configuration policies and mandated security configuration guidelines.

Establishing an initial provisioning baseline is just the start. IT needs to continuously track data center infrastructure for configuration policy compliance and audit readiness on an on-going basis and in a new IT delivery model dominated by high-frequency of changes with physical and virtual compute resources which can be rapidly replicated, moved, provisioned and brought into production based on end-user demands. Manual attempts at tracking and enforcing configuration compliance have proven to be inefficient, resource-intensive and prone to errors in the past, and will be even more so now with broader service availability, security and regulatory compliance implications.

In addition to addressing compliance needs, an integrated configuration management solution can be a central piece of any best practice CMS; creating synergies by automatically detecting changes in key infrastructure components—authorized or otherwise—and invoking remediation rules or compliance policies as needed.

Instances of IT service outages that are due to non-compliant configurations can be further reduced when an accurate picture of the infrastructure landscape can be painted—for the CMS in the form
of discovered configuration data—and for IT operations through visually compelling graphical information that highlights the dependencies between discovered service components. These capabilities are invaluable to IT service desk and operations personnel who need to undertake root-cause and service impact analysis for faster incident resolution and to improve SLA objectives.

Product overview
CA Configuration Automation is a highly scalable solution for configuration management and configuration compliance audit checks with blueprints contents that are based on the Center for Internet Security (CIS) Benchmarks. The Benchmarks provide minimum technical control rules and values for hardening operating systems, middleware and software applications, and network devices in order to meet configuration recommendations by various industry standards and regulations including PCI and SOX compliance.

CA Configuration Automation is available as a stand-alone solution or as part of automation and cloud provisioning solutions from CA Technologies including CA Automation Suite for Data Centers and offers the following key functions:

Infrastructure discovery
• Automatically discover servers, software applications and services in the datacenter.
• Inventory configuration settings for physical and virtual infrastructure components

Topology & dependency mapping visualization
• Visualize the relationships and dependencies between discovered services, servers and applications with an integrated GUI
• Enhance root-cause and service impact analysis with topology maps

Unauthorised change detection
• Capture configuration data and dependency information into snapshots
• Accelerate problem isolation by searching snapshots to find configuration changes
• Track and compare configurations to approved baselines and “gold standards”
• Detect configuration drift and quickly remediate configuration errors

Configuration policy compliance
• Use compliance rules to check whether server and application configurations adhere to compliance policies
• Use built-in rules to facilitate compliance with industry standards such as PCI and DISA
• Enforce security policies by validating that newly provisioned server configurations adhere to industry best practices

Multi-vendor CMDB integration for ITIL change management system
• Easily migrate configuration and dependencies information for CIs to CA CMDB and 3rd party CMDBs such as BMC Atrium CMDB
• Implement best practice enterprise change management systems
Features

Integrated change & configuration compliance management with auto discovery and topology dependency mapping in one comprehensive solution.

Agentless and agent-based software auto-discovery provides comprehensive and flexible discovery options – agentless, softagent and agent-based discovery methods. Agentless discovery enables you to conduct a comprehensive inventory without having to install software on target components whilst agents can be deployed when more in-depth application discovery is required. You can discover applications, databases and servers on - distributed and mainframes (z/Linux) environments.

Profile-based discovery is used to schedule discovery and management operations to run on a recurring basis. With Server Management Profiles, you specify when and what configuration management operations to perform at initial server provisioning and afterwards. For example, using Server Management Profiles you could schedule when configuration snapshots are taken or how often configuration compliance should be verified.

Change detection with configuration snapshots enable you to detect file and parameter level changes in software component configurations. Simply take a snapshot of your configuration settings at any point and compare it to previous or future snapshots to track and detect unauthorized changes. You can also create a baseline snapshot or “gold standard” to detect servers that are out of policy compliance.

Best practice configuration policy management with blueprints provides several hundred blueprint contents with built-in knowledge base for major Web and applications servers, databases, messaging systems, network devices and operating systems (Windows, Linux, Solaris, AIX and HP/UX). Using standard blueprints enables you to quickly discover instances of a component, locate its configuration files, extract configuration settings and determine dependencies and relationships. With the built-in Blueprint Editor, you can create blueprints to support custom applications.

Rules-based compliance is a unique feature designed to enable you to assign rules and policies at the file and parameter levels. Run snapshot data against default value and the rules specified by built-in compliance blueprints (Figure 1). The blueprints are based on CIS Benchmarks and vendor hardware security hardening guidelines for meeting industry mandates such as the Payment Card Industry (PCI) standard. Changes are automatically tracked and you are notified when there is a violation.

Remediation is used to automatically detect changes to critical configuration settings and modify to comply with default values and policies.

Integrated with Enterprise Management solutions from CA Technologies including CA Service Assurance, CA Service Desk Manager (CA CMDB) and CA Automation Suite for Data Centers to support configuration management requirements of IT Operations, IT Service Management and private cloud provisioning.

Reporting & dashboards provides predefined dashboards, visualization graphs and contents, and reports with view, print, export and scheduled e-mail delivery.
Grid architecture provides enterprise scalability in line with enterprise management solutions standards.

What’s new?

• Application dependency mapping visualization
• New visualization UI with predefined graphs and customizable templates
• Telnet-based discovery option
• Windows discovery with WMI Support for Web Services access mode for Blueprint Discovery
• Integrates NDG data into change/compare and compliance operations
• SUDO-based discovery and configuration data collection
• z/Linux (RedHat & SUSE OS) discovery support via SSH or Telnet

Figure A
Rule compliance blueprint
Prepackaged compliance blueprints based on CIS benchmarks are used to ensure that minimum configuration compliance guidelines are met.
Figure B
Server compliance summary result
Automated servers and applications configurations scan result classified by compliance with CIS configuration benchmarks.

Figure C
Visualization & topology mapping
Relationships and dependencies between discovered components and IT services are represented graphically to assist root-cause and service impact analysis.
CA Configuration Automation can help you:

- Improve operational efficiencies while lowering costs for data center and private cloud provisioning
  - Increase utilization of IT staff—automate routine configuration tasks and redeploy IT staff to more strategic projects
  - Improve delivery of IT services—reduce the time it takes to provision compute resources with standardized configurations
- Enforce compliance policies and reduce overall risk
  - Demonstrate configuration compliance through automated audit checks and reports. Quickly identify and remediate policy violations. (Figure B: Server Compliance Summary Result)
  - Improve ability to meet multiple regulatory compliance mandates with common IT controls and reduce duplication of efforts by IT teams
  - Improve IT compliance processes to help meet PCI, SOX and other regulatory mandates using policy-based contents and best practices based on industry benchmarks
- Improve service availability and proactively prevent data center outages
  - Reduce downtime—proactively detect configuration drift before it causes a data center outage. Automatically restore configurations to approved “gold standards”
  - Enforce change control policies and reduce unauthorized change to IT infrastructure
  - Reduce service outages and enhance IT service delivery goals through faster problem resolution by providing accurate configuration information and infrastructure visibility to service desk analysts and change management systems
  - Increase service availability and SLAs with root-cause and service impact analysis

The CA Technologies advantage

CA Configuration Automation helps meet the converged requirements of IT operations for internal configuration policy compliance and the compliance needs of multiple industry mandates that are dependent on effective change control of IT systems. The solution automates repetitive tasks—which can be tedious, resource intensive and prone to human errors—associated with IT policy audit reporting and continuous configuration compliance dictated by current mandates. By offering an integrated platform for discovery, change detection and change remediation it helps ensure that the complex configuration compliance demands of emerging dynamic data centers and private cloud infrastructure can be addressed through intelligent policy-based configuration automation.
CA Configuration Automation is part of the CA Automation Suite for Data Centers solution designed to help you dynamically build and scale IT services and private cloud infrastructure through a modular approach. The suite comprises various integrated market-leading products including CA Server Automation, CA Virtual Automation, CA Process Automation, and CA Configuration Automation.

Higher hardware sales, continued production data center virtualization, and experimentation with cloud strategies are contributing to increasingly dynamic and complex data center and service provider environments that require sophisticated and comprehensive change and configuration management software tools in order to track assets, manage change, maintain up-to-date configurations, enforce corporate standards, and ensure compliance with software license agreements.

To learn more about CA Configuration Automation and other CA Data Center Automation Solutions visit ca.com.