

# Novell® Resource Management:

Delivering the Future of Policy-Driven Solutions

[www.novell.com](http://www.novell.com)

---

BUSINESS WHITE PAPER



**Novell®**

# Table of Contents

Novell Resource Management:  
Delivering the Future  
of Policy-Driven Solutions

---

- 2 EXECUTIVE INTRODUCTION
- 3 THE EVOLUTION OF SYSTEMS  
MANAGEMENT
- 4 UNDERSTANDING POLICY-DRIVEN  
AUTOMATION
- 6 A GENERAL MODEL FOR POLICY-  
DRIVEN AUTOMATION
- 9 DELIVERING THE FUTURE OF  
POLICY-DRIVEN SOLUTIONS

# Executive Introduction



What if your organization could make timely, accurate decisions based upon strategic business intelligence, increasing your ability to achieve success, profitability and growth? What if your employees and partnerships could adapt instantly to changing business conditions? What if you could increase productivity through improved service levels and end-to-end business processes while simultaneously reducing costs? What if you could enable powerful, cross-company solutions while actually increasing your ability to respond to security issues and achieve compliance with governmental regulations? Novell® Resource Management solutions, powered by ZENworks® technology, are laying the foundation to uniquely deliver upon these visionary concepts through significant advancements in the implementation of true Policy-Driven Automation and business integration.

The pace of your business is constantly increasing and the markets you pursue are evolving rapidly. All this change causes you to continually modify the way you do business, and as part of this challenge, your IT environment must evolve at the same rapid pace to meet your changing business needs. However, accommodating change is difficult because your IT environment consists of a wide variety of disparate systems, both tactical and strategic, where each system adds complexity and management burden to your organization. Additionally, your enterprise likely experiences internal conflicts and boundaries (political, organizational, security and physical) that increase heterogeneity and make it even more difficult to create a unified IT infrastructure. Nothing seems to exist to solve these problems associated with rapid change, product limitations and heterogeneity. Even more significant is what is really needed—IT solutions that accommodate your business policies, rather than business policies constrained to the limited capabilities of your individual IT systems.

One approach currently available for accommodating change in IT environments is Configuration Management. Available from a wide variety of vendors, Configuration Management products typically enable organizations to	implement and configure workstations and servers (with limited support for laptops and handhelds), and to manage those configurations as needs change. However, while Configuration Management accommodates change in such devices, the products
---	--

themselves are inflexible in their capabilities and narrow in scope—lacking the ability to manage, influence or integrate with any of the myriad other strategic systems in your enterprise. The problem with Configuration Management products is that they represent “islands” of management and Identity—creating and acting upon their own limited management information in confining ways, rather than integrating with existing corporate knowledge to manage all systems robustly as necessary to achieve business objectives. Configuration Management products can sometimes be made to work with existing business systems, but such integration is most often severely constrained. True integration of these products with strategic systems currently requires costly and time consuming custom development, but because of the rapid pace of change, such efforts are at risk of being outdated before they are even seriously engaged. Ultimately, Configuration Management products often prove to be tactical in nature because of their limited perspective, and therefore have limited usefulness and must be replaced—a costly undertaking—as business requirements evolve.

Fundamentally, business problems aren't constrained to individual devices such as workstations or servers and therefore require a better solution. Real business solutions affect a wide variety of IT systems, and what you need is the capability to centrally manage all systems through an extremely flexible, unified foundation. You need the ability to solve tactical problems while addressing strategic issues as well. You need the ability to integrate the management of

workstations, servers, mobile systems, data, applications and all other IT resources in a easily customizable, timely manner so that their behavior accommodates the business problems you face now and in the future, whatever those problems might be. You need the unique power of Novell Policy-Driven Automation.

### THE EVOLUTION OF SYSTEMS MANAGEMENT

The evolution of systems management towards the promise of Policy-Driven Automation has been long and difficult. Systems management vendors have often promised to dramatically ease the administration of distributed systems, and while efficiencies have been gained, such systems have been highly complex and limited in their capabilities. Something better is needed.

Distributed systems management products were initially introduced to solve the difficulty of configuring a large number of IT systems with a small handful of IT personnel. Such legacy automation products enabled a single administrator to specify a variety of options enabling each management action to be applied to a large number of actual systems. While many Configuration Management vendors currently claim that their systems support the use of Policies, their systems are instead only implementations of this legacy automation model. Such vendors are confusing the term Policy with the concept of administrative options associated with manual actions, and therefore are not truly Policy-based.

The next step in the evolution of systems management was the advent of “desired state”

management of workstations and servers. Under this paradigm, an administrator was required to undertake the arduous task of defining the desired installation of software on target systems based upon all possible hardware and software configurations. Once defined, the managed system was automatically maintained to ensure the integrity of its software. While innovative, desired state management was of limited value because of its narrowly restricted scope. Desired state management dealt only with the software configuration of the target system, and therefore had no ability to manage the overall behavior of the system, its interaction with other systems, or its integration into the greater world of enterprise IT solutions.

#### UNDERSTANDING POLICY-DRIVEN AUTOMATION

Novell is redefining systems management with the development of Policy-Driven Automation. Through this paradigm, organizations manage their systems as a whole by specifying the interaction that is needed between and within systems to implement business-level Policy beyond the confines of the functionality available within individual IT products, thus aligning IT with business success.

So what exactly is "Policy"? Quite simply, "Policy" is a declaration of the applicable administration, management and access associated with company resources. However, unlike legacy automation and desired state management, real Policies make no assumptions about the types or qualities of the IT resources through which

Policies are enforced. Perhaps the best way to illustrate Policy is through a simple, but very realistic, example:

*"We need to tightly protect the security of our corporate contracts. Only qualified lawyers in our corporate Legal department should be able to retrieve, view and edit those contracts. They should only be able to do so during normal business hours, and access should be allowed only from secure locations."*

Note that this Corporate Policy is unbounded by the capabilities of individual IT systems and therefore ignores the limitations of existing Configuration Management products. In fact, implementation of this Policy would require close coordination of the configuration and behavior of a number of disparate IT systems:

1. To leverage existing corporate knowledge, the corporate directory service would be integrated to provide information about users, their assignment to corporate departments such as Legal, and whether or not they are qualified to edit contracts.
2. To increase security and reduce IT workload, automated software distribution services would be integrated to ensure that single sign-on automation software is correctly installed and configured on the workstations of qualified corporate lawyers.
3. To further increase security, automated Secure Identity Management services would be integrated to ensure that randomized

credentials for accessing the contracts repository are granted and stored with the directory services user account of each qualified lawyer. These credentials would be utilized by single sign-on automation services to simplify contract access. Secure Identity Management integration would also include protection of the contracts repository to prevent access except during normal business hours.

- To increase security even more by eliminating the possibility of inappropriate access, automated network configuration services would be integrated to ensure that requests to the contracts repository that originate from outside the corporate legal department subnet are not allowed through the departmental router.

Our seemingly simple Policy involved a complex series of coordinated management actions across a variety of IT systems—a set of actions beyond the capabilities of Configuration Management products currently available. While the highly tangible value of being able to implement Policy such as this is clear, how can these capabilities be achieved? Because of the breadth of management and integration capabilities required, how can a Policy-Driven Automation system be created that crosses system boundaries

while allowing IT resources to be easily managed as one? A complete solution must take into consideration the entire Resource Management stack. Policy-Driven Automation leverages the personality-based hardware configuration, software distribution, patch deployment, data management, remote control and other primary Configuration Management functions as a key component of the resource management capabilities it provides under this new paradigm. The answer can be found in the unique power of Novell Policy-Driven Automation.

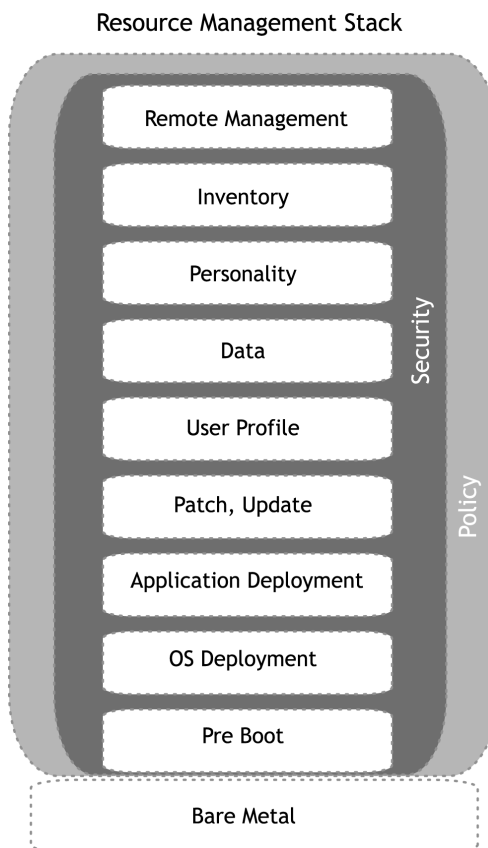


Figure 1. Resource Management Stack

## A GENERAL MODEL FOR POLICY-DRIVEN AUTOMATION

Effective resource management through business-level Policy, including Configuration Management, can be implemented across a wide variety of systems through a model that robustly accommodates the three fundamental components of Policy-Driven Automation: "Actionable Data", "Policy Conditions" and "Policy Actions":

*Figure 2. General model for  
Policy-Driven Automation*

1. **Actionable Data** is the information upon which Policies make decisions. In the same way that employees are limited in their abilities based upon their knowledge, Policies are limited in their decision making abilities based upon the quality and quantity of information at hand. Rather than being limited to making configuration decisions based solely upon hardware and software inventory of workstations and servers, a far superior approach is to provide Policies with the broadest, deepest amount of information about the managed resources—whatever they might be. The greater the information available, the greater the decision-making ability of Policies.

One source of Actionable Data is information that can be automatically discovered about the attributes, configuration and state of

managed resources. For instance, a particular data set might be uniquely managed based upon the performance of the server on which it is stored, the hardware resources of that server, the security of its physical location, the department owning the server, the speed and security of the links between the server and the user accessing it, etc. All of these attributes could be relevant to controlling the administration, management and access of the data set.

Actionable Data can also be provided by trusted internal and external systems. Most enterprises implement a wide variety of systems, and each contains data relevant to managed resources. Organizations require robust mechanisms to accommodate the difficult internal conflicts and boundaries

(political, organizational, security and physical) associated with enterprise systems in order to enable their information to be securely available for Policy to act upon—a capability known as Identity Federation.

Finally, organizations require the ability to securely and scalably manage the Actionable Data to ensure its integrity and availability to Policy. Identity Management capabilities such as Role-Based Administration, Delegation and Workflow integrate Actionable Data and Policy enforcement into the business processes of the organization, thus reducing costs and simplifying administration efforts.

The result of Actionable Data that is collected, Federated and managed in this manner is referred to as “Integrated Identity”—the only effective foundation upon which Policy can be properly and robustly implemented.

2. **Policy Conditions** are the decision making statements that evaluate Actionable Data as relevant to the resources being managed to determine when and how to enforce Policy.

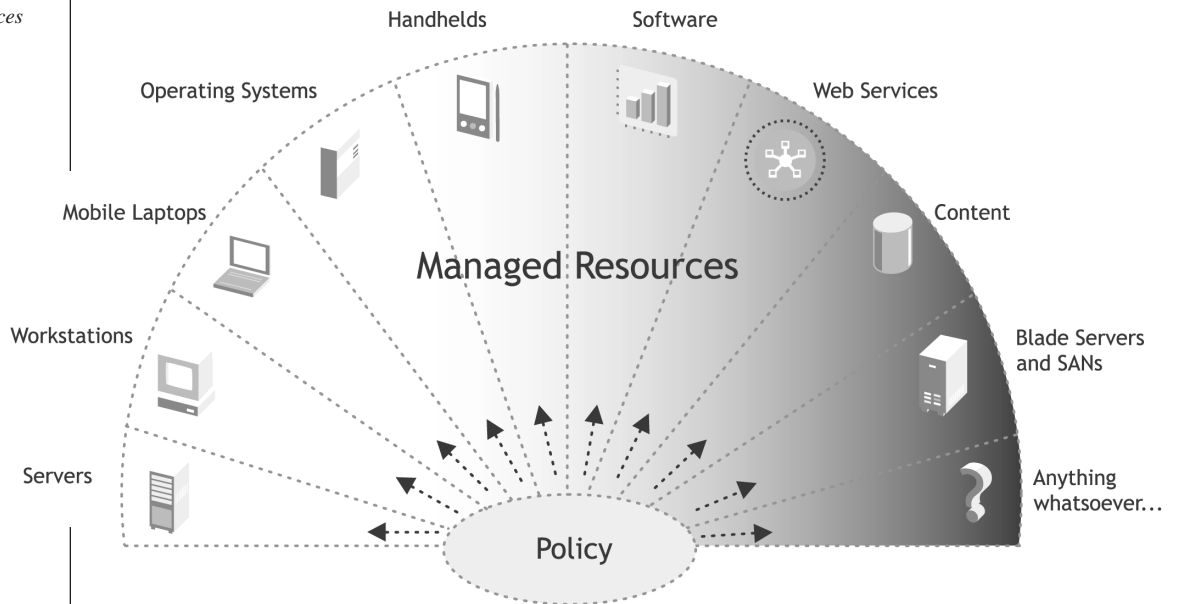
Policy Conditions follow a simple but ultimately powerful “if-then-else” format, such as “if the user attempting to access the contract is a Lawyer in the Legal Department, and if the user has been granted rights as a contract editor, and if the current time is between 8am and 6pm on a weekday, then <allow the access>, else send a warning to the system administrator.”

3. **Policy Actions** enforce the decisions made by Policy Conditions. In our example above, the “<allow the access>” statement would actually detail the exact set of IT actions necessary to allow the access. In our example, this would entail invoking systems to automate the distribution of single sign-on software to the user and the creation and storage of credentials enabling access to the contracts repository. Additional enforcement actions would be invoked to prevent access except during business hours, and to configure the department router to prevent access from outside systems.

This general model for Policy-Driven Automation is vastly superior to alternative paradigms because it supports the management of any type of resource, not just servers and workstations. Our example Policy included integration and configuration of a Secure Identity Management system, a document management repository and a network router as well as a workstation and a server, but did so through a single expression of Policy that represented the state of the IT resources as a business solution rather than requiring error-prone, disparate, disconnected actions by multiple administrators on each IT system involved.

A final component of Policy-Driven Automation is the ability to securely capture and store information about all activities of the system. From this information, customized reports can be generated to facilitate auditing for a variety of solution-specific purposes, such as compliance with governmental regulations. Captured information can also be used to generate events for systems integration, administrator alerts or the triggering of additional Policies of any sort to handle exceptions as most appropriate for your organization.

Figure 3. Managed Resources



## DELIVERING THE FUTURE OF POLICY-DRIVEN SOLUTIONS

Unlike legacy management paradigms that sought solely to reduce administrator effort through limited automation of individual systems, Policy-Driven Automation is the embodiment of how you truly desire to manage your IT resources—according to your business requirements. Policy-Driven Automation seeks to *eliminate* administrator effort through total, continuous automation completely customized to meet your unique needs. Policy-Driven Automation eliminates the barriers of IT systems as islands of Identity and provides a common point for customization and systems integration that other approaches completely lack. Policies are a reflection of business needs rather than the limited capabilities of your IT systems. Policy-Driven Automation is a revolution away from managing individual IT systems, embracing a holistic approach of managing all IT resources as one.

Because it provides such powerful capabilities, Policy-Driven Automation clearly delivers unique compelling value that contributes to business success:

- Greater responsiveness to changing business needs and conditions is enabled through Policies which provide a basis for total automation that speeds IT actions.
- Increased quality of service and enhanced employee productivity are enabled through faster IT response to business needs and requests.

- The potential to significantly reduce costs is enabled through business-focused IT integration and automation.
- More-powerful decision making is enabled by securely and effectively leveraging strategic business data from systems across the enterprise.
- Errors can be eliminated, and security can be significantly increased, because Policies can ensure that nothing is forgotten and that mistakes are avoided.

Novell Resource Management solutions, powered by industry leading ZENworks technology, are uniquely focused on delivering the significant value and robust capabilities of Policy-Driven Automation. Novell Resource Management increases your ability to achieve success, profitability and growth by allowing your organization to efficiently utilize its strategic intelligence and systems in a holistic manner consistent with business objectives. Through its comprehensive vision and approach to Policy-Driven Automation, Novell Resource Management continues to lead the market in its pursuit of uniquely enabling management solutions that empower success.

Novell Resource Management reduces IT costs by delivering open system services that improve the productivity, reliability and security of diverse business environments. For more information about Novell Resource Management and other Novell solutions that can propel your organization, please visit our Web site at: [www.novell.com/solutions/resourcemanagement](http://www.novell.com/solutions/resourcemanagement)

© 2003, 2005 Novell, Inc. All rights reserved. Novell, the Novell logo, the N logo and ZENworks are registered trademarks of Novell, Inc. in the United States and other countries.

\*All other third-party trademarks are the property of their respective owners.

### **Novell Product Training and Support Services**

For more information about Novell worldwide product training, certification programs, consulting and technical support services, please visit:

**[www.novell.com/services](http://www.novell.com/services)**

### **For More Information**

Contact your local Novell Solutions Provider, or visit the Novell Web site at:

**[www.novell.com](http://www.novell.com)**

You may also call Novell at:

1 888 321 4272 US/Canada

1 801 861 4272 Worldwide

1 801 861 8473 Facsimile

### **Novell, Inc.**

404 Wyman Street  
Waltham, MA 02451 USA

**[www.novell.com](http://www.novell.com)**

**Novell**