Making IT Infrastructure Management Easier and More Efficient

An Osterman Research White Paper

Published May 2008
Why You Should Read This White Paper

IT infrastructures are a growing collection of disparate and converging products from various vendors, each with their own management systems, upgrade cycles and so forth. However, all of these technologies must be configured and monitored to ensure the availability of mission-critical applications and services. Deploying, configuring and managing a variety of complex devices from the same vendor, let alone multiple vendors, is a daily battle that challenges even the most experienced administrator.

MANAGING IT INFRASTRUCTURES IS DIFFICULT
The key issues that face IT administrators today, such as managing inventory, guaranteeing system uptime, managing and deploying software updates in heterogeneous environments, and maintaining configuration security and compliance, are pervasive in data centers and network operation centers of all sizes. And, in most environments, these problems have become even more acute due to constraints on IT resources, particularly in a slowing economy. For example, an April 2008 survey of IT decision makers in mid-sized and large organizations found that a large percentage of them face quite serious problems in managing their infrastructures, as shown in the following figure.

![Problems Experienced in Managing IT Infrastructures](chart)

To control costs and leverage IT investments properly requires a unified management solution that can provide extensive visibility, granular control and powerful automation features for the entire infrastructure.
The purpose of this white paper is to discuss these issues, and to provide some information on how Dorado Software can help organizations to more efficiently and cost effectively manage the various components of their IT infrastructure. Specifically, this white paper addresses:

- Configuration management
- Service and application management
- Monitoring and troubleshooting
- The underlying services that tie all of this together
- Information about Dorado Software’s Redcell

**Configuration Management**

Configuration management discovers, monitors and reports on each infrastructure configuration element, or Configuration Item (CI). The general requirements for configuration management are to:

- Identify all CIs (network, servers, storage applications, services)
- Establish relationships between CIs
- Store data in a (preferably) centrally maintained Configuration and Management Database (CMDB).

**DISCOVERY**

Discovery is the first step in taking control of any environment, but it is a step that is complicated by the heterogeneous multi-vendor, multi-technology, multi-protocol nature of most environments in use today. These discovery challenges must be overcome in order to accomplish a number of day-to-day functions, ranging from traditional asset management to managing and enforcing IT compliance policy.

Beyond these tasks, administrators face the ever-growing threat of malicious users attempting to identify exploits and security vulnerabilities, as well as inadvertent mistakes that inevitably will occur in any organization. In order to combat these threats and to increase security, administrators need to be able to discover unapproved or rogue devices that could jeopardize the integrity of the network and interrupt business operations.

Discovery is complicated by the heterogeneous multi-vendor, multi-technology, multi-protocol nature of most environments in use today.
Deep discovery is an automated process that can be based on a specified IP address or addresses, IP address range, or host name. Once the high-level discovery is complete via SNMP v1, 2, 3, WMI, and/or ICMP, the administrator can specify additional supported protocols they wish to use to complete the discovery of their managed resources. After deep discovery, the administrator can add an additional layer of richness to their view of their environment by running an automated link discovery. The connectivity data, when synchronized with asset data in the CMDB, creates a complete picture of an infrastructure that can be represented in highly customizable reports or via a topology view.

**TOPOLOGY**

The connectivity and asset data in the CMDB creates a complete picture of an infrastructure that can be represented in a topology view. This view can be customized to show a variety of topology views in geographical, logical or physical formats. This allows administrators to visualize the interrelationships of managed systems and the underlying infrastructure down to the interconnect level. All views let the user gain access to any managed system by “drilling down” into that device with just a simple click of a mouse. This presents the administrator with multiple options for how they view and perform key management tasks on their infrastructure.

**INVENTORY ASSET MANAGEMENT AND REPORTING**

Another day-to-day requirement for administrators is the ability to manage and report on the inventory of physical elements in their infrastructure. The ability to report on inventory is useful in numerous scenarios including:

- Managing software and hardware versioning
- Tracking warranty information
- Planning replacement and retirement lifecycles.

Also, the ability to readily access and report on this information is crucial for planning for growth and quarterly budget planning cycles.

**PATCHING, PROVISIONING AND COMPLIANCE AUDITING**

As new security threats and regulatory compliance burdens grow, the ability to keep systems up-to-date becomes ever more important. As noted in the previous figure, nearly one-half of organizations find managing and deploying updates in a heterogeneous environment to be difficult or very difficult.

**Service and Application Management**

Service level management allows defining, monitoring and reporting on the IT infrastructure, and constitutes the set of IT staff and systems that are in place to ensure that Service Level Agreements (SLAs) are met. This is a critical exercise for any organization given that SLAs are becoming more important for a variety of systems, including email, customer relationship management systems, enterprise resource planning systems and a host of other mission-critical applications and services.
Monitoring and Troubleshooting

HEALTH MANAGEMENT
Managing the health and guaranteeing the uptime of the infrastructure is of paramount importance to businesses of all sizes – for most end users, this is viewed as the most important function of the IT administrator.

PERFORMANCE MONITORING
In addition to ensuring overall system uptime and health, end users need to be able to monitor key performance indicators to ensure that the data center and the services they provide are running in the most efficient manner possible. It is critical to be able to monitor and chart a variety of subsystems, including processors, memory, the network interface and disks. With access to this data, users can troubleshoot system performance issues, identify bottlenecks, gather insights for redeploying applications, and identify systems that need to be budgeted for upgrade, redeployment or retirement.

COMPLIANCE AND CHANGE MANAGEMENT
In a modern IT organization, change management has two major objectives:

• Ensure that all infrastructure production environment changes are handled so that regulatory compliance can be tracked.

• Relate infrastructure configuration changes to service quality attributes such as capacity, availability and security.

Change management is closely related to SLAs, since change management involves the use of standardized and documented methods for the efficient updating of the IT infrastructure. The goal is to minimize the impact of whatever changes need to occur so that service levels are not negatively impacted.

End users need to be able to monitor key performance indicators to ensure that the data center and the services they provide are running in the most efficient manner possible.

Underlying Services

REMOTE ACCESS AND CONTROL
The ability to remotely access servers and systems from a single location is the key to optimizing IT resources and increasing response times in troubleshooting system and server issues.
Circumstances often arise when the user cannot access the server via the operating system – for example, when a system has power but cannot boot or the OS has crashed or is otherwise unresponsive. If the system is equipped with an IPMI version 1.5 or higher onboard BMC or DRAC card, the user can still manage and troubleshoot the server.

**ROLE-BASED ACCESS CONTROL**

In larger enterprise environments, multiple end users with independent responsibilities may need to access specific parts of the network infrastructure, but regulations may mandate strict requirements for access control. It is important, therefore, to be able to offer multi-level role-based security for single users, as well as group administration and management. Users should be able to easily control access with predefined permission levels that can even be as granular as limiting access down to the level of individual functions. For example, a network administrator would not necessarily need access to any server resources, nor would a desktop administrator require access to any switch or router resources.

**MULTI-VENDOR AND MULTI-TECHNOLOGY SUPPORT**

The vast majority of data centers and network infrastructures use hardware and software from multiple vendors. Consequently, it is extremely important to be able to manage all of these server, system, storage and network resources efficiently.

---

**About Redcell**

**HOW DORADO SOFTWARE CAN HELP**

Dorado Software’s Redcell suite offers compelling infrastructure lifecycle management solutions that address all of these IT issues head-on.

Redcell provides customers with a single solution for complete lifecycle management of IT infrastructures, including visibility, proactive monitoring, change detection and remediation, troubleshooting, OS/file updating, service provisioning and flexible reporting. Redcell offers customers with converging technologies – routers, switches, security, storage, systems, VoIP and more – a unified management solution for applications and services using a single console to ensure network and application availability.

In addition, Redcell’s IT automation features help users simplify the management of their IT infrastructure by incorporating a common operational use model which encompasses the entire IT resource lifecycle. Users are provided the visibility and control to be able to make critical IT business decisions – from a financial, security and/or operational perspective.

**REDCELL INFRASTRUCTURE MANAGER**

Redcell Infrastructure Manager (RIM) is an automated device configuration and administration system built for today’s most advanced and dynamic operation center environments. Offering scalability, multi-technology and multi-vendor support, RIM offers administrators a configuration management system with both an easy-to-use graphical user
interface and powerful scripting capabilities to configure any device in their environment – networking, security, storage, and systems. By normalizing and consolidating how the infrastructure is configured and managed, administrators can save time, reduce errors, increase operational efficiencies and lay the foundation for leveraging the infrastructure for service configuration and performance monitoring.

REDCELL IS FLEXIBLE AND PROACTIVE
In addition to the automation functions available via Redcell’s scheduling capabilities, broader group operations functionality for automation is also available across systems, networking, security, and storage. Users have the flexibility to create static groups and dynamic groups. Static grouping allows administrators to specifically define group membership, while dynamic grouping automatically defines the group’s membership based on filter criteria for either real-time or scheduled operations. Once the resources are grouped, administrators can apply configuration changes or operations to the entire group, thereby dramatically reducing administration time and simplifying management.

Redcell helps achieve those objectives by proactively monitoring all infrastructure elements for configuration changes. All changes are logged and evaluated against company policies and regulatory compliance requirements. Further, associations between service components and infrastructure elements are created during service deployment stored in the CMDB and dynamically updated during service operations so that configuration change events can be correlated as they affect service levels.

The Redcell architecture is completely agentless for all of the domains it manages: Ethernet switches/routers, servers and systems, security devices, printers and Fibre Channel storage.

REDCELL IS SIMPLE
Redcell is straightforward and simple to deploy in enterprise environments of any size for a variety of reasons:

• The Redcell architecture is completely agentless for all of the domains it manages: Ethernet switches/routers, servers and systems, security devices, printers and Fibre Channel storage. This agentless device-driver based architecture allows for faster deployment and faster time-to-value by allowing an administrator to unobtrusively deploy Redcell in their environment.

• Redcell leverages standards-based monitoring and configuration protocols, freeing administrators from concerns about the negatives associated with an agent-based system. These issues include the ongoing management of agent version level and potential problems that may arise with system overhead and interoperability with other applications.
• Redcell offers all of the tools needed to meet today’s key challenges of administrators head-on, and it enables them to deliver key data center services in a cost-effective, efficient, and comprehensive manner

• Redcell offers the modularity and scalability to grow with businesses of all sizes and to ensure that as IT Infrastructure is added it can be managed seamlessly from a single, integrated console.

Summary

Redcell addresses the critical issues facing enterprises of all sizes:

• Discovery
  Redcell addresses the problem of complex discovery via its support for a variety of protocol discovery options and its deep discovery process.

• Topology
  Redcell also integrates event alarms with the topology and alarm conditions appear in the color-coded equipment icons within both geographical and logical topologies.

• Inventory asset management and reporting
  Redcell’s reporting capability extends across all managed domain types and features high levels of customization and report criteria filtering.

• Patching, provisioning and compliance auditing
  Redcell’s hardware and OS patch provisioning allows IT administrators to quickly and easily push BIOS, firmware, OS driver or security updates out to managed Windows™ systems across the network from one central console.

• Monitoring and troubleshooting
  Redcell offers flexible alarm management and customizable event templates.

• Health management
  Redcell provides administrators with a variety of multi-protocol tools that allows for complete health management of the total infrastructure from a single console.

• Performance monitoring
  By selecting from the key performance counters available in Redcell, administrators can monitor and chart all of the key subsystems in the infrastructure.

• Remote access and control
  Via Redcell’s IPMI management interface users can view sensor data, receive SNMP traps and remotely control reboot, power cycling and power state.

• Multi-vendor and multi-technology support
  While Redcell offers the highest levels of integration and management support of Dell
datacenter resources, Redcell also offers the ability to manage other key Tier 1 vendors in the server, system, storage, and networking space.

For More Information

Dorado SOFTWARE

110 Woodmere Road, Ste. 200
Folsom, CA 95630
Tel: +1 916-673-1100
Fax: +1 916-673-1042
www.doradosoftware.com
sales@doradosoftware.com