Network Automation with the Dell Force10 Open Automation Framework

A Dell Technical White Paper

September 2011

Contents

Figures

The Open Virtual Data Center

It has been said that the shift to a virtual data center will be the most significant IT transformation since the invention of the mainframe. This transformation promises to join virtualized computing and storage layers to a virtualized network stack, while enabling new agile models such as cloud computing. At the same time, it is vital for the success of this technology that the transition to the virtual data center not bring back the proprietary restrictions and limitations that were the hallmark of the mainframe era.

While initial virtualization efforts have been very successful at consolidating server and storage resources, organizations and the industry in general are just beginning to understand how these virtualization initiatives will impact their data center networks. Many great minds and diverse organizations are grappling with the best ways to manage the virtualized data center – operating virtual machines, virtual storage, and virtual networking devices in concert to accomplish key application and business goals. Virtualization technology alone can easily result in more complexity – not less – and effective network automation technology is essential in order for the benefits of virtualization to be fully realized.

As with many technologies, some of the initial vendor-sponsored forays into the automation space have attempted to simplify the problem by providing single-source proprietary solutions. Networking vendors in particular have sought to revolutionize traditional data center operational practices with new architectures that work only with their servers and storage. In contrast, Dell realizes that for automation to be truly successful it must represent an evolutionary (rather than revolutionary) step – and it must work in concert with traditional datacenter operational practices.

Most large data centers are complex heterogeneous environments that require considerable customization around standard interfaces and protocols. Dell believes that the network should retain its customary role in automation – responding to orchestration requests from everything from applications, to hypervisors, to management frameworks. Through its Open Network Automation Framework, Dell is pioneering a model that delivers innovative, open standards-based automation technology that will enable organizations to transform their virtualized data center infrastructure – becoming more agile, flexible, and efficient even as they develop new ways to deliver applications and services.

The Promise of Virtualization – Realized Through Automation

To date, much of the adoption of virtualization technology has centered on consolidation, allowing organizations to better utilize and manage their computational and storage resources. Initial benefits of consolidation through virtualization have included:

- Better utilization of servers and storage
- Simple provisioning of virtual machines
- Workload balancing by deploying additional virtual resources

At the same time, most realize that consolidation is only the first step towards a virtualized data center. In particular, the adoption of server and storage virtualization is causing IT managers to examine how virtualization technology impacts their networks, and how the network needs to change to allow virtualization technology to realize its full potential. While most networks today remain relatively static – virtualized networks must become dynamic to match the characteristics of virtualized servers and storage.

In short, IT managers are grapping with two key questions:

- How does the network need to change so that it can function in this new virtual environment?
- How can virtual servers, storage and network elements be managed together in a cohesive synchronized virtualized environment?

Managing the Complete Virtualized Environment

In the past, servers, storage, and networking could all be managed separately, as they were treated as relatively separate domains. Increasingly, however, organizations need to consider how they will manage virtual machines (VMs), virtual storage, and virtual network devices in tandem to benefit the increasingly virtualized applications that they serve. Failure to embrace these challenges can actually result in far greater complexity and higher costs, easily outweighing the benefits obtained from earlier consolidation efforts.

For example, virtual sprawl has already become a sobering reality for many organizations that have embraced virtualized environments. A symptom of this larger management challenge, virtual sprawl can occur very quickly – much faster than physical server sprawl. Creating hundreds or even thousands of virtual machines is relatively fast and simple. Managing large numbers of virtual machines is more complex, presenting challenges that include:

- Tracking and managing large numbers of virtual machines
- Understanding where individual virtual machines are physically hosted
- Understanding who created or owns a particular VM
- Stipulating policy around VM creation, migration, resource allocation, or VM destruction
- Making sure that a migrating VM has access to its required networks, virtual LANS (VLANs), and data
- Securing new VMs by either mandating that a uniform access and protection template be applied to a new VM, or that a finely-tuned VM-specific profile be applied
- Locating stranded or orphaned VMs that never go away, while consuming valuable resources

Put simply, virtualization technology offers greater flexibility at the cost of increased complexity. Automation addresses the greater complexity caused by virtualization, reducing operational costs for large-scale virtualization efforts. Automation ultimately assists with real-time visibility and management of heavily virtualized environments, reducing risk through a policy-driven framework that helps eliminate human-generated errors.

Policy-based event management and enforcement of standard configurations help shorten the path to a tangible return on investments. The result can be improved availability as organizations are able to perform better network management, and remediation may be automated, where appropriate.

Toward Cloud Computing

Cloud computing technology in particular requires and assumes network automation in addition to virtualization. With cloud computing, resources need to be able to grow, shrink and move dynamically as demanded by the dynamic nature of the workload. For example, an overloaded application might need to be relocated to a different server with more CPU capacity. When this happens, the entire virtual environment would need to move as well, including:

- Storage connections
- Networking connections
- VLAN and port profile configurations

More than just moving the VM to a new machine, all of these connections would need to be redefined in advance on the switch where the new host for the VM is connected. Only then would the application have the same access, data, and management networks, and remain connected to the appropriate VLAN with all its previous QoS and security policies. Moves such as this need to be accommodated whether the application is being transported to a virtual machine hosted within the same rack, or across the data center.

Moreover, if these changes result in a network bottleneck, automation would need to allow network devices to respond by:

- Moving domains to encompass more servers or adding I/O
- Reserving bandwidth for specific applications
- Changing policies to prioritize applications
- Providing for multi-tenancy beyond the traditional limited static resource allocation

Customization in Large Complex Environments

Complicating the situation, effective automation must also be multi-level – allowing everything from applications, to virtual machines, to management systems to participate, as required by the data center. With the high level of customization prevalent in large data centers, it is important that data center managers have a way to define what they monitor and what they automate. Counter to a one-size-fits all approach, large organizations require the ability to customize their virtualization and automation solutions to fit their own unique needs.

In large data centers, there is also no presumption that any one vendor has a lock on the network, server, or storage infrastructure – and most are loathe to swap out their existing management infrastructure. Viable automation solutions must work with the established environment, interoperating with a wide variety of heterogeneous servers, storage, and networking equipment. Automation technology must also remain agnostic to hypervisor, virtual switch, and server choices, without artificial constraints that include or exclude any particular approach, vendor, or technology. Ultimately, data centers need to be able to own their own intellectual property, from custom-designed operational models to scripts that are used to achieve automation – requiring an open standards-based approach.

Choosing Open Automation

With automation technology still in the early stages, network vendors have taken a variety of approaches. In order to achieve an out-of-the-box operational model, some networking vendors have chosen proprietary architectures to simplify either the computing and storage stack or the network, or both. Unfortunately, these approaches ultimately constrain adopters to the innovations of a single vendor and limit the ability of the organization to customize their own environment. Different approaches to automating virtualized environments include:

- Vertically-integrated network automation. This approach involves a highly integrated proprietary architecture that requires the customer to source all elements of the stack (servers, storage, networking, management software) from a single vendor, or a closed system of vendors. This approach also usually assumes management of all layers of the operational stack by the network vendor – counter to modern data center practices.
- Network-controlled automation. In this approach, the monitoring, management, and provisioning of virtual environments is controlled from, or by the network, representing a huge cultural and operational shift by data center managers.
- Open network automation. Open network automation exploits open industry standards that allow the data center network fabric to be controlled by existing hypervisor or middleware tools. Because this approach is server and application centric (rather than network centric), it is consistent and tracks well with current data center operations.

Force10's Open Automation Framework

Dell Force10's Open Automation Framework is made possible through the ubiquitous Dell Force10 switch operating system – FTOS – that runs across all Dell Force10 switches and routers. By delivering the same operating system across its entire switch and router line, Dell Force10 ensures that organizations benefit from stable code, a consistent feature set, and simpler software management. FTOS also gives Dell Force10's switches an extensible and autonomous operational model that is essentially more like a server than a traditional switch. FTOS adds server-style intelligence and general programmability to Dell Force10's switches and routers, greatly extending their capabilities.

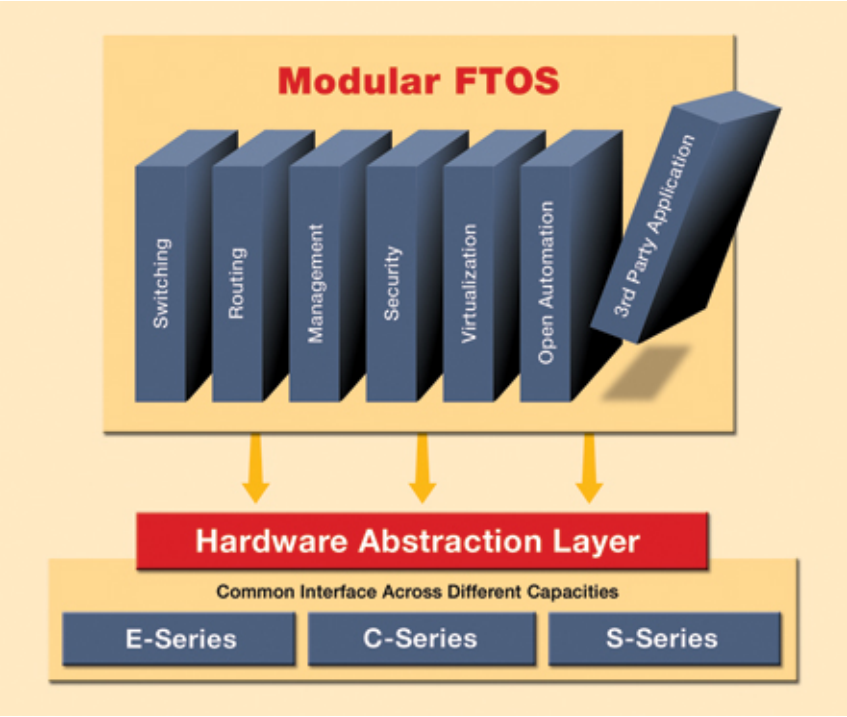
FTOS and the FTOS Command Line Interface (CLI)

An extensible and modular operating system, FTOS is based on NetBSD, with application code developed and maintained by Dell Force10 software engineers. FTOS supports everything from bare-metal switch provisioning to network virtualization, and also provides intelligence and extensibility that allows Dell Force10 switches to participate fully in customized automation. This unified approach offers the following distinct advantages:

- Common management functionality and a common user interface across the Dell Force10 product line make operating the network easier.
- Streamlined product training and a consistent learning curve result since system configuration, diagnostics, troubleshooting, and software maintenance are identical across all platforms.
- Support for the same CLI, SNMP, and XML management models is provided throughout the entire network, greatly simplifying life-cycle management for infrastructure.

A hardware abstraction layer (Figure 1) is used to make FTOS portable across product lines, allowing organizations to deploy applications across multiple switches and routers without recoding for each platform.

Figure 1. Based on NetBSD, the modular and extensible FTOS operating system runs across all Dell Force10 switches and routers.



The NetBSD kernel at the heart of FTOS provides a stable operating system, handling memory allocation and process scheduling, while all other applications run as independent and modular processes in their own protected memory space.

- Separate OS and application functions limit application scope, and provide inherent platform stability.
- Memory protection prevents processes from corrupting each other.
- Preemptive process scheduling prevents processes from monopolizing the CPU.
- Application processes are provided for each Layer 2 and Layer 3 protocol, as well as management functions, security services, and other FTOS functions.

The FTOS CLI is the primary method of managing an FTOS switch or router, and it supports interactive or automated logins using CLI scripting. The CLI is also responsible for communicating with the FTOS application process over inter-process communications (IPC) for sending configuration information or requesting output for a show command. The FTOS CLI combines industry-standard show, configuration, and debugging syntax with enhanced usability and navigation features. As a result, configuration and troubleshooting is similar to working on an IOS platform, but more flexible.

- The FTOS CLI is accessible over the serial console, or via Telnet or SSHv1/v2 for interactive or automated management.
- A “terminal xml” command enables an XML front-end to the CLI.
- Support for common tools such as Expect and RANCID is provided.
- Eventual integration of UNIX-like features such as “grep” and “diff” for scripting.

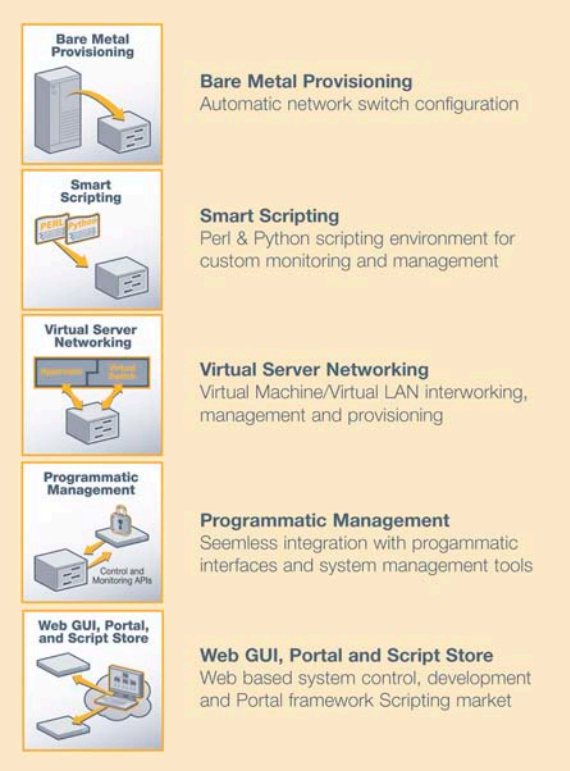
Open Automation Overview

Running on FTOS, Dell Force10’s Open Automation Framework (Figure 2) is designed to transform the data center network into a policy-driven cloud computing fabric, and to provide data center network

managers with greater visibility into how the network is performing. Open Automation incorporates Bare Metal Provisioning, Smart Scripting, Virtual Server Networking, Programmatic Management and Web GUI, Portal and Script Store, which streamline the network fabric's ability to participate in automated, policy-driven, real-time workload allocation in response to changing application and service demands.

The Open Automation and Virtualization Frameworks leverage the company's extensive Technology Alliance Partner Program that today includes more than 25 data center-focused technology partners. Coupled with Force10 technology, these partners provide the foundation for dynamic data centers by aligning compute resources with resource needs.

Figure 2. The Dell Force10 Open Automation Framework.



Bare Metal Provisioning

Automated bare metal configuration reduces operational expenses, accelerates switch installation, simplifies OS upgrades and increases network availability by automatically configuring Dell Force10 switches. This eliminates the need for a network administrator to manually configure the switch, resulting in faster installation, elimination of configuration errors and enforcement of standard configurations. Upon installation, the Dell Force10 switch searches the network for a DHCP server. The DHCP server provides the Dell Force10 switch with an IP address and the location of a TFTP server. The TFTP server maintains a configuration file and an approved version of FTOS, the operating system for Dell Force10 switches. The Dell Force10 switch automatically configures itself by loading the configuration file and FTOS.

Smart Scripting

Smart scripting increases network availability and manageability by allowing network administrators to deploy custom monitoring and management scripts on Dell Force10 switching platforms. With this capability, network administrators can implement version control systems, automatically generate alerts, create custom logging tools and automate management of network devices. Virtually any function that can be performed through the CLI can be implemented with smart scripting. Smart scripting provides a scripting environment that supports Perl and Python, making it easy for IT administrators to quickly develop scripts without having to learn a new scripting language.

Virtual Server Networking

Virtual environments require network infrastructure to be dynamic in order to ensure network connectivity and security policies are maintained when VMs are migrated. Virtual server networking facilitates communications between Dell Force10 network switches and virtual machinge management software to orchestrate automated VM/VLAN provisioning and virtual machine migration. This is a powerful capability that great simplifies the many of the tasks associated with virtualized computing environments. Our virtual server networking software supports VMware vSphere 4.0/4.1 and Citrix XenServer 5.6.

Programmatic Management

Programmatic management greatly improves network manageability by allowing Dell Force10 network devices to be managed by third party system management tools via standard programmatic interfaces. The programmatic management environment and set of interfaces communicate directly with third-party system management tools, avoiding the need for a dedicated network management tool.

Web GUI, Portal & Script Store

Ease and breadth of connectivity remains a paramount necessity for both equipment and development communities. The Web GUI, portal and script store address Web connectivity in general and encompasses two distinct elements: an advanced Web GUI and the OA Dev Exchange Portal. The advanced Web GUI is a significant step up from traditional web-based switching platforms interfaces. Retrieval and update of switch attributes and characteristics are present, but further, the ability to drag and drop changes to the GUI to provide customized skins allow for a level of customization and functionality not previously seen in a tool of this nature. Complementing this, the OA Dev Exchange portal (oadevexchange.com) provides an outlet for full user community interaction, development idea exchange and a script store where scripting products can be sold and development resources can be arranged and contracted.

Automation Use Cases

Organizations ultimately have highly diverse requirements for automation, and automation frameworks must be flexible enough to accommodate a wide range of automation activities. While a particular idea or approach may be advantageous to one organization, it might not be useful to another. Organizations may also choose to implement similar functionality in different ways depending on their own needs. The use cases that follow offer a number of practical examples for ways that the Dell Force10 Open Automation Framework could be used to accomplish a wide range of automation tasks. These descriptions represent only a sampling of the possible automation scenarios, and other approaches are certainly possible.

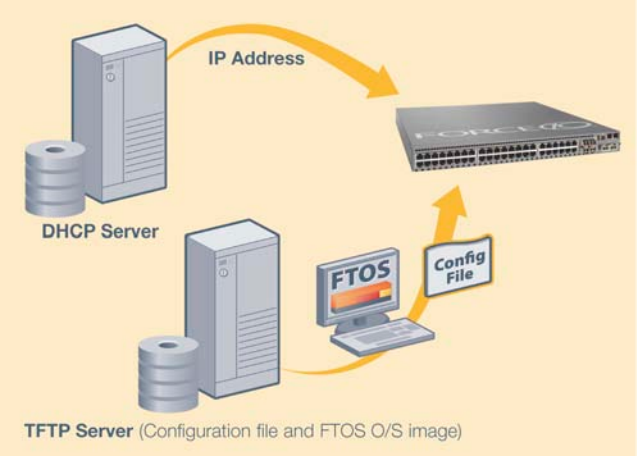
Bare-Metal Provisioning

When deploying or managing a large number of switches, it is often desirable to rapidly and automatically provision network resources. Doing so in an automated fashion helps to:

- Reduce deployment time
- Minimize human error
- Enforce standard and/or secured configurations

Similar to existing server capabilities, FTOS will allow switches to perform bare-metal provisioning – such as that supported on the Dell Force 10 S60 top of rack switch (Figure 3). Through this process, the switch can be configured with an operating system and a detailed configuration based on pre-defined templates. With the Dell Force10 Open Automation Framework, switches advertise their presence after connecting to the network, getting provisioned in return with an appropriate FTOS version, updated startup configuration, and an IP management address through a DHCP and TFTP server.

Figure 3. Bare Metal Provisioning configuration supports rapid provisioning of network resources.



Network Automation with Smart Scripting

Large complex data centers typically have their own unique needs and requirements for monitoring and managing their network infrastructure. Using Smart Scripting on Dell Force10 switches and routers, IT administrators can create custom PERL or Python scripts to manage and interact with their Dell Force10 switches and routers (Figure 4). A wide variety of automation tasks can be implemented, including:

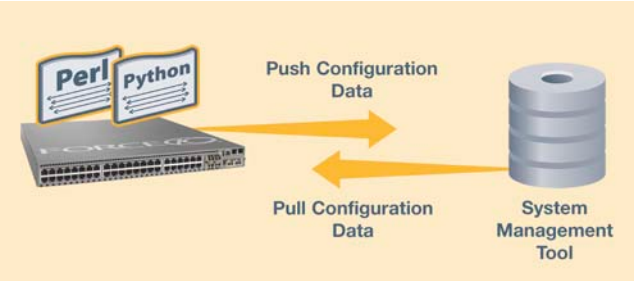
- Automating management
- Building visibility and/or discovery programs
- Creating custom logging
- Reporting configuration information
- Reporting switch memory usage, VLANs, etc.
- Producing custom interfaces with applications
- Supporting custom provisioning

Figure 4. Smart Scripting allows for a wide variety of automation activities to be implemented on Dell Force10 switches and routers.

Configuration Management

Keeping an up-to-date CMDB is critical and challenging, especially in large and complex networked data center environments. As shown in Figure 5, the Dell Force10 Open Automation Framework could be used to automatically send a notification if a switch configuration is changed. At the same time, configuration data could also be retrieved (pulled) from the CMDB to drive actual configuration and management of the switch. For instance, a central database of standard configurations could be maintained. When a change is made to the standard configuration, that configuration could then be pushed to all of the appropriate switches.

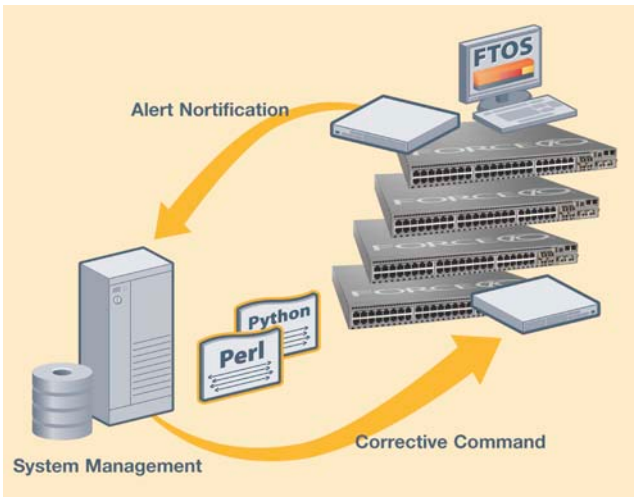
Figure 5. The Dell Force10 Open Automation Framework enables bidirectional communication of configuration data with third party system management tools.



Alert Notification

Proactively noticing and responding to outages and performance issues is vital, particularly in highly automated cloud computing environments. Using standard scripting, organizations use the Dell Force10 Open Automation Framework to build and deploy custom alert modules that notify management tools when network performance issues occur (Figure 6). System management tools or virtualization management tools are able to initiate responses to any issues based on pre-defined policies – potentially deploying additional resources or redeploying virtual machines.

Figure 6. Smart Scripting can provide alert notification from a Dell Force10 switch to third party system management tools.

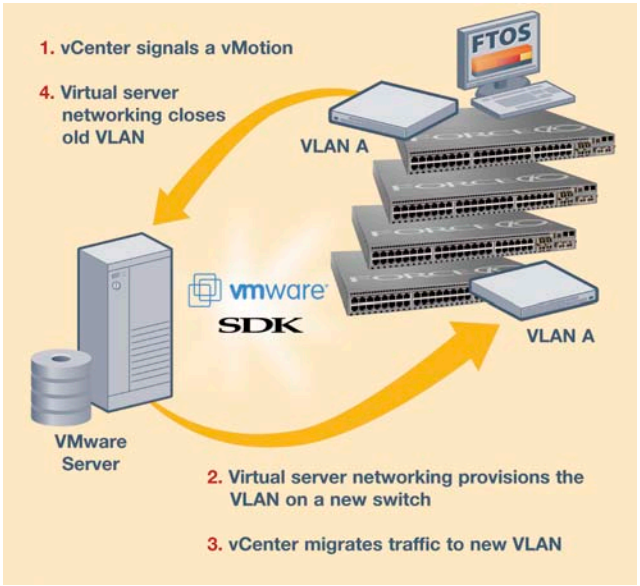


VM/VLAN Auto-Provisioning

For applications to operate seamlessly across a migration event, network configurations must become a part of the process. Associated VLANs must be made available on the physical switches where VMs will be located in advance of moving the virtual machines.

As shown in Figure 7, the Dell Force10 Open Automation Framework could be used with tools such as VMware Vmotion, configuring a VLAN and port on another switch to accommodate a virtual machine migration. In this scenario, a management application such as VMware vCenter would use VMware vMotion to move the virtual machine. In this case the VMware SDK would run directly on the Dell Force10 switch, registering with vCenter. When vCenter initiates a vMotion event, the switch is notified. The switch then provisions the appropriate VLAN and port profile, before the VM is migrated.

Figure 7. Virtual Server Networking communicates with hypervisor management tools, such as VMware vSphere, to coordinate VM and VLAN migration.



Conclusion

Deriving a return on virtualization investments means deploying effective automation techniques that can simplify the virtualized environment while allowing a policy-based deployment model. While many network vendors have chosen a proprietary path to automation, Dell Force10's approach is to utilize open and industry-standard technologies based on the extensible and modular FTOS operating system – across a range of the heterogeneous Dell Force10 switch and routers portfolio.

Rather than asking organizations to rethink their entire computing, storage, and networking stacks, Dell Force10 is committed to operating as seamlessly as possible as a part of the heterogeneous data center. This open and innovative approach gives large complex data center IT departments the control and flexibility they need to deploy powerful Dell Force10 switches and routers without disrupting the existing infrastructure, operations, or policies that drive their organizations – and their bottom lines.