Elastic application delivery services in the cloud

By Fred Johnson, John Von Voros, and Andrew Walker

Enterprises moving to cloud computing need agile, efficient application delivery. F5 Networks® and VMware® technologies integrated in Dell™-hosted cloud environments offer orchestrated automation and provisioning of application networking and security.

Many organizations are advancing strategic initiatives that help them grow their businesses by deploying virtualization and transitioning their data center operations to cloud-based application delivery models. As applications evolve and data-intensive workloads grow in size and frequency, IT organizations are experiencing elevated levels of complexity when managing applications and infrastructure through largely manual processes. As a result, many organizations are looking to expand automation in their IT environments as they take an application-centric view toward its management.

In virtualized and cloud computing environments, organizations have primarily focused their automation efforts on provisioning virtual machines. While this emphasis offers an important step in the deployment process, other equally important infrastructure components such as networking and security tend to be manually configured using separate processes, consoles, and tools. Organizations relying on disjointed deployment methods can experience operational inefficiencies that prevent them from realizing successful business outcomes from cloud computing.

Leveraging streamlined processes can create repeatable, reusable deployments that enhance the quality of the infrastructure. These deployments can also foster improvements that include short deployment cycles and few errors as well as help enhance availability, performance, and the capability to scale applications up and down to meet business demands.

Software-defined data centers

Now that many organizations are taking advantage of virtualization and cloud environments, the ability to automate services delivery allows for efficient provisioning of networking and security services. View this video to discover how integration of F5 and VMware technologies enables automation orchestration in software-defined data centers.

qrs.ly/bz2gcko

IT managers stand to gain added control over their computing environments when application delivery deployment and management is consistent, helps reduce operational costs, and enhances flexibility.

As organizations increasingly become comfortable with virtualization, many are adopting private and public cloud computing as the next step toward utilizing IT as a service. However, adoption of cloud-based platforms brings new challenges such as ensuring security, supporting streamlined end-user access, and maintaining adequate IT control over data and services.

F5 Networks, in conjunction with VMware, offers integrated solutions that enable organizations to implement a VMware vCloud® Ecosystem Framework environment for access to data traffic and workloads that facilitate elastic application deployments. Deep integration of F5 and VMware technologies creates a highly collaborative, responsive, and automated environment designed to deliver repeatable, reliable, and efficient deployment tasks. This integration enables organizations to help reduce operational costs so IT managers can effectively manage complexity and mitigate operational risks, such as deployment errors, that may impede productivity and application availability.

Orchestrating automation and provisioning

VMware vCloud Ecosystem Framework allows third-party partners to integrate with orchestration and provisioning processes, which now include networking and security services. F5 Enterprise Manager™ (EM™) software integrates with vCloud Ecosystem Framework through bidirectional, representational state transfer (REST) application programming interface (API) communications. In effect, this integration has created a combined management plane for F5- and VMware-provided services.

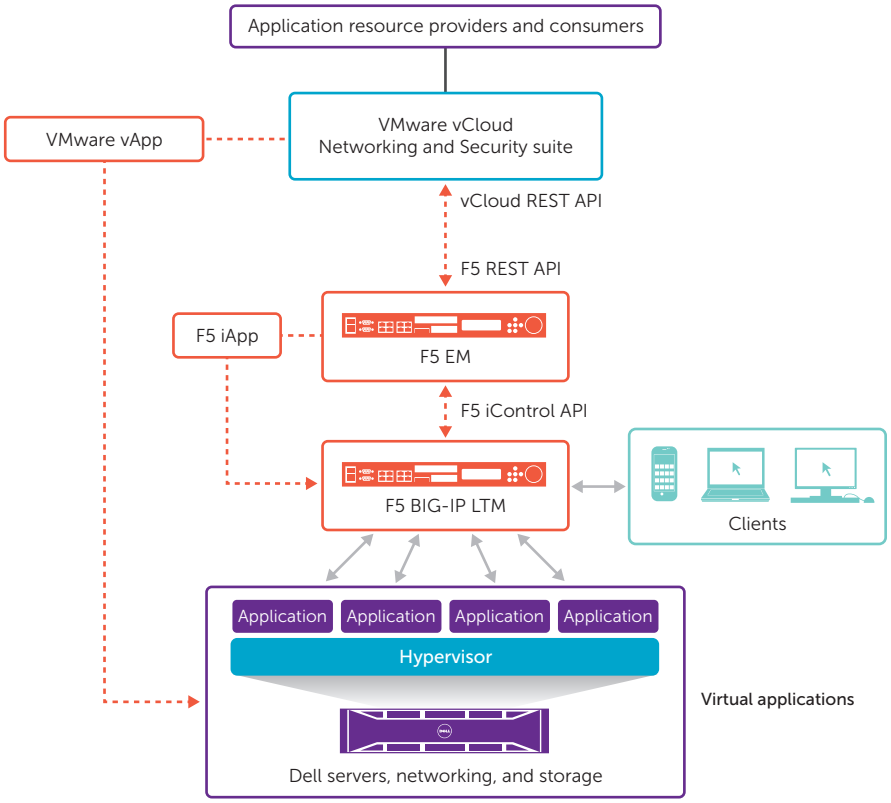

Figure 1. Integration points for F5 Networks technologies within the VMware vCloud Ecosystem Framework environment

F5 technology provides a critical link between the infrastructure and the deployment of applications on top of that infrastructure. vCloud and provisioning and automation capabilities through vCloud APIs in the F5 BIG-IP® suite tie together the applications, application hosting, and the infrastructure to bridge many gaps that have existed. Well-orchestrated automation facilitates the scalability to support virtualization and cloud computing, and efforts from F5—including application delivery networks (ADNs)—and VMware have yielded advancements that directly support the transition that is underway for software-defined data centers.

When provisioning workloads in a vCloud environment, administrators, or business users utilizing self-service implementation, can now provision the network and security services that F5 provides. To provision an application in vCloud using F5 services, an end user first selects a VMware vApp—an application template—from a catalog and then selects an F5 iApp—an infrastructure template—from a services catalog (see Figure 1). VMware vCloud Director can then be deployed to provision and configure VMware and F5 components at the same time and push the changes out to both environments.

VMware vCloud Networking and Security communicates with EM by utilizing APIs to call the specified iApp templates that provision networking, security, resource pools, monitoring, and other necessary application delivery components. EM signals the appropriate BIG-IP units over the F5 iControl® API to execute the iApp template configuration. The processes are completed, and the vCloud systems receive a status on

the changes. This simplified process is designed to get enterprise-level applications up and running in a short amount of time and with few errors.

Over time, EM shares application health updates with the vCloud systems so that it can react appropriately to changes in the environments. If virtual machines are added or removed from the deployment, for example, the F5 iApp runs again automatically to make adjustments to the application networking and security configurations.

By creating repeatable processes, helping eliminate operational inefficiencies, and leveraging vCloud integration with F5 technologies, organizations can minimize time to deployment, human error, operational overhead, and costs. Additionally, consistent application policy implementations help improve overall security posture, end-user experience, and availability, among other benefits.

Deploying robust, integrated cloud computing

Dell vCloud software offers an enterprise-class, multitenant infrastructure-as-a-service (IaaS) public cloud. This cloud infrastructure is hosted in secure Dell data centers. Its hybrid cloud capabilities enable organizations to extend internal data centers by transitioning VMware virtualized workloads to Dell data centers. And options for integrated application delivery and load balancing in the Dell public cloud provide a robust set of services that easily support on-demand application infrastructures.

In addition, many enterprises need on-demand scalability by expanding, or bursting, to external cloud services while helping maintain strong security and high availability in the process. A range of F5 technologies offers the key ingredients designed for creating and maintaining secure, scalable, multitenant private, hybrid, and public cloud services that can be up and running 24/7 (see Figure 2).

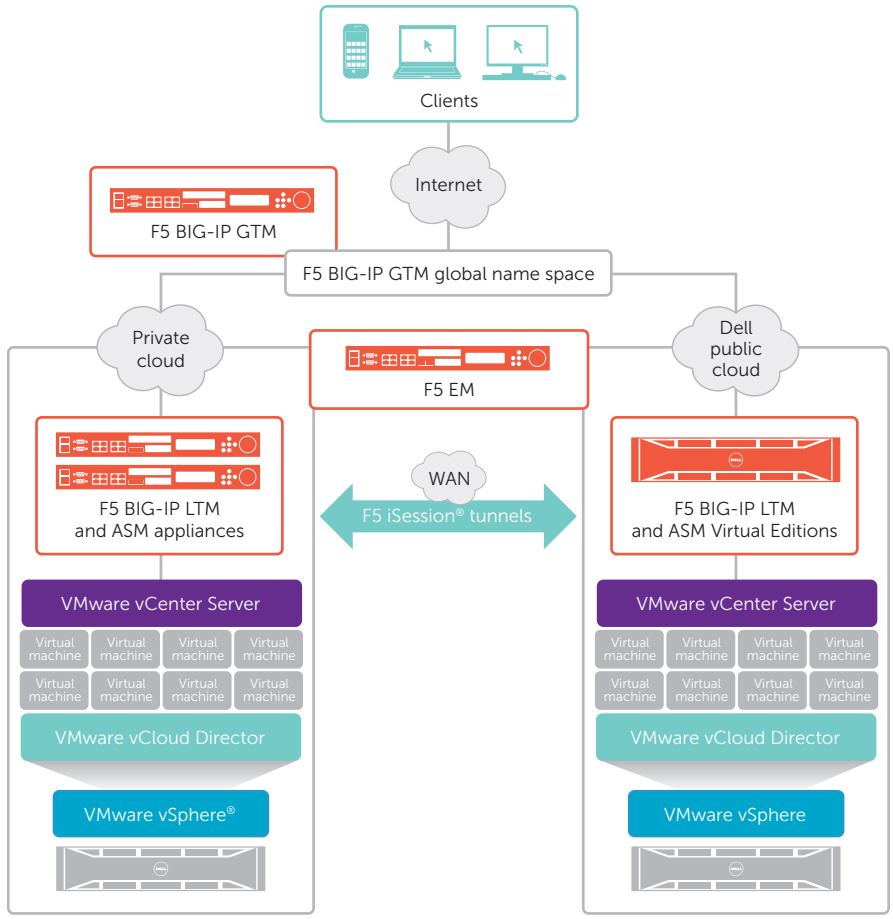

Figure 2. A hybrid cloud data center that leverages Dell public cloud computing services and technologies from F5 Networks and VMware

Designed to leverage a flexible, high-performance application delivery and server load-balancing system, the F5 BIG-IP Local Traffic Manager™ (LTM®) application delivery controller (ADC) can increase operational efficiency and help ensure peak network performance. BIG-IP LTM and its application-centric perspective help optimize network infrastructure for high availability and for security, network, and distributed denial-of-service (DDoS) attack protections.

Protecting business-critical applications is paramount for organizations. F5 BIG-IP Application Security Manager™ (ASM™) software protects mission-critical applications with an agile, Web application firewall (WAF) that is certified by ICSA Labs[1] and offers comprehensive policy-based security. Offering threat assessment and mitigation, Payment Card Industry Data Security Standard (PCI DSS)–compliance reporting, visibility, and high levels of flexibility, BIG-IP ASM is designed to deliver a high-performance WAF that secures applications in traditional, virtual, and cloud computing

[1] For more information on ICSA Labs, visit icsalabs.com.

environments. Dell SecureWorks, an enterprise-level security services provider, offers managed security services for BIG-IP ASM to help simplify WAF management.[2]

F5 BIG-IP Global Traffic Manager™ (GTM™) systems create a global name space—for example, http://app.example.com/—that is an essential element for stitching together applications that are hosted across multiple or hybrid cloud data centers. Client systems can reference the same Domain Name System (DNS)–assigned name to request an application, regardless of the device type or location. This function helps significantly improve the performance and availability of applications by intelligently directing users to a nearby, optimal-performing, or highly available data center. The system offers a dynamic, policy-based DNS provider that allows for granular traffic management. Using high-performance DNS services, the system scales and secures the DNS infrastructure from DDoS attacks, and it can deliver a complete, real-time DNS Security Extensions (DNSSEC) solution.[3] Redirecting clients to recovered applications can be fully automated with VMware vCenter™ Site Recovery Manager (SRM) software.

F5 EM facilitates managing the application delivery infrastructure in a centralized console that enables VMware vCloud Director to instruct BIG-IP devices to deploy application delivery policies. The system maintains two-way communications between VMware systems and the F5 ADC infrastructure that is providing configuration and monitoring services.

Optimizing application delivery and management

The integration of F5 technologies and VMware vCloud helps deliver a consistent, repeatable, and reliable deployment process by enabling automation and giving organizations the visibility needed to react to environmental changes. This virtualized, integrated infrastructure automates the implementation of best practices and security policies to help improve productivity in addition to automating compliance with organizational policies. Leveraging tight integration and key technologies, such as F5 ADNs, helps accelerate cloud computing implementation for achieving successful business outcomes.

F5 technologies integrated with Dell-hosted public cloud platforms that deploy compatible VMware tools offer seamless interoperability for provisioning servers, security, and application networking. By blending application management and application delivery services into a reusable and optimized deployment process, organizations can benefit substantially from enhanced virtualization and cloud computing efficiency. PS

Authors

Fred Johnson is a partner engineer at F5 Networks dedicated to Dell Labs, sales, and Dell technology services.

John Von Voros is a product development manager with over 15 years of experience in Dell technical marketing.

Andrew Walker is a solutions design engineer at F5 Networks focused on Dell technology services worldwide.

Learn more

Dell public cloud services:
qrs.ly/tf2gcky

F5 and VMware vCloud Director:
qrs.ly/nm2gcl2

Operationalizing elastic applications:
qrs.ly/jg2gcl5

Enhancing cloud environments:
qrs.ly/1r2gcln

Automating network provisioning

Software-defined data centers can take advantage of virtualization advances to facilitate provisioning of network resources with the same efficiencies as provisioning servers and storage. View this video to learn how F5 BIG-IP suite integration in VMware networking and security solutions enhances automation and provisioning capabilities.

qrs.ly/jc2gckw

[2] For more information on how Dell SecureWorks provides managed WAF security services for BIG-IP ASM, see "Rock-solid protection for Web application delivery," by Fred Johnson, Allen Vance, and Andrew Walker, in *Dell Power Solutions*, 2012 Issue 3, bit.ly/RItz5M.

[3] For more information on directing end users to optimal data centers using BIG-IP GTM, see "Intelligent Domain Name System resolution for application delivery," by Andrew Walker and Fred Johnson, in *Dell Power Solutions*, 2011 Issue 2, bit.ly/jNK8OF.