Tech Brief

Enabling IT Agility with the F5 BIG-IP System and the VMware vCloud Platform

Data center virtualization has reached maturity, and users are now looking for ways to implement virtual infrastructures to continue the migration of virtualization to private cloud. This demand, driven by the ease of infrastructure implementation and the promise of reduced human error, is met by F5 and VMware integrated solutions.

Contents

Introduction

Over the last several years, server virtualization has helped enterprise IT become more adaptable and efficient by reducing the time required to deliver new servers from months to days or even hours. The ability to augment compute resources by spinning up an image in a VMware vSphere environment has led to faster deployment, more standardized imaging, and fewer IT man-hours invested in preparing and delivering a new server for business use.

However the operational efficiency gained by automatically provisioning compute resources is mitigated by the fact that organizations still must manually provision the different infrastructure services needed to optimally utilize this extra capacity. The resultant network configuration is much more complex than with traditional provisioning, as network personnel have to be aware of all the multi-tenancy and other security parameters associated with the particular network.

VMware and F5 have taken extraordinary steps to lighten the load on operations staff by automating the deployment of an application workload and deploying the network services needed to optimally utilize the application. Most recently, VMware vShield Manager has been updated to help deploy network services on demand for application servers.

The F5 and VMware Partnership

F5, working with VMware through a long-standing partnership, has integrated its BIG-IP Application Delivery Controllers with the VMware vShield environment to automate the provisioning of network components required to support a virtual application (vApp) cluster of VMs. By leveraging the VMware Ready for Networking and Security Program, F5 and VMware have created a solution that helps drastically accelerate the Application Delivery Networking process from weeks to minutes.

This joint solution not only automates the deployment of complex networking services, but also puts in place best practices and processes to ensure data center compliance with regulatory requirements.

The ability to deploy network resources such as load balancing, virtual IPs, DDoS protection, and SSL offload (to name a few) without having to manually instantiate and configure all of the different services brings automated network provisioning in

The BIG-IP system already improved VM density gains, now eases delivery pain

88% of IT organizations improved VM density between 10% and 40% on a typical server with F5.

Source: TechValidate Survey of 105 F5 BIG-IP users
TVID: 975-FFD-F8D

line with the automated provisioning of other critical VM resources such as memory and storage.

The ADC Control Interface

To achieve automated network resource provisioning, several systems and subsystems must interact. The prerequisites for vShield Manager to effectively manage and monitor Application Delivery Controller (ADC) objects in conjunction with a VM are:

- vShield Manager must be in use within the enterprise.
- F5® Enterprise Manager™ must be deployed on the network with access to the relevant F5 BIG-IP® devices.
- F5 Enterprise Manager and the services provided must be registered as a service provider in vShield Manager.
- A VMware vApp template must be configured in vCloud Director to interface with F5 Enterprise Manager.
- One or more F5 iApps™ must be implemented in Enterprise Manager that exposes the necessary portions of network object configuration for the vApp to manipulate.

To find out about iApps and how it fits into the F5 architecture, read F5 iApps: Moving Application Delivery Beyond the Network.

Configuration

First, operators inform vShield Manager that Enterprise Manager is available to service provisioning requests, what types of requests Enterprise Manager can service, and what iApps Templates are available. A link between vApp templates on vShield Manager and iApps Templates on Enterprise Manager is then created. As an intermediate step, vShield Manager verifies the capabilities and availability of Enterprise Manager.

Application Deployment

When a vApp template is utilized to deploy an application, the questions that would normally be asked and answered in the iApps interface on Enterprise Manager are instead asked within vShield Manager as part of the deployment. vShield Manager then calls the iApp and provisions all of the appropriate network resources by executing the iApp with the values the operator has supplied.

Application Modification

When operations needs to modify the vApp parameters, vShield Director tells Enterprise Manager to execute the iApp again, modifying changed elements, removing unused elements, and creating any new elements required.

Normal Monitoring

During normal operations, the health of the network architecture deployed through this mechanism is available as a summary item in the vShield Director management screen. This provides a single point of reference for the state of the VM throughout its lifetime.

Implementation Details

At the core of this F5 and VMware integration that brings networking elements into the sphere of virtualization control is a REST API that allows F5 Enterprise Manager to register the services it provides with vShield Manager. Configuration information flows from vShield Manager into Enterprise Manager, and status information flows back to vShield Manager on a regular basis so that vShield Manager can accurately portray the state of the network.

Behind this interface there is another layer on the networking side. Enterprise Manager is acting as a high-speed gateway to all of the BIG-IP devices being utilized by the virtualization architecture. Enterprise Manager uses the core F5 iControl® programmatic interface to implement the changes in BIG-IP devices as vShield Manager requests them. iControl is a SOAP-based API and software development kit that allows fine-grained access to the objects, rules, and properties that make up BIG-IP networking interfaces. By making a series of iControl calls, Enterprise Manager can place an iApps Template onto a BIG-IP device, run the template, and fill in the necessary fields, thus creating all of the objects necessary to have the Application Delivery Controller be a part of the extended VMware network.

For larger corporations and service providers, iApps Templates offer unparalleled standardization. If the InfoSec team has a standard set of policies that must be applied to all public-facing websites, they can implement those policies through a standardized iApp and use it as the basis for all public-facing applications—so all of those applications will use the policy automatically. Furthermore, by creating a few slightly different iApps, larger organizations can have customized, easy-to-deploy solutions for their varying customer base—for instance, different formats for different customer levels such as gold, silver, and bronze support levels. If one business unit uses Microsoft IIS for web serving but another always utilizes Apache, administrators can save two iApps that are generally the same but customized for the unique needs of each application. By using these iApps, administrators minimize the risk of misconfiguration due to confusion about which settings are best for each solution.

Extending these iApps out to interface with VMware vApps means that not only are there preconfigured custom solutions to meet varying customer needs, but those solutions are integrated directly into the VMware deployment and control interfaces. This further simplifies deployment by providing a single point for administrative staff to touch in order to generate all of the resources they need for application deployment. It is even possible to limit what iApps a given user sees, allowing customized processing for customers or business units without accidental deployment of the wrong iApp.

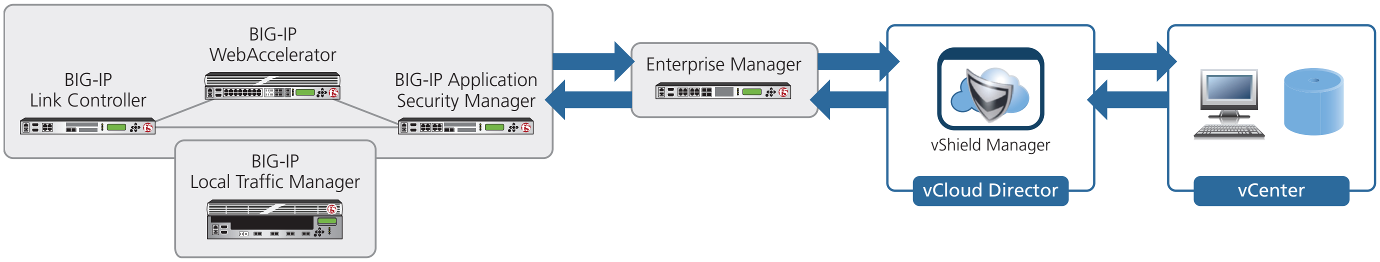

Figure 1: Intra-infrastructure integration in this VMware and F5 architectural solution enables application deployment automation and health monitoring.

Some information required by Enterprise Manager to deploy network resources—such as the IP addresses of servers that will be load balanced—will not be available until after some of the VMware provisioning has occurred. In these cases, vShield Manager will deploy the other portions of the vApp and only call Enterprise Manager to complete the network portions after all necessary information is available. This limits deployment errors and the need to run the iApp on Enterprise Manager multiple times, ensuring that the network objects have all the information they need to run effectively, whether they implement security, balance load, or optimize traffic.

Conclusion

The joint solution that F5 and VMware have partnered to deliver increases the efficiency of IT, improves IT infrastructure agility, and ensures business applications comply with standards. Enterprises and service providers can now offer F5 ADC functionality to application owners from within vShield Director with different service levels for application and multi-tenant environments. The solution not only optimizes the provisioning process, but also brings to bear the advantages of delivering an application in a cloud as a service. As an Elite Technology Alliance Partner with VMware, F5's integration with VMware technology is a team endeavor, guaranteeing support from both organizations for users.

By taking the next step in network evolution, organizations embrace deploying supporting network resources along with the applications they deploy. This greatly reduces the burden on IT, improving both the quality and quantity of support IT is able to offer the rest of the organization.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com