



TRACE3

Tech Brief

Enable a Scalable and Secure VMware View Deployment

A FlexPod data center design complemented by F5 ADCs supports a scalable VMware View solution, as demonstrated and validated by Trace3 and F5.

Matt Quill

Principal Solutions Engineer, F5 Networks

Kevin Martin

Solutions Architect (VMware Specialist), Trace3

Jared Lutgen

Solutions Architect (NetApp Specialist), Trace3

Greg Spencer

Solutions Architect (Cross-Platform Solutions Specialist), Trace3

Erik Durand

Practice Director (Virtualization and Advanced Data Center Infrastructure Offerings), Trace3



Contents

Introduction	3
<hr/>	
How FlexPod and F5 Technologies Enable a Scalable and Secure VMware View Deployment	4
Performance and Scale of VMware View	4
Storage and Infrastructure Efficiency	4
Access and Authentication	5
Replication Acceleration	5
Rapid Deployment	5
<hr/>	
Environment Setup and Configuration	6
FlexPod and BIG-IP Device Setup for VMware View 5.0	7
F5 Prerequisite Setup and Configuration	10
NetApp Environment Setup	11
Setup of the ESX Server Environment	11
<hr/>	
Validation of VMware View 5.0	12
Local PCoIP and RDP	12
SSO Remote Access via BIG-IP APM	13
<hr/>	
Conclusion	13



Introduction

NetApp® and Cisco® have collaborated to provide a validated data center architecture built on the FlexPod™ data center design. This solution accelerates the overall deployment of virtualized Tier 1 applications, enables rapid data center transformation, and accelerates the deployment of new, mission-critical applications such as VMware View. Thus equipped with the flexibility to customize or modify the computing, storage, or switch components in the architecture, enterprise customers now have a fully validated means to dramatically reduce the design and deployment phases of their application environments.

As a complement to the FlexPod validated architecture, F5® BIG-IP® technologies can enhance application performance, ensure application availability, and provide the secure access and remote user authorization necessary for deployment of a virtualized Tier 1 application environment. Deploying VMware View 5.0 on a FlexPod architecture with an F5 Application Delivery Controller (ADC) can extend and enhance the value of FlexPods in a virtual desktop environment. Detailed deployment guidance, which is available through the partnership between F5 and Trace3, supports all aspects of configuration, including that required for the storage, computing, ADC, and application deployments.

About Trace3

Trace3 is a NetApp Star partner and F5 Platinum partner that helps organizations overcome obstacles by partnering with them to develop a strategic approach to meeting business requirements through IT innovation. Trace3 accomplishes its goals through an XARCH® approach, providing a strategic roadmap for IT across three practice areas—data center, user computing, and cloud strategies. Through these practices and disciplines, Trace3 provides a customized roadmap encompassing XARCH Solutions, which allow clients to optimize existing investments while increasing the utilization of human capital and equipment. Trace3 solution sets include products, consulting, training, and resource management in a variety of discipline areas, namely storage, networking, virtualization, security, data protection, applications, and project management. Expertise in all of the relevant components of the enhanced FlexPod architecture enables Trace3 to add strong value to any large enterprise deployment of a turnkey FlexPod solution.



How FlexPod and F5 Technologies Enable a Scalable and Secure VMware View Deployment

Performance and Scale of VMware View

One major challenge to large-scale adoption of VMware View in the enterprise has been the ability to effectively scale the infrastructure components necessary to meet the performance characteristics of a virtual desktop deployment. When designing an overall solution, enterprise architects must accommodate unexpected spikes in performance demand. To accelerate performance and improve the overall user experience of virtual desktops, NetApp and F5 Networks provide critical infrastructure components that enable a virtual desktop environment to scale while maintaining a superior user experience. F5 ADCs improve responsiveness by offloading CPU-intensive processes such as managing SSL traffic, pooling connections to back-end servers, and allowing for adaptive compression of traffic to increase overall performance by up to 60 percent.

A similar improvement in performance may be achieved using NetApp Flash Cache storage acceleration technology. An overall solution that incorporates both F5 and NetApp technologies enables a virtual desktop infrastructure (VDI) deployment that can scale more efficiently. From a storage perspective, this means substantially fewer spinning disks in the overall infrastructure.

Storage and Infrastructure Efficiency

NetApp has pioneered storage efficiency technology to enable enterprises to realize higher levels of performance with less provisioned physical storage. Embedded features such as deduplication, thin provisioning, compression, and Flash Cache acceleration can provide dramatically improved performance while, at the same time, reducing the storage footprint as well as power and cooling costs.

BIG-IP products provide similar efficiencies at the hypervisor and application level. The BIG-IP platform is central to increasing virtual server density by offloading CPU intensive process from the server. Features such as adaptive compression, SSL offload, and connection pooling can increase server density by up to 60 percent, again reducing the footprint of the deployment. As a result, enterprises can more



effectively deploy Tier 1, mission-critical applications in a virtualized environment that complements the validated NetApp data center architecture.

Access and Authentication

With an increasingly mobile and distributed workforce, enterprises and service providers need a way to securely manage access for remote users working with web-based applications. BIG-IP® Access Policy Manager™ (APM) provides a unified access and authentication platform for both remote users and those authorized in the data center. The SSL VPN remote access security provided by BIG-IP APM offers the highest performance available in the market today and scales to over 100,000 users on a single device. BIG-IP APM recognizes user location and securely authenticates local or remote access for users requiring secure access to applications. Using BIG-IP APM in place of the View security server in a VMware View deployment enables access and authentication for up to 100,000 users.

Replication Acceleration

NetApp SnapMirror provides asynchronous replication to a secondary NetApp storage controller to maintain a reliable and efficient disaster recovery environment. To optimize the performance of the WAN link between sites and improve the overall efficiency of replication, source-based deduplication and compression can be initiated on the NetApp device before the replication takes place. Where latency or packet loss is an issue, a BIG-IP® WAN Optimization Module™ (WOM) can optimize, prioritize, and accelerate the replication traffic, reducing overall WAN bandwidth requirements.

Rapid Deployment

In deployments of virtual desktop software like VMware View, the essential NetApp value proposition includes the ability to rapidly deploy hundreds or thousands of virtual desktops with individual customizations and minimal impact on server resources. Using NetApp FlexClone technology, enterprises can rapidly provision thousands of desktop images with individual customizations through a simple click of the mouse. Tightly integrated into VMware vSphere, FlexClone rapidly provisions tens of thousands of desktop images in minutes with zero increase in overall storage utilization.

An additional challenge to deploying large-scale infrastructures is integrating each component into the infrastructure. NetApp provides certified partners with detailed FlexPod guides that rapidly reduce the time needed to deploy this validated data



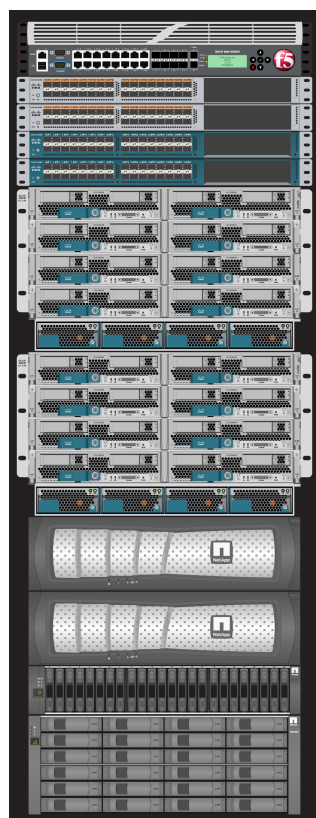
center solution. FlexPod technology not only reduces the time to deploy the physical infrastructure components, but also dramatically reduces the time typically required to test and validate each component. With a validated architecture for storage, computing, and Layer 2 networking, enterprises can reduce the overall time needed to test multiple components to ensure interoperability. Certified NetApp partners such as Trace3 are armed with the appropriate tools to size and adequately configure a FlexPod so that it can scale to meet application and user workloads.

Eliminating complexity and speeding deployment are crucial to the ultimate success of a VMware View solution. FlexPod deployment guides are complemented by F5 deployment guides, which together enable deployment of an Application Ready Solution across platforms.

F5 iApps™ Templates further reduce deployment times. These menu driven, customizable, reusable, and application-specific templates enable administrators to deploy the necessary elements of an ADC solution without requiring expertise in the associated BIG-IP product modules. iApps Templates are reusable, and many existing iApps for specific needs are available for sharing via the F5 DevCentral™ development community. Administrators can also code and configure their own iApps for deployment of non-standard applications with F5 ADCs. The standard iApps Template was used to configure all the necessary components for the VMware View 5.0 environment.

Environment Setup and Configuration

The validation was designed to proceed in two phases and demonstrate both local user connections and remote access to a virtual desktop environment. The validated NetApp environment used both a storage area network (SAN) as well as network-attached storage (NAS) to provision storage to the Cisco Unified Computing System (UCS) blade server components. Each controller in the NetApp architecture had two 8 GB Fibre Channel ports as well as two 10 GB Ethernet ports connected to the Cisco UCS. For purposes of installing and booting the VMware ESX hosts, storage was provisioned via Fibre Channel. The guest storage and virtual desktop were provisioned from NetApp over NFS. NetApp FlexClones were used to rapidly deploy VMware View virtual desktops.



BIG-IP 8900

Nexus 5540A Switches

Cisco 6248UP Fabric Interconnects

Cisco UCS 5108 with B200 Blades

NetApp 3240A Controllers

DS4243 Shelf 1TB SATA

2246 600GB SAS

Figure 1: Physical components in the FlexPod test

FlexPod and BIG-IP Device Setup for VMware View 5.0

To thoroughly validate the value of the combined BIG-IP APM/FlexPod solution, a 10 GB capacity solution was deployed with the FlexPod. Phase One of the deployment used a BIG-IP 8900 appliance licensed for BIG-IP® Local Traffic Manager™ (LTM) as well as BIG-IP APM. Both 10 GB interfaces were configured on the device and plugged into the Nexus 5548 switches.

<input checked="" type="checkbox"/>	UP	3.1	00:23:e9:00:de:dc	10000	1
<input checked="" type="checkbox"/>	UP	3.2	00:23:e9:00:de:dd	10000	1
Enable Disable					

Figure 2: Configuration of the 10 GB interfaces

One NetApp controller was configured with a 10,000 RPM SAS disk shelf and the other was provisioned with 1 TB of SATA storage. The ESX hosts were configured to boot from SAN storage using the SATA storage, and the SAS storage was



provisioned to support the VMware View desktop environment. Configurations included five View Connection Servers to which the BIG-IP device would direct user traffic. All users would access their virtual desktops via the virtual server on the BIG-IP device as opposed to accessing the five View Connection Servers directly. Two ESXi servers were configured to support the virtual desktop pools.

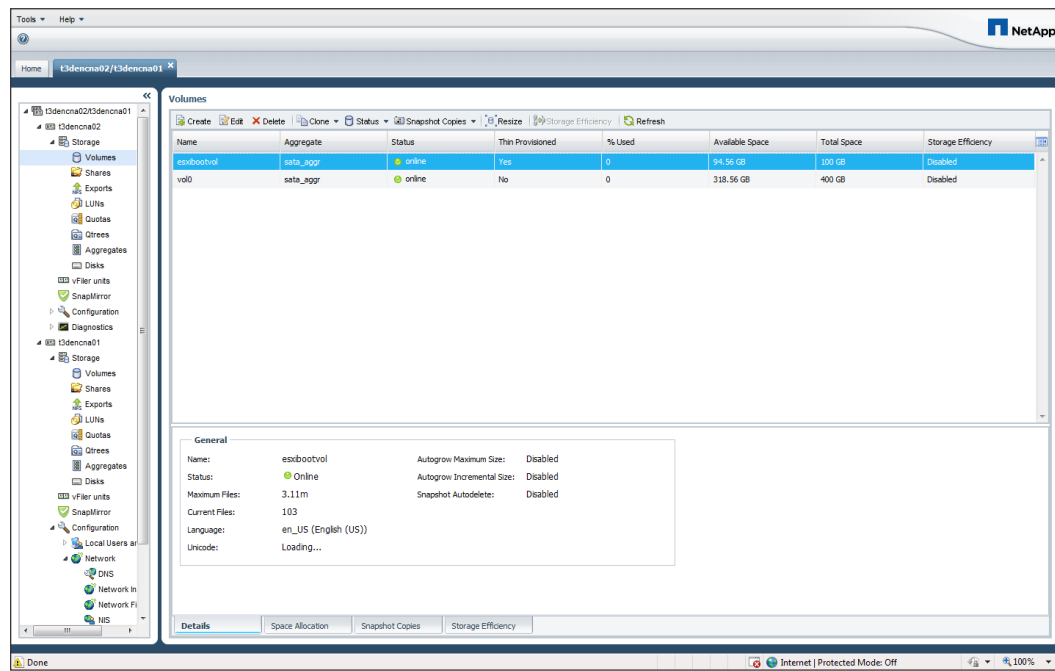


Figure 3: The new NetApp on-command configuration interface showing the 10,000 RPM SAS aggregate storage

To simulate a real-world deployment of a virtual desktop infrastructure (VDI), configuration included two separate virtual desktop pools, one to allow access via PCoIP and the other to allow connections via Microsoft Remote Desktop Protocol (RDP). The purpose was to demonstrate local user connections to a virtual desktop environment via both protocols. The second phase of testing validated remote user access to the VDI environment via BIG-IP APM. In both scenarios, BIG-IP LTM provided basic traffic management and load balancing of the View Connection Servers.

The BIG-IP 8900 device was deployed with software version 11.1 hot fix (HF) 1 to support iApps functionality. The NetApp 3240 controllers were installed with ONTAP 8.1 7-mode RC3. VMware ESX 5.0 was the hypervisor used during all phases of the testing, and vSphere was used to manage the ESX hosts and provision NetApp FlexClones.



QTY	Item	Description	Notes
2	NetApp FAS3240AE	NetApp FAS Controllers	Redundant NetApp FAS controllers for FlexPod architecture
1	DS2246	SAS 600 GB, 10 K RPM, 6 GB disk shelves	High performance disk storage
1	DS4243	SATA 1 TB, 7200 RPM disk shelves	Denser, lower-performance disk storage
2	Flash Cache Module	Flash Cache 512 GB PCIe Module	Flash Cache acceleration technology
2	Cisco UCS 5108	Cisco UCS Chassis	4 B200 blades in chassis used for the purpose of this test
4	Cisco B200 Blades	Cisco Blade Servers	Blades used only in top chassis
2	Cisco Nexus 5548UP	Nexus Unified Switch	Block and NFS connectivity
	Cisco UCS 6248UP	Fabric Interconnects	Network fabric and compute environment management system
1	F5 BIG-IP 8900	BIG-IP LTM and BIG-IP APM	Application delivery and access and authentication

Figure 4: Physical hardware components in the FlexPod and F5 lab setup

To demonstrate the NetApp rapid provisioning of virtual desktops, the test utilized the NetApp plug-in to VMware vSphere to provision 40 separate desktops spread across two separate desktop pools. As FlexClone does not utilize the CPU of the ESX servers, the process of rapidly cloning multiple virtual desktops took only minutes to complete, customize, and boot in ESX.

Each desktop pool was configured to allow separate groups of user logins that would simulate a multi-departmental VDI deployment. For example, users view1 through view6 were configured to have access to pool1 and access their desktops via PCoIP. Users viewRDP1 through viewRDP6 were configured to access desktops in pool2 via RDP.

For this purpose, there were 2 VLANs configured—an internal-facing VLAN for network connections to the back-end View Connection Servers and an external-facing VLAN for client connections. Two self-IP addresses were configured and assigned to each VLAN. While this demonstration environment used the default certificates, for a full production deployment of VMware View on FlexPod, procurement of an SSL certificate from a certificate authority is recommended.



F5 Prerequisite Setup and Configuration

The testing plans encompassed two phases. In the first, only BIG-IP LTM would be deployed via an iApp template to show a hybrid PCoIP and RDP local desktop environment. The second phase combined a scenario where a remote user would receive authentication via BIG-IP APM and access a desktop via single sign-on (SSO) authentication. The additional components specific to BIG-IP APM were configured and generated using the iApp template.

Licenses for both BIG-IP LTM and BIG-IP APM were obtained. Once basic licensing and network/VLAN configuration was completed, all additional configuration was performed using the appropriate iApp template.

Template Selection: Advanced	
Name	F5_VMWARE_View_FlexPod
Template	f5.vmware_view_5.2012_03_07
Device Group	<input checked="" type="checkbox"/> Inherit device group from current partition / path device-group-failover-1259171d665d (Sync-Failover)
Traffic Group	<input checked="" type="checkbox"/> Inherit traffic group from current partition / path traffic-group-1 (floating)

Web Traffic	
How should the BIG-IP system handle encrypted application traffic?	Decrypt HTTPS traffic (SSL Offload)
Critical	This selection is ONLY compatible with VMware View 4.6. If you are using VMware View 5.0, you must select SSL Bridging.
Description	The BIG-IP system accepts encrypted (HTTPS) traffic from clients, decrypts it for processing and optimization, and then sends it to the web servers in unencrypted (HTTP) format. No server resources are required for SSL processing, and the BIG-IP system is the only location where certificates need to be installed and managed. You may need to import a certificate and key before deploying this template. See Local Traffic >> SSL Certificate List for importing certificates and keys.
Select the Certificate that will be used for Accessing the View environment.	default.crt
Select the Key for the certificate above.	default.key

Figure 5: Specific configurations for VMware View 5.0 using the iApp

Virtual Server	
What IP address will the clients use to connect to the View environment?	172.16.67.85
What is the Fully Qualified Domain Name that will be used by clients to access the View environment?	view.trace3.com
Description	The FQDN entered here will be used by the View client to resolve to the virtual IP entered above.
Do the View servers have a route back to application clients via this BIG-IP system?	No
Will you have more than 64,000 connections at one time? If so, you will need to enter at least one IP address for each 64,000 connections.	No
Are the View servers configured to use NTLM authentication?	No
Will clients be connecting to this virtual server primarily over a LAN or a WAN?	WAN

Fig 6: Setup of the virtual server using the iApp



Server Pool			
Which load balancing method do you want to use?	Least Connections (node)		
Which servers do you want this virtual server to reference? (The virtual server will not be available until at least one server is added.)	Address	172.16.64.90	Connection Limit 0 <input type="button" value="X"/>
	Address	172.16.64.91	Connection Limit 0 <input type="button" value="X"/>
	Address	172.16.64.92	Connection Limit 0 <input type="button" value="X"/>
	Address	172.16.64.93	Connection Limit 0 <input type="button" value="X"/>
	Address	172.16.64.94	Connection Limit 0 <input type="button" value="X"/>
<input type="button" value="Add"/>			
Description	By enabling PCoIP the pool members configured on the BIG-IP system will be set to listen to any ports. For more information on this please see the View Deployment Guide.		
Do you want the BIG-IP to queue TCP requests?	No		
How often (in seconds) do you want the BIG-IP system to check on the health of each View server?	30		
What HTTP request should be sent to check the health of each View server?	GET /		
Important	See the Help tab for the F5 recommended HTTP request.		
What string can the BIG-IP system expect to see within the health check response for the server to be considered healthy?	VMware View Portal		

Figure 7: Setup of the server pools using the iApp

NetApp Environment Setup

Two NetApp 3240 controllers were configured with separate disk technologies on each host. The first controller was equipped with a single shelf of 600 GB, 10,000 RPM, SAS disk storage with 22 disks in a single aggregate. The second controller was attached to the 1 TB SATA storage, which was used to provision SAN storage for the ESX servers. The higher performance SAS storage was provisioned for the virtual desktops via NFS to ensure adequate performance for access to remote desktops. To further accelerate performance, Flash Cache was enabled on the second controller. A simple command-line interface (CLI) command on the NetApp controller activated and deactivated Flash Cache.

Setup of the ESX Server Environment

Two ESX servers were set up and provisioned a total of five View Connection Servers on the first (.86) server. The virtual desktops were provisioned with NetApp FlexClone technology as opposed to the VMware Linked Clones feature, since FlexClone utilized the back-end array, is integrated into vSphere, and does not require VMware composer to deploy linked clones. A total of 40 virtual desktops were provisioned across two pools. One pool allowed access to desktops via native PCoIP, a UDP a feature introduced in View 4.5. The second pool was configured to allow access only via Microsoft RDP.



View Connections	172.16.64.90 172.16.64.91 172.16.64.92 172.16.64.93 172.16.64.94
ESX Servers	72.16.64.85 172.16.64.86
BIG-LTM IP Addresses	External: 172.16.67.81 Internal: 172.16.64.81 Virtual Server: 172.16.67.85
Virtual Server FqDN	view.trace3.com

Figure 8: IP address information of the VMware View environment

Validation of VMware View 5.0

Once the testing environment was set up and configured, testing proceeded in two phases to demonstrate access to the VDI environment using both local and remote user scenarios. The first phase focused on PCoIP and RDP access.

Local PCoIP and RDP

The first phase involved user access via PCoIP and RDP to demonstrate the contrasts between the two methods. Each of the five View Connection Servers was configured to point to the IP address of the BIG-IP LTM virtual server (as opposed to pointing individually to each of the five View Connection Servers). Having all users point to a single virtual server IP address enabled the five View Connection Servers to appear as a single installation accessed via a single virtual IP (VIP) address. In this way a View 5.0 installation can effectively scale beyond the 2,000-connection limit of an individual View Connection Server to make a five server, 10,000 user deployment appear like a single server deployment.

An additional benefit of this configuration is performance. The BIG-IP device offloads CPU-intensive processes from the servers, increasing performance and improving virtual server density. This process was validated with user connections made via PCoIP to BIG-IP LTM and then connected directly to the View Connection Server. Connecting via the virtual server, as opposed to connecting directly to an individual View Connection Server, demonstrated approximately a 25 percent performance improvement.



The second set of tests involved accessing the RDP virtual desktop pool. Although the Remote Desktop Protocol takes more time to connect to a virtual desktop than PCoIP does, it is a more commonly used protocol in data centers. In testing, users successfully accessed the virtual desktop via the same BIG-IP LTM virtual server IP address. Testing additionally demonstrated nearly a 30 percent reduction in the time required to access the desktop via BIG-IP LTM compared to direct connection to the View Connection Server.

SSO Remote Access via BIG-IP APM

The second phase of the testing demonstrated the capabilities of remote access via BIG-IP APM. With version 11.x and above, a simple reconfiguration of the iApp was all that was required for the iApp to support the BIG-IP APM deployment. The iApp reconfiguration involved the following sections:

- Configuration and authentication to the domain. In this case, authentication was configured for the 'View' domain.
- A lease pool of IP addresses configured for remote users. In this case, a range of 192.168.1.x addresses was created in the iApp.
- A separate, virtual server IP address. This virtual server address used the previously configured virtual server IP address of BIG-IP LTM as its sole pool member.

Once the iApp was reconfigured, the additional BIG-IP APM objects were configured in the BIG-IP LTM and BIG-IP APM sections of the BIG-IP GUI, and testing proceeded to demonstrate successful remote access via BIG-IP APM.

Conclusion

FlexPod data center architectures have generated substantial momentum in the marketplace and via mutual F5 and NetApp sales channels. Trace3, a leading NetApp and F5 partner, has collaborated with both to rapidly deploy a VMware View 5.0 environment using the storage efficiency of NetApp technologies and the application acceleration of the F5 ADC.

Based on the results of that testing, organizations choosing the validated FlexPod architecture can be assured that their virtualization initiatives can be deployed on a scalable platform with traffic management, access, and authorization provided by the leading ADC in the market. Using the BIG-IP 8900 device to enhance and

Tech Brief

Enable a Scalable and Secure VMware View Deployment

extend the FlexPod data center design enables a full Application Ready Solution that can be simply and rapidly deployed—whether for VMware View, Tier 1 applications, or large-scale transformation of the data center infrastructure. The result is a virtualized infrastructure that provides the enterprise with greater scalability at dramatically reduced footprint, power, and cooling costs.

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

