



F5 White Paper

Managing BIG-IP Devices with HP and Microsoft Network Management Solutions

Using third-party tools such as HP Network Node Manager i and Microsoft System Center Operations Manager, it has never been easier to manage F5 BIG-IP devices.

By

Keith Rickards

Product Management Engineering

Alan Murphy

Technical Marketing Manager



Contents

Introduction	3
HP Network Node Manager i	4
Microsoft System Center Operations Manager	5
Conclusion	7



Introduction

The transition of the traditional physical data center into a dynamic, agile, virtual data center is one of the most widely discussed topics in technology today. It seems that every IT magazine or blog addresses how virtualization is changing the data center. While we see rapid change in many technologies, network and systems management architectures have remained fairly constant over many years. Data center management—of all systems and services in the data center—is still a necessity whether it is through the single view of an entire enterprise management system or of individual components.

Management architecture remains similar to when enterprise data centers first started to crop up: A pull-based architecture in which a central management station makes requests to background processes running on devices that need to be managed. The managed device replies with the requested data (such as network or processor percent utilization) and, as the data returns, the management system reviews this data. The central management station typically includes a database that stores historical data and provides time-based reporting of collected metrics. Management stations can provide automated notifications for events, especially when a device is unavailable or malfunctioning. While the base architecture and function have not changed much, the tools, protocols, standards, notification systems, and reporting techniques that support them have.

Network management systems (NMS) provide insight into device and application performance, system stability, network trouble spots, and a host of other issues that affect a company's ability to provide network services. Recent advances in automated event correlation, data storage and retrieval, as well as open source systems that enable greater integration, have greatly improved today's implementations.

As a critical component of application delivery throughout the data center, F5 has always integrated Application Delivery Controller (ADC) features, such as load balancing, application health checks, network optimization, and application security, with NMS technologies. This integration occurs through traditional means such as Simple Network Management Protocol (SNMP), as well as through F5's open web-based iControl® API. While the F5 BIG-IP® system can be integrated with any existing NMS solution, F5 has partnered with larger NMS vendors to provide out-of-the-box solutions that manage BIG-IP devices as part of a holistic data center management strategy.



The two examples below demonstrate how partner integration with F5 BIG-IP devices enables greater ease of use for existing management systems. The first example reviews a simple method to properly identify all BIG-IP devices managed by Hewlett-Packard (HP) Network Node Manager i. The second example discusses the F5 Management Pack that enables customers running Microsoft® System Center Operations Manager to monitor BIG-IP devices.

HP Network Node Manager i

HP OpenView Network Node Manager (NNM) has been a staple of enterprise network management for many years. Initially, NNM was a network discovery and device availability management platform with support for devices such as early networking hubs and switches. These hubs and switches were monitored using Internet Control Message Protocol (ICMP)—a networking protocol similar to Transmission Control Protocol (TCP) or User Datagram Protocol (UDP)—and SNMP Management Information Bases (MIBs). Unsecured, clear-text requests were made across private networks for basic performance data. Scalability, MIB compatibility, “event storms,” long-term data storage, and reporting were significant issues for these early implementations, which often resulted in management systems being ignored due to their limitations. In fact, some reports estimated that more than 70 percent of these management system deployments were ultimately considered failures by IT organizations.

Over time, HP has evolved and improved NNM through acquisitions and internal development. Today, rebranded as Network Node Manager i (NNMi), HP has created an open, robust event correlation, performance, and availability management platform that achieves true enterprise scale. Through NNMi’s open architecture, HP partners can build interoperability systems to support highly specific data center hardware. For several years, F5 has participated in the HP Enterprise Management Alliance Program (EMAP) to provide joint customers with effective management solutions for F5 products in an HP managed environment. In the NNMi solution, F5 populates the SNMP Object Identifiers (OIDs) database with values and data specific to F5 hardware and application traffic management information. Through F5’s DevCentralSM developer community [Advanced Design and Configuration CodeShare](#) page, F5 has published the OID data in an XML file that can be imported directly into NNMi. (See Figure 1.)

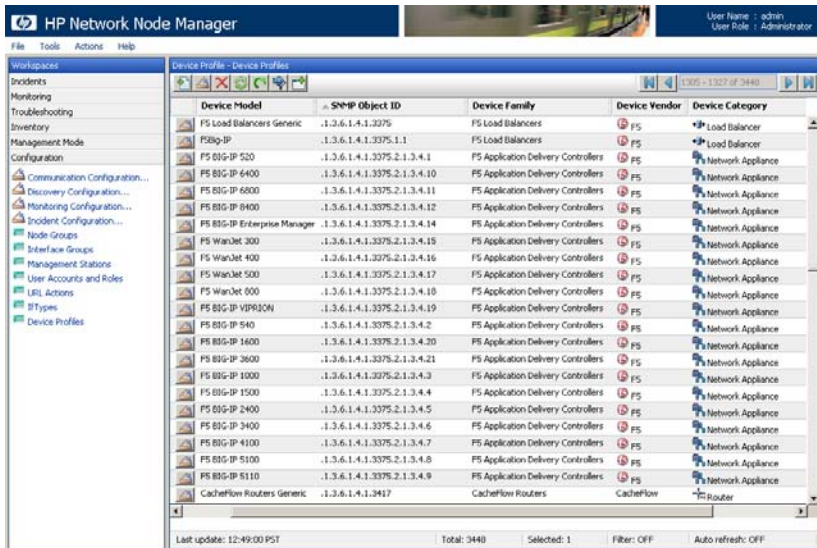


Figure 1: Importing F5 OIDs into NNMi

Microsoft System Center Operations Manager

In many organizations, the responsibility for configuration and operation of BIG-IP devices and the servers that stand behind them crosses several areas of responsibility. Configuration and operation duties may be assigned to security, network, or applications groups, or to all of those groups. The F5 Management Pack for Microsoft System Center Operations Manager provides a bridge among these groups to efficiently collect and report key health metrics about the Application Delivery Network as well as execute configuration changes on the BIG-IP device.

By integrating the F5 Management Pack with current deployments of System Center Operations Manager, it becomes possible to view the health of F5 devices, analyze the performance of the web servers, and report on the utilization of network devices. The F5 Management Pack for System Center Operations Manager uses a variety of management technologies, including iControl, to both report on and configure F5 devices. When the F5 Management Pack is deployed as part of the management solution along with System Center Virtual Machine Manager and System Center Configuration Manager, F5 devices and application traffic can be managed as part of a complete deployment of System Center data center solutions.

As the use of data center automation techniques and server virtualization expands, organizations must maintain visibility of their application servers and the network

infrastructure. By expanding the capabilities of System Center data center solutions with the F5 Management Pack into management of the virtual infrastructure, administrators achieve the required visibility into server system operation and the Application Delivery Network performance. (See Figure 2.) The time to triage trouble areas in the application delivery infrastructure is greatly reduced when operators have insight into the current network state, as well as historical performance data.

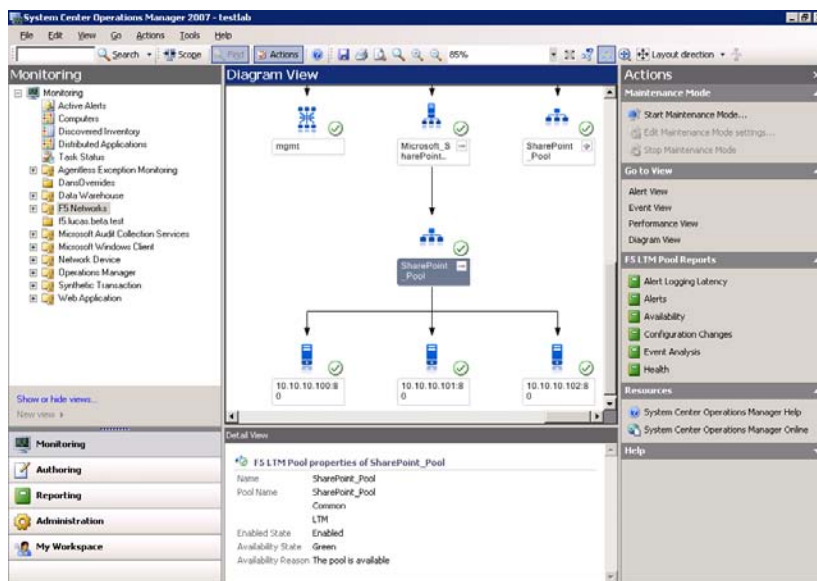


Figure 2: F5 Management Pack for System Center Operations Manager

The F5 Management Pack works with BIG-IP® Local Traffic Manager™ (LTM) and BIG-IP® Global Traffic Manager™ (GTM) and is available as a download from F5 [DevCentral](#). The F5 Management Pack provides a number of preconfigured reports, leveraging the Microsoft SQL Server® Reporting Services built into System Center Operations Manager. The reports can be based on any of the 160 metrics that are available for collection with the F5 Management Pack.

Conclusion

Although it is often one of the least discussed technologies in the data center, management is the backbone of any Application Delivery Network—from the systems that run the applications to the network that delivers those applications. By working collaboratively with partners that build some of the most widely deployed network management tools in the industry, F5 provides the bridge between application system and network infrastructure management. Whether monitoring application health and performance or network devices, F5 demonstrates the commitment to provide customers visibility and control over their entire Application Delivery Network as part of a holistic data center management solution.

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
info.asia@f5.com

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

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



Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries.

© 2009 F5 Networks, Inc. All rights reserved. F5, F5 Networks, the F5 logo, BIG-IP, FirePass, iControl, TMOS, and VIPRIION are trademarks or registered trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. CS58745 1108