BROCADE

September 2015

53-1003958-01

Brocade Virtual Traffic Manager and Microsoft Intelligent Application Gateway

Deployment Guide

Contents

Preface

Welcome to the Brocade Virtual Traffic Manager (vTM) and Microsoft Intelligent Application Gateway Deployment Guide. Read this preface for an overview of the information provided in this guide and contact information. This preface includes the following sections:

- About This Guide

- Contacting Brocade

About This Guide

The Brocade Virtual Traffic Manager and Microsoft Intelligent Application Gateway Deployment guide describes optimization of Microsoft Intelligent Application Gateway farms.

Audience

This guide is written for network operations professionals, server administrators and DevOps professionals familiar with administering and managing Application Delivery Controllers (ADCs), Servers and Applications.

You must also be familiar with:

- Microsoft Intelligent Application Gateway

- Brocade Virtual Traffic Manager

For more details on the Brocade vADC product family, see:

http://www.brocade.com/vADC

Contacting Brocade

This section describes how to contact departments within Brocade.

Internet

You can learn about Brocade products through the company Web site: http://www.brocade.com.

Technical Support

If you have problems installing, using, or replacing Brocade products, contact Brocade Support or your channel partner who provides support. To contact Brocade Support, see http://www.brocade.com/en/support.html.

Professional Services

Brocade Global Services has the expertise to help organizations build scalable, and efficient cloud infrastructures. Leveraging 15 years of expertise in storage, networking, and virtualization, Brocade Global Services delivers world- class professional services, technical support, and education services, enabling organizations to maximize their Brocade investments, accelerate new technology deployments, and optimize the performance of networking infrastructures.

Chapter 1: Solution Overview

This chapter includes the following sections:

- Virtual Traffic Manager Overview

- Microsoft Intelligent Application Gateway

Virtual Traffic Manager Overview

Brocade Virtual Traffic Manager (vTM) is a software-based application delivery controller (ADC) designed to deliver faster and more reliable access to public web sites and private applications. vTM frees applications from the constraints of legacy, proprietary, hardware-based load balancers, which enables them to run on any physical, virtual, or cloud environment. With vADC products from Brocade, organizations can:

- Make applications more reliable with local and global load balancing

- Scale application servers by up to 3x by offloading TCP and SSL connection overhead

- Accelerate applications by up to 4x by using web content optimization (WCO)

- Secure applications from the latest application attacks, including SQL injection, XSS, CSRF, and more

- Control applications effectively with built-in application intelligence and full-featured scripting engine

Virtual Traffic Manager offers much more than basic load balancing. It controls and optimizes end-user services by inspecting, transforming, prioritizing, and routing application traffic. The powerful TrafficScript® engine facilitates the implementation of traffic management policies that are unique to an application by allowing organizations to build custom functionality or to leverage existing features in Virtual Traffic Manager in a specialized way. With vTM, organizations can deliver:

Performance

Improve application performance for users by offloading encryption and compression from the web server by dynamic caching and reducing the number of TCP sessions on the application.

Reliability and scalability

Increase application reliability by load balancing traffic across web and application servers, balancing load across multiple data centers (private or public clouds), monitoring the response time of servers in real-time to decide the fastest way to deliver a service, protecting against traffic surges, and by managing the bandwidth and rate of requests used by different classes of traffic.

Advanced scripting and application intelligence

Manage application delivery more easily with fine-grained control of users and services using TrafficScript, an easy-to-use scripting language that can parse any user transaction, and take specific, real-time action based on user, application, request, or more. Development teams use TrafficScript to enable a point of control in distributed applications, while operations teams use it to quickly respond to changing business requirements or problems within an application before developers can fix it.

Application acceleration

Dramatically accelerate web-based applications and websites in real-time with optional web content optimization (WCO) functionality. It dynamically groups activities for fewer long distance round trips, resamples and sprites images to reduce bandwidth, and minifies JavaScript and combines style sheets to give the best possible response time for loading a web page on any browser or device.

Application-layer security

Enhance application security by filtering out errors in web requests, and protecting against external threats, with the option of a comprehensive Layer-7 firewall to defend against deliberate attacks.
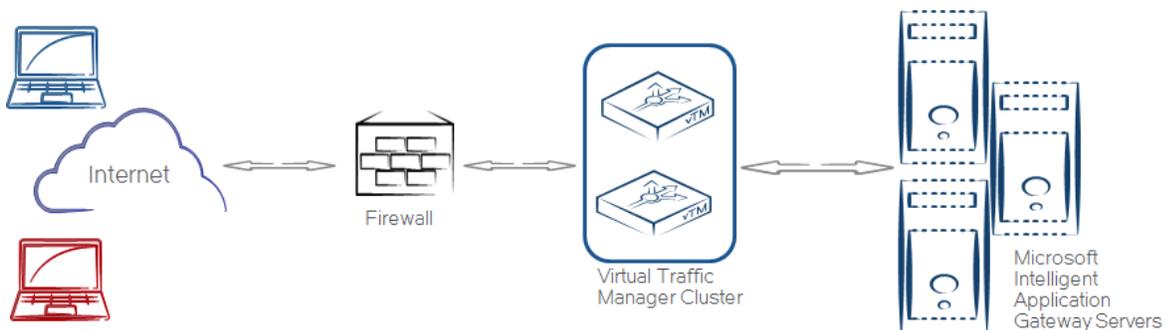
Microsoft Intelligent Application Gateway

Microsoft provides Intelligent Application Gateway provides remote access to applications, networks, and internal resources from diverse client endpoints. Access to multiple internal applications can be given through a single IAG portal, or to a single Web application.

Chapter 2: Microsoft Intelligent Application Gateway Architecture

The deployment architecture including the Traffic Manager and Microsoft Intelligent Application Gateway (IAG) servers is shown in the following topology:

Figure 2-1:   vTM and Microsoft IAG

Intelligent Application Gateway can be quickly, easily and securely integrated into the Traffic Manager. Because access to Intelligent Application Gateway is generally secured using HTTPS, it is recommended to do SSL Decryption on the Traffic Manager thereby reducing the CPU load on the IAG server back-end. Optionally, the traffic from the Traffic Manager to the IAG servers can be re-encrypted. An HTTP protocol server, listening on port 443 and decrypting traffic, should be configured to handle traffic to the Exchange server. Optionally, an HTTP server, listening on port 80 can also be configured with a TrafficScript rule to redirect it to port 443 (https).

Chapter 3: Deploying Traffic Manager for Intelligent Application Gateway

This chapter describes the process for deploying Virtual Traffic Manager to optimize the Intelligent Application Gateway installation. It includes the following sections:

- Requirements

- Configure vTM for Microsoft Intelligent Application Gateway

Requirements

- Brocade Virtual Traffic Manager (10.1 or later)

- Microsoft Intelligent Application Gateway

Note: This deployment guide was certified while the product was with Riverbed and for 9.x or earlier versions of the Traffic Manager.

Configure vTM for Microsoft Intelligent Application Gateway

This section contains step by step instructions on configuring Traffic Manager for Microsoft Intelligent Application Gateway suite:

Component	Procedure	Description
Virtual Traffic Manager (once)	Create Traffic IP Group for Microsoft Intelligent Application Gateway	A single Traffic IP Group must be created For details, see "Create Traffic IP Group"
	Create Pool for the Intelligent Application Gateway server farms (once for each server farm)	A Pool needs to have a set of servers to load-balance. Enter the hostname or IP address of the node along with the TCP/UDP port For details, see "Create Pool"
	Create Virtual Server for the application servers	Create and associate the Virtual Server to the server pool. For details, see "Create Virtual Server"
	SSL decryption	Configure SSL Decryption to enable SSL offloads. For details, see "SSL Decryption"
	Configure Session Persistence	Configure SSL Decryption to enable SSL offloads. For details, see "Configure Session Persistence"

Create Traffic IP Group

A Traffic IP Group (also known as a Virtual IP) will need to be created on which the Virtual server will be listening on. To create a new Traffic IP Group:

1. Navigate to **Services->Traffic IP Groups** and scroll down to **Create a new Traffic IP Group**.

2. Fill in the fields as follows:

    - **Name:** A descriptive name for the application server.

    - **IP Addresses:** An IP Address that is mapped to FQDN of the application.

3. Click **Create Traffic Group**.

Create Pool

A Pool has to be created for the IAG server farm as shown in the topology diagram. To create a new Pool:

1. Navigate to **Services->Pools** and scroll down to **Create a new Pool**.

2. Fill in the fields as follows:

    - **Pool Name:** A descriptive name for the pool ex. Glassfish1-servers

    - **Nodes:** hostname:80 or ipaddress:80 (use port 443, if traffic is re-encrypted)

    - **Monitor:** Select "Simple HTTP"

Create Virtual Server

Create a Virtual server that will handle all the application Traffic. To create a new Virtual Server:

1. Navigate to **Services->Virtual Servers** and scroll down to **Create a new Virtual Server**.

2. Enter the following:

    - **Virtual Server Name:** A descriptive name for the Virtual Server

    - **Protocol:** HTTP

    - **Port:** 443

    - **Default Traffic Pool:** Select the pool created in the step above.

3. Click on **Create Virtual Server**.

4. In the next screen, under **Listening on**, select **Traffic IP Groups** and check the appropriate Traffic IP Group that was created earlier.

5. Set **Enabled:** to **Yes**.

6. Click on the **Update** button to apply changes.

SSL Decryption

In order to perform SSL decryption, the certificate and the private key used for the Virtual Server created in the previous step must be imported into the Traffic Manager.

1. Navigate to **Catalogs->SSL->SSL Certificates catalog**.
2. Click on **Import Certificate** to import the appropriate certificate.

After importing the certificate, enable SSL decryption on the Virtual Server created:

1. Navigate to **Services->Virtual Servers** and select the virtual server that will be performing SSL decryption.
2. Scroll down and click on **SSL Decryption**.
3. Set **ssl_decrypt** to **Yes**.
4. Select the certificate imported in the previous step.
5. Scroll down to the bottom of the page and click **Update**.

Configure Session Persistence

To ensure that clients persist their connections to the load-balanced servers after login, configure the following:

1. Go to **Catalogs -> Persistence** and create a new class called **IAG Persistence**.
2. Set this class to use the **Transparent Session Affinity** method and failure mode of **choose a new node to use**.
3. Click **Update** to finish.
4. Go to **Services -> Pools -> <IAG pool>**-> **Session Persistence**.
5. Select the class from the list and click **Update**.

Configuration Summary

By accessing the **Services →·Config Summary** on the webGUI a complete snapshot of all the configured services is provided. This is very useful table to glance through to get a good understanding of how the services are configured.

Chapter 4: Conclusion

This document briefly discusses how to configure Traffic Manager to load balance traffic to a farm of Microsoft Intelligent Application Gateway servers. Traffic Manager is able to manage traffic in a wide variety of ways, to improve the performance, security, reliability and integrity. Please refer to the product documentation on the Brocade Community Forums (http://community.brocade.com) for examples of how Brocade Virtual Traffic Manager can be deployed to meet a range of service hosting problems.