BROCADE

DEPLOYMENT GUIDE

Brocade Virtual Traffic Manager and Microsoft SharePoint 2010 Deployment Guide

53-1003966-02
22 February 2017

Contents

Preface

About This Guide

The *Brocade Virtual Traffic Manager and Microsoft SharePoint 2010 Deployment Guide* describes how to configure Brocade Virtual Traffic Manager (Brocade vTM) to load-balance and optimize Microsoft SharePoint Server 2010. This deployment guide is designed to be used together with the Brocade vTM documentation.

For more details on the Brocade vADC product family, see http://www.brocade.com/vADC.

Audience

This guide is written for network administrators, Microsoft SharePoint administrators, and developer operations (DevOps) professionals who are familiar with administering and managing both application delivery controllers (ADCs) and Microsoft SharePoint 2010. You should also be familiar with installing and configuring a virtual appliance in a virtual VMware, Hyper-V, or dedicated Linux environment.

About Brocade

Brocade® (NASDAQ: BRCD) networking solutions help the world's leading organizations transition smoothly to a world where applications and information reside anywhere. This vision is designed to deliver key business benefits such as unmatched simplicity, non-stop networking, application optimization, and investment protection.

Innovative Ethernet and storage networking solutions for data center, campus, and service provider networks help reduce complexity and cost while enabling virtualization and cloud computing to increase business agility.

To help ensure a complete solution, Brocade partners with world-class IT companies and provides comprehensive education, support, and professional services offerings (www.brocade.com).

Contacting Brocade

This section describes how to contact departments within Brocade.

Internet

You can learn about Brocade products through the company website: 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.

Document History

Date	Part Number	Description
September 30, 2015	53-1003966-01	Initial release.
February 2017	53-1003966-02	Added Web Accelerator and vWAF content.

Solution Overview

Brocade Virtual Traffic Manager

Brocade Virtual Traffic Manager (Brocade vTM) is a software-based application delivery controller (ADC) designed to deliver faster and more reliable access to public websites and private applications. Brocade vTM frees applications from the constraints of legacy, proprietary, hardware-based load balancers, which enables them to run in 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, and CSRF.
- Control applications effectively with built-in application intelligence and a full-featured scripting engine.

Brocade 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 Brocade vTM in a specialized way. With vTM, organizations can deliver the following:

- **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 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 the user, application, request, or more. Development teams use TrafficScript to enable a point of control in distributed applications, whereas 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 and compresses 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 SharePoint 2010

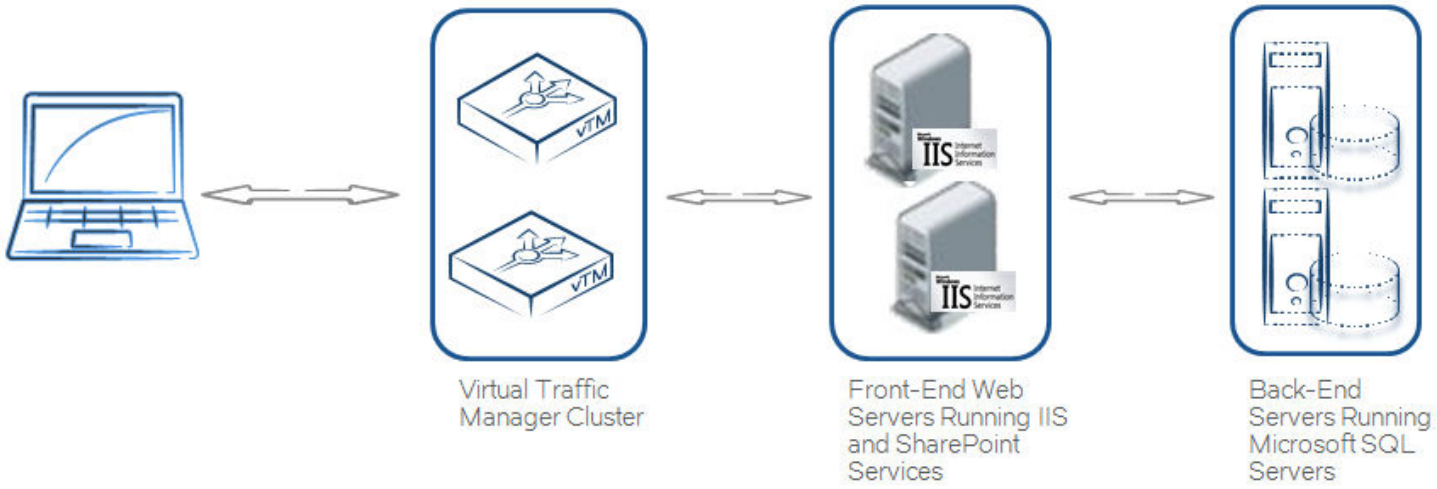
Microsoft SharePoint 2010 is collaboration software that enables people to work together. SharePoint 2010 sites provide a single infrastructure for all your business websites. Using SharePoint 2010, people can set up websites to share information with others, manage documents from start to finish, and publish reports to help everyone make better decisions. Some of the key components of SharePoint 2010 are:

- SharePoint 2010 Composites—Offers tools and components for creating do-it-yourself business solutions. Build no-code solutions to rapidly respond to business needs.
- SharePoint 2010 Insights—Gives everyone access to the information in databases, reports, and business applications. Help people locate the information that they need to make good decisions.
- SharePoint 2010 Communities—Delivers great collaboration tools and a single platform to manage them. Make it easy for people to share ideas and work together the way they want.
- SharePoint 2010 Content—Makes content management easy. Set up compliance measures behind the scenes, with features like document types, retention polices, and automatic content sorting, and then let people work naturally in Microsoft Office.
- SharePoint 2010 Search—A unique combination of relevance, refinement, and social cues helps people find the information and contacts that they need to get their jobs done.

Microsoft SharePoint 2010 Architecture

A typical SharePoint 2010 deployment consists of multiple separate servers running SharePoint services and the Database tier. Multiple sites and subsites are grouped in site collections on each virtual server in IIS that is extended with Windows SharePoint services. Each virtual server has its own set of content databases in SQL Server. The configuration database for the server farm directs each server to the appropriate content database for a given website. The content for the top-level website and any subsites within a site collection is stored in the same content database. Performance and capacity are increased by adding additional servers running Windows SharePoint services and SQL Server. Scaling is achieved by adding more front-end web servers (to increase throughput for the existing content) and by adding top-level websites and subsites (to support more content). Load balancing is achieved using the Virtual Traffic Manager.

FIGURE 1 Topology with SharePoint 2010 and Virtual Traffic Manager



Deploying Brocade Virtual Traffic Manager

This chapter describes the procedures for deploying Brocade Virtual Traffic Manager for load-balancing applications that are deployed in a WebLogic environment.

Requirements

- Brocade Virtual Traffic Manager (10.1 or later)
- Microsoft SharePoint 2010

Configuring Brocade Virtual Traffic Manager

This section provides step-by-step instructions for configuring Brocade Virtual Traffic Manager for SharePoint 2010 to support SSL offloading.

Understanding the Deployment Process

This section walks through the procedures required for load-balancing SharePoint 2010 with the Brocade Virtual Traffic Manager.

Component	Procedure	Description
Virtual Traffic Manager	Creating a Traffic IP Group for the SharePoint Farm	Create a traffic IP group (also known as a virtual IP) on which the virtual server will listen. For details, see Creating a Traffic IP Group for the SharePoint Farm on page 9.
	Creating a Pool Containing Web Front-End Servers and SharePoint Services	A pool must be created for the SharePoint farm managed by the Virtual Traffic Manager. For details, see Creating a Pool Containing Web Front-End Servers and SharePoint Services on page 10.
	Creating a Health Monitor	For details, see Creating a Health Monitor on page 10.
	Configuring Session Persistence	For details, see Configuring Session Persistence on page 10.
	Creating a Virtual Server That Listens to the SharePoint Farm Traffic IP Group	Create a virtual server that handles all the view client traffic. For details, see Creating a Virtual Server That Listens to the SharePoint Farm Traffic IP Group on page 11.
	Configuring SSL Decryption for SSL Offloading	The virtual server created in the previous procedure must be configured to decrypt SSL traffic. For details, see Configuring SSL Decryption for SSL Offloading on page 11.

Creating a Traffic IP Group for the SharePoint Farm

Create a traffic IP group (also known as a virtual IP) on which the virtual server will listen. 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 SharePoint farm site (e.g., sp.mycompany.com)
   - **IP Addresses**—An IP address that will be associated to the FQDN of the SharePoint farm site
3. Click the **Create Traffic Group** button.

Creating a Pool Containing Web Front-End Servers and SharePoint Services

For the SharePoint farm managed by the Virtual Traffic Manager, create a pool using the following steps:

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. (e.g., SP Project Site Pool)
   - **Nodes**—hostname:80 or ipaddress:80
   - **Monitor**—Full HTTP
3. In the next screen, click **Load Balancing**.
4. Under **Algorithm**, select **Perceptive**.
5. Click the **Update** button to apply changes.

Creating a Health Monitor

This section details the steps to create health monitors. The HTTP monitor is used for port 8080 on the Lync front-end pool.

1. Navigate to **Catalogs** > **Monitors**.
2. Scroll down to **Create new monitor**.
3. Enter a name for the new monitor. Set **Type** to **HTTP** and **Scope** to **Node**.
4. Click **Create Monitor**.

Attaching the Monitor to a Pool

After the monitors have been created, they must be attached to the appropriate pool.

1. Navigate to **Services** > **Pools** and select the pool to which the monitor will be attached.
2. Scroll down and click **Health Monitoring**.
3. Add the appropriate health monitor.

Configuring Session Persistence

Transparent session affinity persistence is required for the pool created in the previous procedure. To configure session persistence:

1. Navigate to **Catalogs** > **Persistence**.
2. Provide a descriptive name for the persistence class.
3. Click **Create Class**.
4. Select **Transparent session affinity** in **Basic Settings**.
5. Click **Update** to apply changes.

6. Navigate to **Services** > **Pools** and select the pool that was created earlier.
7. Navigate to **Session Persistence** and click **Edit**.
8. Select the session persistence class created, and click **Update** to apply changes.

Creating a Virtual Server That Listens to the SharePoint Farm Traffic IP Group

To handle all the view client traffic, create a virtual server using the following steps:

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 (e.g., sp.mycompany.com)
   - **Protocol**—HTTP
   - **Port**—443 (Note: 443 port is used for SSL offloading)
   - **Default Traffic Pool**—The pool created for this service in the previous section
3. Click **Create Virtual Server**.
4. In the next screen, under **Listening on**, select **Traffic IP Groups** and check the traffic IP group that was created earlier.
5. Set **Enabled** to **Yes**.
6. Click the **Update** button to apply the changes.

Configuring SSL Decryption for SSL Offloading

The virtual server created previously must be configured to decrypt SSL traffic.

Importing the Certificate

To perform SSL decryption, the certificate and the private key used for the virtual server created previously must be imported into the Virtual Traffic Manager.

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

Enabling SSL Decryption on the Virtual Server

After importing the certificate, enable SSL decryption on the virtual server created.

1. Navigate to **Services** > **Virtual Servers** and select the virtual server created for the SharePoint farm website that will be performing SSL decryption.
2. Scroll down and click **SSL Decryption**.
3. Set **ssl_decrypt** to **Yes**.
4. Select the certificate imported in Step 2 of Importing the Certificate on page 11.
5. Scroll down to the bottom of the page and click **Update**.

Configuration Summary

By accessing **Services** > **Config Summary** on the web GUI, a complete snapshot of all configured services is provided. This is a very useful table to understand how the services are configured.

Additional Optional Functionality on Brocade Virtual Traffic Manager

Brocade Virtual Traffic Manager has capabilities beyond a legacy load balancer to enhance the performance and manageability of your Microsoft SharePoint 2010 environment. Here are some common capabilities and best practices for deploying Brocade Virtual Traffic Manager to enhance your Microsoft SharePoint 2010 deployment.

Service-Level Monitoring

Service-level monitoring monitors the responses of your SharePoint servers and sends alerts should these fall below an expected threshold of performance. In addition to sending alerts, a TrafficScript rule can be written and configured to remove the service or server from the pool until the performance issue has been remediated, to reprioritize traffic and even to reallocate bandwidth. Essentially, by using a TrafficScript rule for service-level monitoring, services can be controlled and managed.

Global Load Balancing

Global load balancing enables Client Access Servers to be distributed across multiple locations, for Disaster Recovery (DR) or based on their geographic proximity to a data center. As a common issue when failing over to a DR location, services will become unavailable until the DNS Time-to-Live (TTL) expires, so that clients can resolve the IP address of the DR location. Configuring Virtual Traffic Manager for global load balancing using Active/Passive mode improves and utilizes failover Recovery Time Objective (RTO) since it is no longer constrained by the DNS TTL.

Web Browser Restriction for SharePoint Websites

Virtual Traffic Manager can be used to filter or redirect unsupported web browsers, such as Internet Explorer 6.0, from accessing the SharePoint farm. By doing so, users with unsupported browsers can be notified or blocked from access. Web browser restriction can be done through TrafficScript for a SharePoint virtual server.

Create a TrafficScript rule from **Catalog** > **Rules** and link it to its appropriate virtual server. The following sample TrafficScript redirects Internet Explorer 6.0 to another website. Alternatively, a bad request response can be used by uncommenting the code below and removing the redirection code line.

```
#// TS Rule for redirecting HTTP requests based on client browser
$debug = 0; // Change value to 1 if debug needed
$browser = http.getHeader("user-agent");
if(string.contains ($browser, "MSIE 6.0"))
{
   http.redirect("http://www.brocade.com");
   if ($debug > 0) { log.info("Request Redirected");}
    #or uncomment the lines below and delete the lines above
#http.sendResponse( "400 Bad Request", "text/plain","Bad Request", "");
```

```
   #if ($debug > 0) { log.info("Bad Request");}
}
```

Bandwidth Management for Internet and Intranet Zones

Using the Bandwidth Management feature of Virtual Traffic Manager, Internet bandwidth traffic can be limited or lowered to throttle the Intranet bandwidth requirement or to prioritize Intranet traffic. This can be useful for websites that are externally exposed and for search engines, which consume Internet bandwidth for searches. Bandwidth classes are assigned per pool in Virtual Traffic Manager.

To limit a bandwidth for the Internet zone, assign a bandwidth class to its virtual server using the following steps:

1. Navigate to **Catalogs** > **Bandwidth**.
2. Provide a descriptive name for the bandwidth class.
3. Determine the bandwidth and scope of the bandwidth.
4. Click **Update** to apply changes.
5. Navigate to **Services** > **Virtual Servers** and select the virtual server for the Internet zone.
6. Select **Classes** under **Bandwidth Management** and select the bandwidth class created earlier.
7. Click **Update** to apply changes.

   Use a TrafficScript to limit the bandwidth dynamically for the Internet zone. For example, limit the bandwidth for downloading files above 10 Mb, and then assign the TrafficScript to the virtual server created for the Internet zone URL. Use the following TrafficScript to limit the download bandwidth speed for binary files. Bandwidth can also be limited for different content types, such as audio and video.

```
#// TS Rule for bandwidth control
$debug = 0; // Change value to 1 if debug needed
$mime = http.getResponseHeader("Content-Type");
if(string.contains ($mime, "application/octet-stream"))
{
   $length = http.getResponseHeader("Content-Length");

#More than 10Mb binary file size, like Word document
   if($length > 10240000)
   {
      connection.setBandwidthClass( "file" );
             if ($debug > 0) { log.info("Bandwidth limit set");}
   }
}
```

Configuring Clustering for Virtual Traffic Manager

To provide high availability and fault tolerance for Virtual Traffic Manager, multiple instances of vTM can be joined into a cluster and configured to load-balance or act in active-passive mode for fault tolerance.

Perform the following steps to join a Virtual Traffic Manager to an existing cluster.

1. Navigate to **System** > **Traffic Managers**.
2. Scroll down to **Add or Remove Traffic Managers** and click **Join a Cluster**.
3. Click **Next** on **Getting Started**.
4. Select the cluster to join and click **Next**.

5. Check the certificate used for the cluster, provide a username and password for the cluster, and click **Next** to continue.
6. Select **Yes**, allow it to host traffic IPs immediately, and click **Next**.
7. In the **Summary** page, click **Finish** to join the vTM to the cluster.

Web Accelerator and vWAF Functions

Web Accelerator

Web Accelerator is a Virtual Traffic Manager feature that is available in the Enterprise edition of the Brocade vTM. Web Accelerator enables vTM to perform a full range of optimization techniques on HTML pages, including inspecting and modifying them. It also performs the following optimizations on the page resources as the client fetches them:

- Minification and compression of JavaScript files
- Minification and compression of style sheets
- Background images inlined or versioned
- Web fonts versioned
- Resampling of image content
- Compression of all resources

Full control over the above-mentioned individual optimization parameters is also possible with Web Accelerator. There are built-in Web Accelerator profiles available with the Express profile being the most common one designed to match a wide range of applications. Other profiles for Microsoft SharePoint applications are also available in the product.

For Microsoft SharePoint 2010, enable the Web Accelerator for the HTTP service using the following procedure.

1. Click the virtual server on which Web Accelerator is to be enabled. Within that, click **Web Accelerator**.
2. In the **Basic Settings** section, enable the Web Accelerator functionality by selecting **yes** in the options for **aptimizer!enabled**.
3. Under **Catalogs > Web Accelerator > Application Scopes**, create a new application scope.
4. Enter any name for the application scope. This name will show up in the list of scopes to choose under **Virtual Server Web Accelerator Settings**.
5. Under **hostnames**, enter the hostname for the HTTP service.
6. Keep the rest of the settings as defaults, and click **Create Application Scope**.
7. Under the virtual server settings for Web Accelerator, expand the **Web Accelerator Profiles** section, and select the newly created application scope.
8. To the right of the selected application scope, select **Web Accelerator Profile**. In this case, select **SharePoint 2010**.
9. Click **Update**.

Virtual Web Application Firewall

Brocade Virtual Web Application Firewall (Brocade vWAF) is a scalable security platform for off-the-shelf solutions and custom applications. It lets you apply business rules to online traffic, screening for attacks such as SQL injection and cross-site scripting (XSS), while securing outgoing traffic to help compliance with PCI-DSS and HIPAA. Brocade vWAF can be run as an add-on to the vTM to enable both load balancing and application firewall services on a single instance.

Apart from custom rule configurations that are possible on the vWAF, there is a ruleset called baseline protection that protects applications from the most common application-layer attacks that exist today, such as the following:

- Path Traversal
- Shell Command Injection
- SQL Injection
- Code Injection
- Cross-Site Scripting (XSS)
- Common Attacks
- LDAP Injection
- Scanner
- XPATH Injection

The following procedure documents the configuration of the Brocade Virtual Web Application Firewall for baseline protection of the Microsoft SharePoint 2010 application for HTTP services.

1. On the vTM, navigate to **System > Application Firewall** and click the **afm_enabled** radio button, followed by **Update** (ensure that the **Confirm** checkbox is checked).
2. Click the **Application Firewall** tab on the vTM.
3. Click **Administration**, and then select **Baseline Management**.
4. From this screen, either download the latest Virtual Web Application Firewall baseline signatures from Brocade Communities and click **Upload** or click the **Download from Server** option if your vTM+vWAF has Internet connectivity.
5. In the **Application Firewall** UI, click **Application Control** and select **Application Creation Wizard**.
6. Enter a name for the application, and click **Continue**.
7. Choose the detection mode that will enable the firewall rules to be applied to production traffic. Choose the protection mode for not affecting production traffic and whether you want to test the rules and check the logs for their accuracy. Click **Continue**.
8. In the **customer key** screen, leave the default, and click **Continue**.
9. In the **hostname** screen, enter the exact FQDN/IP address (typically, this is the TIP group address) by which users/clients will access the application. You can enter multiple values for one application simply by clicking **Add hostname** after adding one. Click **Continue**.
10. In the next screen, leave the default logging level to reduced logging unless there is a need to monitor the complete logs. Click **Continue**.
11. In the next screen, choose the option to enable full request logging and selecting the number of days for data retention. If indefinite, leave it to the default **0**. Click **Continue**.
12. In the next screen, choose to run the **Baseline Protection** wizard. Click **Continue** and then click **Finish**.
13. In the **Baseline Protection** wizard, click **Next** on the **Overview** screen.
14. Choose the baseline version to use. Click **Next**.
15. Leave the rest of the screens to their defaults, and, finally, click **Finish**.
16. Click the **Virtual Traffic Manager** tab to go back to the vTM UI.
17. Select the virtual server on which the vWAF service is to be enabled, and select **enabled** for the **Application Firewall** option, and click **Update**.

    You can reach out to the Brocade support team for help on more advanced and customized configuration of the Web Accelerator and the Virtual Web Application Firewall.

Conclusion

This document discusses how to configure Brocade Virtual Traffic Manager to optimize the deployment of the Microsoft SharePoint 2010 application. Virtual Traffic Manager is able to make intelligent load-balancing decisions and improve the performance, security, reliability, and integrity of the traffic in this environment. 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 solve a range of service-hosting problems.