BROCADE

DEPLOYMENT GUIDE

# Brocade Virtual Traffic Manager and Microsoft SharePoint 2013 Deployment Guide

*53-1003967-02*
*22 February 2017*

# Contents

# Preface



## About This Guide

The *Brocade Virtual Traffic Manager and Microsoft SharePoint 2013 Deployment Guide* describes how to configure Brocade Virtual Traffic Manager (Brocade vTM) to load-balance and optimize Microsoft SharePoint Server 2013. 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.

You should also be familiar with:

- Microsoft SharePoint 2013 Web Applications, SharePoint Apps, and Office Web Apps 2013
- 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 2015 | 53-1003967-01 | Initial release. |
| February 2017 | 53-1003967-02 | 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 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 them.
- **Application Acceleration**—Dramatically accelerate web-based applications and websites in real time with optional web content optimization (WCO) functionality. WCO 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 2013

Many improvements and new features have been introduced in SharePoint 2013. Among these new features and capabilities is the new Authentication and Authorization architecture that enables application delivery controllers or load balancers to be configured without persistence or sticky sessions. This is done through claims and the Distributed Cache service in SharePoint 2013, which distributes the authentication tokens among the web front-end servers, improving memory utilization and avoiding re-authentication of users. SharePoint 2013 uses the following claims-based authentication methods:

- Windows claims
- Security Assertion Markup Language (SAML)-based claims
- Form-based authentication claims

For more technical information on how SharePoint 2013 uses the Distributed Cache service and claims to avoid session affinity configuration on load balancers, refer to What's new in authentication for SharePoint 2013.

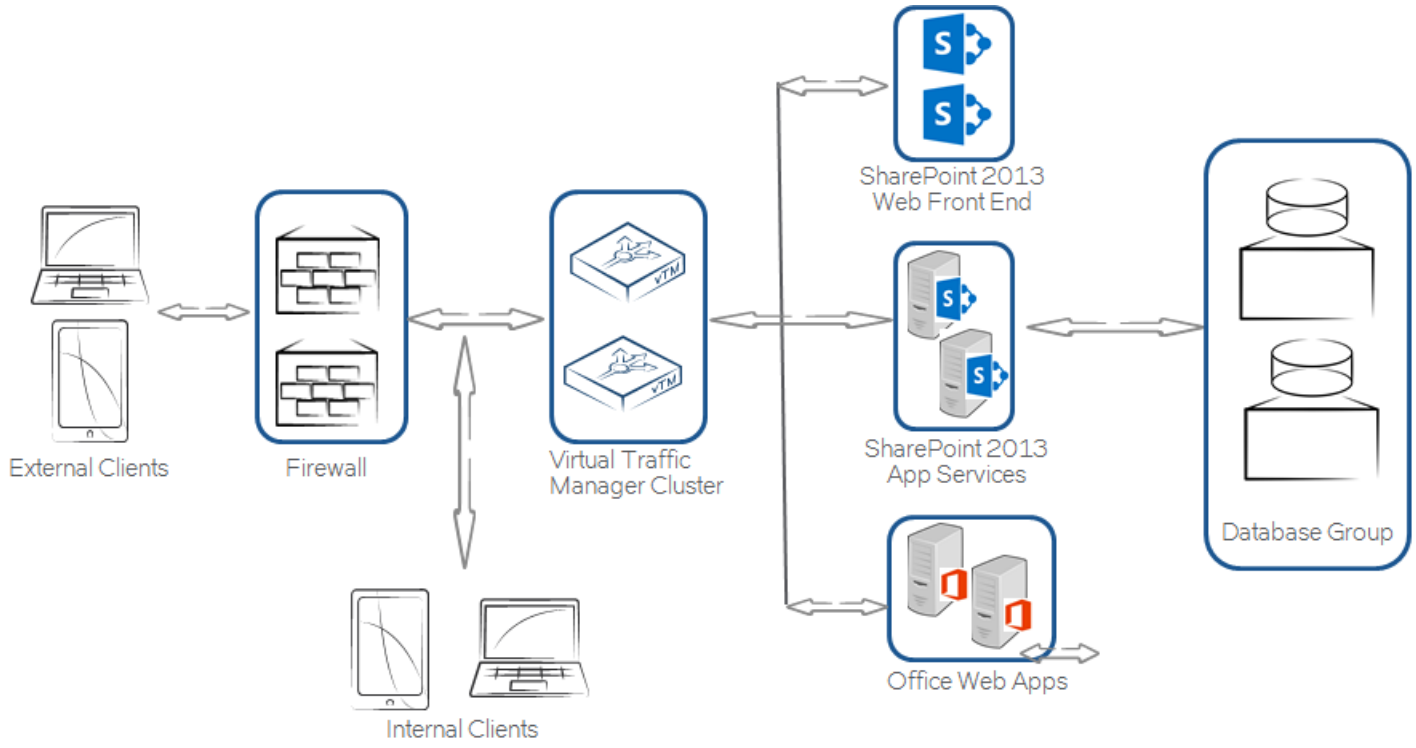
In addition, the links below provide a complete list of the new features and capabilities of SharePoint 2013, which are helpful for understanding the new features and the deployment of SharePoint 2013 farms.

- *Capabilities and Features in SharePoint 2013*
- *What's New in Microsoft SharePoint Server 2013*
- *Discontinued Features and Modified Functionality in Microsoft SharePoint 2013*

# Microsoft SharePoint 2013 Architecture

A typical SharePoint 2013 deployment consists of the web tier, the application tier, and the database tier. SharePoint 2013 uses an internal load-balancing algorithm to share the load among the servers in the application tier to improve performance and capacity through the database tier. Servers in the web tier act as the web front-end servers to handle client requests; accessibility to SharePoint farms can be scaled by adding additional web front-end servers. Brocade Virtual Traffic Manager helps load-balance the web front-end servers.

**FIGURE 1** Topology with SharePoint 2013 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 2013

## Brocade Virtual Traffic Manager with SharePoint 2013 Without SSL Offloading

This section provides step-by-step instructions for configuring Brocade Virtual Traffic Manager for simple load balancing of SharePoint 2013 web front-end servers without SSL offloading. Repeat these steps for other SharePoint Apps, such as My Sites.

> NOTE
> Session persistence is not required. SharePoint 2013 uses the Distributed Cache service to cache authentication tokens on each web front-end server.

### Understanding the Deployment Process

This section walks through the procedures required for load-balancing SharePoint 2013 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 11. |
| | 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 That Contains Web Front-End Servers and SharePoint Services on page 11. |
| | Creating a Virtual Server That Listens to the SharePoint Farm Traffic IP Group | Create a virtual server that handles all view client traffic. For details, see Creating a Virtual Server That Listens to the SharePoint Farm Traffic IP Group 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 That Contains 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: 443 or ipaddress: 443 (Note: use port 80 if HTTP is used)
   - **Monitor**—Full HTTP (Note: use Full HTTP if HTTP is used)
3. In the next screen, click **Load Balancing**.
4. Under **Algorithm**, select **Least Connections**.
5. Click the **Update** button 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**—SSL HTTPS
   - **Port**—443
   - **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.

## 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.

# Brocade Virtual Traffic Manager with SharePoint 2013 With SSL Offloading

This section provides step-by-step instructions for configuring Brocade Virtual Traffic Manager for simple load balancing of SharePoint 2013 with SSL offloading. To configure a SharePoint 2013 farm to support SSL offloading, use the instructions in the sections of the Appendix. Repeat these steps for other SharePoint Apps, such as My Sites.

NOTE

Session persistence is not required. SharePoint 2013 uses the Distributed Cache service to cache authentication tokens on each web front-end server.

## Understanding the Deployment Process

This section walks through the procedures required for load-balancing SharePoint 2013 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 12. |
| | 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 That Contains Web Front-End Servers and SharePoint Services on page 12. |
| | Creating a Virtual Server That Listens to the SharePoint Farm Traffic IP Group | Create a virtual server that handles all view client traffic. For details, see Creating a Virtual Server That Listens to the SharePoint Farm Traffic IP Group on page 13. |
| | Configuring SSL Decryption for SSL Offloading | The virtual server created in the previous step must be configured to decrypt SSL traffic. For details, see Configuring SSL Decryption for SSL Offloading on page 13. |

## 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 That Contains 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 **Least Connections**.
5. Click the **Update** button to apply changes.

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

To handle all 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: port 443 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 13.
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.

# Configuring SharePoint Apps Using a Separate Traffic IP Group

This section provides step-by-step instructions for configuring Brocade Virtual Traffic Manager for SharePoint 2013 Apps using a separate Traffic IP group. Use this approach if a different domain is used for SharePoint 2013 Apps; traffic can then be load-balanced for SharePoint Apps using another Traffic IP group.

## Understanding the Deployment Process

This section walks through the procedures required for load-balancing SharePoint 2013 with Brocade Virtual Traffic Manager.

| Component | Procedure | Description |
|---|---|---|
| Virtual Traffic Manager | Creating a Traffic IP Group for SharePoint 2013 Apps | 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 SharePoint 2013 Apps on page 14. |
| | Creating a Pool Containing SharePoint Apps Services | A pool must be created for the SharePoint Apps services managed by the Virtual Traffic Manager. For details, see Creating a Pool That Contains SharePoint Apps Services on page 14. |
| | Creating a Virtual Server That Listens to the SharePoint 2013 Apps Traffic IP Group | Create a virtual server that handles all SharePoint 2013 Apps traffic. For details, see Creating a Virtual Server That Listens to the SharePoint 2013 Apps Traffic IP Group on page 15. |
| | Configuring Session Persistence for the SharePoint Apps Services Pool | Transparent session affinity persistence is required for the SharePoint Apps services pool. For details, see Configuring Session Persistence for the SharePoint Apps Services Pool on page 15. |

## Creating a Traffic IP Group for SharePoint 2013 Apps

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 Apps (e.g., mycompanyapps.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 That Contains SharePoint Apps Services

For the SharePoint 2013 Apps services 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., SharePoint 2013 Apps)
   - **Nodes**—hostname: 443 or ipaddress: 443
   - **Monitor**—Full HTTPS
3. In the next screen, click **Load Balancing**.
4. Under **Algorithm**, select **Least Connections**.
5. Click the **Update** button to apply changes.

## Creating a Virtual Server That Listens to the SharePoint 2013 Apps Traffic IP Group

To handle all SharePoint 2013 Apps 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., mycompanyapps.com)
   - **Protocol**—SSL HTTPS
   - **Port**—443
   - **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 Session Persistence for the SharePoint Apps Services Pool

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

1. Navigate to **Services** > **Pools** and select the pool that was created earlier.
2. Navigate to **Session Persistence** and click **Edit**.
3. Select **Transparent session affinity**, and click **Update** to apply changes.

# Configuring SharePoint Apps Using an Existing Virtual Server

This section provides step-by-step instructions for configuring Brocade Virtual Traffic Manager for SharePoint 2013 Apps using an existing virtual server. Use this approach if SharePoint Apps use a single virtual server that is configured for the SharePoint farm. It is assumed that Virtual Traffic Manager is already configured for the SharePoint farm that is using SSL offloading on Virtual Traffic Manager.

# Understanding the Deployment Process

This section walks through the procedures required for load-balancing SharePoint 2013 with Brocade Virtual Traffic Manager.

| Component | Procedure | Description |
|---|---|---|
| Virtual Traffic Manager | Creating a Pool Containing SharePoint Apps Services | A pool must be created for the SharePoint 2013 Apps services managed by Virtual Traffic Manager. For details, see Creating a Pool That Contains SharePoint Apps Services on page 16. |
| | Configuring Session Persistence for the SharePoint Apps Services Pool | Transparent session affinity persistence is required for the SharePoint Apps services pool. For details, see Configuring Session Persistence for the SharePoint Apps Services Pool on page 16. |
| | Creating a TrafficScript Rule to Forward Requests to the Pool Created Previously | To share the existing virtual server, a TrafficScript rule is needed. The TrafficScript rule looks at the host header to differentiate traffic that belongs to the SharePoint Apps. For details, see Creating a TrafficScript Rule to Forward Requests to the Appropriate Pool on page 17. |

# Creating a Pool That Contains SharePoint Apps 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., SharePoint 2013 Apps)
   - **Nodes**—hostname: 443 or ipaddress: 443
   - **Monitor**—Full HTTPS
3. In the next screen, click **Load Balancing**.
4. Under **Algorithm**, select **Least Connections**.
5. Click the **Update** button to apply changes.
6. Return to the pool created, and select **SSL Settings**.
7. Set **ssl_encrypt** to **Yes**.
8. Click the **Update** button to apply changes.

# Configuring Session Persistence for the SharePoint Apps Services Pool

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 TrafficScript Rule to Forward Requests to the Appropriate Pool

To share the existing virtual server, a TrafficScript rule is needed. The TrafficScript rule looks at the host header to differentiate traffic that belongs to the SharePoint Apps. The actual TrafficScript code can be found in the Appendix.

### *Enabling a TrafficScript Variable in Traffic Manager*

First ensure that variable_pool_use is enabled. This allows a variable to be used when calling pool.select(), which is called in the TrafficScript rule.

1. Navigate to **System** > **Global Settings** > **Other Settings**.
2. Set **trafficscript!variable_pool_use** to **Yes**.
3. Scroll down to the bottom of the page and click the **Apply** button.

### *Configuring and Associating a TrafficScript with the Virtual Server*

1. Navigate to **Catalogs** > **Rules**.
2. Create a new rule:
   - **Name**—A descriptive name for the rule (e.g., SharePoint Apps Rule)
   - Use TrafficScript Language
3. Click **Create Rule**.
4. Use the TrafficScript in Appendix on page 27 for syntax.
5. Click the **Update** button.
6. Navigate to **Services** > **Virtual Servers** and select the virtual server that will be performing the TrafficScript.
7. Scroll down and click **Rules**.
8. Assign the TrafficScript to the request rules by clicking **Add Rule**.

# Office Web Apps 2013

This section provides step-by-step instructions for configuring Brocade Virtual Traffic Manager for Office Web Apps 2013. Microsoft Office Web Apps 2013 is a web-based version of the Microsoft Office suite that can integrate with Exchange, Lync, and SharePoint. In a typical SharePoint deployment, Office Web Apps servers are also deployed and integrated with SharePoint 2013. Use this guide to configure Virtual Traffic Manager to load-balance Office Web Apps 2013.

Microsoft Office Web Apps 2013 can be configured to allow SSL offloading. For more information, refer to the TechNet article at http://technet.microsoft.com/en-us/library/jj219455.aspx.

## Understanding the Deployment Process

This section walks through the procedures required for load-balancing SharePoint 2013 with the Brocade Virtual Traffic Manager.

| Component | Procedure | Description |
|---|---|---|
| Virtual Traffic Manager | Creating a Traffic IP Group for Office Web Apps 2013 | 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 Office Web Apps 2013 on page 18. |

| Component | Procedure | Description |
|---|---|---|
| | Creating a Pool Containing Office Web Apps Servers | A pool must be created for the Office Web Apps services managed by Virtual Traffic Manager. For details, see Creating a Pool That Contains Office Web Apps Servers on page 18. |
| | Configuring Session Persistence for the Office Web Apps Pool | Transparent session affinity persistence is required for the Office Web Apps pool. For details, see Configuring Session Persistence for the Office Web Apps Pool on page 18. |
| | Creating a Virtual Server That Listens to the Office Web Apps Traffic IP Group | Create a virtual server that handles all Office Web Apps traffic. For details, see Creating a Virtual Server That Listens to the Office Web Apps Traffic IP Group on page 19. |
| | (Optional) Configuring SSL Decryption for SSL Offloading | Perform this procedure only if SSL offloading is configured for Office Web Apps servers. For details, see Configuring SSL Decryption for SSL Offloading on page 19. |

# Creating a Traffic IP Group for Office Web Apps 2013

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., officeweb.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 That Contains Office Web Apps Servers

For the Office Web Apps service 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., Office Web Apps)
   - **Nodes**—hostname: 80 or ipaddress: 80 (Note: use port 443 if SSL-offload is not configured on Office Web Apps servers)
   - **Monitor**—Full HTTP (Note: use Full HTTPS if SSL-offload is not configured on Office Web Apps servers)
3. In the next screen, click **Load Balancing**.
4. Under **Algorithm**, select **Least Connections**.
5. Click the **Update** button to apply changes.

# Configuring Session Persistence for the Office Web Apps Pool

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 Office Web Apps Traffic IP Group

To handle all Office Web Apps 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 (Note: use SSL HTTPS if SSL-offload is not configured on Office Web Apps servers)
   - **Port**—443
   - **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

Perform the steps in this section only if SSL offloading is configured for Office Web Apps servers.

## *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 19.
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 2013 environment. Here are some common capabilities and best practices for deploying Brocade Virtual Traffic Manager to enhance your Microsoft SharePoint 2013 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 clients 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 utilizes and improves failover Recovery Time Objective (RTO) since global load balancing 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 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 2013**. Use the SharePoint 2013 Custom Website template when using SharePoint that is heavily customized with third-party web parts and a custom look.
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 2013 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.

# Common Troubleshooting Tips

This chapter describes tips for troubleshooting common deployment issues.

## Uploading Certificates to Virtual Traffic Manager

When uploading certificates to Virtual Traffic Manager, these must be in PEM format. For your certificates that are not in PEM format, tools are available to convert CER (without a key) and PFX (with a key) formats to PEM format, such as OpenSSL. To upload a certificate used by an Exchange server, export the certificate once with a private key and once without a private key. Use the following commands to convert the certificate to PEM format.

**Convert a DER File (.crt .cer .der) to PEM**

```
openssl x509 -inform der -in <certificate filename>.cer -out certificate.pem
```

**Convert a PKCS#12 File (.pfx .p12) Containing a Private Key and Certificates to PEM**

```
openssl pkcs12 -in <certificate key filename>.pfx -out certificatekey.pem -nodes
```

# Conclusion

This document discusses how to configure Brocade Virtual Traffic Manager to optimize the deployment of the Microsoft SharePoint 2013 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.

# Appendix

## Configuring Alternate Access Mapping for SSL Offloading on SharePoint 2013

To enable SSL offloading on Virtual Traffic Manager for SharePoint 2013, an alternate access mapping should be configured for the SharePoint farm to allow HTTP access to the farm. To configure alternate access mappings:

1. Log in to the **Central Administration** website.
2. Navigate to **Application Management** and select **Configure alternate access mappings**.
3. Select **Add Internal URLs**.
4. Enter the HTTP URL of the SharePoint website in the **URL protocol**, **host**, and **port** fields (e.g., website: https://sp.mycompany.com Alternate Access: http://sp.mycompany.com).

## Configuring Binding in IIS

Perform the following steps on each web front-end server in the farm.

1. Log in to a SharePoint web front-end server.
2. Open Internet Information Services (IIS) Manager.
3. On the left pane, under **Sites**, select the SharePoint farm website.
4. Select **Bindings** on the right pane.
5. Click **Add** in **Site Bindings**, and enter the following details:
   - **Type:** http
   - **IP Address:** Select the IP assigned to this SharePoint website farm
   - **Port:** 80
   - **Host name:** SharePoint website farm URL
6. Click **OK** and then **Close**.

## Configuring SharePoint Search Result for Alternate Access Mappings

Perform the following steps if search through alternate access mapping does not show HTTPS results.

> NOTE
> Performing full index crawling may take a significant amount of time depending on the SharePoint data size.

1. Log in to the SharePoint **Central Administration** website.

2. Navigate to **System Settings** > **Manage Services on Server**.
3. Select **SharePoint Server Search**, and then select **Search Service Application**.
4. On the left pane under **Crawling**, select **Content Sources**.
5. Select the **Content Source** that is hosting the HTTPS SharePoint farm URL.
6. Ensure that the alternate access mappings URL is included in **Start Addresses**, or add the URL.
7. Click **OK** to save.
8. Navigate to **Index Reset**.
9. Click **Reset Now**.
10. Navigate to **Content Sources**, and ensure that Content Source Crawling is **starting**.

# TrafficScript Code for SharePoint 2013 Apps Using an Existing Virtual Server

The following TrafficScript code is used to direct incoming SharePoint Apps traffic to its corresponding pool.

```
#// TS Rule for redirecting SharePoint traffic to relevant pools
# SharePoint Apps TrafficIP
$debug = 0; // Change value to 1 if debug needed
$apps_pool = "SharePoint Apps TrafficIP";
$farm_pool = "SP Project Site Pool";
$path = http.getPath();
$pool = "";

$header = http.getHostHeader();
if(string.contains( $ header, "apps.mycompany.com" )) {
    $pool = $apps_pool;
        if ($debug > 0) { log.info("SharePoint Apps Pool Selected");}
} else {
    $pool = $farm_pool;
        if ($debug > 0) { log.info("SP Project Site Pool Selected");}
}
pool.select ( $pool );
```