BROCADE

DEPLOYMENT GUIDE

# Brocade Virtual Traffic Manager and Microsoft Exchange 2013 Deployment Guide

*53-1003936-03*
*27 February 2017*

# Contents

# Preface



## About This Guide

The *Brocade Virtual Traffic Manager and Microsoft Exchange 2013 Deployment Guide* describes how to configure Brocade Virtual Traffic Manager (Brocade vTM) to load-balance and optimize Microsoft Exchange 2013 Client Access Servers (CASs). 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 Exchange administrators, and developer operations (DevOps) professionals who are familiar with administering and managing both application delivery controllers (ADCs) and Microsoft Exchange network protocols such as EWS, EAC, PS, POP, and IMAP. You should also be familiar with installing and configuring a virtual appliance in a virtual VMware, Hyper-V, or dedicated Linux environment.

## 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 |
|---|---|---|
| January 2016 | 53-1003936-01 | Initial release. |
| January 2017 | 53-1003936-02 | Minor corrections. |
| February 2017 | 53-1003936-03 | Added Web Accelerator and vWAF content. |

# Solution Overview



This chapter describes how Brocade Virtual Traffic Manager provides advanced load balancing and application delivery controller features for Microsoft Exchange 2013; the factors that you need to consider when designing your Virtual Traffic Manager deployment; and how and when to implement the most commonly used features.

## 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.

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 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. 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.

# What's New in Microsoft Exchange 2013

Microsoft Exchange 2013 has undergone significant enhancements since Microsoft Exchange 2010. One of the most important changes is the separation of server roles to Client Access Server (CAS) and Mailbox Server. The Client Access Server's primary role is a proxy that connects and authenticates clients to the Exchange 2013 Mailbox Server. The Mailbox Server is responsible for rendering all data, including rendering web content and routing e-mail. Because of this change, persistence (sticky sessions) are not required on load balancers, because the CAS is a stateless proxy server for connecting clients to a Mailbox Server.

In addition, in Exchange 2013, all communication between the client and the server is done through the RPC over HTTP protocol, also known as Outlook Anywhere. Exchange 2013 also supports the use of a Layer 4 load balancer to distribute requests at the transport layer.

Other notable changes in Exchange 2013 include:

- Unlike Microsoft Exchange 2010, CAS array configuration is not required in Microsoft Exchange 2013 because multiple CAS servers with the same host name can be load-balanced and configured for high availability.
- RPC/TCP is no longer supported. All service access is through Outlook Anywhere (RPC/HTTP).
- All Exchange services now require secure connections. Microsoft does not support SSL offloading.
- The Hub Transport Server role is no longer available in Microsoft Exchange 2013 and is handled by the Transport Service on the Mailbox Server and the Front End Transport Service on CAS servers.

For a complete list of new features and changes in Exchange 2013, refer to the following Microsoft TechNet links:

- What's discontinued in Exchange 2013
- Architectural changes in load balancing for Exchange Server 2013

# Why Brocade vTM to Load-Balance and Optimize Microsoft Exchange 2013

Brocade Virtual Traffic Manager has significant advantages over other ADCs for load-balancing and optimizing Microsoft Exchange 2013.

## Application-Centric View

- Ability to deploy a separate ADC per application or tenant
- Ability to dynamically right-size the Brocade virtual deployment to fit the application needs
- Dynamic provisioning and scaling of ADC resources

## Designed with Service Providers in Mind

- 64-bit software that can be deployed in a VMware or Hyper-V environment or as a dedicated software installation, instead of a physical appliance
- Multicore packet processing for scalability
- Robust APIs for simple automated provisioning and management

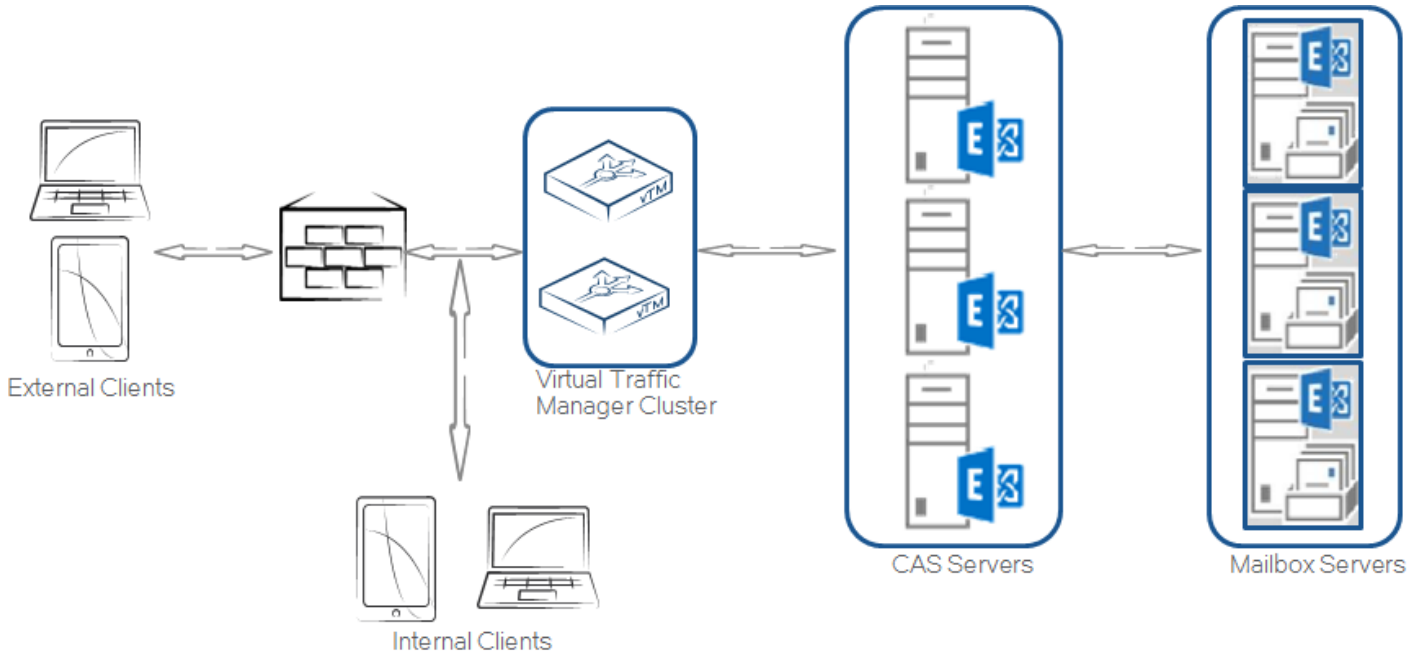
## Designed for Services

- Global load balancing, SSL offloading, caching, and service-level management
- Application firewalling and web content optimization
- Robust and open APIs

# Microsoft Exchange 2013 Architecture

Brocade Virtual Traffic Manager can be easily deployed to an existing network infrastructure with little to no changes required on the network. Brocade Virtual Traffic Manager can be deployed to support both internal and external clients. DNS is used to redirect traffic for internal and external clients to Brocade Virtual Traffic Manager. DNS configuration is used to redirect traffic for Outlook clients to Brocade Virtual Traffic Manager. Brocade vTMs can be clustered to provide high availability and load balancing to support a large amount of traffic and fault tolerance.

**FIGURE 1** Microsoft Exchange Server




Exchange 2013 HTTPS services can be load-balanced using any of the following deployment scenarios.

| Deployment Type | Pros | Cons |
|---|---|---|
| Single Virtual Traffic Manager with Single Pool | • Quick setup<br>• Consumes less resources on vTM | • No health monitoring per Exchange HTTP service |
| Multiple Virtual Servers with Multiple Pools | • Quick setup<br>• Consumes less resources on vTM<br>• Health monitoring per Exchange HTTP service | • Multiple external IP addresses and URLs |
| Single Virtual Server with Multiple Pools | • Health monitoring per Exchange HTTP service<br>• Single external IP address and URL | • More difficult to set up<br>• Consumes more resources on vTM |

# Deploying Brocade Virtual Traffic Manager



This chapter describes the procedures for deploying Brocade Virtual Traffic Manager for load-balancing and optimizing Microsoft Exchange 2013 Client Access Servers (CASs).

# Requirements

- Brocade Virtual Traffic Manager (10.1 or later)
- Microsoft Exchange 2013

The following are the prerequisites for deploying Microsoft Exchange 2013 with Brocade Virtual Traffic Manager.

## Exchange 2013 Port Requirements

The following table describes the ports used by Exchange 2013.

| CAS Service Name | Protocol | TCP Port | Description |
|---|---|---|---|
| Outlook Anywhere (OA) | HTTPS | 443 | Also known as RPC over HTTP, allows clients using Microsoft Outlook 2007, 2010, and 2013 to connect to their Exchange servers. |
| Autodiscover | HTTPS | 443 | Helps Outlook clients with automatic configuration and profile settings. |
| Exchange Web Service (EWS) | HTTPS | 443 | Enables client applications to communicate with Exchange servers. |
| Exchange Admin Center (EAC) | HTTPS | 443 | New web-based management console that replaced Exchange Management Console (EMC) and Exchange Control Panel (ECP) in Exchange 2010. |
| Outlook Web Access (OWA) | HTTPS | 443 | Provides access to Outlook and e-mails through the web. |
| Exchange ActiveSync (EAS) | HTTPS | 443 | Provides the Exchange protocol for mobile synchronization. |
| Offline Address Book (OAB) | HTTPS | 443 | Provides a copy of address lists that the user can access while disconnected from the network. |
| PowerShell (PS) | HTTPS | 443 | Also known as Exchange Management shell, provides a powerful command-line interface for administration tasks and automation. |
| POP3 | POP3/ POP3s | 110, 995 | Post Office Protocol 3 is an e-mail protocol that supports offline mail processing. |
| IMAP4 | IMAP4/ IMAP4s | 143, 993 | Interactive Mail Access Protocol is an e-mail protocol that supports offline and online mail processing. |

## Certificate Requirement

In the Exchange 2013 CAS server, all communications are done through HTTPS. Data is encrypted using certificates. A client can be redirected to a different CAS server in a CAS array other than the CAS server that authenticated it originally. To avoid having the client authenticate again against a different server and to ensure that data is decrypted correctly, use a certificate that is shared among the CAS servers and Brocade Virtual Traffic Manager (vTM).

A single certificate using Subject Alternative Name (SAN) extension can be used to support all services on a CAS server. If separate certificates are used for different services, ensure that those certificates are imported into all other CAS servers and vTMs as appropriate.

## Brocade Virtual Traffic Manager Platform Support

Brocade Virtual Traffic Manager is available on different platforms such as Linux, Solaris, Hyper-V, and VMware; it can be installed as pure software or as a virtual appliance. The Brocade Virtual Traffic Manager is available for download at http://my.brocade.com.

# Configuring Multiple Virtual Servers for Each Exchange HTTP Service



The Exchange 2013 architecture supports the use of Layer 4 load balancing for CAS arrays since no protocol or service is rendered on the CAS server. Because of this architecture change, CAS servers are now stateless, and persistence on the Virtual Traffic Manager is not required.

Deploying the Virtual Traffic Manager with multiple virtual servers requires provisioning an IP address for each virtual server created for every Exchange HTTP service. This approach provides health monitoring per HTTP service, and each virtual server can be managed independently from one another.

| Component | Procedure | Description |
|---|---|---|
| Virtual Traffic Manager (repeat for each service) | Creating a Traffic IP Group for Each Exchange HTTP Service | A traffic IP group must be created for each Exchange service. For details, see Creating Traffic IP Groups on page 13. |
| | Creating a Pool for Each Exchange HTTP Service | Enter the hostname or IP address of the node, along with the TCP/UDP port. For details, see Creating Pools on page 14. |
| | Selecting a Monitor for the Pool | Select a health monitor for the pool. For details, see Creating Pools on page 14. |
| | Creating a Virtual Server for Each Exchange HTTP Service | Create and associate the virtual server to the server pool of choice and the traffic IP group to listen on. For details, see Creating Virtual Servers on page 15. |
| | Configuring SSL Decryption | Configure SSL decryption to enable SSL offloads. For details, see Configuring SSL Decryption on page 15. |

## Creating Traffic IP Groups

Identify the Exchange HTTP services offered by the CAS servers, and create a traffic IP group for each service.

Create a traffic IP group (also known as a virtual IP) on which the virtual server will be listening.

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 traffic IP group (e.g., owa.company.com)
   - **IP Addresses**—An IP address that will be associated to the FQDN of this service
3. Click the **Create Traffic Group** button.

   Repeat Steps 1 to 3 for each Exchange service that will be load-balanced through Brocade Virtual Traffic Manager.

# Creating Pools

For each of the identified Exchange HTTP services, 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., OWA service)
   - **Nodes**—hostname:443 or ipaddress:443
   - **Monitor**—No monitor (this is covered in detail in a later section)
3. In the next screen, click **Load Balancing**.
4. Under **Algorithm**, select **Perceptive**.
5. Click the **Update** button to apply changes.
6. Click **SSL Settings**.
7. Check the **Yes** button next to **ssl_encrypt**.
8. Click the **Update** button to apply changes.
9. Navigate to **Pool** > **Connection Management**, and make the following changes:
   - **Max_connect_time**: 5-10 sec (left to user preference)
   - **Max_reply_time**: 120 sec (default RPC and ISS timeout template in Exchange 2013)
   - **Queue_timeout**: 120 sec (default RPC and ISS timeout template in Exchange 2013)
   - **Node_connclose**: yes (make sure to cut traffic to a node when failure occurs)
10. Repeat Step 1 through Step 9 to create a pool for each Exchange HTTP service.

# Creating Monitors

This section details the steps to create health monitors.

> NOTE
> Advanced external monitors can be written in any language of choice and be associated with the pool.

Create a health monitor to monitor the health of a pool.

1. Navigate to **Catalogs** > **Monitors**.
2. Scroll down to **Create new monitor**.
3. Give the new monitor a descriptive name.
4. Set the type to **HTTP monitor** and the scope to **Node**.
5. Click **Create Monitor** to create the monitor.
6. In the subsequent configuration page, scroll down and set **use_ssl** to **Yes**.
7. Change **host_header:** to the service URL path (e.g., owa.company.com).
8. Change **Path:** to **/<Path>/healthcheck.htm** (e.g., /OWA/healthcheck.htm).
9. Change **status_regex** to **^200$** .
10. Change **body_regex** to **.*200 OK**.
11. Scroll down to **Apply Changes** and click the **Update** button.
12. Navigate to **Services** > **Pools** and select the pool that the monitor will be attached to.

13. Scroll down and click **Health Monitoring**.
14. Add the appropriate health monitor.

    Repeat Steps 1 to 14 to create a health monitor for each Exchange HTTP service pool. Refer to the following table for the path that should be used for each service.

| Service Name | Path |
|---|---|
| Outlook Anywhere (OA) | /rpc/healthcheck.htm |
| Autodiscover | /Autodiscover/healthcheck.htm |
| Exchange Web Service (EWS) | /EWS/healthcheck.htm |
| Exchange Admin Center (EAC) | /ECP/healthcheck.htm |
| Outlook Web Access (OWA) | /OWA/healthcheck.htm |
| Exchange ActiveSync (EAS) | /Microsoft-Server-ActiveSync/healthcheck.htm |
| Offline Address Book (OAB) | /OAB/healthcheck.htm |
| PowerShell (PS) | /PowerShell/healthcheck.htm |

# Creating Virtual Servers

For each of the identified Exchange HTTP services, create a virtual server by 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., owa.company.com)
   - **Protocol**—HTTP
   - **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 appropriate traffic IP group that was created for the OWA service.
5. Set **Enabled** to **Yes**.
6. Click the **Update** button to apply the changes.

   Repeat Step 1 through Step 6 to create a virtual server for each Exchange HTTP service.

# Configuring SSL Decryption

To perform SSL decryption, the certificate and the private key used for the virtual server created in the previous task 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.

   After importing the certificate, enable SSL decryption on the virtual server created.
3. Navigate to **Services** > **Virtual Servers** and select the virtual server created for POP3 that will be performing SSL decryption.
4. Scroll down and click **SSL Decryption**.

5. Set **ssl_decrypt** to **Yes**.
6. Select the certificate imported in Step 2.
7. Scroll down to the bottom of the page and click **Update**.

# Configuration Summary

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

# Configuring a Single Virtual Server for All Exchange HTTP Services with Multiple Pools



This approach uses a single IP address that is mapped to the FQDN of all Exchange HTTP services and uses multiple pools for each service. Using a TrafficScript, Virtual Traffic Manager directs the traffic to its appropriate pool, and each pool can be monitored separately.

This section contains step-by-step instructions to configure Virtual Traffic Manager for a single virtual server for all Exchange HTTP services with multiple pools.

| Component | Procedure | Description |
|---|---|---|
| Virtual Traffic Manager (repeat for each service) | Creating a Traffic IP Group for each Exchange HTTP Service | A single traffic IP group must be created for all Exchange services. For details, see Creating Traffic IP Groups on page 17. |
| Virtual Traffic Manager (repeat for each service) | Creating a Pool for Each Exchange HTTP Service | Enter the hostname or IP address of the node, along with the TCP/UDP port. For details, see Creating Pools on page 18. |
| | Selecting a Monitor for the Pool | Select a health monitor for the pool. For details, see Creating Monitors on page 18. |
| Virtual Traffic Manager (once) | Creating a Virtual Server for Each Exchange HTTP Service | Create and associate the virtual server to the server pool of choice and the traffic IP group to listen on. For details, see Creating Virtual Servers on page 19. |
| Virtual Traffic Manager (as required) | Configuring SSL Decryption | Configure SSL decryption to enable SSL offloads. For details, see Configuring SSL Decryption on page 19. |
| Virtual Traffic Manager (as required) | Creating and Associating a Traffic Script That Forwards the Requests to the Appropriate Pool with the Virtual Server | Configure a traffic script to forward requests to relevant pools. For details, see Creating and Associating a Traffic Script That Forwards the Requests to the Appropriate Pool with the Virtual Server on page 20. |

## Creating Traffic IP Groups

Create a traffic IP group (also known as a virtual IP) on which the virtual server will listen.

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 Exchange HTTP services (e.g., mail-lb.company.com)
   - **IP Addresses**—An IP address that will be associated to the FQDN of all Exchange HTTP services
3. Click the **Create Traffic Group** button.

# Creating Pools

For each of the identified Exchange HTTP services, 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., OWA service)
   - **Nodes**—hostname:443 or ipaddress:443
   - **Monitor**—No monitor (this is covered in detail in a later section)
3. In the next screen, click **Load Balancing**.
4. Under **Algorithm**, select **Perceptive**.
5. Click the **Update** button to apply changes.
6. Click **SSL Settings**.
7. Check the **Yes** button next to **ssl_encrypt**.
8. Click the **Update** button to apply changes.
9. Navigate to **Pool** > **Connection Management**, and make the following changes:
   - **Max_connect_time**: 5–10 sec (left to user preference)
   - **Max_reply_time**: 120 sec (default RPC and ISS timeout template in Exchange 2013)
   - **Queue_timeout**: 120 sec (default RPC and ISS timeout template in Exchange 2013)
   - **Node_connclose**: yes (make sure to cut traffic to a node when failure occurs)

   Repeat Step 1 through Step 9 to create a pool for each Exchange HTTP service.

# Creating Monitors

This section details the steps to create health monitors.

> NOTE
> Advanced external monitors can be written in any language of choice and be associated with the pool.

Create a health monitor to monitor the health of a pool.

1. Navigate to **Catalogs** > **Monitors**.
2. Scroll down to **Create new monitor**.
3. Give the new monitor a descriptive name.
4. Set the type to **HTTP monitor** and the scope to **Node**.
5. Click **Create Monitor** to create the monitor.
6. In the subsequent configuration page, scroll down and set **use_ssl** to **Yes**.
7. Change **host_header:** to the service URL path (e.g., owa.company.com).
8. Change **Path:** to **/<Path>/healthcheck.htm** (e.g., /OWA/healthcheck.htm).
9. Change **status_regex** to **^200$** .
10. Change **body_regex** to **.*200 OK**.
11. Scroll down to **Apply Changes** and click the **Update** button.
12. Navigate to **Services** > **Pools** and select the pool that the monitor will be attached to.

13. Scroll down and click **Health Monitoring**.
14. Add the appropriate health monitor.

    Repeat Steps 1 to 14 to create a health monitor for each Exchange HTTP service pool. Refer to the table below for the path that should be used for each service.

| Service Name | Path |
|---|---|
| Outlook Anywhere (OA) | /rpc/healthcheck.htm |
| Autodiscover | /Autodiscover/healthcheck.htm |
| Exchange Web Service (EWS) | /EWS/healthcheck.htm |
| Exchange Admin Center (EAC) | /ECP/healthcheck.htm |
| Outlook Web Access (OWA) | /OWA/healthcheck.htm |
| Exchange ActiveSync (EAS) | /Microsoft-Server-ActiveSync/healthcheck.htm |
| Offline Address Book (OAB) | /OAB/healthcheck.htm |
| PowerShell (PS) | /PowerShell/healthcheck.htm |

# Creating Virtual Servers

To handle all Exchange 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
   - **Protocol**—HTTP
   - **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 appropriate traffic IP group that was created for the OWA service.
5. Set **Enabled** to **Yes**.
6. Click the **Update** button to apply the changes.

# Configuring SSL Decryption

To perform SSL decryption, the certificate and the private key used for the virtual server created in the previous task 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.

   After importing the certificate, enable SSL decryption on the virtual server created.
3. Navigate to **Services** > **Virtual Servers** and select the virtual server created for Exchange HTTP services that will be performing SSL decryption.
4. Scroll down and click **SSL Decryption**.

5. Set **ssl_decrypt** to **Yes**.
6. Select the certificate imported in Step 2.
7. Scroll down to the bottom of the page and click **Update**.

# Creating and Associating a Traffic Script That Forwards the Requests to the Appropriate Pool with the Virtual Server

Because a single virtual server is used for all Exchange 2013 HTTP services, incoming traffic should be forwarded to an appropriate pool. This can be done through TrafficScript in Brocade Virtual Traffic Manager. To create a traffic script that can accept variables, perform the following steps.

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.
4. Navigate to **Catalogs** > **Rules**.
5. Create a new rule:
   - **Name**—A descriptive name for the rule (e.g., Exchange 2013 Single Traffic IP)
   - Use TrafficScript Language
6. Click **Create Rule**.
7. Use the TrafficScript in Appendix on page 36 for the syntax.
8. Click the **Update** button.
9. Navigate to **Services** > **Virtual Servers** and select the virtual server created for Exchange HTTP services that will be performing the TrafficScript.
10. Scroll down and click **Rules**.
11. Assign the TrafficIP script to the request rules by clicking **Add Rule**.

# Configuration Summary

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

# Configuring a Single Virtual Server with a Single Pool



Deploying Brocade Virtual Traffic Manager as a single virtual server with a single pool for all Exchange 2013 HTTP services is the simplest and quickest approach. In this scenario, Brocade Virtual Traffic Manager simply load-balances the traffic that passes through to the CAS servers, and a health monitor can be configured for only one service. The disadvantage of using of this approach is that if the monitoring service is unhealthy, all other services will become unavailable. Flexibility in terms of management and the load-balancing algorithm is not individual but by group.

| Component | Procedure | Description |
|---|---|---|
| Virtual Traffic Manager (once) | Creating a Traffic IP Group for Exchange Services | A single traffic IP group must be created for all Exchange services. For details, see Creating Traffic IP Groups on page 21. |
| | Creating a Pool for Each Exchange HTTP Service | A pool must 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 Creating Pools on page 21. |
| | Selecting a Monitor for the Pool | Select a health monitor for the pool. For details, see Creating Monitors on page 22. |
| | Creating a Virtual Server for Each Exchange HTTP Service | Create and associate the virtual server to the server pool. For details, see Creating Virtual Servers on page 23. |
| | Configuring SSL Decryption | Configure SSL decryption to enable SSL offloads. For details, see Configuring SSL Decryption on page 23. |

## Creating Traffic IP Groups

Create a traffic IP group (also known as a virtual IP) on which the virtual server will listen.

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 Exchange HTTP services (e.g., mail.company.com)
   - **IP Addresses**—An IP address that will be associated to the FQDN of all Exchange HTTP services
3. Click the **Create Traffic Group** button.

## Creating Pools

A pool must be created for each service that is managed by the Virtual Traffic Manager. 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
   - **Nodes**—hostname:443 or ipaddress:443
   - **Monitor**—No monitor
3. In the next screen, click **Load Balancing**.
4. Under **Algorithm**, select **Perceptive**.
5. Click the **Update** button to apply changes.
6. Click **SSL Settings**.
7. Check the **Yes** button next to **ssl_encrypt**.
8. Click the **Update** button to apply changes.
9. Navigate to **Pool** > **Connection Management**, and make the following changes:
   - **Max_connect_time**: 5–10 sec (left to user preference)
   - **Max_reply_time**: 120 sec (default RPC and ISS timeout template in Exchange 2013)
   - **Queue_timeout**: 120 sec (default RPC and ISS timeout template in Exchange 2013)
   - **Node_connclose**: yes (make sure to cut traffic to a node when failure occurs)

# Creating Monitors

This section details the steps to create health monitors.

> NOTE
> Advanced external monitors can be written in any language of choice and be associated with the pool. Select an Exchange HTTP service for health monitoring.

In this example, the OWA service will be monitored. The HTTP monitor is used for port 443 for the OWA service.

1. Navigate to **Catalogs** > **Monitors**.
2. Scroll down to **Create new monitor**.
3. Give the new monitor a descriptive name.
4. Set the type to **HTTP monitor** and the scope to **Node**.
5. Click **Create Monitor** to create the monitor.
6. In the subsequent configuration page, scroll down and set **use_ssl** to **Yes**.
7. Change **host_header:** to the service URL path (e.g., owa.company.com).
8. Change **Path:** to **/OWA/healthcheck.htm**.
9. Change **status_regex** to **^200$**.
10. Change **body_regex** to **.*200 OK**.
11. Scroll down to **Apply Changes** and click the **Update** button.
12. Navigate to **Services** > **Pools** and select the pool that the monitor will be attached to.
13. Scroll down and click **Health Monitoring**.
14. Add the appropriate health monitor.

# Creating Virtual Servers

Create a virtual server that will handle all Exchange 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**—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 appropriate traffic IP group that was created earlier.
5. Set **Enabled** to **Yes**.
6. Click the **Update** button to apply the changes.

# Configuring SSL Decryption

To perform SSL decryption, the certificate and the private key used for the virtual server created in the previous task 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.

   After importing the certificate, enable SSL decryption on the virtual server created.
3. Navigate to **Services** > **Virtual Servers** and select the virtual server that will be performing SSL decryption.
4. Scroll down and click **SSL Decryption**.
5. Set **ssl_decrypt** to **Yes**.
6. Select the certificate imported in Step 2.
7. 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 glance through to get a good understanding of how the services are configured.

# Configuring IMAP4 and POP3



The IMAP4 and POP3 services on Exchange 2013 enable mail clients that support the IMAP4 and POP3 protocols to access Exchange 2013 CAS servers running the IMAP4 and POP3 services. By default, these services are disabled in Exchange 2013. To support these protocols, IMAP4 and POP3 services must be enabled.

For more information about how to manage and configure POP3 and IMAP4 in Exchange 2013, see http://technet.microsoft.com/en-us/library/jj657728.

| Component | Procedure | Description |
|---|---|---|
| Virtual Traffic Manager (once each for the POP3 and IMAP4 services) | Creating a Traffic IP Group for Both POP3 and IMAP4 Services | A traffic IP group must be created on which a virtual server listens. For details, see Creating Traffic IP Groups on page 24. |
| | Creating a Pool for Both POP3 and IMAP4 Services | A pool must 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 Creating Pools on page 24. |
| | Creating a Virtual Server for Both POP3 and IMAP4 Services | Create and associate a virtual server to the server pool. For details, see Creating Virtual Servers on page 25. |
| | Configuring SSL Decryption for Both POP3 and IMAP4 Services | Configure SSL decryption to enable SSL offloads. For details, see Configuring SSL Decryption on page 25. |

## Creating Traffic IP Groups

Create a traffic IP group (also known as a virtual IP) on which the virtual server will listen.

1. Navigate to **Services** > **Traffic IP Groups** and scroll down to **Create a new Traffic IP Group**.
2. Enter the following:
   - **Name**—A descriptive name for the POP3 and IMAP4 pool, assuming that the POP3 and IMAP4 FQDN resolves to the same traffic IP group (e.g., pop.company.com)
   - **IP Addresses**—An IP address that will be associated to the FQDN of the POP3 and IMAP4 service
3. Click the **Create Traffic Group** button.

## Creating Pools

For each 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
   - **Nodes**—hostname:110 or ipaddress:110
   - **Monitor**—POP
3. In the next screen, click **Load Balancing**.

4. Under **Algorithm**, select **Perceptive**.
5. Click the **Update** button to apply changes.

   Repeat Steps 1 to 5 to create a new pool for IMAP4 using port 143 for the **Nodes**.

   For IMAP4, the health monitor should be a TCP transaction monitor. Perform the following steps to create a new health monitor.
6. Navigate to **Catalogs** > **Monitors** and scroll down to **Create New Monitor**. Type a name and select **TCP Transaction Monitor**.
7. Use the following values for parameters:
   - close_string: **logout\r\n**
   - delay: **10**
   - response_regex: *** OK.***
   - timeout: **10**
8. Navigate to **Services** > **Pools** and under **Health Monitoring**, select the created monitor.

# Creating Virtual Servers

To handle all the 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
   - **Protocol**—POP3
   - **Port**—995
   - **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 appropriate traffic IP group that was created for the service.
5. Set **Enabled** to **Yes**.
6. Click the **Update** button to apply the changes.

   Repeat Steps 1 to 6 to create a virtual server for IMAP4 using **Protocol: IMAP4** and **Port: 993**.

# Configuring SSL Decryption

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

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

   After importing the certificate, enable SSL decryption on the virtual server created.
3. Navigate to **Services** > **Virtual Servers** and select the virtual server created for POP3 that will be performing SSL decryption.
4. Scroll down and click **SSL Decryption**.
5. Set **ssl_decrypt** to **Yes**.

6. Select the certificate imported in Step 2.
7. Scroll down to the bottom of the page and click **Update**.

   Repeat Steps 1 to 7 to enable SSL decryption on the virtual server for IMAP4.

# Configuration Summary

By accessing the **Services** > **Config Summary** on the web GUI, a complete snapshot of all configured services is provided. This is a very useful table to glance through to get a good understanding of 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 Exchange 2013 environment. Here are some common capabilities and best practices for deploying Brocade Virtual Traffic Manager to enhance your Microsoft Exchange 2013 deployment.

## Service-Level Monitoring

Service-level monitoring continually checks the responses of your CAS servers and sends alerts should these fall below an expected threshold of performance. In addition to sending alerts, TrafficScript can be used to remove the service or server from the pool until the performance issue has been fixed. TrafficScript can also be used to reprioritize traffic and even to reallocate bandwidth. This capability increases the availability and service level of Microsoft Exchange.

Configuring the Virtual Traffic Manager for service-level monitoring of Exchange 2013 is outside the scope of this document. For more information, please contact Brocade.

## Global Load Balancing

Global load balancing enables Client Access Servers to be distributed across multiple locations, for either business continuity/disaster recovery or for locating the servers geographically closer to end users. This enables seamless failover if a datacenter has an outage and greater performance for users distributed geographically.

Configuring the Virtual Traffic Manager for global load balancing is outside the scope of this document. For more information, please contact Brocade.

## Limiting Access for ECP and PowerShell HTTP Services

In Exchange 2013, all services are SSL-based and are hosted on a single website; therefore, other administrative services such as Exchange Control Panel and PowerShell can be accessed through the same URL. For greater security, it is often desirable to control access to these services.

Brocade Virtual Traffic Manager offers flexibility in securing access to ECP and PowerShell services with one of the following techniques:

- **Authentication**—Using authenticators and a TrafficScript rule to perform authentication.

- **Restricting access based on IP**—Source IPs can be monitored to allow only certain IPs or subnets to have access to these services.
- **Accessing different services through a specific URL**—As discussed earlier, Exchange services are hosted on a single website, and thus different services can be accessed through the same URL. For example, *owa.company.com/owa* is used to access Outlook Web Access, and the same website *owa.company.com/ecp* can be used to access Exchange Control Panel. Brocade Virtual Traffic Manager can be configured through a TrafficScript rule to ensure that the ECP service can be accessed only via the *ecp.company.com/ecp* URL.

For example, the following sample TrafficScript provides access to ECP through a specific URL. Assign this TrafficScript to virtual services that provide the Exchange HTTP service.

```
$hostheader = http.getHostHeader();
$debug = 0; // Change value to 1 if debug needed
if( ($hostheader != "ecp.company.com") && (http.getPath() == "/ecp"))
{
   http.sendResponse( "400 Bad Request", "text/plain","Bad Request", "");
   if ($debug > 0) { log.info("Request classified as Bad");}
}
```

For more information on securing access to ECP and PowerShell, please contact Brocade.

# Removing ActiveSync Access from Specific Device Types

Mobile device ActiveSync traffic can be optimized by removing access from unapproved device types, meaning that only approved device types can access Microsoft Exchange 2013. Brocade Virtual Traffic Manager can be configured to block access via specific devices over ActiveSync by using a TrafficScript rule like the following.

```
$phone = http.getHeader( "user-agent" );
$debug = 0; // Change value to 1 if debug needed
if(string.contains( $phone, "Apple" ) && (http.getPath() == "/Microsoft-Server-ActiveSync") )
{
   http.sendResponse( "400 Bad Request", "text/plain","Bad Request", "");
      if ($debug > 0) { log.info("Request classified as Bad");}
}
```

For more information on securing access for specific device types, contact Brocade.

# Digital Certificates and SSL

All communication between client and server is done through SSL. Brocade Virtual Traffic Manager can use certificates to decrypt incoming services such as POP3 and IMAP4. In addition, Brocade vTM provides SSL offloading for earlier versions of Exchange like Exchange 2010. To provide SSL decryption and offloading, the certificates should be imported into Brocade Virtual Traffic Manager.

Microsoft best practices recommend the use of trusted third-party SAN certificates that can represent multiple domain names, and Brocade recommends that you follow these suggestions and best practices provided by Microsoft on TechNet:

http://technet.microsoft.com/en-us/library/dd351044

# Redirecting OWA HTTP Requests to SSL

Brocade Virtual Traffic Manager can easily be configured to help clients that access OWA through nonencrypted port 80 to be automatically redirected to connect on SSL.

This section contains step-by-step instructions for configuring Virtual Traffic Manager for redirecting all HTTP requests to SSL:

- Create a virtual server with the traffic pool set to discard.
- Create and associate a traffic script to redirect to the proper SSL URL.

## Creating a Virtual Server with the Traffic Pool Set to Discard

Create a virtual server to handle all OWA traffic by performing the following steps.

1. Enter the following:
   - **Virtual Server Name**—A descriptive name for the virtual server
   - **Protocol**—HTTP
   - **Port**—80
   - **Default Traffic Pool**—discard
2. Click **Create Virtual Server**.
3. In the next screen, set **Enabled** to **Yes**.
4. Click the **Update** button to apply changes.

## Creating and Associating a Traffic Script to Redirect to the Proper SSL URL

1. Navigate to **Catalogs** > **Rules**.
2. Create a new rule:
   - **Name**—A descriptive name for the rule (e.g., OWA_Redirect_SSL)
   - Use TrafficScript Language
3. Click **Create Rule**.
4. Use the TrafficScript in Appendix on page 36 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**.

# Configuring Clustering for Brocade Virtual Traffic Manager

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

Use the following steps to join a Brocade 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, and provide a username and password for the cluster. Click **Next** to continue.
6. Select **Yes, and 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



ATTENTION

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

## Web Accelerator

Web Accelerator is a 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 Exchange, enable the Web Accelerator for the OWA service using the following procedure.

1. Click the virtual server on which Web Accelerator is 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 the **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 application scope selected, select **Web Accelerator Profile**. In this case, select **Express**.
9. Click **Update**.

# 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 Web Application Firewall for baseline protection of the Microsoft Exchange application, specifically for the 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 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**.

## RPC over HTTP

By design, RPC over HTTP is not compatible with Brocade vWAF. However, we can prevent RPC traffic from going to the vWAF by using TrafficScript and checking for the URL path.

The following example TrafficScript checks for "rpc" in the URL path, whitelists the traffic, and bypasses the vWAF for such traffic.

```
if ( string.startswith($path, "/rpc/") ) {
   connection.data.set("enforcer.whitelist", 1);
}
```

Select the virtual server of interest, and add this TrafficScript rule to the Request rules. Make sure to place this TrafficScript rule ahead of the Enforcer rule such that it is executed before the Enforcer TrafficScript.

# Common Troubleshooting Tips

This chapter describes tips for troubleshooting common deployment issues.

## Uploading Certificates to Traffic Manager

When uploading certificates to 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 Exchange 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 meet a range of service hosting problems.

# Appendix

## TrafficScript Code to Configure Brocade Virtual Traffic Manager for a Single Virtual Server with Multiple Pools

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

```
#// TS Rule for Exchange 2013 for a Single VS with Multiple Pools
# Please declare the names of the pools you have configured, and ensure
# that the trafficscript!variable_pool_use Global setting is set to 'yes'

$owa_pool = "Exchange 2013 OWA";
$autodiscover_pool = "Exchange 2013 Autodiscover";
$ecp_pool = "Exchange 2013 ECP";
$ews_pool = "Exchange 2013 EWS";
$eas_pool = "Exchange 2013 EAS";
$oab_pool = "Exchange 2013 OAB";
$ps_pool = "Exchange 2013 PowerShell";
$oa_pool = "Exchange 2013 OA";
$debug = 0; // Change value to 1 if debug needed

$path = http.getPath();
$pool = "";

# Exchange Autodiscover Pool
if( string.startsWithI( $path, "/autodiscover" ) ) {
    $pool = $autodiscover_pool;
    if ($debug > 0) { log.info("Auto Discover Pool Selected");}
}
# Exchange Control Panel Pool
else if( string.startsWithI( $path, "/ecp" ) ) {
    $pool = $ecp_pool;
    if ($debug > 0) { log.info(" Exchange Control Panel Pool Selected");}
}
# Exchange Web Services Pool
else if( string.startsWithI( $path, "/ews" ) ) {
    $pool = $ews_pool;
    if ($debug > 0) { log.info("Exchange Web Services Pool Selected");}
}
# Exchange Active Sync Pool
else if( $path == "/Microsoft-Server-ActiveSync" ) {
    $pool = $eas_pool;
    if ($debug > 0) { log.info("Exchange Active Sync Pool Selected");}
}
# Exchange Offline Address Book Pool
else if( string.startsWithI( $path, "/oab" ) ) {
    $pool = $oab_pool;
    if ($debug > 0) { log.info("Offline Address Book Pool Selected");}
}
# Exchange PowerShell Pool
else if( string.startsWithI( $path, "/PowerShell" ) ) {
    $pool = $ps_pool;
    if ($debug > 0) { log.info("PowerShell Pool Selected");}
}
# Exchange Outlook Anywhere Pool
else if( $path == "/rpc/rpcproxy.dll" ) {
    $pool = $oa_pool;
    if ($debug > 0) { log.info("Outlook Anywhere Pool Selected");}
```

```
}
# Exchange Outlook Web Access Pool
else {
    $pool = $owa_pool;
    if ($debug > 0) { log.info("Outlook Web Access Pool Selected");}
}
pool.select ( $pool );
```

# TrafficScript Code to Redirect All HTTP Requests to HTTPS

The following TrafficScript code is used to redirect OWA HTTP requests to HTTPS.

```
#// TS Rule for redirecting HTTP requests to HTTPS
# Exchange 2013 OWA Redirect SSL
# Redirect to OWA URL if user tried default website
$debug = 0; // Change value to 1 if debug needed

$hostheader = http.getHostHeader();
if (http.getPath() == "/")
{
    http.redirect("https://".$hostheader."/owa");
         if ($debug > 0) { log.info("Redirected to OWA URL");}
}
```