Kemp Web Application Firewall

Feature Description

UPDATED: 07 January 2020

Copyright Notices

Copyright © 2002-2020 Kemp Technologies, Inc. All rights reserved. Kemp Technologies and the Kemp Technologies logo are registered trademarks of Kemp Technologies, Inc.

Kemp Technologies, Inc. reserves all ownership rights for the LoadMaster and Kemp 360 product line including software and documentation.

Used, under license, U.S. Patent Nos. 6,473,802, 6,374,300, 8,392,563, 8,103,770, 7,831,712, 7,606,912, 7,346,695, 7,287,084 and 6,970,933

 Copyright 2002-2020, Kemp Technologies, All Rights Reserved

Table of Contents

1 Introduction 5
1.1 Document Purpose 5
1.2 Intended Audience 6
2 Configuring WAF 7
2.1 Resource Considerations 7
2.2 Balancing WAF Resource Utilization with High Load Applications 7
2.3 WAF Rule Management 8
2.3.1 Commercial Rules 8
2.3.1.1 Automatic Downloading and Updating of Commercial Rules 8
2.3.1.2 Manual Downloading and Updating of Commercial Rules 10
2.3.2 Custom Rules 11
2.3.2.1 Delete/Download a Custom Rule or Data File 12
2.4 Configure WAF Options for a Virtual Service 12
2.5 Backing Up and Restoring a WAF Configuration 15
2.6 WAF WUI Options 16
2.6.1 WAF Settings in the Main Menu of the LoadMaster WUI 16
2.6.2 WAF Options in the Virtual Service Modify Screen 18
2.6.3 WAF Event Log 22
2.6.4 WAF Options in the Extended Log Files Screen 23
2.6.5 Enable WAF Debug Logging 24
2.6.6 WAF Statistics 25

 Copyright 2002-2020, Kemp Technologies, All Rights Reserved

2.6.6.1 Home Page 25

2.6.6.2 Statistics Page 26

2.6.7 WAF Misconfigured Virtual Service Status 27

3 Troubleshooting 29

3.1 WAF Logging 29

3.2 WAF Compatibility with Kerberos Constrained Delegation (KCD) 29

3.3 Unable to Download/Update Rules 29

References 30

Last Updated Date 31

 Copyright 2002-2020, Kemp Technologies, All Rights Reserved

1 Introduction

The Kemp Web Application Firewall (WAF) enables secure deployment of web applications, preventing Layer 7 attacks while maintaining core load balancing services, which ensures comprehensive application delivery and security. WAF functionality directly augments the LoadMaster's existing security features to create a layered defence for web applications - enabling a safe, compliant and productive use of published services.

> WAF is only available on certain subscriptions. Please contact a Kemp representative if needed.

When WAF is enabled, the WAF engine scans every incoming HTTP packet – running through each assigned rule individually and deciding what action to take if a rule is matched. The rules can be run on requests and responses.

WAF can protect against attacks, such as:

- Injection
- Cross-Site Scripting (XSS)
- Unvalidated redirects and forwards
- Missing function-level access control
- Sensisitve data exposure
- Security misconfiguration
- Broken authentication and session management

For a more detailed overview of the WAF feature, refer to the WAF section in the **Kemp LoadMaster, Product Overview**.

1.1 Document Purpose

The purpose of this document is to describe the WAF features and provide step-by-step instructions on how to configure the WAF settings in the Kemp LoadMaster.

For further information and assistance, refer to our Kemp Support site for Support contact details: http://kemptechnologies.com/load-balancing-support/kemp-support/.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

1.2 Intended Audience

This document is intended to be read by anyone who is interested in finding out more about the Kemp WAF functionality.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

2 Configuring WAF

2.1 Resource Considerations

> Utilizing WAF can have a significant performance impact on the LoadMaster deployment. Please ensure that the appropriate resources are allocated.

For virtual and bare metal LoadMaster instances, a minimum of 2GB of allocated RAM is required for operation of WAF. The default memory allocation for Virtual LoadMasters and LoadMaster Bare Metal instances before LoadMaster Operating System version 7.1-22 is 1 GB of RAM. If this default allocation has not been changed, modify the memory settings before attempting to proceed with WAF configuration. If the check box to enable WAF is greyed out, it could mean that the LoadMaster does not have enough memory to run WAF.

2.2 Balancing WAF Resource Utilization with High Load Applications

The WAF subsystem uses a significant amount of system resources. When enabling WAF, you should avoid overconsuming system resources that are needed for load balancing Virtual Services. When WAF starts to consume resources at a level that impacts overall system performance, one or more of these symptoms can be observed:

- High CPU utilization
- High memory utilization
- InterProcess Communication (IPC) issues between Layer 7 and WAF processes
- Decreased Virtual Service throughput
- Increased Virtual Service latency

There are essentially two ways of dealing with these issues:

- Disable WAF completely on one or more Virtual Services.
- Tailor the applied rulesets used on each Virtual Service to reduce the rules applied to the minimum necessary for secure operation.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

Best practice for WAF rulesets is to avoid a blanket application of a ruleset, and instead enable only those rules in the ruleset that are specifically required for your application.

Note that internal processing and communication between WAF and Layer 7 in version 7.2.36 is enhanced to help mitigate resource exhausting issues through smarter thread and resource management. Best practice is still to enable a minimum set of rules instead of enabling the entire ruleset.

2.3 WAF Rule Management

If you have a WAF license and WAF Support, Kemp provides a number of commercial rules, such as **ip_reputation**, which can be set to automatically download and update daily. These commercial rules are targeted to protect against specific threats to which packaged and custom applications are vulnerable. The Kemp-provided commercial rules are available when signed up to a WAF subscription.

These commercial rules are automatically downloaded and installed if WAF is licensed and enabled and rules have not been installed yet. If the automatic download or installation fails, an appropriate error log is generated.

You can also upload other rules, such as the **ModSecurity** core rule set which contains generic attack detection rules that provide a base level of protection for any web application.

You can also write and upload your own custom rules, if required.

With the WAF-enabled LoadMaster, you can choose whether to use Kemp-provided rules (which can be set to automatically download), custom rules that can be uploaded or a combination of both. The sections below provide details regarding commercial rules and custom rules.

2.3.1 Commercial Rules

The Kemp-provided commercial rules can be set to automatically download and install. They can also be manually downloaded and installed. The sections below explain how to use each method.

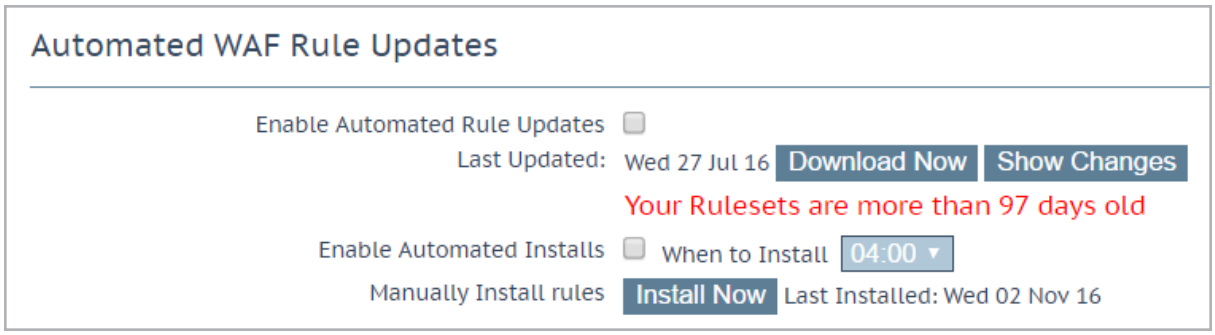
> Kemp-provided commercial rules are only available when you sign up for a WAF subscription.

2.3.1.1 Automatic Downloading and Updating of Commercial Rules

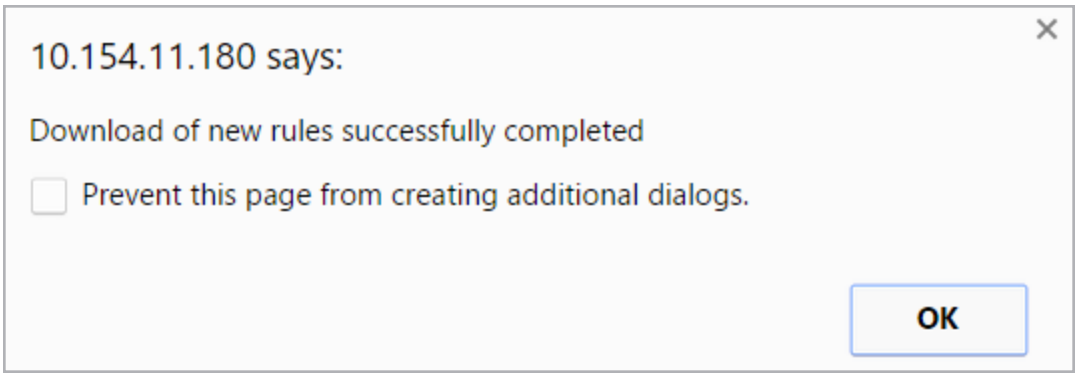
Before enabling automatic installation of WAF rules, you must first download and install the latest rules. Follow the steps below to configure automatic download and installation settings for WAF commercial rules:

1. In the main menu, select **Virtual Services > WAF Settings**.

 Copyright 2002-2020, Kemp Technologies, All Rights Reserved

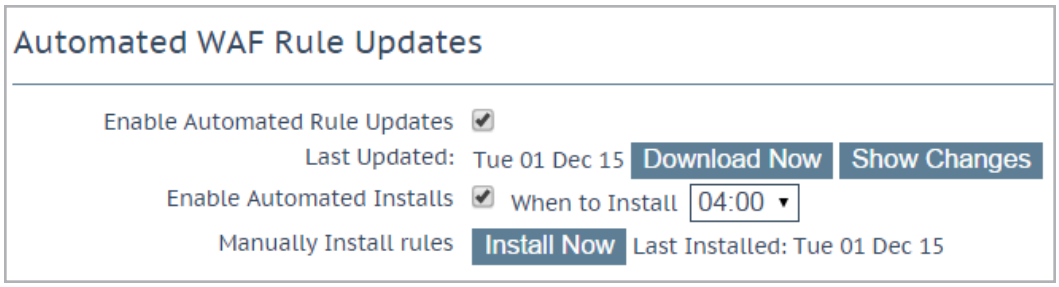


2. Click the **Download Now** button to download the latest WAF rules.



3. Click **OK** on the success message.

4. Click **Install Now** to install the latest rules.



5. To enable the automatic download of updates to WAF commercial rule files, select the **Enable Automated Rule Updates** check box.

> The automatic and manual download options are greyed out if WAF support has expired. If this is the case, contact Kemp to renew your subscription.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

6. To enable automatic installation of the updated WAF commercial rule files, select the **Enable Automated Installs** check box.

> By default, the **Enable Automated Installs** and **Manually Install rules** options are greyed out. The rules must be downloaded for the first time before these options become available.

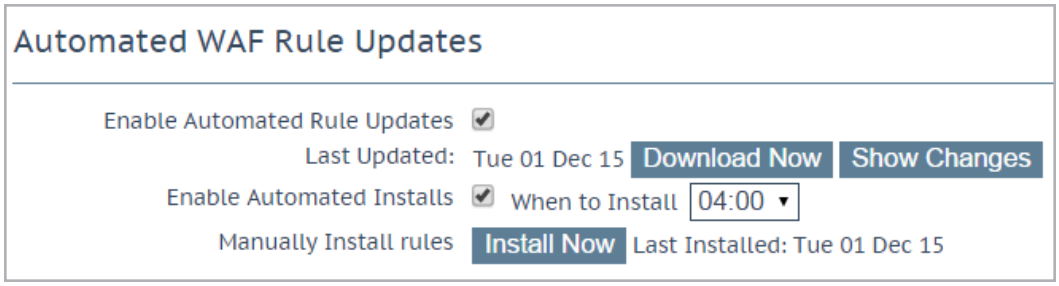
7. Select the time (hour of the day) at which to automatically install the commercial rule updates.

> The WAF rules must be assigned to a Virtual Service to take effect. For instructions on how to assign WAF rules to a Virtual Service, refer to the **Configure WAF Options for a Virtual Service** section.

2.3.1.2 Manual Downloading and Updating of Commercial Rules

To manually download and install the commercial rule file updates, follow the steps below:

1. In the main menu, select **Virtual Services > WAF Settings**.



2. Click **Download Now** to download the WAF rules now.

> A warning message appears if the rules have not been updated in the last 7 days or if they have not been downloaded at all.

3. After the rules are downloaded, the **Show Changes** button appears. Click this button to retrieve a log of changes that have been made to the Kemp WAF rule set.

4. Click **Install Now** to manually install the commercial rule updates.

> The WAF rules must be assigned to a Virtual Service in order to take effect. For instructions on how to assign WAF rules to a

 Copyright 2002-2020, Kemp Technologies, All Rights Reserved

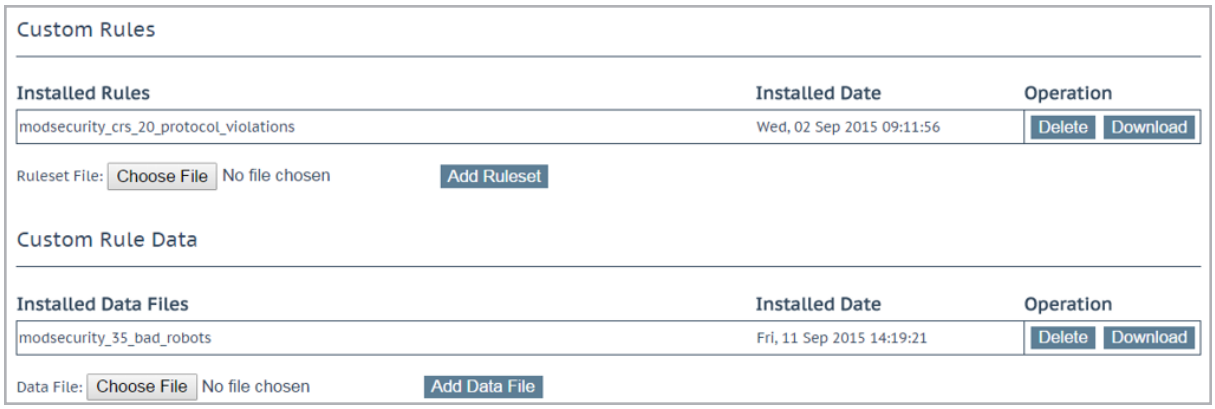
Virtual Service, refer to the **Configure WAF Options for a Virtual Service** section.

2.3.2 Custom Rules

Third party rules, such as the ModSecurity core rule set can be uploaded to the LoadMaster. You can also write your own custom rules which can be uploaded. The **WAF Rule Management** screen enables you to upload **Custom Rules** (.conf) and associated **Custom Rule Data** (.data or .txt) files. You can also upload gzip-compressed Tarball files (.tar.gz), which contain multiple rule and data files.

To upload rule and data files, follow the steps below:

1. In the main menu, select **Virtual Services > WAF Settings**.



2. To upload custom rules; in the **Installed Rules** section, click **Choose File**.

Individual rules can be uploaded as .conf files. Alternatively, you can load a package of rules in a .tar.gz file, for example, the ModSecurity core rule set.

3. Browse to and select the rule file(s) to be uploaded.
4. Click **Add Ruleset**.
5. To upload any additional data files; in the **Custom Rule Data** section, click **Choose File**.

The additional files are for the rules' associated data files. If you uploaded a Tarball in the **Browse to and select the rule file**

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

> **(s) to be uploaded.** step, the rules and data files can be packaged together.

6. Browse to and select the additional data files to be uploaded.
7. Click **Add Data File**.

The rules are now available to assign within the Virtual Services modify screen. Refer to the next section to find out how to configure the Virtual Service to use the installed rules (commercial or custom).

2.3.2.1 Delete/Download a Custom Rule or Data File

Custom rules and data files can be deleted or downloaded by clicking the relevant buttons.

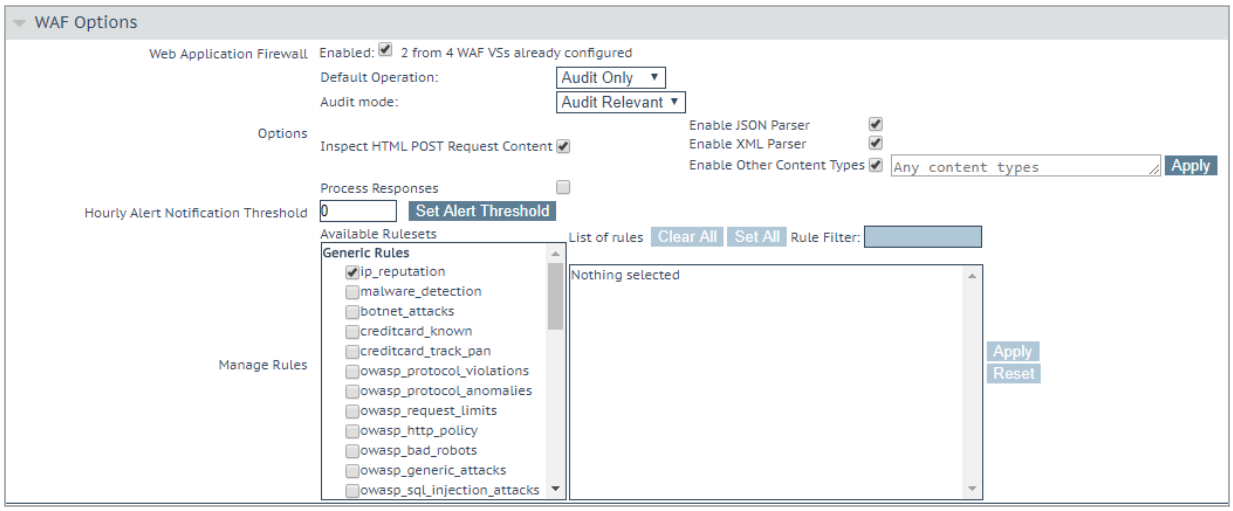
> If a rule is assigned to a Virtual Service, it will not be available for deletion.

2.4 Configure WAF Options for a Virtual Service

WAF settings can be configured for each individual Virtual Service. Follow the steps below to configure the WAF options in a Virtual Service. For more information on each of the fields, refer to the **WAF WUI Options** section.

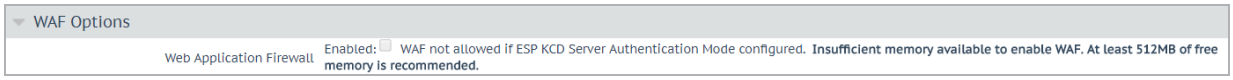
1. In the main menu of the LoadMaster WUI, select **Virtual Services > View/Modify Services**.
2. Click **Modify** on the relevant Virtual Service.
3. Expand the **WAF Options** section.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved



4. By default, WAF is disabled. To enable WAF, select **Enabled**.

> The maximum number of WAF-enabled Virtual Services is the total (unused or available) RAM (in MB)/512 MB. For example: 8 GB/512 MB = 16 WAF-enabled Virtual Services. When the maximum is reached, no additional Virtual Services can be enabled with WAF.



> A message displays if there is insufficient memory available to enable WAF.

> A message is displayed next to the **Enabled** check box displaying how many WAF-enabled Virtual Services exist and the maximum number of WAF-enabled Virtual Services that can exist. If the maximum number of WAF-enabled Virtual Services is reached, the **Enabled** check box is greyed out.

5. Specify the **Default Operation** type.

> The **Default Operation** is what occurs if no action is specified in the relevant rule.

 Copyright 2002-2020, Kemp Technologies, All Rights Reserved

Audit Only: This is an audit-only mode – logs are created but requests and responses are not blocked.

Block Mode: Either requests or responses are blocked based on the assigned rules.

6. Specify the **Audit mode**.

There are three audit modes:
- **No Audit:** No data is logged.
- **Audit Relevant:** Logs data that is of a warning level and higher. This is the default option for this setting.
- **Audit All:** Logs all data through the Virtual Service.

Selecting the **Audit All** option produces a large amount of log data. Kemp does not recommend selecting the **Audit All** option for normal operation. However, the **Audit All** option can be useful when troubleshooting a specific problem.

7. Specify whether or not to **Inspect HTML POST Request Content**.

The **Inspect HTML POST Request Content** option is disabled by default. If you enable this option, three more check boxes become available that allow you to enablethe processing of JavaScript Object Notation (JSON), XML requests, and other content types.

8. Specify whether or not to **Process Responses**.

The processing of response data can be CPU and memory intensive.

9. Specify the **Hourly Alert Notification Threshold** and click **Set Alert Threshold**.

This is the number of incidents per hour before sending an alert. Setting this to **0** disables alerting.

10. Assign rulesets by selecting them in the **Available Rulesets** section.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

11. Individual rules can be enabled/disabled per ruleset by selecting/clearing them in the box on the right.

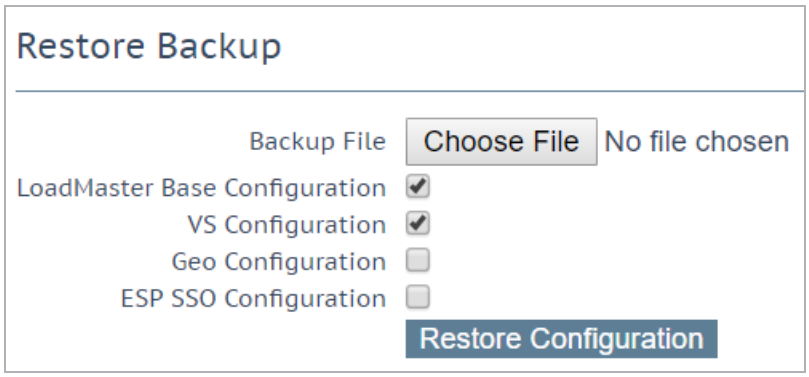
> If any OWASP rule sets are enabled, owasp_setup is enabled automatically because it contains settings common to all OWASP rule sets.

Rules can be filtered by entering a filter term in the **Rule Filter** text box.
Clicking **Clear All** disables all rules for the selected ruleset.
Clicking **Set All** enables all rules for the selected ruleset.
Clicking the **Reset** button disables any rule sets and rules selected since the last time you clicked **Apply**.

12. When finished enabling/disabling the relevant rulesets and rules, click **Apply**.

> Application-specific and application-generic rules cannot both be assigned to the same Virtual Service. If you try to do this, an error message (**Cannot assign Application Specific and Application Generic rules simultaneously**) appears to inform you that this is not possible.

2.5 Backing Up and Restoring a WAF Configuration



A backup of the LoadMaster configuration can be taken by going to **System Configuration > System Administration > Backup/Restore** and clicking **Create Backup File**.

The configuration can be restored from this screen also. Note that the Virtual Service settings can be restored by selecting **VS Configuration** and the rules can be restored by selecting **LoadMaster Base Configuration**.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

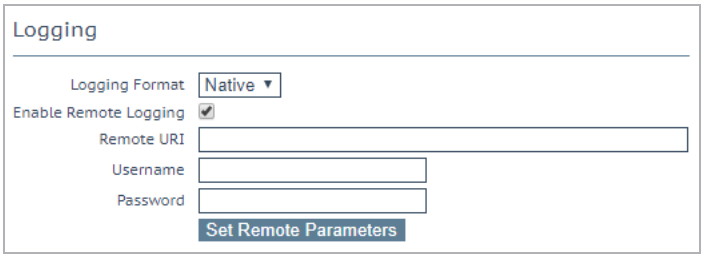
A WAF configuration can only be restored onto a LoadMaster with a WAF license.

2.6 WAF WUI Options

This section describes the different WAF fields available in the LoadMaster WUI. There are WAF WUI options in the **WAF Settings** section of the main menu and in the Virtual Service modify screen. Refer to the sections below for field descriptions.

2.6.1 WAF Settings in the Main Menu of the LoadMaster WUI

You can get to this screen by selecting **Virtual Services > WAF Settings** in the main menu of the LoadMaster WUI.



Logging Format

Select either Native or JSON depending on what format you want the audit logs to appear in.

Enable Remote Logging

This check box enables you to enable or disable remote logging for WAF.

Remote URI

Specify the Uniform Resource Identifier (URI) for the remote logging server.

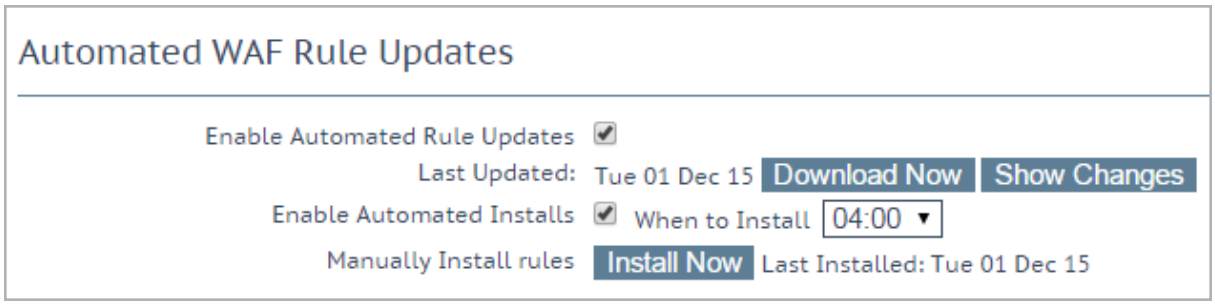
Username

Specify the username for the remote logging server.

Password

Specify the password for the remote logging server.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved



> The automatic and manual download options are greyed out if the WAF subscription has expired.

Enable Automated Rule Updates

Select this check box to enable the automatic download of the latest WAF rule files. This is done daily, if enabled.

Last Updated

This section displays the date when the last rules were downloaded. It gives you the option to attempt to download the rules now. It also displays a warning if rules have not been downloaded in the last 7 days. The **Show Changes** button is displayed if the rules have been downloaded. This button can be clicked to retrieve a log of changes that have been made to the Kemp WAF rule set.

Enable Automated Installs

Select this check box to enable the automatic daily install of updated rules at the specified time.

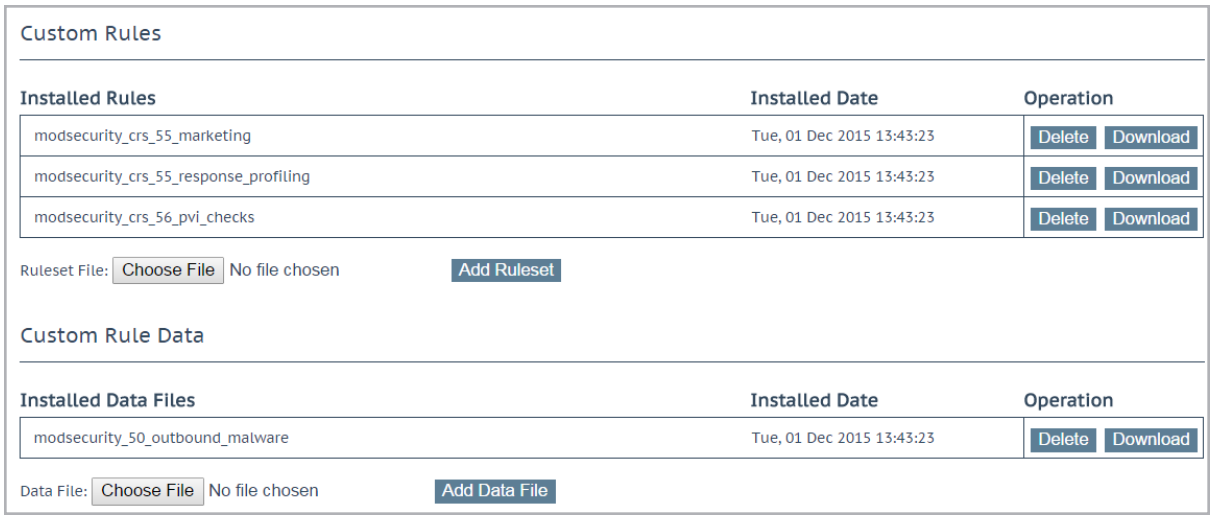
When to Install

Select the hour at which to install the updates every day.

Manually Install rules

This button enables you to manually install rule updates, rather than automatically installing them. This section also displays when the rules were last installed.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved



Custom Rules

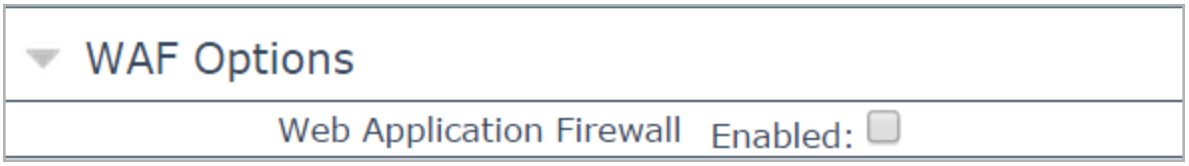
This section enables you to upload custom rules and associated data files. Individual rules can be loaded as .conf files or you can load a package of rules in a gzip-compressed Tarball (.tar.gz) file.

Custom Rule Data

This section enables you to upload data files that are associated to the custom rules.

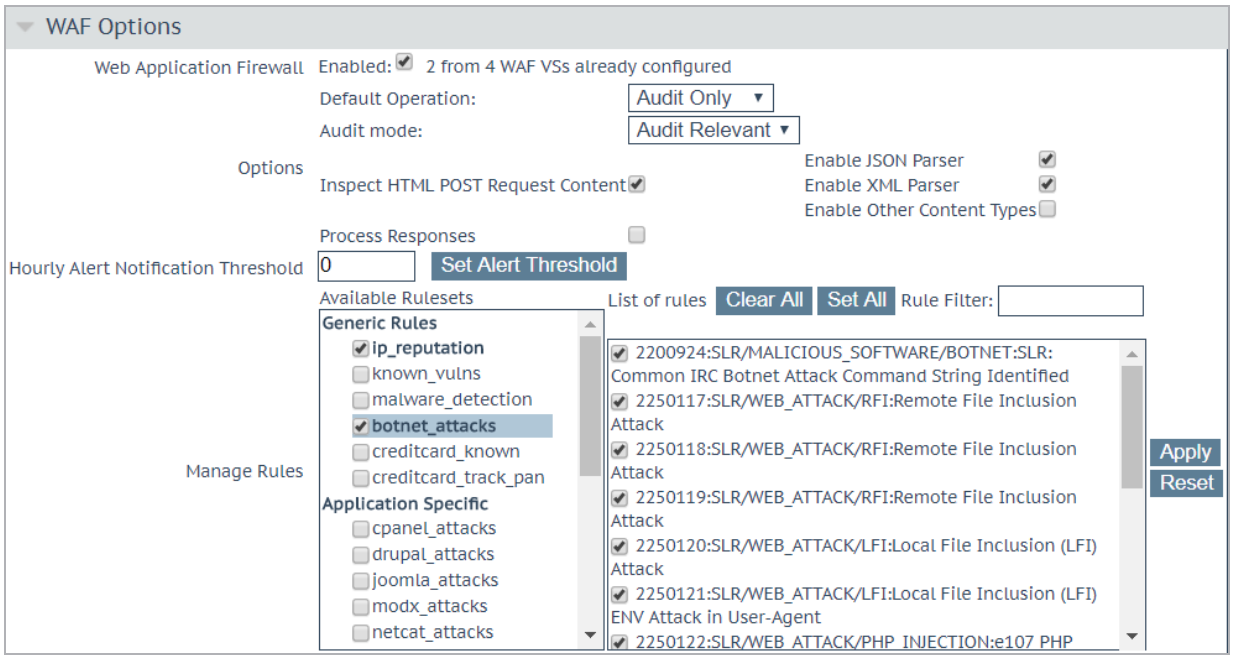
2.6.2 WAF Options in the Virtual Service Modify Screen

You can get to the Virtual Service WAF Options by selecting **Virtual Services > View/Modify Services** in the main menu, clicking **Modify** on the relevant Virtual Service and expanding the **WAF Options** section.



By default, WAF is disabled. To enable WAF, select the **Enabled** check box.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved



The WAF feature must be enabled before you can configure these options. Select the **Enabled** check box to enable WAF on this Virtual Service.

Default Operation

Specify the Default Operation type:

- **Audit Only:** This is an audit-only mode – logs are created but requests and responses are not blocked. It is recommended when first using WAF to enable **Audit Only** mode for a period of time. During this time you should analyze the logs and adjust the rules and settings as needed before enabling **Block Mode** . This ensures that no legitimate traffic is blocked.
- **Block Mode:** Either requests or responses are blocked based on the assigned rules.

Audit mode

Audit logs are produced according to the specifications on the following website: https://github.com/SpiderLabs/ModSecurity/wiki/ModSecurity-2-Data-Formats

Select what logs to record:

- **No Audit:** No data is logged.
- **Audit Relevant:** Logs data which is of a warning level and higher. This is the default option for this setting.
- **Audit All:** Logs all data through the Virtual Service.

 Copyright 2002-2020, Kemp Technologies, All Rights Reserved

> Selecting the **Audit All** option produces a large amount of log data. Kemp does not recommend selecting the **Audit All** option for normal operation. However, the **Audit All** option can be useful when troubleshooting a specific problem.

Inspect HTML POST Request Content

Enable this option to also process the data supplied in POST requests.

> The **Inspect HTML POST Request Content** option is disabled by default. Three additional options (**Disable JSON Parser, Disable XML Parser**, and **Enable Other Content Types**) only become available if **Inspect HTML POST Request Content** is enabled.

Enable JSON Parser

Enable verification of JavaScript Object Notation (JSON) POST requests.

Enable XML Parser

Enable verification of Extensible Markup Language (XML) POST requests.

Enable Other Content Types

Enable verification of POST content types (other than XML/JSON).

> Enabling the inspection of any other content types may increase system resource utilization (CPU and memory). A specific list of content types should be considered.

When the **Enable Other Content Types** option is enabled, a text box is provided to enter a comma-separated list of POST content types allowed for WAF analysis. By default, all types (other than XML/JSON) are enabled.

> WAF does not block attack requests if the POST request does not contain the 'content-type' header, even if **Inspect HTML POST Request Content**, **Enable JSON Parser**, **Enable XML Parser**, and Enable **Other Content Types** check boxes are all enabled. This is a WAF rule issue and can be solved by having a

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

> rule to check if there is no 'content-type' present in the request header and forcing the URL-encoded parser in the WAF rules.

Process Responses

Enable this option to verify response data sent from the Real Servers.

> This can be CPU and memory intensive so only enable this if necessary.

> If a Real Server is gzip encoding, WAF will not check that traffic, even if **Process Responses** is enabled.

Hourly Alert Notification Threshold

This is the threshold of incidents per hour before sending an alert email. Setting this to **0** disables alerting.

Rules

This is where you can assign/un-assign generic, application-specific, application-generic and custom rules to/from the Virtual Service.

> You cannot assign application-specific and application-generic rules to the same Virtual Service.

Individual rules within each ruleset can be enabled/disabled as required. To enable a ruleset, select the relevant check box. If you have not enabled/disabled rules in that ruleset previously, all rules are enabled by default in the right box. If you have previously enabled/disabled rules in that ruleset, within that Virtual Service – the rules retain their previous settings.

You can enable/disable individual rules as needed by selecting the relevant ruleset on the left and selecting/clearing the rules on the right.

> Some rules or rule sets may have dependencies on other rules. There is no dependency check in the LoadMaster when rules are disabled - before disabling any rule, be aware of any rule chains or dependencies.

When finished making changes, click **Apply**.

Clicking the **Clear All** button disables all rules for the selected ruleset.

Clicking the **Set All** button enables all rules for the selected ruleset.

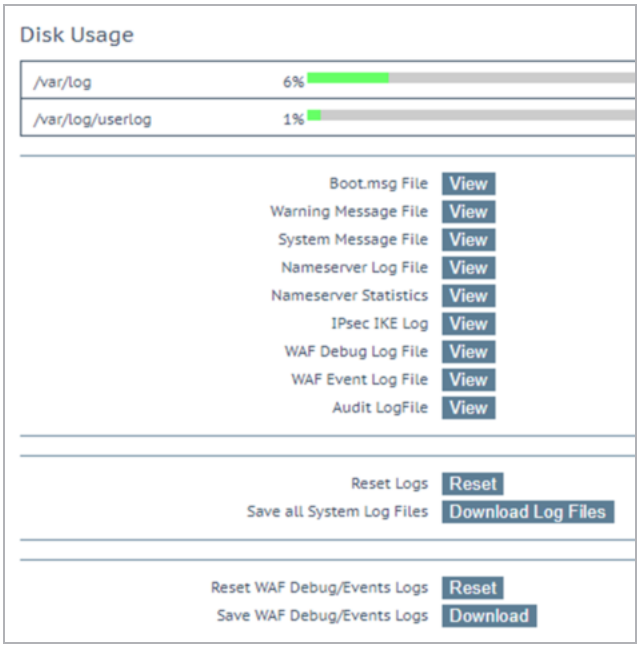
 Copyright 2002-2020, Kemp Technologies, All Rights Reserved

Text can be entered in the **Rule Filter** text box to filter the rules to only show rules that contain the filter text.

Clicking **Reset** disables all rulesets and rules.

> Only assign the rules that are required. All assigned rules will be checked against, so a large number of assigned rules can lead to high CPU usage.

2.6.3 WAF Event Log

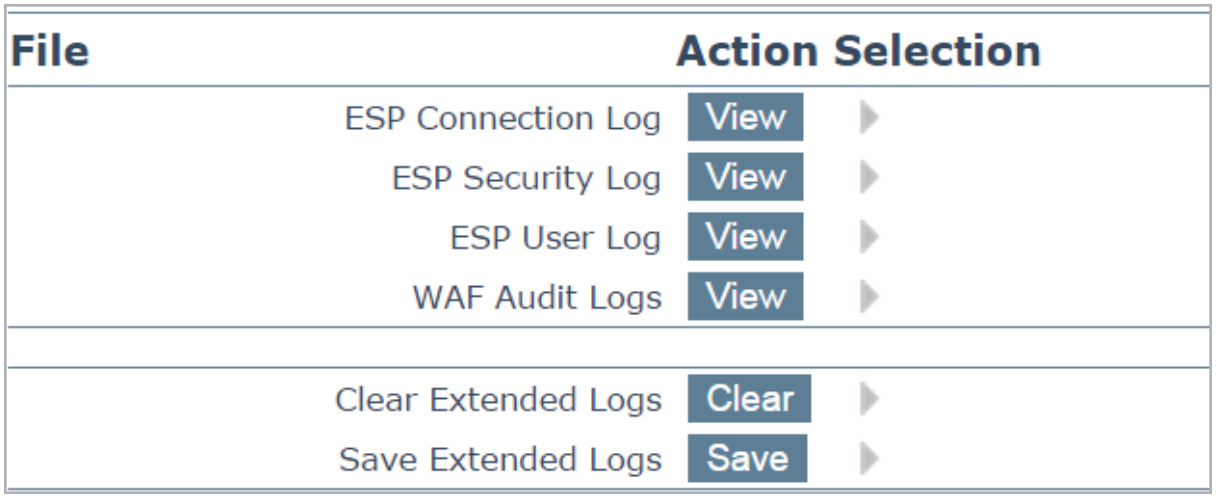


You can view the WAF Event Log by going to **System Configuration > Logging Options > System Log Files** and clicking the relevant **View** button. This log file contains all WAF alerts and automatically update to show new events.

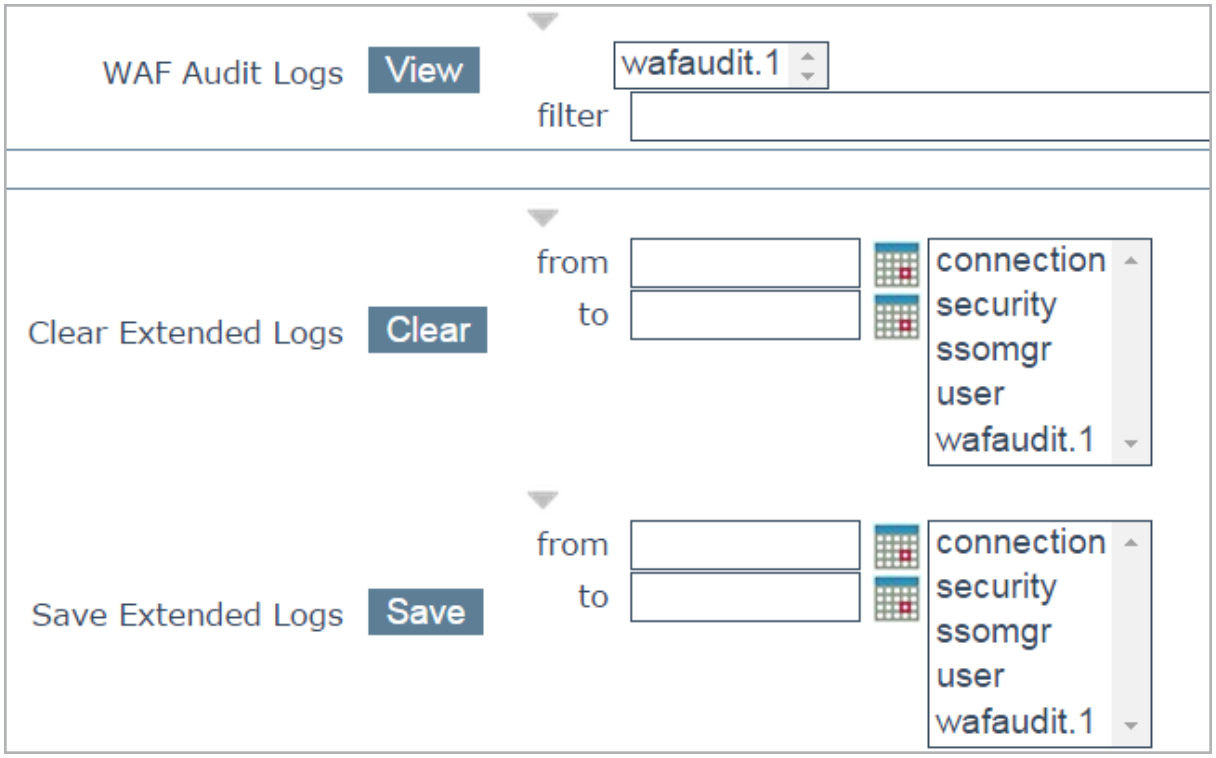
You can also reset and/or download the WAF debug/event logs by clicking the relevant buttons.

 Copyright 2002-2020, Kemp Technologies, All Rights Reserved

2.6.4 WAF Options in the Extended Log Files Screen



The **Extended Log Files** screen provides options for logs relating to the ESP and WAF features. These logs are persistent and will be available after a LoadMaster reboot. To view all of the options click the icons.



Copyright 2002-2020, Kemp Technologies, All Rights Reserved

> In addition to WAF logs, ESP logs are also available on this screen. For more information, refer to the **Edge Security Pack (ESP), Feature Description**.

WAF Audit Logs: recording WAF logs based on what has been selected for the **Audit mode** drop-down list (either **Audit Relevant** or **Audit All**) in the **WAF Options** section of the Virtual Service modify screen.

To view the logs, select the appropriate log file and click the relevant **View** button.

The number listed in each log entry corresponds to the ID of the Virtual Service. To get the Virtual Service ID, first ensure that the API interface is enabled (**Certificates & Security > Remote Access > Enable API Interface**). Then, in a web browser address bar, enter **https://<LoadMasterIPAddress>/access/listvs**. Check the **index** of the Virtual Service. This is the number that corresponds to the number on the audit log entry.

One or more archived log files can be viewed by selecting the relevant file(s) from the list of file names and clicking the **View** button. You can filter the log files by entering a word(s) or regular expression in the **filter** field and clicking the **View** field.

Clear Extended Logs

All extended logs can be deleted by clicking the **Clear** button.

Specific log files can be deleted by filtering on a specific date range, selecting one or more individual log files in the log file list or selecting a specific log type (for example connection, security or user) in the log file list and clicking the **Clear** button. Click **OK** on any warning messages.

Save Extended Logs

All extended logs can be saved to a file by clicking the **Save** button.

Specific log files can be saved by filtering on a specific date range, selecting one or more individual log files in the log file list or selecting a specific log type (for example connection, security or user) in the log file list and clicking the **Save** button.

2.6.5 Enable WAF Debug Logging

WAF debug traces can be enabled by clicking the **Enable Logging** button at **System Configuration > Logging Options > System Log Files**.

> This generates a lot of log traffic. It also slows down WAF processing. Only enable this option when requested to do so

 Copyright 2002-2020, Kemp Technologies, All Rights Reserved

by Kemp Technical Support. Kemp does not recommend enabling this option in a production environment.

The WAF debug logs are never closed and they are rotated if they get too large. AFP (in general) needs to be disabled and re-enabled (by clearing and re-selecting the **Enabled** check box) in all WAF-enabled Virtual Service settings to re-enable the debug logs. Alternatively, perform a rule update (in the **WAF Settings** screen), with rules that are relevant for the Virtual Service(s).

2.6.6 WAF Statistics

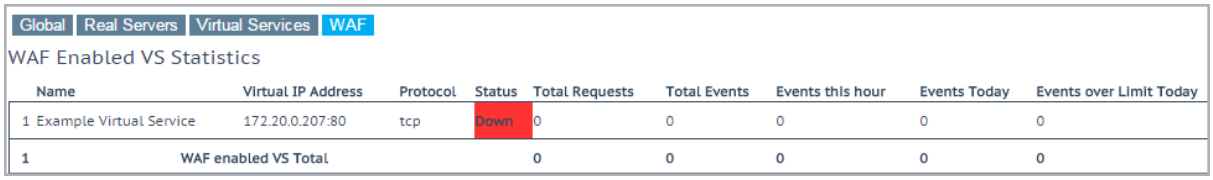
2.6.6.1 Home Page

The **WAF Status** section isdisplayed on the WUI home page if at least one Virtual Service has WAF enabled. The values shown here are as follows:

- The total number of requests handled by the WAF (shows all requests, whether they were blocked or not). Two requests are recorded for each connection – one incoming and one outgoing request.
- The total number of events handled by the WAF (therefore requests that were blocked).
- The number of events that have happened in the current hour (since xx.00.00).
- The number of events that have happened since 00.00 am (local time).
- The number of times the event counter has gone over the configured warning threshold today. For example, if the threshold is set to 10 and there has been 20 events, this counter will be set to 2. The warning threshold is set on a per-Virtual Service basis by filling out the **Hourly Alert Notification Threshold** field in **WAF Options** in the Virtual Service modify screen. For further information, refer to the **WAF Settings in the Main Menu of the LoadMaster WUI** section.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

2.6.6.2 Statistics Page



To get to the WAF statistics page in the LoadMaster WUI, go to **Statistics > Real Time Statistics > WAF**. These statistics refresh every 5 to 6 seconds. The following items are displayed on this screen:

Count: The left-most column displays the total number of WAF-enabled Virtual Services.

Name: The name of the WAF-enabled Virtual Service.

Virtual IP Address: The IP address and port of the Virtual Service.

Protocol: The protocol of the Virtual Service (tcp or udp).

Status: The status of the Virtual Service. For information on each of the possible statuses, refer to the **Web User Interface (WUI), Configuration Guide** .

Total Requests: The total number of requests handled by the WAF (shows all requests, whether they were blocked or not). Two requests are recorded for each connection – one incoming and one outgoing request.

Total Events: The total number of events handled by the WAF (therefore, requests that were blocked).

Events this hour: The number of events that have happened in the current hour (since xx.00.00).

Events Today: The number of events that have happened since 00.00 am (local time).

Events over Limit Today: The number of times the event counter has gone over the configured warning threshold today. For example, if the threshold is set to 10 and there has been 20 events, this counter will be set to 2. The warning threshold is set on a per-Virtual Service basis by filling out the **Hourly Alert Notification Threshold** field in **WAF Options** in the Virtual Service modify screen. For further information, refer to the **WAF Settings in the Main Menu of the LoadMaster WUI** section.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

VIP 172.20.0.102	
Address	172.20.0.102
Port	80
Protocol	tcp
Active Conns	0
Total Conns	0
Total Bytes	0
Real Servers	0
Persist Entries	0
WAF	Enabled
Requests	0
Incidents	0
Incidents/Hour	0
Incidents/Day	0
Incidents/Dayover	0

These WAF statistics can also be seen in the Virtual Service statistics screen (go to **Statistics > Real Time Statistics > Virtual Services** and then click the **Virtual IP Address** link).

2.6.7 WAF Misconfigured Virtual Service Status

Status
● WAF Misconfigured

On the **View/Modify Services** screen in the LoadMaster WUI, the **Status** of each Virtual Service is displayed. If the WAF for a particular Virtual Service is misconfigured (for example, if there is an issue with a rule file), the status changes to **WAF Misconfigured** and turns to red.

If the Virtual Service is in a **WAF Misconfigured** state, all traffic stops flowing. WAF can be disabled for that Virtual Service to

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

stop the traffic being blocked, if required, while troubleshooting the problem.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

3 Troubleshooting

Refer to the sections below for some information relating to WAF troubleshooting.

3.1 WAF Logging

All events are logged but there may be a delay in them being available for Administrator viewing. For further information on the WAF logging options, refer to the **WAF Event Log** and **Enable WAF Debug Logging** sections.

3.2 WAF Compatibility with Kerberos Constrained Delegation (KCD)

As of the 7.2.40 LoadMaster firmware version, you cannot enable both WAF and KCD at the same Virtual Service level. For example:

- If WAF is enabled in the parent Virtual Service, you cannot enable KCD as the **Server Authentication Mode** in the parent Virtual Service

- If KCD is enabled in the parent Virtual Service, you cannot enable WAF

However, you can enable ESP/KCD in the SubVS and then enable WAF in the parent Virtual Service.

If you had WAF and KCD enabled at the same level before upgrading to 7.2.40 and you upgrade the firmware to 7.2.40 or above, the configuration will not be changed. File attachments in SharePoint will not work. To resolve this, enable WAF on the parent Virtual Service and ESP/KCD on the SubVS.

The following combination is not supported: WAF with ESP Client Certificate authentication and KCD.

3.3 Unable to Download/Update Rules

Kemp recommends adding the Kemp Licensing Server URL (**alsi.kemptechnologies.com** and **alsi2.kemptechnologies.com**) as allowed URLs on your firewall to ensure all licensing features work, including the downloading and updating of WAF rules.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

References

Unless otherwise specified, the following documents can be found at http://kemptechnologies.com/documentation

Edge Security Pack (ESP), Feature Description

Kemp LoadMaster, Product Overview

Web User Interface (WUI), Configuration Guide

Copyright 2002-2020, Kemp Technologies, All Rights Reserved

Last Updated Date

This document was last updated on 07 January 2020.

Copyright 2002-2020, Kemp Technologies, All Rights Reserved