ESP Steering Groups

Technical Note

UPDATED: 08 December 2020

Copyright Notices

Table of Contents

1 Introduction

The Kemp LoadMaster Edge Security Pack (ESP) has the ability of steering client traffic to individual Real Servers in a Virtual Service based on the Active Directory (AD) group membership of users initiating client traffic. An example scenario would be a Virtual Service which has four Real Servers. Two Real Servers could be configured to have a primary association with Active Directory Group 1 and two Real Servers could be configured to have a primary association with AD Group 2. When a user attempts to access the Virtual Service, their group membership will be verified and the information used to steer their request to the appropriate Real Servers. If the Real Servers selected based on group membership are not available, the default behavior is to fall back to the assigned scheduling method for the Virtual Service.

1.1 Document Purpose

The purpose of this document is to provide information and instructions on how to configure the LoadMaster to steer client traffic based on group membership. For more information on the ESP feature and options in general, refer to the **ESP, Feature Description**.

1.2 Intended Audience

This document is intended for network and application administrators that are interested in finding out more about using ESP for steering client traffic based on AD group membership in the Kemp LoadMaster.

1.3 Related Firmware Version

Published with LMOS version 7.2.48.3 LTS. This document has not required changes since 7.2.48.3 LTS. However, the content is in sync with the latest LoadMaster LTS firmware.

1.4 Prerequisites

Before configuring ESP steering groups in LoadMaster, it is assumed that the following prerequisites have been met:

- The relevant configuration has been made in the Active Directory, (i.e. setting up user groups and adding the relevant users to the relevant groups.)

- A determination has been made as to which groups will be used to steer traffic to which Real Servers.

- The relevant Virtual Service(s) and Real Server(s) have been created and configured as needed. For information on how to configure Virtual Services, and the various features available in the Kemp LoadMaster, refer to the Kemp Documentation page: http://kemptechnologies.com/documentation/.

- An appropriate **Client Authentication Mode** is being used (steering groups are not available for **Basic Authentication** or **SAML** authentication).

- Kerberos Constrained Delegation (KCD) is not in use (steering groups do not work with KCD).

2 How ESP Steering Groups Work

A description of how the ESP steering groups work is provided below:

1. The names of the desired Active Directory groups to perform steering on are entered into the **Steering Groups** text box in the Virtual Service modify screen in the LoadMaster.

2. When steering groups are specified in a Virtual Service and a user logs in, the username is tested to check if it exists in any of the steering groups, starting from the left.

3. If there is a match, the index of the matching group is returned in a cookie to the client. The index of the steering group is determined based on the position of the steering group in the **Steering Groups** text box, (i.e. the first group in the list has an index of 1, the second has an index of 2 and so on.) If the user is in multiple groups, the index of the first group in which the user is found is returned.

4. Content rules should be created to match each of the steering groups and assigned to the relevant Real Servers. On subsequent logins, the index number is used steer the traffic to the relevant Real Server.

For step-by-step instructions on how to configure this, refer to the **Configure ESP Steering Groups in the LoadMaster** section.

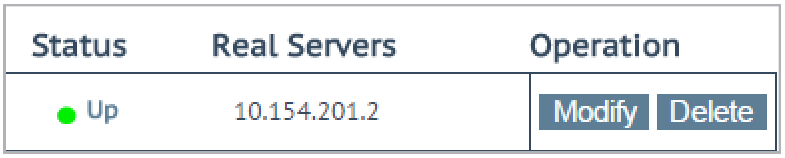
3 Configure ESP Steering Groups in the LoadMaster

Follow the steps in the sections below to configure ESP steering groups in the LoadMaster.

3.1 Set the ESP Steering Groups in the Virtual Service(s)

To configure ESP steering groups, follow the steps below in the Kemp LoadMaster Web User Interface (WUI). ESP SSO Domain settings must already be configured on the LoadMaster for this to function properly. See the **ESP, Feature Description** for details on configuring SSO Domains

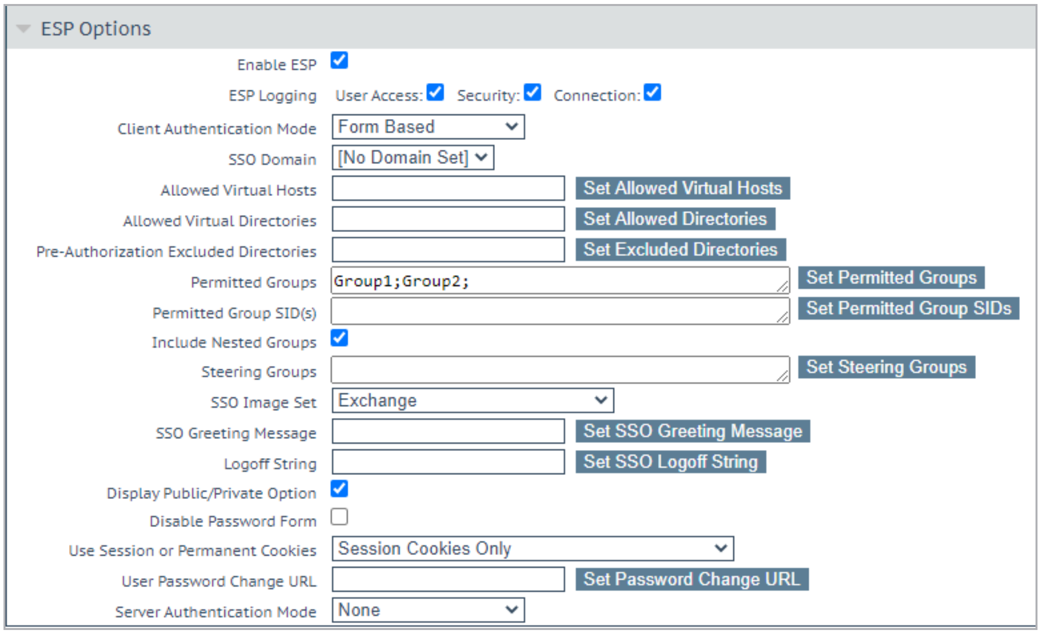
1. In the main menu, go to **Virtual Services > View/Modify Services**.



Status	Real Servers	Operation
● Up	10.154.201.2	Modify Delete

2. Click **Modify** on the relevant Virtual Service.

3. Expand the **ESP Options** section and check the **Enable ESP** check box.



ESP Options

Enable ESP	☑
ESP Logging	User Access: ☑ Security: ☑ Connection: ☑
Client Authentication Mode	Form Based
SSO Domain	[No Domain Set]
Allowed Virtual Hosts	
Allowed Virtual Directories	
Pre-Authorization Excluded Directories	
Permitted Groups	Group1;Group2;
Permitted Group SID(s)	
Include Nested Groups	☑
Steering Groups	
SSO Image Set	Exchange
SSO Greeting Message	
Logoff String	
Display Public/Private Option	☑
Disable Password Form	☐
Use Session or Permanent Cookies	Session Cookies Only
User Password Change URL	
Server Authentication Mode	None

4. Select the appropriate **Client Authentication Mode** (steering groups are not available when using **Basic Authentication** or **SAML** authentication).

5. Enter the Active Directory group names which contain members that are allowed to access the service in the **Permitted Groups** field and click the **Set Permitted Groups** button.

6. Enter the Active Directory group names that will be used for steering traffic in the **Steering Groups** field and click the **Set Steering Groups** button.

Use a semi-colon to separate multiple group names.

The steering group index number will correspond to the location of the group in this list. In the example above - Group1 has an index of 1 and Group2 has an index of 2.

Do not enter the same group name in both the **Permitted Groups** and **Steering Groups** fields. This causes a conflict. When you specify a steering group, it is assumed to behave like a permitted group, so you do not need to enter the same group in both the **Permitted Groups** and **Steering Groups** fields.

7. Enable or disable the **Include Nested Groups** option.

This field relates to the **Permitted Groups** setting. Enable this option to include nested groups in the authentication attempt. If this option is disabled, only users in the top-level group will be granted access. If this option is enabled, users in both the top-level and first sub-level group will be granted access.

8. Configure any other settings as needed.

3.1.1 Notes about Permitted Groups and Steering Groups

Some notes around the permitted groups and steering groups are below:

- The **Permitted Groups** and **Steering Groups** entered should correspond to groups configured in the Active Directory.

- The permitted groups are the groups that are allowed to access this Virtual Service. When set, if a user logs in to an application published by this Virtual Service, the user must be a member of at least one of the groups specified.
- The **Permitted Group SID(s)** (security identifiers) field is the equivalent of the **Permitted Groups** field. If specifying permitted groups, you can complete either the **Permitted Groups** field or the **Permitted Groups SID(s)** field. In the **Permitted Group SID(s)** field:
  - You can specify the Group SIDs that are allowed to access this Virtual Service. After you type the groups, click **Set Permitted Group SIDs**.
  - You can a list of group SIDs of up to 64 bytes and 2048 characters in length.
  - Each group is separated by a semi-colon. Spaces are used to separate bytes in certain group SIDs. Here is an example: **S-1-5-21-703902271-2531649136-2593404273-1606**. SIDs can be found by using the **get-adgroup-Identity GroupName** command.
- The **Steering Groups** steer client traffic to subsets of Real Servers in a Virtual Service based on group membership.
- Multiple groups are supported per Virtual Service up to a maximum of 2048 characters in length.
- Performance may be impacted if a large number of groups are entered on a single Virtual Service.
- The steering group(s) entered must also be specified as permitted groups.
- If steering groups are specified for a Virtual Service, the group membership is tested for each group in the list - starting from the left. If there is a match - the first matching group is the one that will be used to steer the traffic.
- Groups entered are validated using an LDAP query to Active Directory
- The group(s) specified must be valid groups in the Active Directory domain that is specified in the SSO domain associated with the Virtual Service. The SSO domain name in the LoadMaster must be set to the Active Directory name as opposed to the DNS name of the service. For example, if the SSO domain in the LoadMaster is set to webmail.example but this is not the actual Active Directory domain FQDN, it will not function. Instead, the SSO domain would need to be set to .example.com.

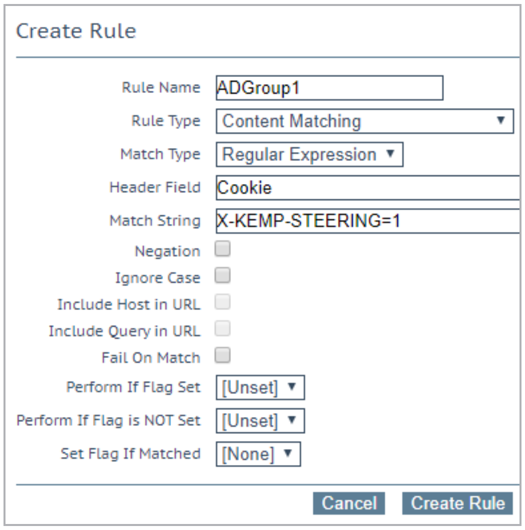
- Multiple groups should be separated by a semi-colon (**;**). A space will not separate the groups since some group names may contain a space, such as **Domain Users**.
- The following characters are not allowed in permitted group names:
/ : + *
- The authentication protocol of the SSO domain must be LDAP when using these groups.
- The groups should be specified by name, not by full distinguished name (for example, “testgroup” as opposed to “CN=testgroup,CN=Users,DC=kemptech,DC=com”)
- If the Virtual Service configuration is updated while a user has an open session, the request may not be steered as expected. You could flush the cache as a workaround, but this would clear the cache for all Virtual Service users meaning they are forcibly disconnected.
- Do not enter the same group name in both the **Permitted Groups** and **Steering Groups** fields. This causes a conflict. When you specify a steering group, it is assumed to behave like a permitted group, so you do not need to enter the same group in both the **Permitted Groups** and **Steering Groups** fields.

3.2 Create the Content Rules

When a user logs in, the index number of the first matching steering group is used to create a cookie. The index number of the steering groups correspond to the order of the groups in the **Steering Groups** field in the Virtual Service, (that is, the first group has an index of 1, the second has an index of 2 and so on.)

The cookie is called **X-Kemp-STEERING**. Content rules should be created and added to the relevant Real Server(s) in order to match the relevant steering group and steer the traffic appropriately. To create a content rule for this purpose, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **Rules & Checking > Content Rules**.
2. Click **Create New**.



Create Rule

Rule Name	ADGroup1
Rule Type	Content Matching ▾
Match Type	Regular Expression ▾
Header Field	Cookie
Match String	X-KEMP-STEERING=1
Negation	□
Ignore Case	□
Include Host in URL	□
Include Query in URL	□
Fail On Match	□
Perform If Flag Set	[Unset] ▾
Perform If Flag is NOT Set	[Unset] ▾
Set Flag If Matched	[None] ▾

3. Enter a recognizable **Rule Name**.

4. Ensure the **Rule Type** is set to **Content Matching**.

5. Ensure the **Match Type** is set to **Regular Expression**.

6. Enter **Cookie** as the **Header Field**.

7. Enter **X-Kemp-STEERING=<IndexOfSteeringGroup>**, for example **X-Kemp-STEERING=1** to match the first group in the Steering Groups list.

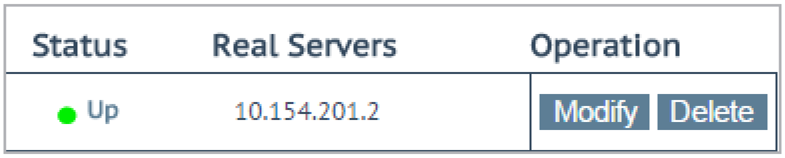
8. Click **Create Rule**.

9. Repeat these steps for any other steering groups, as needed.

3.3 Assign the Content Rule(s) to the Real Server(s)

After creating the content rules, the rules need to be assigned to the relevant Real Server(s) in order to steer the traffic to those Real Servers based on the steering group. To assign a content rule to a Real Server, follow the steps below:

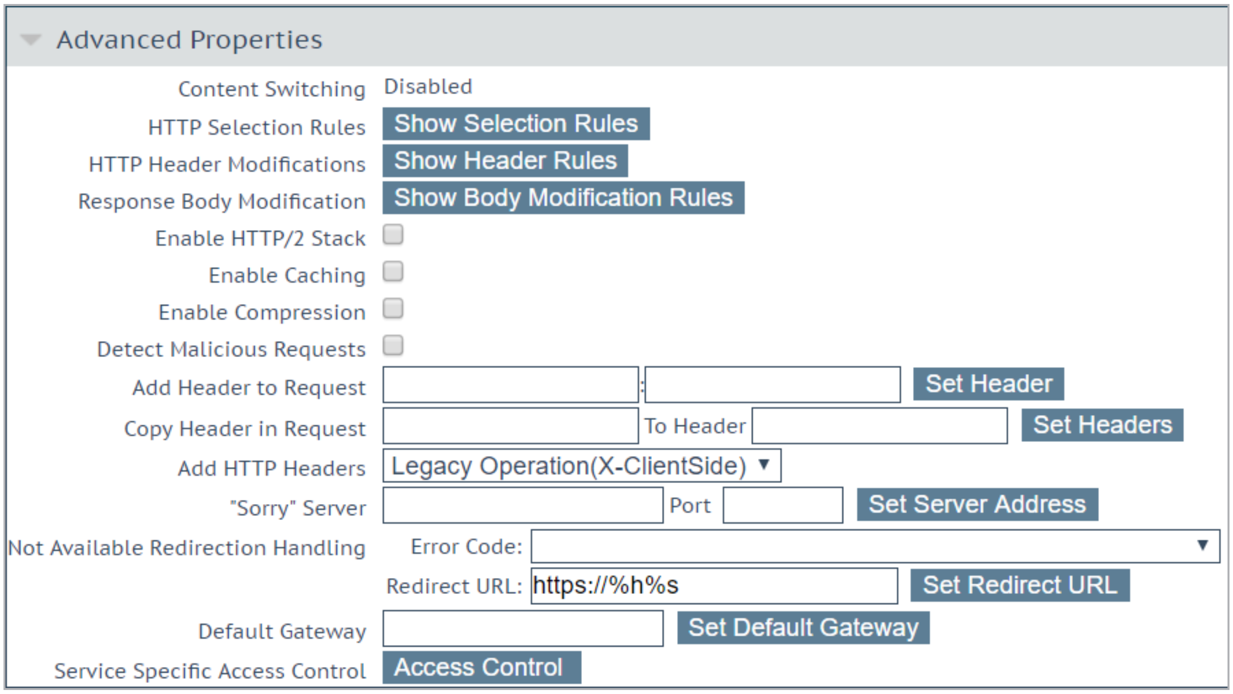
1. In the main menu of the LoadMaster WUI, go to **Virtual Services > View/Modify Services.**



Status	Real Servers	Operation
● Up	10.154.201.2	Modify Delete

2. Click **Modify**.

3. Expand the **Advanced Properties** section.

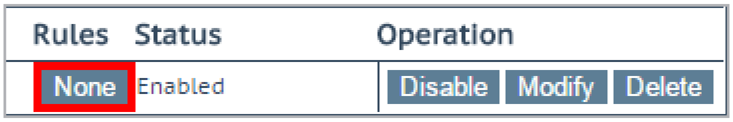


Advanced Properties

Content Switching	Disabled
HTTP Selection Rules	Show Selection Rules
HTTP Header Modifications	Show Header Rules
Response Body Modification	Show Body Modification Rules
Enable HTTP/2 Stack	□
Enable Caching	□
Enable Compression	□
Detect Malicious Requests	□
Add Header to Request	: Set Header
Copy Header in Request	To Header Set Headers
Add HTTP Headers	Legacy Operation(X-ClientSide) ▼
"Sorry" Server	Port Set Server Address
Not Available Redirection Handling	Error Code: ▼
	Redirect URL: https://%h%s Set Redirect URL
Default Gateway	Set Default Gateway
Service Specific Access Control	Access Control

4. Click **Enable** in the **Content Switching** section.

5. Expand the **Real Servers** section.

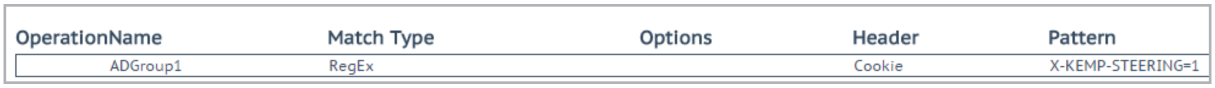


Rules	Status	Operation
None	Enabled	Disable Modify Delete

6. Click the **None** button in the **Rules** column for the relevant Real Server.

7. Select the relevant rule from the **Rule** drop-down list.

8. Click **Add**.



OperationName	Match Type	Options	Header	Pattern
ADGroup1	RegEx		Cookie	X-KEMP-STEERING=1

9. Repeat these steps to assign the other rules to the relevant Real Servers, as needed.

If a content rule which matches on a steering group with the index 1 has been assigned to a Real Server, users in the first steering group listed in the **Steering Groups** field will be directed to that Real Server - if it is available. If the Real Server is not available, the traffic distribution will default to the **Scheduling Method** selected for the Virtual Service.

4 References

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

ESP, Feature Description

Last Updated Date

This document was last updated on 08 December 2020.