Content Switching for Azure

Reference Architecture

VERSION: 1.0

UPDATED: Feb 2016

Copyright Notices

Table of Contents

1 Introduction

The vast variety of software and solutions available in Microsoft's Azure cloud, coupled with the fact that a virtual instance present only a single IP address, creates the need for advanced content switching capabilities. KEMP's LoadMaster offers comprehensive content switching features tightly integrated into a single product along with a broad set of L4-L7 features including SSL decrypt/re-encrypt, application firewalling, SSO and authentication. Having a single point for configuration and management of these features greatly simplifies building sophisticated services by connecting multiple applications across multiple cloud regions.

.

1.1 Document Purpose

This document provides a brief overview of some of the content switching capabilities offered by KEMP's LoadMaster, and provides an example of a typical deployment. The example shows the steps needed to implement a solution using the integrated features in LoadMaster. This typical content switching scenario provides users seamless access to multiple Azure services via a single URL.

1.2 Intended Audience

This document applies to:

- Cloud and Network Architects
- Administrators
- Developers of:
    - Online services that require security features such as user authentication
    - Applications that require the protection of a WAF e.g. for PCI compliance

.

2 Uses for Content Switching

Optimized to run natively inside of the Microsoft Azure cloud platform, Virtual LoadMaster (VLM) for Azure delivers full L4-7 load balancing and application delivery services for Azure-hosted workloads.

With its built-in L7 content switching capabilities LoadMaster can direct traffic based on the content of:

- Request URL
- HTTP Header
- Source IP Address
- Body of the request

Sophisticated pattern matching can be applied to these parameters to achieve precise control over how traffic is directed.

Some common applications of Content Switching are:

• URL Switching - Dedicated application pools for specific directories or file extensions can be used when application design calls for it.

• Hostname Specific Servers – An Azure VM presents a single public IP. Multiple hostnames can be associated with it and LoadMaster can identify requests to different hosts and direct them accordingly.

• Source IP Specific Sites - By opening internal sites to specific external IPs, you can allow distributors, partners or remote offices to access specific content. Similar techniques can be used to provide premium access to certain services for privileged customers.

LoadMaster is also capable of Header Modification. This is another way LoadMaster leverages regular expressions to manipulate traffic on the fly. Header modifications can be used to insert, remove or modify HTTP headers either in requests or responses or to modify URLs before they are passed to real servers. Some typical examples are listed in the following table.

Modification	Result
Removing the “Server” header from responses	obscures potentially secure server details
Adding the “Connection: close” header	to force connections to close after the response is sent
Replacing “http” with “https” in the Location field	alleviates unnecessary redirection and avoids redirection loops
Reroute requests for the root of a webserver to a specific directory.	commonly used in Exchange deployments to direct requests to the OWA directory
Adding the ‘secure’ attribute to cookies being sent by the real server	ensures sensitive session data is never sent unencrypted
Removing the “Via” header	avoids server interactions with proxies

Modifications such as those listed above could be made individually in connected real servers, however setup and administration of load balanced instances is greatly simplified by making all required settings in the LoadMaster itself.

2.1 Content Switching Example

The following section describes how to set up a LoadMaster to support a number of web services with differing levels of access controls. The chosen architecture comprises three web services as shown in Figure 1.

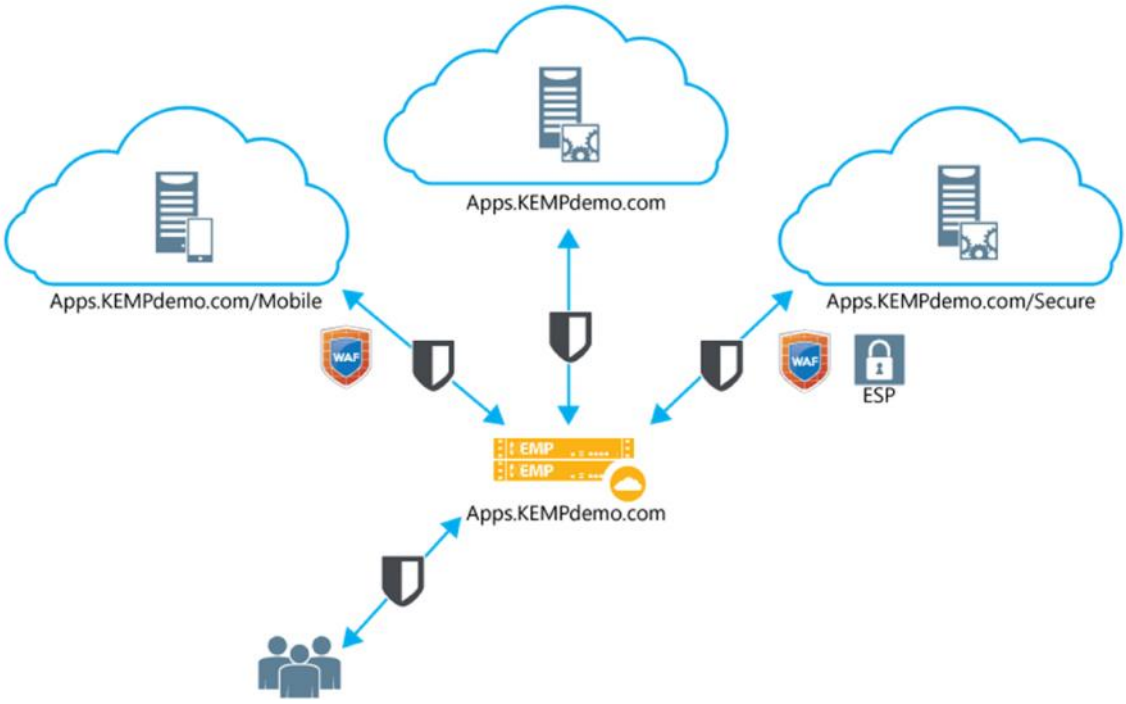

Fig. 1

The services are all accessed through one primary URL. Differing levels of protection and access control can be configured within the LoadMaster depending on the user request.

2.2 Implementation

This example uses three preconfigured web services as shown in figure 2. Note that they do not all have to be running in the same Azure region. Appropriate client requests will direct traffic to the required service. This solution allows multiple PaaS offerings to be aggregated under a single URL and provides secure connections to the services.

Fig. 2

The next step is to create custom domains within the Azure portal.

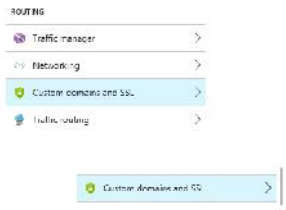

Fig. 3

Each domain will require an SSL certificate to be uploaded to ensure a secure connection to the App Services. The LoadMaster is configured to re-encrypt SSL traffic .

Fig. 4

Azure offers the ability to “Bring your own Domain”. This was set up for each App Service. This requires a TXT record to be created in External DNS to verify the new domain name. The IP address for each service should be noted as these will be used in the LoadMaster to configure the Real Servers.

Fig. 5

Next, certificates must be uploaded for each App Service.

Fig. 6

In the Azure portal, the *Custom domains and SSL* tile now shows the new hostname and certificate.

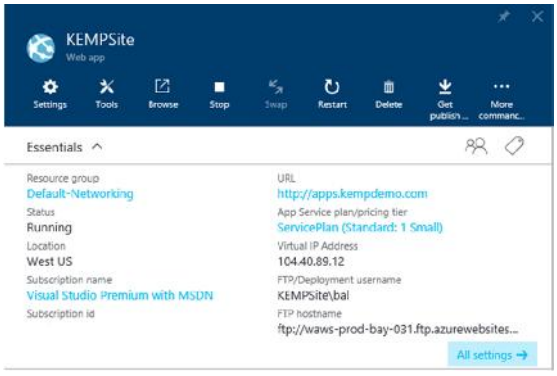

Fig. 7

The summary for the KEMPSite App Service now shows correct URL. Note the Virtual IP address. This will be used as the real server.

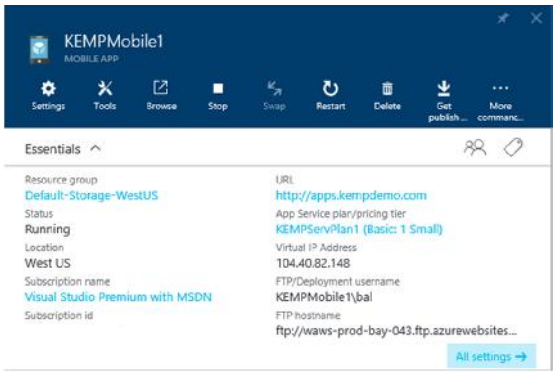

Fig. 8

Similarly, figure 8 shows the configuration of the Mobile service.

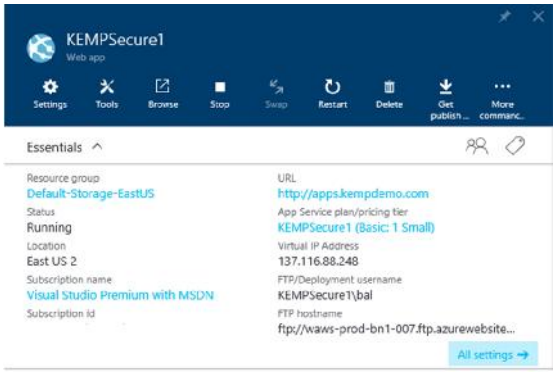

Fig. 9

And finally, figure 9 shows details for the Secure service, which is running in the East US domain.

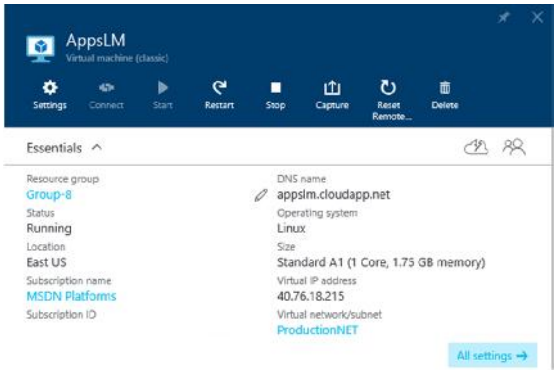

Fig. 10

Figure 10 shows details of the Virtual LoadMaster (VLM for Azure) named “AppsLM”. In this case the Classic deployment method was used. The procedure for installing the LoadMaster from the Azure Marketplace is described in the KEMP documentation. This Virtual IP address will be used

for the DNS record **apps.kempdemo.com.** The LoadMaster will receive traffic for this URL, decrypt, process, re-encrypt and steer requests to the appropriate service.

Fig. 11

Figure 11 shows the Virtual Service for apps.kempdemo.com. There are three Sub Virtual Services, one for each of the App Services. The basic service, KEMPSite, is just doing Layer7. Traffic to the KEMPMobile site is protected by WAF, and the KEMPSecure site is doing Layer7, WAF, and also uses ESP for authentication. The IP address for the Real Servers are shown here, these are the IP address were noted in the summary for each App Service.

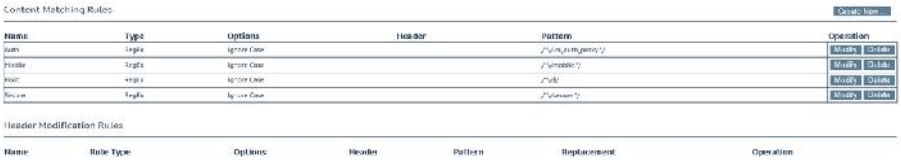

Fig. 12

The content matching rules for this configuration are listed in figure 12. These are processed to route traffic to the correct App Service/SubVS.

“Root” is used for the basic KEMPSite, “Mobile” will be used for the KEMPMobile Site and “Secure” will be used for the KEMPSecure Site and is augmented by the “Auth” rule to control user access to the KEMPSecure Site. This is used in ESP for pre-authentication.

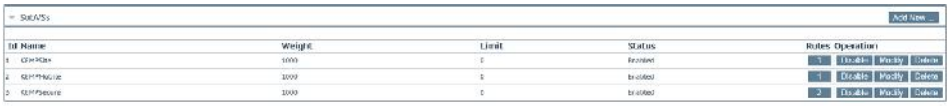

Fig. 13

These rules are applied to the SubVSs. Note that KEMPSecure has two rules; one is for /Secure and the other is for the pre-authentication.

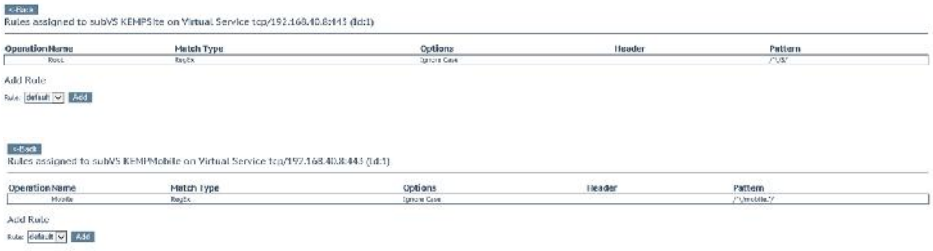

Fig 14

Above we see the single rules applied to the KEMPSite and KEMPMobile sites.

Fig. 15

And figure 15 shows the two rules for KEMPSecure.

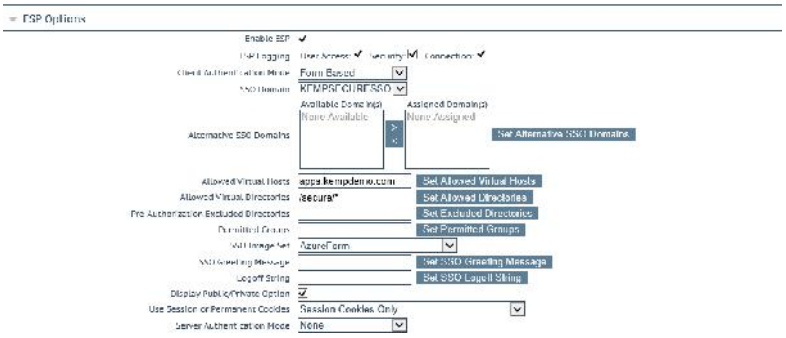

Fig. 16

In the LoadMaster WUI, the Edge Security Pack (ESP) is enabled for the KEMPSecure site. A custom SSO form was added as described in the ESP documentation. The example configuration is now fully configured and ready to serve traffic.

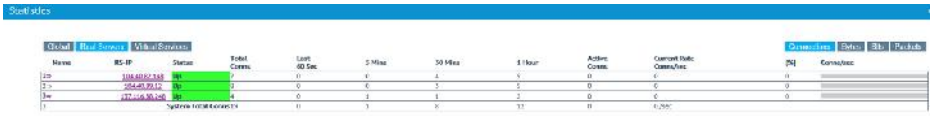

Fig. 17

The LoadMaster WUI can be used to monitor the state of the connected real servers. The statistics show the connections to each of the App Services.

2.3 Requirements

In order to deploy LoadMaster in Azure, a Microsoft subscription and access to the Azure portal (portal.azure.com) are required. Within the portal, the chosen LoadMaster and its associated virtual environment should be prepared first before proceeding with any additional configuration.

References

Additional supporting documents can be found at http://kemptechnologies.com/loadmaster-documentation. The following items in the feature description section address the example above and also provide additional information on configuration for virtual services, security and content switching.

- Virtual Services and Templates
- Sub Virtual Services
- RSA Two Factor Authentication
- Edge Security Pack (ESP)
- Content Rules
- LoadMaster for Azure
- HA for Azure

Document History

Date	Change	Reason for Change	Version	Resp.
Feb 2016	Initial release	First version	1.0	CB

