



Content Switching for Azure

Reference Architecture

VERSION: 1.0

UPDATED: Feb 2016

Copyright Notices

Copyright © 2002-2016 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 product line including software and documentation. The use of the LoadMaster Exchange appliance is subject to the license agreement. Information in this guide may be modified at any time without prior notice.

Microsoft Windows is a registered trademarks of Microsoft Corporation in the United States and other countries. All other trademarks and service marks are the property of their respective owners.

Limitations: This document and all of its contents are provided as-is. KEMP Technologies has made efforts to ensure that the information presented herein are correct, but makes no warranty, express or implied, about the accuracy of this information. If any material errors or inaccuracies should occur in this document, KEMP Technologies will, if feasible, furnish appropriate correctional notices which Users will accept as the sole and exclusive remedy at law or in equity. Users of the information in this document acknowledge that KEMP Technologies cannot be held liable for any loss, injury or damage of any kind, present or prospective, including without limitation any direct, special, incidental or consequential damages (including without limitation lost profits and loss of damage to goodwill) whether suffered by recipient or third party or from any action or inaction whether or not negligent, in the compiling or in delivering or communicating or publishing this document.

Any Internet Protocol (IP) addresses, phone numbers or other data that may resemble actual contact information used in this document are not intended to be actual addresses, phone numbers or contact information. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual addressing or contact information in illustrative content is unintentional and coincidental.

Portions of this software are; copyright (c) 2004-2006 Frank Denis. All rights reserved; copyright (c) 2002 Michael Shalayeff. All rights reserved; copyright (c) 2003 Ryan McBride. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE ABOVE COPYRIGHT HOLDERS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the above copyright holders..

Portions of the LoadMaster software are copyright (C) 1989, 1991 Free Software Foundation, Inc. -51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA- and KEMP Technologies Inc. is in full compliance of the GNU license requirements, Version 2, June 1991. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Portions of this software are Copyright (C) 1988, Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions of this software are Copyright (C) 1998, Massachusetts Institute of Technology

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Portions of this software are Copyright (C) 1995-2004, Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Portions of this software are Copyright (C) 2003, Internet Systems Consortium

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

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



Table of Contents

1	Introduction	5
1.1	Document Purpose	5
1.2	Intended Audience	5
2	Uses for Content Switching	6
2.1	Content Switching Example	8
2.2	Implementation	8
2.3	Requirements	13
	References	14
	Document History	15

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.

Uses for Content Switching

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.

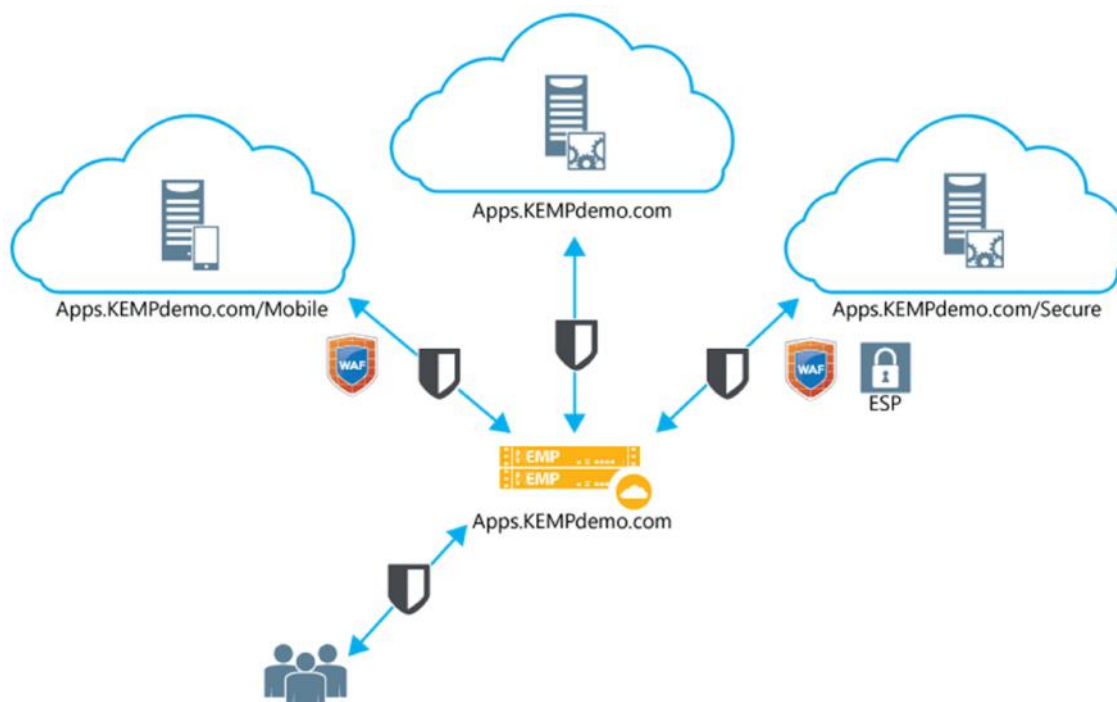


Fig. 1

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.

Content Switching Reference Architecture



Uses for Content Switching

NAME	STATUS	APP TYPE	APP SERVICE PLAN	LOCATION
KEMPMobile1	Running	Mobile app	KEMPService1	West US
KEMPSecure1	Running	Web app	KEMPService1	East US 2
KEMPSite	Running	Web app	ServicePlan	West US

Fig. 2

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

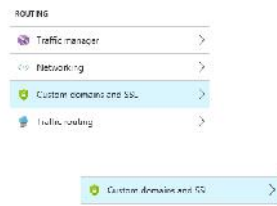


Fig. 3

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.

Uses for Content Switching



Fig. 5

Next, certificates must be uploaded for each App Service.

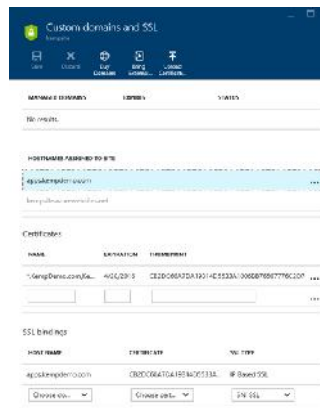


Fig. 6

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

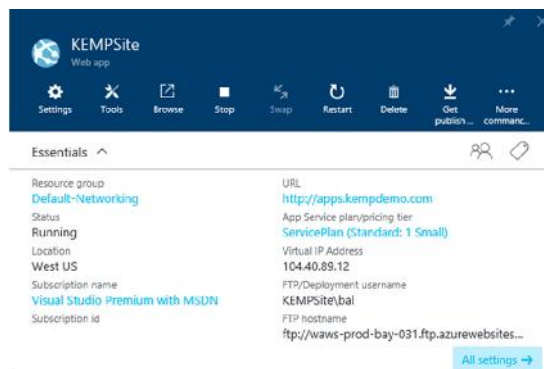


Fig. 7

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

Uses for Content Switching

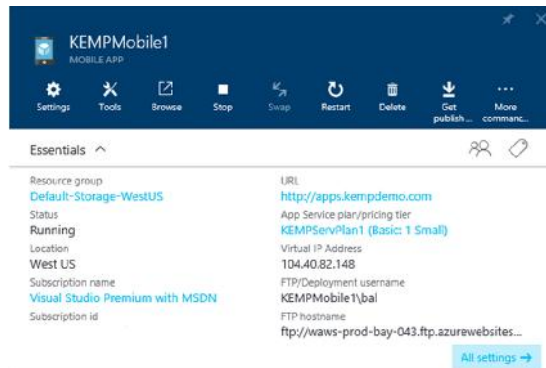


Fig. 8

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

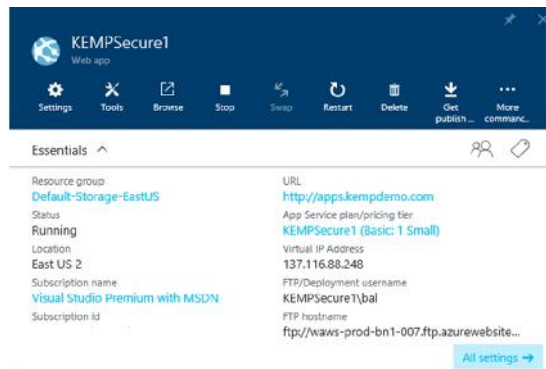


Fig. 9

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

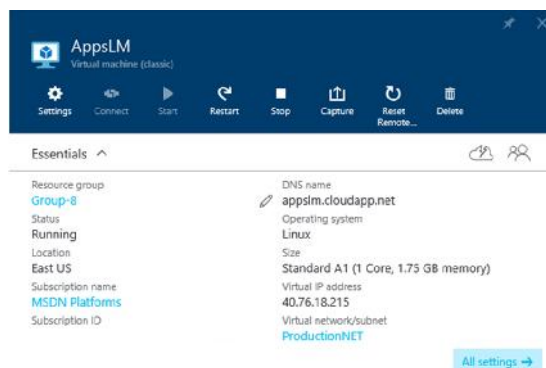


Fig. 10

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

Content Switching Reference Architecture



Uses for Content Switching

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.

Virtual IP Address	Port	Name	Layer	Certificate Installed	Status	Real Servers	Operation
192.168.40.44	80	Application	L7	*apps.kempdemo.com	Yes	192.168.40.45 192.168.40.46	Modify Delete
#1	80	KEMPSite	L7		Yes	192.168.40.45	Modify
#2	80	KEMPMobile	L7+WAF		Yes	192.168.40.46	Modify
#3	80	KEMPSecure	L7+WAF+ESP		Yes	192.168.40.45	Modify

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.

Name	Type	Options	Header	Pattern	Operation
Auth	Regex	Ignore Case		/(.*)auth(.*)/	Redirect Delete
Mobile	Regex	Ignore Case		/(.*)mobile/	Redirect Delete
Root	Regex	Ignore Case		/(.*)/	Redirect Delete
Secure	Regex	Ignore Case		/(.*)secure/	Redirect Delete

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.

Of Name	Weight	Limit	Status	Rules	Operation
1. KEMPSite	1000	0	Enabled		Redirect Modify Delete
2. KEMPMobile	1000	0	Enabled		Redirect Modify Delete
3. KEMPSecure	1000	0	Enabled		Redirect Modify Delete

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.

Operation Name	Match Type	Options	Header	Pattern
Root	Regex	Ignore Case		/(.*)/

Operation Name	Match Type	Options	Header	Pattern
Mobile	Regex	Ignore Case		/(.*)mobile/

Fig 14

Uses for Content Switching

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

Operation Name	Match Type	Options	Header	Pattern
Enable	Secure	Ignore Date		/*/*/*/*/*/*
Enable	Audit	Ignore Date		/*/*/*/*/*/*

Add Rule

Fig. 15

And figure 15 shows the two rules for KEMPSecure.

ESP Options

- Enable ESP:
- Enable Logging: (User Address, User Agent, Connection)
- Client Authentication: (Form Based, KEMPSite, KEMPMobile)
- Available Domains: [None Available] | Assigned Domains: [None Assigned] | [Set Alternative SSO Homepage](#)
- Allowed Virtual Hosts: [Set Allowed Virtual Hosts](#) (app.kemp.com)
- Allowed Virtual Directories: [Set Allowed Directories](#) (secure)
- Pre Authorization Excluded Directories: [Set Excluded Directories](#)
- Permitted Groups: [Set Permitted Groups](#)
- URL Rewrite Rule: [Set SSO Redirecting Message](#) (None) | [Set SSO Layout String](#)
- Display Public/Private Option: (Session Cookies Only)
- Use Session or Permanent Cookies: (Session Cookies Only)
- Server Authentication Mode: (None)

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.

Host	Real Server	App Services	Total Conn	Last 60 Sec	5 Min	30 Min	1 Hour	Active Conn	Current Rate Conn/Sec	PM	Conn/Sec
128	104.45.92.113	App	0	0	0	0	0	0	0		
129	104.45.92.112	App	0	0	0	0	0	0	0		
130	104.45.92.114	App	0	0	0	0	0	0	0		
System Total/Active			0	0	0	0	0	0	0		

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

Document History

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