Copyright Notices

Copyright © 2002-2013 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 trademark 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 AND 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 No. 6,473,802 and 6,374,300
# Table of Contents

1 Introduction .......................................................................................................................... 5
  1.1 Document Purpose ........................................................................................................ 5
  1.2 Intended audience .......................................................................................................... 5
2 Load Balancing AD FS ........................................................................................................... 6
3 Example Environment Setup ................................................................................................. 9
4 Prerequisites .......................................................................................................................... 12
  4.1 DNS ................................................................................................................................ 12
  4.2 AD FS SSL Certificate Import on LoadMaster ............................................................... 12
5 Virtual Service (VS) Configuration ....................................................................................... 14
  5.1 Configure an AD FS Internal Farm Virtual Service ...................................................... 14
  5.2 Configure an AD FS Proxy Farm Virtual Service ......................................................... 17
References ................................................................................................................................ 19
Document History .................................................................................................................... 20
1 Introduction

Active Directory Federation Services (AD FS) is a Microsoft identity access solution. It was an optional component of Microsoft Windows Server® 2003 R2. It is now built into Windows Server® 2008 and Windows Server® 2012. AD FS helps to establish trust relationships and reduces the need for provisioning and managing user accounts. Its implementation provides clients (internal or external to the trusted internal LAN) with simplified access to systems and applications relying on claims-based authorization. AD FS also supports web Single-Sign-On (SSO) technologies to improve UX across multiple protected applications.

Trust relationships are used to project a user’s digital identity and access rights to trusted partners and can be deployed in multiple organisations in order to facilitate business-to-business (B2B) transactions between trusted partner organisations.

1.1 Document Purpose

This documentation is intended to provide guidance on how to configure KEMP LoadMaster products to provide high availability for an AD FS 2.0 environment. This documentation is created using a representative sample environment described later in the document. As this documentation is not intended to cover every possible deployment scenario it may not address unique setup or requirements. The KEMP Support Team is always available to provide solutions for scenarios not explicitly defined.

1.2 Intended audience

It is assumed that the reader is a server/network administrator or a person otherwise familiar with networking and general computer terminology and is familiar with AD FS technology.
2 Load Balancing AD FS

The core components of AD FS are as follows:

- An AD FS server which is responsible for issuance of claims and user authentication. This server must be able to connect to a Domain Controller. It authenticates users from multiple domains via Windows Trust. The AD FS server can be set up in a cluster to ensure high availability.

- An AD FS proxy server which protects the AD FS server from internet-based threats. The AD FS proxy server also authenticates users from the internet. Again, the AD FS proxy server can be set up in a cluster to ensure high availability.

- An AD FS configuration database which can be stored in an SQL database or Windows Internal Database (maximum of 5 servers) but not both at the same time. This database stores the following items:
  - Relying Party Trust
  - Certificates
  - Claim Provider Trust
  - Claims description
  - Service configuration
  - Attributes

The diagram below shows a common authentication process flow for applications located in a resource organization and secured with AD FS, of which Office 365 is a popular example. The steps, which correspond to the numbers in the diagram, are outlined as follows.
Figure 2-1: Load Balancing the AD FS Server Farm

1. The internal user tries to access the AD FS-enabled resource.
2. The client is redirected to the resource’s Federation Service.
3. If the resource’s federation service is configured as a trusted partner, the client is redirected to the organisation’s internal Federation Service.
4. The AD FS server uses the Active Directory to authenticate the user.
5. The AD FS server sends an authorization cookie to the client. This contains the signed security token and a set of claims for the resource partner,
6. The client connects to the resource partner’s Federation Service where the token and claims are verified. If appropriate, the resource partner may send a new security token.
7. The client presents the new authorisation cookie with the security token to the resource in order to access it.
3 Example Environment Setup

In our example deployment, “KEMP Demo” has deployed AD FS 2.0 in their environment to facilitate claims-based authentication for their Exchange 2010 infrastructure and allow for SSO capabilities across applications. The deployment contains the following:

- Two AD FS 2.0 Servers
- Two AD FS 2.0 Proxy Servers
- Two Exchange 2010 Multi-Role Servers
- A KEMP LoadMaster High Availability (HA) Cluster

A name space of owaADFS.KEMPdemo.com is used for access to the Microsoft Exchange environment. A name space of myADFS.KEMPdemo.com is used for access to the AD FS environment. Split DNS is implemented, which allows these name spaces to be used both internally and externally in the environment.

The following scenarios are defined:

- Internal access to Outlook Web App (OWA) using the internal AD FS farm, both of which are being load-balanced by the KEMP LoadMaster
- External access to OWA using the Proxy Farm and Internal Farm all three of which are being load-balanced by the KEMP LoadMaster
The following diagrams represent the respective environments:

**Figure 3-1: Internal user access**
Figure 3-2: External user access
4 Prerequisites

There are some prerequisites to be aware of before deploying the KEMP LoadMaster with AD FS.

It is assumed that the AD FS 2.0 environment is already set up and the KEMP LoadMaster has been installed. We recommend reviewing the LoadMaster Web User Interface (WUI), Configuration Guide.

At a minimum, the following actions should be completed:

- Implemented Active Directory, AD FS, Domain Name System (DNS), Federation Server Proxy (FSP), and other Microsoft requirements
- Configured the application servers to support claims-based authentication
- Installed the LoadMaster on the same network as the servers
- Established access to the LoadMaster WUI

4.1 DNS

Access to the DNS used in the environment must be available. This is needed to set up name resolution of the AD FS services to the virtual service IP addresses that will be configured on the KEMP LoadMaster.

4.2 AD FS SSL Certificate Import on LoadMaster

The AD FS SSL certificate has to be imported into the LoadMaster before deployment. To import the certificate, follow the steps below:

1. Log in to the relevant Virtual Load Master (VLM).
2. In the main menu, click Certificates and select SSL Certificates.

![Figure 4-1: Manage Certificates screen](image)

3. Click the Import Certificate button.
4. Click **Browse...** next to the **Certificate File** field.
5. Browse to and select the certificate file.
6. Click **Open**.
7. Browse to and select the Key File if needed.
8. Enter the **Pass Phrase** of the certificate.
9. Enter a name for the certificate in the **Certificate Identifier** field.
10. Click the **Save** button.
11. If it works a success message will be displayed. Click **OK**.

Despite the fact that clients establish a single Transmission Control Protocol (TCP) connection with the AD FS server to request and receive a security token, certain applications can suffer from multiple login redirections if persistence is not enabled on the load balancer. For this reason, a Layer 7 service is used, along with SSL bridging, to allow for the more intelligent forms of persistence that are not available at Layer 4 or when SSL traffic is not terminated at the LoadMaster.
5  Virtual Service (VS) Configuration

Steps on how to configure the AD FS Virtual Services that can be used are outlined in the sections below.

5.1  Configure an AD FS Internal Farm Virtual Service

Follow the steps below to configure a VS:

1. Log in to the relevant VLM.
2. In the main menu, click Virtual Services and select Add New.

3. Enter the Virtual Address. This is the Virtual IP address used for the service and must be unique and not in use by any other device on the network.

4. Enter 443 in the Port field.
5. Enter a name for the VS in the Service Name (Optional) field.
6. Ensure that tcp is selected as the Protocol.
7. Click Add this Virtual Service.

8. Expand the SSL Properties section.

10. A warning may appear. Click OK.
11. Select **Reencrypt**.
12. Expand the **Standard Options** section.

13. Select **Super HTTP** as the persistence **Mode**.
14. Select **1 Hour** for the **Timeout** value.
15. Select **least connection** as the **Scheduling Method**.
16. Expand the **Real Servers** section.

17. In the first **Real Server Check Parameters** field, select **HTTPS Protocol**.
18. Enter `/federationmetadata/2007-06/federationmetadata.xml` in the URL text box and click the **Set URL** button.
19. Select the **Use HTTP/1.1** check box.
20. Select **GET** as the **HTTP Method**.
21. Click the **Add New…** button.
Figure 5-7: Real Server parameters

22. Enter the IP address of the server to be added to the real server pool. Click **Add This Real Server**. A success message will be displayed after adding. Click **OK**. Repeat this for any other real servers that need to be added.

23. In the main menu, click **Certificates** and select **SSL Certificates**.

Figure 5-8: Manage Certificates screen

24. Locate the certificate that was added earlier. In the **VS to Add** dropdown menu, select the VS that has just been added and click the **Add VS** button.

25. In the main menu, click **Virtual Services** and select **View/Modify Services**.

Figure 5-9: VS up

26. Confirm that the service is listed with a **Status** of **Up** and that all added member servers are listed in black, non-bold font.

Figure 5-10: Test address

27. Test access to the AD FS Internal Farm by opening a browser and going to `https://<AD FS URL>/ADFS/ls/idpininitiatedsignon.aspx` and following the instructions to log in.
28. Once all other Microsoft-defined AD FS prerequisites and application configurations are complete, test access to the application to ensure authentication success. To do this, open a browser and go to https://owAD FS/<AD FS URL>/owa.

A successful login will result in access to the protected application.

5.2 Configure an AD FS Proxy Farm Virtual Service

The steps to set up an AD FS Proxy Farm are almost identical to the ones listed above in Section 5.1. The only difference is, you should give the Virtual Service a different name and after Step 15 above, follow the steps below:

1. Expand the Advanced Properties section.

   ![Advanced Properties section](image)

   Figure 5-12: Advanced Properties section

2. Select Enable Caching.

3. Select Enable Compression.

   The maximum cache usage should be configured dependent upon the number of services on the LoadMaster that are leveraging this feature.

4. Expand the Real Servers section.
5. In the first **Real Server Check Parameters** drop-down list, select **HTTPS Protocol**.
6. Enter `/adfs/ls/idpInitiatedSignon.aspx` in the **URL** text box and click **Set URL**.
7. Select **GET** as the **HTTP Method**.
8. Continue from **Step 21** in Section 5.1.
References

The following documents are referred to in this document:

1. LoadMaster Web User Interface (WUI), Configuration Guide
   http://www.kemptechnologies.com/documentation
<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Version</th>
<th>Resp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>August-2013</td>
<td>Initial draft</td>
<td>Initial draft of document</td>
<td>v.1.0</td>
<td>LB</td>
</tr>
</tbody>
</table>