



**Single Sign-on
(SSO)
for Azure
Reference Architecture**

VERSION: 1.0

UPDATED: Feb 2016



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	6
1.1	Document Purpose	6
1.2	Intended Audience	6
2	Implementing Single Sign-On with LoadMaster	7
2.1	Setting Up Single Sign-On in Azure	8
2.2	Implementation	9
	References	22
	Document History	23

1 Introduction

Microsoft's Azure cloud is attractive to the growing number of companies who wish to expand or migrate their existing on-premises infrastructure to use easily configurable, on-demand resources. This is especially true where Microsoft infrastructure is extensively deployed in-house as the services offered by Microsoft in Azure will be very familiar.

Where companies are building hybrid environments, making the transition as seamless as possible – both from an architectural standpoint as well as the user perspective – is critical. In addition, finding a solution that is simple to configure and manage is equally important. Virtual LoadMaster, running in the Azure Cloud, provides comprehensive load balancing and content switching capabilities allowing multiple applications and web services to be aggregated, and the integrated Edge Security Pack (ESP) provides authentication and Single Sign-On services.

1.1 Document Purpose

This document describes how to set up LoadMaster to allow single sign-on to an application in a hybrid environment. The example uses SharePoint as the application running in the Azure Cloud, and shows integration with Azure Active Directory domain services.

1.2 Intended Audience

This document applies to:

- Cloud and Network Architects
- System and Security Administrators.

2 Implementing Single Sign-On with LoadMaster

KEMP's LoadMaster includes the Edge Security Pack (ESP) which features:

- End point authentication for pre-authentication
- Persistent logging and reporting for user logging
- Single Sign-On (SSO) across Virtual Services
- LDAP Authentication from the LoadMaster to the Active Directory
- Basic authentication communication from a client to the LoadMaster
- Dual-factor authentication

This allows for a great deal of flexibility in configuring user access to applications. It provides a viable alternative to Microsoft TMG and can be used with security tokens such as the Department of Defence CAC (Common Access Card).

2.1 Setting Up Single Sign-On in Azure

The following section describes how to set up a LoadMaster within the Azure cloud to provide single sign-on capability for an application.

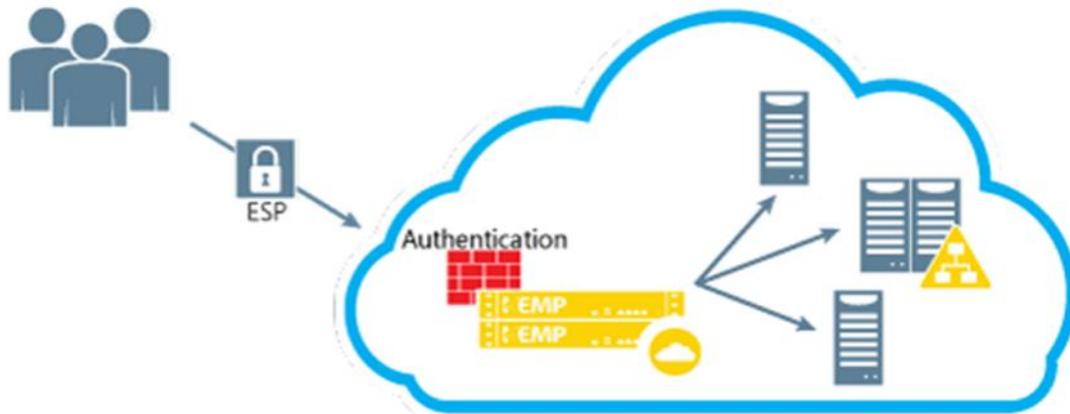


Fig. 1

For this example, SharePoint was chosen as the application and is assumed to have already been set up in Azure. Additional software configuration, both in Azure and on-premises, is required to set up Active Directory Domain Services as a precursor to setting up ESP on the LoadMaster.

2.2 Implementation

Setting up the LoadMaster with ESP is relatively straightforward, however there are a number of steps initially to configure the Active Directory Domain Services. This was chosen to illustrate how LoadMaster can be used in connecting to, or migrating to, the Azure cloud.

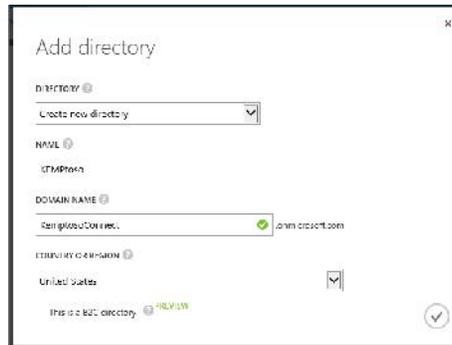


Fig. 2

Starting in the Azure portal, Figure 2 shows how to begin creating a new Azure Active Directory within the Azure subscription

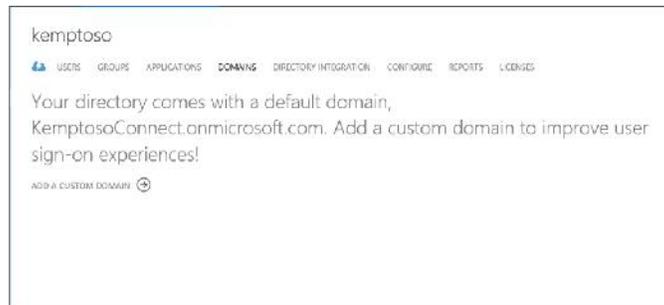


Fig. 3

The next step is to add a custom domain which will span the cloud and on-premises environments.

Single Sign-on Reference Architecture



Implementing Single Sign-On with LoadMaster

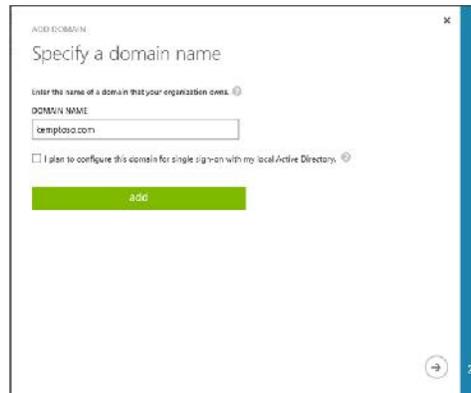


Fig. 4

It is important for this domain to match the on-premises naming.

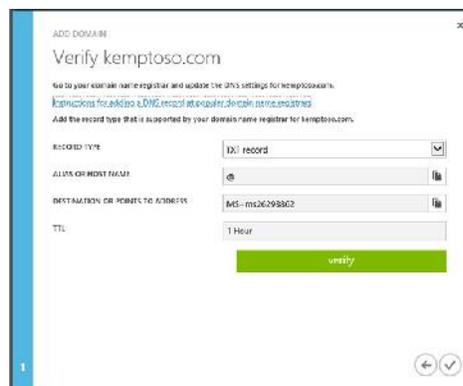


Fig. 5

You must add a TXT record in external DNS to verify adding this domain according to the instructions provided by your domain name registrar.

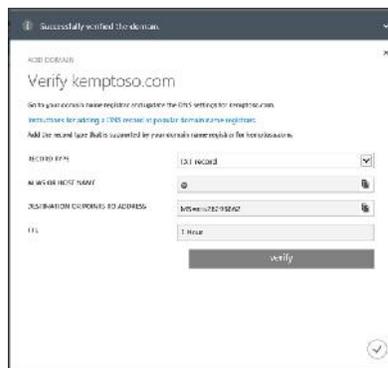


Fig. 6

Implementing Single Sign-On with LoadMaster

Once the record is added you can click on “verify” to complete this task and confirm success. Note that DNS propagation will need to occur so there may be a delay before this record becomes available



Fig. 7

The next part involves creating a user account in Azure AD. This will be used when synchronizing your on premises environment to Azure AD.

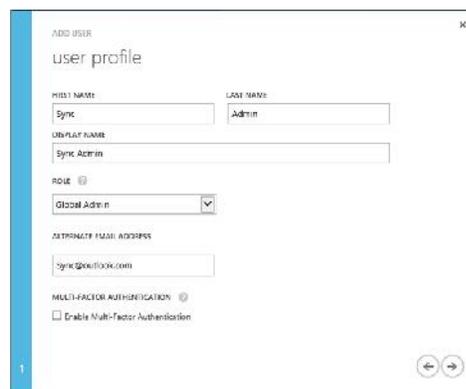


Fig. 8

The user called “sync” will have the necessary administrative rights to permit the synchronization across AD in the cloud.

Implementing Single Sign-On with LoadMaster

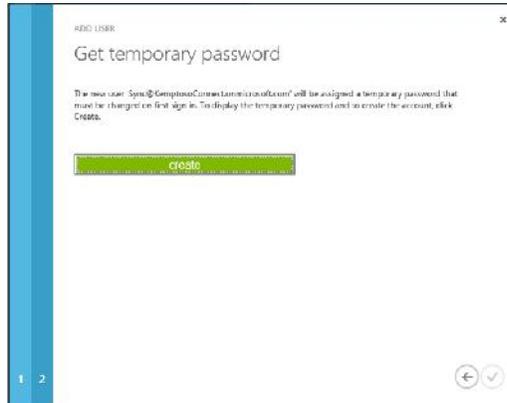


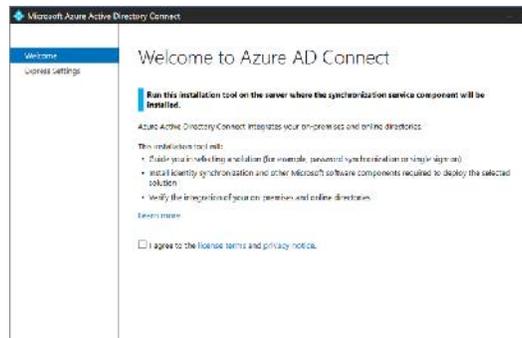
Fig. 9

Make sure to note the password for this new user as this will be needed when starting the AD synchronization.



Fig. 10

Next create a new group in Azure AD to use for administrators. The group must be named “AAD DC Administrators”. You can add users to this group after you run Azure Active Directory Connect in a later step.



Then you must download and install Azure AD Connect on an on premises server according to Microsoft documentation.

Implementing Single Sign-On with LoadMaster

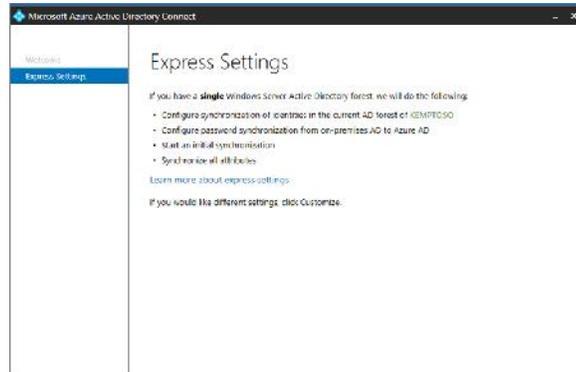


Fig. 12

For this example the basic setting were used.

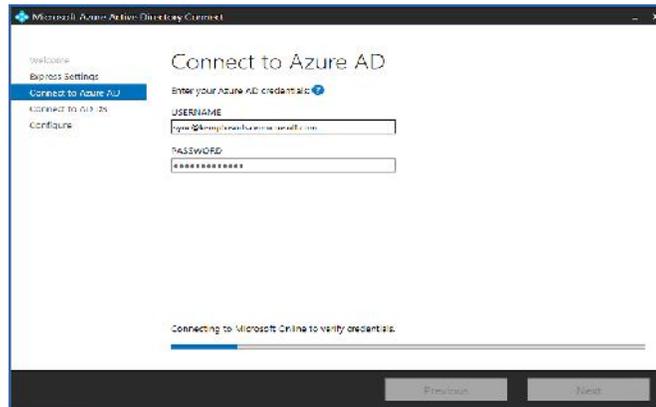


Fig. 13

Now that all the initial preparation is complete, log in with the “sync” account you created in Azure AD to open the connection to the cloud environment.

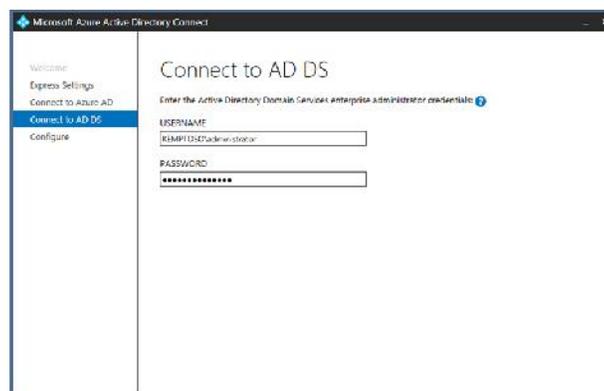


Fig. 14

Implementing Single Sign-On with LoadMaster

The enter your on-premises Enterprise Administrator credentials and both the cloud and on-premises environments will be ready for synchronization.

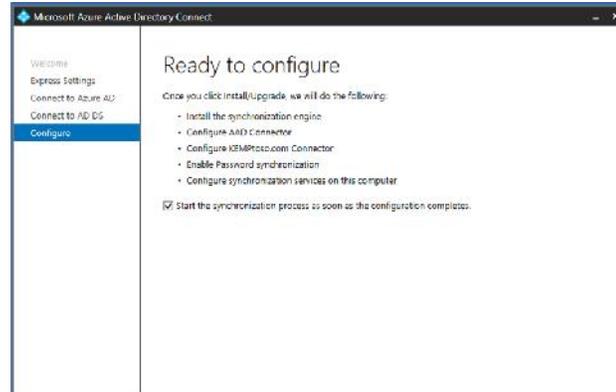


Fig 15

This example uses default configuration options. Configuration can then begin.

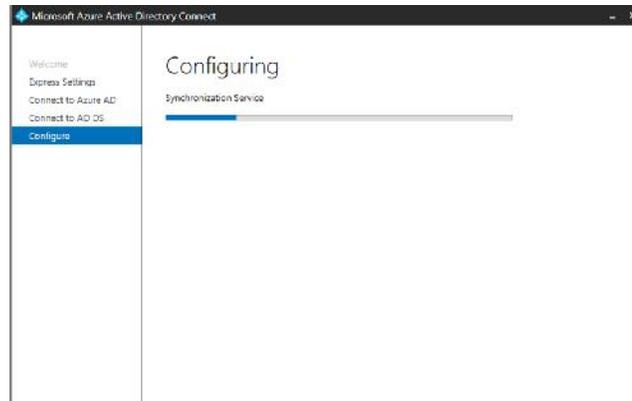


Fig. 16

The synchronization may take some time depending on the amount of data involved.

Implementing Single Sign-On with LoadMaster

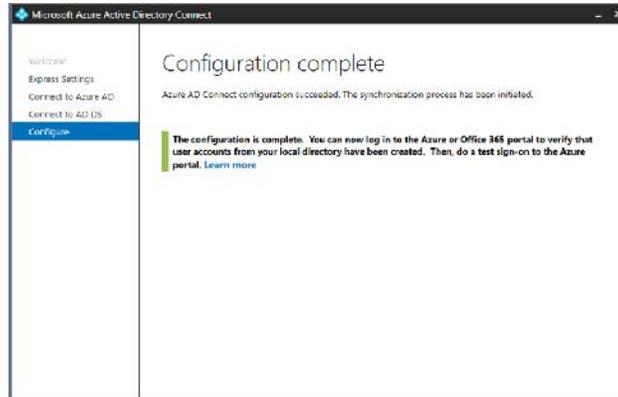


Fig. 17

Once complete, you should carry out some tests to ensure the process has worked as expected.

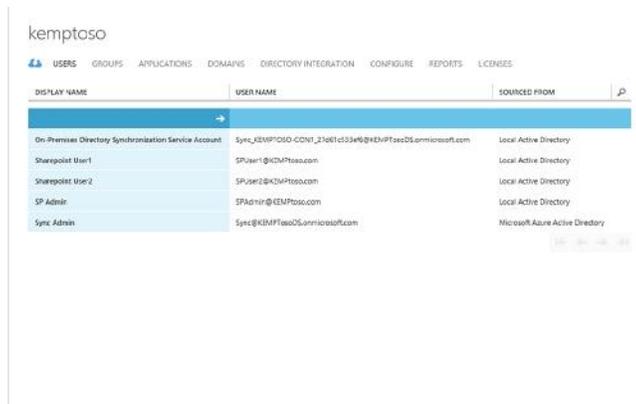


Fig. 18

Connect to Azure and open your Azure Active Directory domain. Then select "USERS" and verify the synchronization completed. Typical results are shown in figure 18.

Implementing Single Sign-On with LoadMaster

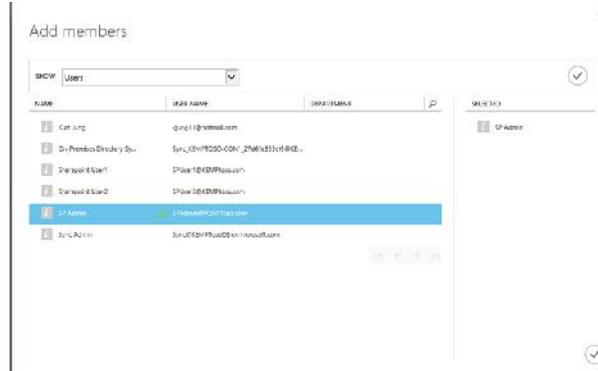


Fig. 19

Next, select “GROUPS” and add the users to the group “AAD DC Administrators”. These are the users that will require administrator functions, for example to add servers to domain.

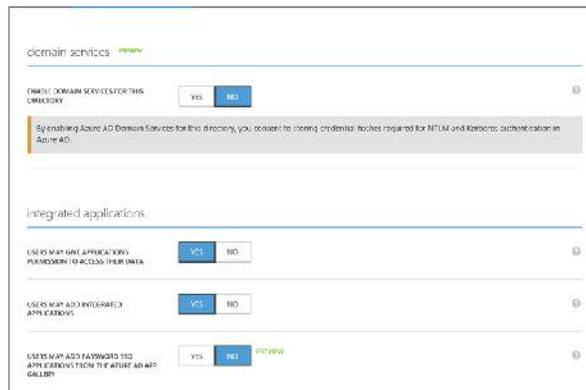


Fig. 20

Connect to Azure and open your Azure Active Directory domain. Then select the configure tab and select “YES” to enable Domain Services.

Implementing Single Sign-On with LoadMaster

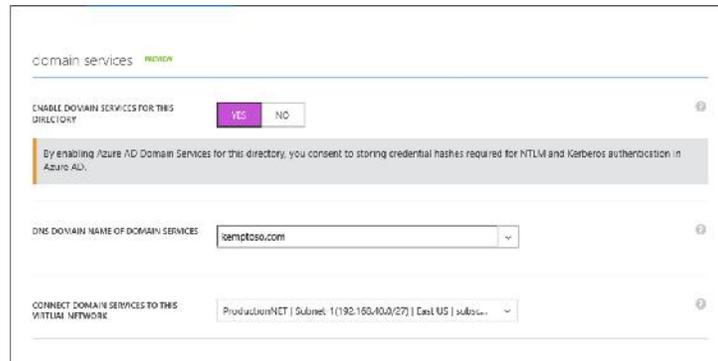


Fig. 21

In the drop down options, select your on premises domain name and the Virtual Network you want to use.



Fig. 22

This process will take a little while to complete, and domain services will then be operational.

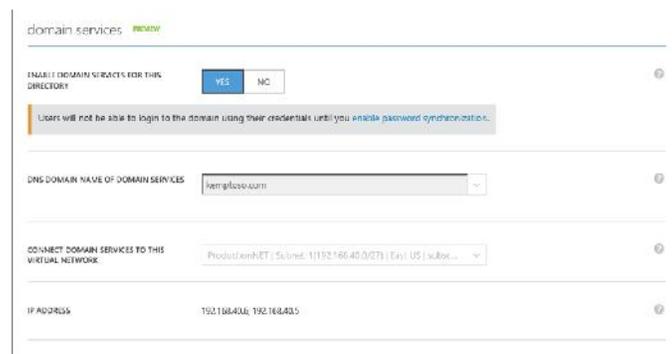


Fig. 23

In the Portal, under domain services you will presented with two IP addresses to use.

Single Sign-on Reference Architecture



Implementing Single Sign-On with LoadMaster

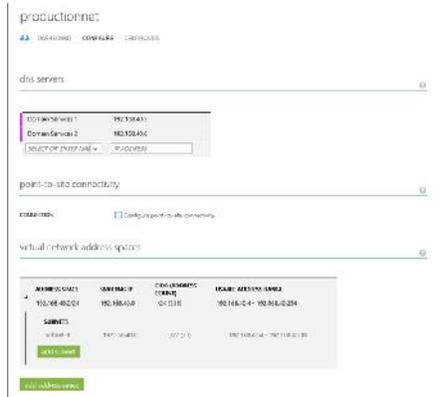


Fig. 24

Now make changes to your Virtual Network configuration to use the new Directory Service IP address for your DNS Servers.

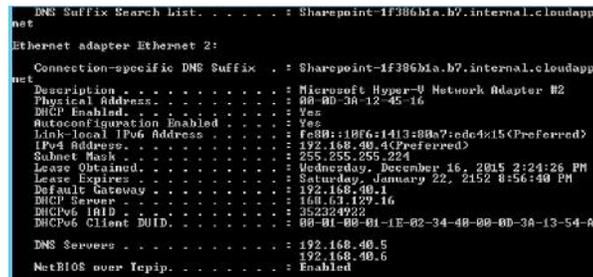


Fig. 25

Your virtual machines will now have these two IP address for DNS.

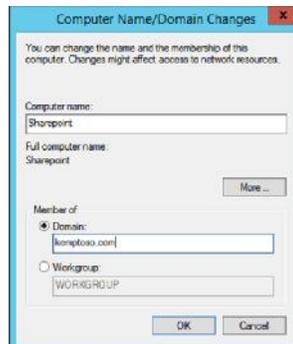


Fig. 26

Now return to the on-premises environment to make the final changes. Add your server running in Azure to Active Directory. This will be the SharePoint server set up for this example.

Implementing Single Sign-On with LoadMaster



Fig. 27

Then you must provide a user account that is a member of the AAD DC Administrator Group

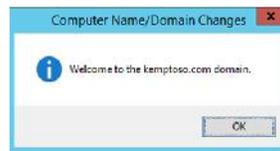


Fig. 28

And now the domain integration is complete and you can connect to the LoadMaster to set up the user access.



Fig. 29

First, add new SSO domain called "AzureDS" to the LoadMaster.

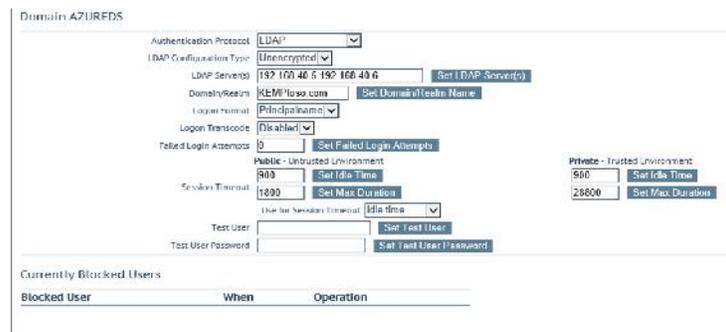


Fig. 30

Implementing Single Sign-On with LoadMaster

Then configure the settings for new SSO domain. The “LDAP Servers” selection must point to Azure AD Domain Services using the IP addresses provided above.

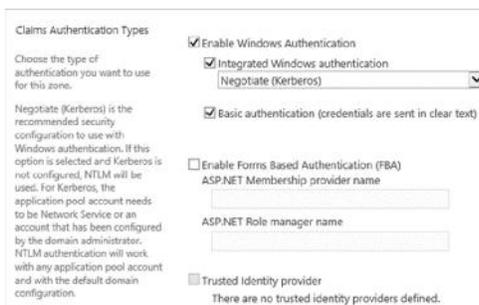


Fig. 31

This example uses Basic Authentication for the SharePoint Web Application.

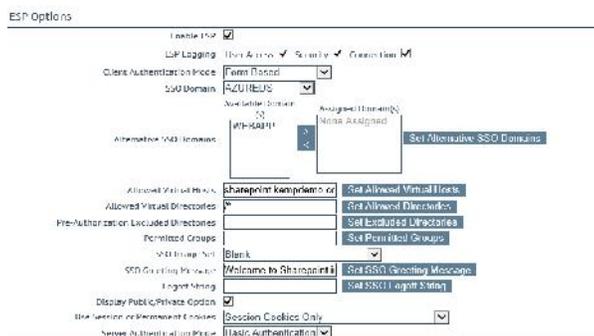


Fig. 32

Navigate to “ESP Options” to enable ESP and select the SSO domain. You can also configure the SSO banner in this screen.

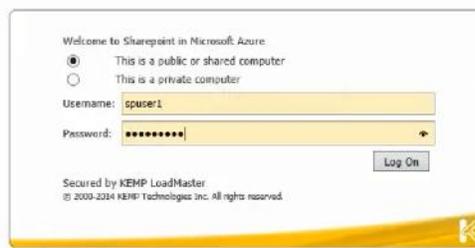


Fig. 33

Once configuration of the LoadMaster is complete, single sign-on is enabled. Figure 33 shows the SSO banner and welcome message that was set up earlier. Users will be required to log in through this to access the SharePoint application.

Single Sign-on Reference Architecture



Implementing Single Sign-On with LoadMaster

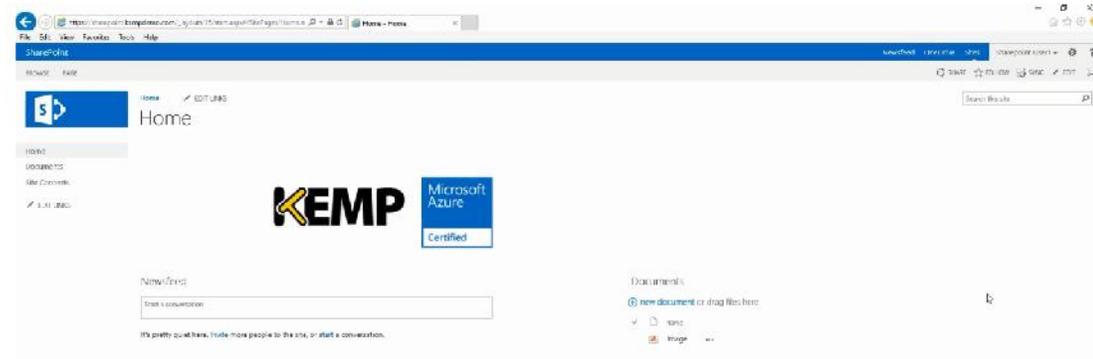


Fig. 34

Once the user has successfully logged in they will have access to the SharePoint site hosted in the Azure Cloud.

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 and security.

- Edge Security Pack (ESP)
- LoadMaster for Azure
- HA for Azure

Microsoft provides documentation and access to Azure AD Domain Services download: <https://azure.microsoft.com/en-us/services/active-directory-ds/>

Document History

Document History

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