Single Sign-on (SSO) for Azure

Reference Architecture

VERSION: 1.0

UPDATED: Feb 2016

Table of Contents

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.

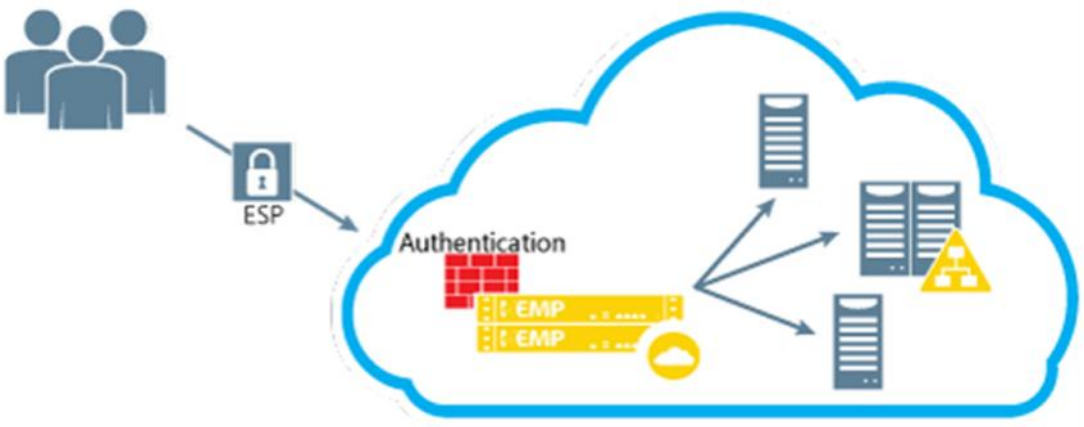


Fig. 1

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.

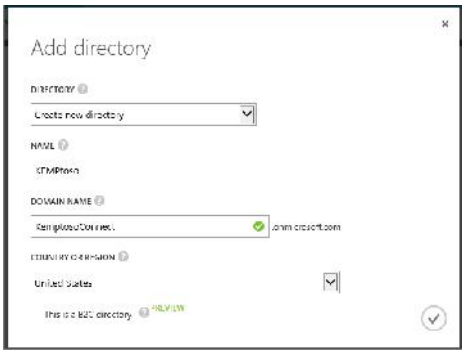


Fig. 2

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.

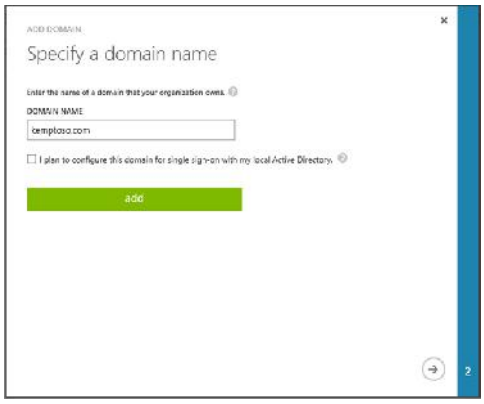


Fig. 4

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

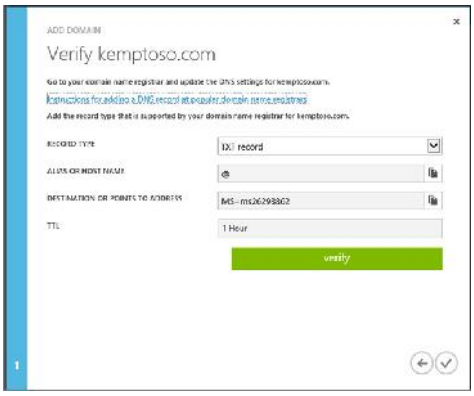


Fig. 5

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

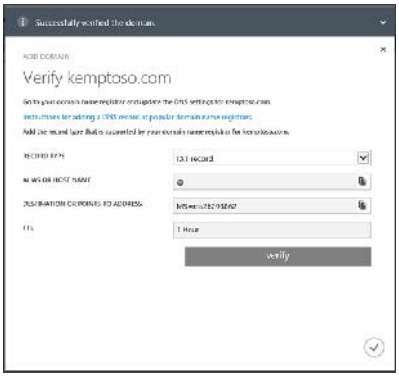


Fig. 6

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.

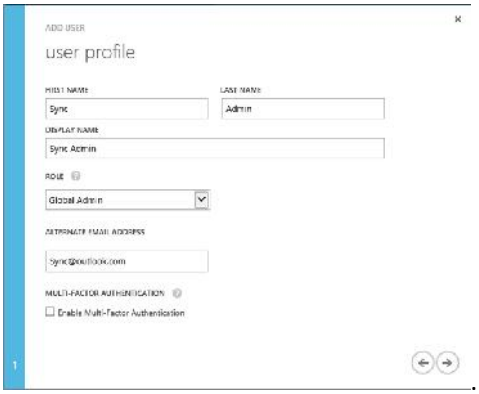


Fig. 8

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

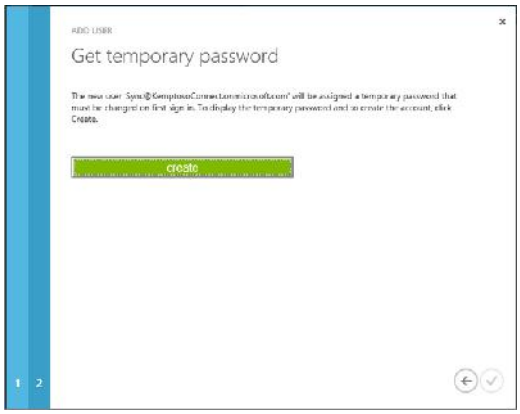
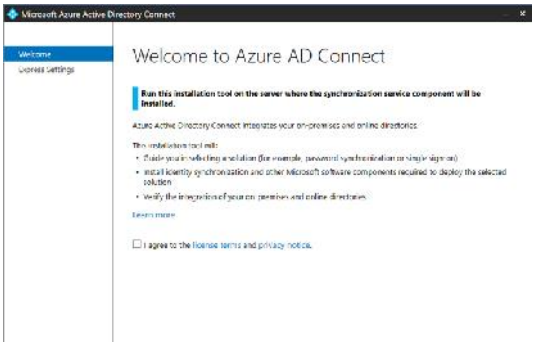


Fig. 9

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.

.

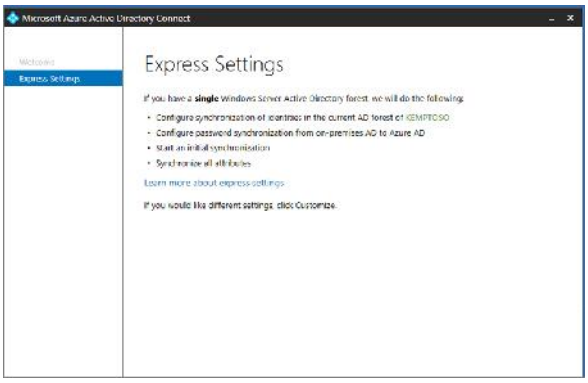


Fig. 12

For this example the basic setting were used.

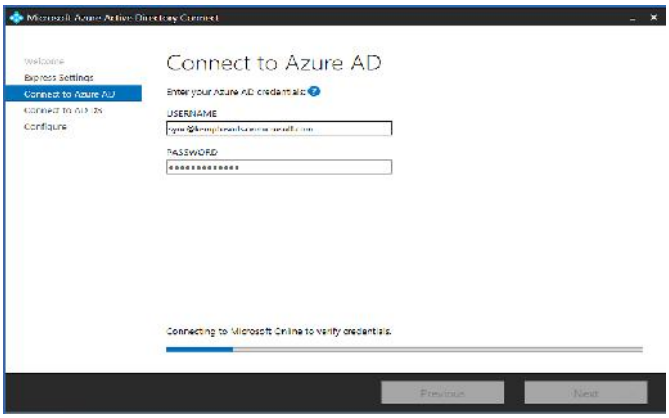


Fig. 13

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.

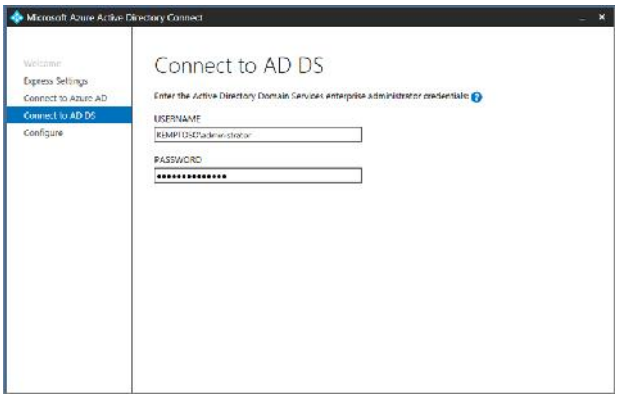


Fig. 14

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

.

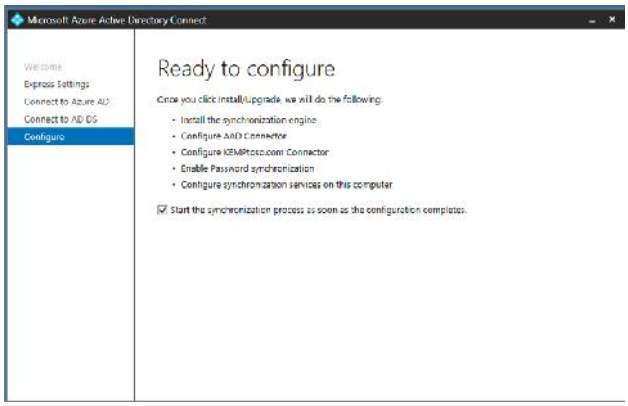


Fig 15

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

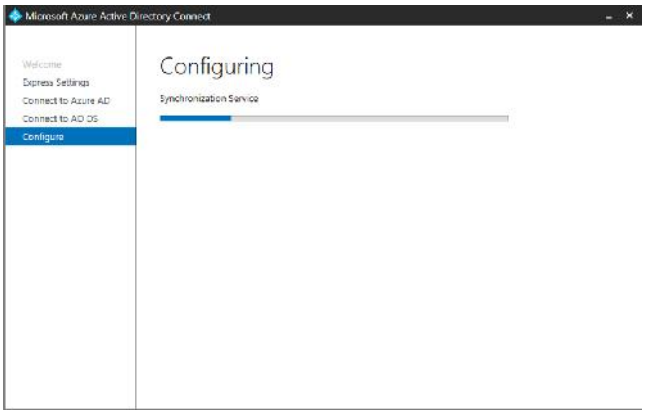


Fig. 16

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

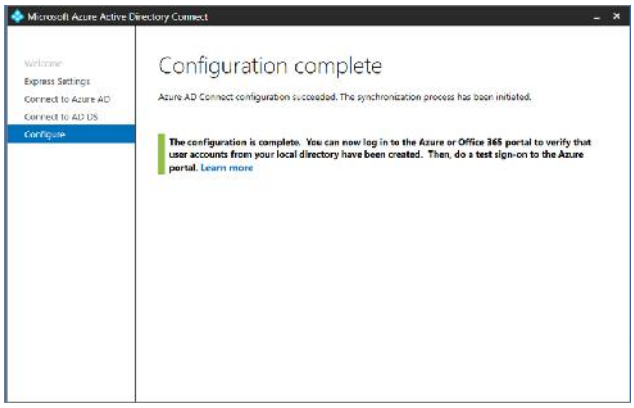


Fig. 17

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

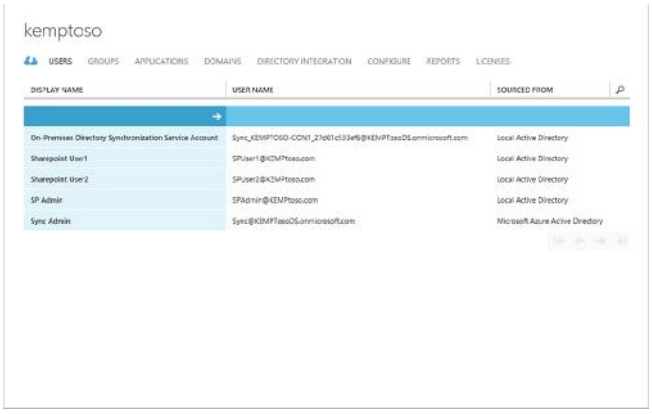


Fig. 18

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.

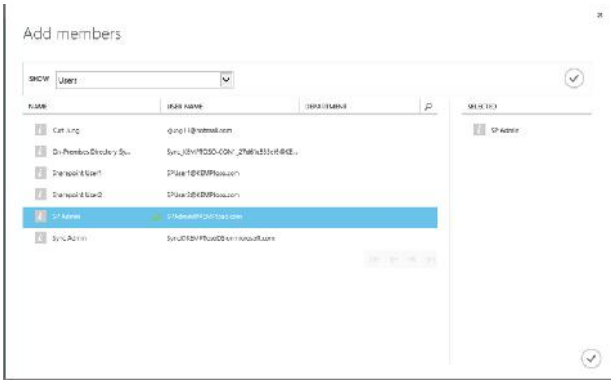


Fig. 19

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.

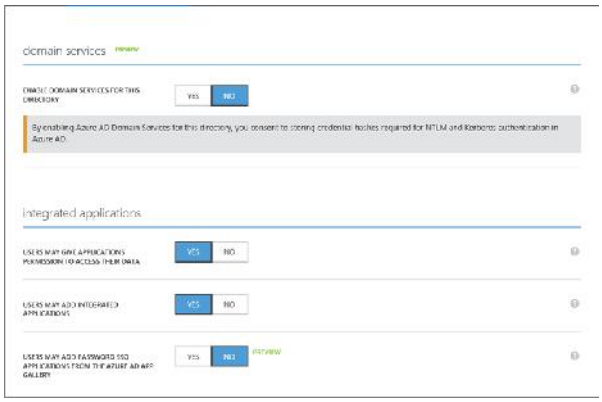


Fig. 20

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

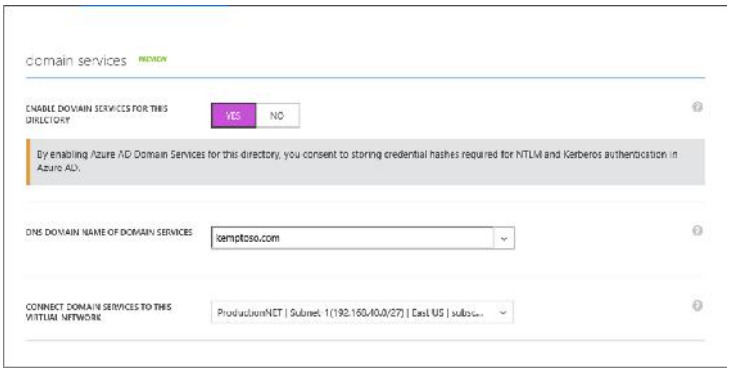


Fig. 21

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.

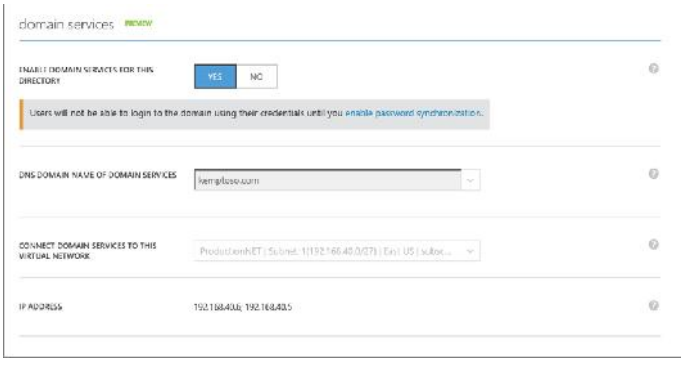


Fig. 23

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

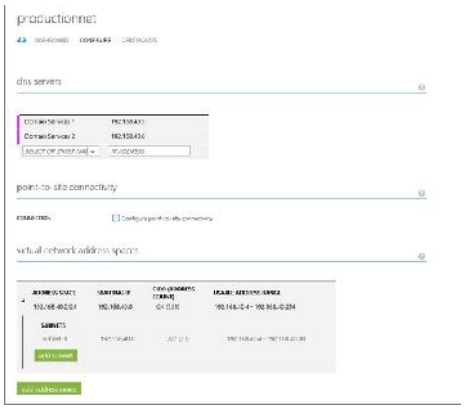


Fig. 24

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

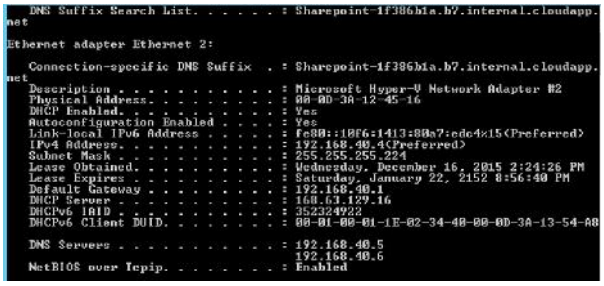


Fig. 25

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

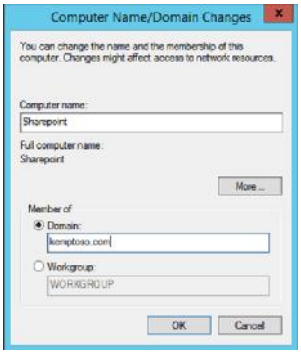


Fig. 26

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.

Fig. 27

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

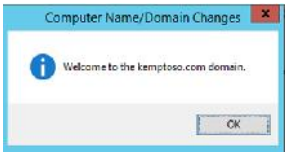


Fig. 28

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.

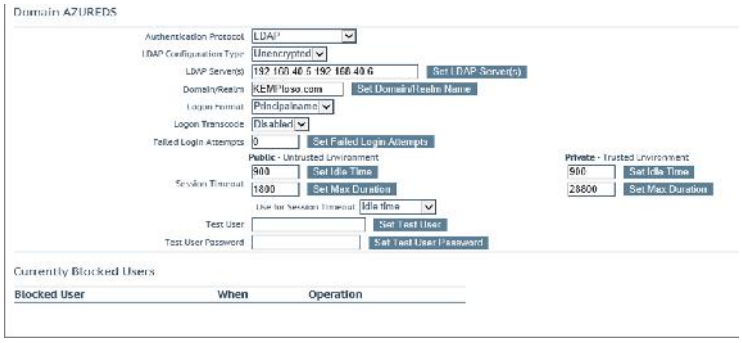


Fig. 30

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.

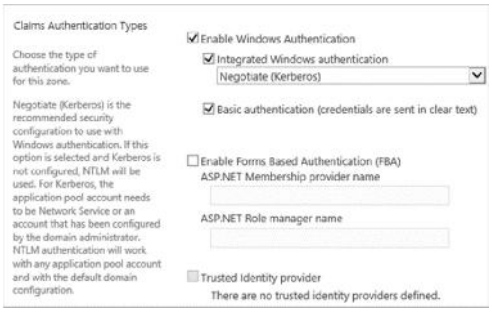


Fig. 31

This example uses Basic Authentication for the SharePoint Web Application.

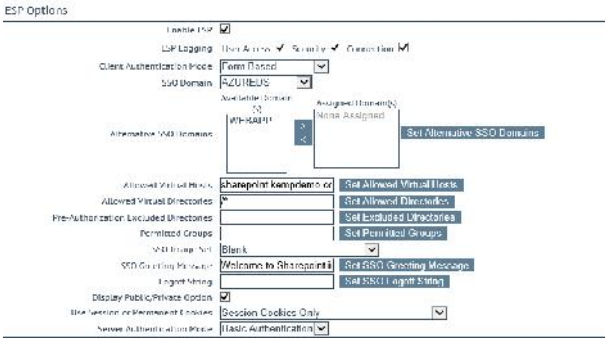


Fig. 32

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

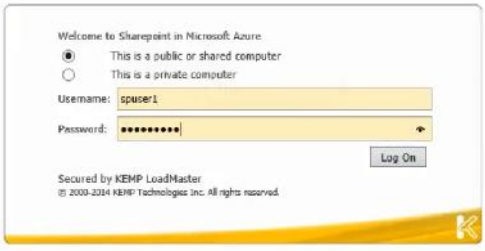


Fig. 33

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.

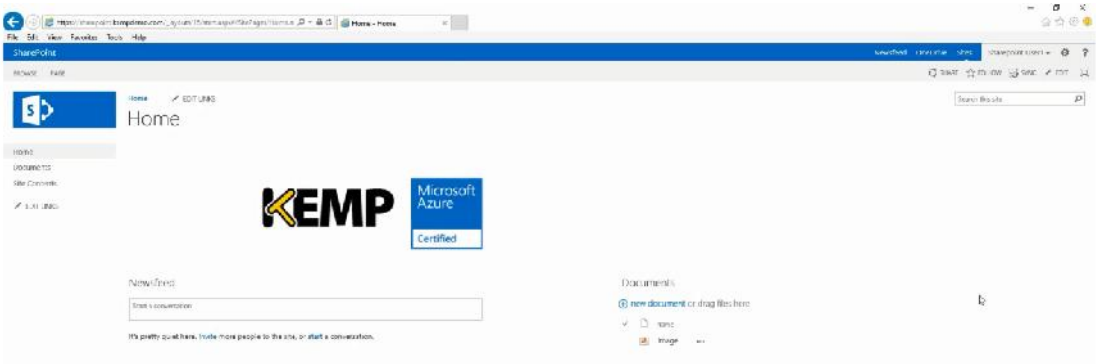


Fig. 34

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

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

