# AD FS Design Considerations and Deployment Options

*By Shane Jackson*

*Blog: ShaneJacksonITPro.wordpress.com*

*Twitter: @shane00jackson*

Lately I have been working more and more with ADFS, mainly because of the Office 365 / Exchange Hybrid / Exchange Online deployments I have been doing.

So I thought I share my experiences, what I have learned and resources I've used. In this article I'll be covering the following:

1. Overview of ADFS
2. ADFS Deployment Steps
3. ADFS Sizing
4. Publishing ADFS externally (ADFS Proxy)
5. High Availability
6. Disaster Recovery
7. ADFS Configuration Database – WID or SQL?
8. Using ADFS for Conditional Access
9. How to migrate ADFS from one server / farm to another
10. Switching Office 365 Identity Model from Cloud Only to Federated
11. ADFS Backup
12. Troubleshooting ADFS
13. What if ADFS can't be recovered?

## 1. Overview of ADFS

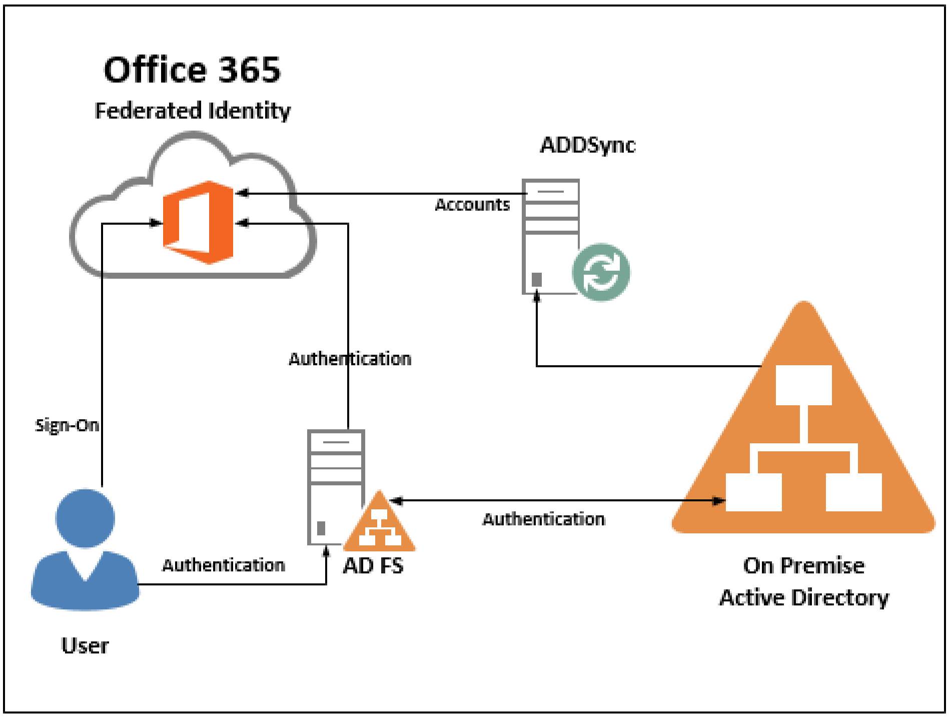
What is ADFS? As described here https://msdn.microsoft.com/en-us/library/bb897402.aspx

- *AD FS is a standards-based service that allows the secure sharing of identity information between trusted business partners (known as a federation) across an extranet*

For all the ADFS deployments I have done, I can describe its function as follows

- *Provides a mechanism for authentication to Office 365 services to be made against the customers on-premise Active Directory*

The following diagram illustrates ADFS providing an authentication mechanism to Office 365



Of course, this authentication service is not limited Office 365 and can be utilized with other 3rd parties

## 2. ADFS Deployment Steps

There are of number of great blogs describing step by step how to deploy ADFS.  The most comprehensive step by step guide I have come across for deploying Exchange Hybrid, and integrating with ADFS for single sign on, is from Henrik Walther @HenrikWalther on msexchange.org and is available here

**Configuring an Exchange 2013 Hybrid Deployment and Migrating to Office 365 (Exchange Online)**

http://www.msexchange.org/articles-tutorials/office-365/exchange-online/configuring-exchange-2013-hybrid-deployment-migrating-office-365-exchange-online-part1.html

Key thing when following these guides is to ensure that the version of ADFS you are deploying matches the steps described in the blog.  There are differences in the steps for ADFS 2.0 and ADFS 3.0

Other ADFS deployment guides include

**How To Install ADFS 2012 R2 For Office 365**

http://blogs.technet.com/b/rmilne/archive/2014/04/28/how-to-install-adfs-2012-r2-for-office-365.aspx

This ADFS 2012 R2 guide from Rhoderick Milne @RhoderickMilne covers 3 elements

1. Install ADFS
2. Install ADFS Proxy

3. Leverage ADFS with Office 365

## 3. ADFS Sizing

This http://technet.microsoft.com/en-us/library/ff678034.aspx

link provides guidelines for hardware requirements (memory, CPU etc.) for federation servers and federations proxies.

| H/W Requirement | Minimum | Recommended |
|---|---|---|
| CPU Speed | Single Core, 1 GHz | Quad Core, 2Ghz |
| RAM | 1 GB | 4 GB |
| Disk Space | 50 MB | 100 MB |

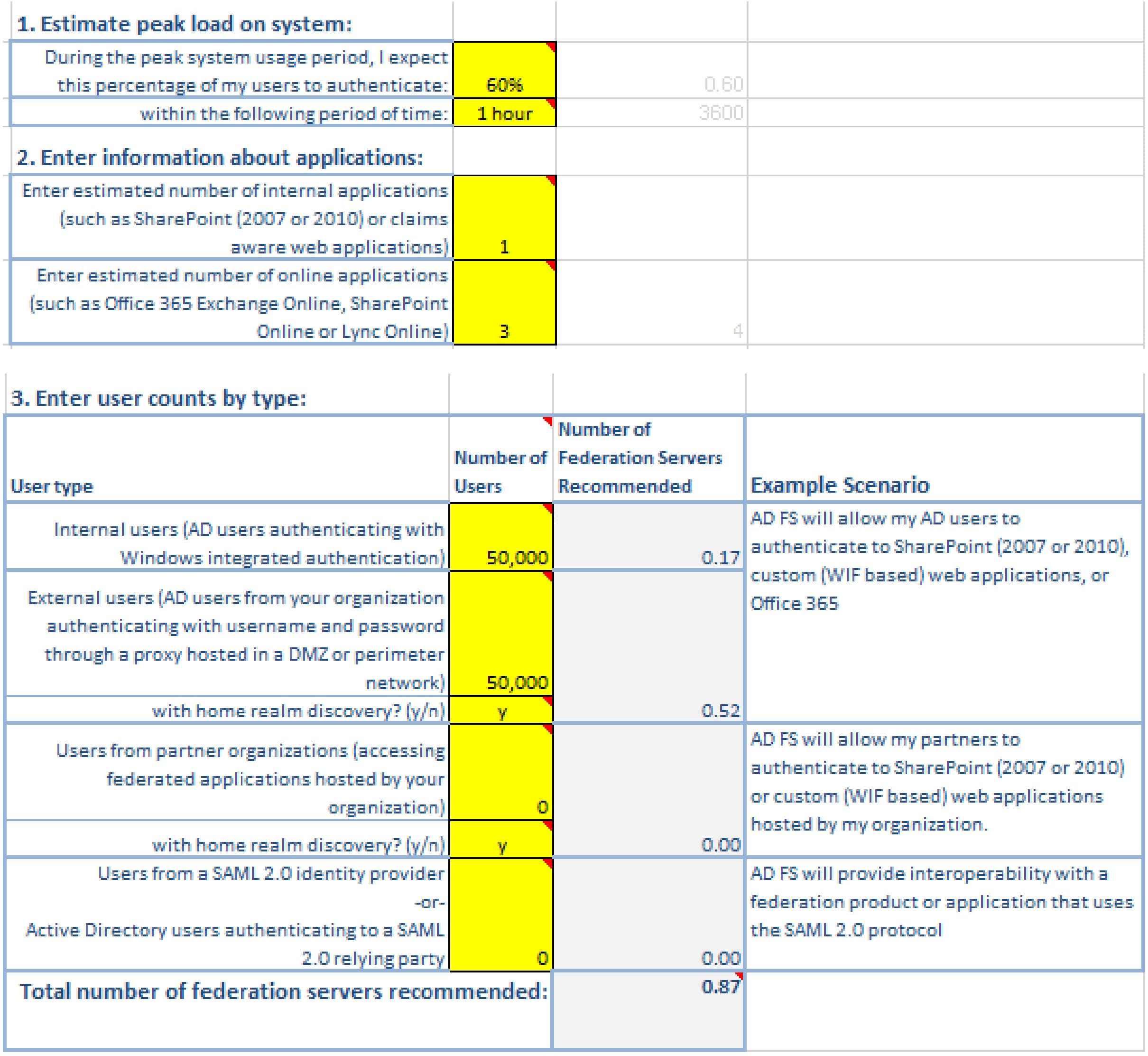
However, as per this link, https://msdn.microsoft.com/en-us/library/azure/dn151324.aspx
based on following server specification

| H/W Requirement | Recommended |
|---|---|
| CPU Speed | Dual Quad Core, 2Ghz |
| RAM | 4 GB |
| Disk Space | 100 MB |

The number of users per server is as follows

| Number of Users | Number of Servers |
|---|---|
| < 1000 | Can deploy ADFS on 2 existing Domain Controllers. Then load balance with separate NLB servers<br>Can deploy ADFS proxy on existing web servers |
| 1000-15000 | 2 dedicated federation servers<br>2 dedicated proxy servers |
| 15,000-60,000 | 3-5 dedicated federation servers<br>2 dedicated proxy servers |

I have come across this http://www.microsoft.com/download/en/confirmation.aspx?id=2278 calculator to calculate how many ADFS servers are required. However, I didn't find this very useful. According to the calculations as you can see below, a single ADFS server can service 50,000 internal users and 50,000 external users authenticating to 3 external applications and 1 internal application. I wouldn't trust these calculations and would stick to the previous table



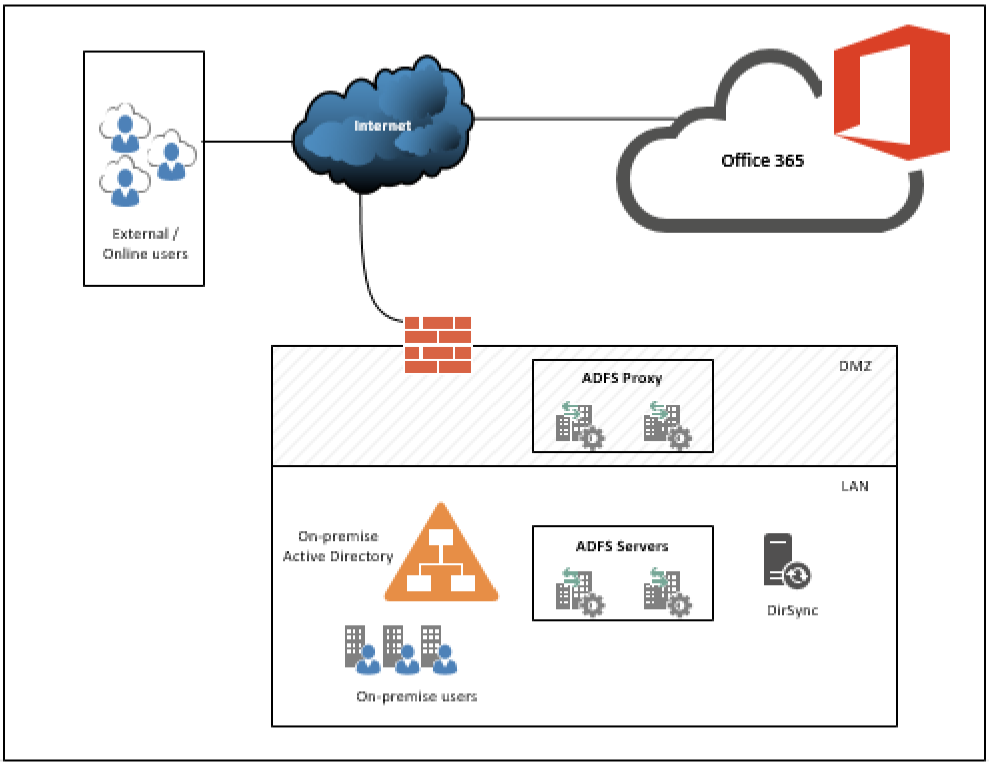
| 1. Estimate peak load on system: | | | |
|---|---|---|---|
| During the peak system usage period, I expect this percentage of my users to authenticate: | 60% | 0.60 | |
| within the following period of time: | 1 hour | 3600 | |
| **2. Enter information about applications:** | | | |
| Enter estimated number of internal applications (such as SharePoint (2007 or 2010) or claims aware web applications) | 1 | | |
| Enter estimated number of online applications (such as Office 365 Exchange Online, SharePoint Online or Lync Online) | 3 | 4 | |

### 3. Enter user counts by type:

| User type | Number of Users | Number of Federation Servers Recommended | Example Scenario |
|---|---|---|---|
| Internal users (AD users authenticating with Windows integrated authentication) | 50,000 | 0.17 | AD FS will allow my AD users to authenticate to SharePoint (2007 or 2010), custom (WIF based) web applications, or Office 365 |
| External users (AD users from your organization authenticating with username and password through a proxy hosted in a DMZ or perimeter network) | 50,000 | | |
| with home realm discovery? (y/n) | y | 0.52 | |
| Users from partner organizations (accessing federated applications hosted by your organization) | 0 | | AD FS will allow my partners to authenticate to SharePoint (2007 or 2010) or custom (WIF based) web applications hosted by my organization. |
| with home realm discovery? (y/n) | y | 0.00 | |
| Users from a SAML 2.0 identity provider<br>-or-<br>Active Directory users authenticating to a SAML 2.0 relying party | 0 | 0.00 | AD FS will provide interoperability with a federation product or application that uses the SAML 2.0 protocol |
| **Total number of federation servers recommended:** | | 0.87 | |

## 4. Publishing ADFS Externally

ADFS can be published externally using an ADFS proxy as illustrated in this diagram



The process is documented very well in the links provided earlier in this blog.

**Configuring an Exchange 2013 Hybrid Deployment and Migrating to Office 365 (Exchange Online)**

http://www.msexchange.org/articles-tutorials/office-365/exchange-online/configuring-exchange-2013-hybrid-deployment-migrating-office-365-exchange-online-part1.html

**How To Install ADFS 2012 R2 For Office 365**

http://blogs.technet.com/b/rmilne/archive/2014/04/28/how-to-install-adfs-2012-r2-for-office-365.aspx

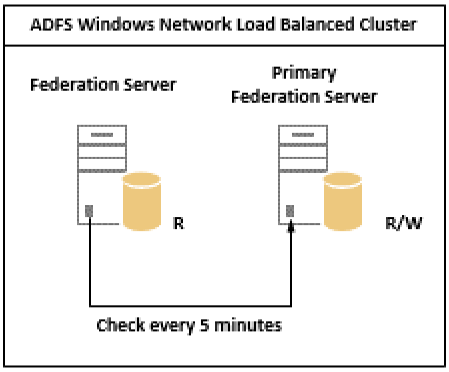
However, the name ADFS Proxy suggests that it is an ADFS role that is performing the proxy. Prior to Windows 2012 R2 it was. However, with Windows 2012 R2 the ADFS Proxy role has been removed and we now use the Web Application Proxy (WAP). The reason I mention this is that the WAP service can provide reverse proxy functionality for other applications such as Skype for Business and Exchange as described here

**Setting up Windows Application Proxy for Exchange 2013**

http://blogs.technet.com/b/jrosen/archive/2013/12/28/setting-up-windows-application-proxy-for-exchange-2013.aspx

## 5. High Availability

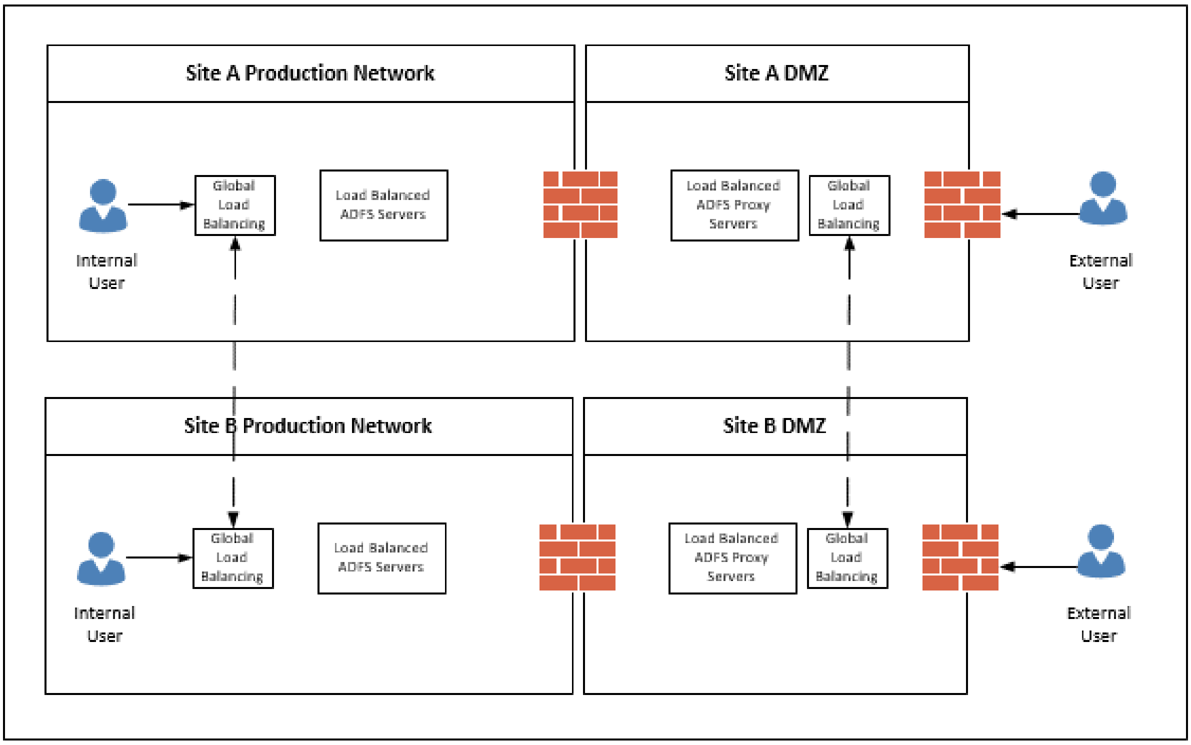
High availability for ADFS can be achieved by deploying two or more federation servers in a farm, and load balancing using Windows Network Load balancing (WNLB). Changes to the ADFS configuration database (WID) are replicated automatically every 5 mins to every server in the farm. The primary server holds a read / write copy of the WID database while the other federation servers in the farm hold a read only copy


ADFS Windows Network Load Balanced Cluster
Federation Server
Primary Federation Server
R
R/W
Check every 5 minutes

The process is described in detail here http://www.msexchange.org/articles-tutorials/office-365/exchange-online/configuring-exchange-2013-hybrid-deployment-migrating-office-365-exchange-online-part3.html

The ADFS Proxy can also be made highly available using Windows Network Load balancing (WNLB) in the same way.

It is possible, and supported, to deploy an ADFS farm across two sites in an Active / Active configuration as illustrated in the following diagram:

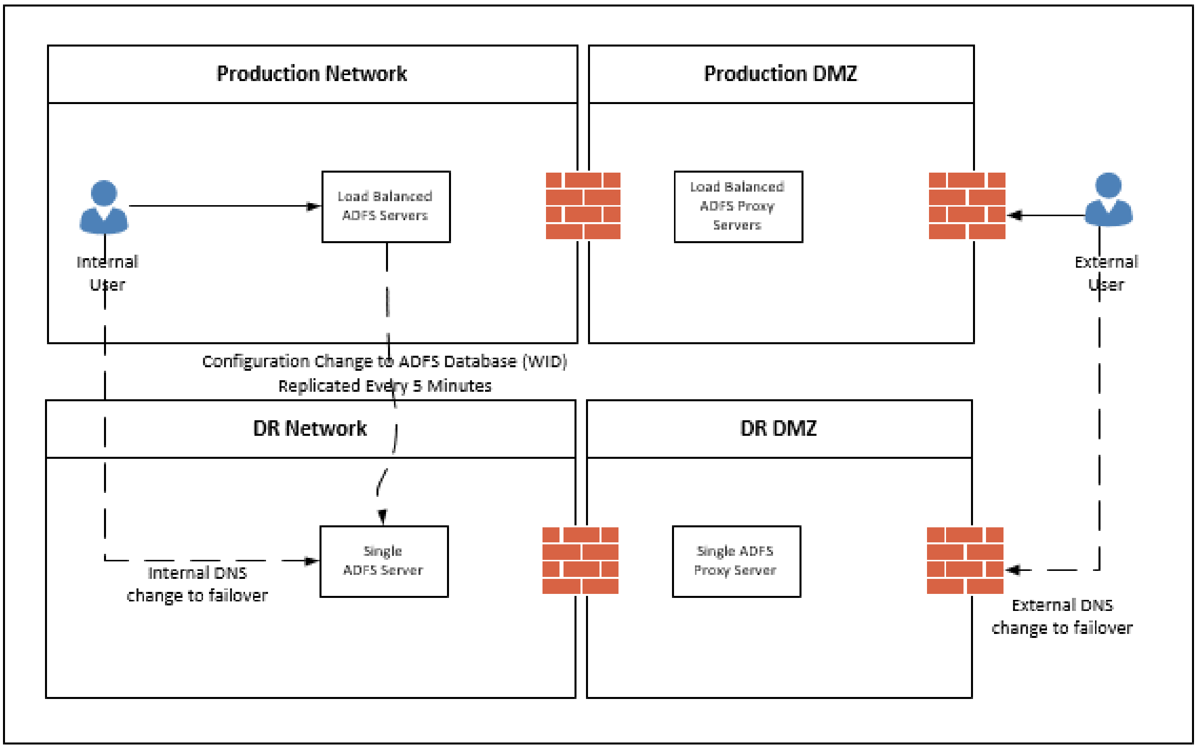

Site A Production Network
Internal User
Global Load Balancing
Load Balanced ADFS Servers
Site A DMZ
Load Balanced ADFS Proxy Servers
Global Load Balancing
External User
Site B Production Network
Internal User
Global Load Balancing
Load Balanced ADFS Servers
Site B DMZ
Load Balanced ADFS Proxy Servers
Global Load Balancing
External User

Load balancers with Global Load Balancing Service (GLBS) capability would need to be deployed in both sites internally. Also, externally, a GLBS service would be required (e.g. http://www.cloudfloordns.com/) @cloudfloordns

This link describes this scenario and also the implications / considerations if deploying ADFS components in Azure https://technet.microsoft.com/en-US/library/dn509536.aspx

## 6. Disaster Recovery

A DR solution for ADFS could include deploying an additional ADFS server, and ADFS proxy server in a second datacentre.  The following diagram illustrates the solution


Production Network
Production DMZ
Internal User
Load Balanced ADFS Servers
Load Balanced ADFS Proxy Servers
External User
Configuration Change to ADFS Database (WID) Replicated Every 5 Minutes
DR Network
DR DMZ
Single ADFS Server
Single ADFS Proxy Server
Internal DNS change to failover
External DNS change to failover

The built-in ADFS farm replication will ensure the ADFS configuration is replicated between all servers in the farm every 5 minutes by default. (assuming there is network connectivity between the datacentres)

This process to failover is described here https://community.office365.com/en-us/f/613/t/44639.

It's a straightforward process that involves the following steps

1. Point the internal and external DNS names for ADFS to the DR server
2. Convert the DR ADFS server to the primary server

## 7. ADFS Configuration Database – Windows Internal Database (WID) or SQL?

Another consideration is which database option to choose.  For most AD FS deployments, Microsoft recommends the Federation Server Farm with WID and Proxies deployment topology as the default choice.  This has been the case in all the deployments I have completed.

Yes, WID is limited to only 5 servers in the farm, but this has been more than enough for any deployments I have been looking as. As per

https://msdn.microsoft.com/en-us/library/azure/dn151324.aspx

we can see that each ADFS server can support 15,000 users. So 3 ADFS in production, and 2 in DR, can provide HA in production (1 server failure) and DR for 30,000 users. So far this has covered all the ADFS deployments I have done.

There are two main reason that I can think of as to why you would add the complexity, overhead and computing resources required for SQL clustering or mirroring to an ADFS design:

1. Providing HA & DR for more than 30,000 users (i.e. can have more than 5 ADFS servers)
2. Geographic load balancing (Active / Active across two datacentres), where network limitations prevent replication between the primary and secondary farm servers. SQL allows merged replication, and targeting of the nearest SQL node which lowers latencies and improves the overall experience

A comparison of WID vs SQL can be found here.

http://blogs.technet.com/b/ucando365talks/archive/2014/04/15/adfs-high-availability-quick-reference-guide-for-administrators-implement-single-sign-on-for-office-365.aspx#.Vd3YrflViko

And Yes, it is possible to migrate from WID to SQL as described here

http://social.technet.microsoft.com/wiki/contents/articles/948.ad-fs-2-0-migrate-your-ad-fs-configuration-database-to-sql-server.aspx

## 8. Conditional Access

Another benefit to deploying ADFS is that we can use it to control access to Office 365 services. ADFS includes the following 4 client access policies:

| Scenario | Description |
|---|---|
| Block all external access to Office 365 | Office 365 access is allowed from all clients on the internal corporate network, but requests from external clients are denied based on the IP address of the external client. |
| Block all external access to Office 365 except Exchange ActiveSync | Office 365 access is allowed from all clients on the internal corporate network, as well as from any external client devices, such as smart phones, that make use of Exchange ActiveSync. All other external clients, such as those using Outlook, are blocked |
| Block all external access to Office 365 except browser-based applications | Blocks external access to Office 365, except for passive (browser-based) applications such as Outlook Web Access or SharePoint Online |
| Block all external access to Office 365 except for designated Active Directory groups | This scenario is used for testing and validating client access policy deployment. It blocks external access to Office 365 only for members of one or more Active Directory group. It can also be used to provide external access only to members of a group. |

Full details of these policies and how to configure them can be found here:

**Configuring Client Access Policies**

https://technet.microsoft.com/en-us/library/dn592182.aspx

## 9. Migrate ADFS from one server / farm to another

I have come across the scenario whereby my customer has an existing ADFS deployment with no HA or DR, but required both.

In this scenario I will build out a new ADFS HA & DR solution, and will not try to retro fit HA into a live ADFS deployment. The reasons for this are:

1. I would have to make changes to the ADFS live environment during the deployment
2. I would have to take the live ADFS offline to test HA and DR.

If I build a new ADFS in parallel, I can export the configuration and settings from the existing ADFS and fully test before going live. The go live is a simple DNS change (both internal and external) to point the ADFS namespace e.g. sts.domain.local at the new ADFS infrastructure.

The following links describe the migration process:

1. Prepare to Migrate the AD FS 2.0 Federation Server - http://technet.microsoft.com/en-us/library/jj648429.aspx
2. Prepare to Migrate the AD FS 2.0 Federation Server Proxy - http://technet.microsoft.com/en-us/library/jj648427.aspx
3. Migrate the AD FS 2.0 Federation Server - http://technet.microsoft.com/en-us/library/jj648428.aspx
4. Migrate the AD FS 2.0 Federation Server Proxy - http://technet.microsoft.com/en-us/library/jj648424.aspx

## 10. Switching Office 365 Identity Model from Cloud Only to Federated (ADFS)

Another scenario you might come across (as I did) is an organization who has deployed Office 365 with cloud only identities, but now want to switch to a Federated Identity model (ADFS).

As described in this blog by the Office 365 team, https://blogs.office.com/2014/05/13/choosing-a-sign-in-model-for-office-365/ Office 365 has 3 identity models:

1. **Cloud Identity:** Accounts are created and managed in Office 365 and stored in Azure Active Directory. There is no connection to the on premise active directory
2. **Synchronized Identity:** The on premise accounts and password hashes are synchronized to Office 365. Authentication takes place in the Azure Active Directory

3. **Federated Identity:** The on premise accounts are synchronized to Office 365. Authentication takes place in the on premise Active Directory using ADFS

It is possible to migrate from Cloud Identity to Federated Identity. However, it is a two stage process:

1. Stage 1: Cloud to Synchronize
   a. The on premise directory is synchronized with Office 365 and the accounts “merged” with the cloud identities
2. Stage 2: Synchronized to Federated
   a. The domain is converted to a federated domain

## 11. ADFS Backup

A backup (copy) of the following are needed in order to restore / recover the ADFS infrastructure:

1. Details of the ADFS Service Account
2. An export of the SSL certificate including the private key
3. An export of the ADFS configuration

The process to collect this data is described in detail in the Prepare to Migrate a WID Farm > Export Service Settings section of the following:

**Prepare to Migrate the AD FS 2.0 Federation Server**

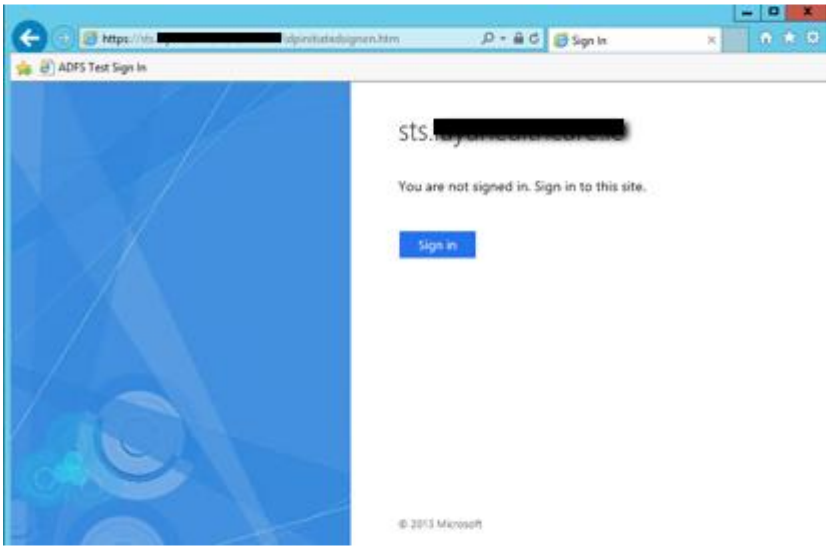
https://technet.microsoft.com/en-us/library/jj648429.aspx

## 12. Troubleshooting ADFS

You can verify if ADFS is working by browsing to the following address (both internally and externally)

[https://sts.domain.com/adfs/ls/IdpInitiatedSignon.aspx](https://sts.domain.com/adfs/ls/IdpInitiatedSignon.aspx)

(Replace the ***sts.domain.com*** with the name space for your own ADFS)



https://sts.[redacted]idpinitiatedsignon.htm

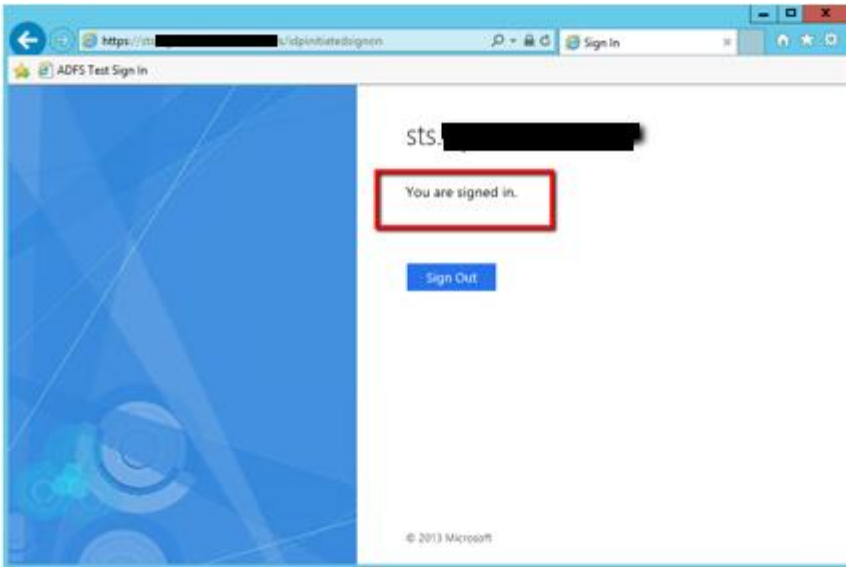
sts.[redacted]

You are not signed in. Sign in to this site.

© 2013 Microsoft

Click “Sign in”

If you are prompted for credentials, enter your UPN login and password



https://sts[redacted]s/idpinitiatedsignon

Sign In

ADFS Test Sign In

sts.[redacted]

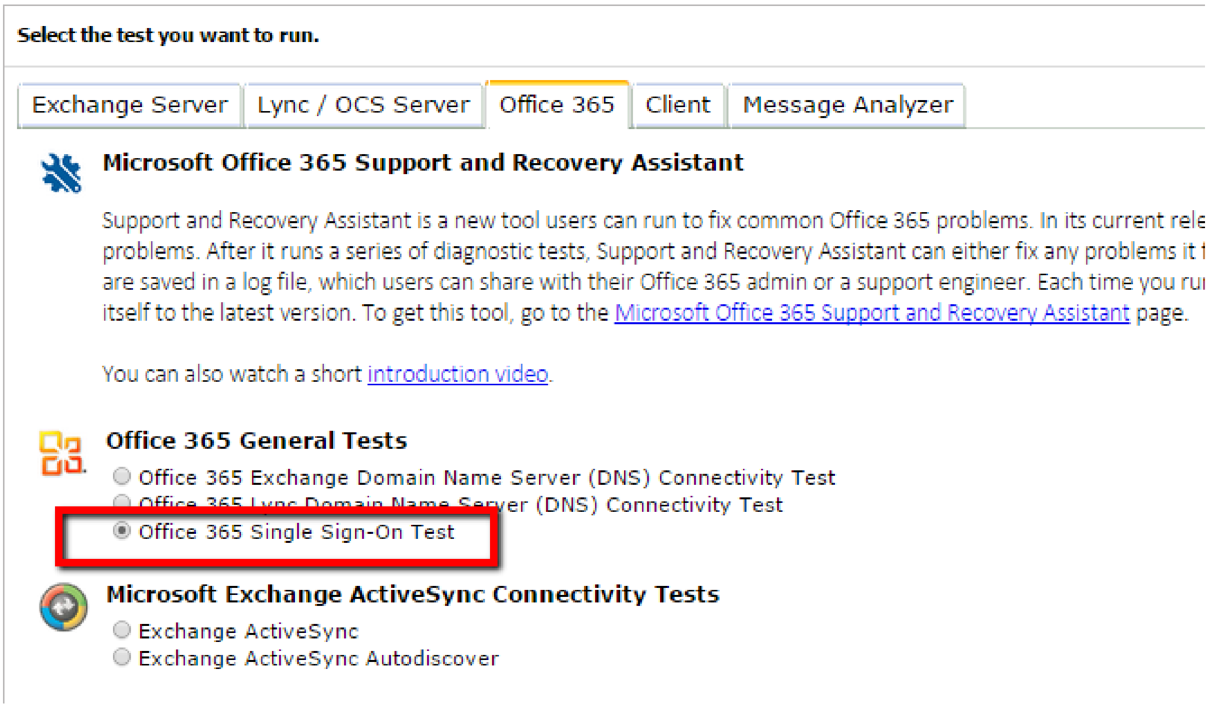
You are signed in.

Sign Out

© 2013 Microsoft

Confirm you are signed in. If this is not working, then you can use the following troubleshooting resources:

1. Run the Microsoft ADFS Connectivity Analyzer Tool from here
2. https://www.testexchangeconnectivity.com/



**Select the test you want to run.**

**Microsoft Office 365 Support and Recovery Assistant**

Support and Recovery Assistant is a new tool users can run to fix common Office 365 problems. In its current rele problems. After it runs a series of diagnostic tests, Support and Recovery Assistant can either fix any problems it f are saved in a log file, which users can share with their Office 365 admin or a support engineer. Each time you rui itself to the latest version. To get this tool, go to the Microsoft Office 365 Support and Recovery Assistant page.

You can also watch a short introduction video.

**Office 365 General Tests**

○ Office 365 Exchange Domain Name Server (DNS) Connectivity Test
○ Office 365 Lync Domain Name Server (DNS) Connectivity Test
● Office 365 Single Sign-On Test

**Microsoft Exchange ActiveSync Connectivity Tests**

○ Exchange ActiveSync
○ Exchange ActiveSync Autodiscover

3. Premier Field Engineering (PFE) ADFS Deep Dive: Troubleshooting
http://blogs.technet.com/b/askpfeplat/archive/2015/06/15/adfs-deep-dive-troubleshooting.aspx

## 13. What if ADFS can't be recovered?

There is one other recovery mechanism that I have come across in the event that the ADFS infrastructure is unavailable or can't be recovered. And that is to disable federation of your domain. This will effectively change your Office 365 authentication mechanism from Single Sign On (Federated) to Same Sign On (Synchronized). The Office 365 request will authenticate against the synchronized account in Office 365 Directory, and not against the on-premise account. Note: One small (and important) requirement – password synchronization is enabled with ADDSync (DirSync)

This scenario and the procedure is described by Exchange MVP Gary Steere @GS_MCM on his blog here

**Disable Federation to Office 365 When ADFS is Down**

http://ithinkthereforeiehlo.com/disable-federation-to-office-365-when-adfs-is-down/#.VZuu9_lViko

**Note:** This is a different process from the Technet description of disabling federation using the Convert-MsolDomainToStandard command because this requires ADFS to be available

To disable federation:

1. Click the Microsoft Azure Active Directory Module for Windows PowerShell shortcut to open a Windows PowerShell workspace that has the cmdlets
2. Run the following commands to connect PowerShell to Azure Active Directory
   - **$msolcred = get-credential**
   - **connect-msolservice -credential $msolcred**
3. Run the following command:
   - **Set-MsolDomainAuthentication -DomainName mydomain.com –Authentication Managed**

Tip: Always enable password synchronization with DirSync, even if you going to use ADFS for authentication

As always, I welcome constructive comments and feedback