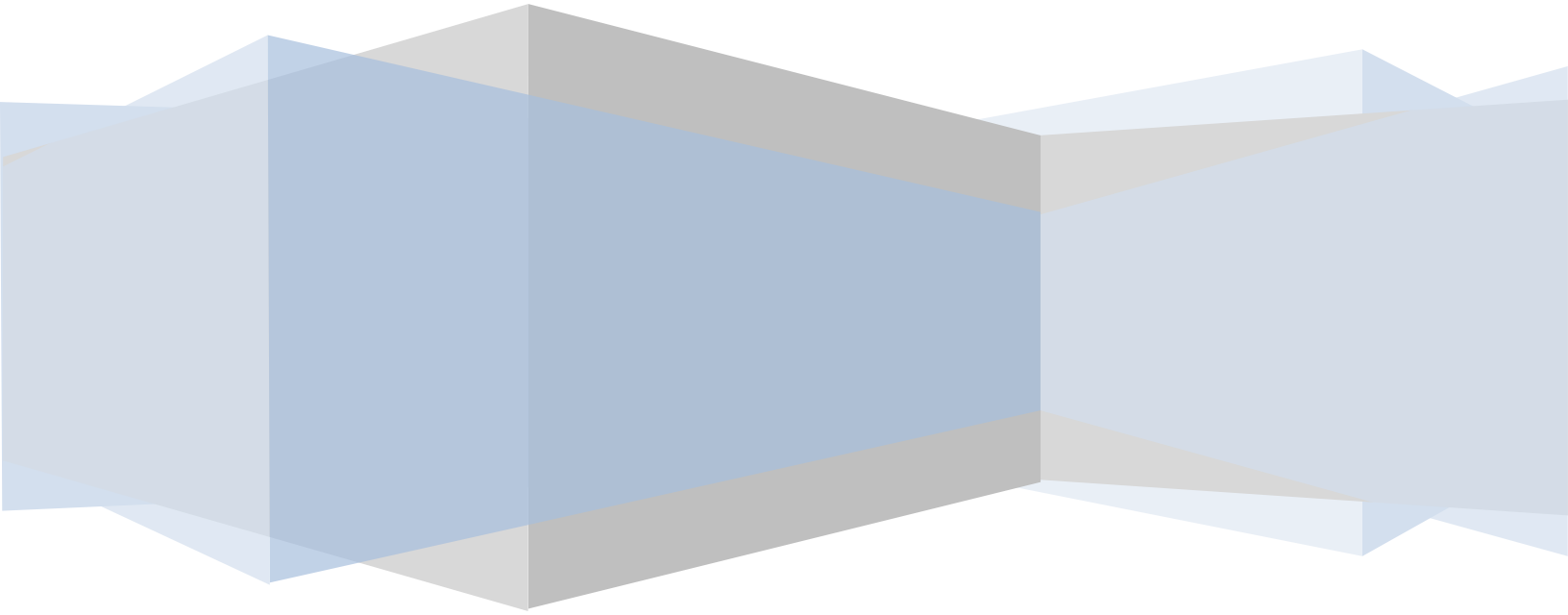
www.TheCloudMouth.com

Integrating Active Directory Federation Services (ADFS) with Office 365 through IaaS

A White Paper

Loryan Strant – Office 365 MVP



Introduction

This purpose of this whitepaper is to explain the value proposition of implementing Active Directory Federation Services for cloud solutions such as Office 365, and why this particular function / workload would be better placed in a solution such as Infrastructure as a Service (IaaS) instead of on-premises.

More recently, businesses are realising that user identifications and passwords are no longer enough to safeguard data. In effect, companies are implementing stronger and more sophisticated authentication systems to make sure that their assets are secure from unauthorised accesses. However, the demand for more security brings a toll on user experience. Multiple user names and passwords need to be remembered and entered- hence causing a dent on productivity.

Single Sign-On (SSO) is a solution which allows users to log-in once and be granted access to multiple systems within a company's network. For example, users will no longer be prompted to log-in multiple times to the company's Active Directory, Office 365, CRM (Customer Relationship Management) platform, HRM (Human Resource Management) platform and any other line of business applications.

Despite the convenience that SSO brings, only a few companies adopt it due to its accompanying costs. Most businesses believe that implementing a SSO is an expensive endeavour – as there is a need to implement an identity management solution on-premises such as Active Directory Federation Services (ADFS). However these concerns can be a thing of the past as organisations can utilise solutions such as Infrastructure as a Service (IaaS) an experience the benefits of SSO through ADFS together with other cloud-based productivity applications like Office 365.

How does Active Directory Federation Services Work?

Microsoft's ADFS integrates with Windows Servers giving users SSO access to multiple systems and applications utilised by the business. ADFS provides a greater level of protection to applications over the Internet by using claims-based authentication. Claims-based authentication works by verifying the user from a collection of "claims" about their identity from a trusted token. ADFS then works by giving users a single prompt to sign-on, allowing access to multiple systems and

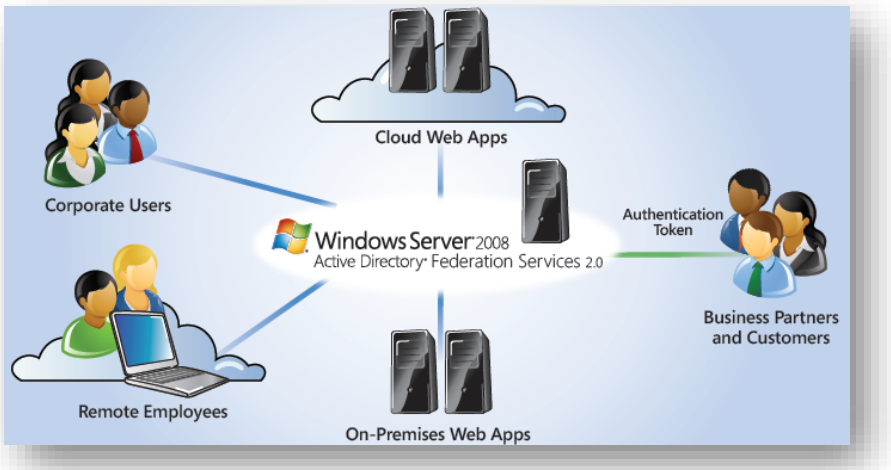


Figure 1: How Active Directory Federation Services Works

applications even if they are located across different networks.

ADFS is beneficial if companies wanted to integrate with partners, vendors and other stakeholders located in different networks, even locations. The Resource organisation component of ADFS allows businesses to own and manage resources that can be retrieved from the web. In this case, ADFS servers and ADFS-enabled web servers (proxies) are deployed to facilitate management access across multiple networks. This facet is also beneficial for third parties or partners that needed access to company networks and resources. The Account organisation aspect of ADFS on the other hand allows organisations to create and manage user accounts by implementing the ADFS server role which is required for local user authentication.

Using ADFS on Office 365

Using ADFS for Office 365 allows business to implement a SSO mechanism that allows access to both on-premises and cloud applications with a single login. With ADFS, organisations no longer have to maintain multiple sets of user names and passwords, as well as improving security for cloud implementations as it gives administrators a greater level of control such as password policies, desktop restrictions, lock-outs and the likes without necessarily replicating the on-premises set-up to Office 365. ADFS also improves access control to Office 365 as administrators can set it to be accessed internally, online or both.

With the use of ADFS to Office 365, organisations can choose to use strong authentication and in general improve security as there is a single control for user credentials across all services. The figure below shows how on-premises Active Directory with ADFS communicates with Office 365 in the cloud.

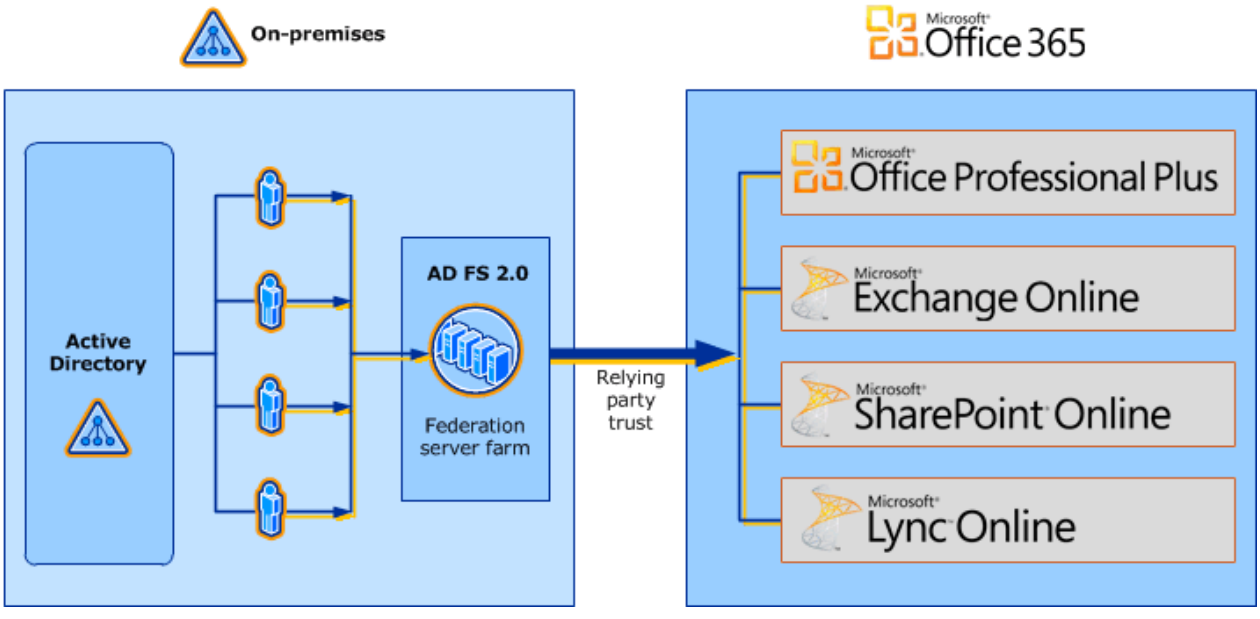


Figure 2: How ADFS Integrates with Office 365

Setting up ADFS creates a "relying party trust" between ADFS and Office 365. This connection between the on-premises Active Directory and Office 365 is made secure by ADFS through authentication tokens, by which a successful authenticate will allow the user to access services from Office 365.

In order to implement ADFS for an organisations on-premises and cloud environments, there is a need to have ADFS deployed on-premises. While organisations can get away with the bare minimum of server requirements for ADFS (eg. 3 servers in total: member server for directory synchronisation, ADFS server, ADFS proxy) it is highly recommended that a total of 5 servers be utilised in a high availability model.

This may require organisations to purchase additional server licences, certificates, firewalls, and configure the environment – a very expensive and technically challenging task especially for organisations that do not have IT as their core business. This also can work against the basic reason organisations choose to utilise Office 365 – to cut down on the amount of servers they are responsible for.

However by utilising cloud-based services such as IaaS, organisations can easily implement the ADFS workload and its associated components in the cloud – ultimately keeping costs constrained on a financial and technical level.

Why Use IaaS for ADFS Implementation for Office 365

IaaS as a cloud-service is founded on the principles of economies of scale – this means that since the organisation is renting-out a virtual space from their IaaS supplier's enterprise-grade servers, the costs associated in deploying ADFS are dramatically reduced. With IaaS, there is no longer a need to purchase expensive hardware, purchase software licenses, or continually maintaining and monitor the server's health. With the Microsoft Server and Cloud Platform, organisations can choose from different models of deployment: private or public cloud.

Private Cloud	**Public Cloud**
In a private cloud environment, resources and configurations are controlled by the organisation. Businesses prefer private cloud to host more mature applications, cater to relatively higher performance requirements, comply with various government regulations and other business requirements**.**	The public cloud is based on a "pay as you go" model wherein cost is dependent on the resources that the organisation consumes. In addition, public cloud is fast to switch to a production environment and allows customers to scale easily.
Hosted Private Cloud A combination of service control, direction on architectural design together with the benefits of datacenter outsourcing. The hosted private cloud gives businesses flexibility yet at the same times the benefits of maintaining a hosted system or application.	**Shared Public Cloud** The fastest to implement, the easiest to scale and lowest cost to avail - that's how shared public cloud works. In this style of cloud organisations share a physical infrastructure with other companies; yet in a very secured and enterprise-level multi-tenant service. The supplier manages the architecture, customisation and security aspects as well.
	Dedicated Public Cloud Some organisations may require a customised

	environment and require more security and robust performance, in which case a dedicated public cloud option is selected. Its functionality is more like the Shared Public Cloud but with more room for alteration in accordance with organisational requirements.

Most IaaS providers offer either fixed price packages or pay-as-you-go models. Hosting ADFS infrastructure in an IaaS environment would not cost more than a few hundred dollars per month – far cheaper than the on-premises alternative.

Key players in the IaaS marketplace are brands such as Amazon Web Services, Rackspace, and lately Windows Azure.

Hosting ADFS infrastructure in the Windows Azure IaaS environment can provide customers with a higher level of access as their environment would be closer to their Office 365 tenant than if they chose to host with an alternative IaaS provider.

What Does ADFS in IaaS Look Like?

There are several different models organisations can take when implementing ADFS in an IaaS environment.

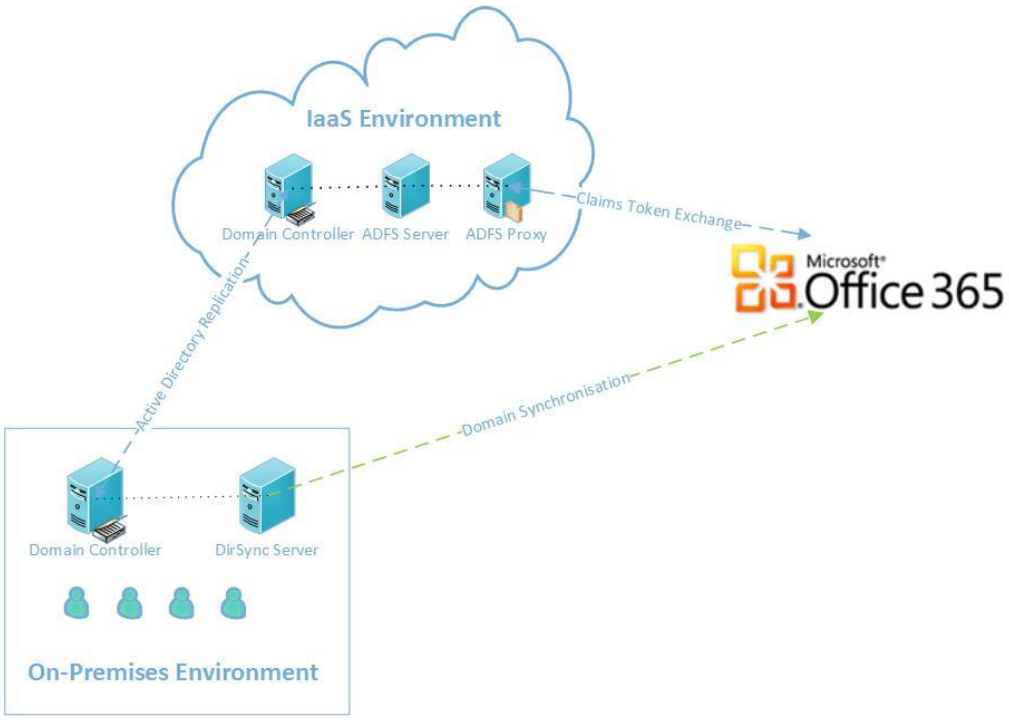


Figure 3: ADFS in IaaS Connected to Office 365

In the above scenario the ADFS components are completely located in the IaaS environment with a local domain controller for faster authentication, as well providing continued access in case of network disruption between the ADFS server and on-premises Active Directory.

At present Microsoft does not support the implementation of Directory Synchronisation in an IaaS environment, due to this only one scenario has been presented above.

Conclusion

With more and more organisations realising the need to have more secure and more sophisticated authentication systems to protect its assets from unauthorised accesses, the SSO capability of ADFS is a solution which allows users to sign-in once and be granted access to multiple systems within a company's network and also to applications in the cloud such as Office 365. Using IaaS to integrate ADFS to both a business' AD and Office 365 can bring a whole lot of benefits such as improved productivity, mobility, security and control. With the right implementation and deployment, ADFS and Office 365 can help businesses achieve greater resilience and performance, while at the same time minimise costs associated with such by taking advantage of cloud computing's economies of scale.