Identity and Access Management in the Cloud Era

Office 365 Leading Adoption

White Paper

An Analysis of the IAM Landscape

Leveraging the cloud to bring cost effectiveness and efficiency to an organisation must always be coupled with advanced security measures. The explosion of mobile devices, fragmented network access and multiple operating systems makes identity management a big challenge. Although there are already a number of Identity and Access Management (IAM) products out in the market today, each has their own limitation that could put one's system at risk. Centrify through its wide range of products is able to provide firms both basic and advanced identity access management solutions making a fully integrated security possible – across all platforms, across all devices and in a unified way. Because Centrify leverages the cloud for its SaaS solution, companies can take advantage of the benefits of the cloud – cost effectiveness and efficiency without heavy upfront costs brought by on-premises implementations while retaining their security posture.

Table of Contents

Introduction

The rapid uptake of cloud and mobile services has brought Identity and Access Management (IAM) to the forefront of solution adoption. Previously employees were not permitted to bring and use their own personal devices due to security risks posed to the corporate network. Now however, companies encourage not only their staff but also their customers to use their own devices (commonly referred to as BYOD). In fact, a study done by IDC revealed that about 70% of employees access corporate information through their personal devices. It is estimated that by 2015 approximately 15 billion smart phones, notebooks and tablets will be accessing corporate networks. With the proliferation of smart phones and the diversity of cloud applications that are accessed by people through highly fragmented connections and environments, new challenges for identity management arise.

Cloud applications have paved the way for an explosion in data growth. With partners and external organisations connecting to corporate applications and services, not only identity data but also business processes and analytics are being consumed and processed - control to access these services and data must be maintained. IAM's role becomes vital due to the increasing counts of identity that require connection to huge sets of heterogeneous information and systems. An account secured by passwords and group memberships is simply no longer enough.

Office 365 Leading SaaS Adoption

While SaaS is not a new concept, and has in fact been commonly available for over a decade – solutions like Office 365 lead the mass market adoption of more and more SaaS solutions.

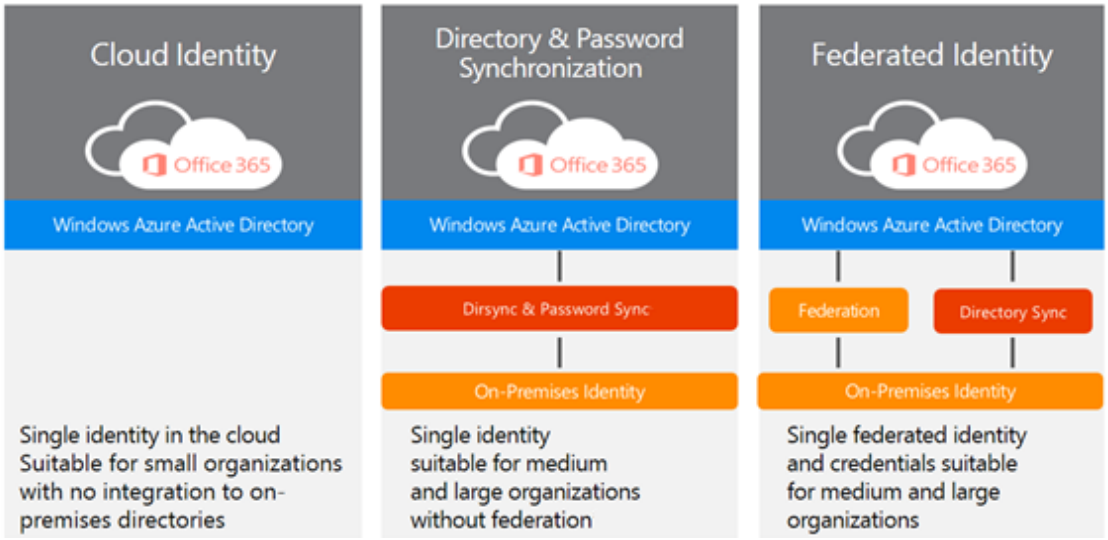
In recent years the IT landscape has filled with many "as a Service" solutions with SaaS being the most prevalent due to its corporate appeal by moving entire workloads to the cloud.

As more and more organisations take up solutions like Office 365 – the next logical step is to look at what other cloud-based solutions can be utilised to allow the organisation to focus on its core operations. While this is not always the case (eg. an organisation may have had Salesforce.com well before they moved to Office 365), it can certainly be seen that Office 365 leads adoption of SaaS applications within most organisations that subscribe to its services. After migrating to Office 365 CIOs commonly ask the question "what else can we do in the cloud?" much to the chagrin of the IT staff.

The problem with the Office 365 first approach is that organisations will predominantly look at what Microsoft requires by way of identity management and control, instead of a holistic journey-based approach to see where *else* the organisation will implement cloud solutions.

Identity Options for Office 365

For customers choosing to make the journey to Office 365 there are only 3 off-the-shelf choices available for managing identities in the underlying Windows Azure Active Directory (WAAD) environment:



Cloud Identity

The cloud identity scenario is generally suitable for small businesses that either do not have an on-premises Active Directory in place, or are in the process of decommissioning it as they move to utilise more services from the cloud.

The issue in this scenario is that identities must now be managed in Office 365 separately to any other cloud-based application that is utilised. In addition, these other 3rd party applications similarly require identity management which adds further stress to the IT department (especially in the case of adds/moves/changes). This thus ultimately becomes both a security and an operational efficiency concern.

Directory & Password Synchronization

With the recent addition of built-in password synchronisation as part of the Directory Synchronisation tool (DirSync), more customers are choosing this approach due to its simplicity. The cloud-based object is effectively a copy of the on-premises mastered object in Active Directory and as such any controls and security restrictions must be applied on the cloud object. While DirSync with password sync is an effective approach to creating & deleting users in Office 365 – it still faces the same limitation as with the previous Cloud Identity approach.

Federated Identity

Implementing federation between an on-premises Active Directory and Office 365 provides a more seamless and controlled method of managing user identities. Building on the strength of user creation by the DirSync application, a federated identity leverages the on-premises Active Directory to determine the relevant level of access and control. Many organisations do not have any form of federation services set up, and as such implementing Active Directory Federation Services (AD FS) is a one-time effort purely for the purpose of managing Office 365 identities.

The Identity Challenge of Office 365 Deployments

For many organisations Office 365 is generally their first foray into large deployments of cloud-based applications. While they may already utilise some cloud-based systems such as Salesforce and WebEx – these are generally in small clusters of users or departments. Office 365 presents a challenge in that it affects every single user in the organisation.

The largest roadblock in Office 365 deployments is the consideration of and implementation of the identity management solution. Most organisations have lived relatively insular lives as far as identity – in that Active Directory provides all the management and controls required for all Line of Business applications and internal systems.

With the deployment of Office 365 these same organisations must now look at how they can extend their Active Directory to the cloud and connect it with Office 365 by way of WAAD. The key issues brought by this approach are:

- Short-sighted focus only on Office 365
- Reaction to a deployment roadblock
- No roadmap for future cloud service adoption
- Insufficient controls and management options available

The net result is that once organisations have made their decisions on how to proceed with their Office 365 identity management, they are left with exactly that – an identity management solution purely for the purposes of Office 365.

It is actually at this point that organisations should potentially pause longer and evaluate their long term cloud plans and how they will be able to manage identities moving forward.

Traditional Approaches in Cloud Identity Management

Due to the increase in access diversity and information consumption, traditional approaches in cloud identity management such as user names and passwords no longer suffice. Typically, this type of authentication works as a form of knowledge-based proofing of something that only the user knows (i.e. user name and password). However the security strength of this authentication is often low - as in this approach credentials may be stored as clear text or a hash within each application's database. Users are only authenticated separately to these disparate identity stores with varying (or unknown) degrees of security.

A more sophisticated approach for user name and password management can come in the form of password management systems which provide the guise of single sign-on (SSO) and can also facilitate more advanced user name and password authentication to Windows applications, cloud applications and web platforms. Through their SSO-like architecture, software vendors such as Citrix were able to provide central password management system which can lessen the risks associated to end-security lapses and external attacks. It also allows organisations to centralise application access and termination through manipulating the primary network logon. Unfortunately these types of solutions are too simplistic and rigid – leaving little room to move with modern times and in an increasingly mobile workforce. Employees now expect to access emails and corporate documents through their mobile phones and tablets. Many also use consumer-grade cloud storage applications such as Dropbox, SkyDrive and Google Drive to storing and share documents. Traditional password management solutions failed to cater for this need and are being over taken by more mature methods of managing identity and access.

Modern Approaches in Cloud Identity Management

Active Directory Federation Services are a more advanced platform for Identity Management available for free from Microsoft and built on Windows Server infrastructure. AD FS works by simplifying application access yet making them claims-aware by providing a Security Assertion Markup Language (SAML) token. The SAML contains attributes obtained from Active Directory needed by the application to authenticate. AD FS' single sign-on functionality also enables users to log on once to the corporate network and carry authentication across all services. In this solution an organisation must *federate* its Active Directory to relevant cloud applications in order to allow and control access.

As promising at it seems AD FS has a lot of limitations. Firstly - adopting AD FS doesn't fall in line with the goals of moving applications to the cloud with solutions such as Office 365. While cost cutting is one of the primarily goals of moving to the cloud, adopting AD FS contradicts such financial model by having to purchase and set-up one's own infrastructure. The need to build

federation gateways to connect to cloud applications like Dropbox, Salesforce and Office 365; and deploy certificates to ensure proper interaction of users further adds to the cost. Setting up layers of redundancy to prevent single points of failure also bears hardware/software and licensing costs up front. The more users are in an organisation – the larger the solution has to scale which adds additional servers, licensing, maintenance and support.

For companies with less than 100 users, adopting AD FS is not a viable solution. The budget and effort investment outweigh the benefits of security and as such small to midsize enterprises (SMEs) need to find a more cost efficient alternative. And for large enterprises, any AD FS implementation would also need to take into consideration future (or existing) support for the multitude of other potential cloud applications, some of which may not be trivial to implement with AD FS.

Challenges and Considerations with AD FS

In practice when deploying ADFS, and depending on the size of an organisations environment, the following challenges should be considered:

- The need for additional on-premises infrastructure (with consideration for redundancy, network infrastructure)
- Ongoing support and maintenance for AD FS
- High level of skill to setup, integrate and maintain other non-Microsoft 3rd party applications and portal access for those applications

Cloud Based Identity Management Solution in the Market

Cloud-based solutions such as IAM Cloud's Federate 365 and Microsoft's own Windows Azure Active Directory Services (WAAD) cater to the demand for cloud-based Identity Management solution in the market.

Federate 365

Federate 365 is a cloud application hosted in Windows Azure and primarily works like AD FS without the need for on-premises infrastructure; in effect eliminating the high capital costs associated with hardware and licenses. Because it is hosted on the cloud and built for the purpose - Federate 365 not only works seamlessly with Office 365 but also prevents single point of failure. Being fully hosted on Windows Azure, Federate 365 builds on redundant Internet connections, network infrastructure, federation servers, federation proxy servers and hardware load balancers; without high total cost of ownership. Some limitations worth considering are lack of mobile/BYOD support and lack of support for the myriad of other 3rd party apps. Additionally Federate 365 focuses only on Office 365 at the expense of other applications.

Windows Azure Active Directory

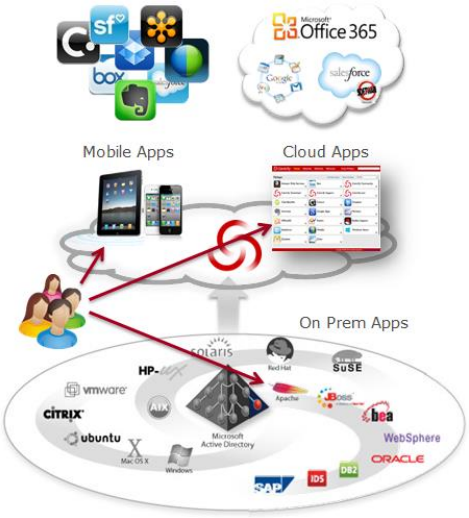
WAAD on the other hand is an Identity Management solution based on a REST-based service enabling identity service across Microsoft cloud products such as Windows Azure, Office 365, Dynamics CRM Online, Windows Intune and some other third party cloud services. Through WAAD, it is possible to integrate a company's existing AD to apply policy controls and authentication across other cloud services. WAAD also makes it possible to add itself to its respective users' Azure subscription, thereby making granting or revoking application access permissions relatively easy.

Limitations of this Approach

These cloud based Identity Management solutions however come with limitations. WAAD for example gives little room for users for configuration. For example, once you add a Directory in WAAD, you cannot delete it unless the request has been escalated to Azure support. WAAD Application Access Enhancements (WAAD AAE) also requires you to replicate your AD to the cloud before you can use it for software as a service (SaaS) applications. There is also no seamless desktop SSO using Integrated Windows Authentication (IWA); as well as no support for mobile and tablet applications on iOS and Android. WAAD AAE also has very limited support for the varying operating systems (i.e. UNIX, Linux and Mac) deployed on-premises and also doesn't support zero sign-on with PAM, Kerberos, NTLM and SDK for applications deployed on-premises.

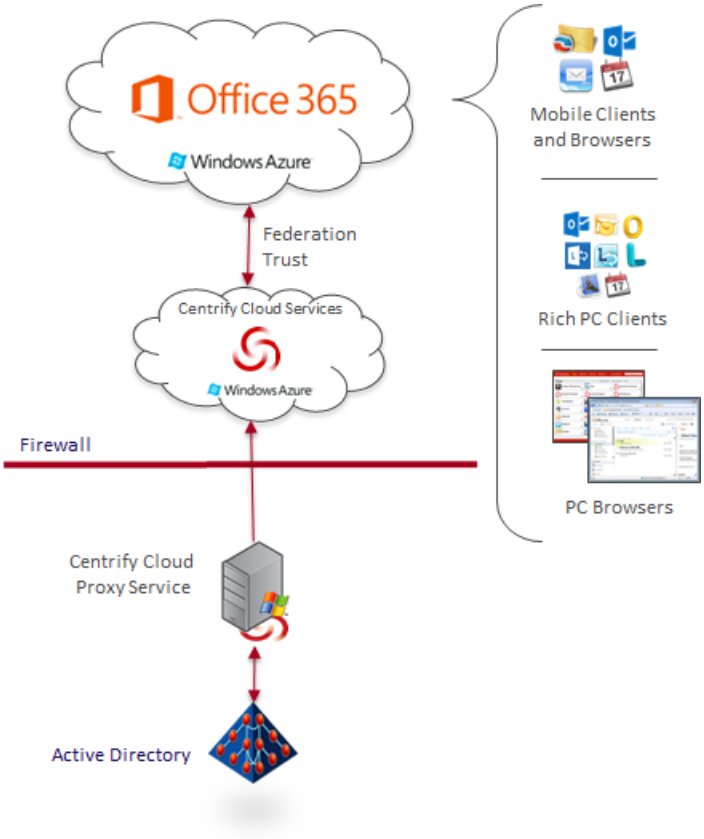
Centrify as a Unified Identity Management Solution for Office 365 & beyond

The best current answer to this cloud identity problem is Centrify as it provides a unified identity service solution that solves the security challenges introduced by cloud services while also bringing operational efficiency to play. Centrify provides organisations with a more streamlined way of leveraging their existing identity infrastructure to centrally manage authentication access, control, privilege management, policy enforcement together with auditing not only for cloud but also on-premises systems. In addition, Centrify also integrated its SSO feature set with, at time of writing, close to one thousand 3rd party applications. A few of the most popular are Office 365, Salesforce.com, Webex, Concur, Postini, Google Apps and Box. It also caters to Apps specific plugins for Apache, JBoss, WebLogic, Websphere, DB2, SAP ABAP and SAP Java.



Its support for Office 365 is unparalleled, due to its ease of solution deployment for federated identities from on-premises Active Directory environments. With Centrify there is no need for servers in the DMZ, inbound firewall holes or public certificates. An additional benefit is the relatively fast time to implement and utilise the solution.

Centrify's core value proposition is to continue to use your existing investment in Active Directory, including processes, tools and helpdesk skillset.



Centrify removes the "hidden costs" associated with moving to the cloud with its SaaS solution by:

- Greatly simplifying the federation process
- Leverage your existing Active Directory assets
- Remove the silos of identity and identity proliferation
- Solve both an efficiency problem and security problem especially around identity governance associated with onboarding/offboarding of employees to cloud based services
- Solving the multiplying phenomena of BYOD at the same time (i.e. most users will also want to use Office 365 or other 3rd party applications on their mobile devices)

Finally, Centrify also extends this beyond cloud to on-premises applications, servers, Macs, iPads and Android devices. Enterprises thus can extend the use of their existing Active Directory infrastructure beyond just that of Microsoft Windows to "anything", be it cloud or otherwise. This provides for clear security and operational benefits that should not be ignored. Want group policy applied to the cloud as well as Macs? You got it.

Centrify is a Gold Certified Microsoft Partner that provides the simplest federated identity solution for the most cloud applications and including mobile support.

Summary

Leveraging the cloud to bring cost effectiveness and efficiency to a company must always be coupled with advanced security measures. The explosion of mobile devices, fragmented network access and multiple operating systems makes identity management a big challenge. Although there are already a number of IAM products out in the market today, each has their own limitation that could put organisation's systems at risk. Centrify through its wide range of identity and access management products is uniquely positioned to provide firms a variety of simple through to advanced identity management solutions – making a fully integrated security management possible across all platforms, across all devices. And because Centrify leverages the cloud as well for its IAM solution, companies can take advantage of the benefits of the cloud – cost effectiveness and efficiency without heavy upfront costs brought by on-premises implementations.