onelogin

WHITEPAPER

CHOOSING THE RIGHT ACTIVE DIRECTORY INTEGRATION FRAMEWORK FOR YOUR CLOUD APPLICATION PORTFOLIO

Brian Desmond
www.briandesmond.com

April 3, 2014

www.onelogin.com • 150 Spear Street, Suite 1400, San Francisco, CA 94015 • 855.426.7227

INTRODUCTION

The problems that IT Professionals face with "the cloud" generally involve extending a multitude of processes outside of the trust boundary of the corporate network. These processes must be extended across the Internet and in to the untrusted datacenters of the companies that provide applications and services. For example, processes such as provisioning and deprovisioning, authentication and authorization, and of course a means to report on access and compliance.

The default choice for many organizations is to begin with an evaluation of Microsoft's solution-set. Microsoft is often the incumbent vendor, competitively priced, and can be extremely aggressive when they decide to enter a market. Microsoft tends to focus on solutions that first address the countless requirements within the confines of the Microsoft ecosystem, while third parties are free to address use cases across multiple platforms and technologies. The goal of this paper is to provide you with a solid understanding of the variables involved in choosing the right directory integration approach for your organization's cloud application portfolio.

IDENTITY MANAGEMENT AND THE CLOUD

In some organizations, establishing efficient, automated identity management for on-premises directories and applications is an ongoing project that involves countless consultants and complex project plans. Extending identity management to the cloud rarely offers the same degree of time and resources.

The prospect of re-engineering and extending identity management to an ever-evolving set of cloud services and applications is a scary prospect. This is further complicated by the relatively real-time nature of cloud projects. That is, cloud applications can be made available instantly without the traditional burdens of IT infrastructure, and they are typically accessible from anywhere.

The cost of traditional identity management approaches do not scale when compared to the monthly costs of cloud applications. Addressing identity management in the cloud needs to be done in a cost effective, efficient, and most importantly, sustainable manner.

Applications

Part of the challenge with cloud-hosted applications is that each application and service provider makes their decisions about how best to integrate the application with their customers. For example, the integration methodologies for two key players – Office 365 and Salesforce – are substantially different. With traditional on-premises applications, IT usually has a large degree of input in how applications are integrated with existing tools and processes. Without this input, each cloud application becomes an independent design and implementation effort that may have little or no similarity to other applications.

This problem has created a marketplace for a new set of solutions from Microsoft and third parties such as OneLogin that aim to abstract the identity management thread of cloud application management.

Office 365

Many organizations have begun their push to the cloud with a small handful of applications. Microsoft's Office 365 offering is the driving force for many, but getting to the point where Office 365 is seamlessly integrated and ready for use is not a small project. The services needed to seamlessly leverage the Office 365 solution set are complex and often expensive to implement. Smaller organizations may find the cost of Office 365 offset by the costs and complexities of Microsoft's native solution to the identity management component of Office 365.

At a minimum, Office 365 will require the deployment of the Microsoft

Azure AD Directory Synchronization appliance. To deliver single sign-on without storing passwords in the cloud, Active Directory Federation Services (AD FS) must also be deployed. Finally, AD FS must be operated in a highly available manner so that the benefits of the Office 365 SLA can be realized by the organization.

Taking this into account, it may be faster, easier, and cheaper for some organizations to address the Office 365 identity management challenge with a third party solution. OneLogin is one example of a third party provider that addresses Office 365 identity management in a manner that may be faster to deploy and/or simply more economical.

Three Authentication Methods

Traditional authentication – validation of user credentials – in an on-premises application is generally accomplished in a few different ways. The first and most common way is by integrating the application with an existing directory such as Active Directory or any number of other LDAP directory servers on the market. Countless applications use the LDAP protocol to achieve this integration and IT organizations are well accustomed to supporting this approach. A less desirable, but still prevalent approach is an isolated user store that is maintained within the confines of the application. This second approach offers rapid deployment, but it trades long- term security and reporting capabilities since fundamental provisioning and deprovisioning tasks must take place directly in the application.

The third approach, which is rapidly gaining popularity, is federated authentication. Federated authentication is the mainstream solution to authentication (but not necessarily authorization) for cloud applications and services. Federation enables IT to securely extend their on-premises directory to the cloud via a set of standardized protocols.

Unlike LDAP authentication to an on-premises directory, managing federated identity systems and platforms is frequently not a skill that

IT organizations have in-house. Furthermore, the skills to design, deploy, and operate identity federation platforms are not yet broadly available in the marketplace. While skillsets such as managing Active Directory Domain Services have been maturing for over a decade, many organizations are just beginning to broadly deploy federated identity.

Authorization

Authorization – controlling who has access to what – is a facet of identity management that is critical to protecting the interests of the business. The problem is that authorization is implemented in disparate ways. On-premises software has the same problem. For example, complex Enterprise Resource Planning (ERP) platforms like PeopleSoft and SAP offer fine grained access control models within the application that administrators can use to control access, while many less complex applications simply rely on a short list of hard-coded roles to manage access. The multiplying factor with cloud applications is twofold. First, there is often no programmatic or database access to the application's security layer, thereby making automation difficult, and secondly, IT has little to no control over upgrades to the cloud application which makes keeping up with the security model a potentially never ending task.

Provisioning and Deprovisioning

Ensuring that users have access to the tools they need on their first day of work is an important responsibility not only for IT, but also across the business. The business cannot afford to have a new employee sitting idle (or one that has changed roles) due to a lack of access. While on-premises applications typically have drawn out deployment initiatives that enable IT to take the time necessary to address the provisioning aspect of the application, the on-demand nature of cloud applications does not always lend itself well to this task.

When a user leaves the organization, or changes roles within the organization, their accounts and access to applications must be removed or modified. When this does not occur in a timely manner, the organization is exposed to the risk of accidental or intentional behaviors that can lead to security breaches, disclosure of sensitive information, or worse. Furthermore, with cloud-hosted applications, licensing is often on a per user basis. This means that untimely deprovisioning can lead to unnecessary charges for inactive users.

There are countless solutions on the marketplace that address the fundamental identity management processes of provisioning and deprovisioning extremely well. The challenge is that while these solutions have broad turnkey coverage for common on-premises directories, databases, and applications, the task of rapidly extending these identity management toolsets to a wide range of cloud applications is not easy.

BRING YOUR OWN DEVICE

Hand in hand with the move to the cloud has been the trend of IT consumerization. The demand for end users to bring their own devices to work – smartphones, tablets, netbooks, etc. – and the desire to work from anywhere adds an additional dimension of complexity to managing identities in the cloud. Some IT Professionals will joke that BYOD stands not for Bring Your Own Device, but instead for Bring Your Own Disaster.

The key dimension that BYOD adds to the cloud identity management discussion is an extension of controlling access to applications and data. Instead of simply addressing who has access, the questions of where the application is being accessed from, and how the application is being accessed must also be considered.

When access to applications and data occurs from outside the boundaries of the corporate network, an additional level of assurance is often necessary. End users can lose phones and tablets that hold stored credentials, which may provide permanent access to applications and services. Adding a second factor of authentication is an important capability.

In addition to security, BYOD elevates expectations around convenience and simplicity. While applications may be readily accessible via portals and shortcuts on the Intranet, this simplicity may not extend to mobile devices. Hunting for application login screens from a mobile device can be a frustrating experience. Identity management platforms that deliver an easy single sign-on experience across mobile devices can help meet the demands of today's increasingly mobile workforce.

MICROSOFT'S SOLUTION

Microsoft has a long history in identity management and they are rapidly evolving their platform and services to offer an identity management solution that enables security in the cloud. Their solution is not limited to enabling organizations to move to Office 365, but, instead, it enables organizations to extend identity to virtually any cloud application or service.

The fundamental component of Microsoft's identity management platform is Active Directory Domain Services (AD DS). Any IT professional who has managed a Windows based network has undoubtedly spent time managing AD DS. Microsoft has evolved this platform to offer federation via Active Directory Federation Services (AD FS) and more recently, Microsoft Azure Active Directory. While all three of these components share a common root to their name – Active Directory, the skills needed to manage each component are vast and in many cases, unrelated.

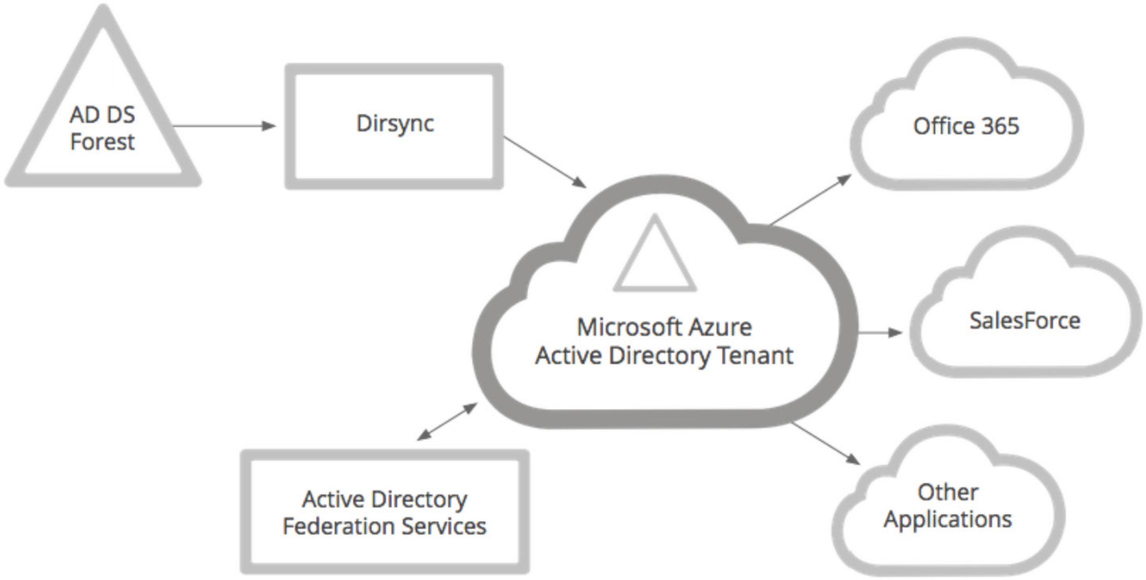

Figure 1 shows the high level Microsoft cloud identity management architecture.

Active Directory Domain Services

Active Directory Domain Services (AD DS) is the cornerstone of the Active Directory brand and a mainstay in practically every IT infrastructure. Organizations have invested over a decade building their AD DS infrastructures as well as perfecting identity management processes that manage the users and groups in the directory. This investment is not going away, and it becomes even more critical as organizations begin harnessing cloud applications and services.

Regardless of the direction an organization takes with regard to cloud identity management, chances are, their Active Directory will remain the source of authority for traditional user and group information, as well as passwords. While Microsoft offers the ability to easily synchronize Active Directory passwords to Microsoft Azure Active Directory, most organizations will probably find the risk of this (even with the additional hashing protections offered) to be too great. Instead, federation technology will be a mandatory component of the overall cloud identity architecture.

Microsoft Azure Active Directory

Microsoft Azure Active Directory is the youngest and perhaps most misunderstood component of Microsoft's cloud identity management solution set. The crux of the confusion lies in the nearly fifteen year history IT Professionals have with AD DS and the basic expectation of feature parity that Microsoft's cloud offerings have typically demonstrated with respect to their on-premises counterparts. Currently, there are wide ranging difference between the Active Directory IT Professionals traditionally think of and the reality of what Azure Active Directory is designed to do.

Simply put, Azure Active Directory is targeted towards managing identities and applications in the cloud. Microsoft's cloud properties (most notably, Office 365) depend on Azure AD to provide identity information. Azure AD can also be leveraged by IT Professionals to enable relationships with third party applications and services (be it a major player such as Salesforce or Box, or any other application that supports federation) as well as with corporate applications.

Azure Active Directory's Access Panel interface can be made available to end users to provide a one-stop shop for all of the cloud applications a user has access to.

Traditional Active Directory tasks that IT Professionals are used to, such as joining machines to a domain and performing desktop management tasks with Group Policy are not available in Azure AD. Azure AD also does not support the LDAP protocol. Instead, it supports a variety of federation protocols (such as SAML and WS-Federation). To integrate a traditional on-premises application with Azure AD, the application must already support federated authentication, or, if only LDAP authentication is supported, the application must be updated to support federation. In addition to using LDAP for authentication, many applications also rely on LDAP to consume information from the directory. With Azure AD, application developers can instead read and write data from an Azure AD tenant through the use of a series of REST based APIs.

Microsoft Azure Active Directory Premium Features

At a minimum, Office 365 will require the deployment of the Microsoft Azure Active Directory Directory Synchronization appliance. To deliver single sign-on without storing passwords in the cloud, Active Directory Federation Services (AD FS) must also be deployed. Finally, AD FS must be operated in a highly available manner so that the benefits of the Office 365 SLA can be realized by the organization.

The complete Azure AD feature set varies depending on whether or not the premium version of Azure AD has been purchased. While many of the basic directory and federation features are available for free in the basic edition, the features that make Azure AD a competitive cloud identity management solution are licensed via the premium edition. The Azure AD premium edition is licensed on a per-user basis and includes all of the premium features for each user.

The premium feature set of Azure Active Directory is focused around four areas:

- **Branding and Customization** – The Azure AD sign-in pages and Access Panel can be branded to resemble the organization's brand and IT's look-and-feel for corporate services and applications. This includes replacing the default Azure AD logos with custom logos.
- **Group Based Access Control** – Groups can be used to control access to applications federated with Azure AD. In addition, users can request to join groups that grant access to applications and group owners can approve requests via the Azure AD Access Panel. Administrators can also delegate end users the ability to create and manage their own groups.
- **Self Service Password Management** – Self-service password recovery for users that have their password stored solely in Azure AD. Users who login via federated authentication (e.g. AD FS) or via

a password synchronized with Azure AD Directory Synchronization cannot take advantage of this feature.

- **Multi-Factor Authentication** – Users can be required to register for and provide a second factor of authentication (SMS (text) message, voice call, or push notification to an app) at login time.
- **Advanced Reporting** – The advanced security reports available in the premium version of Azure AD provide common IT security reports centered on application and device usage and security analytics that detect irregular and suspicious activity.

Prerequisites for Azure Active Directory

Microsoft Azure Active Directory is not a turnkey out of the box solution for the most common scenarios. In order to marry Azure AD with existing identities in an on-premises AD DS forest, organizations must first deploy the Azure AD Directory Synchronization appliance. To leverage single sign-on capabilities whereby user passwords are stored in the on-premises AD DS forest, Active Directory Federation Services (AD FS) must also be configured and deployed.

Azure AD Directory Synchronization is relatively straightforward to deploy. For organizations with less than 50,000 user, group, and contact objects that will be synchronized, the Azure AD Directory Synchronization appliance can be installed using the supplied wizard with minimal input on the part of the administrator. Organizations with larger directories will need to make the full version of Microsoft SQL Server available to host the Azure AD Directory Synchronization database.

Once the Azure AD tenant is populated, organizations can start taking advantage of its capabilities as well as dependent services like Office 365. Office 365 has an additional licensing enablement step that must be performed for each user that needs access to services such as Exchange Online, Lync Online, SharePoint Online, and so forth. This step is not performed by Azure AD Directory Synchronization. Instead, administrators must either manually license users for services or develop a custom scripted solution to automate this step.

Microsoft's turnkey Directory Synchronization appliance runs in to challenges when complex enterprise Active Directory topologies that involve multiple forests come in to play. The Directory Synchronization appliance can only be used in a single forest topology. For many organizations, this is more than sufficient, but, for organizations with multiple forests, the directory synchronization prerequisite to an Office 365 and/or Azure AD deployment can be a significant roadblock. Synchronizing multiple forests with Microsoft's native solution set requires a custom deployment of Forefront Identity Manager 2010 R2 (FIM). Designing and deploying FIM for this purpose generally requires the use of specialized consultants plus the added burden of ongoing maintenance.

While the Azure AD Directory Synchronization appliance can synchronize passwords from the on-premises AD DS forest to Azure AD, most organizations will likely opt to keep passwords out of Azure AD and instead depend on federation for authentication. Organizations with multiple forests will not be able to take advantage of the password synchronization capabilities of Azure AD Directory Synchronization. Federation with Azure AD is the elephant lurking in the back of the room. While deploying Azure AD Directory Synchronization is generally a trivial exercise, establishing and maintaining a highly available AD FS infrastructure is not trivial.

Active Directory Federation Services

Microsoft's identity federation platform, Active Directory Federation Services (AD FS) has evolved substantially since the first version was released in 2011. AD FS 2.0 was a major overhaul, and the current version shipping with Microsoft Server 2012 R2, AD FS 3.0 adds significant functionality. In all cases, complexity is a key concern. The skill-set necessary to manage and configure an AD FS infrastructure is not well aligned with the skill-set of typical AD DS administration. Instead, in addition to typical Microsoft infrastructure administration, AD FS administration generally requires an understanding of federation protocols and a familiarity with web applications at the protocol level.

AD FS is an extremely capable solution that can bridge on-premises identity infrastructure to cloud applications and services. The latest version of AD FS introduces the web application proxy server role that can enable a broader degree of single sign-on by enabling federated access to traditional on-premises applications that use Kerberos authentication. AD FS 3.0 also gives organizations the opportunity to further secure access to applications by requiring multiple factors of authentication either on an application or location basis. AD FS is also a fundamental component of Microsoft's BYOD strategy. In order to take advantage of the Workplace Join features introduced in Microsoft Server 2012 R2, AD FS 3.0 must be in place.

These capabilities come with a potentially significant infrastructure cost. Simply put, the service level agreements (SLAs) that cloud hosted services offer are a moot point if the AD FS infrastructure that brokers logins to these applications and services isn't running at the same service level (or higher).

Prerequisites for Azure Active Directory

Highly available AD FS is primarily predicated on load balancing multiple sets of servers. Figure 2 shows a typical highly available AD FS deployment in a single datacenter. For organizations with advanced requirements, SQL Server may be required, and AD FS will probably be deployed in multiple geographically dispersed datacenters with the addition of a global traffic management solution to manage requests across datacenters.

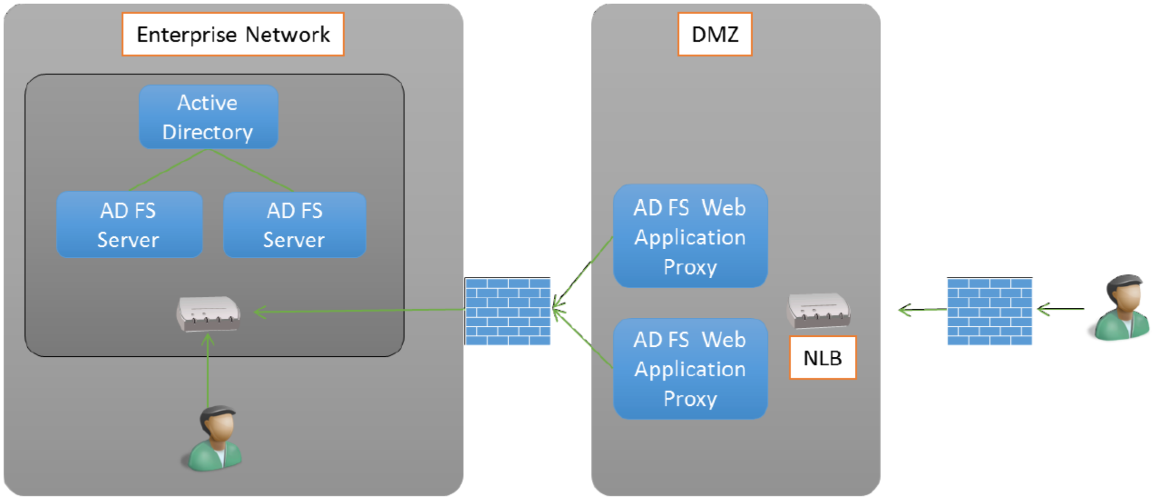

Figure 2 Highly Available Single Datacenter AD FS Reference Architecture

These dependencies add several layers of complexity to AD FS, and require collaboration across multiple teams. For example, in many enterprises, load balancers and global traffic management solutions (e.g. F5 Global Traffic Managers or Cisco Global Site Selectors are generally managed by dedicated networking teams). SQL Server may require support from a database administration team, and the addition of SQL Server clustering will add a dependency on a storage management team as well.

Figure 3 shows one approach to highly available AD FS across multiple datacenters with the addition of SQL Server to take advantage of advanced AD FS features like token replay detection and SAML artifact resolution.

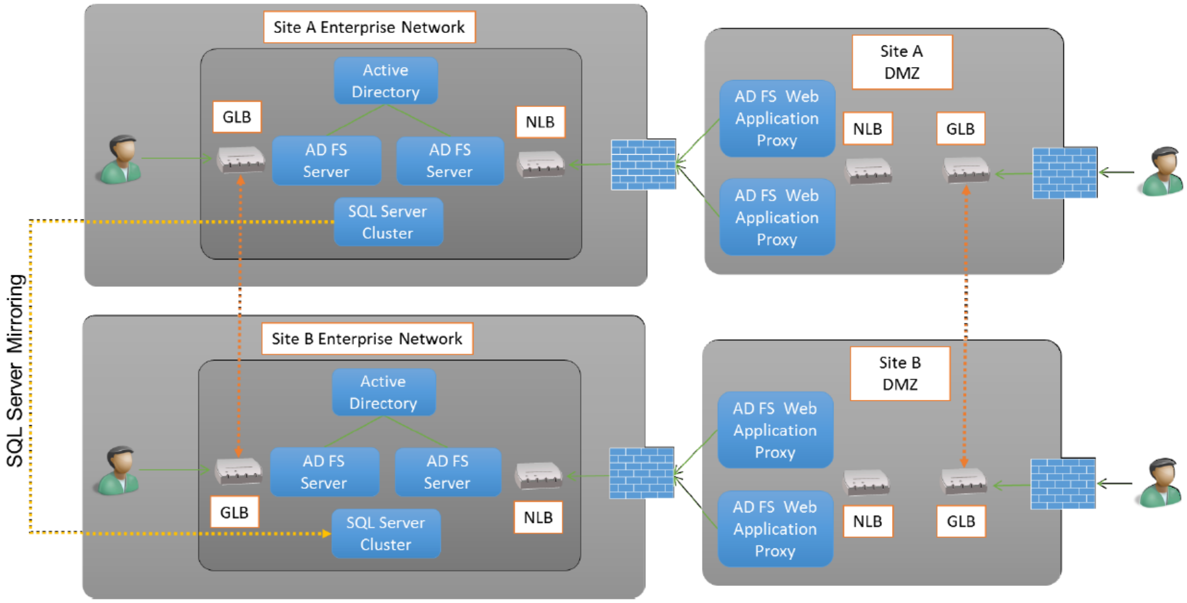

Figure 3 Highly Available Multiple Datacenter AD FS Reference Architecture

Bringing all of these teams together to deliver on a service level is a goal that large enterprises achieve at varying levels, but the coordination and complexity always exists. Smaller organizations that need to deliver the same level of availability that a solution such as the one in Figure 2 shows may not have the same number of teams or individuals involved, but they probably will also not have the same level of technical expertise across all functions available.

CONCLUSION

Microsoft has a rapidly evolving platform for cloud identity management that centers on their Active Directory brand. Taking advantage of this platform requires deploying a highly available Active Directory Federation Services infrastructure (AD FS), and in many cases, populating, maintaining, and federating with Microsoft Azure Active Directory. The cost to deploy and fully take advantage of this platform is often a hidden cost. Microsoft advertises the free edition of Microsoft Azure Active Directory, and the free edition is a very capable platform for federation with cloud applications. The hidden costs often lie with AD FS, the need for the Azure AD Premium edition, and in translating existing identity management processes to function in the age of the cloud. While AD FS shares a brand with Active Directory Domain Services (AD DS), a technology that is widely deployed and understood, the skills AD DS administrators have developed over the course of fifteen years do not translate well to AD FS.

Third party solution providers have recognized these problems and built turnkey solutions that deliver rapid cloud identity management without the overhead and setup complexity of Microsoft's solution. OneLogin is one such example of a third party that integrates with well entrenched components of the identity management stack like AD DS and simultaneously delivers rapid setup and one click access to countless cloud applications.

COMPARING MICROSOFT AZURE ACTIVE DIRECTORY WITH ONELOGIN

The table below highlights the capabilities of the Microsoft platform for integrating with a cloud application portfolio as well as capabilities from OneLogin.

	Microsoft Azure Active Directory	Microsoft Azure Active Directory Premium Edition	OneLogin
Application Support			
Application Catalog	1,021[1]	1,021[1]	3,532[1]
Office 365 Availability	✓	✓	✓
Hybrid Exchange Online	✓	✓	✓
Desktop Applications	✓	✓	✓
Integrate third-party SAML applications	✓	✓	✓
Integrate on-premises SAML applications	✓	✓	✓
Password Vaulting for form-based apps	✓	✓	✓
SAML Toolkits for custom apps			✓
Add your own form-based apps			✓
Directory Integration			
Active Directory directory synchronization	✓	✓	✓
High Availability	AD FS	AD FS	✓
Multi-Forest AD directory synchronization	FIM 2010 R2[2]	FIM 2010 R2[2]	✓
Generic LDAP directory synchronization	FIM 2010 R2[3]	FIM 2010 R2[3]	✓
Google directory synchronization			✓
Workday directory synchronization			✓
SAML Service Provider Interface	✓	✓	✓
Real-time bi-directional directory sync			✓
Unify mixed directory types (meta-directory)	FIM 2010 R2	FIM 2010 R2	✓
Manageability			
REST API	✓	✓	✓
VPN Integration		MFA Server	✓
RADIUS Support		MFA Server	✓
Group Based Access Control to Applications		✓	✓

[1] As of March 23, 2014

[2] Microsoft's Azure AD Directory Synchronization appliance only supports a single forest. Microsoft makes an Azure AD connector available for Forefront Identity Manager 2010 R2 to enable multi-forest synchronization scenarios.

[3] The Azure AD connector for Forefront Identity Manager 2010 R2 can be used to synchronize generic LDAP directories.

	Microsoft Azure Active Directory	Microsoft Azure Active Directory Premium Edition	OneLogin
Manageability (Continued)			
Provisioning with Entitlements[4]	✓	✓	✓
Just In Time Provisioning			✓
Delegated Authentication[5]			✓
Admin “Assume User” view			✓
Rules-based AD attribute mappings[6]			✓
End User Experience			
Desktop SSO to Cloud Apps (IWA)	AD FS	AD FS	✓
Active Directory Single-Sign-On	AD FS	AD FS	✓
Mobile SSO App Portal	✓	✓	✓
Self-Service Password Reset	✓	✓	✓
Branded Sign-On Page		✓	✓
Embeddable SSO App Portal (e.g. in an intranet)			✓
External Users SSO (customers and partners)			✓
Self-Registration Profiles			✓
Personal Apps			✓
Secure Notes			✓
Federated Search			✓
Security and Compliance			
User Password Synchronization	✓	✓	✓
Create custom password policies	✓	✓	✓
Combine AD Authentication w/ PKI Certificates	AD FS	AD FS	✓
Combine AD Auth. w/ IP address restrictions	AD FS	AD FS	✓
Advanced Security Reporting		✓	✓
Role-based Access Control to Applications		✓	✓
Multi-Factor Authentication (MFA) Phone App		✓	✓
MFA via SMS		✓	✓
MFA Policies			✓
Pre-integrated with 3rd Party MFA			✓
Choice of US or EU data residency			✓

[4] For example, not just create the user in Salesforce, but also assign him to the Standard User profile.

[5] For example, a double hop authentication into Service A, and then Service A impersonates the user into Service B.

[6] Use any attribute in AD as an indicator for application or policy assignments as well as bulk operations.

ABOUT THE AUTHOR

Brian Desmond is a Microsoft infrastructure expert focused heavily on Active Directory, Identity Management, Exchange, and recently, Office365 architecture/engineering projects for higher education and commercial enterprise customers. Brian has worked in numerous large scale enterprise deployments at various Fortune 100 and larger scale organizations as well as dozens of K-12 and Higher Education institutions and public sector customers across state and local government. Outside of conventional consulting and support roles, Brian has deep expertise managing and building combined offshore/onshore delivery teams in delivery locations around the globe. Since March 2003, Brian has been recognized as a Microsoft MVP for Active Directory for his contributions to the Microsoft technical communities at large. Brian is also the author of Active Directory, 5th Edition published by O'Reilly as well as a frequent contributor to leading industry publications. You can often find him speaking at conferences and events worldwide.

ABOUT ONELOGIN

OneLogin is the innovator in enterprise identity management and provides the industry's fastest, easiest and most secure solution for managing user identities, both in the cloud and behind the firewall. Ranked #1 in Network World Magazine's review of SSO tools, OneLogin's cloud identity management platform provides secure single sign-on, multi-factor authentication, integration with common directory infrastructures such as Active Directory and LDAP, user provisioning and more. OneLogin is SAML-enabled and pre-integrated with more than 3,500 applications commonly used by today's enterprises, including Microsoft Office 365. OneLogin, Inc. is backed by The Social+Capital Partnership and Charles River Ventures.