Removing Identity Barriers for Office 365

Windows IT Pro

SPONSORED BY

okta

Since its 2011 introduction, Microsoft Office 365 has undergone explosive growth in two ways: the number of subscribers has ballooned, and Microsoft has held a torrid pace for updates, shipping more than 450 updates between June 2014 and June 2015 alone. Despite their efforts, there are still some significant challenges to Office 365 adoption, including issues around identity management (or, more precisely, the design and management of identity management systems). In this paper, we'll examine the Office 365 identity management landscape, highlight the relevant challenges, and point to potential solutions.

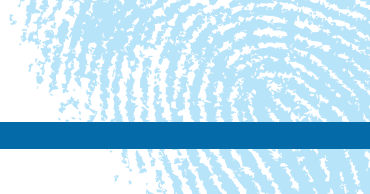
Introduction

Office 365 has grown into a huge software business in its own right; Microsoft's own estimates don't specify how much of its $6 billion-plus annual run rate for cloud services can be credited to Office 365, but it's a safe bet that it's the majority share—and that run rate is increasing steadily. Part of this growth has been due to the features and functionality in Office 365; potential customers compare the complete feature set (which includes Exchange, Skype for Business, and SharePoint, plus cloud-only components such as Delve and OneDrive for Business) to their on-premises implementation and recognize the value of the suite offering. Other customers, running older versions of on-premises Exchange, migrate to Exchange Online only but then adopt other Office 365 services to get more value from their existing license cost.

Another part of the growth of Office 365 has come from organizations that are seeking more reliability, security, and uptime. One of the key points of Microsoft's sales pitch has been that their heavily secured data centers, spread throughout the world, provide superior uptime and security.

In both cases, customers moving to Office 365 have to face the challenges of managing their users' identities to securely grant access to data and services stored in Office 365. Smaller customers are typically moving to Office 365 from unmanaged environments where they have no central identity store or directory service on-premises. An example might be a small avionics shop that moved from Google Apps services to Office 365, creating new cloud-based accounts for each user. For these customers, most of the challenges revolve around provisioning users through the Office 365 Admin Center.

Larger customers typically already have some kind of on-premises directory: frequently it's Windows Active Directory, but sometimes it's another directory system. These organizations face more challenges; they have to determine where the source of identity authority will be, how they will synchronize their cloud and on-premises identities, and how they will maintain a robust and secure identity management (IdM) environment.



Identity management challenges

IdM is central to effective organizational resource management and control, so understanding the challenges posed by the Office 365 IdM architecture and its unique requirements is a critical part of planning and implementing a robust IdM solution for Office 365.

Azure Active Directory: a challenger emerges

Office 365 has had a huge impact on the on-premises Exchange Server, Skype/Lync, and SharePoint markets, and Microsoft is betting that the same thing will happen with Active Directory. The Azure Active Directory (Azure AD) product line is targeted at, eventually, replacing on-premises AD as Microsoft's central IdM system. Right now, Azure AD comes in three editions:

- The Free edition is automatically included in every Azure and Office 365 subscription. The Free edition offers what's basically an invisible container to hold user accounts, group objects, and permissions for Office 365 services. When you create a user account in Office 365, or synchronize on-premises accounts to Office 365, they're stored here. However, the Free tier doesn't allow you to run your own applications against it, and it's feature-poor compared to the other two editions.
- The Basic edition "provides application access and self-service identity management." That's Microsoft's way of saying that you can tie Azure AD Basic into your own on-premises applications; it also provides self-service password reset, basic branding and customization, supports proxy publishing so you can use it with web-based applications, and offers a formal service level agreement of 99.9% uptime. It includes some useful reporting and auditing options not present in the Free edition.
- The Premium edition, licensed per user, includes support for multi-factor authentication, self-service group management (so that users can create their own security groups and manage their own group memberships, subject to administrative controls you set up), and self-service password reset so that users can change their own password through a web page and have the change written back to on-premises AD. At Ignite 2015, Microsoft announced that they would be adding machine-learning-powered security reporting and analytics to Azure AD Premium.

It's important to understand that Azure AD is not a drop-in replacement for on-premises AD because it lacks some key features: it doesn't support group policy objects, can't be used to assign permissions to on-premises objects such as file shares, and can't perform common

tasks such as registering printers so users can search for them. Microsoft is aggressively adding features to Azure AD, and organizations that choose to adopt Azure AD as their primary directory will benefit from that investment, but for now it's better to think of Azure AD as being a new cloud directory, not a replacement for on-premises AD.

Directory synchronization

Because Active Directory is so prevalent as a directory system, many organizations will find that they need directory synchronization in place for Office 365. The purpose behind dirsync in the Office 365 environment is to ensure that the Azure AD partition used by each Office 365 tenant has a complete copy of the on-premises objects and attributes needed to enable full hybrid operation. For example, one key part of hybrid Exchange connectivity is providing a global address list (GAL) consistent between users whose mailboxes are on-premises and those homed on Exchange Online. Dirsync makes the GAL work properly, in addition to other hybrid features such as the SharePoint Online "people picker" interface.

Dirsync operations pose several challenges. First, Microsoft only officially supports two dirsync tools. The Microsoft Identity Manager (MIM) 2015 product is an extremely full-featured, complex, heavy on-premises product that gives you a great deal of flexibility in exchange for its complexity and cost. Microsoft bundles MIM licenses with Azure AD Pre-

mium, lowering its marginal cost for those customers, however the servers, initial deployment and ongoing maintenance costs can be significant. MIM requires servers and infrastructure, and designing and operating MIM deployments is a skillset that most organizations don't have in house already, raising staffing costs. While MIM allows extensive customization, much of this customization requires you to write your own code, raising the expense and complexity even further.

Most Office 365 customers will instead choose to use the Azure Active Directory Connect (AADConnect) suite, which is based on the same core code as MIM 2015 but is intended to be more like an appliance that you set up once and then leave alone. Both MIM and AADConnect allow you to choose which domains or organizational units (OUs) you want to synchronize, and both support filtering based on AD attributes. (For more specifics on dirsync tools, see the section "Microsoft's identity solutions" later in this paper.)

Second is that the synchronization process will take whatever's in the on-premises AD and push it to the cloud—if your AD contains outdated, incorrect, or non-standardized data, so will Office 365. While Microsoft provides a tool known as IDFix to check for and fix AD attribute problems that may cause replication issues, the bigger issue is that most Office 365 adopters don't or can't take time to clean up their AD environment (possibly including consolidating domains, removing outdated groups, and so on) before they turn on synchronization.

Third is that Office 365 dirsync assumes that you're using AD as your primary enterprise directory. While this is a reasonable assumption for most customers, a sizable number of organizations are using alternate directory solutions that themselves have to sync with or connect to AD.

Finally, many customers who want to move to Office 365 find that the topology limits imposed by Microsoft's dirsync tools pose challenges of their own. For example, merger and

acquisition (M&A) activity usually results in some sort of consolidation of IT assets, but Microsoft's dirsync tools don't support some common topologies.

Identity federation and SSO

The basic idea behind federation is simple: when a user requests access to a cloud service, instead of directly authenticating the user, the cloud service will pass the authentication request to the federation server, which will then query on-premises domain controllers for the answer and return an appropriate security token. Identity federation enables single sign-on (SSO), arguably one of the most sought-after enterprise features in Office 365 deployments. Users don't want to have to remember and use multiple sets of credentials for their on-premises and cloud services, so Microsoft has attacked the problem of providing SSO by offering Active Directory Federation Services (AD FS). There are separate versions of AD FS included with Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

The benefits of federation are obvious: identity decisions are made on-premises, using the authoritative directory as the direct source. This improves security and allows for SSO. In addition, a properly configured federation service can tie together additional applications besides Office 365. For example, if you're using Amazon Web Services (AWS), you might want to federate AWS with your on-premises directory so that your AWS administrators and developers can log in with their standard AD credentials.

Federation isn't without its drawbacks though. The biggest one is that the federation infrastructure becomes a single point of failure. Consider the common case of an Office 365 customer with a single data center located in an area vulnerable to natural disasters. In normal operations, users can authenticate through federation as long as they can connect to the Internet, and as long as Office 365 can reach the on-premises federation servers. While a datacenter failure won't affect users' data or services because they're in the cloud, it will prevent users from being able to log in at all—even if they have Internet connectivity and can reach the Office 365 service—because the federation infrastructure in the datacenter is unavailable.

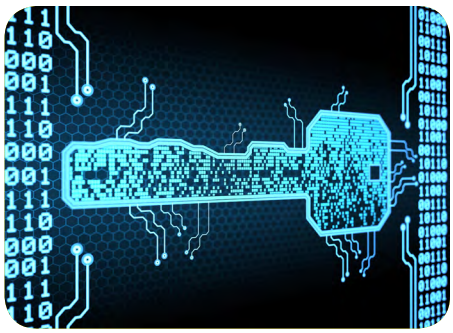
A related problem is that management and monitoring of the federation service becomes increasingly important once federation becomes a potential single point of failure. Because in normal operations federation is mostly a "set and forget" workload, it's tempting to leave those servers alone but doing so increases the risk that an undetected failure will cause downtime.

The work required to federate on-premises AD with applications can be daunting, too. Different federation vendors support different applications, and it's important to ensure both that your chosen federation solution supports the applications you use and that the application itself can be federated. For example, SharePoint 2013 fully supports OAuth and is known to work with several federation products, but there are a few federation services whose makers haven't fully documented the steps required to make their services work properly with major enterprise applications.

Mobility support

Business doesn't just run on the desktop any more. The definition of "mobile device" is broader than ever before: tablets and smartphones are used alongside both corporate-managed and personally-owned laptops that can synchronize with corporate resources both on-premises and in the cloud. At first thought, this might not seem like an identity management issue-- but devices have identities too, and just like users, these device identities have to be registered and managed, and device access has to be controlled in some way.

Microsoft's solutions for mobile device management include the Office 365 mobile device management feature set and Microsoft Intune; the former offers a subset of features from



the latter. These tools compete with a variety of third-party mobility management products from companies such as Cisco, VMware, and Good Technology. All of these tools provide some degree of control over several aspects of mobility management:

- Controlling who can enroll devices and what kinds of devices can be enrolled
- Applying conditional access policies to control what resources devices can access. For example, a conditional access policy might allow only certain users to synchronize mail but not files stored in OneDrive for Business.
- What device settings and policies can be automatically applied. This is more a function of what policies a given device family supports, although different mobility management solutions vary widely in the degree of control and monitoring they provide for policy application.

Because mobile devices are increasingly capable and powerful, one common issue that arises is how to build a management infrastructure that works more like the familiar world of group policy objects. For the most part, organizations that are using GPOs to manage Windows clients find that they can't apply exactly the same controls to those devices. Microsoft's solution is to point to the management features of Intune, which largely replace GPOs on full Windows clients and provide a consistent feature set across mobile and traditional Windows devices.

Addressing Office 365 identity challenges

Identity management is a complex problem. Microsoft has made a great deal of progress in deploying critical IdM features to Office 365, but there are still some challenges facing organizations as they adopt Office 365—and not all of these challenges can be solved by technical means.

Directory strategy

Perhaps the most important choice facing customers who are considering moving to Office 365 is what directory to use. A significant number of new Office 365 customers don't have on-premises AD; they're moving from an unmanaged environment where users log on to

their devices using local accounts to one where they can create cloud-only accounts in Office 365. Larger customers are much more likely to have on-premises AD, and that raises some interesting questions:

- Is it better to create new user accounts directly in the cloud and keep two sets of identities for users, allowing a clean start, or to use synchronization and federation to carry over existing identities?
- Are there existing on-premises applications that you would want to connect to Azure AD through SSO? Are there new web-based applications that you're thinking about using that can be integrated through federation?
- Do the additional features of Azure AD Premium provide enough value to justify its additional cost?
- How operationally mature is your existing directory services environment? Do you need to invest time and money in additional training, monitoring, or high availability to get it ready for the transition to Office 365?

Directory synchronization

Microsoft wants administrators to think of dirsync as something that only needs to be set up once and then can run unattended for years. The truth is that dirsync is a critical part of environments that have on-premises AD, and—as with any other critical system—it must be monitored and managed. The operational impact of a dirsync failure may be low or high, depending on the volume of directory changes that occur daily and their importance to business operations—simple changes such as employee last name changes are minor, but larger changes such as adding or removing user accounts or password changes must be promptly synchronized to maintain data consistency.

High availability options for Microsoft's dirsync tools are fairly limited. AADConnect can use a standby staging server that reads and stores directory changes but doesn't push them to Azure AD until activated, but there is no supported way to provide automatic failover or high availability for AADConnect, and the knowledge level required to design, operate, and maintain highly available MIM installations will be beyond the means of most potential customers.

Identity federation

Federation offers significant benefits, including easy SSO for users and the ability to centralize IdM on the on-premises directory. However, managing federation can be challenging. As with dirsync, monitoring and maintaining your federation solution is critical.

Microsoft's AD FS 3.0 is included at no extra cost with Windows Server 2012 R2, and it is straightforward to install and configure in simple topologies. However, it requires on-premises servers; more complex or larger topologies require careful planning, and the AD FS management tools are somewhat limited unless your administrators are comfortable using PowerShell. The biggest potential problem with AD FS for most organizations is its potential to be a single point of failure. Large organizations that already have multiple, geographically distributed data centers can create multiple AD FS farms, one per datacenter, and use load balancing to distribute traffic for a resilient solution—but for organizations without those resources, guaranteeing access to AD FS can be a significant challenge.

> "One of the things that attracted us to Okta as an identity management system was that it allowed us to simplify and streamline the account provisioning process for Office 365. Ultimately we chose Okta over ADFS because Okta did so much more for us than just the authentication."
>
> —Stephen Landry, CIO, Seton Hall University

Application integration

Some Microsoft customers only use Microsoft applications, but the majority of corporate, government, and academic organizations have a heterogeneous environment where applications such as Salesforce.com, SAP, Workday, and Autotask provide critical business services alongside Microsoft's enterprise products. Cost-effective IdM requires that all of these applications be united around the smallest possible number of core directory services. Microsoft wants that core service to eventually be Azure AD, but the fact is that for

almost all organizations today, on-premises AD is the key service that applications depend on. As new web- and on-premises applications emerge from Microsoft, its partners, and its competitors, it becomes increasingly difficult to provision and manage identities for those applications using Microsoft's own toolset.

> "The great thing about Okta and what they've done is that they've made identity core— core to your business and core to everything that goes on. We deployed Office 365 initially prior to Okta using *Microsoft's ADFS products and then Okta made available their ADFS replacement product. What we found quickly was that the Okta solution was much simpler and it's more effective. We were probably one of the first customers that embraced that with Okta."
>
> —Chris Thibault, Lead Systems Engineer, First American Equipment Finance

Standards-based identity federation systems offer the best possible path forward for application integration. Instead of relying on one-to-one partnerships between your identity vendor and a specific application, using a system that broadly supports open standards such as OAuth and SAML 2.0 helps minimize the number of compatibility issues and hassles you, and your users, face.

User provisioning is an often-neglected area of identity management. Organizations that have traditionally relied on Microsoft's on-premises AD tools for creating and managing users often find that,u ser provisioning for a heterogeneous set of applications is a more complex task than they first realized—a task that requires a provisioning product with clear

neutrality and a track record of connecting deeply to many applications from different app vendors. While Office 365 is an important investment, most organizations want choice and the flexibility to go outside of the Microsoft set of cloud applications while still keeping rich identity management functionality across all their applications. Although Microsoft has built some provisioning integrations to other vendors, their provisioning catalog has not grown much or as deeply as other identity management solutions.

Conclusion

Identity management in Office 365 poses significant challenges around application capacity, availability, and functionality. Single sign-on, and identity provisioning and management are critical parts of deploying and integrating Office 365, and, while Microsoft's standard tools are sufficient for simple deployments, more complex or business-critical deployments require additional attention to availability, application integration, security, and management.