Speeding Office 365 Implementation Using Identity-as-a-Service

White paper

August 2015

This white paper is sponsored by Centrify.

In little more than two years since its introduction, about 50 million paid subscribers are already using Microsoft's Office 365 productivity suite.[1] With Office 365's year-over-year growth of well over 100%, it is clear that companies continue to trust Microsoft to help them run their businesses—and to help them adopt cloud-based technologies. And now you are considering the move from an on-premises install of your core productivity applications to that of a cloud-based solution. The advantages are obvious: lower ongoing licensing costs, and less administrative management overhead including updates and vulnerability patches. Despite all of the benefits, there are still plenty of pain points involved in Office 365 adoption—especially when it comes to deployment.

IT administrators will recognize some of the biggest headaches: provisioning new users, managing multiple directories, managing passwords, securing mobile deployments, and managing new types of licensing challenges—not to mention usage tracking and reporting. Now add to this management overhead your already-deployed cloud applications—administrators are definitely earning their pay.

Looking deeper at each pain point, we start to see some commonalities:

- Provisioning new users: Adding new users can present its own challenges, and especially adding them into an Office 365 environment, simply because of the expansive nature of user attributes available. If a company already has its own Active Directory, then it must extend that to Office 365.
- Managing multiple directories: In many cases, established companies have a legacy directory and quite possibly core legacy applications that lock them into that directory. Administering multiple directories becomes an ongoing multivendor integration project that adds additional management overhead to IT departments as user accounts need to be created, managed and deleted in multiple locations.
- Password management: Without a true single sign-on solution or federated process, password management can quickly result in user dissatisfaction: Users will need to sign on multiple times, first for network access and then to reach their apps. This requirement will likely result in overburdening IT with manual tasks including large numbers of password reset requests. Keeping user passwords and credentials synced in a multi-directory environment exponentially increases complexity.
- Mobile deployments: Times have changed such that all employees now expect to be empowered to access many, if not all, of their core applications from mobile devices. BYOD is also beginning to be the norm in many environments. Although Microsoft has made strides to allow IT administrators to automate rollout of mobile applications to new employees, the process has a long way to go, especially when it comes to provisioning mobile devices for email through Exchange. All too often a company's IT department must still manually provision mobile users or troubleshoot access issues, even in what are supposed to be automated solutions.
- Licensing challenges: Rolling out Office 365 does avoid the massive headache of multiple sets of licenses for both client machines and servers, but deploying and managing Office 365 licenses for users is still far from an automated, turnkey solution.

[1] Paid subscription estimate obtained from http://windowsitpro.com/blog/80-million-exchange-online-users-office-365-progress-continues

Applying the correct license to newly created users is typically a manual process. Each subscription requires a user's device(s) to communicate with Office Licensing Service and the Activation and Validation Service to obtain and activate a product key. To roll out licensing to more than one user at a time requires Microsoft PowerShell scripts.

- Tracking and reporting: Beyond deployment, ongoing user management tracking and reporting is another layer of complexity with Office 365. IT admins need to identify inactive users and free up licenses for use by new employees. Admins also need to monitor various quota and storage levels across multiple services that can include Exchange and SharePoint, among others.

The commonality that appears when we see these challenges next to each other? They are all linked to identity.

The IDaaS Advantage

The lion's share of these issues are confronted with initial deployment and provisioning of your user base. And that is where an Identity-as-a-Service (IDaaS) solution can come to the rescue, helping your IT department take maximum advantage of your existing, well-planned identity infrastructure. With IDaaS, you can quickly enable single sign-on, multifactor authentication, privileged identity management, auditing for compliance, and mobile device management.

An IDaaS solution eases the burden of provisioning Office 365 accounts. IDaaS lets you on-board users and pre-assign roles using your existing directory, whether Active Directory or LDAP. IDaaS also generally makes it easier to de-provision or reassign users to a different group, and it automatically triggers appropriate changes to the user's software entitlements for Office 365.

Another advantage of IDaaS is that it allows you to utilize, or *federate,* your pre-existing user identity from multiple sources or types of identity management including Active Directory and LDAP directories. Specifically, federating means linking a person's electronic identity and attributes that are stored across multiple identity management systems. By federating identity from a central directory, you can give your users a single sign-on to Office 365 while making the rollout much simpler for your IT department. Federation is also important when looking beyond Office 365 and toward managing all of the other applications deployed to users in general. Federation is what manages access to thousands of other Software-as-a-Service (SaaS) and on-premises applications from any device—all based on a single user identity.

Users want single sign-on (SSO) access. This process requires a combination of technologies that allow users to sign in once and be authenticated to a variety of applications and systems. SSO is a property of access control of multiple related but independent software systems. There are several forms of supporting security and authentication technologies and configurations. They include Kerberos, WS-Federation, Security Assertion Markup Language (SAML) and others, which rely on the exchange of user security information between an enterprise and a service provider. An IDaaS solution can be used to simplify implementation and management of these advanced forms of security and authentication when it comes to providing user access to Office 365.

Users also want to be able to rely on their own devices; while Office 365 allows them to work from any device, the service also increases the complexity of managing user mobility. User privileges and licenses need to be tracked across devices and locations. An IDaaS solution can simplify this cumbersome process.

As you think about Office 365 provisioning and ongoing management, it's important to remember that the directory will need to be managed and synchronized with your existing corporate directory service. Microsoft's tools for synchronizing Active Directory with Office 365 require additional on-premises infrastructure, as well as a large investment in time and expertise to configure and deploy. An IDaaS solution can streamline this process, easing the management burden for IT staff while enabling users to work securely in Office 365.

Evaluating Identity-as-a-Service Solutions

Getting the greatest benefits from Office 365 means helping your users access all of the service's functionality from a variety of devices and clients. For a Windows PC, there are the desktop versions of Word, Excel, PowerPoint, Outlook, Lync, and OneDrive for Business. Add to that the web versions of the same applications (minus Lync). And the mobile Microsoft ecosystem of the above applications in app format combined with native email, calendar, and contacts for iOS, Android, and Windows Phone. A complete Office 365 deployment also shifts server versions of Exchange, SharePoint, and Lync to Microsoft's online versions.

An IDaaS solution also needs to make it easy for IT to create and manage user IDs, passwords, and privileges in a way that is completely unobtrusive for users.

Architecture

In many ways, differences in architecture between identity management solutions boil down to where identity, credentials, and privileges are stored, and the mechanisms with which this critical information is shared between on-premises and cloud-based systems.

These solutions must make it as easy and secure as possible to manage the integration of identity into cloud and in-house resources in such a way that the directory service exists as a single identity management repository that can be leveraged across devices, services, and locations.

One method is to store identity information only in the cloud, with no integration to on-premises directories. This approach may work for new organizations (especially if they are small and have not invested in infrastructure), but it is unlikely to work for most existing businesses. The best IDaaS solution for companies that don't want on-premises directories is to use a single cloud directory that streamlines identity management and security across Office 365 and other cloud solutions such as Salesforce.com, ServiceNow, Workday, and Zendesk. It also must work with a variety of platforms such as Windows PCs, Macs, and mobile devices. In this example, identity information might be stored in Windows Azure Active Directory and federated to other cloud applications. However, setting up this process is less than straightforward and requires the use of multiple Microsoft tools. Microsoft Azure Active Directory has a SaaS app catalog for adding SSO for other applications, but its scope is limited, as is support for custom applications. Furthermore, Microsoft's solution is built for Windows PCs, not mobile devices, and it requires the addition of Microsoft Enterprise Mobility Management to manage SSO on mobile devices.

Another method is to synchronize directory and password information between on-premises systems and Office 365. This is what takes place using Azure Active Directory Connect to copy identity information between on-premises Active Directory and Windows Azure Active Directory. It requires additional servers (at least two based on your organization's current configuration of Microsoft systems), a variety of tools including the Azure Active Directory Connect tool to initially replicate between on-premises Active Directory and Windows Azure Active Directory, and PowerShell scripting to replicate additions and modifications beyond the initial replication.

Directory Synchronization

The synchronization architecture mentioned above involves some major security implications. First and foremost, user IDs and passwords are copied between on-premises and cloud environments, creating the potential for an attacker to capture and used them to obtain access to sensitive company information.

In addition, the on-premises and cloud environments could fall out of sync while, depending on the frequency with which PowerShell scripts are invoked, changes made in Active Directory may not be replicated immediately to Windows Azure Active Directory. Imagine a scenario where an Active Directory password is reset and there is a lag before the Office 365 password is reset—and users don't know which password to use to log in to either system. This would certainly result in a help desk call. Moreover, this leaves a gap in security. For example, when users leave the company, their Active Directory accounts might be disabled but their Office 365 accounts still active. Administrators can always manually synchronize the two directories, although most IT management is already familiar with how inefficient and error-prone manual processes can be.

Imagine a scenario where an Active Directory password is reset and there is a lag before the Office 365 password is reset—and users don't know which password to use to log in to either system.

Some IDaaS offerings use a replication-based architecture that requires storing a complete copy of your organization's identity data from Active Directory in their cloud. Some even require the use of Microsoft Azure Active Directory Connect for integration with Office 365. These two factors mean that these IDaaS solutions suffer from the same shortcomings as the Microsoft solutions—and identity replication in general—as discussed in the preceding paragraph.

A third method is to federate identity between Active Directory and Windows Azure Active Directory. In the Microsoft world, this is done using Active Directory Federation Services (ADFS) and Azure Active Directory Connect. That sounds simple, but implementation typically requires four additional servers (two in the DMZ and two behind the firewall). It also requires opening additional ports on the firewall, third-party certificates, and custom PowerShell scripting to tie it all together. All of this may add as many as three to four weeks of planning and configuration to your Office 365 implementation timeline. Although ADFS and Azure Active Directory Connect are free, four servers could cost your organization $20,000 or more.

Real-Time Identity Federation

The best IDaaS solution is one that combines simplicity with power and minimizes operational overhead. For example, instead of requiring the management of separate internal and external directory services, an IDaaS solution should utilize a single, federated directory. It should do so by installing an application on any domain-joined server inside your firewall, without the need for additional hardware, firewall reconfiguration, or third-party certificates. An extensible IDaaS solution federates identity not only from Active Directory to Office 365, but also to other cloud solutions. On-premises directory data in Active Directory or LDAP remains within the organization, which decreases potential security risks. In the best case, a single IDaaS application is the only software you need, unlike other solutions that require an additional on-premises federation server and third-party certificates.

Support for hybrid on-premises and cloud-based directories, meaning the ability to use a combination of local and cloud-based directories, varies among IDaaS providers. Managing multiple directories through a single interface is critical, as is the ability to manage multiple Active Directory forests, perhaps as the result of M&A activity.

An IDaaS solution should include the ability to manage access to Office 365 by internal and external users and groups. For example, an organization could store full-time employees' identity in existing Active Directory, employees from a recent acquisition in a separate Active Directory forest, customers in LDAP, and contractors or partners in separate directories hosted in the IDaaS provider's cloud.

Another factor to consider when evaluating IDaaS providers is the depth of support for Office 365 licensing options. License management is not simply a yes or no feature; there are important degrees of granularity. Office 365 uses multiple types of enterprise licenses based on the Office productivity and online conferencing components that a user may access. Look for an IDaaS solution that allows for role-based license management; this will allow you to optimize your IT budget by dividing or sharing licenses across different users or groups. Microsoft and many other IDaaS solutions offer very little granularity in managing licenses. Enterprises get the greatest benefit from an IDaaS solution that allows license management by license type, user, and group and provides detailed usage tracking and reporting. This increased flexibility allows IT departments to purchase fewer high-end licenses and ensures that users get access to the features they need. The better the license tracking features and reporting capabilities that an IDaaS solution has, the greater the benefit to IT departments, which don't have to overbuy but instead can more simply see, track, and consume the licenses they already have.

Mobile Integration

Mobile integration and management of identity across mobile platforms are other key factors to consider when evaluating IDaaS. Mobile is undoubtedly a core part of any IT strategy, because business users want to work on mobile devices. Securing applications starts with securing the devices used for access. The best way to enable employee mobility safely, especially when using a combination of cloud and on-premises solutions, is through an IDaaS solution that offers robust mobile management capabilities.

Look for an IDaaS solution that includes mobile device management (MDM), mobile application management (MAM), and policy-based access controls. These tools enable IT organizations to support and maximize the productivity of a diverse workforce. Companies can establish and

maintain security requirements for mobile devices, ensure compliance with regulatory requirements, maintain data privacy, and protect corporate intellectual property. Tightly integrating identity with MAM and MDM enables users to work on their preferred device safely and securely both inside and outside the corporate firewall.

MDM focuses on the device, with features such as remote wipe and lock for lost or stolen devices. This is the most basic level of mobile management, and it is necessary to provide a secure mobile platform for employee productivity. Quick, easy, policy-based provisioning is an essential component of MDM. A self-service portal allows employees the ability to enroll and manage their own devices, and it reduces administrative overhead.

MAM provides the capability to push, manage, and wipe mobile applications on mobile devices, provide SSO capabilities, and ensure that corporate and personal data remain separate. IT sets application and data policy in advance based on an employee's identity, then allows employees to enroll their personal devices and have apps automatically pushed to them. This also includes the management of native mail, calendar, and contacts apps plus the certificates that are required for these apps to securely interact with Exchange or Office 365.

The ability of an IDaaS solution to manage mobile users via Active Directory policies will save your IT organization time and effort. To decrease cost and integration effort, look for an IDaaS solution that will work directly with Active Directory and not require additional software such as Microsoft's Enterprise Mobility Suite. Centralized device management over Active Directory gives IT administrators a single location to manage security settings, profiles, certificates, and restrictions. Group Policy–based management extends this functionality and allows you to establish device policies based on business need. Assigning devices to users in Active Directory ensures accountability and easy reporting.

Conclusion

Office 365 is rapidly proving to be a valuable productivity tool in the IT arsenal. This is evidenced by the explosive growth of Office 365 rollout, especially within the past year. However, many IT organizations discover that despite the significant advantages of Office 365, such as lower ongoing licensing costs and decreased management overhead—including updates and vulnerability patches— a number of pain points remain in adopting the cloud productivity solution. These include provisioning, directory management, password management, mobile management, licensing, and usage tracking and reporting.

IDaaS is a valuable tool for easing those pain points, but IDaaS solutions are not all the same and require careful evaluation. Key insight into selecting the right IDaaS solution comes through a careful examination of architecture, mobile management, and other capabilities.

About Sarrel Group

Sarrel Group is a technology product assessment, editorial services, and IT consulting firm with offices in New York City and San Francisco. Sarrel Group helps technology companies develop sales and marketing programs based on lab-tested validation of their products' competitive advantages. For more information, please visit www.sarrelgroup.com or call 866-MSARREL.

About Centrify

Centrify strengthens enterprise security by managing and securing user identities from cyber threats. As organizations expand IT resources and teams beyond their premises, identity is becoming the new security perimeter. With our platform of integrated software and cloud-based services, Centrify uniquely secures and unifies identity for both privileged and end users across today's hybrid IT world of cloud, mobile and data center. The result is stronger security and compliance, improved business agility and enhanced user productivity through single sign-on. Over 5000 customers, including half of the Fortune 50 and over 80 federal agencies, leverage Centrify to secure their identity management. Learn more at www.centrify.com.