Modernizing Active Directory for Azure and Office 365

Guidelines for a smooth Office 365 implementation with Azure Active Directory

Written by Darren Mar-Elia, president and CTO of SDM Software and Microsoft MVP

INTRODUCTION

In medium and large businesses, Microsoft's cloud services are gaining momentum. Cloud-based products like Office 365 are appealing if you're an IT manager who would rather administer services — Active Directory (AD), Exchange Online, Lync Online, SharePoint Online, OneDrive and others — than administer servers.

Microsoft is making the transition easy by offering free tools, particularly for migrating and/or integrating from your on-premises AD to Azure AD. Maybe a little too easy, in fact, if you have started purchasing licenses and migrating resources to the cloud before laying the groundwork for a smooth transition. While the tools may help you succeed in leaving hardware behind, you may also inadvertently migrate years of clutter and obsolete data into your new cloud environment.

Azure AD is designed to take full advantage of Microsoft cloud services like Office 365 and help companies turn a new page on user authentication. When you're synchronizing to the cloud from an internal AD that you've first organized, managed and cleaned up — that is, modernized — your Azure AD will serve you and your cloud strategy more efficiently.

This paper emphasizes the value of modernizing your organization's AD before migrating to Azure and Office 365. It offers perspectives on modernizing and integrating your on-premises AD into Azure so that you can enjoy less administration of on-premises hardware and software and introduce your organization to identity as a service.

RE-EXAMINING YOUR ACTIVE DIRECTORY

The rush to adopt Office 365 is on, with the number of Office 365 commercial seats in use nearly doubling from 2013 to 2014.[1]

Since Azure AD is the cloud-based user authentication and authorization service that Office 365 uses, that rush may catch you off guard. Before moving the organization to Office 365, be sure to get your AD house in order first. AD and Azure AD play a prominent role in successfully adopting Microsoft's cloud

[1] Paul Rubens, "Microsoft Office 365 Adoption Takes Off, War With Google Apps Rages On," CIO.com, January 22, 2015

services. To enjoy the lower costs of hardware, software and maintenance that your cloud strategy promises, you have to think first about your internal AD, then Azure AD, then services like Office 365.

That may be a new mindset in your organization, even if you rely on AD for essentials like user authentication and authorization, file server access, applications and infrastructure. But with a technology like AD that has steadily grown in size and complexity in many companies since 1999, it pays to heed Microsoft's recommendation to move to the cloud with a leaner AD:

> "Microsoft believes it's a good time to modernize your infrastructure since there have been many advances in technology in the past decade that can drive significant IT benefits and business value. It's important and necessary to have a clean and streamlined AD environment when taking advantage of all benefits of technology like Office 365 and other cloud-based applications and infrastructure. Modernizing is especially important for those moving to Windows Server 2012, as its successful deployment requires a clean and manageable Active Directory."
>
> *Mark Linton, General Manager of OEM Product Management Group, Microsoft*

Before moving the organization to Office 365, be sure to get your AD house in order first.

Consider a few of the factors that can affect the health of AD and your migration to Azure AD:

- IT shops that have used AD from its infancy and grown up organically with it may have adopted less-than-optimal ways of organizing AD. They may still have legacy processes around who is creating, editing and deleting objects and where those objects get created.
- Commonly accepted practices used to include creating a root AD domain with no resources. If you followed and maintained that practice, it could have a substantial impact on your move into the world of Office 365.
- Microsoft used to recommend using the domain as the security boundary for isolating resources in Active Directory, then changed their advice in favor of using the forest. Some administrators took to creating multiple forests, which they might now want to reorganize or consolidate before integrating with Azure AD and Office 365, as integrating multiple forests into Azure AD results in a number of complexities that can prolong the deployment substantially.
- Companies facing governmental or regulatory requirements may have to be selective in the objects they synchronize between their internal AD and Azure AD to ensure continued compliance. This can be difficult if your internal AD is disorganized, or characterized by regulated objects mixed in with non-regulated ones.

Thus, the move to Office 365 sets the stage for modernizing AD.[2]

THE 4 BASICS OF MODERNIZING ACTIVE DIRECTORY

Modernizing AD is the process of taking a fresh look at how you organize and maintain it. A modernized AD structure makes it easier to run Office 365 and Azure AD in four particular areas:

1. Normalized structure

Fewer domains and forests are generally better. Normalizing AD means reducing the number of forests and the security boundaries they represent as much as practical. Smart companies manage their access and privileges consistently across an AD deployment, and have the groups representing those accesses well controlled and arranged by business function.

2. Consolidated and cleaned-up OUs

One of the biggest obstacles to implementing Office 365 smoothly is a scattered organizational unit (OU) structure. If you're granting access to mailboxes and SharePoint resources based on groups whose objects exist in many different trees or hierarchies within Active Directory, you're asking for trouble.

Azure AD synchronizes all containers in your AD by default (for specific object classes such as users, groups and contacts) unless you set it to synchronize only specific OUs. That means that the OU is your ideal level of control as an administrator, so it pays to consolidate by ensuring that all of your user objects are under a single or a nested OU structure, for instance.

[2] For more details on re-examining your AD, refer to the Quest white paper, "Modernizing Your Active Directory Environment."

The best OU structure is the one that fits your organization, whether by geography, function or business unit. But it is important to avoid having user objects spread across different hierarchies within AD, which is common in AD deployments that have been around for a long time.

Suppose you had user objects in three distinct structures within a single, on-premises AD domain. You would have to synchronize all three of those OUs to Azure AD separately, which is a headache, especially if those OUs also contain objects that you don't want to synchronize (for example, application service accounts or security [non-distribution groups]). Unfortunately, it would be a bigger headache to synchronize the entire domain with all of the admin and service accounts that have nothing to do with running Office 365 in Azure AD. Your lack of a consolidated OU structure would obligate you to spend time and effort repeatedly filtering what you synchronize, and your process would become more brittle when you had to move objects around.

3. Good security delegation and good management

In a solid OU structure, your groups, users and computers are well delegated. In other words, it's well secured, with access to objects granted to only the people that need it. While there isn't a direct correlation between your internal AD structure and Azure AD (Azure AD doesn't support the concept of OUs today), there is a delegation model within Azure AD, and so ensuring that you have a good idea of "who manages what" will help transition administration to Azure AD. In addition, Azure AD is introducing the concept of administrative units, which are a form delegation that allows you to cordon off certain objects to be managed by subsets of administrators. Having a clean delegation structure within internal AD can help make it easier to take advantage of these Azure AD constructs going forward.

4. Solid provisioning and deprovisioning

In theory, granting access to users when they need it and removing it when they no longer need it is perfect. In practice, maintaining that process is more difficult. Users naturally assume and change roles in the organization and need access to different resources during their tenure. When they leave, the organization removes their access. If your organization is rigorous in provisioning, reprovisioning and deprovisioning users in on-premises AD, it will enjoy similar benefits with Azure AD. But if it takes you six months to disable the user account in your on-premises AD when an employee resigns, then you'll pay six months of per-user fees for Azure AD and Office 365 subscriptions that nobody is using.

THE SIGNIFICANCE OF OFFICE 365

Once your AD house is in order, you can turn your attention to the question of why Office 365 is important. Adoption rates suggest that many companies have already satisfied themselves with a variety of answers:

- **Expense** — The most compelling reason is that it is expensive to run Office or products like Exchange, Lync and SharePoint, especially at scale. The products grow in complexity with each release, motivating many organizations to get out of the business of maintaining back-office infrastructure.
- **Business criticality** — The communication, productivity and collaboration embodied in Office products are essential, so in effect it now requires specialized administrative knowledge, high availability and strong IT processes to keep your business running. Not all organizations have those resources or can afford them.
- **Commodity status** — Unless you derive revenue from providing IT services and keeping infrastructure running, those functions are not at the core of your business. Your business goals will be better served by purchasing services and allowing Microsoft to provide them.
- **Financial model** — Even for small-to-medium businesses, Office 365 has the potential to change the financial model for IT. Instead of spending on high CAPEX for back-end hardware, network, and the monitoring and management that go with them, companies can move to the OPEX of a monthly, per-user cost.
- **Ease of transition** — Microsoft is making the transition from on-premises to cloud-based services easy by offering free tools like OnRamp for Office 365, IdFix, Exchange Server Deployment Assistant

Azure AD synchronizes all containers (but not all object classes) in your AD unless you set it to synchronize only specific OUs.

and several related toolkits. Even smaller IT teams have what they need for a successful migration.

Administer services, not servers

Nevertheless, to authenticate Office 365 users, you will still need to store user identities in Azure AD, which means synchronizing on-premises AD to the cloud. You will still need to make decisions about synchronizing passwords or federating, based on the size of your organization, your security concerns and your technical depth.

But the decision-making process boils down to administering services or administering servers.

> If it takes you six months to disable an unneeded user account in your on-premises AD, then you'll pay six months of per-user fees for subscriptions that nobody is using.

GETTING TO IDENTITY AS A SERVICE WITH AZURE AD

Among the most important services organizations will start administering is cloud-based identity. In the context of Office 365, Azure AD represents this kind of identity as a service.

How does Azure AD differ from on-premises AD?

Whereas some cloud services simply replicate the functions of on-premises applications, Azure AD is a multi-tenant service designed to support identity and access management. It is more closely related to Active Directory Lightweight Directory Services (ADLDS) than to on-premises AD in terms of its structure (though it does not support an LDAP interface today), with several enhancements:

- Azure AD can store only a subset of the object classes and attributes associated with on-premises AD, such as user objects, contacts, groups and group memberships.
- Instead of OUs, Azure AD has administrative units, intended for delegating objects in an Azure AD tenant.
- You manage Azure AD using PowerShell or the RESTful Graph API, rather than with LDAP.
- The Azure AD delegation model is much simpler than regular AD, with only a handful of administrative roles available.
- Azure AD doesn't support Kerberos or NTLM authentication. It uses simple authentication if passwords are held in the tenant, or federated authentication back to your on-premises AD if not.

Azure AD is not simply AD domain controllers running in the cloud.[3] It is made for authentication and authorization in support of cloud-based services like Office 365 that seek to integrate with an Azure AD identity. Hence, identity as a service.

Synchronizing on-premises AD with Azure AD

When you provision a mailbox in Office 365, the mailbox is associated with an Azure AD user object. First, however, your Azure AD identity is associated with your on-premises user identity. Microsoft provides a couple of mechanisms for integrating Office 365 with your Azure AD or on-premises AD, so you have some decisions to make.

To populate (or provision) Azure AD, you must synchronize it with on-premises AD users, contacts and groups. Microsoft provides free synchronization tools like DirSync; its successor, Azure AD Sync Services; and soon, a new offering called Azure AD Connect that is even more lightweight.

- Free, Basic or Premium? — Microsoft offers three different editions of Azure AD:[4]
  - Free offers user and group management, accommodates up to 500,000 directory objects and spans the first steps toward integrating identities into Azure AD. If you are simply trying to get Office 365 up and running, you can use the Free edition and one-way or two-way synchronization to integrate all your users and groups into Azure AD.
  - Basic adds group-based access management, self-service password reset for cloud applications and a customizable environment for launching applications.

[3] Note that this is possible over a virtual private network between domain controllers and virtual machines running AD in Azure. However, the result is not the same as what Azure AD delivers.

[4] For a detailed comparison of Free, Basic and Premium editions of Azure Active Directory, visit http://azure.microsoft.com/en-us/pricing/details/active-directory/.

    - Premium adds protection features like multifactor authentication (MFA), mobile device management features and group-based single sign-on (SSO) to thousands of software-as-a-service (SaaS) applications.
- One-way or two-way? — One-way synchronization pushes updates from your on-premises AD up to Azure AD only. Alternatively, two-way synchronization (available in all editions) allows self-service apps like password reset and group management to run in the Azure cloud and write changes to Azure AD, which then get written back to your on-premises AD.
- Authenticate on premises or in Azure AD? — When you log in to a cloud service like Outlook Web App in Office 365, you must enter the credentials (user name and password) from on-premises AD. There are two ways to handle that, depending on your own security requirements:
    - Synchronize on-premises AD passwords for user accounts using Azure AD Sync Services or Azure AD Connect, and validate the password in Azure AD. This option is preferable for small or medium IT shops.
    - Validate the password using the on-premises AD. This option is better suited to enterprises. A sample configuration would include a SAML or WS-Trust relationship between software like AD Federation Services (ADFS) running on premises and Azure AD in the cloud. Once configured, the login process would transparently pass your on-premises credentials to the Office 365 tenant with no special actions on your part.

Once in Azure AD, possibilities open up

Once you've synchronized your modernized, on-premises AD with Azure AD, you can take advantage of other identity-related Microsoft Azure services:

- SSO in the cloud — Instead of having to run your federation services on premises, you can federate in the cloud. Microsoft's relationships with SaaS providers like Salesforce and Workday enable you to perform all authentication and authorization in Azure AD.
- MFA — Similarly, you can add MFA to your identities in the cloud rather than deploy it on premises.
- Access to Office 365 ProPlus — Many enterprises have subscribed to Office 365 ProPlus for cloud access to both mobile and desktop versions of applications like Word, Excel, Outlook and PowerPoint. Activating those applications requires credentials in Azure AD.
- Cloud-based identity management — Most important, the advantages of cloud-based identity management start to come within reach with Azure AD. Instead of having to provision and deprovision identities on premises, you can use the tools in Azure AD (especially Premium edition) for self-service management of passwords and groups, and use the Graph API to provision and deprovision objects programmatically. That paves the way for identity as a service.

Modernizing AD is the first step

Integration with Azure AD is not an overnight process. Even as you begin to provision Azure AD, your on-premises AD will remain your anchor for day-to-day activities like joining machines to the domain, managing Group Policy and authenticating users of on-premises applications for the foreseeable future.

Having both feet planted firmly in both worlds requires a modernized, well-managed, on-premises AD, because much of what you do there also makes its way into Azure AD. When unused objects are synchronized to Azure AD, they can lead to confusion, unauthorized access to cloud resources, needless per-user charges and the loss of some of the AD management advantages for which Azure was designed.

> Instead of spending on high CAPEX for back-end hardware, network, and the monitoring and management that go with them, companies can move to the OPEX of a monthly, per-user cost.

CONCLUSION

Office 365 requires Azure AD, and a stable Azure AD requires a modernized, on-premises AD, with a normalized structure, consolidated OUs, good security delegation and solid provisioning. Failing this modernization, the complexities of integrating into Azure AD grow and the benefits of Office 365 shrink.

> Microsoft's move into cloud services represents an opportunity to wean yourself off the data center and begin to run your back end in the cloud.

Microsoft's move into cloud services represents an opportunity to wean yourself off the data center and begin to run your back end in the cloud. As you reduce the number of areas that require in-house expertise, you remove yourself from the business of administering infrastructure and can instead focus on administering services — especially identity as a service — to your users.

YOUR TURN

Microsoft makes it easy to test Azure AD at microsoftazure.com. With a Microsoft account, you can activate a synchronization server from on-premises AD to an Azure AD tenant that allows you to create users and groups. Explore the concepts described in this paper and gauge the fit for your organization.

Visit http://azure.microsoft.com/en-us/documentation for documentation, video, automation scripts and other resources.

ABOUT THE AUTHOR

Darren Mar-Elia is a Microsoft MVP and president and CTO of SDM Software. He has more than 30 years of experience in IT and software development, including serving as CTO for Windows management solutions at Quest.

Darren has written or contributed to many books on Windows management and is a contributing editor for Windows IT Pro magazine. He also created the popular GPOGuy.com website for Group Policy and is a frequent speaker at conferences on Windows infrastructure topics.

© 2016 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal .

Trademarks

Quest, and the Quest logo are trademarks and registered trademarks of Quest Software Inc. in the U.S.A. and other countries. For a complete list of Quest Software trademarks, please visit our website at www.quest.com/legal. All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (www.quest.com) for regional and international office information.