Redmond INTELLIGENCE

EXPERT RESEARCH ON MICROSOFT TECH

BEST PRACTICES

Eliminate On-Premises Active Directory Dependency

BY NICK CAVALANCIA

SPONSORED BY okta

In just about every organization in the world, people have a tendency to avoid change. Business processes, vendors, methods and tactics are all used simply because they always have been. Active Directory has become one of those staples in organizations that seems to fit this model. Reaching its 20-year mark, AD has become the central focal point for identity, applications, collaboration and security. And rightly so, when AD came out with Windows 2000 Server, it was an advancement in directory services that was scalable, extensible, and multi-purposed, allowing organizations to simplify the work of enabling users to access data and applications.

But times have changed.

The evolution of the cloud over the last 10 years has caused organizations to rethink identity, authentication, security, access and applications. Active Directory—the one-time king of on-premises directory services—no longer is the right choice for many organizations that are moving to a "cloud-first" business model.

Even Microsoft's Azure AD is a signal that on-premises AD isn't a fit for a cloud-first world. Human Resources Management Systems (HRMS) and business applications are now all in the cloud, meaning that the use of on-premises AD only adds to the complexity of a world of technology that has moved on without it.

The reason? The cloud needs *identity*, of which directory services is a component. Identity offers the cloud a centralized service that provides secure authentication to a distributed set of cloud applications, while centralizing the management of identities throughout their lifecycle.

While organizations can (and do) continue to utilize AD, the reality is that cloud applications are becoming an increasingly critical part of business operations. The reliance upon AD technology not designed for the cloud (nor fully meeting its identity needs) will only hinder growth, innovation and productivity.

Because of this, it is critical that organizations seek to shift their dependency upon on-premises AD and move to cloud-first solutions that will support the identity needs of the organization today and in the future.

This report covers some best practices to follow as you plan and/or work toward eliminating your organization's dependency on on-premises AD.

The first step revolves around breaking a 20-year old habit.

BEST PRACTICE #1: STOP THE AD-CENTRIC THINKING

AD has done a lot of good for organizations throughout the last 20 years. Enterprise-wide, it has served as the central repository for accounts and passwords and as the basis for collaboration, messaging, and security. In essence, *AD has been the center of your universe.* So, before you begin your journey to eliminate on-premises AD in favor of a cloud-based identity-centric architecture, it is absolutely critical that you work to change your thinking about AD. Without doing so, you run the risk of simply looking for a cloud identity platform that integrates with AD.

Given that the shift to the cloud has moved well past the need for any kind of on-premises directory service, *it's time to stop thinking everything needs to revolve around AD*.

There are a few reasons why on-premises AD can no longer be the center of your directory, identity or security strategies:

- **It uses legacy protocols and standards:** AD was built at a time when the cloud wasn't even conceived. It's based on the lightweight directory access protocol (LDAP), relying on NT LAN Manager (NTLM) and Kerberos protocols for authentication and remote procedure calls (RPC) for communication between applications. These are age-old protocols that have long-since been replaced. Cloud-based applications today use Security Assertion Markup Language (SAML) and Open Authorization (OAuth) for authentication, and REpresentational State Transfer (REST) APIs for communication between applications. In short, *on-premises AD is old and, largely, incompatible*.

- **It is not *in* the cloud:** Microsoft has created Azure AD, a completely new version of AD that lives in the cloud and is based on the newer protocols. But on-premises AD has no home in the cloud. You could obviously put some domain controllers up in the cloud, but the very existence of Azure AD makes the case that not even Microsoft thinks on-premises AD belongs in the cloud. Which brings us to the final point.

- **It is not designed for the cloud:** The cloud has evolved into a mesh of applications, directories and services that are fabricated in many ways to interact with one another by default. Any kind of integration at this point with on-premises AD is only done as a gateway to get those customers that are still stuck there into the cloud with the hopes of doing everything mentioned inside this report.

Being AD-centric made sense at a time when AD *was* the de facto standard for directory services in the world. Today, that is just no longer the case. So, attempting to continue to innovate with an AD-centric mindset is only going to stifle any advances in today's cloud-first world.

Instead, the thinking needs to shift to leveraging a *cloud-based identity platform* and allow AD to exist as just one of many directories, servicing legacy on-premises applications.

If you are there, you can move to the next best practice to help determine what identity should look like for a *cloud-enabled version* of your organization.

BEST PRACTICE #2: IDENTIFY WHAT YOU NEED FROM AN IDENTITY PLATFORM

Before you can implement an identity platform, it is necessary to consider how identity will be specifically used within your organization. As you walk through the following list of potential needs, consider how each is or is not met by your use of AD. In organizations that have doubled down on AD, there are lots of AD-centric integrations that may require a complete rearchitecting when moving to the cloud.

The assumption here is that you have not yet made the jump to a cloud-based identity platform. In that spirit, consider the following needs as both a template to pinpoint some of the considerations that will help you select an identity platform, as well as the beginnings of a design template of what the environment will need to look like post-implementation:

- **User Needs:** Your need to centrally authenticate those using some part of your environment may go well beyond just employees. Consider whether there is a need to include customers, employees, partners, contractors and others within your supply chain. These distinct groups of individuals may have varying needs and would require an identity platform designed to handle disparate needs.

- **Environment Needs:** Your chosen identity platform will need to support a very specific list of applications, systems, platforms and directories that will be dependent upon it. Applications may need to be modernized and, in some cases, moved to the cloud. In the case of anything that will need to remain on-premises, it may be possible to update authentication protocols to be compatible with your chosen identity platform.

- **Identity Needs:** There are a number of aspects to how identity can be used. At a minimum (and depending on the vendor), you should be thinking about using an identity platform to provide one or more of the following functions:

  - **Authentication:** This includes Single Sign-On (SSO), multi-factor authentication (MFA) and session control.

  - **Authorization:** This involves defining and maintaining roles, rules and privileged access to be used when users desire access to various parts of the environment.

- **Directory Services:** A central identity store is foundational, as is the synchronization among directories and applications within your environment.

- **Management:** An ability to easily provision and deprovision should exist, leveraging self-service and delegation to expand the responsibility of maintaining the environment beyond that of just IT.

Devices: This should be almost a non-issue, as nearly every cloud-focused identity service is Web-based and is, therefore, device-independent. Even so, be certain any and all devices you want to have included as part of your implementation are supported either via browser or device app.

Security & Compliance: *Visibility* and *control* are two of the primary challenges of moving any part of your operations to the cloud. Without these two firmly in place, it is nearly impossible to know your organization is secure and that it meets the necessary compliance mandates. A critical part of your implementation is to identify parts of the environment that are security concerns or that fall under compliance, requiring visibility into, and control over, who has access and when access is utilized.

Dependencies: The existing environment already has some dependencies you will need to work through. For example, some on-premises Microsoft applications are very dependent on AD to function. You'll need to list any application, service or directory dependencies to ensure the architecture of a new cloud-centric environment will meet the operational needs of any and all applications.

With a comprehensive list of requirements, you are better positioned to identify the right identity platform to meet your needs. You will also ensure that the implementation of a new identity-centric architecture, which is not dependent upon AD, is designed around the specific operational requirements of your organization.

BEST PRACTICE #3: RELOCATE UNTETHERED IDENTITIES TO THE CLOUD

Without the cloud, on-premises AD has still been used by organizations to host accounts for users who are not employees of the organization. Contractors, partners and temp workers that do not actually require access to anything on-premises and are solely using cloud applications that still exist within AD. These untethered users should be considered the first wave of identities that can be most easily moved to the cloud. Placing them into your identity cloud makes more sense for a number of reasons:

- **Having them in AD is a security risk:** Every additional account that exists in on-premises AD adds to the attack surface. Hackers look to gain access to your network through compromising user credentials, and these users are the ones that are least concerned about your organization's security.

- **Having them in AD is unnecessary:** Assuming these non-employee accounts are leveraging cloud-based resources and applications, using AD as the identity repository is only done because you have no cloud-based option. In reality, they do not need to be in AD.

- **Having them in the cloud better facilitates access to cloud resources:** Today, everything these accounts access may have some method of integration with AD. But as the organization changes, shifts to the cloud, and begins to innovate, newer cloud applications are going to require a cloud-based identity platform so you can provide controlled access.

Relocating untethered identities to the cloud is probably one of the simplest and easiest ways to reduce the dependency on AD.

BEST PRACTICE #4: CONSIDER AN HRMS AS THE EMPLOYEE SYSTEM OF RECORD

Every organization has taken advantage of those expected fields in AD (such as phone, address and title) that provide needed details about users and made AD a usable directory beyond its authentication function. But, because on-premises AD will no longer be the focal point of your identity, there needs to be a central employee system of record (ESR) that exists *outside* of AD. In fact, in a proper identity-centric implementation, the ESR isn't even updating AD directly; it's instead updating your identity platform, which, in turn, updates AD (among the other directories that may exist).

The most appropriate choice for an ESR is your Human Resources Management System (HRMS). It's constantly updated with the most current employee information (such as role, title, department, location and phone) that can be utilized by an identity platform and/or individual directories.

This approach has a few benefits:

- **Achieved Consistency:** Disparate directories with no central identity platform pulling them together yield inconsistent data. Decentralized syncing also will not do it, as no two directories share the exact same schema (look at AD and Azure AD—even they do not match perfectly on every attribute). By using an ESR that leverages your identity platform to distribute account attributes to all directories and applications involved, the organization will have a singular consistent set of details shared throughout.

- **Improved Accuracy:** IT is not exactly rushing to keep the attributes of each user and group account updated, right? The previously mentioned inconsistencies would also yield inaccurate management. For example, an identity platform could provide access to an application based on the department to which a user belongs. If the details within the user's identity are not updated, access is not granted. Instead, by using an HRMS as your ESR, the data used to update both your identity platform and the directories and applications it services is accurate and up-to-date. This facilitates automated provisioning and deprovisioning, elevating the productivity of IT and users alike.

- **Enhanced Security:** Good decisions are based on good data. And security is often based on an individual's department, title, role or location. With accurate account and attribute details in play, the organization is better positioned to ensure appropriate security permissions and policies are in place, limiting access across the various data sets, applications and platforms that are in use—both on-premises and in the cloud.

The concept of using something far more authoritative than on-premises AD as your ESR fits within the grand scheme of shifting to the cloud. The ESR would sync with your cloud-based identity platform, providing up-to-date details for each user identity. The identity platform, in turn, would sync with each integrated directory service (including on-premises AD), ensuring consistency throughout the environment.

With AD becoming just one of many directories, using an HRMS makes sense in your path to reduce dependency on AD—as it is effectively being used as your ESR today.

BEST PRACTICE #5: INCORPORATE HETEROGENEOUS DEVICES

Identity in the cloud needs to work seamlessly for users of traditional business endpoints, personal devices and anything that fits somewhere in the middle. And as part of moving away from dependence on AD, it's necessary to incorporate every possible device necessary to ensure a positive end user experience and security posture regardless of the devices end users choose to use with your identity platform.

The challenge is that mobile OSes generally are not designed with business needs in mind, they are often insecure (from a corporate perspective), and they are largely out of the control of IT. What is needed is a way to create a controlled environment on any device that can facilitate authentication, and provide secure access to corporate applications and resources without requiring that the device be within a traditional network perimeter. This is where using Unified Endpoint Management (UEM) that is integrated into your identity platform solves the problem.

Besides the fact that you can provide "anytime, anywhere, any device" access to your entire organization, there are a number of benefits to using a combination of UEM and your identity platform:

- **Security:** The very same authentication methods and access management controls in place for your traditional endpoints are enforced on a mobile device, creating a secure environment in which to work, regardless of the device used.

- **Visibility:** IT regains the ability to see who is connecting, on which device, from which network, wanting to run what application.

- **Control:** In essence, the use of UEM makes the device the perimeter. So, within the UEM application, IT has full control over whether a user can log on, use an application or access resources.

- **Productivity:** If properly designed, a seamless user experience between traditional endpoints and mobile devices is achieved for every part of the process, from authentication to access.

UEM that is integrated with AD usually lacks the needed native integrations with cloud applications and is solely focused on delivering on-premises applications. Using an UEM solution that integrates with your identity platform is yet another step in reducing reliance on AD while improving access to cloud applications and those on-premises applications that have been modernized.

ELIMINATING YOUR NEED FOR AD

You have relied on AD for two reasons: First, it is *all you have known* for years and, second, it's *all you have needed.* But as the need to remain competitive increases, organizations like yours are forced to consider a shift to the cloud. The cloud's evolution exposes the harsh truth that *on-premises AD is no longer truly adequate*.

The use of a cloud-based identity platform provides the opportunity to move identity and access management to the cloud, but it also requires your organization's willingness to let go of AD. It is going to take time and effort to fully implement a cloud identity platform, but the first step is to begin to move away from AD.

By following the best practices in this report, you will be taking steps to eliminate the need for AD by changing the way you *think* about AD's role; identifying *what you need* from cloud identity to simplify the transition; *moving identities* in the cloud that should not really still be on-premises; *leveraging an ESR* that ensures accurate, consistent and current data throughout the environment; and extending the centralized control and accessibility *to every device*.

As you search for a cloud identity platform that will meet your needs, consider asking the following questions:

1. **Does your identity platform *require* AD?** (You want to hear a resounding *"No"*)

2. **Does it *support* AD?** (It should, as you will need time to shift completely off of AD)

3. **Does it integrate with the cloud applications we use?** (Consider your list here)

4. **Can we manage employee, customer, contractor and partner identities?** (Yes)

5. **Can we leverage our HRMS as the employee system of record?** (Yes)

6. **Which devices can we use to extend our use of your identity platform?** (All of them)

Nick Cavalancia *is a contributing analyst with Redmond Intelligence and a Microsoft Most Valuable Professional (MVP). Cavalancia has more than 25 years of IT experience, which includes having owned a managed services provider company focused on small and midsize businesses and an enterprise IT consulting company.*

ABOUT REDMOND INTELLIGENCE

Redmond Intelligence provides independent and objective research and advisory services to technology buyers and vendors in the Microsoft ecosystem. Written by technical subject matter experts, Redmond Intelligence reports dive into the details of the Microsoft stack to provide actionable insights and concrete guidance. Projects range in scope from Solution Spotlights covering products in the Microsoft ecosystem to survey-based research reports to custom papers. For more information, visit *RedmondIntelligence.com*.

ABOUT THE SPONSOR

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,000 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 6,500 organizations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers.

To learn how Okta can help you reduce dependency on Active Directory, read the Increase Business Agility by Reducing Your AD Footprint blog, watch the Minimize Active Directory Dependency webinar or visit okta.com.