WHITE PAPER

Office 365 Single Sign-On: High Availability without High Complexity

For most organizations, the move to Office 365 (O365) is a leap forward in user experience, productivity, it simplification, and savings. But organizations that fail to implement Single Sign-On (SSO) reliably can slip backwards in several key areas. Risk can actually increase and productivity suffer.

Abstract

This technology brief will explain why highly reliable SSO between your on-premise network and O365 is so important, why that implementation is surprisingly difficult to achieve using the accessory tools provided with O365, and how Centrify leverages your preexisting, multiple-site Active Directory (AD) infrastructure to make SSO reliable yet simple.

Every Organization Needs Reliable SSO With O365

A distinction is often made between "enterprise" technologies that are appropriate only for large enterprises and those that are practical and valuable to small and medium businesses (SMBs) as well. SMBs often view this distinction differently than technology vendors. A great example is the effort, complexity, and expense required to provide SSO between on-premise networks and O365 and even more so to make it highly reliable.

Out of the box, O365 requires a separate user account and group administration. This requirement is an immediate step backward for end users, IT staff, and the organization as a whole. End users now need to remember or attempt to synchronize two passwords instead of one. End users must enter their credentials multiple times: once to access their workstation and on-premise servers and again to access O365. If they close their browsers, they must re-authenticate the next time they access the cloud.

IT staff must now provision not one AD account for new hires but also an additional account in O365. With each department's information split between on-premise applications and the cloud, IT finds itself maintaining duplicate group memberships between the two environments. Redundant user accounts and groups have been repeatedly demonstrated not only to increase work and degrade user experience but also inevitably to create risk as entitlements become outdated and credentials fail to be revoked. Such problems were big issues more than a decade ago, before AD gained its current ubiquity and enabled organization to centralize identity information within their networks.

But organizations that roll out a basic ADFS implementation create a perilous single point of failure which can render O365 inaccessible to users even when the O365 service itself is fully operational.

Obviously, SSO with O365 is required for any organization with on-premise IT, regardless of size, if the organization plans to avoid these problems during its move to the cloud. Microsoft offers SSO between on-premise and O365 with Active Directory Federation Services (ADFS) a native component of Windows Server and the dirsync utility which provides synchronization between AD and Office 365.

ADFS High Availability is Out of Reach

One of the benefits of O365 is the high availability that automatically comes with the cloud. Many organizations would never migrate to the cloud unless O365 could meet or exceed their current availability commitment. For other organizations, O365's availability is a key value proposition that motivates the switch.

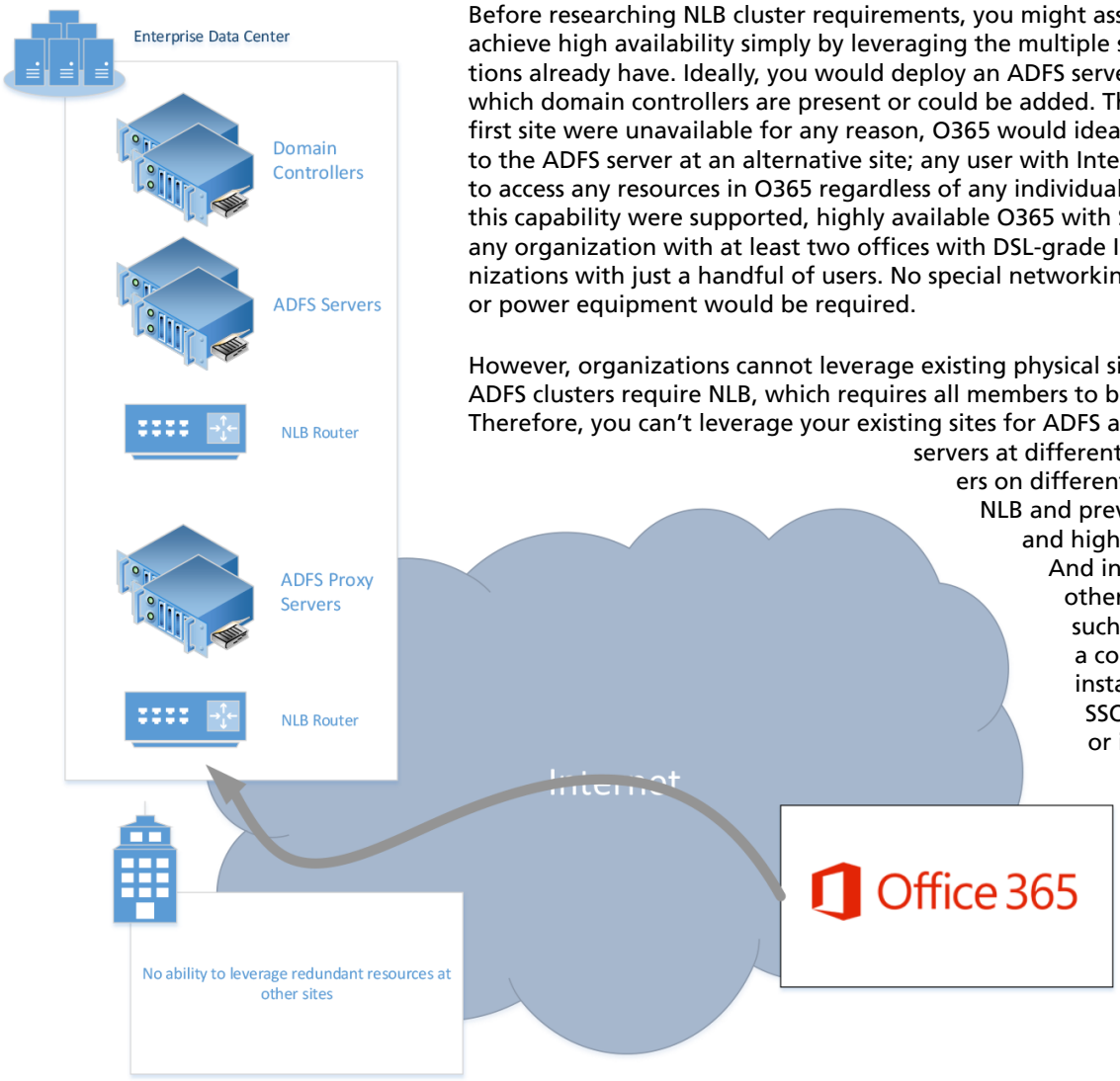
Therefore, organizations need SSO *and* high availability. However, implementing a highly reliable SSO for O365 with ADFS is simply not an option for most organizations. High-availability ADFS relies on Network Load Balancing (NLB) clusters, which require cluster members to be on the same subnet[1]. This key requirement for ADFS high availability creates several issues that make it impractical for all but the largest organizations. Even then, ADFS high availability is questionable.

But organizations that roll out a basic ADFS implementation create a perilous single point of failure which can render O365 inaccessible to users even when the O365 service is fully operational.

In this brief we make 2 two assumptions that apply to most organizations:

- The organization has at least two physical sites (e.g., offices, branches, data centers) that are connected by VPN or WAN.
- If one site fails for any reason, management requires O365 to remain available to
    - users at other sites that are still operational,
    - telecommuters,
    - users at the first site who can move to an alternate location.

1. http://technet.microsoft.com/en-us/library/hh831698.aspx



Before researching NLB cluster requirements, you might assume that you could achieve high availability simply by leveraging the multiple sites that most organizations already have. Ideally, you would deploy an ADFS server at two or more sites in which domain controllers are present or could be added. Then again, if ADFS at the first site were unavailable for any reason, O365 would ideally automatically failover to the ADFS server at an alternative site; any user with Internet access would be able to access any resources in O365 regardless of any individual physical site's status. If this capability were supported, highly available O365 with SSO would be in reach of any organization with at least two offices with DSL-grade Internet—even small organizations with just a handful of users. No special networking hardware, WAN services, or power equipment would be required.

However, organizations cannot leverage existing physical sites in this way because ADFS clusters require NLB, which requires all members to be on the same IP subnet. Therefore, you can't leverage your existing sites for ADFS availability. Placing ADFS servers at different sites places those servers on different subnets, thus breaking NLB and preventing ADFS clustering and highly available SSO to O365. And in case you are wondering, other manual cutover scenarios such as retargeting O365 to a completely different ADFS instance or simply turning off SSO are either unsupported or impractical.

The crux of the problem is twofold:

NLB does not protect against problems that affect the entire site.

Such problems include power outages, Internet connection failures, and disasters such as fire and flood. Only the largest organizations house an enterprise data center in a hardened physical building, in a region with low incidence for disaster and with redundant power systems, redundant Internet connections entering the building from opposite sides of the block, fire suppression systems, and all the other related technologies that are required for a single data center to remain operative under any condition.

NLB does not permit the deployment of ADFS servers at different sites.

This issue is vexing because if you have two locations connected by VPN with a domain controller at both locations, you have the makings for high availability. The more physically separate the two sites, the more independent their power, Internet connectivity, and physical disaster probability. Even two offices in the same region can usually use different Internet providers and purchase inexpensive battery backup systems.

The good news is that you can achieve highly available SSO for Office 365 without ADFS.

High Availability Isn't the Only Issue with ADFS

Besides the difficulty of achieving high availability, ADFS has other issues:

- 4 servers required. Two clustered servers in the DMZ; two clustered servers behind the firewall
- Required hole in firewall
- Required third-party certificates
- Time: One to two weeks for Office 365; days to weeks for additional apps
- ADFS is free as part of a Windows Server license but additional hardware and services can easily cost $25,000 or more

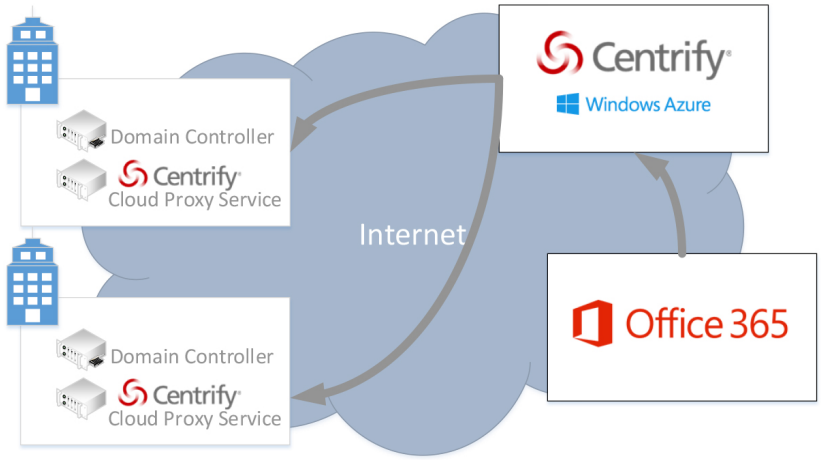
Centrify for Office 365

Centrify for Office 365 completely eliminates the need for ADFS and Dirsync.

Centrify for Office 365 completely eliminates the need for ADFS and dirsync. Centrify easily leverages your existing sites to provide highly available SSO to O365, allowing your users to continue working regardless of what happens at different locations.

To achieve reliable SSO for O365, simply follow these steps:

1. Register for the Centrify Cloud Service.
2. Perform the 5-minute Centrify cloud proxy service install at each site using (optionally) existing Windows.



Centrify then automatically configures O365 to use the Centrify Cloud Service to authenticate your users.

Centrify for Office 365 is a Microsoft-validated, Azure-based service that offers the industry's most easy-to-deploy and comprehensive solution for AD-based SSO, user provisioning, and mobile management. End users will love the SSO and self-service features. IT will love the centralized access control and visibility. And Centrify supports hundreds of other Software as a Service (SaaS) apps, so your users can get secure SSO to all your cloud-based applications.

Challenges	With ADFS	With Centrify
Additional hardware	Two clustered servers in the demilitarized zone (DMZ); two clustered servers behind the firewall	None
Firewall reconfiguration	Required hole in firewall	None
Third-party certifications	Required	None
Support for additional SaaS apps	Required individual configuration and debugging	A rich catalog of pre-integrated apps
Time to implement	1 to 2 weeks for Office 365; days to weeks for additional apps	Less than an hour for Office 365 or any other app
Total expense	Up to and in excess of $25,000 for additional hardware and services	Free for up to 3 apps

Centrify provides a complete, Microsoft-validated replacement for ADFS and DirSync for Office 365 SSO. ADFS and DirSync require specialized knowledge and significant investments in high-availability clustered servers, both inside the firewall and in the DMZ. Centrify for Office 365 delivers direct, seamless integration with AD in minutes, without additional time and expense to install and configure new infrastructure.

Centrify automatically includes additional benefits, such as a secure browser SSO via a user portal, user self-service, and one-click mobile access to SaaS apps. Centrify's solution for Office 365 SSO has passed Microsoft's rigorous "Works with Office 365" validation process.

Try Centrify for Office 365 today by starting here: https://www.centrify.com/cloud/cloud-service-registration.asp.

About Centrify

Centrify provides Unified Identity Services across data center, cloud, and mobile—resulting in one single login for users and one unified identity infrastructure for IT. Centrify's software and cloud services let organizations securely leverage their existing identity infrastructure to centrally manage authentication, access control, privilege management, policy enforcement, and compliance across on-premise and cloud resources. More than 4,500 customers have deployed Centrify across millions of servers, applications, and mobile devices to optimize costs and increase agility and security. With Centrify, organizations are reducing their costs associated with identity lifecycle management and compliance by more than 50 percent.

Founded in 2004 by Tom Kemp, Adam Au, and Paul Moore, Centrify is headquartered in Sunnyvale, California, with additional development and regional offices in Seattle, Hong Kong, London, Munich, Brisbane, and Sao Paulo. Centrify is a privately held company backed by top-tier venture capital firms Mayfield, Accel Partners, INVESCO Private Capital, Sigma West, and Index Ventures. These investors have funded some of the world's most successful technology companies, including Citrix, Facebook, Veritas, JBoss, MySQL, Riverbed, and Skype. Our partners include Microsoft, Samsung, Apple, Red Hat, Canonical, and others. To date, the company has more than 4,500 customers, including nearly half of the Fortune 50.

Since releasing its initial product in 2005, Centrify has expanded its portfolio from one product to a suite of software and cloud services that span your data center, cloud, and mobile environment with comprehensive support for more than 400 systems and 1,000+ applications. Benefits of the Centrify offering include:

Centrify Your Users. Gives users the single login users want.

Centrify Your Security. Apply the same identity policies across data center, cloud, and mobile.

Centrify Your IT. Leverage Active Directory to centrally manage data center, cloud, and mobile.

As organizations increasingly supplement and replace their on-premise IT infrastructure with cloud and mobile platforms, Centrify believes efficiently and securely managing user's digital identities in this hybrid IT environment becomes even more important. Our vision of delivering unified identity services that centrally manage identities across data center, cloud, and mobile is integral to every product and solution we develop. We believe the end result of one single login for users and one unified architecture for IT is a compelling value proposition for you and your organization. To learn more, check out our Products and Solutions pages today.

About Randy Franklin Smith

Randy Franklin Smith is an internationally recognized expert on the security and control of Windows and Active Directory security. Randy publishes www.UltimateWindowsSecurity.com and wrote The Windows Server 2008 Security Log Revealed—the only book devoted to the Windows security log. Randy is the creator of LOGbinder software, which makes cryptic application logs understandable and available to log-management and SIEM solutions. As a Certified Information Systems Auditor, Randy performs security reviews for clients ranging from small, privately held firms to Fortune 500 companies, national, and international organizations. Randy is also a Microsoft Security Most Valuable Professional.

Disclaimer

UltimateWindowsSecurity.com is operated by Monterey Technology Group, Inc. Monterey Technology Group, Inc. and Centrify Corporation make no claim that use of this whitepaper will ensure a successful outcome. Readers use all information within this document at their own risk.

Contact Centrify

CENTRIFY HEADQUARTERS
SUNNYVALE, CALIFORNIA
+1 (408) 542-7500

WEB
www.centrify.com

EMAIL
info@centrify.com

CENTRIFY EMEA
+44 (0) 1344 317950

CENTRIFY ASIA PACIFIC
(+61) 1300 795 789

CENTRIFY LATIN AMERICA
+55-11-9999-10156

