Centrify®

WHITE PAPER

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

Contents

Abstract

For most organizations, the move to Office 365 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 increases and productivity suffers.

This white paper will explain why highly reliable SSO between your on-premises network and Office 365 is so important, why that implementation is surprisingly difficult to achieve using the accessory tools provided with Office 365, and how Centrify leverages your preexisting, multiple-site Active Directory (AD) infrastructure to make SSO reliable yet simple.

Every Organization Needs Reliable SSO With Office 365

A distinction is often made between "enterprise" technologies that are appropriate only for large enterprises, and those that are also practical and valuable to small and medium businesses (SMBs). SMBs often view this distinction differently than technology vendors. A great example is the effort, complexity, and expense required to provide highly reliable single sign-on (SSO) between on-premises networks and Office 365.

> "Organizations that roll out a basic AD FS implementation create a perilous single point of failure that can render Office 365 inaccessible to users, even when the Office 365 service itself is fully operational."

Out of the box, Office 365 requires a separate user and group administration accounts. This requirement is an immediate step backwards 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 twice: once to access their workstation and on-premises servers and again to access Office 365. If they close their browsers, they must re-authenticate the next time they access the cloud.

IT staff must now provision Active Directory (AD) account for new hires, and an additional account in Office 365. With each department's information split between on-premises applications and the cloud, IT finds itself maintaining duplicate group memberships between the two environments. Maintaining redundant user accounts and groups increase work and degrade user experience, and create risk as entitlements become outdated, and credentials fail to be revoked.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.

Single sign-on to Office 365 is required for any organization with on-premises IT, regardless of size, if the organization plans to avoid user account synchronization problems during its move to the cloud. Microsoft offers SSO between on-premises networks and Office 365 with Active Directory Federation Services (AD FS)—a native component of Windows Server—and the DirSync utility, which provides synchronization between AD and Office 365.

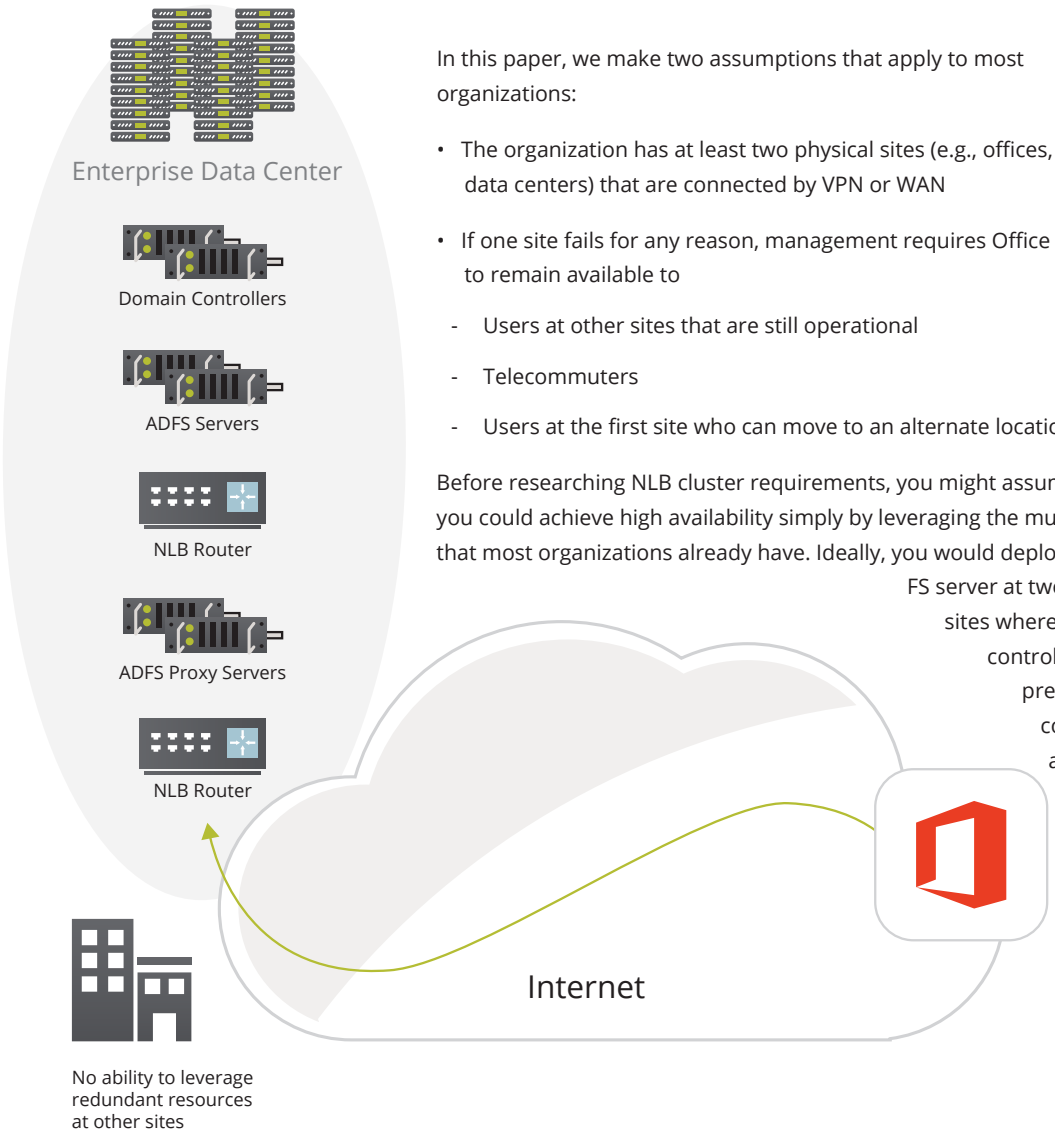
AD FS High Availability is Out of Reach

One of the benefits of Office 365 is the high availability that automatically comes with the cloud. Many organizations would never migrate to the cloud unless Office 365 could meet or exceed their current availability commitment. For other organizations, Office 365's availability is a key value proposition that motivates the switch.

Therefore, organizations need SSO and high availability. However, implementing highly reliable SSO for Office 365 with Active Directory Federation Services (AD FS) is simply not an option for most organizations. High-availability AD FS relies on Network Load Balancing (NLB) clusters, which require cluster members to be on the same subnet.[1] This key requirement for AD FS high availability creates several issues that make it impractical for all but the largest organizations. Even then, AD FS high availability is questionable.

Organizations that roll out a basic AD FS implementation create a perilous single point of failure that can render Office 365 inaccessible to users—even when the Office 365 service is fully operational.

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



In this paper, we make 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 Office 365 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

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 AD FS server at two or more sites where domain controllers are present or could be added.

If AD FS at the first site were unavailable for any reason, Office 365 would ideally automatically failover to the AD FS server at an alternative site. Any user with Internet access would be able to access any resources in Office 365 regardless of the status of any individual physical site. If this capability were supported, highly available Office 365 with SSO would be in reach of any organization with at least two offices with DSL-grade Internet—including small organizations with just a handful of users. No special networking hardware, WAN services, or power equipment would be required.

However, in reality, organizations cannot leverage existing physical sites in this way, because AD FS clusters require Network Load Balancing, which requires all members to be on the same IP subnet, or the VLAN must be extended across both sites—not a networking best practice.

Therefore, you can't leverage your existing sites for AD FS high availability. Placing AD FS servers at different sites puts those servers on different IP subnets, thus breaking NLB, and preventing AD FS clustering and highly available SSO to Office 365.

High Availability Isn't the Only Issue with AD FS

AD FS typically requires the following:

- Four servers: Two clustered servers in the DMZ, two clustered servers behind the firewall
- Various ports opened in the firewall
- Third-party certificates
- Setup time: One to two weeks for Office 365; days to weeks for additional apps
- AD FS is free as part of a Windows Server license but additional hardware and services can cost $25,000 or more

And in case you are wondering, other manual cutover scenarios such as retargeting Office 365 to a completely different AD FS instance, or simply turning off SSO are either unsupported or impractical.

The crux of the problem is twofold:

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

NLB doesn't protect against problems like 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.

2. NLB does not permit the deployment of AD FS 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 AD FS.

Centrify Identity Service for Office 365

Eliminating the need for AD FS and DirSync

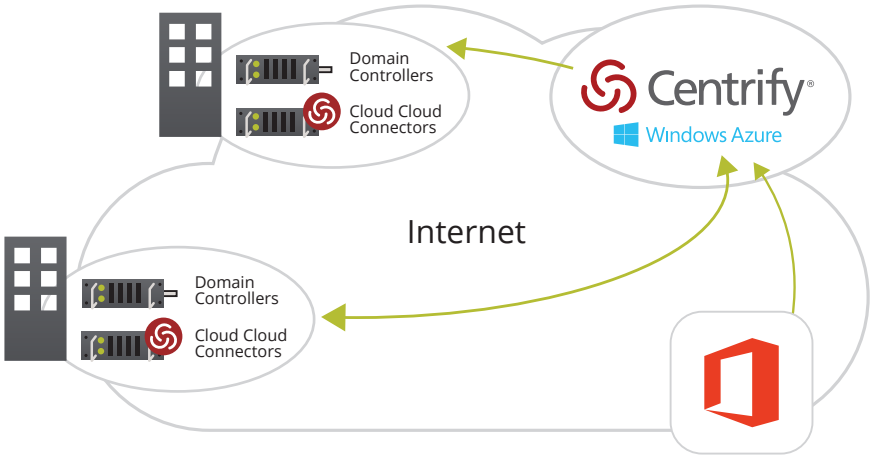
Centrify Identity Service for Office 365 completely eliminates the need for AD FS and DirSync. Centrify easily leverages your existing sites to provide highly available SSO to Office 365, allowing your users to continue working, regardless of what happens at different locations.

To achieve reliable SSO for Office 365, simply follow these steps:

1. Register for the Centrify Identity Service.
2. Perform the 5-minute Centrify Cloud Connector installation at each site using (optionally) existing Windows.

Centrify then automatically configures Office 365 to use the Centrify Cloud Service to authenticate your users.

Centrify Identity Service for Office 365 is a Microsoft-validated, Azure-based service that offers the industry's most easy-to-deploy and comprehensive solution for single sign-on using an organization's existing directory service (Active Directory, Centrify Cloud Directory, or both). It also provides 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 secure single sign-on to both cloud apps and on-premises apps.



Challenges	With AD FS	With Centrify
Additional hardware	Two clustered servers in the demilitarized zone (DMZ); two clustered servers behind the firewall	None
Firewall reconfiguration	Requires various ports be opened in the firewall	None
Third-party certifications	Required	None
Support for additional cloud or on-premises 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

Single sign-on to Office 365

Centrify provides a complete, Microsoft-validated replacement for AD FS and DirSync for Office 365 SSO. AD FS and DirSync require specialized knowledge and significant investments in high-availability clustered servers, both inside the firewall and in the DMZ. Centrify Identity Service 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 secure browser SSO via a user portal, user self-service, and one-click mobile access to cloud and on-premises apps. Centrify's single sign-on solution for Office 365 has passed Microsoft's rigorous "Works with Office 365" validation process.

Try Centrify Identity Service for Office 365 today by starting here:
https://www.centrify.com/free-trial/identity-service-form/

About Centrify

Centrify provides unified identity management across data center, cloud and mobile environments that result in single sign-on (SSO) for users and a simplified identity infrastructure for IT. Centrify's unified identity management software and cloud-based Identity-as-a-Service (IDaaS) solutions leverage an organization's existing identity infrastructure to enable single sign-on, multi-factor authentication, privileged identity management, auditing for compliance and enterprise mobility management.

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 per- forms 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.

SANTA CLARA, CALIFORNIA	+1 (669) 444-5200
EMEA	+44 (0) 1344 317950
ASIA PACIFIC	+61 1300 795 789
BRAZIL	+55 11-3958 4876
LATIN AMERICA	+1 305 900 5354
EMAIL	sales@centrify.com
WEB	www.centrify.com