

Seamless Simplicity

Domain Services for Windows Now Supported in Novell Open Enterprise Server 2

This article first appeared in the October 2008 issue of *Novell Connection* magazine.

Novell Open Enterprise Server 2 Support Pack 1 will include the much anticipated Domain Services for Windows service, another significant element that provides greater simplicity and interoperability. (See Figure 1.) Last year, *Novell Connection* magazine provided an in-depth look at how this new component would deliver seamless cross-authentication between Windows Active Directory environments and Linux eDirectory environments for file and print services. (See [Domain Services for Windows](#).) This article extends that discussion by providing you with guidance on when you should take advantage of this new service.

Since one of the main benefits of Domain Services for Windows is the ability to authenticate to a Novell Open Enterprise Server 2 Linux server without the Novell client, some might wonder how Domain Services for Windows differs from the CIFS protocol support also included in this upcoming support pack. (See [We Are Here For You](#).) The answer is that CIFS aids users who want basic access to the Linux file system using a Windows share without all the overhead of an Active Directory-style presentation. In other words, users don't need the Microsoft Management Console or Windows Group Policy support; they just want to be able to map a drive. (See Figure 2.)

However, Domain Services for Windows is for organizations that want to consistently present their users with a complete Active Directory-style environment, regardless of whether those users need to access Linux servers or Windows servers. In fact, the basic premise behind Domain Services for Windows is the power to enable a Novell Open Enterprise Server 2

Linux server to appear as if it is an Active Directory server. This ability allows users to log in and authenticate to an Active Directory server with a native Windows client using their eDirectory usernames and passwords. In environments with both eDirectory and Active Directory, administrators can create a cross-domain trust between these identity stores that allows cross-forest authentication and authorization. (See Figure 3.)

> Why Should I Use Domain Services for Windows?

For many organizations, the ability to standardize on an Active Directory-style desktop environment can be a significant benefit. By no longer using the Novell client and moving to a completely native Windows desktop environment, you can simplify desktop image management and reduce its related costs. For example, you might have a mixed environment with a set of Novell Open Enterprise Server users, a set of Microsoft Windows Server users, and yet a third set of users leveraging both. If this is the case, you likely have to maintain a separate image library for each set of users at considerable cost and effort.

In this scenario, Domain Services for Windows can dramatically decrease your complexity and maintenance costs by allowing you to standardize on a single Windows desktop image. You would no longer need a separate image for your Novell—or mixed Windows and Novell—environments, because your users could authenticate to either server type using a completely native desktop Windows environment.

In addition to simplifying image library management for administrators, Domain Services for Windows can deliver productivity gains to your users. Since you can use Domain Services for Windows to create a cross-domain trust between Active Directory and eDirectory, your users no longer have to authenticate separately to the different back-end environments. They just authenticate once and can then access files on either their Linux or Windows servers. Some additional benefits of the new functionality of Domain Services for Windows surfaced during beta testing. One benefit involves applications that require an Active Directory domain for authentication. While Novell hasn't fully tested this capability, it appears that certain applications requiring Active Directory authentication can seamlessly authenticate to Domain Services for Windows, thus providing a single sign-on capability for users. When you authenticate to Domain Services for Windows, these applications will recognize the Domain Services for Windows credentials as authentic and automatically log you into the application without prompting you again for your username and password. Novell has verified this

Figure 1: *Novell Domain Services for Windows is installed as a Add-on Product from within the YaST install*

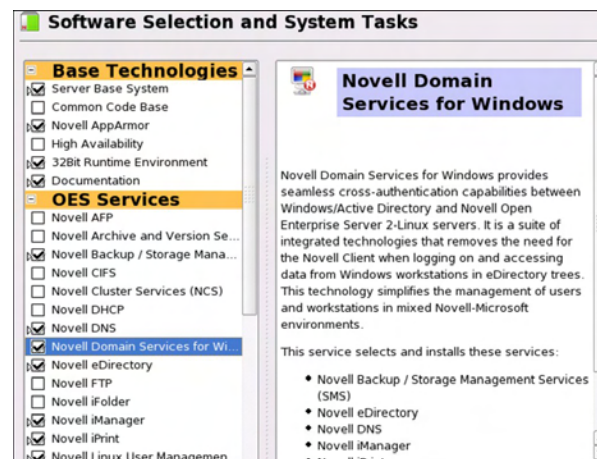
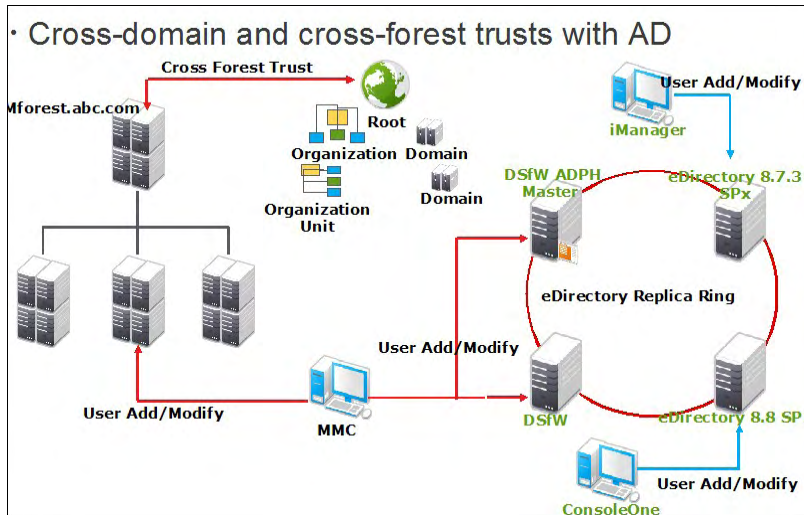


Figure 2: You can manage Novell Domain Services for Windows environments with both Novell iManager and Microsoft Management Console



behavior on both Citrix Presentation Server and a NetApp filer application, and preliminary investigations indicate that similar types of applications may behave this way as well.

> Things to Consider

If your organization wants to present an Active Directory-style authentication for both your Linux and Windows servers, Domain Services for Windows offers very definite benefits. But keep in mind some considerations before taking advantage of its functionality:

The first consideration deals with dependencies on login scripts. When using Domain Services for Windows, you no longer use the Novell client, thus eliminating Novell login scripts. A lack of log-in scripts might not be a problem for your organization, but some users have very elaborate and powerful login scripts that they rely on to set up their user environment just the way they like it. While you can recreate the login script functionality with the Microsoft Group Policy Editor, there is currently no import or export capability to facilitate this process. You would need to recreate these scripts for each user moving to an Active Directory-style login.

Another consideration, although a fairly minor one for most, is that without the client, users cannot use the *purge* and *salvage* commands. *Salvage* has long given users the

ability to view and recover files they've deleted from a Novell Storage Services volume. Of course, even though a clientless user loses the salvage capability, there is nothing to keep an administrator from recovering these lost files for a user. *Purge* is the *salvage* command's lesser-used cousin. It allows users to permanently delete their files. Once again, even though users cannot use this command, administrators can still purge files as needed.

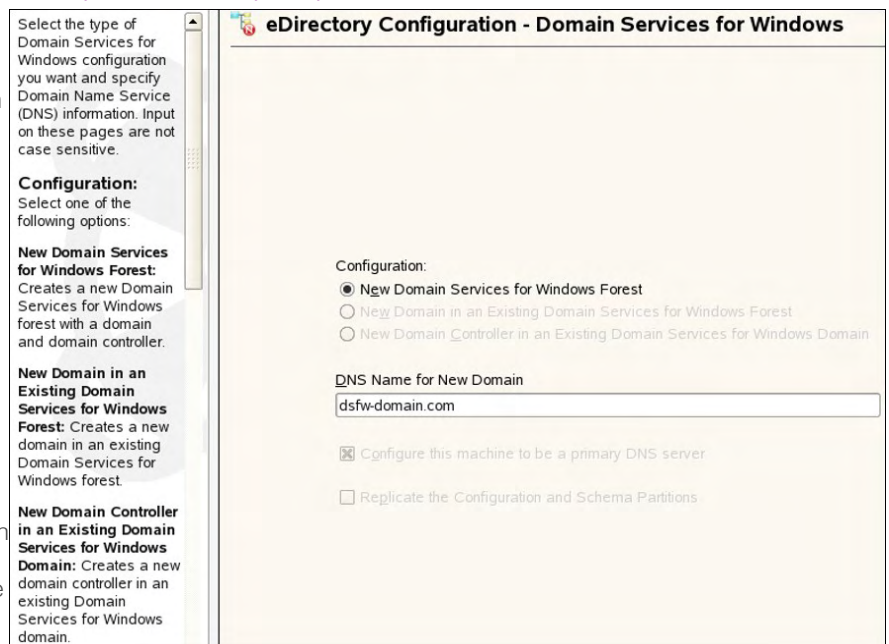
In addition to losing access to the *purge* and *salvage* commands, without the client, users also lose the ability to set the *delete inhibit* and *rename inhibit* Novell Storage Services file system rights. With the *delete inhibit* attribute, a file can be opened, viewed, edited, saved, renamed and copied, but it cannot be deleted. With the *rename inhibit* attribute, a file can be opened, viewed, edited, saved, copied

and deleted, but it cannot be renamed. It should be noted that, if these attributes have already been set, they will still be enforced whether users have the client or not. But without the Novell client, users cannot assign these settings to a file.

Simply put, just determine if your users rely on these commands or attributes as you decide if or how you'll take advantage of Domain Services for Windows.

Another consideration that you should make before deploying Domain Services for Windows is whether or not

Figure 3: With Novell Domain Services for Windows you can create a cross-domain trust between eDirectory and Active Directory identity stores that allows cross-forest authentication and authorization



your users need access to NetWare servers or previous versions of Linux servers running Novell Open Enterprise Server. To access these servers, users will need the Novell client, or the servers will need to be configured with CIFS support.

One final consideration deals with LDAP. When you communicate via LDAP to a server that has been configured as a Domain Services for Windows server, it will communicate back using Active Directory-style LDAP instead of eDirectory-style LDAP. This isn't typically a problem for most simplistic LDAP operations such as authentication, but there are a number of Novell applications, such as GroupWise, that expect eDirectory-style LDAP responses.

However, there are a few ways you can get around this issue. The first way is to simply change the port assignments on the calling application to point to a different port on the Domain Services for Windows server—one that is configured to provide eDirectory-style LDAP responses. Another method is to configure the calling application to communicate instead with a different server

running eDirectory. The third method would be to add a request control to force the Domain Services for Windows server to return eDirectory-style LDAP communications.

> **Tell Us What You Want**

Based on its original design criteria, Domain Services for Windows delivers exactly what it promises: a method to authenticate to a Linux server using standard Windows protocols that carries over to a Windows Active Directory environment. You've seen in this article, the solution also delivers some additional benefits, and as testing and usage of the service continues, more benefits will surface. Even more important, Novell plans to continue to develop and improve the service to better meet your needs. In fact, Novell wants to hear how you would like to see Domain Services for Windows enhanced. Download the open beta at www.novell.com/beta, test drive the service, and then send your ideas to dsfw-feedback@novell.com so you can enjoy the benefits of even greater interoperability and simplicity tailored to your needs. **N**