Technical White Paper
DESKTOP

www.novell.com

Using SUSE® Linux Enterprise Desktop with Microsoft* Active Directory* Infrastructure

Novell®

Table of Contents:

Simplifying Management, Security and Usability in a Heterogeneous IT Environment

SUSE Linux Enterprise Desktop 10 is the only enterprise-class Linux desktop operating system designed to allow direct integration with Windows domains—giving you a heterogeneous environment that behaves like a unified network for both users and administrators.

Heterogeneous IT environments are a fact of life. Today's information-driven enterprises have grown up with Microsoft* and have come to depend heavily on Microsoft operating systems. And that means they have had to work hard to integrate home-grown, legacy and proprietary solutions within a predominantly Microsoft environment.

Today, Linux* and open source software promise to transform IT economics, security and functionality for companies looking for an alternative to Microsoft. But for the foreseeable future, many companies will only be able to implement open source software side by side with Microsoft, rather than as a rip-and-replace alternative. Or they may attempt to migrate to open source over time, gradually phasing out Microsoft platforms to avoid the cost and disruption of deploying a completely new IT infrastructure.

In either scenario, adding Linux to the mix threatens to make the IT environment more complex to manage and use, because the IT staff now has to deploy, retrain and maintain two separate environments for authenticating to the network and accessing services and resources.

One of the greatest attractions of the Microsoft environment is Active Directory*, which provides a hierarchical framework for managing, controlling access to and enforcing security for all Windows* objects on the network—resources, services and users. If only Active Directory could also be used to manage Linux-based objects, you would have a single point of administration for all Windows and Linux systems, while providing a single sign-on experience for users to access all the resources they need.

That's exactly what SUSE® Linux Enterprise Desktop 10 from Novell® allows you to do. It's the only enterprise-class Linux desktop operating system designed to allow direct integration with Windows domains—giving you a heterogeneous environment that behaves like a unified network for both users and administrators.

With SUSE Linux Enterprise Desktop 10, there's no complex synchronization or metadirectory scheme to maintain, and no need to administer two separate systems or deal with multiple vendors. There's no need to pay for a proprietary solution to install on top of your Linux OS. And there's no need to manage separate environments using separate tools.

Most important, your users have a single identity and a single, secure sign-on to access network services and resources no matter which operating system they're using—Windows or Linux.

Active Directory Integration: A Typical Scenario

Over the years, most enterprises have made a huge investment in Windows servers and workstations, using Active Directory to organize and manage the network, define workgroups, enforce authentication policies and assign privileges. At the same time, forward-thinking IT managers have kept an eye on the world of Linux and open source software, waiting for the day when enterprise-class, license-free solutions would emerge to offer significant cost savings and greater freedom of choice.

That day has arrived with SUSE Linux Enterprise Desktop 10—a general-purpose,

license-free desktop platform that provides unparalleled flexibility and performance for business users. SUSE Linux Enterprise Desktop 10 is designed to help businesses dramatically reduce costs, improve end-user security and increase workforce productivity. So now companies can choose from several options. They can ignore the new open source opportunities altogether and stick with the familiar Windows environment. They can migrate the entire IT environment to Linux.

Or—by far the most likely choice for a typical enterprise—they can keep much of their Windows infrastructure intact while migrating selected groups to Linux as time, budget and user roles allow. They may specify Linux for all new purchases, and replace older Windows machines with Linux at the end of the Windows lifecycle. Or they may identify operational areas where moving to Linux provides clear advantages, keeping Windows in other areas.

In each of these scenarios, the company is introducing Linux clients into an existing environment of Windows servers and clients to achieve specific business goals. By allowing newly deployed Linux systems to join the Windows domain, companies can minimize disruption for end users, allow single sign-on authentication and access without regard to OS type, keep a single IT management framework and enforce a single set of security policies.

Active Directory integration supports the business and IT goals that drive the decision to migrate to Linux in the first place: improving the match between technology and task, eliminating single-vendor dependence, easing the transition for users, improving security and—above all—cutting costs.

Active Directory integration supports the business and IT goals that drive the decision to migrate to Linux in the first place: improving the match between technology and task, eliminating single-vendor dependence, easing the transition for users, improving security and—above all—cutting costs.

Benefits of an Integrated Linux and Microsoft Environment

Integrating SUSE Linux Enterprise Desktop machines with Active Directory enables you to:

- *Make Linux clients behave as Windows clients, taking all account information from the Active Directory domain controller and seamlessly accessing services and resources within the Active Directory infrastructure*
- *Use single sign-on for secure access to a Windows domain, including Web servers, proxy servers, e-mail servers and other network services*
- *Tighten security by requiring users to remember just one login and password—with no need to reauthenticate against different servers*
- *Mount network shares to allow Linux users to work with data stored on Windows servers without having to provide user credentials separately for each share*
- *Share files and folders transparently between Linux and Windows workstations*
- *Manage all user accounts, authentication data and security policies centrally, with no need to touch every workstation or run separate consoles for each environment*
- *Ensure that account and password policies are enforced uniformly on both Windows and Linux clients*
- *Support offline authentication so that users can log on to their local machines even while they're unable to contact the domain controller—for example, while traveling—or when the Active Directory server is unavailable*
- *Avoid vendor lock-in with the freedom to choose the best platform for each user and application and to migrate at your own pace*
- *Reduce costs for licensing software, training users and managing the heterogeneous environment*

SUSE Linux Enterprise Desktop 10 ships with a choice of desktop environments: GNOME and KDE. Both of these desktops provide a familiar and convenient GUI that makes it easy for former Windows users to migrate to Linux and become quickly productive using conventional menus, dialogs and folders.

and—above all—cutting costs. To fulfill these needs while appealing to users and IT administrators formerly working in a Windows environment, a Linux solution must meet four essential criteria:

- *It must seamlessly integrate Linux-based client machines into a Windows domain.*
- *It should provide a desktop feature set substantially equivalent to the Windows desktop.*
- *It must provide an easy-to-use graphical user interface (GUI) that former Windows users can adopt with a minimal learning curve.*
- *It should require no configuration changes on the server side, retaining compatibility with the existing Windows infrastructure and minimizing disruption as users migrate.*

SUSE Linux Enterprise Desktop 10 is designed to meet all these criteria by enabling easy, complete integration with Active Directory. After a simple configuration, described later in this paper, a Linux client can log into the Windows domain as easily as a Windows client. Linux users then have the same authentication, file, print and other network functionality as Windows users.

SUSE Linux Enterprise Desktop 10 ships with a choice of desktop environments: GNOME and KDE. Both of these desktops provide a familiar and convenient GUI that makes it easy for former Windows users to migrate to Linux and become quickly productive using conventional menus, dialogs and folders. No modifications to Linux or the desktop environment are required, except for the simple client configuration that enables SUSE Linux Enterprise Desktop clients to join an existing Windows domain.

Core Components of the Active Directory Integration Solution

Let's take a closer look at the core technologies that enable easy integration of SUSE Linux Enterprise Desktop with Active Directory. In order for the Active Directory server and the Linux client to properly communicate, both sides need to adhere to two protocols:

- **LDAP.** *Lightweight Directory Access Protocol (LDAP) is widely used to structure, manage and query directory services over TCP/IP networks. It provides a hierarchical "tree" model for organizing objects in the directory, and allows you to create schemas that define object classes, and to assign attributes that define the members of each class. A Windows domain controller with Active Directory can use LDAP to exchange directory information with Windows clients—and, in this solution, with Linux clients. An open source version of LDAP, OpenLDAP, is used for integrating SUSE Linux Enterprise Desktop with Active Directory.*
- **Kerberos.** *Using symmetric-key cryptography mediated by a trusted third party, Kerberos allows clients and servers to mutually authenticate to one another and to communicate securely even over a public network. Because a client can trust Kerberos to reliably authenticate the identity of all other client devices, "kerberized" single sign-on solutions can grant access to any authorized service or resource on the network. And because Windows supports Kerberos, it can be used to enable single sign-on even for Linux clients authenticating to a Windows domain.*

In addition to the LDAP and Kerberos protocols, certain components on the client machine enable processing of account and authentication data. These core components include:

- **Winbind.** *Part of the Samba project, the winbind daemon handles all communication with the Active Directory server. Essentially, the winbind daemon binds the Linux workstation to the Windows domain, making the Linux client "look like" an ordinary Windows machine to the Windows server and eliminating the need for duplicate accounts and passwords.*
- **NSS.** *The Name Service Switch (NSS) provides a standardized programming interface for accessing all kinds of naming information on Linux systems, including users, groups, networks, hostnames and IP addresses. NSS is designed to allow the creation of separate modules to access naming information from various sources. The NSS module used in the Novell solution is nss_winbind, which interacts directly with the winbind daemon to access user and group names located on an Active Directory server.*
- **PAM.** *The Pluggable Authentication Modules (PAM) framework provides a set of libraries you can use to develop applications that rely on authentication, independent of the underlying authentication mechanism. The details of specific authentication mechanisms are implemented as separate plug-in modules. Different PAM modules can be "stacked" on one another to enable complex authentication/authorization scenarios. In the Novell solution, the pam_winbind module interacts directly with the winbind daemon to authenticate Linux users to the Windows domain using Kerberos. Stacked on top of pam_winbind, the pam_mkhomedir module is used to create the user's home directories after authentication has succeeded.*

With these components in place, each application that uses PAM for authentication purposes—including login, ssh and Gnome Display Manager (GDM) and KDE Display Manager (KDM)—can authenticate users against the Active Directory server.
‘

Kerberized applications—including file managers, Web browsers and e-mail clients—use the Kerberos credential cache created by pam_winbind during the authentication process to access Kerberos tickets for users, making them part of the single sign-on framework as well.

Novell is the only vendor that offers a complete, enterprise-class desktop that includes full Active Directory compatibility as a standard feature, rather than as an add-on that's difficult to configure and limited in functionality.

You can join an existing Active Directory domain during installation of SUSE Linux Enterprise Desktop, or you can join from a previously installed system by activating Windows user authentication using YaST.

This architecture, enabling single sign-on to the Windows domain for Linux machines and applications, is shown in the accompanying figure.

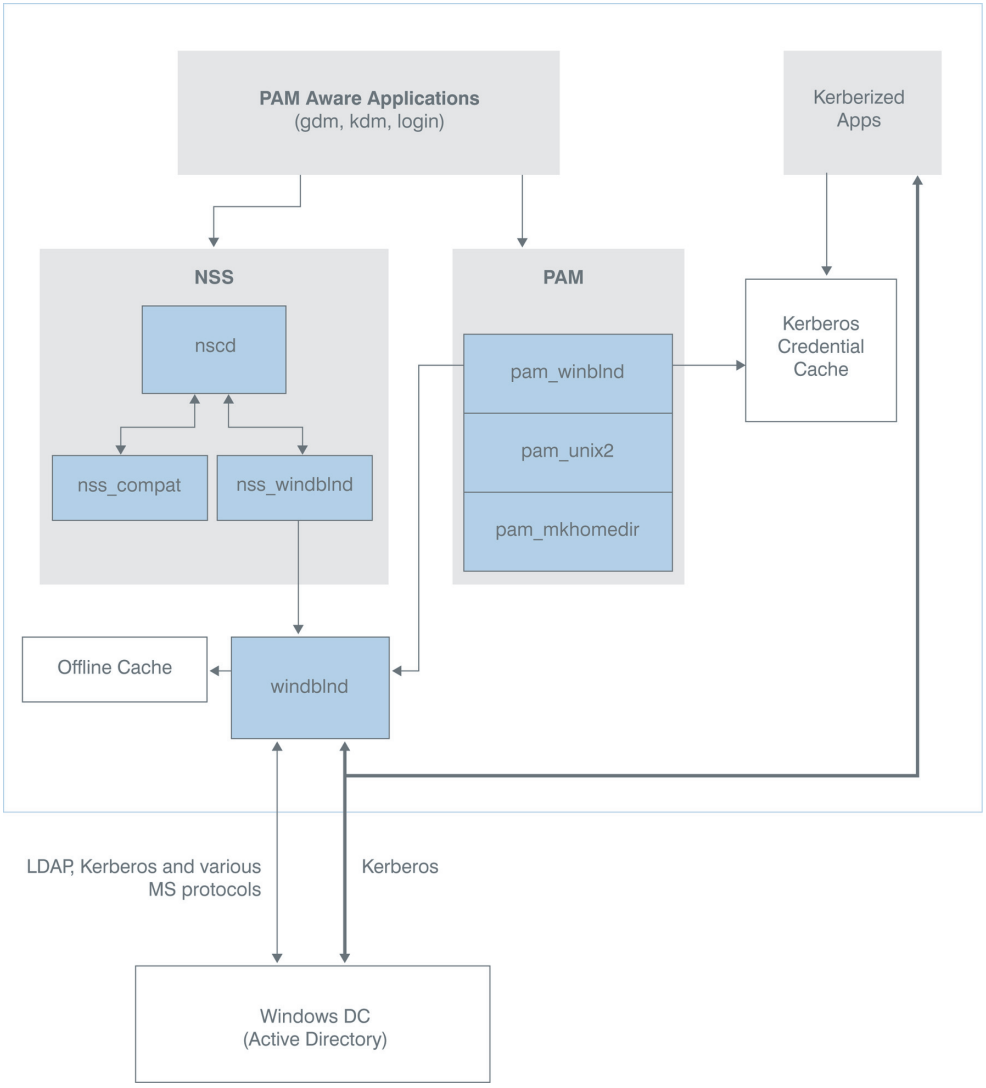

Figure 1. *Linux to Active Directory Authentication*

What Makes the Novell Implementation Different?

Other vendors offer solutions for integrating Linux machines with Active Directory. But Novell is the only vendor that offers a complete, enterprise-class desktop that includes full Active Directory compatibility as a standard feature, rather than as an add-on that's difficult to configure and limited in functionality. Active Directory integration within SUSE Linux Enterprise Desktop 10 offers several advantages over any other solution available today:

Full Integration with the Desktop Environment

All the components for full Active Directory integration are included in the standard desktop operating system. There's nothing else to buy or integrate.

- *Active Directory integration can be easily configured using the YaST Domain Membership module, which can be run either during the Linux desktop installation process or on a previously installed system.*
- *Both of the desktop display managers included in the solution—GDM and KDM—fully support authenticating against and logging into Active Directory domains. Users can enjoy full support for Active Directory in the desktop applications they use, whether working in a KDE or GNOME desktop environment.*
- *The solution offers full support in offline environments as well as online. The winbind daemon enforces password policies even in an offline state, reacting according to the policies configured in Active Directory and tracking failed login attempts. Valid Kerberos tickets that were acquired before losing the connection with the Active Directory server can still provide access to other network resources, and when a machine is completely disconnected, it can receive new Kerberos tickets immediately upon reconnecting. These offline capabilities are essential for users who roam between networks or who need to work in-flight or other places a network is unavailable.*

No Server-side Configuration

The SUSE Linux Enterprise Desktop solution for Active Directory integration works out of the box.

- *On the desktop side, only a simple configuration is required, which can be applied retroactively to Linux systems already in deployment. On the server side, Active Directory integration requires no change whatsoever from your current configuration.*
- *Competing solutions require modifications to the Active Directory domain controller and Domain Name System (DNS) server, and may require you to use particular versions and configurations of Web and application servers as well.*

Open Source

With SUSE Linux Enterprise Desktop, all tools and features for Active Directory integration are built using open source code.

- *Extensions to existing projects—such as Samba—that make the solution possible were finalized in close cooperation with the open source community, and have been embraced and integrated into the official open source code base by the appropriate project teams.*
- *The development model is transparent, and because the source code is available to anyone, there's a worldwide community of engineers working to find and fix any issues, add enhancements and ensure security. Open source code is subject to very broad testing and review, and thus any software bugs and security vulnerabilities are typically found and fixed much more quickly than in proprietary products.*

- *Other Active Directory integration solutions for Linux rely on proprietary source code, forcing you to trust a single vendor to provide reliable operation, future enhancements and timely security patches.*

Configuring SUSE Linux Enterprise Desktop as an Active Directory Client

For flawless interaction between client and server when joining an Active Directory domain, Novell recommends the following client-side configurations:

- **DNS.** *In a common Microsoft Windows environment, DNS is configured via Dynamic Host Configuration Protocol (DHCP). If DHCP does not provide the DNS information (for example, in a test environment), you can configure the Linux client manually to use a DNS server that can forward DNS requests to the Active Directory DNS server. Alternatively, you can configure the client to use the Active Directory DNS server as the name service data source.*
- **NTP.** *The Linux client must have its time set accurately in order to successfully authenticate via Kerberos. Novell recommends using a central Network Time Protocol (NTP) time server for this purpose. This can be the NTP server that's running on your Active Directory domain controller already. If the clockskew between your Linux host and the domain controller exceeds a specified limit, Kerberos authentication fails and the client is logged in using the weaker NT LAN Manager (NTLM) authentication.*
- **DHCP.** *If your client uses dynamic network configuration with DHCP, you should configure DHCP to provide the same IP and hostname to the client. The most foolproof way of doing this is to use static IP addresses.*
- **Firewall.** *To browse your network neighborhood, either mark the interface used for browsing as part of the internal zone, or else disable the firewall entirely. To change the firewall settings on your client, log in as root and start the YaST firewall module. Then do* one *of the following:*
  - **Option 1:** To make the interface part of the internal zone, select *Interfaces*. Select your network interface from the list of interfaces and click *Change*. Select *Internal Zone* and click *OK* to apply your settings. Exit the firewall module by choosing *Next*, then *Accept*.
  - **Option 2:** To disable the firewall, set *Service Start* to *Manually* and exit the firewall module by choosing *Next*, then *Accept*.

It is also possible to configure or disable the firewall during installation.

Active Directory Account

To log in to an Active Directory domain, you need a valid user account for the domain. This account is provided by the Active Directory administrator. Be prepared with the valid Active Directory username and password for a domain administrator account when you're ready to join the domain from your Linux client, as described below.

You can join an existing Active Directory domain during installation of SUSE Linux Enterprise Desktop, or you can join from a previously installed system by activating Windows user authentication using YaST. Let's take a look at the latter method—joining the Active Domain directory from an existing Linux desktop. Here are the steps:

1. Start YaST and provide your root (administrator) password.
2. Start Network Services _ Windows Domain Membership.
3. Enter the domain to join at Domain or Workgroup in the Windows Domain Membership screen.
   ≥ If the DNS settings on your host are properly integrated with the Windows

DNS server, enter the Active Directory domain name in its DNS format (msdomain.example.com).

If you enter the short name of your domain (also known as the pre-Windows 2000 domain name), YaST must rely on NetBIOS name resolution instead of DNS to find the correct domain controller. If the domain controller is on the same subnet as the Linux client, you can click *Browse* to list the NetBIOS domains and select the desired domain.

4. Check *Also Use SMB Information for Linux Authentication* to use Active Directory for Linux authentication.
5. Check *Create Home Directory on Login* to automatically create a local home directory for your Active Directory user on the Linux machine.
6. Check *Offline Authentication* to allow domain users to log in even if the Active Directory server is temporarily unavailable or a network connection is unavailable.
7. Click *Finish* and confirm the domain join when prompted.
8. Provide the password for a Windows domain administrator account on the Active Directory server and click *OK*.

That's all it takes to configure an existing SUSE Linux Enterprise Desktop 10 machine as an Active Directory desktop client. And it's even easier to perform the configuration when first installing Linux on a new or redeployed machine.

Logging In

You can now log in to the Active Directory domain from either a GNOME or KDE desktop by simply selecting the domain and entering the username and password.

Just as easily, you can log in using a text-based console by entering *DOMAIN\user* at the *login*: prompt and providing the password. And you can even log in to the Active Directory client machine remotely using SSH:

1. At the login prompt, enter:
   ssh DOMAIN\\user@hostname
   You can escape the \domain and login with another \sign.
2. Provide the user password.

Note that in all cases—GUI, text console or remote login—a single sign-on provides access to all the authorized services and resources in the Active Directory domain. And the same login can even authenticate users to their local machine while it's disconnected from the network—a useful feature for mobile and occasionally connected PCs.

Learn More About SUSE Linux Enterprise and Active Directory Integration

We've given you an overview of Active Directory support in SUSE Linux Enterprise Desktop 10, including what it does, how it's typically used, the benefits it provides to end users and the enterprise, core components, how to configure the solution and join the Active Directory domain and how to log in with single sign-on to access all authorized services and resources on the domain.

If this overview has sparked your interest, there's a lot more information available that lets you really get under the hood and learn all there is to know about this unmatched solution for integrating your heterogeneous Windows and Linux environment. To learn more, check out these resources:

For the IT Administrator

SUSE Linux Enterprise Desktop Deployment Guide, Chapter 11, "Active Directory Support"

For the End User

SUSE Linux Enterprise Desktop GNOME User Guide, Chapter 1, "Getting Started with the GNOME Desktop," Section 1.1.4, "Accessing Files on the Network"

www.novell.com

SUSE Linux Enterprise Desktop KDE User Guide, Chapter 9, "Accessing Network Resources," Section 9.4, "Managing Windows Files"

All of these documents are available on the Novell Web site at: www.novell.com/documentation/sled10/. And of course, you're always welcome to contact your Novell representative for more information.

Contact your local Novell Solutions Provider, or call Novell at:

1 888 321 4272 U.S./Canada
1 801 861 4272 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.
404 Wyman Street
Waltham, MA 02451 USA

Novell