Easy Active Directory integration with Likewise Open

STAYING ACTIVE

Likewise Open provides smooth integration with Active Directory environments. We show you how to install and configure the admin-friendly authentication system. **BY WALTER NEU**

The Likewise Open authentication system [1] integrates Linux clients with the Active Directory environment. Of course, you can also configure Active Directory through Samba and its supporting cast of characters [2], but the Likewise solution offers several benefits for easier configuration and administration.

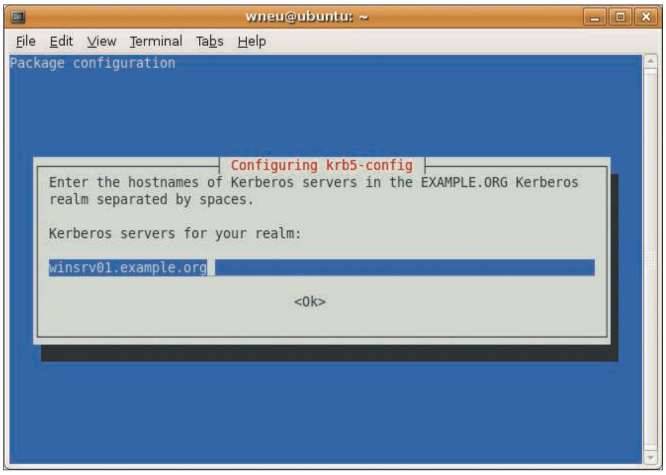
The free, GPL'd version of Likewise supports authentication against Active Directories, the authorization of kerberized services, and even single sign-on. This might sound a lot like Samba, which does the same things; in fact, the project manager of Likewise, Gerald Carter, is a long-term member of the Samba core developer team. Likewise Open builds on the work by Samba, although it adds many of its own features.

Ready-to-Run Packages

Likewise packages are available for Red Hat, Novell, and Canonical distributions, a couple of commercial Unix systems, and Mac OS X.

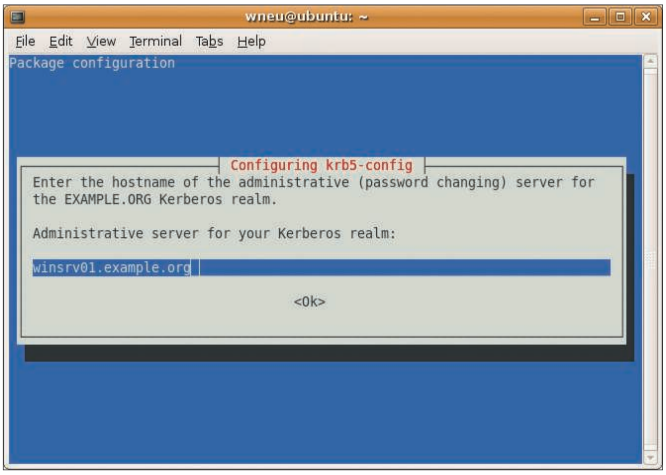
The Likewise website features version 5.0, although the distribution-specific packages include version 4, which I will use for this article. Ubuntu users will find the likewise-open and likewise-open-gui packages in the Universe repository. The Likewise packages include a number of dependencies – mainly related to Kerberos. Likewise Open relies on the MIT version of Kerberos as a back

tauro79, Fotolia



```
Package configuration

Configuring krb5-config
Enter the hostnames of Kerberos servers in the EXAMPLE.ORG Kerberos
realm separated by spaces.

Kerberos servers for your realm:

winsrv01.example.org

<Ok>
```

Figure 1: The Ubuntu package manager prompts you for the name of the Kerberos server when you install the Kerberos packages.



```
Package configuration

Configuring krb5-config
Enter the hostname of the administrative (password changing) server for
the EXAMPLE.ORG Kerberos realm.

Administrative server for your Kerberos realm:

winsrv01.example.org

<Ok>
```

Figure 2: You must specify the administrative server for the Kerberos realm.

end [3]. During installation on Ubuntu, the package prompts the admin to specify the Kerberos and administrative servers (Figures 1 and 2).

Besides a working Active Directory (AD) server and a domain structure managed by Windows, Likewise has two main requirements: a working name server to resolve DNS names and a synchronized system clock. If the client and server clocks are more than five minutes out of sync, the Kerberos server will refuse to issue tickets, which is a security measure to prevent replay attacks.

New Configuration Approach

Adding a raw Linux system to an AD domain requires a fair amount of configuration work [2]. The Likewise Agent handles most of this work, adding itself to the Name Service Switch (NSS) and Pluggable Authentication Modules (PAM) on the local client.

Server-side, the agent passes on authentication requests to the Kerberos 5 server and the LDAP-based AD. To allow this to happen, the package installs a couple of libraries and configuration files. For example, */lib/libnss_lwidentity.so* integrates Likewise with NSS, and */--etc/pam.d/-pam_lwidentity.so-* does the same thing for PAM. The */etc/security/pam_lwidentity.conf* configuration file sets up the module, and the interface to the remote domain controller is implemented by the Likewise Winbind server, likewise-winbindd. The server has its own configuration file, */etc/samba/lwiauthd.conf*, which is similar to the *smb.conf* file from the Samba package.

Likewise Open integrates these components to support a transparent domain login for the users. The login process passes the username and password to PAM. The *pam_lwidentity.so* module communicates with the Likewise authentication service, which generates a secret key from the username and password. The Likewise daemon uses the secret key to request an initial Ticket Granting Ticket (TGT) from the Kerberos Authentication Server, which runs as part of the Key Distribution Center (KDC) on the AD Server.

On presenting the TGT, the Likewise authentication service receives service tickets for other network services, such as SSH. Users can thus log on to kerberized servers without entering their passwords a second time.

Set up the Likewise installation package on each Linux machine that will become a member of the AD domain (and will be managed by Likewise). If you use the installation packages from the website, Likewise Open will be installed by using a Bitrock Installer – an executable whose file name ends with *installer*. To run the program, you must become root and follow the instructions on the screen.

Listing 1: Joining a Domain

```
# domainjoin-cli join example.org Administrator
Joining to AD Domain: example.org
With Computer DNS Name: ubuntu.example.org

Administrator@EXAMPLE.ORG's password:
Enter Administrator@EXAMPLE.ORG's password:
SUCCESS
```

The installer displays information about the OSS licenses for the installed components before Likewise sets up its files. After this, the Installer points the administrator to *domainjoin-cli*, which is located in the */-usr/centeris/bin/* directory (thus contravening the FHS [4] conventions; the distribution packages and later versions of Likewise correct this error). The agent stores logging information in */var/log/lw-identity/* or – if you use the version from the Ubuntu repository – in */var/log/likewise-open*.

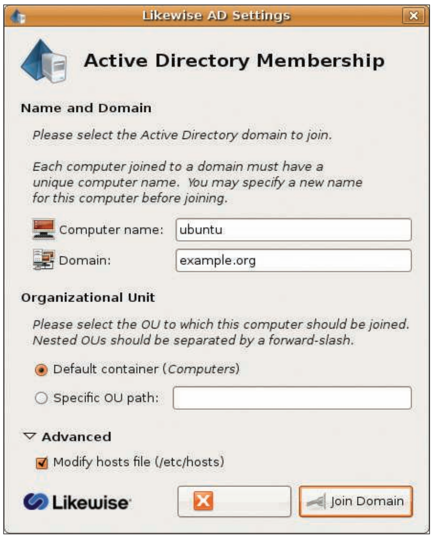
Come On In

An AD domain requires both the user and the client systems to become members. The act of setting up a machine account in Microsoft's directory service is referred to in AD-speak as "Joining the domain."

A command-line tool, *domainjoin-cli*, lets the root user join the AD domain, creating a machine account in the directory in the process. The *domainjoin-cli* tool accepts the *join* option and the domain as arguments. The domain argument must be specified as a fully qualified DNS name.

On top of this, the command expects the name of a user authorized to create computer accounts in the AD environment. Listing 1 shows a computer called *ubuntu* joining the *example.org* domain. The *Administrator* account has the required privileges for this step.

The second option for joining a domain is the



Likewise AD Settings

Active Directory Membership

Name and Domain

Please select the Active Directory domain to join.

Each computer joined to a domain must have a unique computer name. You may specify a new name for this computer before joining.

Computer name: ubuntu

Domain: example.org

Organizational Unit

Please select the OU to which this computer should be joined. Nested OUs should be separated by a forward-slash.

● Default container (Computers)

○ Specific OU path:

Advanced

☑ Modify hosts file (/etc/hosts)

Figure 3: The Likewise Open GUI expects the DNS name of the domain and the hostnames.

Likewise Open GUI (Figure 3), however, the GUI is not included with the likewise-open core package. To add the GUI, just install likewise-open-gui and launch it with root privileges by entering *domainjoin-gui*.

Manual and Automatic

In both cases, Likewise Open handles the configuration work in the background, removing the need for complex manual steps. The software modifies the configurations for user interaction with AD (see Figure 4), including the files required for Kerberos communications with the KDC *krb5.conf* and the PAM files in */etc/pam.d/**.

To log in using a Linux client domain, users must have a home directory on the client. Likewise creates the directory locally if you modify */-etc/security/pam_lwidentity.conf*.

The */--etc/nsswitch.conf* file tells Likewise Open to take control again and specify the *lwidentity* method. The NSS name service checks local files such as */etc/passwd* first:

```
passwd: files lwidentity
group:  files lwidentity
```

If it fails to find an account, it then accesses the AD. This means that local users can still access the local machine if AD fails.

Careful Configuration

Likewise is careful about configuring the Linux system. It creates backups of any files it modifies, adding a suffix of *.lwidentity.bak*, and for good reason: Running *domainjoin-cli leave* as root at the command line or in the GUI removes the machine account.

In this case, Likewise restores any configuration files that have been changed. Likewise uses the */etc/samba/lwiauthd.conf* file to let administrators set configuration options for their own Winbind system; you might be familiar with these settings if you use Samba in an AD environment.

Individual Configuration

The *template shell* parameter sets the login shell centrally for all domain users. The user's home directory is not defined in the AD user database; thus, you will need to specify the path in the configuration file with the Samba *template homedir* parameter:

```
template shell    = /bin/bash
template homedir = /home/%D/%U
```

Likewise-Winbind replaces *%D* with the short domain name and *%U* with the domain user.

To avoid name collisions in trust relationships, it makes sense to add the domain to the user's path – and to apply the defaults for user directories. If you do not change the configuration, Likewise Open will use the backslash as the separator between domains and usernames. Of course, the backslash has a special meaning in Unix shells. Experts recommend changing this to, say, the plus character on all your clients by using *winbind separator*.

If you only have one domain, you can set *winbind use default domain = yes* to avoid separating the domain and usernames. If you fail to do so, the domain users supplied by Winbind will not work unless you add a domain prefix. Restarting the likewise-open *init* script applies the changes.

Verbose

The likewise-open package contains three diagnostics tools – *lwinet*, *lwimsg*, and *lwiinfo* – that are useful for debugging, among other things.

Because Likewise is based on the Samba Winbindd code, the tools will handle the tasks normally performed by the Samba Winbind daemon. By entering *lwiinfo*, you can check the connection to the domain controller.

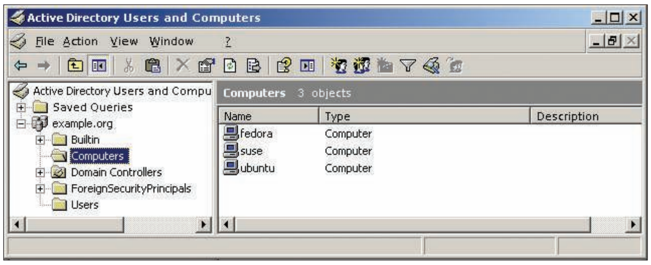
The tool corresponds to *wbinfo* in the Samba suite. Both of these tools query the Winbind daemon. For example, *lwiinfo -u* lists all the domain users in the default domain:

```
EXAMPLE+mokr000
EXAMPLE+phkr000
EXAMPLE+wane000 [...]
```

The same principle applies to groups in the directory service, which are output by the *-g* option. This ensures that Linux knows the AD names. Entering *lwiinfo -g* lists the known groups:

```
EXAMPLE+accounts
EXAMPLE+marketing [...]
```

Again, Likewise uses the + character, configured in *lwiauthd.conf*, as the Win-



Active Directory Users and Computers

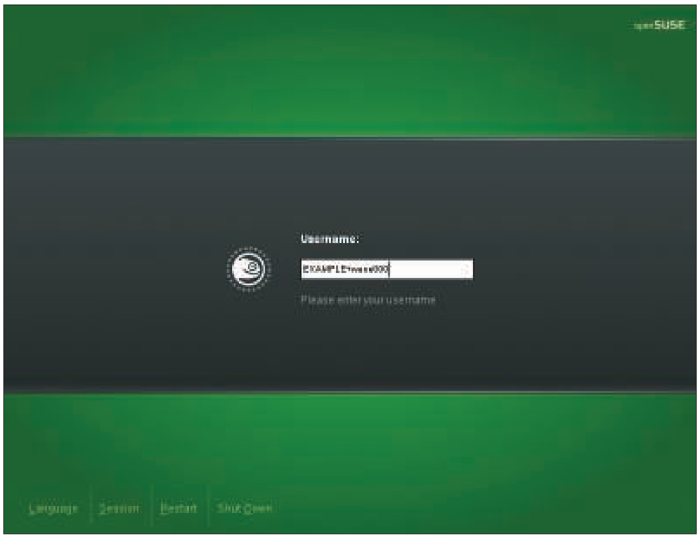
Computers 3 objects

Name	Type	Description
fedora	Computer	
suse	Computer	
ubuntu	Computer	

Figure 4: After joining the domain, Likewise creates a machine account for the ubuntu computer in Active Directory.

Listing 2: klist Displays Local Tickets

```
$ klist
Ticket cache: FILE:/tmp/krb5cc_1560282197
Default principal: wane000@EXAMPLE.ORG

Valid starting     Expires            Service principal
08/12/08 13:48:08  08/12/08 23:48:08  krbtgt/EXAMPLE.ORG@
EXAMPLE.ORG
        renew until 08/19/08 13:48:08
08/12/08 13:48:08  08/12/08 23:48:08  SUSE$@EXAMPLE.ORG
        renew until 08/19/08 13:48:08
```



Username: EXAMPLE+wane000

Please enter your username

Figure 5: The GDM display manager requests a login name on authentication. In this AD, the name consists of the domain name, EXAMPLE, a plus sign as a separator, and the username.

bind separator. The *lwimsg* tool corresponds to *smbcontrol* and is used to control Winbindd, setting the debug level, for example. The counterpart to the Samba *net* tool, which is used for remote administration of a domain, is *lwinet*.

After installing the software, it is a good idea to try logging on to AD. The user name format has to match the format defined for the directory service. For example, if you keep the default setting for domain and username separation, but change the separator to the plus sign, users will need to enter their names as *DOMAIN + username* when they log in at the console or with a desktop manager (see Figure 5):

```
ubuntu Login: EXAMPLE+wane000
Password:
EXAMPLE+wane000@ubuntu:~$
```

As mentioned before, Likewise authenticates users via the Kerberos protocol by requesting a TGT from the KDC before going on to install the ticket locally on the client as */tmp/krb5cc_UID* (see Listing 2). The *klist* command displays a user's valid tickets.

A user who has a ticket can access kerberized services on the network without logging on separately with the network service.

Single Sign-on

To allow a network service to grant a user password-less access, the administrator has to assign a Service Principal Name (SPN) to the service. The name identifies the service within the AD environment. The service requests a service ticket for the Service Principal from the KDC, identifying itself with its TGT.

The SPN comprises a service definition, followed by a slash and the fully qualified hostname of the server, an at sign, and the domain.

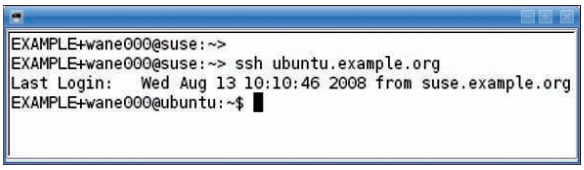
Listing 3: Tickets in the Credentials Cache

```
$ klist
Ticket cache: FILE:/tmp/krb5cc_1560282197
Default principal: wane000@EXAMPLE.ORG

Valid starting          Expires             Service principal
08/13/08 15:48:29        08/14/08 01:48:30    krbtgt/EXAMPLE.ORG@EXAMPLE.ORG
          renew until   08/20/08 15:48:29
08/13/08 15:48:30        08/14/08 01:48:30    SUSE$@EXAMPLE.ORG
          renew until   08/20/08 15:48:29
08/13/08 15:48:38        08/14/08 01:48:30    host/ubuntu.example.org@
          renew until   08/20/08 15:48:29
08/13/08 15:48:38        08/14/08 01:48:30    host/ubuntu.example.org@EXAMPLE.
ORG
          renew until   08/20/08 15:48:29
```

Service definitions include *host*, *ftp*, or *pop*. If a user establishes an SSH connection to another Likwise-managed AD member computer, the kerberized service presents the user's TGT and requests a service ticket from the KDC for, say, the SPN *host/ubuntu.example.org@EXAMPLE.ORG* – this assumes that the local ticket cache does not already have a ticket. The service ticket contains the user ID of the requesting user and the session key. Likewise Open encrypts this with the server key and stores it in the user cache like the TGT (see Listing 3).

The SSH client automatically sends the encrypted service ticket and an encrypted timestamp to validate the authenticator's *sshd*. This guarantees that each ticket request is unique, while ensuring that the client really does possess the session key. Without the authenticator, it would be easier for an attacker to sniff a ticket off the network traffic and launch a replay attack.

The server validates the service ticket presented to it. To to so, it refers to the local keytab file, */etc/krb5.keytab*. The file stores the server key, which the server uses to decrypt the service ticket, thus revealing the session key. The authenticator is based on the session key; if it succeeds, the user is authenticated without a password (Figure 6).



```
EXAMPLE+wane000@suse:~>
EXAMPLE+wane000@suse:~> ssh ubuntu.example.org
Last Login:   Wed Aug 13 10:10:46 2008 from suse.example.org
EXAMPLE+wane000@ubuntu:~$
```

Figure 6: Likewise implements a single sign-on through Kerberos. Users do not need to enter a password to log on.

Establishing a Connection

Likewise Open automatically configures existing SSH clients and clients on joining the domain, allowing them to use Kerberos to authenticate in the future. Server-side, Likewise adds the lines

```
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
```

to the */etc/ssh/sshd_config* configuration file. Likewise also adds the following lines for an SSH client:

```
GSSAPIAuthentication yes
GSSAPIDelegateCredentials yes
```

Listing 4: pam_mount Mounts Samba Shares

```
<?xml version="1.0" encoding="UTF-8"?>
<pam_mount>
<volume user      = "*"
        server     = "SAMBASERVER"
        mountpoint = "/home/EXAMPLE/%(USER)/Document"
        path       = "%(USER)"
        fstype     = "smbfs" />
</pam_mount>
```

The *GSSAPIDelegateCredentials* instruction passes the TGT to the target server. For all other settings, the software uses the Generic Security Services API (GSSAPI), a generic interface for security services such as Kerberos.

Local

The first time a domain user logs on to a client, Likewise Open uses PAM (*pam_lwidentity.so*) to set up local user directories. Alternatively, the *pam_mount* module can mount central user directories on a remote server with SMB/CIFS [5]. This guarantees all users access to their own files independent of the client they use to log in. The share is defined by a line in */etc/security/pam_mount.conf* that uses the *volume* keyword:

```
volume user filesystem server ⮐
share mountpoint options ⮐
cipher path
```

Use of a wildcard * for the *user* parameter tells the module to insert the name of the user. The *filesystem* can be *smbfs* or *cifs*. The *server* can be an IP address or a NetBIOS name, and *share* can use the ampersand, &, as a wildcard for the username.

The last three parameters are not typically needed; dashes will be fine in this case:

```
volume * smbfs SAMBASERVER & ⮐
/home/EXAMPLE/&/Documents - - -
```

Whether you mount the *Documents* subdirectory or the complete home directory is a matter of taste and will depend on how an organization arranges its central servers.

If the mount point does not exist, the PAM *pam_mount* module, with a setting of *mkmountpoint 1*, creates it. As of version 0.29, *pam_mount* stores the configuration in an equivalent XML format, as shown in Listing 4.

Before the *sufficient* entries in the *auth* section of */etc/pam.d*, you can insert an entry for the module. Listing 5 shows a configuration in the *common-auth* and *common-session* files on Ubuntu. To avoid the need for users to repeatedly enter their passwords, the *try_first_pass = yes* entry in the */etc/security/pam_lwidentity.conf* file enables the option for retrying a password entered previously.

More in the Commercial Version

Besides the open source version of Likewise, the US-based Likewise Software corporation offers a commercial version of its software, Likewise Enterprise [6]. The commercial version has support for AD group policies on top of the functionality offered by the free version; the product defines around 500 default policies. The Likewise Administrative Console can use a Linux or Unix machine to manage AD records.

On top of this, Likewise Enterprise supports Linux desktops, referring to AD to retrieve settings and restrictions. This enables the implementation of strict security policies. The Enterprise variant is available free of charge for evaluation purposes, or for US$ 250 as a server version. The company offers two levels of commercial support.

A New Face

Once configured, Likewise Open offers the same functional scope as a combination of Samba, Kerberos, PAM, and NSS. It takes many pesky setup tasks off the administrator's hands and supports centralized and platform-independent user management. The ticket-based Kerberos authentication service and single sign-on is a bonus.

If you enjoy working with Likewise Open, you might appreciate the extra features offered by the commercial version or the benefits of professional support. The only manual work left to the administrator is that of managing centralized user directories. ■

Listing 5: Setting up pam_mount

```
# /etc/pam.d/common-auth
auth     required    pam_mount.so
auth     sufficient  /lib/security/pam_lwidentity.so
auth     requisite   pam_unix.so nullok_secure try_first_pass
auth     optional    pam_smbpass.so migrate missingok

# /etc/pam.d/common-session
session  optional   pam_mount.so
auth     sufficient /lib/security/pam_lwidentity.so
session  required   pam_unix.so
```

INFO

[1] Likewise Open: *http://www.likewisesoftware.com/products/likewise_open/*

[2] "Linux with Active Directory" by Walter Neu, *Linux Magazine*, November 2008, pg. 28

[3] MIT Kerberos: *http://web.mit.edu/kerberos/*

[4] File Hierarchy Standard: *http://www.pathname.com/fhs/*

[5] Mounting home directories with PAM: *http://pam-mount.sourceforge.net/*

[6] Likewise Enterprise: *http://www.likewisesoftware.com/products/likewise_enterprise*

THE AUTHOR

Walter Neu works as a system administrator for Eurodata. He is also a lecturer in computer science, teaching Linux 101, Windows networking, and web server technology at ASW Berufsakademie Saarland, University of Cooperative Education, Sankt Ingbert, Germany.