



Mercurion Systems, Inc.

**Information Technology Consulting and Support
Services**

Phone: 919.266.5957 Fax: 919.217.5769
<http://www.mercurionsystems.com>

LINUX AUTHENTICATION VIA ACTIVE DIRECTORY

Products: Linux (with PAM), Active Directory (on Windows Server 2003)

Overview

Operating systems based on the Linux kernel are growing in popularity and functionality. In particular, these systems are increasingly being used in conjunction with proprietary operating systems such as Microsoft Windows Server 2003. The complementary strengths of each operating system make such heterogeneous combinations very helpful; however, this heterogeneity also adds administrative complexity when it comes to managing user accounts and passwords.

This technical document describes one method (there are several) for authenticating logins to a Linux-based operating system via Active Directory. This method uses Kerberos for the authentication process and LDAP (Lightweight Directory Access Protocol) for UID/GID resolution.

More Information

Extending the Active Directory Schema

First, the Active Directory schema must be extended to support the storage of Linux/Unix-specific attributes, such as UID, GID, and home directory. There are a couple of different ways to extend the Active Directory schema; this document is written from the perspective of using Microsoft Services for UNIX 3.5, a free download available from Microsoft's web site.

To extend the Active Directory schema using SFU, run the SFU setup application and install the NIS Server component. (Install other components as needed.) Initially, this must be done on the domain controller that currently holds the Schema Master FSMO role.

Creating an LDAP Bind Account

Second, an ordinary user account must be created to support binding to LDAP from the Linux system(s). This account does not need any elevated privileges whatsoever. Use the standard Active Directory tools (such as Active Directory Users & Computers) to create this account and set the password. Make a note of the location of this account; that information will be required later when configuring the LDAP lookups from the Linux servers.

Mapping a Security Principal to an Account

In order for Kerberos to work, a Kerberos security principal must be mapped to an Active Directory account. Generally, user accounts are used for this process; there should be one account created for each Linux host that will authenticate against Active Directory. However, it makes more sense to use computer accounts for the Linux-based computers. To do so requires only a small change in the command line that is needed.

To map a Kerberos security principal to a computer account and generate the keytab that is required, use the following command line (note that the lines have been wrapped for readability):

```
ktpass -princ host/fqdn@REALM -mapuser DOMAIN\name$  
-crypto DES-CBC-MD5 -pass password -ptype KRB5_NT_PRINCIPAL  
-out filename
```

If the Active Directory domain is example.com, then the corresponding Kerberos realm is EXAMPLE.COM (Kerberos realms are always in uppercase). If the Linux server to be authenticated by Active Directory is linuxserver.example.com, then the command to run would look something like this (this assumes that a computer account named LINUXSERVER has already been created in Active Directory):

```
ktpass -princ linuxserver/linuxserver.example.com@EXAMPLE.COM  
-mapuser EXAMPLE\LINUXSERVER$ -crypto DES-CBC-MD5 -pass password  
-ptype KRB5_NT_PRINCIPAL -out c:\linuxserver.keytab
```

The file generated by this command (linuxserver.keytab) then needs to be securely transferred to the server in question. This can be accomplished using SFTP, SCP, or physical media (floppy, USB drive, etc.).

Configuring PAM for Kerberos

Pluggable Authentication Modules (PAM) are the piece that allow Linux authentication schemes to be customized and extended. PAM configurations vary between Linux distributions; this section is written from the perspective of configuring PAM on a Red Hat-based distribution (this would include Red Hat Linux, Fedora Core Linux, Red Hat Enterprise Linux, CentOS, and others).

To add Kerberos authentication, we modify the system-auth file in /etc/pam.d. Most other files in this directory use PAM's stacking functionality to tie directly to system-auth, so changes made in system-auth will automatically affect all the other PAM-integrated applications.

The file listing at the top of the following page shows a system-auth file that has been modified to support Kerberos authentication.

/etc/pam.d/system-auth		
auth	required	/lib/security/\$ISA/pam_env.so
auth	sufficient	/lib/security/\$ISA/pam_unix.so likeauth nullok
auth	sufficient	/lib/security/\$ISA/pam_krb5.so use_first_pass
auth	required	/lib/security/\$ISA/pam_deny.so
account	required	/lib/security/\$ISA/pam_unix.so
password	required	/lib/security/\$ISA/pam_cracklib.so retry=3 type=
password	sufficient	/lib/security/\$ISA/pam_unix.so nullok use_authok md5 shadow
password	required	/lib/security/\$ISA/pam_deny.so
session	required	/lib/security/\$ISA/pam_limits.so
session	required	/lib/security/\$ISA/pam_unix.so

This system-auth configuration tries the local Unix password mechanism first, and if that is successful then no other checks are required. If not, then Kerberos is consulted using the same authentication credentials.

This is only half the puzzle. Users still won't be able to login to a Linux server with an Active Directory username and password until LDAP lookups for UID/GID resolution are also configured.

Configuring LDAP

The use of the `nss_ldap` module allows Linux to use Active Directory as an LDAP server for the purposes of resolving UIDs and GIDs to human-readable names (and vice versa). The `nss_ldap` module is typically installed by default and is configured using the `ldap.conf` file in the `/etc` directory. This is shown below.

/etc/ldap.conf	
host	w.x.y.z
base	ou=Name,dc=example,dc=com
binddn	cn=LDAP,cn=Users,dc=example,dc=com
bindpw	<bindpassword>
scope	sub
ssl	no
nss_base_passwd	ou=Name,dc=example,dc=com
nss_base_shadow	ou=Name,dc=example,dc=com
nss_base_group	ou=Name,dc=example,dc=com
nss_map_objectclass	posixAccount user
nss_map_objectclass	shadowAccount user
nss_map_objectclass	posixGroup group
nss_map_attribute	uid sAMAccountName
nss_map_attribute	uidNumber msSFU30UidNumber
nss_map_attribute	gidNumber msSFU30GidNumber
nss_map_attribute	loginShell msSFU30LoginShell
nss_map_attribute	gecos name
nss_map_attribute	userPassword msSFU30Password
nss_map_attribute	homeDirectory msSFU30HomeDirectory
nss_map_attribute	uniqueMember msSFU30PosixMember
nss_map_attribute	cn cn

Note in this file the inclusion of several pieces of information that were gathered earlier. To properly configure LDAP, the location of the LDAP bind account (the account created earlier specifically for systems to bind to Active Directory), the LDAP bind account's password, and the base DN (the base location where to look for accounts in Active Directory) are all needed in this file.

In addition, also note the "nss_map_attribute" lines, which map Linux attributes to the corresponding attributes in Active Directory.

Once LDAP has been properly configured, Linux now needs to be instructed to look in LDAP when looking for UID, GID, or other information. This is accomplished by editing the nsswitch.conf file, stored in the /etc directory.

```
/etc/nsswitch.conf
(previous lines omitted)

passwd:  files ldap
shadow:  files ldap
group:   files ldap

(following lines omitted)
```

For brevity, only the affected lines from nsswitch.conf are recreated here. On the lines for passwd, shadow, and group, simply append "ldap" to the existing entry then. Once this configuration is done, then Linux will use LDAP to match UID, GID, and name information.

Other Notes

This document was tested specifically with Active Directory on Windows Server 2003 running in native mode (both the forest functional level and the domain functional level were set to Windows Server 2003). Red Hat Linux 9.0 and CentOS 4.1 (a clone of Red Hat Enterprise Linux 4) were tested on the Linux side. Earlier versions of Active Directory should behave much the same, as should other Linux distributions.

Related Articles/Resources

There are numerous resources available on the Internet that describe the use of Kerberos and LDAP for Linux/AD integration; those resources are too numerous to mention here but were referenced during the creation of this document.

Legal Information

This document was created by Mercurion Systems, Inc., and may be freely distributed as long as it is distributed without modification and in its entirety. Mercurion Systems assumes no liability as a result of using the information contained in this document.