Redbooks Paper

Dr. Manfred Gnirss
Frank Kirschner

Advanced LDAP User Authentication: Limiting Access to Linux Systems Using the Host Attribute

Abstract

This IBM® Redpaper provides information to help customers, Business Partners, and IBM technical people plan, implement, and manage a central security solution for user authentication with a method to limit user access to Linux systems based on information stored in a central LDAP directory.

In an environment with multiple Linux systems, keeping user information in a central LDAP directory is a proven technology to avoid having to store identical user information on each system. This simplifies user administration tasks since only one central directory has to be managed. In addition to storing personal user information, it is possible to limit user access to specific Linux systems by adding restriction information in user account definitions in the LDAP directory. This paper shows how to configure Linux systems to limit host access with a central LDAP directory.

Introduction

Authentication of Linux users with a central LDAP directory instead of using information stored locally on the system (in /etc/passwd and in /etc/shadow) is an established practice to reduce administration effort in an environment with multiple Linux systems. See *Securing Linux for zSeries with a Central z/OS LDAP Server (RACF),* REDP-0221 and the PADL Software Pty Ltd Web site for more information.

To use LDAP for user authentication you need to install and configure pam_ldap, nss_ldap, and LDAP client, and configure each service that should participate in LDAP authentication (ssh, telnet, sudo, ftp, and so forth). The user information must be accessible from LDAP. Example 1 shows part of an LDAP client configuration where the address of the LDAP server and the search base is specified.

Example 1 Part of an LDAP configuration file

```
# $OpenLDAP: /etc/openldap/ldap.conf
# LDAP Defaults
host os390r27.boeblingen.de.ibm.com
base o=ibm
ldap_version 3
```

The order in which authentication is checked is determined in the individual service configuration files. Example 2 shows a typical configuration for login with Secure Shell (ssh) access.

Example 2 Extract of a configuration example for secure shell access (/etc/pam.d/sshd)

```
#%PAM-1.0:  /etc/pam.d/sshd
auth required   pam_nologin.so
auth required   pam_env.so
auth sufficient pam_ldap.so
auth required   pam_unix2.so use_first_pass
account sufficient      pam_ldap.so
account required        pam_unix2.so
account required        pam_nologin.so
session required        pam_unix2.so    none
session required        pam_limits.so
```

In this example users are first authenticated against an LDAP directory. If no user entry is in the directory, the user is locally authenticated. This search order ensures that locally defined l users (such as root) can be authenticated.

To resolve user information, the Name Service Switch (nss) can be configured as shown in Example 3.

Example 3 Part of a sample nss configuration file (/etc/nsswitch.conf)

```
# /etc/nsswitch.conf
# An example Name Service Switch config file.
passwd: ldap compat
group:  ldap compat
shadow: ldap compat
```

To use PAM authentication with LDAP, all necessary information for a Linux user must be available in the LDAP directory. The minimum set is defined in the posixUser object class (cn, uid, uidNumber, gidNumber, homeDirectory). Additional information like the userPassword and loginShell attribute also may be necessary. Example 4 has a possible user entry in an LDAP directory.

Example 4 Example of a simple LDAP Directory entry for a Linux user

```
dn: cn=Manfred Gnirss, ou=people, ou=TMCC, o=ibm
givenname: Manfred
objectclass: top
objectclass: account
objectclass: posixAccount
objectClass: shadowAccount
cn: Manfred Gnirss
uid: gnirss
uidnumber: 42123
gidnumber: 100
homedirectory: /home/gnirss
loginshell: /bin/bash
userPassword: *****
sn: Gnirss
```

This setup allows multiple Linux hosts to authenticate users defined in a central repository. This simplifies the system administrator's user management task when creating a Linux system (for example, by cloning a Linux system under z/VM® on an IBM zSeries® server, or when buying a new hardware box with a Linux system). See *Server Consolidation with Linux for zSeries*, REDP-0222 and *Cloning Linux Images in z/VM*, REDP-0301 for an example of cloning Linux servers in z/VM.

Limiting access to Linux systems

Normally, all users defined in a central LDAP directory have access to every host which authenticates against that directory. In some cases, it is desirable to restrict access to specific hosts for certain users defined in LDAP. This can be accomplished using the host attribute of the account objectclass.

To illustrate, consider the LDAP user directory shown in Example 5. In the example, we see the gnirss user is granted access to three systems using the host attribute.

Example 5 Example of a simple LDAP Directory entry for a Linux user with host attributes

```
dn: cn=Manfred Gnirss, ou=people, ou=TMCC, o=ibm
givenname: Manfred
objectclass: top
objectclass: posixAccount
objectclass: shadowAccount
objectclass: account
cn: Manfred Gnirss
uid: gnirss
uidnumber: 42123
gidnumber: 100
homedirectory: /home/gnirss
loginshell: /bin/bash
userPassword: *****
host: tmcc02.boeblingen.de.ibm.com
host: tmcc03.boeblingen.de.ibm.com
host: itso07.poughkeepsie.us.ibm.com
sn: Gnirss
```

We describe two methods for limiting access to Linux systems using the host attribute in a user entry in the LDAP directory in the following sections.

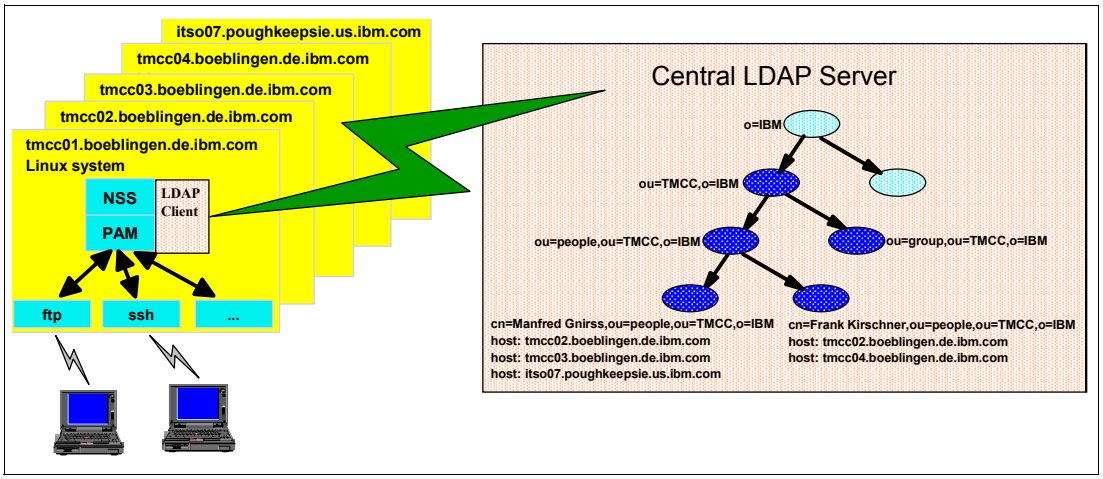

Figure 1 Structural illustration for limiting access of users to individual systems

One simple method

For each user, you can specify all systems (hostnames) the user can access. This is done with a filter in the LDAP configuration file and telling PAM to check for the host attribute, as shown in Example 6.

Example 6 Limiting access to specific user

```
# $OpenLDAP: /etc/openldap/ldap.conf
# LDAP Defaults
host os390r27.boeblingen.de.ibm.com
base o=ibm
ldap_version 3
use pam_filter |(host=\*)(host=\*.boeblingen.de.ibm.com)(host=tmcc02.boeblingen.de.ibm.com)
```

Users who have host attribute values of "*" or "`boeblingen.de.ibm.com`" or "`tmcc02.boeblingen.de.ibm.com`" are allowed to log into the system. This method is not very flexible since specific information is stored on the local Linux systems, and each system must be individually configured. Therefore, this method is not our first choice.

General method

A preferable method is to have identical LDAP configuration files on each host that do not have to be maintained separately. This is done by storing host information in the central LDAP directory. A check is performed to determine whether the host attribute specified in LDAP matches the hostname on the local system. The hostname is not coded in the local LDAP configuration file, but rather is retrieved from the system using the gethostname() system call. PAM authentication is not performed in the authentication phase, but rather in the account phase. The authentication phase verifies the identity of the user; the account phase determines if the authenticated user is allowed to access the system.

Therefore, the configuration setup has to specify:

- That the host attribute must be checked. This is done using the entry in the LDAP configuration file:

  `pam_check_host_attr yes` (see Example 7)

- How to deal with the result of this check. This is determined by the logic in the /etc/pam.d service configuration files. The logic is specified by an expression that is evaluated during the account phase, as shown in Example 8.

Example 7 Limiting access to specific user

```
# $OpenLDAP: /etc/openldap/ldap.conf
# LDAP Defaults
host os390r27.boeblingen.de.ibm.com
base o=ibm
ldap_version 3
pam_check_host_attr yes
```

The PAM configuration file syntax is defined in Chapter 4 of the Linux-PAM System Administrators' Guide. The general syntax is:

```
service-name module-type control-flag module-path args
```

Note: The service-name is omitted when the service is configured as a separate file in the /etc/pam.d directory.

The control-flag parameter is specified as either a set of name=value pairs, or a specific keyword. The *sufficient* control-flag keyword expands to:

```
[success=done new_authtok_reqd=done default=ignore]
```

To restrict access based on the specification of the host attribute in the LDAP user entry, the check triggered by the pam_check_host_attr parameter must return PAM_PERM_DENIED. This is implemented using the perm_denied=bad expression in the PAM configuration file. The complete control-flag expression for sufficient checks with host-based limitation is:

```
account [success=done new_authtok_reqd=done perm_denied=bad default=ignore] pam_ldap.so
```

We use this expression in the /etc/pam.d configuration file, as shown in Example 8. This prohibits users from accessing systems that are not specified by the host attribute in their user entry in the LDAP directory.

Note: This setup also still allows local user definitions in /etc/passwd and /etc/shadow to continue to work on the system.

Example 8 The ssh configuration file for host attribute authentication

```
#%PAM-1.0 /etc/pam.d/sshd
auth required   pam_nologin.so
auth required   pam_env.so
auth sufficient pam_ldap.so
auth required   pam_unix2.so use_first_pass # set_secrpc
account [success=done new_authtok_reqd=done perm_denied=bad default=ignore] pam_ldap.so
account required        pam_unix2.so
account required        pam_nologin.so
session required        pam_unix2.so    none     # trace or debug
session required        pam_limits.so
```

Unfortunately, the current version of the pam_ldap module (version156) does not provide the same support for wildcards that is available with the pam_filter mechanism (see "One simple method" on page 4).

Storing additional person-related data in a user entry

LDAP authentication relies on attributes defined to the posixAccount object class for a user entry. Typically, additional user attributes are added to an LDAP user entry using the inetOrgPerson and organizationalPerson objectclasses. Ideally, we would like to extend the posixAccount object class (adding the host attribute). However, we discovered this was not possible if existing user entries include the inetOrgPerson objectclass.

Note: The posixAccount and inetOrgPerson objectclasses are both STRUCTURAL types. Extended schema checking implemented by z/OS Version 1 Release 4 Security LDAP Server forbids adding attributes to existing STRUCTURAL objectclasses. Similar behavior also is found on newer versions of other LDAP servers like OpenLDAP Server 2.1 and IBM IDS 5.0.

To overcome this problem, we use the special ibm-auxAccount objectclass. This is defined to be an AUXILARY type (which can be extended by adding attributes). We define the host attribute in the ibm-auxAccount objectclass. We show an example LDAP user entry in Example 9.

Example 9 Person entry which allows adding a host attribute of object class ibm_auxAccount

```
dn: cn=Manfred Gnirss, ou=people, ou=TMCC, o=ibm
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: posixAccount
objectclass: shadowAccount
objectclass: ibm-auxAccount
cn: Manfred Gnirss
uid: gnirss
uidnumber: 42123
gidnumber: 100
homedirectory: /home/gnirss
loginshell: /bin/bash
telephonenumber: 120-4093
street: Schoenaicher Str. 220
mail: gnirss@de.ibm.com
departmentnumber: 3300
employeenumber: 0661234
roomnumber: 14-039
givenname: Manfred
postalcode: 71032
l: Boeblingen
postaladdress: Schoenaicher Str. 220
host: tmcc02.boeblingen.de.ibm.com
host: tmcc03.boeblingen.de.ibm.com
host: itso07.poughkeepsie.us.ibm.com
sn: Gnirss
```

In this example, we see the gnirss user is granted access to three systems:

```
host: tmcc02.boeblingen.de.ibm.com
host: tmcc03.boeblingen.de.ibm.com
host: itso07.poughkeepsie.us.ibm.com
```

The schema file (shown in Example 10) which contains the object class ibm-auxAccount can be downloaded from:

ftp://www.redbooks.ibm.com/redbooks/REDP0221

Example 10 Schema file which is compatible with inetOrgperson

```
(
1.3.18.0.2.6.576
NAME 'ibm-auxAccount'
DESC 'Auxiliary object class containing same information as account object class from
RFC 1274'
AUXILIARY
SUP top
MUST uid
MAY ( description $ host $ l $ o $ ou $ seeAlso )
 )
```

Note: A userPassword attribute is not needed if Native Authentication is used to authenticate passwords stored in RACF® (as described in *Securing Linux for zSeries with a Central z/OS LDAP Server (RACF),* REDP0221).

The ibm-auxAccount object class is only required if the LDAP user entry includes the inetOrgPerson objectlass. If the inetOrgPerson object class is not used, the posixAccount object class can hold the host attribute.

Summary

It is relatively simple to set up and configure a central LDAP repository for keeping user information and host information to limit access of users to individual Linux systems. The setup and configuration on these Linux systems is completely independent from any user information and does not require individual adaptation. This simplifies administration when cloning and adding Linux systems.

References

IBM Redbooks/Redpieces

Securing Linux for zSeries with a Central z/OS LDAP Server (RACF), REDP0221, by Erich Amrehn, Ulrich Boche, and Dr. Manfred Gnirss

http://www.redbooks.ibm.com/redpapers/pdfs/redp0221.pdf

Server Consolidation with Linux for zSeries, REDP 0222, by Erich Amrehn, Joachim Jordan, Frank Kirschner, and Bill Reeder

http://www.redbooks.ibm.com/redpapers/pdfs/redp0222.pdf

Cloning Linux Images in z/VM, REDP0301, by Gregory Geiselhart, Tung-sing chong, and Michael Donovan

http://www.redbooks.ibm.com/redpapers/pdfs/redp0301.pdf

Referenced Web sites

Web site of PADL Software Pty Ltd contains Open Source products like nss ldap and PAM ldap:

http://www.padl.com

The Linux-PAM System Administrators' Guide, by Andrew G. Morgan

http://docs.linux.cz/pam/pam.html

The team that wrote this paper

This paper was produced during a workshop and subsequent experiments and implementations at the Technical Marketing Competence Center in the IBM Laboratory in Boeblingen, Germany.

Manfred Gnirss is an IT specialist at the IBM Technical Marketing Competence Center (TMCC) and the Linux Center of Competence, Boeblingen, Germany. He holds a PhD in theoretical physics from the University of Tuebingen, Germany. Before joining the TMCC, he worked in z/VM and z/OS® configuration development. Currently he is involved in several Linux for zSeries Proof-of-Concept projects running at the TMCC.

Frank Kirschner is a consultant and IT specialist for trustsec IT solutions GmbH (Germany). He has worked with Linux since 1992, and is currently working for the IBM Technical Marketing Competence Center in Boeblingen (Germany). He is one of the maintainers of the Debian GNU/Linux distribution port for zSeries. His experience also includes security, OSS, and programming in Java™, Perl, and C.

Our thanks to the following people for their contribution to this paper:

Ulrich Boche, Timothy Hahn, Joel Hermann, Gregory Geiselhart, and Alison Chandler.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

This document created or updated on April 28, 2004.

Send us your comments in one of the following ways:

- Use the online **Contact us** review redbook form found at:
  ibm.com/redbooks
- Send your comments in an Internet note to:
  redbook@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYJ Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

@server®	z/VM®	Redbooks™
Redbooks (logo) ™	zSeries®	RACF®
ibm.com®	IBM®	S/390®
z/OS®		

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.