Title: DOMAIN SPECIFICATION SYSTEM FOR AN LDAP ACI ENTRY

Abstract: A domain specification system for an LDAP ACI entry provides a system for specifying an ACI domain entry in an access control command line that controls access to a resource. The access control command specifies resources using a Universal Resource Locator (URL) format that contains the name of the resource. A target scope value specifies the scope of access to be granted to a user which can be limited to a single entry, a subtree, or a single level. A search filter is part of the resource specification. The ACI applies only to entries in the subtree rooted at the resource name that match the filter. A list of attributes is also contained in the resource specification and the ACI applies only to attributes in the resource that are named in the list. The access control command specifies the type of access to be granted to a user which includes, but is not limited to: deny, read, write, and any other privileges that the system supports. The access control command also specifies the required user attributes for access to a resource. The directory server matches the required attributes with the accessing user’s attributes and grants the type of access listed only if the user has the required attributes.
For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
Domain Specification System for an LDAP ACI Entry

BACKGROUND OF THE INVENTION

TECHNICAL FIELD

The invention relates to accessing resources in a directory structure in a computer environment. More particularly, the invention relates to controlling access to resources within an LDAP directory structure in a computer environment.

DESCRIPTION OF THE PRIOR ART

A Lightweight Directory Access Protocol (LDAP) directory (such as Netscape Communications Corporation's Directory Server) is a collection of "entries." Each entry has a name (called the Distinguished Name) and a list of attribute values.

The entries in a directory are organized in a tree structure, with major groupings that are subdivided into smaller units. A directory might contain several organization entries, each of which contains several organizationalUnit entries. These entries can be further subdivided.

LDAP provides search operations that can be performed over specified portions of the directory tree. Trees and subtrees, therefore, are a natural way to deal with data stored in an LDAP directory.

Entries and attributes correspond to a wide variety of data types such as personnel information, server configuration, business relationships, and user preferences. Since all entries contain important information, a method is required to restrict the availability of specific information to authorized users.

The Netscape Directory Server allows an ACI entry to be created which controls access to data stored in the directory tree. The ACI entry contains rules to determine which users of the directory should be allowed to have access. One
of the components of the ACL rule is a description of which entries the rule applies to. The entry is essentially a resource specification (e.g., data, printers, servers, etc.).

The method used to control access in an LDAP system is via Access Control Lists (ACL). The Directory Server Administrator (DSAdmin) creates basic ACL rules that grant specific users access to entries in the directory.

Previous methods required the DSAdmin to specify separate attributes in the command line for a resource which was cumbersome and confusing. An additional problem with previous approaches was that the DSAdmin could not restrict the affect of the ACL to a single node or single level of nodes.

It would be advantageous to provide a domain specification system for an LDAP ACL entry that gives the system administrator the ability to easily specify resources that are accessible by a user. It would further be advantageous to provide a domain specification system for an LDAP ACL rule that allows the system administrator to restrict a user's access to a single node or single level of nodes.

**SUMMARY OF THE INVENTION**

The invention provides a domain specification system for an LDAP ACL rule. The system allows a system administrator to specify and control access to directory resources by specifying the resource using an easily understood standardized format. In addition, the invention provides a system that allows the system administrator to restrict a user's access to a single node or single level of nodes.

A preferred embodiment of the invention provides a system for specifying an ACL domain entry in an access control command line that controls access to a resource. The access control command specifies resources using a Universal Resource Locator (URL) format.

The resource specification contains the name of the resource. A target scope value specifies the scope of access to be granted to a user. The scope can be limited to a single entry, a subtree, or a single level.
A search filter is part of the resource specification. The ACL applies only to entries in the subtree rooted at the resource name that match the filter. A list of attributes is also contained in the resource specification and the ACL applies only to attributes in the resource that are named in the list.

The access control command specifies the type of access to be granted to a user which includes, but is not limited to: read, write, and any other privileges that the system supports.

The access control command also specifies the required user attributes or credentials for access to a resource. The directory server matches the required attributes with the accessing user's attributes and grants the type of access listed only if the user has the required attributes.

Other aspects and advantages of the invention will become apparent from the following detailed description in combination with the accompanying drawings, illustrating, by way of example, the principles of the invention.

**BRIEF DESCRIPTION OF THE DRAWINGS**

Fig. 1 is a diagram of an LDAP directory structure according to the invention; and

Fig. 2 is a block schematic diagram of an example of server interaction with user ACI rules and system resources according to the invention.

**DETAILED DESCRIPTION OF THE INVENTION**

The invention is embodied in an domain specification system for an LDAP ACI entry in a computer environment. A system according to the invention allows a system administrator to specify and control access to directory resources by specifying the resource using an easily understood standardized format. In addition, the invention provides a system that allows the system administrator to restrict a user's access to a single node or single level of nodes.

A Lightweight Directory Access Protocol (LDAP) directory (such as Netscape Communications Corporation's Directory Server) is a collection of "entries." Each
entry has a name (called the Distinguished Name) and a list of attribute values. The entries in a directory are organized in a tree structure, with major groupings that are subdivided into smaller units. A directory might contain several organization entries, each of which contains several organizationalUnit entries. These entries can be further subdivided.

LDAP provides search operations that can be performed over specified portions of the directory tree. Trees and subtrees, therefore, are a natural way to deal with data stored in an LDAP directory.

Entries and attributes correspond to a wide variety of data types such as personnel information, server configuration, business relationships, and user preferences. Since all entries are stored within a single directory, a method is required to restrict the availability of specific information to authorized users.

The Netscape Directory Server allows an ACI attribute to be created which controls access to data stored in the directory tree. The ACI attribute contains rules to determine which users of the directory should be allowed to have access.

Referring to Fig. 1, a simple LDAP directory structure is shown. The organization designation (o=Arius.com) 101 is at the root of the directory structure. Here, the directory structure contains a server subtree 102 and people subtree 103. Under each subtree are multiple related entries. In this example, a typical user entry 104 contains the user’s information such as the user’s name (here uid=prasanta) 105.

The method used to control access in an LDAP system is via Access Control Lists (ACL). The Directory Server Administrator (DSAadmin) creates basic ACL rules that grant specific users access to entries in the directory. The ACI entry 106 in the user’s entry 104 specifies resources that the user has access to by using ACL syntax.

Current Products

Previous approaches required three separate values to specify the domain of an ACI entry:

- target
- targetfilter
- targetattrs
Target

The name (Distinguished Name) of one of the LDAP entries. The ACI rule will apply to all entries in the subtree rooted at the specified entry.

Targetfilter

Specifies a standard LDAP search filter. The ACI rule will apply only to entries (as restricted by target) which match the filter.

Targetattrs

Specifies a list of attributes. The ACI rule will apply only to the named attributes with the directory entries.

The DSAdmin had to specify each of the values in a command line. For example:

aci: (target = "o=Arius.com") (targetattr = "cn, sn, mail, uid") (targetfilter = (position>level2)) allow(read) user=joe

However, the problem with the previous approaches was that the DSAdmin could not restrict the affect of the ACI to a single node or single level of nodes. Additionally, three separate values must be specified for the ACI, which is confusing.

A preferred embodiment of the invention adds a value called Targetscope that allows the ACI to be restricted to a more specific range. The ACI command line is also specified in an LDAP URL format, thereby standardizing the command line format.

Targetscope

One of the values BASE, SUB and ONE is specified. These values have the same meaning as defined for LDAP search operations (as specified by the Internet Engineering Task Force (IETF)) and define the scope of access (i.e., one entry, one level, or an entire subtree). The ACI entry will be restricted to the same set of entries as would be considered in an LDAP search.
A preferred embodiment of the invention improves the specification of the domain by allowing the user to apply the ACI rules to a single entry, entries at the next level of the tree only, or the entire subtree. Previous approaches could specify only the entire subtree. Various schemes for filtering the entries within the subtree have been used to approximate the results of the invention's targetscope method. However, none of the prior approaches can exactly match the invention's results.

Unifying the Rules: LDAP URL

The invention uses the LDAP Universal Resource Locator (URL) format to include all four components of the domain specification. An LDAP URL specification looks like:

```
```

When the LDAP URL applies to the current server, the <serverspec> portion is left empty. To describe the domain of an ACI, the other fields are filled with the data from the four values specified above. The URL form becomes:

```
```

The invention improves over previous approaches by bringing the complete description of the domain into a standard form which is already familiar to users.

Using the example above, the URL resource specification using all four values is as follows:

```
aci: (target = ldap://o=Arius.com?cn.sn.mail.uid?SUB?(position>level2))allow(read)user=joe
```

This follows the format:

```
aci: <resource><ALLOW/DENY><rights><condition>
```

where:
- rights = read, write, or any other privileges that the system recognizes.
- condition = the attribute requirements for user access.
With respect to Fig. 2, the Server 202 checks the ACI rule 201 for the resource when the user attempts access to a resource 203. The condition attributes are checked against the current user. If the ACI specification 201 allows the user access, then the Server 202 grants access to the resource 203.

Although the invention is described herein with reference to the preferred embodiment, one skilled in the art will readily appreciate that other applications may be substituted for those set forth herein without departing from the spirit and scope of the present invention. Accordingly, the invention should only be limited by the Claims included below.
CLAIMS

1. A process for specifying an ACI domain entry that controls access to a resource in a computer environment, comprising the steps of:
   providing a system administrator defined access control command;
   said access control command specifies the name of said resource;
   said access control command lists a target scope value;
   wherein said target scope specifies the scope of access to be granted to a user; and
   said access control command specifies the type of access to be granted to a user.

2. The process of Claim 1, wherein said type of access includes, but is not limited to: deny, read, write, and any other privileges that the system supports.

3. The process of Claim 1, wherein said access control command specifies the required user attributes for access to said resource.

4. The process of Claim 3, wherein the directory server matches said required attributes with the accessing user’s attributes and grants said type of access only if the user has said required attributes.

5. The process of Claim 1, wherein said access control command specifies said resource using a Universal Resource Locator (URL) format.

6. The process of Claim 1, wherein said access control command specifies a search filter; and wherein said access command applies only to entries that match said filter.

7. The process of Claim 1, wherein said access control command specifies a list of attributes; and wherein said access control command applies only to attributes in said resource that are listed in said list.

8. An apparatus for specifying an ACI domain entry that controls access to a resource in a computer environment, comprising:
   a system administrator defined access control command;
   said access control command specifies the name of said resource;
said access control command lists a target scope value;
wherein said target scope specifies the scope of access to be granted to
a user; and
said access control command specifies the type of access to be granted
to a user.

9. The apparatus of Claim 8, wherein said type of access includes, but is not
limited to: deny, read, write, and any other privileges that the system supports.

10. The apparatus of Claim 8, wherein said access control command specifies
the required user attributes for access to said resource.

11. The apparatus of Claim 10, wherein the directory server matches said
required attributes with the accessing user's attributes and grants said type of
access only if the user has said required attributes.

12. The apparatus of Claim 8, wherein said access control command specifies
said resource using a Universal Resource Locator (URL) format.

13. The apparatus of Claim 8, wherein said access control command specifies
a search filter; and wherein said access command applies only to entries that
match said filter.

14. The apparatus of Claim 8, wherein said access control command specifies
a list of attributes; and wherein said access control command applies only to
attributes in said resource that are listed in said list.

15. A program storage medium readable by a computer, tangibly
embodi ng a program of instructions executable by the computer to perform
method steps for specifying an ACI domain entry that controls access to a
resource in a computer environment, comprising the steps of:
providing a system administrator defined access control command;
said access control command specifies the name of said resource;
said access control command lists a target scope value;
wherein said target scope specifies the scope of access to be granted to
a user; and
said access control command specifies the type of access to be granted
to a user.
16. The method of Claim 15, wherein said type of access includes, but is not limited to: deny, read, write, and any other privileges that the system supports.

17. The method of Claim 15, wherein said access control command specifies the required user attributes for access to said resource.

18. The method of Claim 17, wherein the directory server matches said required attributes with the accessing user's attributes and grants said type of access only if the user has said required attributes.

19. The method of Claim 15, wherein said access control command specifies said resource using a Universal Resource Locator (URL) format.

20. The method of Claim 15, wherein said access control command specifies a search filter; and wherein said access command applies only to entries that match said filter.

21. The method of Claim 15, wherein said access control command specifies a list of attributes; and wherein said access control command applies only to attributes in said resource that are listed in said list.
AMENDED CLAIMS

[received by the International Bureau on 07 June 2001 (07.06.01);
original claims 1, 5, 8, 12, 15, 19 amended; remaining claims unchanged (4 pages)]

1. A process for specifying an ACI domain entry that controls access to a resource in a computer environment, comprising the steps of:
   5 providing a system administrator defined access control command;
   said access control command specifies the name of said resource;
   said access control command lists a target scope value;
   wherein said target scope specifies the scope of access to be granted to a user;
   wherein said access control command specifies the type of access to be granted to a user; and
   wherein said access control command is expressed in an LDAP Universal Resource Locator (URL) format in an ACI rule.

2. The process of Claim 1, wherein said type of access includes, but is not limited to: deny, read, write, and any other privileges that the system supports.

3. The process of Claim 1, wherein said access control command specifies the required user attributes for access to said resource.

4. The process of Claim 3, wherein the directory server matches said required attributes with the accessing user's attributes and grants said type of access only if the user has said required attributes.
5. The process of Claim 1, wherein said target scope value specifies one of the values: BASE, SUB, or ONE.

6. The process of Claim 1, wherein said access control command specifies a search filter; and wherein said access command applies only to entries that match said filter.

7. The process of Claim 1, wherein said access control command specifies a list of attributes; and wherein said access control command applies only to attributes in said resource that are listed in said list.

8. An apparatus for specifying an ACI domain entry that controls access to a resource in a computer environment, comprising:
   a system administrator defined access control command;
   said access control command specifies the name of said resource;
   said access control command lists a target scope value;
   wherein said target scope specifies the scope of access to be granted to a user; and
   wherein said access control command specifies the type of access to be granted to a user; and
   wherein said access control command is expressed in an LDAP Universal Resource Locator (URL) format in an ACI rule.

9. The apparatus of Claim 8, wherein said type of access includes, but is not limited to: deny, read, write, and any other privileges that the system supports.
10. The apparatus of Claim 8, wherein said access control command specifies the required user attributes for access to said resource.

11. The apparatus of Claim 10, wherein the directory server matches said required attributes with the accessing user’s attributes and grants said type of access only if the user has said required attributes.

12. The apparatus of Claim 8, wherein said target scope value specifies one of the values: BASE, SUB, or ONE.

13. The apparatus of Claim 8, wherein said access control command specifies a search filter; and wherein said access command applies only to entries that match said filter.

14. The apparatus of Claim 8, wherein said access control command specifies a list of attributes; and wherein said access control command applies only to attributes in said resource that are listed in said list.

15. A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for specifying an ACI domain entry that controls access to a resource in a computer environment, comprising the steps of:
   providing a system administrator defined access control command;
   said access control command specifies the name of said resource;
   said access control command lists a target scope value;
wherein said target scope specifies the scope of access to be granted to a user; and

wherein said access control command specifies the type of access to be granted to a user; and

wherein said access control command is expressed in an LDAP Universal Resource Locator (URL) format in an ACI rule.

The method of Claim 15, wherein said type of access includes, but is not limited to: deny, read, write, and any other privileges that the system supports.

The method of Claim 15, wherein said access control command specifies the required user attributes for access to said resource.

The method of Claim 17, wherein the directory server matches said required attributes with the accessing user's attributes and grants said type of access only if the user has said required attributes.

The method of Claim 15, wherein said target scope value specifies one of the values: BASE, SUB, or ONE.

The method of Claim 15, wherein said access control command specifies a search filter; and wherein said access command applies only to entries that match said filter.
FIG. 1

dn: uid=prasantac,ou=People,c=Arius.com,c=US
sn: Behera
uid: prasantac
employeetype: employee
mail: prasantac@arius.com
telephonenum: 9999
objectclass: top
objectclass: person
ou: R&D Development
ou: Server Applications Division
l: Mountainview
cn: Prasantac Behera
aci: ACL Syntax

FIG. 2

User

Server

Resource

ACL

201

202

203
**INTERNATIONAL SEARCH REPORT**

**A. CLASSIFICATION OF SUBJECT MATTER**

IPC 7 H04L29/12 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database consulted during the international search (name of database and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX, IBM-TDB

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
</table>

Further documents are listed in the continuation of box C.

* Special categories of cited documents:
  * "A" document defining the general state of the art which is not considered to be of particular relevance
  * "E" earlier document but published on or after the international filing date
  * "I" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another document or other special reason (as specified)
  * "O" document referring to an oral disclosure, use, exhibition or other means
  * "P" document published prior to the international filing date but later than the priority date claimed

* "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

* "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

* "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

* "A" document member of the same patent family

Date of the actual completion of the international search: 21 March 2001

Date of mailing of the international search report: 09/04/2001

Name and mailing address of the ISA
European Patent Office, P.6, 5201 Patentlaan 2 NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Fax. 31 851 epo nl, Fax: (+31-70) 340-3016

Authorized officer: Lievens, K
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>&quot;COMMAND LINE METHOD FOR MANAGING ACCESS CONTROL PROFILES FOR ALIASES&quot; IBM TECHNICAL DISCLOSURE BULLETIN, IBM CORP., NEW YORK, US, vol. 38, no. 6, 1 June 1995 (1995-06-01), pages 513-514, XP000520755 ISSN: 0018-8689 the whole document</td>
<td>1-21</td>
</tr>
</tbody>
</table>