Network Working Group
INTERNET DRAFT
Intended Category: Experimental

L. Hedstrom
Independent Consultant
L. Howard
PADL Software Pty. Ltd.
D. Siegmund
Apple Computer, Inc.

Expires in six months from 3 May 2002

DHCP Options for Locating LDAP Servers
<draft-hedstrom-dhc-ldap-02.txt>

Status of this Memo

Notice

their respective owners.

Abstract

This document defines a new DHCP option for delivering configuration information to LDAP (Lightweight Directory Access Protocol) clients. The information returned is represented as LDAP URLs, as specified in the LDAPv3 URL draft[1].

The DHCP client may use the URLs returned by the DHCP server to locate an LDAP server for the client's network. The URL may include the TCP port of the LDAP server, and the distinguished name which identifies the base object for searching.

1. Introduction

This draft defines a new option in the Bootstrap Protocol (BOOTP) and the Dynamic Host Configuration Protocol (DHCP)[1],[2] to enable LDAP clients to find LDAP servers, their ports and base distinguished names (DNs), among other attributes. The configuration is returned to the DHCP client as a list of LDAP URLs (according to the syntax defined in [3]).

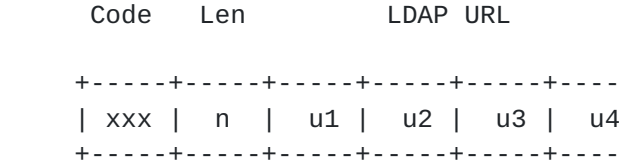
The LDAP server name, or IP address, is mandatory. The LDAP port number is optional; the default assigned port is 389. While the the base DN is also optional, we anticipate that it will normally be specified. Even if the base DN is specified in the DHCP message, it may be ignored by the client in preference of a locally defined DN.

LDAP attribute list and filter components may be specified, but they are optional and can be ignored by the client. The clients must honor the LDAP search scope, if present in the returned URLs.

2. LDAP option

This option specifies one or more LDAP URLs for the client to use to access LDAP servers. URLs should be listed in order of preference (notwithstanding section 3 of this document). Multiple URLs are separated with a literal space.

The code for this option is <xxx>. Its minimum length is 1.



In the following examples, the value of the option is shown as a

string enclosed in double-quotes. The quotes themselves are not part of the option value, they are shown merely to delimit the start and end of the option.

This example specifies the LDAP server, and the base DN:

"ldap://ldap.ace.com/o=Ace%20Industries"

LDAP over SSL is supported using the ldaps protocol, e.g.

"ldaps://ldap.ace.com:636/o=Ace%20Industries"

This example specifies multiple URLs:

"ldap://my.ace.com/o=My%20Ace ldap://ldap.ace.com/o=Ace%20Industries"

3. URL extensions for server location

Two new extensions are defined, x-weight and x-priority. Both these extensions are optional, and it is not required that they be supported by an LDAP client using DHCP in the manner described above.

The extensions have the same meanings as defined in RFC2782 [4]. The client must attempt to contact the target host with the lowest-numbered priority (denoted by x-priority) it can reach, and target hosts with the same priority should be tried in pseudo random order. The syntax of the x-priority extension is an integer in the range 0-65535.

When selecting a target from those that have the same priority, the chance of contacting a specific one should be proportional to its weight. The syntax of the x-weight extension is an integer in the range 1-65535. When there is no load balancing to be done, the weight should be zero or the extension omitted. If the x-priority extension is omitted, then the order of URLs returned determines their preference.

For example:

ldap://ldap.ace.com/o=Ace%20Industries??sub??x-weight=0,x-priority=10

denotes the LDAP server ldap.ace.com, serving the naming context o=Ace Industries, with a weight of 0 and a priority of 10.

4. URL extensions for server binding

The bindname extension, defined in [3], may be used to specify the

distinguished name with which the LDAP client should bind to the server.

The x-bindpw extension (defined here) may be used to provide the client with bind credentials for binding to an LDAP server, although it should be noted that this information may be easily retrieved by malicious DHCP clients, and is thus of little use.

5. Security considerations

Security considerations discussed in [3], particularly with respect to the provision of authentication information, are directly applicable here. Additionally, it should be noted that providing LDAP server information by a broadcast protocol such as DHCP may allow unauthorized clients to learn the location of and authentication information for LDAP servers and hence pose as valid clients. This presents a security problem when sensitive information, such as user passwords, is published via LDAP servers.

The DHCP protocol provides no mechanisms for the client to verify the validity and correctness of the received information. The security considerations in [1] discuss several weaknesses, particularly the problem with unauthorized DHCP servers.

References

[1] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131.

[2] Alexander, S., and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132.

[3] T. Howes and M. Smith., "The LDAP URL Format", RFC 2255.

[4] Vixie, P., A. Gulbrandsen and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782.

Authors' Addresses

Leif Hedstrom
23 Terrace Ave
Half Moon Bay, CA
USA
leif@ogre.com

Luke Howard
PO Box 59
Central Park Vic 3145
Australia
lukeh@padl.com

Dieter Siegmund
1 Infinite Loop
MS 302-4K
Cupertino, CA 95014
USA
dieter@apple.com