Network Working Group
Internet-Draft
Expires: March 2007

Giuseppe Paterno'
Independent Consultant
September 2006

DHCP Option for LDAP Directory Services discovery

Status of this Memo

Abstract

This document defines an experimental DHCP option for delivering configuration information for LDAP services. Through this option, the client receives an LDAP URL [8] of the closest available LDAP server/replica that can be used to authenticate users or look up any useful data.

1. Introduction

The Lightweight Directory Access Protocol (LDAP) [1] is an access protocol for directories. LDAP allows distributed environment so that replica copies exists into a given organization or even the Internet. In most organizations, LDAP is used to allow user authentication and databases lookup such as hosts, groups or e-mail addresses.

The current methodologies of defining LDAP parameters are limited to statically configuring the servers into the clients or seldom by specifying them into the appropriate DNS RR records [2]. The disadvantage of the first solution is that the client is unable to dynamically reconfigure/provision the system, while the disadvantage of the last solution is that the client is unable to locate the closest available replica, therefore not optimizing the network for large organizations.

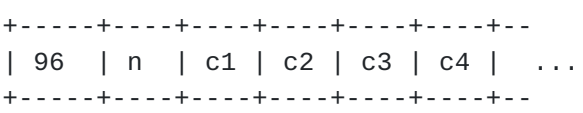
The need is to have a methodology to autoconfigure LDAP clients with the closest available replica: the advantages provide relief in administration tasks and optimization of configuration of mobile clients (ex: laptops, PDAs, ...) or devices (ex: multifunction printers, IP phones, ...).

This specification describe an experimental DHCP option [5] that carries LDAP information for the clients of the network. The LDAP URL Option delivers an LDAP URL string to the client in accordance to RFC 2255 [8]. An LDAP URL contains several useful information, such as Base DN or search scope, that helps the client in looking up information on the LDAP server.

2. LDAP URL Option

This option specifies the LDAP URL that the client will autoconfigure for the directory lookups. The LDAP URL option has to be encoded in accordance of RFC 2255 [8] and the string should NOT be zero terminated.

The code for this option is 95. The maximum possible length for this option is 255 bytes. Note: this option is listed in [4], but has to be confirmed by IANA. See IANA Considerations for details.



3. Considerations on LDAP access

The Base DN is not always enough to lookup an entry in the LDAP directory, expecially when user authentication and profiling (UID, GID, ...) is involved. The LDAP directory might be structured in different ways in the organization and cannot be determined in advance. As such, whenever is not specified, for user authentication/profiling the client should lookup information as for RFC-2307 [3], i.e.:

- Users should be under the "ou=People" organizational unit;
- Groups should be under the "ou=Group" organizational unit;
- Hosts should be under the "ou=Hosts" organizational unit.

Geographically distributed environments should have a different Base DN for countries or locations and DHCP hosts in that location should receive LDAP Base DN accordingly, es: "dc=italy, dc=example, dc=com".

This hierarchy is recommended, but not mandatory. If the hierarchy can't be defined in advance, a subtree scope is highly recommended. The client, be either an authentication mechanism or a general lookup (say an e-mail client), MUST perform a subtree search of the base DN when the "sub" scope have been specified in the LDAP URL.

4. Security Considerations

DHCP currently provides no authentication or security mechanisms. Potential exposures to attack are discussed in section 7 of the DHCP protocol specification [5]. In particular, these DHCP options allow an unauthorized DHCP server to misdirect an LDAP client to a nonexistent LDAP server or even a spoofed LDAP server. These threats are similar to any DHCP options specified. Whenever any potential intruder might connect to the network (say for example in a Wireless environment), the author suggests to introduce IEEE 802.1x to enforce network access.

Whenever sensitive information has to be looked up in the LDAP directory, the author strongly suggests to use SSL to secure the communication channel between the client and the server. This MUST be specified by providing "ldaps" as the URL scheme (eg: "ldaps://ldap.example.com/").

For security reason, an administrator or even default server configuration might deny anonymous bind the to LDAP server. Although the bindname extension can be used (as for [8]), the author suggests not to specify such option because DHCP information are sent over a clear channel, therefore can be easily eavesdropped. The author suggests two methodologies. The first is to use a restricted

anonymous access to LDAP: through the use of ACLs/ACIs is possible to restrict information that an anonymous clients might request/receive. The second -preferred- is that the client should use its own credential (be a human user or a machine account), such as kerberos ticket or PKI certificate, to authenticate against the LDAP server.

5. IANA Considerations

IANA has assigned a value of 95 for the DHCP LDAP server option described in this document. However this option has been recovered [4] because no-one has published an RFC and therefore is ready to be reassigned: it has to be confirmed by IANA.

6. References

[1] Wahl, M., Howes, T. and S. Kille,
"Lightweight Directory Access Protocol (v3)",
RFC-2251, December 1997.

[2] A. Gulbrandsen, P. Vixie,
"A DNS RR for specifying the location of services (DNS SRV)",
RFC-2052, October 1996.

[3] L. Howard,
"An Approach for Using LDAP as a Network Information Service",
RFC-2307, March 1998.

[4] R. Droms,
"Unused Dynamic Host Configuration Protocol (DHCP) Option Codes",
RFC-3679, January 2004.

[5] Alexander, S. and R. Droms,
"DHCP Options and BOOTP Vendor Extensions",
RFC-2132, March 1997.

[6] Bradner, S.,
"Key words for use in RFCs to Indicate Requirement Levels",
RFC-2119, March 1997.

[7] Droms, R.,
"Dynamic Host Configuration Protocol",
RFC-2131, March 1997.

[8] T. Howes, M. Smith,
"The LDAP URL Format"
RFC-2255, December 1997

[9] J. Hodges, R. Morgan, M. Wahl,

"Lightweight Directory Access Protocol (v3):
Extension for Transport Layer Security",
RFC-2830, May 2000

7. Author's Address

Giuseppe Paterno'
Casella Postale 27
20090 Trezzano Sul Naviglio (MI)
Italy
E-mail: gpaterno@gpaterno.com