INTERNET-DRAFT
Document: draft-ietf-crisp-lw-user-00.txt
Expires: January, 2003
Category: Experimental

Eric A. Hall
July 2002

Defining and Locating Contact Persons using the Internet Resource Query Service

1. Abstract

This document defines LDAP schema and searching rules for contact persons, in support of the Internet Resource Query Service described in [ldap-whois].

2. Definitions and Terminology

This document unites, enhances and clarifies several pre-existing technologies. Readers are expected to be familiar with the following specifications:

RFC 2247 - Using Domains in LDAP/X.500 DNs

RFC 2251 - Lightweight Directory Access Protocol (v3)

RFC 2252 - Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions.

RFC 2254 - The String Representation of LDAP Search Filters

RFC 2798 - Definition of the inetOrgPerson LDAP Object Class

[ir-dir-req] - <draft-newton-ir-dir-requirements-00.txt> - Internet Registry Directory Requirements

[ldap-whois] - <draft-ietf-crisp-lw-core-00.txt> - The Internet Resource Query Service and the Internet Resource Schema

The following abbreviations are used throughout this document:

DIT (Directory Information Tree) - A DIT is a contained branch of the LDAP namespace, having a root of a particular distinguished name. "dc=example,dc=com" is used throughout this document as one DIT, with many example entries being stored in this DIT.

DN (Distinguished Name) - A distinguished name provides a unique identifier for an entry, through the use of a multi-level naming syntax. Entries are named according to their location relevant to the root of their containing DIT. For example, "cn=inetResources,dc=example,dc=com" is a DN which uniquely identifies the "inetResources" entry within the "dc=example,dc=com" DIT.

RDN (Relative DN) - An RDN provides a locally-scoped unique identifier for an entry. A complete, globally-unique DN is formed by concatenating the RDNs of an entry together. For example, "cn=admins,cn=inetResources,dc=example,dc=com"

consists of two RDNs ("cn=admins" and "cn=inetResources") within the "dc=example,dc=com" DIT. RDNs are typically only referenced within their local scope.

OID (Object Identifier) - An OID is a globally-unique, concatenated set of integers which provide a kind of "serial number" to attributes, object classes, syntaxes and other schema elements.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

3. The inetOrgPerson Object Class

This document provides several contact-related attributes which use LDAP URLs to reference inetOrgPerson entries. Whenever one of these contact attributes are returned, a separate query for the inetOrgPerson entry associated with the contact attribute will be required if the details of that contact are needed. In order to facilitate programmatic access to this data, LDAP URLs provided in contact attributes MUST refer to entries which use the inetOrgPerson object class, MUST refer to an entry in a DIT which uses the domainComponent object class syntax ("dc="), and MUST specify the LDAP or LDAPS protocol-types for the URL.

The model put forth in this document allows each contact attribute to refer to a variable number of contacts. In this model, a query for a contact attribute MAY return a variable number of LDAP URLs, and each of these contacts can then be queried individually. This allows for multiple explicit contacts per role, while also providing predictable naming and query structures.

The target entries MAY exist anywhere in the LDAP hierarchy (as long as they follow the domainComponent naming syntax). It is expected that pre-existing inetOrgPerson entries will be used for this purpose. If this is not desirable or feasible, then an entry MUST be created which meets the minimum requirements defined in this document. Regardless of where the entry is located, the target inetOrgPerson entries MUST conform with the schema specification defined in RFC 2798.

The target inetOrgPerson entries MAY have any number of attributes defined, with any number of access restrictions, as required by local security policies, government regulations or personal

privacy concerns. However, the mail attribute MUST be defined, MUST be valid, and MUST have anonymous read permissions. Furthermore, all of the attributes MUST be secured against anonymous add, delete and modify permissions.

4. inetOrgPerson equalityMatch

The inetOrgPerson object class entries can be searched using relatively simple equalityMatch filters.

In order to ensure that all of the relevant entries (including any referrals) are found, the search filters for these resources MUST specify two distinct elements: the object class of the resource being queried, and the naming element of the resource specified as a distinguished name attribute.

For example, using the notation format described in RFC 2254, the search filter expression for the inetOrgPerson entry associated with "cn=admins,ou=admins,dc=example,dc=com" would be structured as "(&(objectclass=inetOrgPerson)(cn:dn:=admins))", using "ou=admins,dc=example,dc=com" as the search base. This would find all entries with the object class of inetOrgPerson (including all of the referral entries for inetOrgPerson entries) where the distinguished name contained the "cn" attribute of "admins".

The input source and search base for these matches will vary according to the query being processed, but whenever an equalityMatch is called for during query processing, the above methods MUST be used in order to ensure that all of the related entries are located.

Response entries MAY be fully-developed entries, or MAY be referrals generated from entries which have the referral object class defined. Any attribute values which are received MUST be displayed by the client. If a subordinate reference referral is received, the client MUST restart the query, using the provided data as the new search base. If any continuation reference referrals are received, the client SHOULD start new queries for each reference, and append the output of those queries to the original query's output.

5. Security Considerations

This document describes an application of the LDAPv3 protocol, and as such it inherits the security considerations associated with LDAPv3, as described in section 7 of RFC 2251.

By nature, LDAP is a read-write protocol, while the legacy WHOIS service has always been a read-only service. As such, there are significant risks associated with allowing unintended updates by unauthorized third-parties. Moreover, allowing the LDAP-WHOIS service to update the underlying delegation databases could result in network resources being stolen from their lawful operators. For example, if the LDAP front-end had update access to a domain delegation database, a malicious third-party could theoretically take ownership of that domain by exploiting an authentication weakness, thereby causing ownership of the domain to be changed to another party. For this reason, it is imperative that the LDAP-WHOIS service not be allowed to make critical modifications to delegated resources without ensuring that all possible precautions have been taken.

The query processing models described in this document make use of DNS lookups in order to locate the LDAP servers associated with a particular resource. DNS is susceptible to certain attacks and forgeries which may be used to redirect clients to LDAP servers which are not authoritative for the resource in question.

Some operators may choose to purposefully provide misleading or erroneous information in an effort to avoid responsibility for bad behavior. In addition, there are likely to be sporadic operator errors which will result in confusing or erroneous answers.

This document provides multiple query models which will cause the same query to be answered by different servers (one would be processed by a delegation entity, while another would be processed by an operational entity). As a result, each of the servers may provide different information, depending upon the query type that was originally selected.

For all of the reasons listed above, it is essential that applications and end-users not make critical decisions based on the information provided by the LDAP-WHOIS service without having reason to believe the veracity of the information. Users should limit unknown or untrusted information to routine purposes.

Finally, there are physical security issues associated with any service which provides physical addressing and delivery information. Although organizations are generally encouraged to provide as much information as they feel comfortable with, no information is required.

6. IANA Considerations

This document defines an application of the LDAPv3 protocol rather than a new Internet application protocol. As such, there are no protocol-related IANA considerations.

However, this document does define several LDAP schema elements, including object classes, attributes, syntaxes and extensibleMatch filters, and these elements should be assigned OID values from the IANA branch, rather than being assigned from a particular enterprise branch.

Finally, this document also describes several instances where public DNS and LDAP servers are queried. It is expected that IANA will establish and maintain these LDAP servers (and the necessary DNS SRV domain names and resource records) required for this service to operate. This includes providing SRV resource records in the generic TLDs and the root domain, and also includes administering the referenced LDAP servers.

7. Author's Addresses

Eric A. Hall
ehall@ehsco.com

8. References

RFC 2247 - Using Domains in LDAP/X.500 DNs

RFC 2251 - Lightweight Directory Access Protocol (v3)

RFC 2252 - Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions.

RFC 2254 - The String Representation of LDAP Search Filters

[ir-dir-req] - <draft-newton-ir-dir-requirements-00.txt> - Internet Registry Directory Requirements

[ldap-whois] - <draft-ietf-crisp-lw-core-00.txt> - The Internet Resource Query Service and the Internet Resource Schema

9. Acknowledgments

Portions of this work were funded by Network Solutions, Inc.