Internet Draft
<draft-bannister-dbis-netgroup-05.txt>
Category: Informational
Expires January 25, 2016

M. R. Bannister
Prose Consulting Ltd.

July 24, 2015

# Directory-Based Information Services: Netgroups and Netservices

## Status of this Memo

Distribution of this memo is unlimited.

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 25, 2016.

Comments are solicited and should be addressed to the author.

## Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This document extends Directory-Based Information Services (DBIS) described in [draft-bannister-dbis-mapping-00] to support netgroup and netservice databases.

A netgroup database schema SHALL be backwards compatible with the Network Information Service [NIS] but stored within [X.500] entries so that they may be resolved with the Lightweight Directory Access Protocol [RFC4510]. A netgroup database represents groups of hosts, users and domains.

A netservice database schema is a new extension to netgroups that allows administrators to describe services or configuration options for a user or system based upon their netgroup membership.

This document describes configuration maps [draft-bannister-dbis-mapping-00] for netgroup and netservice databases, and database entries referenced by those maps.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED" and "MAY" in this document are to be interpreted as described in [RFC2119].

Table of Contents

## 1. Concepts

### 1.1. Domains

The term "domain" used within this document does not refer to DBIS domains [draft-bannister-dbis-mapping-00] but rather to DNS domains [RFC1034].

### 1.2. Common ABNF Productions

A number of attributes in this document are described using ABNF notation defined in [RFC5234]. These attributes rely on the productions defined below as well as those defined in section 1.4 of [RFC4512]:

```
ALPHA-LOW   = %x61-7A   ; lowercase "a"-"z"
ASTERISK    = %x2A      ; asterisk "*"
ATSIGN      = %x40      ; at sign "@"
COLON       = %x3A      ; colon ":"
SLASH       = %x2F      ; forward slash "/"

non-alpha   = DIGIT / HYPHEN / USCORE
keyname     = 1*(ALPHA / non-alpha)
keyname-low = 1*(ALPHA-LOW / non-alpha)
```

## 2. Configuration Maps

### 2.1. Scope

All databases described in this document use the standard configuration maps defined in [draft-bannister-dbis-mapping-00], section 3.

Additionally, dbisMapConfig entries for netgroup and netservice databases SHALL have assigned the object classes dbisNetgroupConfig and dbisNetserviceConfig respectively.

It is RECOMMENDED that the dbisMapConfig entry for a netgroup or netservice database have the dbisMapFilter attribute set according to the following table:

| Database | dbisMapFilter |
|---|---|
| netgroup | objectClass=netgroupObject |
| netservice | objectClass=netserviceDescriptor |

### 2.2. Example Configuration Map Entries

The following gives an example of a configuration map entry for a netgroup database:

```
dn: cn=netgroup,en=sales.corp,ou=domain-mappings,o=infra
objectClass: top
objectClass: dbisMapConfig
```

```
    objectClass: dbisNetgroupConfig
    cn: netgroup
    dbisMapDN: cn=netgroup,ou=dbis,o=infra
    dbisMapFilter: objectClass=netgroupObject
    profileTTL: 900
    description: Primary netgroup database
```

The following gives an example of a configuration map entry for a netservice database:

```
    dn: cn=netservice,en=sales.corp,ou=domain-mappings,
     o=infra
    objectClass: top
    objectClass: dbisMapConfig
    objectClass: dbisNetserviceConfig
    cn: netservice
    dbisMapDN: cn=netservice,ou=dbis,o=infra
    dbisMapFilter: objectClass=netserviceDescriptor
    profileTTL: 900
    description: Primary netservice database
```

## 3. Database

### 3.1. netgroup

#### 3.1.1. Definition

A netgroup database contains entries that represent hosts, users and domains and which are associated with a case sensitive netgroup name.

DBIS netgroups allow groups of users and hosts to be defined with the following scope variance:

- All users on all hosts in a given domain.

- All users on specific hosts.

- Named users regardless of host.

- Named users on all hosts in a given domain.

- Named users on specific hosts.

#### 3.1.2. Object Classes

##### 3.1.2.1. Introduction

A dbisMapConfig entry for a netgroup database SHALL be assigned the

object class dbisNetgroupConfig.

A netgroup SHALL be defined by an LDAP entry with the object class netgroupObject.

#### 3.1.2.2. dbisNetgroupConfig

The dbisNetgroupConfig class is defined as follows:

```
objectclass ( 1.3.6.1.4.1.23780.219.1.3 NAME 'dbisNetgroupConfig'
  DESC 'DBIS netgroup configuration map'
  SUP dbisMapConfig STRUCTURAL )
```

#### 3.1.2.3. netgroupObject

The netgroupObject class is defined as follows:

```
objectclass ( 1.3.6.1.4.1.23780.219.1.4 NAME 'netgroupObject'
  DESC 'DBIS netgroup entry'
  SUP top STRUCTURAL
  MUST en
  MAY ( netgroupHost $ netgroupUser $ netgroupTriple $
        exactNetgroup $ description $ manager $ disableObject ) )
```

### 3.1.3. Attributes

#### 3.1.3.1. en

The name of the netgroup is stored in the LDAP attribute en which is defined in [draft-bannister-dbis-mapping-00]. The en attribute MUST be associated with a netgroupObject entry and SHALL form the RDN.

If required, alias entries may be defined according to section 2.6 of [RFC4512] and as permitted by section 1.2 of [draft-bannister-dbis-mapping-00].

#### 3.1.3.2. netgroupHost

A host that is a member of a netgroup is stored in the netgroupHost attribute that MAY be assigned to a netgroupObject entry:

```
attributetype ( 1.3.6.1.4.1.23780.219.2.8 NAME 'netgroupHost'
  DESC 'Host or domain that is assigned to a netgroup'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

The string representation of the netgroupHost attribute SHALL match the following grammar, which uses the common ABNF productions defined

in section 1.2 of this document:

```
host             = keyname-low
domain           = keyname-low *(DOT keyname-low)
host-domain      = host DOT domain
all-domain       = ASTERISK DOT domain

netgroupHost     = host / host-domain / all-domain
```

A DUA SHALL de-reference any aliases and convert host name and domain name components to lower case characters prior to forming a netgroupHost attribute or filter containing one. This is explained further in section 6.2 of this document.

#### 3.1.3.3. netgroupUser

A user who is a member of a netgroup is stored in the netgroupUser attribute that MAY be assigned to a netgroupObject entry:

```
attributetype ( 1.3.6.1.4.1.23780.219.2.9 NAME 'netgroupUser'
  DESC 'User who is assigned to a netgroup'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )
```

The string representation of the netgroupUser attribute SHALL match the following grammar, which uses the common ABNF productions defined in section 1.2 of this document as well the productions defined in section 3.1.3.2:

```
user             =  keyname
user-host        =  user ATSIGN host
user-host-domain =  user ATSIGN host-domain
user-all-domain  =  user ATSIGN all-domain

netgroupUser     =  user / user-host
netgroupUser     =/ user-host-domain / user-all-domain
```

A DUA SHALL convert host name and domain name components to lower case characters prior to forming a netgroupUser attribute or filter containing one. This is explained further in section 6.2 of this document.

#### 3.1.3.4. netgroupTriple

For backwards compatibility with RFC2307 client software, DBIS also permits netgroup membership to be expressed in the form of netgroup triples (see section 6.1) by providing one or more netgroupTriple

attributes that MAY be assigned to a netgroupObject entry:

```
attributetype ( 1.3.6.1.4.1.23780.219.2.37 NAME 'netgroupTriple'
  DESC 'Case exact netgroup triple'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

A DUA SHALL convert host name and domain name components to lower case characters prior to forming a netgroupTriple attribute or filter containing one. This is explained further in section 6.2 of this document.

#### 3.1.3.5. exactNetgroup

Members of other netgroups may be inherited by this netgroup by providing additional netgroup names to inherit in one or more exactNetgroup attributes that MAY be assigned to a netgroupObject entry:

```
attributetype ( 1.3.6.1.4.1.23780.219.2.10 NAME 'exactNetgroup'
  DESC 'Case exact netgroup name associated with this entry'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )
```

The DUA SHALL validate that a netgroup referenced by this attribute exists and is enabled. If the netgroup is not defined, or if it has been disabled with the disableObject attribute, then it SHALL NOT be included in the response to the client.

#### 3.1.3.6. description

The description attribute MAY be associated with a netgroupObject entry to provide an arbitrary description of the entry.

#### 3.1.3.7. manager

The manager attribute MAY be associated with a netgroupObject entry to provide one or more DNs of the individuals, groups or systems that are responsible for maintaining the entry.

#### 3.1.3.8. disableObject

A netgroup entry MAY be disabled by setting the disableObject attribute [draft-bannister-dbis-mapping-00] to TRUE. If an entry is disabled, then the DUA SHALL behave as if the netgroup does not exist. The DUA MAY optionally provide a separate mechanism for

listing disabled entries, but they MUST be clearly marked as disabled so that no confusion can arise.

### 3.1.4. Example Netgroup Entry

The following is an example of a netgroupObject entry in LDIF format [RFC2849]:

```
dn: en=sales-mgmt,ou=netgroup,ou=sales,o=infra
objectClass: top
objectClass: netgroupObject
en: sales-mgmt
netgroupHost: picard.sales.corp
netgroupHost: *.fleet.sales.corp
netgroupUser: mark@riker.sales.corp
netgroupUser: julie@*.market.sales.corp
exactNetgroup: board-mgmt
exactNetgroup: board-mgmt-remote
description: Sales Management Privileges
```

### 3.1.5. Determining Host Membership

A DUA SHOULD perform a reverse DNS lookup of a host's primary IP address in order to determine the fully-qualified domain name to be used for netgroup matching. A host MUST meet one of the following conditions to be considered a member of a netgroup:

a) Unqualified host name converted to lowercase matches netgroupHost attribute exactly. In this scenario the netgroupHost attribute is also unqualified.

b) Fully-qualified host name converted to lowercase matches netgroupHost attribute exactly.

c) The netgroupHost attribute uses the all-domain pattern, and the fully-qualified domain name converted to lowercase matches this attribute when the ASTERISK DOT prefix is removed.

### 3.1.6. Determining User Membership

A user MUST meet one of the following conditions to be considered a member of a netgroup:

a) The netgroupUser attribute contains no ATSIGN and the user name matches the netgroupUser attribute exactly.

b) The user name matches the user component of the netgroupUser attribute exactly, and the unqualified host name of the DUA which

is obtained as described in section 3.1.5 and converted to lowercase matches the host component of the netgroupUser attribute exactly.

c) The user name matches the user component of the netgroupUser attribute exactly, and the fully-qualified host name of the DUA which is obtained as described in section 3.1.5 and converted to lowercase matches the host-domain component of the netgroupUser attribute exactly.

d) The user name matches the user component of the netgroupUser attribute exactly, the netgroupUser attribute uses the all-domain pattern and the fully-qualified domain name of the DUA which is obtained as described in section 3.1.5 and converted to lowercase matches this attribute when the ASTERISK DOT prefix is removed.

## 3.2. netservice

### 3.2.1. Definition

A netservice database maps netgroups to services and privileges. Netservices may be used to determine what applications should run on a host, how they should be configured, and what actions users can or cannot perform.

The string representation of the fully-qualified netservice name SHALL match the following grammar, which uses the common ABNF productions defined in section 1.2 of this document:

```
service-name       = keyname
service-descriptor = keyname *(SLASH keyname)

en                 = service-name COLON service-descriptor
```

The service-name component identifies the service, while the service-descriptor is a path delimited by forward slashes that identifies a sub-component or subsystem within the service. An application is free to interpret the name of a netservice in whichever way it suits, although it is suggested that a netservice identifies either a privilege or a configuration that can be applied at the host-level or user-level.

The service-name is represented in LDAP by an entry with the netserviceObject class. Each slash-delimited component of the service-descriptor are child objects in LDAP with the netserviceDescriptor class.

### 3.2.2. Object Classes

#### 3.2.2.1. Introduction

A dbisMapConfig entry for a netservice database SHALL be assigned the object class dbisNetserviceConfig.

A netservice SHALL be defined by an LDAP entry with the object class netserviceObject.

#### 3.2.2.2. dbisNetserviceConfig

The dbisNetserviceConfig class is defined as follows:

```
objectclass ( 1.3.6.1.4.1.23780.219.1.5
  NAME 'dbisNetserviceConfig'
  DESC 'DBIS netservice configuration map'
  SUP dbisMapConfig STRUCTURAL )
```

#### 3.2.2.3. netserviceObject

The netserviceObject class SHALL be assigned to the entry that represents the service-name and is defined as follows:

```
objectclass ( 1.3.6.1.4.1.23780.219.1.6 NAME 'netserviceObject'
  DESC 'DBIS netservice top-level entry'
  SUP netserviceDescriptor STRUCTURAL
  MUST en
  MAY ( description $ manager $ disableObject ) )
```

#### 3.2.2.4. netserviceDescriptor

The netserviceDescriptor class SHALL be assigned to each entry that represents service-descriptor components and is defined as follows:

```
objectclass ( 1.3.6.1.4.1.23780.219.1.7
  NAME 'netserviceDescriptor'
  DESC 'DBIS netservice descriptor entry'
  SUP top STRUCTURAL
  MUST en
  MAY ( exactNetgroup $ exactNetservice $
        description $ manager $ disableObject ) )
```

### 3.2.3. Attributes

#### 3.2.3.1. en

The service-name of the netservice and each service-descriptor is stored in LDAP attributes of type en which is defined in [draft-bannister-dbis-mapping-00]. The en attribute MUST be associated with

a netserviceObject and netserviceDescriptor entry, and SHALL form the RDN of each.

If required, alias entries may be defined according to section 2.6 of [RFC4512] and as permitted by section 1.2 of [draft-bannister-dbis-mapping-00].

#### 3.2.3.2. exactNetgroup

Users or hosts are granted a netservice if they are members of one or more netgroups identified by exactNetgroup attributes that MAY be assigned to a netserviceDescriptor entry. The exactNetgroup attribute is defined in section 3.1.3.5 of this document.

The DUA SHALL validate that a netgroup referenced by this attribute exists and is enabled. If the netgroup is not defined, or if it has been disabled with the disableObject attribute, then it SHALL NOT be considered when determining netservice grants.

#### 3.2.3.3. exactNetservice

Grants from other netservices may be inherited by using one or more exactNetservice attributes that MAY be assigned to a netserviceDescriptor entry:

```
attributetype ( 1.3.6.1.4.1.23780.219.2.11 NAME 'exactNetservice'
  DESC 'Case exact netservice name associated with this entry'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )
```

Each netservice identified by the exactNetservice attribute SHALL be a fully-qualified netservice name as defined in section 3.2.1 of this document.

The DUA SHALL validate that a netservice referenced by this attribute exists and is enabled. If the netservice is not defined, or if it has been disabled with the disableObject attribute, then it SHALL NOT be considered when determining netservice grants.

If the netservice is defined, then the same users or hosts that are granted that netservice will be granted this one too.

#### 3.2.3.4. description

The description attribute MAY be associated with a netserviceObject or netserviceDescriptor entry to provide an arbitrary description of the entry.

#### 3.2.3.5. manager

The manager attribute MAY be associated with a netserviceObject or netserviceDescriptor entry to provide one or more DNs of the individuals, groups or systems that are responsible for maintaining the entry.

#### 3.2.3.6. disableObject

A netservice entry MAY be disabled by setting the disableObject attribute to TRUE. If an entry is disabled, then the DUA SHALL behave as if the netservice does not exist. The DUA MAY optionally provide a separate mechanism for listing disabled entries, but they MUST be clearly marked as disabled so that no confusion can arise.

The disableObject attribute may be set on either the netserviceObject or netserviceDescriptor entry. If set on the netserviceObject entry then the DUA SHALL treat all netserviceDescriptor entries underneath as disabled too.

### 3.2.4. Example Netservice Entries

The following are example netservice entries in LDIF format [RFC2849]:

```
dn: en=ssh,ou=netservice,o=infra
objectClass: top
objectClass: netserviceDescriptor
objectClass: netserviceObject
en: ssh
description: Secure Shell Service

dn: en=login,en=ssh,ou=netservice,o=infra
objectClass: top
objectClass: netserviceDescriptor
en: login
exactNetgroup: all-hosts
exactNetservice: ftp:login
exactNetservice: web:login/anonymous

dn: en=ftp,ou=netservice,o=infra
objectClass: top
objectClass: netserviceDescriptor
objectClass: netserviceObject
en: ftp
description: FTP Service

dn: en=login,en=ftp,ou=netservice,o=infra
```

```
objectClass: top
objectClass: netserviceDescriptor
en: login

dn: en=web,ou=netservice,o=infra
objectClass: top
objectClass: netserviceDescriptor
objectClass: netserviceObject
en: web
description: Web Service

dn: en=login,en=web,ou=netservice,o=infra
objectClass: top
objectClass: netserviceDescriptor
en: login

dn: en=anonymous,en=login,en=web,ou=netservice,o=infra
objectClass: top
objectClass: netserviceDescriptor
en: anonymous
```

These example entries define a netservice called ssh:login that will be granted to members of the all-hosts netgroup. If this netservice is granted, the ftp:login and web:login/anonymous netservices, also defined above, will be granted automatically.

## 4. Common Attributes

### 4.1. Scope

Additional attributes that are either used within this document or required by other documents using DBIS netgroups are defined or referenced below.

### 4.2. notNetgroup

One or more netgroup names that are to be excluded from a particular configuration entry are provided in notNetgroup attributes:

```
attributetype ( 1.3.6.1.4.1.23780.219.2.12 NAME 'notNetgroup'
  DESC 'Case exact netgroup name NOT to be associated
        with this entry'
  EQUALITY caseExactMatch
  SUBSTR caseExactSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )
```

The DUA SHALL validate that a netgroup referenced by this attribute exists and is enabled. If the netgroup is not defined, or if it has

been disabled with the disableObject attribute, then it SHALL NOT be included in the response to the client.

## 5. Attribute Syntax

The following syntaxes are used by the attributes defined in this document:

| Syntax OID | Value | Reference |
|---|---|---|
| 1.3.6.1.4.1.1466.115.121.1.15 | Directory String | [RFC4517] |
| 1.3.6.1.4.1.1466.115.121.1.26 | IA5 String | [RFC4517] |

## 6. Implementation Notes

### 6.1. NIS Netgroups

DBIS netgroups differ in their definition from NIS netgroups and from netgroups defined in RFC2307, which use triples of the format:

(host,user,domain)

where "host" is the canonical host name of the client system requesting a service, "user" is the user name requesting a service, and "domain" is the domain name of the service being requested. If the host, user or domain field is blank then the NIS netgroup applies to any client host, user or domain respectively.

The most common use of NIS netgroups is for defining groups of hosts and users while the domain component is typically left blank.

DBIS separates the triple into two separate attributes, netgroupHost and netgroupUser, and also redefines the domain component to be used to represent all hosts in a given domain. A set of mapping rules may be used for converting between the DBIS netgroup string representation described in sections 3.1.3.2 and 3.1.3.3 and a list of NIS netgroup triples. In the following grammar, the rule beginning t- is selected based on the information supplied in the netgroupHost or netgroupUser attribute. By removing the leading t- one can deduce the name of the matching rule from 3.1.3.2 or 3.1.3.3:

```
t-host            = LPAREN host COMMA COMMA RPAREN
t-host-domain     = LPAREN host-domain COMMA COMMA RPAREN
t-all-domain      = LPAREN COMMA COMMA domain RPAREN
t-user            = LPAREN COMMA user COMMA RPAREN
t-user-host       = LPAREN host COMMA user COMMA RPAREN
```

```
t-user-host-domain = LPAREN host-domain COMMA user COMMA RPAREN
t-user-all-domain  = LPAREN COMMA user COMMA domain RPAREN

triple-any   =  t-host / t-host-domain / t-all-domain
triple-any   =/ t-user / t-user-host / t-user-host-domain
triple-any   =/ t-user-all-domain

triples      = t-any *(SPACE t-any)
```

### 6.2. Forming netgroupHost or netgroupUser Entries

Netgroup membership SHALL be expressed in terms of canonical names only. Host names SHALL therefore be alias de-referenced before used in a netgroupHost attribute or netgroup filter.

As the user name component of the netgroupUser attribute is case sensitive while the other components are not, a DUA SHALL convert host name and domain name components to lower case characters prior to forming a netgroupHost or netgroupUser attribute or filter containing one. This is to ensure that the exact case match performed on these attributes will not fail on host name or domain name due to a case mismatch.

### 6.3. Common Search Filters

#### 6.3.1. Search Parameters

This section provides example LDAP search filters [RFC4515] for obtaining database entries with commonly used input criteria.

To simplify the examples, all databases are assumed to have been defined with only a single configuration map entry (dbisMapConfig). However, [draft-bannister-dbis-mapping-00] permits multiple such entries, so an implementation must support this, increasing the number of search operations as necessary to locate all of the database entries in scope.

This document does not consider how to incorporate passwd or hosts database entries that use the exactNetgroup attribute as an alternative means of specifying netgroup membership. For example search filters using the passwd or hosts databases, see [draft-bannister-dbis-passwd-00] and [draft-bannister-dbis-hosts-00] respectively.

The base DN used in the search operations described in this section comes from the dbisMapDN attribute assigned to the dbisMapConfig entry. Note that a dbisMapConfig entry may have more than one of these.

Where it appears in search filters below, the text "dbisMapFilter" refers to the value assigned to the attribute of the same name in the corresponding dbisMapConfig entry. Note that netgroup and netservice databases have different dbisMapConfig entries. Class and attribute names used in these search filters may be modified by the dbisMapClass and dbisMapAttr attribute assigned to the dbisMapConfig entry.

In all filters below, fully-qualified DNS domain names are to be obtained as described in section 3.1.5.

### 6.3.2. Find Configuration Map for Domain

To locate the configuration map for a given DBIS domain, search for entries underneath the dbisDomainObject entry [draft-bannister-dbis-mapping-00].

Netgroup maps can be found with the following search filter:

```
(&(objectClass=dbisNetgroupConfig)(!(disableObject=TRUE)))
```

Netservice maps can be found with:

```
(&(objectClass=dbisNetserviceConfig)(!(disableObject=TRUE)))
```

### 6.3.3. List All Entries

Netgroups and netservices are enumerated by applying the dbisMapFilter as follows:

```
(&(dbisMapFilter)(!(disableObject=TRUE)))
```

This filter returns all enabled entries.

### 6.3.4. Find Specific Netgroup or Netservice

If a netgroup or netservice is known by "name", its definition is located using the following search filter:

```
(&(dbisMapFilter)(!(disableObject=TRUE))(en=name))
```

If this is a netservice and the entry returned is a netserviceDescriptor and not a netserviceObject, then an additional test SHALL be performed for the disableObject attribute on the parent netserviceObject to determine whether this netservice is disabled, as defined in section 3.2.3.6.

When searching for specific netservices by name, this filter may

return more than one result, as namespace uniqueness is determined by the path and not by the name of a single LDAP entry.

### 6.3.5. Find Netgroups By Membership

To obtain a list of all netgroups that a user with the login name "user", who is logged into a system named "host" with the fully-qualified DNS domain name "domain" is a member of, the following search filter may be used:

```
(&(dbisMapFilter)(!(disableObject=TRUE))(|
    (netgroupUser=user)
    (netgroupUser=user@host.domain)
    (netgroupUser=user@\2a.domain)
))
```

To obtain a list of all netgroups that a system named "host" with the fully-qualified DNS domain name "domain" is a member of, the following search filter may be used:

```
(&(dbisMapFilter)(!(disableObject=TRUE))(|
    (netgroupHost=host)
    (netgroupHost=host.domain)
    (netgroupHost=\2a.domain)
))
```

If the user or host is not an explicit member of the netgroup, implicit membership needs to be determined by recursively examining each exactNetgroup attribute in the result set as the netgroup may inherit members from other netgroups. An example search filter for achieving this is in section 6.3.6. To prevent infinite loops, a DUA SHALL NOT test any netgroup more than once during a single membership operation.

### 6.3.6. Member of a Specific Netgroup

To determine if a user with the login name "user", who is logged into a system named "host" with the fully-qualified DNS domain name "domain" is a member of a specific netgroup called "name", the following search filter may be used:

```
(&(dbisMapFilter)(!(disableObject=TRUE))(en=name)(|
    (netgroupUser=user)
    (netgroupUser=user@host.domain)
    (netgroupUser=user@\2a.domain)
))
```

To determine if a system named "host" with the fully-qualified DNS

domain name "domain" is a member of a specific netgroup called "name", the following search filter may be used:

```
(&(dbisMapFilter)(!(disableObject=TRUE))(en=name)(|
    (netgroupHost=host)
    (netgroupHost=host.domain)
    (netgroupHost=\2a.domain)
))
```

If the user or host is not an explicit member of the netgroup, implicit membership needs to be determined by recursively examining each exactNetgroup attribute in the result set. This can be achieved by repeating the above search filters on successive netgroups. A DUA SHALL NOT test any netgroup more than once during a single membership operation.

### 6.3.7. Which Netgroups are Enabled?

Sometimes it is necessary to determine from a list of netgroups which ones are enabled. This can be performed using one search operation. In this example the netgroups being tested are called "netgr1", "netgr2" and "netgr3":

To determine if a system named "host" with the fully-qualified DNS domain name "domain" is a member of a specific netgroup called "name", the following search filter may be used:

```
(&(dbisMapFilter)(!(disableObject=TRUE))
    (|(en=netgr1)(en=netgr2)(en=netgr3)))
```

### 6.3.8. Find Netservices By Membership

To obtain a list of all netservices that are assigned to the netgroup called "netgroup", the following search filter may be used:

```
(&(dbisMapFilter)(!(disableObject=TRUE))
    (exactNetgroup=netgroup))
```

The netservice name may then be derived from the DNs of the returned entries. For example "en=anonymous,en=login,en=web,dbisMapDN" represents the netservice web:login/anonymous.

Each entry returned may list additional netservices to be assigned by use of the exactNetservice attribute.

If any netservice entry found is a netserviceDescriptor and not a netserviceObject, then an additional test SHALL be performed for the disableObject attribute on the parent netserviceObject to determine

whether this netservice is disabled, as defined in section 3.2.3.6.

### 6.3.9. Member of a Specific Netservice

To determine if a netgroup has been assigned a specific netservice, the netservice name must be split into a path name consisting of 'en=...,en=...' so that a specific entry with the object class netserviceDescriptor can be looked up underneath dbisMapDN. If this entry has an exactNetgroup attribute matching the desired member name, then a match has been found.

For example, the netservice web:login/anonymous would become the path 'en=anonymous,en=login,en=web' underneath dbisMapDN. The netserviceDescriptor matching this DN contains the definition of the given netservice. The exactNetgroup attribute associated with this entry contains the list of netgroups assigned the web:login/anonymous netservice.

Additionally, the following search filter can be used to locate netservices that include one called "netservice" in their definition and which are assigned to a netgroup called "netgroup":

```
(&(dbisMapFilter)(!(disableObject=TRUE))
    (exactNetservice=netservice)
    (exactNetgroup=netgroup))
```

If any entry is returned by a search with this filter then a match has been found.

## 7. Security Considerations

The security considerations discussed in [draft-bannister-dbis-mapping-00] apply equally to this document.

## 8. References

### 8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2849] Good, G., "The LDAP Data Interchange Format (LDIF) - Technical Specification", RFC 2849, June 2000.

[RFC4510] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map", RFC 4510, June 2006.

[RFC4512] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): Directory Information Models", RFC 4512, June 2006.

[RFC4515] Smith, M., Ed., and T. Howes, "Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters", RFC 4515, June 2006.

[RFC4517] Legg, S., Ed., "Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules", RFC 4517, June 2006.

[RFC4519] Sciberras, A., Ed., "Lightweight Directory Access Protocol (LDAP): Schema for User Applications", RFC 4519, June 2006.

[RFC5234] Crocker, D., Ed., and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[draft-bannister-dbis-mapping-00] Bannister, M. R., "Directory-Based Information Services: Mapping Objects", draft-bannister-dbis-mapping-00.txt, August 2013.

[draft-bannister-dbis-passwd-00] Bannister, M. R., "Directory-Based Information Services: Users and Groups", draft-bannister-dbis-passwd-00.txt, August 2013.

[draft-bannister-dbis-hosts-00] Bannister, M. R., "Directory-Based Information Services: Hosts, Networks and Devices", draft-bannister-dbis-hosts-00.txt, August 2013.

## 8.2. Informative References

[X.500] Weider, C. and J. Reynolds, "Executive Introduction to Directory Services Using the X.500 Protocol", FYI 13, RFC 1308, March 1992.

[NIS] Wikipedia, "Network Information Service", <http://en.wikipedia.org/wiki/Network_Information_Service>.

Author's Address

Mark R. Bannister
Prose Consulting Ltd.
73 Claygate Lane
Esher, Surrey, KT10 0BQ
United Kingdom

Tel: +44 7764 604316
EMail: dbis@proseconsulting.co.uk