draft-bannister-dbis-netgroup-04

dbis : netgroup

Ce document étend DBIS pour supporter les bases de données se service réseaux et groupes réseaux. Un schéma de base de netgroup devrait être compatible avec NIS mais stocké dans des entrées X.500 pour qu'ils puissent être résolus via lDA. Une base de netgroup représente des groupes d'hôtes, d'utilisateurs et de domaines.

Domaine

Le terme "domaine" utilisé dans ce document ne réfère pas aux domaines DBIS mais aux domaines DNS.

scope

Toutes les bases décrites dans ce document utilise les maps de configuration standard définies dans draft-bannister-dbis-mapping. Additionnellement, les entrées dbisMapConfig pour les bases netgroup et netservice devraient être assignés aux objectClass dbisNetGroupConfig et dbisNetserviceConfig, respectivement.

Il est recommandé que l'entrée dbisMapConfig pour un netgroup ou une base netservice ait l'attribut dbisMapFilter mis en accord avec la table suivante :

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

Exemple

Exemple de configuration d'une entrée de map de configuration pour une base netgroup :

```
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
```

Exemple de configuration d'une entrée de map de configuration pour une base netservice :

```
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
```

netgroup - définition

Une base netgroup contient les entrées qui représente les hôtes, les utilisateurs et les domaines et qui sont associés avec une nom netgroup sensible à la casse. les netgroups DBIS permettent aux groupes d'utilisateurs et aux hôtes d'être définis avec les variances de scope suivant :

- Tous les utilisateurs dans tous les hôtes d'un domaine donné
- Tous les utilisateurs dans des hôtes spécifiques
- Les utilisateurs nommés sans regarder l'hôte
- Les utilisateurs nommés dans tous les hôtes dans un domaine donné
- Les utilisateurs nommés dans des hôtes spécifiques.

objecClass

Une entrée dbisMapConfig pour une base netgroup devrait avoir l'objectClass dbisNetgroupConfig. Un netgroup devrait être définis par une entrée LDAP avec l'objectClass netgroupObject.

dbisNetgroupConfig

dbisNetgroupConfig est définis comme suit :

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

netgroupObject

netgroupObject est définis comme suit :

```
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 ) )
```

en

Le nom du netgroup est stocké dans l'attribut en qui est définis dans draft-bannister-dbis-mapping. L'attribut en doit être associé avec l'entrée netgroupObject et devrait former le RDN. Si requis, des entrées alias peuvent être définies.

netgroupHost

Un hôte qui est membre d'un netgroup est stocké dans l'attribut netgroupHost qui peut être assigné à une entrée netgroupObject :

```
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 )
```

Le représentation chaîne de l'attribut netgroupHost devrait matcher la grammaire suivante, qui utilise les productions ABNF :

```
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
```

Un DUA devrait dé-référencer les alias et convertir les composants de nom d'hôte et de domaine en caractères minuscule avant de former un attribut netgroupHost ou un filtre.

netgroupUser

Un utilisateur qui est un membre d'un netgroup est stocké dans l'attribut netgroupUser qui peut être assigné à une entrée netgroupObject :

```
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} )
```

La représentation chaîne de l'attribut netgroupUser devrait matcher la grammaire suivante, qui utilise les production ABNF :

```
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
```

Un DUA devrait convertir les composants de nom d'hôte et de domaine en caractères minuscule avant de former un attribut netgroupUser ou un filtre.

netgroupTriple

Pour compatibilité avec la rfc2307, DBIS permet aux membre des netgroup d'être exprimés sous la forme de triplets netgroup en fournissant un ou plusieurs attributs netgroupTriple qui peuvent être assignés à une entrée netgroupObject :

```
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 )
```

Un DUA devrait convertir les composants de nom d'hôte et de domaine en caractères minuscule avant de former un attribut netgroupTriple ou un filtre.

exactNetgroup

Les membres d'autres netgroups peuvent être hérités par ce netgroup en fournissant des noms de netgroup additionnels dans un ou plusieurs attributs exactNetgroup qui peut être assigné avec une entrée netgroupObject :

```
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} )
```

Les DUA devraient valider qu'un netgroup référencé par cet attribut existe et est actif. Si le netgroup n'est pas définis, ou s'il a été désactivé avec l'attribut disableObject, il ne devrait pas être inclus dans la réponse au client.

description

L'attribut description peut être associé avec une entrée netgroupObject pour fournir une description arbitraire de l'entrée

manager

L'attribut manager peut être associé avec une entrée netgroupObject pour fournir un ou plusieurs DN d'individus, de groupes ou systèmes qui sont responsable de la maintenance de cette entrée.

disableObject

Une entrée netgroup peut être désactivé en définissant l'attribut disableObject à TRUE. Si une entrée est désactivée, le DUA se comporte comme si le netgroup n'existe pas. Le DUA peut optionnellement fournir un mécanisme séparé pour les entrées désactivées, mais elles doivent être clairement marquées comme désactivées pour qu'aucune confusion ne se produise.

Exemple d'entrée netgroup

```
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
```

Déterminer les hôtes membres

Un DUA devrait effectuer une recherche DNS inversée de l'adresse IP primaire de l'hôte pour déterminer le nom fqdn à utiliser pour le netgroup correspondant. Un hôte doit rencontrer un des conditions suivantes pour être considéré un memre d'un netgroup :

a) Un nom d'hôte non qualifié convertis en minuscule correspond exactement à l'attribut netgroupHost. Dans ce scénario l'attribut netgroupHost est également non qualifié.

b) Le nom d'hôte pleinement qualifié convertis en minuscule correspond exactement à l'attribut netgroupHost.

c) L'attribut netgroupHost utilise le motif all-domain, et le nom de domaine pleinement qualifié convertis en minuscule correspond à cet attribut quand le préfix est supprimé.

Déterminer les utilisateurs membres

Un utilisateur doit rencontrer un des conditions suivantes pour être considéré un membre d'un netgroup :

a) L'attribut netgroupUser ne contient pas le ATSIGN et le nom d'utilisateur correspond exactement à l'attribut netgroupUser

b) Le nom d'utilisateur matche exactement le composant user de l'attribut netgroupUser, et le nom d'hôte non qualifié du DUA qui est obtenu comme décris précédemment et convertis en minuscule correspond exactement au composant hôte de l'attribut netgroupUser

c) Le nom d'utilisateur correspond exactement au composant utilisateur de l'attribut netgroupUser, et le nom d'hôte pleinement qualifié du DUA correspond exactement au composant domain d'hôte de l'attribut netgroupUser.

d) Le nom d'utilisateur correspond exactement au composant utilisateur de l'attribut netgroupUser qui utilise le motif all-domain et le nom de domaine pleinement qualifié du DUA correspond à cet attribut quand le préfix est supprimé.

netservice

Une base netservice mappe les netgroups aux services et privilèges. Les netservices peuvent être utilisé pour déterminer quelles applications devraient fonctionner sur un hôte, comment ils devraient être configurés, et quelles actions les utilisateurs peuvent ou non effectuer.

La représentation chaîne d'un nom netservice pleinement qualifié devrait correspondre à la grammaire suivante, qui utilise les production ABNF :

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

Le composant service-name identifie le service, et le service-descriptor est un chemin délimité par des slash qui identifie un sous-composant ou un sous-système dans le service. Une application est libre d'interpréter le nom d'un netservice de la manière qui lui convient, bien qu'il est suggéré qu'un netservice identifie soit un privilège soit une configuration qui peut être application au niveau de l'hôte ou utilisateur.

Le service-name est représenté dans LDAP par une entrée avec l'objectClass netserviceObject. Chaque composant délimité par un slash du service-descriptor sont des objets enfants dans LDAP avec l'objectClass netserviceDescriptor.

ObjectClass

Une entrée dbisMapConfig pour une base netservice devrait avoir l'objectClass dbisNetserviceConfig. Un netservice devrait être définis par une entrée LDAP avec l'objectClass netserviceObject.

dbisNetserviceConfig

La classe dbisNetserviceConfig est définie comme suit :

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

netserviceObject

La classe netserviceObject devrait être assigné à l'entrée qui représente un service-name et est définis comme suit :

```
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 ) )
```

netserviceDescriptor

La classe netserviceDescriptor devrait être assigné à chaque entrée qui représente les composants service-descriptor et est définis comme suit :

```
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 ) )
```

Attributes

en

Le nom du netgroup est stocké dans l'attribut LDAP en qui est définis dans draft-bannister-dbis-mapping. L'attribut en doit être associé avec une entrée netgroupObject et devrait former le RDN. Si requis, des entrées alias peuvent être définies.

netgroupHost

Un hôte qui est membre d'un netgroup est stocké dans l'attribut netgroupHost qui peut être assigné à une entrée netgroupObject :

```
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 )
```

Un hôte qui est membre d'un netgroup est stocké dans l'attribut netgroupHost qui peut être assigné à une entrée netgroupObject :

```
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 )
```

La représentation chaîne de l'attribut netgroupHost devrait matcher la grammaire suivante, qui utilise les productions ABNF :

```
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
```

Un DUA devrait déréférencer tout alias et convertir les composant nom d'hôte et nom de domaine en minuscule avant de traiter l'attribut netgroupHost ou un filtre le contenant.

netgroupUser

Un utilisateur qui est membre d'un netgroup est stocké dans l'attribut netgroupUser qui peut être assigné à une entrée netgroupObject :

```
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} )
```

La représentation chaîne de l'attribut netgroupUser devrait matcher la grammaire suivante, qui utilise les production ABNF :

```
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
```

La représentation chaîne de l'attribut netgroupUser devrait matcher la grammaire suivante, qui utilise les production ABNF :

```
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
```

Un DUA devrait convertir les composant nom d'hôte et nom de domaine en minuscule avant de traiter un attribut netgroupUser ou un filtre le contenant.

netgroupTriple

Pour compatibilité avec la rfc2307, DBIS permet également l'appartenance exprimé sous la forme de triplet netgroup en fournissant un ou plusieurs attributs netgroupTriple qui peuvent être assignés à une entrée netgroupObject :

```
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 )
```

Un DUA devrait convertir les composant nom d'hôte et nom de domaine en minuscule avant de traiter un attribut netgroupTriple ou un filtre le contenant.

exactNetgroup

Les membres d'autres netgroup peuvent être hérités par ce netgroup en fournissant des noms de netgroup additionnels dans un ou plusieurs attributs exactNetgroup qui peuvent être assignés à une entrée netgroupObject :

Le DUA devrait valider qu'un netgroup référencé par cet attribut existe et est activé. Si le netgroup n'est pas définis, ou s'il a été désactivé avec l'attribut disableObject, il ne doit pas être inclus dans la réponse au client.

manager

L'attribut manager peut être associé avec une entrée netgroupObject pour fournir un ou plusieurs DN d'individus, groupes ou systèmes qui sont responsable de la maintenance de l'entrée.

disableObject

Une entrée netgroup peut être désactivée en définissant l'attribut disableObject à TRUE.

Exemple d'entrée Netgroup

```
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
```


```
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
```


Déterminer les hôtes membre

Un utilisateur doit rencontrer un des conditions suivantes pour être considéré un membre d'un netgroup :

a) L'attribut netgroupUser ne contient pas de ATSIGN et le nom d'utilisateur correspond exactement à l'attribut netgoupUser

b) Le nom d'utilisateur correspond au composant user de l'attribut netgroupUser, et le nom d'hôte non-qualifié du DUA convertis en minuscule correspond au composant hôte de l'attribut netgroupUser.

c) Le nom d'utilisateur correspond au composant user de netgroupUser, et le nom d'hôte pleinement qualifié du DUA convertis en minuscule correspond au composant de domaine hôte de l'attribut netgroupUser.

d) Le nom d'utilisateur correspond au composant user de l'attribut netgroupUser, l'attribut netgroupUser utilise le motif all-domain et le nom de domaine pleinement qualifié du DUA convertis en minuscule correspond à cet attribut quand le préfix ASTERISK DOT est supprimé.

netservice

Une base netservice mappe les netgroups à des services et privilèges. Les netservices peuvent être utilisé pour déterminer quelles applications devraient fonctionner sur un hôte, comment ils devraient être configurés, et quelles actions les utilisateurs peuvent faire ou non.

La représentation chaîne d'un nom netservice pleinement qualifié devrait suivre la grammaire suivante, qui utilise les production ABNF :

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

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

Le composant service-name identifie le service, alors que le service-descriptor est un chemin délimité par les anti-slash qui identifie un sous-composant ou un sous-système dans le service. Une application est lible d'interpréter le nom d'un netservice de la manière qui lui convienne, bien qu'il soit suggéré qu'un netservice identifie soit un privilège ou une configuration qui peut être appliqué au niveau de l'hôte ou utilisateur.

service-name est représente dans LDAP par une entrée avec l'objectClass netserviceObject. Chaque composant délimité de service-descriptor sont des objets enfants dans LDAP avec l'objetClass netserviceDescriptor.

Classes d'objet

Une entrée dbisMapConfig pour une base netservice devrait être assignée avec l'objectClass dbisNetserviceConfig

dbisNetserviceConfig

La classe dbisNetserviceConfig est définie comme suit :

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

La classe dbisNetserviceConfig est définie comme suit :

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

netserviceObject

La classe netserviceObject devrait être assignée à l'entrée qui représente le service-name et est définie comme suit :

```
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 ) )
```

netserviceDescriptor

La classe netserviceDescriptor devrait être assignée à chaque entrée qui représente des composants service-descriptor et est définie comme suit :

```
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 ) )
```

Attributs

en

Le service-name de netservice et chaque service-descriptor sont stockés dans des attributs LDAP de type en qui est définis dans draft-bannister-dbis-mapping. L'attribut en doit être associé avec une entrée netserviceObject et netserviceDescriptor, et devrait former le RDN. Si requis, des entrées alias peuvent être définies.

exactNetgroup

Les utilisateurs et les hôtes bénéficient d'un netservice s'ils sont membre d'un ou plusieurs netgroups identifiés par les attributs exactNetgroup qui peuvent être assignés à une entrée netserviceDescriptor.

exactNetservice

d'autres netservices peuvent être hérités en utilisant un ou plusieurs attributs exactNetservice qui peuvent être assignés à une entrée netserviceDescriptor :

```
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} )
```

Chaque netservice identifié par l'attribut exactNetservice devrait être un nom netservice pleinement qualifié. Le DUA devrait valider qu'un netservice référencé par cet attribut existe et est activé. Si le netservice n'est pas définis, ou s'il n'a pas été désactivé avec l'attribut disableObject, il ne devrait pas être considéré.

description

L'attribut description peut être associé avec une entrée netserviceObject ou netserviceDescriptor pour fournir une description arbitraire de l'entrée.

manager

L'attribut manager peut etre associé avec un netserviceObject ou netserviceDescriptor pour fournir un ou plusieurs DN des individus, groupes ou systèmes qui sont responsables de la maintenance de l'object.

disableObject

Une entrée netservice peut être désactivée en définissant l'attribut disableObject à TRUE. Si une entrée est désactivée, le DUA devrait se comporter comme si l'entrée n'existait pas. Le DUA peut optionnellement fournir un mécanisme séparé pour lister les entrées désactivées, mais doit les marquer clairement comme désactivés. L'attribut disableObject peut être définis sur soit dans l'entrée netserviceObject soit netserviceDescriptor. Si définis dans l'entrée netserviceObject, le DUA devrait traiter toutes les entrées netserviceDescriptor présents comme désactivés également.

Exemple d'entrées netservice

L'exemple suivante montre des entrées netservice au format ldif :

```
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
```

Ces entrées exemple définissent un netservice appelé ssh :login qui est permis aux membres de du netgroup all-hosts. Si ce netservice est activé, les netservices ftp :login et web :login, également définis, seront activés automatiquement.

Attributs communs

Des attributs additionnels qui sont soit utilisés dans ce document ou requis par d'autres documents en utilisant les netgroups sont définis ou référencés ci-dessous.

notNetgroup

Un ou plusieurs netgroups qui sont exclus d'une entrée de configuration particulière sont fournis dans les attributs notNetgroup :

```
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} )
```

Syntaxe d'attribut

Les syntaxes suivantes sont utilisées par les attributs définis dans ce 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]
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Notes d'implémentation

netgroups NIS

les netgroups DBIS diffèrent des netgroups NIS et des netgroups définis dans la rfc2307, qui utilise des triplets au format : **(host,user,domain)**, où "host" est le nom d'hôte canonique du système client demandant un service, "user" est le nom d'utilisateur qui demande un service, et "domain" est le nom de domaine du service demandé. Il les champs host, user et domain sont vides, alors le netgroup NIS s'applique à tous les hôtes, utilisateurs, ou domaines respectivement.

L'utilisation la plus commune des netgroups NIS est pour définir des groupes d'hôte et d'utilisateurs alors que le domaine est généralement laissé vide.

DBIS sépare le triplet en 2 attributs séparés, netgroupHost et netgroupUser, et redéfinis également le composant domaine à utiliser pour représenter tous les hôtes dans un domaine donné. Un jeu de règles de mappage peut être utilisé pour convertir la représentation chaîne de netgroup DBIS et une liste de triplets netgroup NIS. Dans la grammaire suivante, la règle commençant par t- est sélectionnée en fonction de l'information fournie dans l'attribut netgroupHost ou netgoupUser. En supprimant le t- on peut déduire le nom de la règle de correspondance :

```
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)
```

Former les entrées netgroupHost ou netgroupUser

L'appartenance à un netgroup devrait être exprimé en termes de noms canoniques uniquement. Vu que le composant username de l'attribut netgroupUser est sensible à la casse alors que les autres composants ne le sont pas, un DUA devrait convertir les composants nom d'hôte et nom de domaine en minuscule avant de former un attribut netgroupHost ou netgroupUser ou un filtre le contenant. C'est pour s'assurer que la correspodance effectuée sur ces attributs n'échoueront pas sur le nom d'hôte ou le nom de domaine sur à une problème de casse.

Paramètres de recherche

Cette section fournis des exemples de filtres de recherche pour obtenir des entrées de base avec les critères communément utilisés.

Pour simplifier les exemples, on assume que toutes les base ont une seul entrée de map de configuration (dbisMapConfig). Cependant, le draft-bannister-dbis-mapping permet d'utiliser plusieurs entrées, donc pour qu'une implémentation le supporte, le nombre d'opérations de recherche nécessaire pour localiser toutes les entrées de base doit être augmenté.

Ce document ne considère pas comment incorporer les entrées de base hosts ou passwd qui utilisent l'attribut exactNetgroup comme moyen alternatif pour spécifier les membre de netgroup.

Le DN de base utilisé dans les opérations de recherche décris dans cette section vient de l'attribut dbisMapDN assigné à l'entrée dbisMapConfig. Noter qu'une entrée dbisMapConfig peut en avoir plusieurs.

Quand il apparaît dans les filtres de recherche ci-dessous, le texte "dbisMapFilter" réfère à la valeur assignée à l'attribut de même nom dans l'entrée dbisMapConfig correspondante. Noter que les base netgroup et netservice utilisé dans ces filtres de recherche peuvent être

modifiés par l'attribut dbisMapClass et dbisMapAttr assigné à l'entrée dbisMapConfig. Dans tous les filtres ci-dessous, les noms de domaine DNS pleinement qualifiés sont obtenus comme décris dans la section "Déterminer les hôtes membre".

Trouver la Map de configuration pour le domaine

Pour localiser la map de configuration pour un domaine DBIS donné, recherche les entrées sous l'entrée dbisDomainObject

Les maps netgroup peuvent être trouvés avec le filtre de recherche suivant
(&(objectClass=dbisNetgroupConfig)(!(disableObject=TRUE)))
Les maps netservice avec :
(&(objectClass=dbisNetserviceConfig)(!(disableObject=TRUE)))

Lister toutes les entrées

Les netgroup et netservices sont énumérés en appliquant le dbisMapFilter comme suit :
(&(dbisMapFilter)(!(disableObject=TRUE)))

Trouver un netgroup ou netservice particulier

Is un netgroup ou netservice est connu par "nom", sa définition est localisée en utilisant le filtre de recherche suivant :
(&(dbisMapFilter)(!(disableObject=TRUE))(en=name))
Si c'est un netservice et que l'entrée retournée est un netserviceDescriptor et pas un netserviceObject, alors un test additionnel devrait être effectué sur l'attribut disableObject sur le netserviceObject parent pour déterminer si le netservice est désactivé.

En recherchant des netservice spécifiques par nom, ce filtre peut retourner plus d'un résultat, vu que l'unicité de l'espace de nom est déterminé par le chemin et non par le nom dans une entrée LDAP.

Trouver des netgroup par membership

Pour obtenir une liste de tous les netgroups qu'un utilisateur avec le nom de login "user", qui est connecté sur un hôte nommé "host" avec le domaine DNS "domain" est un membre, le filtre de recherche suivant peut être utilisé :

(&(dbisMapFilter)(!(disableObject=TRUE))(|(netgroupUser=user)(netgroupUser=user@host.domain)(netgroupUser=user@\2a.domain))
Pour obtenir une liste de tous les netgroups qu'un système nommé "host" avec le nom dns "domaine" est un membre, le filtre suivant peut être utilisé :
(&(dbisMapFilter)(!(disableObject=TRUE))(|(netgroupHost=host)(netgroupHost=host.domain)(netgroupHost=\2a.domain)))
Si l'utilisateur ou l'hôte n'est pas un membre explicite du netgroup, le membreship implicite doit être déterminé en examinant récursivement chaque attribut exactNetgroup dans le jeu de résultat. Pour empêcher les boucles infinies, un DUA ne devrait pas tester un netgroup plus d'une fois durant une opération de membership.

Membre d'un netgroup spécifique

Pour déterminer si un utilisateur avec un nom "user", qui est loggé sur un hôte nommé "host", avec un nom de domaine "domain" est un membre d'un netgroup spécifique appelé "name", le filtre de recherche suivant peut être utilisé :

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

Pour déterminer si un système nommé "host" avec le nom de domaine "domain" est un membre d'un netgroup spécifique appelé "name", le filtre de recherche suivant peut être utilisé :

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

Si l'utilisateur ou l'hôte n'est pas un membre explicite du netgroup, un membership implicite doit être déterminé en examinant récursivement chaque attribut exactNetgroup dans le jeu de résultat.

Quels Netgroups sont activés

parfois il est nécessaire de déterminer depuis une liste de netgroups quels sont ceux qui sont activés. Cela peut être effectués en utilisant une opération de recherche. Dans cet exemple les netgroups testés sont appelés "netgr1", "netgr2" et "netgr3".

Pour déterminer si une système nommé "host" avec le nom de domaine "domaine" est un membre d'un netgroup spécifique appelé "name", le filtre suivant peut être utilisé :

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

Trouver des netservices par membership

Pour obtenir une liste de tous les netservices qui sont assignés au netgroup appelé "netgroup", le filtre suivant peut être utilisé :

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

Le nom netservice peut être dérivé du DN des entrées retournées. Par exemple, "en=anonymous,en=login,en=web,dbisMapDN" représente le netservice web :login/anonymous.

Chaque entrée retournée peut lister des netservices additionnels assignés par l'attribut exactNetservice

Si une entrée netservice trouvé est un netserviceDescriptor et non un netserviceObject, un test supplémentaire devrait être effectué pour l'attribut disableObject sur le netserviceObject parent pour déterminer si le netservice est désactivé.

Membre d'un netservice spécifique

Pour déterminer si un netgroup a été assigné à un netservice spécifique, le nom netservice doit être splitté en un nom de chemin consistant de 'en=...,en=...' pour qu'une entrée spécifique avec l'objectClass netserviceDescriptor puisse être recherchée sous dbisMapDN. Si cette entrée a un attribut exactNetgroup correspondant au nom de membre désiré, une correspondance est trouvée.

Par exemple, le netservice web :login/anonymous devient le chemin 'en=anonymous,en=login,en=web' sous dbisMapDN. Le netserviceDescriptor correspondant à ce DN contient la définition du netservice donné. L'attribut exactNetgroup associé avec cette entrée contient la liste des netgroups assignés au netservice web :login/anonymous.

De plus, le filtre de recherche suivant peut être utilisé pour localiser les netservices qui incluent en netservice appelé "netservice" dans leur définitions et qui sont assignés au netgroup nommé "netgroup" :

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

Si une entrée est retournée par une recherche avec ce filtre alors une correspondance a été trouvée.