draft-chu-ldap-logschema-00

Schéma de log du protocol LDAP

Pour faciliter l'administration distante et l'audit des opérations serveurs LDAP, il est désirable de fournir les logs opérationnels du serveur eux-même comme annuaire LDAP. Ces logs peuvent être également utilisés comme log de changements persistants pour supporter divers mécanismes de réplication. Ce document définis un schéma qui peut être utilisé pour représenter toutes les requêtes qui sont traitées par un serveur LDAP.

Control Syntax

Une valeur de Control syntax représente un contrôle LDAP tel qu'utilisé par un client ou un serveur. Il consiste de l'OID numérique du contrôle, le flag de criticité, et d'un OctetString optionnel contenant la valeur du contrôle.

La notation ASN.1 est :

```
Control ::= SEQUENCE {
 controlType LDAPOID,
 criticality BOOLEAN DEFAULT FALSE,
 controlValue OCTET STRING OPTIONAL }
```

La description de syntaxe ldap est :

```
( LOG_SCHEMA_SYN.1 DESC 'Control' )
```

Types d'attributs Généraux

These attributes are common to all of the LDAP request records

```
( LOG_SCHEMA_AT.1 NAME 'reqDN'
DESC 'Target DN of request'
EQUALITY distinguishedNameMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
SINGLE-VALUE )

( LOG_SCHEMA_AT .2 NAME 'reqStart'
DESC 'Start time of request'
EQUALITY generalizedTimeMatch
ORDERING generalizedTimeOrderingMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
SINGLE-VALUE )

( LOG_SCHEMA_AT .3 NAME 'reqEnd'
DESC 'End time of request'
EQUALITY generalizedTimeMatch
ORDERING generalizedTimeOrderingMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
SINGLE-VALUE )
```

```
( LOG_SCHEMA_AT .4 NAME 'reqType'
DESC 'Type of request'
EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )

( LOG_SCHEMA_AT .5 NAME 'reqSession'
DESC 'Session ID of request'
EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )

( LOG_SCHEMA_AT .6 NAME 'reqAuthzID'
DESC 'Authorization ID of requestor'
EQUALITY distinguishedNameMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
SINGLE-VALUE )

( LOG_SCHEMA_AT .7 NAME 'reqResult'
DESC 'Result code of request'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE )

( LOG_SCHEMA_AT .8 NAME 'reqMessage'
DESC 'Error text of request'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )

( LOG_SCHEMA_AT .9 NAME 'reqReferral'
DESC 'Referrals returned for request'
SUP labeledURI )

( LOG_SCHEMA_AT .10 NAME 'reqControls'
DESC 'Request controls'
EQUALITY objectIdentifierFirstComponentMatch
SYNTAX LOG_SCHEMA_SYN.1 X-ORDERED 'VALUES' )

( LOG_SCHEMA_AT .11 NAME 'reqRespControls'
DESC 'Response controls of request'
EQUALITY objectIdentifierFirstComponentMatch
SYNTAX LOG_SCHEMA_SYN.1 X-ORDERED 'VALUES' )
```

Types d'attributs spécifiques aux requêtes

Ces attributs sont spécifiques à un simple type de requêtes ldap :

```
( LOG_SCHEMA_AT .12 NAME 'reqId'
DESC 'ID of Request to Abandon'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE )
```

```
( LOG_SCHEMA_AT .13 NAME 'reqVersion'
DESC 'Protocol version of Bind request'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE )

( LOG_SCHEMA_AT .14 NAME 'reqMethod'
DESC 'Bind method of request'
EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )

( LOG_SCHEMA_AT .15 NAME 'reqAssertion'
DESC 'Compare Assertion of request'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )

( LOG_SCHEMA_AT .16 NAME 'reqMod'
DESC 'Modifications of request'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
EQUALITY octetStringMatch
SUBSTR octetStringSubstringsMatch )

( LOG_SCHEMA_AT .17 NAME 'reqOld'
DESC 'Old values of entry before request completed'
EQUALITY octetStringMatch
SUBSTR octetStringSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

( LOG_SCHEMA_AT .18 NAME 'reqNewRDN'
DESC 'New RDN of request'
EQUALITY distinguishedNameMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
SINGLE-VALUE )

( LOG_SCHEMA_AT .19 NAME 'reqDeleteOldRDN'
DESC 'Delete old RDN'
EQUALITY booleanMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE )

( LOG_SCHEMA_AT .20 NAME 'reqNewSuperior'
DESC 'New superior DN of request'
EQUALITY distinguishedNameMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
SINGLE-VALUE )

( LOG_SCHEMA_AT .21 NAME 'reqScope'
DESC 'Scope of request'
EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )

( LOG_SCHEMA_AT .22 NAME 'reqDerefAliases'
DESC 'Disposition of Aliases in request'
EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
```

```
SINGLE-VALUE )

( LOG_SCHEMA_AT .23 NAME 'reqAttrsOnly'
DESC 'Attributes and values of request'
EQUALITY booleanMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE )

( LOG_SCHEMA_AT .24 NAME 'reqFilter'
DESC 'Filter of request'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE )

( LOG_SCHEMA_AT .25 NAME 'reqAttr'
DESC 'Attributes of request'
EQUALITY caseIgnoreMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

( LOG_SCHEMA_AT .26 NAME 'reqSizeLimit'
DESC 'Size limit of request'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE )

( LOG_SCHEMA_AT .27 NAME 'reqTimeLimit'
DESC 'Time limit of request'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE )

( LOG_SCHEMA_AT .28 NAME 'reqEntries'
DESC 'Number of entries returned'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE )

( LOG_SCHEMA_AT .29 NAME 'reqData'
DESC 'Data of extended request'
EQUALITY octetStringMatch
SUBSTR octetStringSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40
SINGLE-VALUE )
```

Classes d'objets d'audit de base

Cette classe contient les attributs communs à toutes les requêtes ldap. Les autres classe héritent toutes de cette classe :

```
( LOG_SCHEMA_OC .1 NAME 'auditObject' DESC 'OpenLDAP request
auditing' SUP top STRUCTURAL MUST ( reqStart $ reqType $ reqSession )
MAY ( reqDN $ reqAuthzID $ reqControls $ reqRespControls $ reqEnd $
reqResult $ reqMessage $ reqReferral ) )
```

Ces classes d'objet sont utilisées pour agréger les opérations de lecture et d'écriture sous des classes parent communs :

```
( LOG_SCHEMA_OC .2 NAME 'auditReadObject' DESC 'OpenLDAP read request
record' SUP auditObject STRUCTURAL MUST reqDN )

( LOG_SCHEMA_OC .3 NAME 'auditWriteObject' DESC 'OpenLDAP write
request record' SUP auditObject STRUCTURAL MUST reqDN )
```

Classes d'objets spécifiques aux requêtes

Chaque requête ldap a sa propre classe d'objet contenant tous les attributs nécessaire pour représenter une instance de cette requête :

```
( LOG_SCHEMA_OC .4 NAME 'auditAbandon' DESC 'Abandon operation' SUP
auditObject STRUCTURAL MUST reqId )

( LOG_SCHEMA_OC .5 NAME 'auditAdd' DESC 'Add operation' SUP
auditWriteObject STRUCTURAL MUST reqMod )

( LOG_SCHEMA_OC .6 NAME 'auditBind' DESC 'Bind operation' SUP
auditObject STRUCTURAL MUST ( reqDN $ reqMethod $ reqVersion ) )

( LOG_SCHEMA_OC .7 NAME 'auditCompare' DESC 'Compare operation' SUP
auditReadObject STRUCTURAL MUST reqAssertion )

( LOG_SCHEMA_OC .8 NAME 'auditDelete' DESC 'Delete operation' SUP
auditWriteObject STRUCTURAL MAY reqOld )

( LOG_SCHEMA_OC .9 NAME 'auditModify' DESC 'Modify operation' SUP
auditWriteObject STRUCTURAL MUST reqMod MAY reqOld )

( LOG_SCHEMA_OC .10 NAME 'auditModRDN' DESC 'ModRDN operation' SUP
auditWriteObject STRUCTURAL MUST ( reqNewRDN $ reqDeleteOldRDN ) MAY
( reqNewSuperior $ reqOld ) )
( LOG_SCHEMA_OC .11 NAME 'auditSearch' DESC 'Search operation' SUP
auditReadObject STRUCTURAL MUST ( reqScope $ reqDerefAliases $
reqAttrsonly ) MAY ( reqFilter $ reqAttr $ reqEntries $ reqSizeLimit
$ reqTimeLimit ) )

( LOG_SCHEMA_OC .12 NAME 'auditExtended' DESC 'Extended operation'
SUP auditObject STRUCTURAL MAY reqData )
```

Classe conteneur générique

Cette classe d'objet peut être utilisée pour l'entrée parent des enregistrements :

```
( LOG_SCHEMA_OC .0 NAME 'auditContainer' DESC 'AuditLog container'
SUP top STRUCTURAL MAY ( cn $ reqStart $ reqEnd ) )
```

Discussion du schéma - AuditObject

1. reqDN : le DN de l'entrée à laquelle le requête s'applique. Dans le cas d'une requête ModRDN, le reqDN donne le DN de l'entrée

avant qu'elle ait été modifiée. Dans le cas d'un requête Search, le reqDN est le DN de base de la recherche. Syntaxe : DN.

2. reqStart : la date du début de la requête sur le serveur. **reqEND** : la date de la fin de la requête sur le serveur. Les timestamps doivent avoir une résolution suffisante pour s'assurer que les valeur de reqStart et reqEnd sont uniques. Les serveurs devraient utiliser reqStart ou reqEnd comme RDN de l'enregistrement. Ce choix permettra de les les enregistrements dans l'ordre ascendant, bien que les 2 alternatives peuvent produire des résultats différents. Dans le cas où l'horloge du serveur ne fournir pas de temps suffisamment précis, une simple compteur peut être utilisé dans la partie fractionnelle des secondes. Syntaxe : generalizedTime.

3. reqType : le type de la requête : **abandon**, **add**, **bind**, **compare**, **delete**, **modify**, **modrdn**, **search** ou **extended{OID}**. Pour les requêtes étendues, d'OID de la requête est inclue dans la chaîne. Syntaxe : DirectoryString

4. reqSession : une valeur qui est une constante pour toutes les opérations se produisant dans une séquence bind/unbind. Syntaxe : DirectoryString

5. reqAuthzID : L'identité d'authorisation utilisé pour effectuer la requête. Généralement la même que reqDN de la requête bind ayant le même reqSession, mais peut être altéré par divers contrôles et autres traitements. Syntaxe : DN

6. reqResult : Le code de résultat LDAP de la requête complétée. Cette valeur peut être omise pour les requêtes qui n'ont pas de résultat définis (ex : abandon et unbind) et pour les requêtes qui ont été abandonnées. Syntaxe : Integer

7. reqMessage : Le message d'erreur textuel accompagnant le résultat, s'il y'en a un. Syntaxe : DirectoryString

8. reqReferral : Les référants qui ont accompagné le résultat, au format URI LDAP. Syntaxe : DirectoryString

9. reqControls : le jeu de contrôles de requête accompagnant une requête. **seqRespControls** : le jeu de contrôles de réponse accompagnant le résultat de la requête. Chaque valeur représente un seul contrôle. l'ordre est préservé en utilisant l'extension de schéma X-ORDERED 'VALUES'. Syntaxe : Control

AuditContainer

reqStart : le timestamp du premier enregistrement dans le log. **reqEnd** : le timestamp du dernier enregistrement dans le log. Syntaxe : generalizedTime

Abandon

reqId : l'ID d'une requête à abandonner. Syntaxe : Integer

Bind

reqVersion : La version du protocol du la requête. Syntaxe : Integer

reqMethod : La méthode bind. Soit Simple, soit SASL/mécanisme. Syntaxe : DirectoryString

Compare

reqAssertion : L'AVA de la requête. Syntaxe : DirectoryString

Rename

reqNewRDN : Le nouveau rdn de la requête. Syntaxe : DN

reqDeletedOldRDN : le deleteOldRDN de la requête. Syntaxe : Boolean

reqNewSuperior : le nouveau DN supérieur de la requête. Syntaxe : DN.

Add et Modify

reqMod : Les modifications de la requête. L'encodage est définis par la grammaire suivante (ABNF) :

```
mod = attr ":" modop
attr = AttributeDescription from [RFC2251]
modop = add / delete / replace / increment
add = "+" sp value
delete = "-" [ sp value ]
replace = "=" [ sp value ]
increment = "#" sp value
sp = " "
value = AttributeValue from [RFC2251]
```

Note que les requêtes Add utilisent uniquement le format add modop. Syntaxe : OctetString

reqOld : Les valeurs précédente d'un attribut modifié. L'encodage est sous la forme **attr " :" sp value**, en utilisant la même forme que reqMod. Syntaxe : OctetString

Delete

reqOld : le valeurs précédente d'une entrée supprimée. L'encodage est le même que plus haut. Syntaxe : OctetString

Search

reqScope : le scope de la recherche. base, one, sub ou subord. Syntaxe : DirectoryString

reqDerefAliases : le paramètre derefAliases de la recherche. never, searching, finding, ou always. Syntaxe : DirectoryString

reqAttrsOnly : le paramètre typesOnly de la requête. Syntaxe : Boolean

reqFilter : Le filtre de la recherche. Syntaxe : DirectoryString

reqSizeLimit : La limite de taille de la requête

reqTimeLimit : Le limite de temps de la requête. Syntaxe : Integer

reqAttr : Les attributs spécifiquement demandés. Syntaxe : DirectoryString

reqEntries : Le nombre total d'entrées retournées pour cet requête. Syntaxe : Integer

Extended

reqData : Les données accompagnant le requête. Syntaxe : OctetString

Exemples

Dans les exemples suivants les enregistrements résident sous "cn=log" et sont nommés par leur attribut "reqStart"

dn : reqStart=20051017081049.000000Z,cn=log

```
objectClass: auditBind
reqStart: 20051017081049.000000Z
reqEnd: 20051017081049.000001Z
reqType: bind
reqSession: 0
reqAuthzID:
reqDN: cn=manager,dc=example,dc=com
reqResult: 0
reqVersion: 3
reqMethod: SIMPLE

dn: reqStart=20051017081049.000002Z,cn=log
objectClass: auditSearch
reqStart: 20051017081049.000002Z
reqEnd: 20051017081049.000003Z
reqType: search
reqSession: 0
reqAuthzID: cn=Manager,dc=example,dc=com
reqDN: dc=example,dc=com
reqResult: 0
reqScope: one
reqDerefAliases: never
reqAttrsOnly: FALSE
reqFilter: (objectClass=*)
reqSizeLimit: -1
reqTimeLimit: -1
reqEntries: 3

dn: reqStart=20051017081049.000004Z,cn=log
objectClass: auditObject
reqStart: 20051017081049.000004Z
reqEnd: 20051017081049.000005Z
reqType: unbind
reqSession: 0
reqAuthzID: cn=Manager,dc=example,dc=com
```

requête Add

Enregistrement issue de l'ajout d'une entrée dans l'annuaire :

```
dn: reqStart=20051017083706.000001Z,cn=log
objectClass: auditAdd
structuralObjectClass: auditAdd
reqStart: 20051017083706.000001Z
reqEnd: 20051017083706.000002Z
reqType: add
reqSession: 4
reqAuthzID: cn=Manager,dc=example,dc=com
reqDN: ou=People,dc=example,dc=com
reqResult: 0
reqMod: objectClass:+ organizationalUnit
reqMod: ou:+ People
reqMod: description:+ A bunch of people will be here
reqMod: structuralObjectClass:+ organizationalUnit
reqMod: entryUUID:+ f16734aa-d334-1029-9290-cd8deceec6b0
reqMod: creatorsName:+ cn=Manager,dc=example,dc=com
reqMod: createTimestamp:+ 20051017083706Z
reqMod: entryCSN:+ 20051017083706Z#000000#00#000000
reqMod: modifiersName:+ cn=Manager,dc=example,dc=com
reqMod: modifyTimestamp:+ 20051017083706Z
```

Notez que les attributs opérationnels écrits avec la requête sont inclus dans le log. Toutes les statistiques associées avec une entrée seront exposées, permettant à un client de réplication d'avoir une copie complète de l'entrée.

Requête Modify

Enregistrement issue d'une entrée modifiée dans l'annuaire

```
dn: reqStart=20051017083734.000010Z,cn=log
objectClass: auditModify
reqStart: 20051017083734.000010Z
reqEnd: 20051017083734.000011Z
reqType: modify
reqSession: 1
reqAuthzID: cn=Manager,dc=example,dc=com
reqDN: ou=People,dc=example,dc=com
reqResult: 0
reqMod: description:-
reqMod: entryCSN:= 20051017083734Z#000003#00#000000
reqMod: modifiersName:= cn=Manager,dc=example,dc=com
reqMod: modifyTimestamp:= 20051017083734Z
reqOld: description: A bunch of people will be here
```

Dans cet exemple, l'attribut description a été supprimé de l'entrée. Sa valeur original est enregistrée dans l'attribut reqOld.

Requête Rename

Enregistrement issue du renommage d'une entrée dans l'annuaire

```
dn: reqStart=20051017083734.000018Z,cn=log
```

```
objectClass: auditModRDN
reqStart: 20051017083734.000018Z
reqEnd: 20051017083734.000019Z
reqType: modrdn
reqSession: 1
reqAuthzID: cn=Manager,dc=example,dc=com
reqDN: ou=People,dc=example,dc=com
reqResult: 0
reqNewRDN: ou=Populi
reqDeleteOldRDN: TRUE
```

Requête Delete

Enregistrement issue de la suppression d'une entrée dans l'annuaire

```
dn: reqStart=20051017083734.000020Z,cn=log
objectClass: auditDelete
reqStart: 20051017083734.000020Z
reqEnd: 20051017083734.000021Z
reqType: delete
reqSession: 1
reqAuthzID: cn=Manager,dc=example,dc=com
reqDN: ou=Populi,dc=example,dc=com
reqResult: 0
reqOld: ou: Populi
reqOld: objectClass: organizationalUnit
reqOld: structuralObjectClass: organizationalUnit
reqOld: entryUUID: f16734aa-d334-1029-9290-cd8deceec6b0
reqOld: creatorsName: cn=Manager,dc=example,dc=com
reqOld: createTimestamp: 20051017083706Z
reqOld: entryCSN: 20051017083734Z#000007#00#000000
reqOld: modifiersName: cn=Manager,dc=example,dc=com
reqOld: modifyTimestamp: 20051017083734Z
```

Notes d'usage

Les serveurs peuvent implémenter seulement un sous-jeu de ces attributs, ou fournir des mécanismes de configuration pour réduire la plage d'opération couverte dans les logs. Les clients de réplication travaillant depuis un log complet peuvent utiliser un filtre de recherche avec les termes **"(&(objectClass=AuditWriteObject)(reqResult=0))"** pour filtrer les enregistrements peut utile.

Considérations IANA

En accord avec la rfc3383 :

```
OpenLDAP_Experimental = 1.3.6.1.4.1.4203.666
LOG_SCHEMA = OpenLDAP_Experimental.11.5
LOG_SCHEMA_AT = LOG_SCHEMA.1
LOG_SCHEMA_OC = LOG_SCHEMA.2
LOG_SCHEMA_SYN = LOG_SCHEMA.3
```