
slapo-accesslog

Overlay accesslog

Overlay de log des accès. Il permet d'enregistrer tous les accès à la base de données dans une autre base.

Configuration

logdb <suffix> Spécifie le suffix d'une base de données à utiliser pour stocker les enregistrements.

logops <operations> Spécifie quel types d'opérations logger. (abandon, add, bind, compare, delete, extended, modify, modrdn, search, unbind, et les alias writes (add, delete, modify, modrdn), reads (compare, search), session (abandon, bind, unbind) et all (toutes les opérations))

logbase <operations><baseDN> Spécifie un jeu d'opérations qui seront loggés uniquement s'ils se produisent dans une arborescence spécifique de la base, et délimités par le caractère 'l'

logold <filter> Spécifie un filtre pour matcher les entrées supprimées et modifiées. Si l'entrée match le filtre, l'ancienne entrée sera loggées avec la requête en cour.

logoldattr <attr> Spécifie une liste d'attributs loggés.

logpurge <age><interval> Spécifie la durée maximal pour les entrées à maintenir dans la base. et la fréquence de scan de la base pour les anciennes entrées. le format de date est [ddd+]hh :mm[:ss]. ex : logpurge 2+00 :00 1+00 :00 pour un scan quotidien avec suppression des entrées de plus de 2 jours.

logsuccess TRUE | FALSE à TRUE, les enregistrement seront loggés uniquement si la requête produit un succès. défaut : FALSE

Schéma

accesslog utilise le schéma audit décrit ici. ce schéma est conçu spécifiquement pour cet overlay.

auditObject 2 classes en sont dérivés : auditReadObject et auditWriteObject.

reqStart

reqEnd Fournissent l'heure de début et de fin de l'opération.

reqType Décrit le type d'opération qui est loggée.

reqSession Identifiant commun à toutes les opérations associées avec la même session LDAP

reqDN DN de la cible de l'opération

reqAuthzID DN de l'utilisation qui a effectué l'action

reqControls

reqRespControls Gèrent les contrôles envoyés par le client dans la requête et retourné par le serveur.

reqResult Code de résultat LDAP de l'opération

reqMessage message d'erreur s'il y'en a un

reqReferral Gère les référant qui ont été retournés avec le résultat de la requête.

```
( 1.3.6.1.4.1.4203.666.11.5.2.1 NAME 'auditObject' DESC 'OpenLDAP request auditing' SUP top STRUCTURAL MUST (
reqStart $ reqType $ reqSession ) MAY ( reqDN $ reqAuthzID $ reqControls $ reqRespControls $ reqEnd $
reqResult $ reqMessage $ reqReferral ) )
```

(1.3.6.1.4.1.4203.666.11.5.2.4 NAME 'auditAbandon' DESC 'Abandon operation' SUP auditObject STRUCTURAL MUST reqId)

(1.3.6.1.4.1.4203.666.11.5.2.5 NAME 'auditAdd' DESC 'Add operation' SUP auditWriteObject STRUCTURAL MUST reqMod)

(1.3.6.1.4.1.4203.666.11.5.2.6 NAME 'auditBind' DESC 'Bind operation' SUP auditObject STRUCTURAL MUST (reqVersion \$ reqMethod))

(1.3.6.1.4.1.4203.666.11.5.2.7 NAME 'auditCompare' DESC 'Compare operation' SUP auditObject STRUCTURAL MUST reqAssertion)

(1.3.6.1.4.1.4203.666.11.5.2.8 NAME 'auditDelete'
DESC 'Delete operation' SUP auditWriteObject STRUCTURAL MAY reqOld)

(1.3.6.1.4.1.4203.666.11.5.2.9 NAME 'auditModify' DESC 'Modify operation' SUP auditWriteObject STRUCTURAL MAY reqOld MUST reqMod)

(1.3.6.1.4.1.4203.666.11.5.2.10 NAME 'auditModRDN' DESC 'ModRDN operation' SUP auditWriteObject STRUCTURAL MUST (reqNewRDN \$ reqDeleteOldRDN) MAY (reqNewSuperior \$ reqOld))

(1.3.6.1.4.1.4203.666.11.5.2.11 NAME 'auditSearch' DESC 'Search operation' SUP auditReadObject STRUCTURAL MUST (reqScope \$ reqDerefAliases \$ reqAttrsOnly) MAY (reqFilter \$ reqAttr \$ reqEntries \$ reqSizeLimit \$ reqTimeLimit))

(1.3.6.1.4.1.4203.666.11.5.2.12 NAME 'auditExtended' DESC 'Extended operation' SUP auditObject STRUCTURAL MAY reqData)