

---

# slapo-dds

## Overlay dds

Overlay de services d'annuaire dynamique. implémente la rfc 2589 et permet de définir des objets dynamique, caractérisés par la classe d'objet `dynamicObject`.

## OPTIONS

**dds-max-ttl <ttl>** TTL max ( de 86400 à 31557600 )

**dds-min-ttl <ttl>** TTL minimum pour les opérations de refresh.

**dds-default-ttl <ttl>** TTL par défaut pour les nouveaux objets créés

**dds-interval <ttl>** Interval entre les vérifications d'expiration

**dds-tolerance <ttl>** Spécifie une durée supplémentaire à ajouter au timer qui attend pour supprimer les objets expirés

**dds-max-dynamicObjects <num>** Spécifie le nombre max d'objets dynamiques qui peuvent exister simultanément dans un contexte de nommage.

**dds-state TRUE|false** Spécifie si la fonctionnalité est activée ou non. Les proxy non pas besoin de gérer ces objets mais necessitent d'informer le frontend du support de ces objets.

## Contrôle d'accès

cet overlay restreint l'opération refresh en nécessitant l'accès **manage** sur l'attribut **entryTtl**. Vu que c'est un attribut NO-USER-MODIFICATION, aucune écriture directe n'est possible. l'overlay convertit donc l'opération refresh en une modification interne pour modifier **entryTtl** avec le jeu de contrôle relax.

La rfc 2589 recommande que les clients anonymes ne devraient pas être autorisés à refresh un objet dynamique :

**access to attrs=entryTtl by users manage by \* read**

Restreindre refresh au créateur de l'objet :

**access to attrs=entryTtl by dnattr=creatorsName manage by \* read**

Assument que Meetings est un attribut de DN valides, permettant aux utilisateurs de commencer une conférence et rafraîchir ; empêcher les participant de refresh, et seul le créateur peut le supprimer :

**access to dn.base="cn=Meetings" attrs=children by users write**

**access to dn.onelevel="cn=Meetings" attrs=entry by dnattr=creatorsName write by \* read**

**access to dn.onelevel="cn=Meetings" attrs=participant by dnattr=creatorsName write by users selfwrite by \* read**

**access to dn.onelevel="cn=Meetings" attrs=entryTtl by dnattr=participant manage by \* read**

## Réplication

Cette implémentation fournie une implémentation réduite de la réplication. Seul les masters peuvent manipuler l'expiration des objets. En répliant ces objets, on peut explicitement inclure la classe `dynamicObject` et l'attribut `entryTtl`. cette implémentation introduit un nouvel attribut opérationnel, `entryExpireTimestamp`, qui contient le timestamp d'expiration. Il doit être exclus de la réplication avec :

**syncrepl ...**

**exattrs=entryTtl,entryExpireTimestamp**