OpenLDAP - Limites

configuration des limites de slapd

Il est généralement préférable de limiter les ressources du serveur pour qu'il soit accessible à tous les clients. OpenLDAP fournit 2 type de limites : un limite de taille, qui peut être restreinte par le nombre d'entrées qu'un client peut récupérer en une seule opération, et une limite de temps, qui restreint le temps qu'une opération peut se poursuivre.

Limites Soft et Hard

L'administrateur du serveur peut limiter les limites **hard** et **soft**. Les limites **soft** sont les valeurs de limite par défaut, les limites **hard** sont les limites qui ne peuvent pas être dépassée par les utilisateurs LDAP.

Les clients LDAP peuvent spécifier leur propre limites de taille et de temps pour les opérations de recherche.

Si le client spécifie une limite alors la plus faible des valeurs entre celle-ci et la **hard limit** sera choisie. Si le client ne spécifie pas de limite, la **soft limit** s'applique.

Le rootdn n'est pas sujet à ces limites.
sizelimit {<integer>|unlimited} # défaut 500
timelimit {<integer>|unlimited} # défaut 3600
Une forme étendue permet aux limites soft et hard d'être séparés.
sizelimit size[.{soft|hard|unchecked}]=<integer> [...]
timelimit time.{soft=<integer>} [...]
exemple
sizelimit size.soft=10 size.hard=75
Le mot clé **unchecked** spécifie une limite du nombre d'entrées que le serveur va examiner une fois qu'il a crée un lot de résultats candidat en utilisant les indices. Ça peut être très important dans les gros annuaires, quand une recherche qui ne peut pas être satisfaite depuis un index peut nécessiter d'examiner des millions d'entrées.

Limites par base

Chaque base de donnée peut avoir ses propres limites. La syntaxe est plus flexible, et permet différentes limites à appliquer à différentes entités. le terme entité est utilisé pour indiquer l'ID de la personne ou du processus qui a initié l'opération LDAP. Dans **slapd.conf** le mot clé est **limits**. En utilisant le backend slapd config, l'attribut correspondant est **olcLimits**. La syntaxe est la même dans les 2 cas.

limits <who> <limit> [<limit> [...]]
la clause limits peut être spécifiée plusieurs fois. Le serveur examine chaque clause jusqu'à ce qu'il en trouve une qui corresponde à l'ID qui a requis l'opération. Si aucune correspondante n'est trouvée, les limites globales sont utilisées.

Spécifier à qui s'applique les limites

La partie <who> peut prendre les valeurs suivante :
`*_____All, including anonymous and authenticated users`

```
anonymous_____________________Anonymous (non-authenticated) users
users_________________________Authenticated users
self__________________________User associated with target entry
dn[.<basic-style>]=<regex>___Users matching a regular expression
dn.<scope-style>=<DN>________Users within scope of a DN
group[/oc[/at]]=<pattern>____Members of a group
```

Spécifier des limites de temps

time.soft=<integer>
où integer est la durée en seconde.
si soft ou hard ne sont pas spécifiés, la valeur est utilisée pour les 2 :
limits anonymous time=27
la valeur unlimited peut être utilisé pour supprimer la limite de temps hard :
limits dn.exact="cn=anyuser,dc=example,dc=org" time.hard=unlimited
spécifier des tailles limites.
size[.soft|hard|unchecked]=integer>
où integer est le nombre d'entrée maximum que slapd va retourner.

Limites de taille et résultats paginés

Si le client LDAP ajoute le **pagedResultsControl** pour les opérations de recherche, la limite de taille hard est utilisée par défaut, parce que la requête pour une taille de page spécifique est considérée comme une requête explicite pour une limitation sur un nombre d'entrée à retourner. Cependant, la taille limite s'applique au compteur total des entrées retournées dans la recherche, et pas dans une simple page.

size.pr={<integer>|noEstimate|unlimited}

integer est la taille de page maximum si aucune taille implicite n'est donnée. **noEstimate** n'a pas d'effet dans l'implémentation courante vu que le serveur ne retourne pas une estimations de taille de résultat. **unlimited** indique qu'aucune limite n'est appliquée à la taille de page maximum.

size.prtotal contrôle le nombre total d'entrées qui peuvent être retournés par une recherche paginée. Par défaut la limite est la même que la limite size.hard.

size.prtotal={<integer>|unlimited|disabled}

unlimited supprime la limite sur le nombre d'entrée qui peuvent être retournés par une recherche paginée. **disabled** peut être utilisé pour désactiver sélectivement les recherche de résultat paginés.

Exemples

cet exemple applique des limites de temps et de taille pour toutes les recherche par les utilisateurs, excepté rootdn.
sizelimit 50
timelimit 10
Limites hard et soft global : Il est parfois utile de limiter la taille des résultats mais de permettre aux clients de demander une limite plus élevée si nécessaire. Cela peut être fait en définissant des limites soft et hard séparés :
sizelimit size.soft=5 size.hard=100
Pour se prémunir des clients qui font des recherches non-indexées inefficaces, ajouter la limite unchecked :
sizelimit size.soft=5 size.hard=100 size.unchecked=100
Donner des limites plus grandes pour des utilisateurs spécifiques.
limits dn.exact="cn=anyuser,dc=example,dc=org" size=100000
limits dn.exact="cn=personnel,dc=example,dc=org" size=100000
limits dn.exact="cn=dirsync,dc=example,dc=org" size=100000

Il est généralement mieux d'éviter de mentionner des utilisateurs spécifiques dans la configuration serveur. Une meilleur manière est de donner des limites supérieurs à un groupe :

limits group/groupOfNames/member="cn=bigwigs,dc=example,dc=org" size=100000

Limiter qui peut faire des recherche paginées

limits group/groupOfNames/member="cn=dirsync,dc=example,dc=org" size.prtotal=unlimited

limits users size.soft=5 size.hard=100 size.prtotal=disabled

limits anonymous size.soft=2 size.hard=5 size.prtotal=disabled