rfc3088

OpenLDAP Root Service - Service de référencement LDAP expérimental

Le projet OpenLDAP opère comme service de référencement d'accès aux annuaires LDAP, connu comme le "OpenLDAP Root Service". Le système Automatisé génère des références basée sur les informations d'emplacement de service publiées dans les enregistrement DNS SRV RR. Ce document décris ce service.

Les annuaires LDAP utilisent un schéma de nommage hiérarchique hérité de X.500. Traditionnellement, les déploiements X.500 ont utilisé un schéma de nommage géo-politique. Cependant, l'infrastructure d'enregistrement et les services de localisation dans beaucoups de portions du nommage hiérarchique sont inadéquates ou non-existants.

La construction d'un annuaire global nécessite une infrastructure d'enregistrement et un service de localisation robuste. L'utilisation du nommage basé sur le domaine internet permet aux services d'annuaire LDAP de faire un levier vers une infrastructure d'enregistrement DNS des enregistrement de ressource DNS SRV existants pouvant être utilisé pour localiser les services.

La plupart des implémentations LDAP existantes ne supportent pas la localisation des services d'annuaires en utilisant les DNS SRV RR. Cependant, la plupart des serveurs supportent la génération de références vers des serveurs supérieurs. Ce service fournis un service LDAP root que les serveur peuvent utilisé comme leur service référant supérieur.

Un client peut également utiliser le service directement pour localiser les services associés avec un DN arbitraire dans la hiérarchie.

Note : les mécanismes utilisé par le service sont expérimentaux. Les descriptions fournies par ce document ne sont pas définitifs.

Générer des références basées sur les DNS SRV RR

Le service mappe un DN vers un fqdn en utilisant l'algorithme suivant :

```
domain = null;
foreach RDN left-to-right // [1]
{
 if not multi-valued RDN and RDN.type == domainComponent
 {
  if ( domain == null || domain == "." )
  { // start
   domain = "";
  }
  else
  { // append separator
   domain .= ".";
  }
  if ( RDN.value == "." )
  { // root
   domain = ".";
  }
  else
  { // append domainComponent
   domain .= RDN.value;
  }
  continue;
 }
```

```
 domain = null;
}
```

Exemples

Distinguished Name	Domain
DC=example,DC=net	example.net
UID=jdoe,DC=example,DC=net	example.net
DC=.	. [2]
DC=example,DC=net,DC=.	. [3]
DC=example,DC=.,DC=net	net [4]
DC=example.net	example.net [5]
CN=Jane Doe,O=example,C=US	null
UID=jdoe,DC=example,C=US	null
DC=example,O=example,DC=net	net
DC=example+O=example,DC=net	net
DC=example,C=US+DC=net	null

Notes

0) Une version ultérieur utilisera un mécanisme standardisé

1) Une version ultérieur de ce service peut utiliser un algorithme droit-à-gauche.

2) La rfc2247 ne statut pas sur la manière de mapper le domaine représentant là racine de l'arborescence vers un DN. On suggère que la racine du domaine soit mappé à "DC=." et qu'il soit inversable

3) La rfc2247 statut que le domaine "example.net" devrait être mappé au dn "DC=example,DC=net", et non "DC=example,DC=net,DC=.", ce n'est pas notre intention d'introduire ou supporter un domaine alternatif au mappage de DN.

4) La rfc2247 statut que le domaine "example.net" devrait être mappé au dn "DC=example,DC=net", et non "DC=example,DC=.,DC=net", ce n'est pas notre intention d'introduire ou supporter un domaine alternatif au mappage de DN.

5) La rfc2247 statut que la valeur d'un type d'attribut DC est un composant de domaine. Il ne devrait pas contenir plusieurs composants de domaine multiple. Une version ultérieur de ce service peut mapper ce domaine à null ou être encodé pour retourner un erreur de DN invalide.

Si le domaine est null ou ".", le service stop tout traitement et retourne noSuchObject. Une version ultérieur de ce service peut annuler le traitement si le domaine résultant est un domaine top-level.

Localiser les services LDAP

Le service root localise les services associés avec une nom de domaine pleinement qualifié en requêtant le DNS pour les enregistrements de ressoure LDAP SRV. Pour le domaine example.net, le service devrait émettre une demande SRV pour le domaine "_ldap._tcp.example.net". Une requête réussie va retourner un ou plusieurs enregistrements de ressources sous la forme :

_ldap._tcp.example.net. IN SRV 0 0 389 ldap.example.net.

Si aucun enregistrement de ressource LDAP SRV n'est retourné ou une erreur DNS se produit, le service annule tout traitement et retourne noSuchObject. Une version ultérieur de ce service gérera mieux les erreurs.

Construire les réferences LDAP

Pour chaque DNS SRV RR retourné pour le domaine, une URL LDAP est construite. Pour l'enregistrement ci-dessus, l'url serait :

ldap ://ldap.example.net :389/

Ces URL sont ainsi retournées dans le référant. Les URL sont actuellement retournés dans l'ordre du resolver.

Opérations du protocole

Cette section décris comment le service effectue des opération LDAP de base. Le service supporte les opérations étendues prévues via certains contrôles.

Opérations de base

Les opérations de base retournent un résultat référant si le DN cible peut être mappé à un jeu d'URLs LDAP comme décris ci-dessus. Sinon, une réponse noSuchObject ou autre réponse appropriée est retournée.

Opération Bind

Ce service accepte le bind anonyme. Tous les autres bind retournent un code non 0. En particulier, les clients qui envoient des accréditifs en texte claire vont recevoir un unwillingToPerform avec un texte d'avertissement. Vu que ce service est en lecture seule, l'authentification lDAP v3 n'est pas supportée.

Unbind

Une fois une demande unbind reçue, le serveur abandonne toutes requêtes faites par le client et déconnecte.

Extended

Le service ne reconnaît actuellement aucune opération étendue.

Update

Une version future de ce document peut retourner unwillingToPerform pour toutes les opérations de modification vu que c'est un service non authentifié.

Controle ManageDSAit

Le service supporte le contrôle ManageDSAit. Si les informations de l'emplacement DNS sont disponible pour de DN de base lui-même, le service retourne unwillingToPerform pour les opérations autre que de recherche. Pour les opérations de recherche, une entrée va être retourné si elle est dans le scope et correspond au filtre fournis. Par exemple :

```
c: searchRequest {
 base="DC=example,DC=net"
 scope=base
 filter=(objectClass=*)
 ManageDSAit
}

s: searchEntry {
 dn: DC=example,DC=net
 objectClass: referral
 objectClass: extensibleObject
 dc: example
 ref: ldap://ldap.example.net:389/
 associatedDomain: example.net
}
s: searchResult {
 success
}
```

Si les informations d'emplacement DNS sont disponible pour la portion DC d'une entrée subordonnée, le service retourne noSuchObject avec le matchedDN à la portion DC de la base pour la recherche et les opérations de mise à jours :

```
c: searchRequest {
 base="CN=subordinate,DC=example,DC=net"
 scope=base
 filter=(objectClass=*)
 ManageDSAit
}

s: searchResult {
 noSuchObject
 matchedDN="DC=example,DC=net"
}
```

Utiliser le service

Les serveurs peuvent être configurés pour référer les requêtes à <ldap ://root.openldap.org :389>. Bien que les clients peuvent utiliser le service directement, Ce n'est pas encouragé. Les clients devraient utiliser un service local et utiliser ce service seulement quand il est référencé. Le service supporte LDAPv3 et LDAPv2+ sur TCP/IPv4. Une version future de ce document supportera TCP/IPv6 ou d'autres protocoles de transport/internet.

Disponibilité

Ce service fonctionne actuellement sur un seul hôte. Cet hôte et les ressources réseaux associées ne sont pas exhaustives. On peut facilement augmenter la disponibilité à la demande. Le service peut également être facilement dupliqué localement.

Interopérabilité du protocole

Le serveur implémente toutes les fonctionnalités LDAPv3 nécessaire au service. LDAPv2 de supporte pas les referral et donc ne peut pas être utilisé par ce service. LDAPv2+ fournis des extensions à LDAPv2, incluant les référants. Une future version de ce document supprimera le support le LDAPv2+.

Considérations de sécurité

Ce service fournis des informations aux clients anonymes. Cette information est dérivée des annuaires publiques, appelés DNS.

L'utilisation de l'authentification nécessiterait aux clients de divulguer des informations au service. Cela serait une invasion non-nécessaire.

Le manque de chiffrement permet l'écoute des demandes et réponses. Une version ultérieur de ce service pourrait supporter le chiffrement.

La protection de l'intégrité des informations n'est pas fournie par le service. Le service est sujet à diverses formes d'attaques DNS. Une version ultérieur de ce document peut supporter DNSSEC et fournir une protection d'intégrité.

Le service est sujet à diverses attaque DOS. Une version ultérieur de ce document nécessiterait une meilleur protection pour de tels attaques.