rfc4521

Extentions LDAP

Mécanisme de découverte

LDAP ne fournis aucun mécanisme pour qu'un serveur découvre les capacité des clients. L'attribut **supportedControl** du RootDSE est utilisé pour avertir des opérations étendues supportées. l'attribut **supportedFeatures** est utilisé pour avertir des fonctionnalités. D'autres attributs du RootDSE peut être utilisés pour avertir d'autres capacités.

LDAP est conçus pour supporter unicode. les options de tag de langue (rfc 3866) fournissent un mécanisme pour tag les valeurs avec des informations de langue.

Extensions d'opération LDAP

Les extensions devraient utiliser les contrôles pour définir des extensions qui complémentent des opérations existantes, sinon, il est préférable de définir des opérations étendues.

Contrôles

Les contrôles sont recommandés pour étendre de opérations existantes. Une opération existante peut être une opération de base, une opération étendue, une modification de mot de passe ou une opération définie comme extension d'une opération de base ou étendue.

Les extensions ne devraient pas retourner de réponse à moins que le serveur sait que le client peut utiliser ce contrôle. Une opération existante peut être étendue pour retourner des messages **IntermediateResponse**. Les contrôles ne devraient pas définir de sémantique additionnelles à la criticité des contrôles.

Étendre l'opération Bind avec des contrôles

Les contrôles attachés aux messages de requête et de réponse d'une opération Bind ne sont pas protégés par une couche de sécurité établie par l'opération bind.

Étendre l'opération StartTLS avec des contrôles

Les contrôles attachés aux messages de requête et de réponse d'une opération StartTLS ne sont pas protégés par la couche de sécurité.

Étendre l'opération de recherche avec des contrôles

L'opération de recherche a 2 phases :

- trouver l'objet de base
- Rechercher les objets à ou sous l'objet de base.

Les contrôles étendant la recherche devraient clairement statuer sur quelle(s) phase(s) le contrôle s'applique.

Étendre les opérations update avec des contrôles

Les opération update ont des propriétés d'atomicité, consistance, isolation et durabilité (ACID)

atomicité : tous ou aucun des changements demandés ont été fait

consistance : L'état DIT résultant doit être conforme au schéma et d'autres contraintes

isolation : les états intermédiaires ne sont pas exposés

durabilité : l'état DIT résultant est préservé jusqu'à une mise à jours ultérieure.

En définissant un contrôle qui demande des changements additionnels, ces changements ne devraient pas être traités comme partie d'une transaction séparée

Réponses intermédiaires

Les extensions devraient utiliser les messages **IntermediateResponse** au lieu des messages **ExtendedResponse** pour retourner des résultats intermédiaires.

Notifications non-sollicitées

Les notifications non-sollicitées permettent à un serveur de notifier le client d'évènements non associés avec l'opération courante. Ces extensions doivent être conçues de manière à ce qu'un serveur n'envoie ces notification que s'il sait que le client peut utiliser ces notifications.

Code de résultat

Les extensions qui spécifient de nouvelles opérations ou améliorent des opérations existantes ont souvent besoin de nouveaux code de résultat. L'extension doit être conçue de manière à ce qu'un client ait une indication clair de la nature du résultat.

Types de message LDAP

Les extensions peuvent spécifier de nouveaux types de messages LDAP en étendant le choix **protocolOp** de la séquence **LDAPMessage**, mais c'est généralement inapproprié et non-nécessaire. Cependant, dans certains cas, de nouveaux mécanismes d'extensions devraient être définis.

Méthodes d'authentification

Bind supporte 2 méthodes d'authentification, simple et SASL. Il est recommandé que les nouveau processus d'authentification soient définis comme mécanisme SASL.

Extension de schéma

Les extensions définissant des éléments de schéma LDAP doivent fournir la définition de schéma conformément avec la syntaxe définie.

Syntaxes LDAP

Chaque syntaxe LDAP est définie en terme d'ASN.1. Chaque extension détaillant une syntaxe LDAP doit spécifier les données ASN.1 associées avec la syntaxe.

Matching Rules

3 types basique de règle de correspondance peuvent être associés avec un type d'attribut. En plus, LDAP fournis un mécanisme de règle extensible.

Autres mécanismes étendu

Chaque option est identifiée par une chaîne de lettres, nombre et tirets. Cette chaîne devrait être courte.

Les extensions interagissant avec des identité d'authorisation devraient supporter le format authzId. ce format est extensible.

Les extensions d'URL LDAP sont identifiées par une chaîne courte, un descripteur, la chaîne devrait être courte.