

Le Format d'URL de LDAP

1. Statut de ce document

Ce document spécifie un protocole standard d'Internet pour la communauté Internet, et ne sera éprouvé qu'après plusieurs discussions et suggestions. Merci de vous référer à l'édition courante du " Internet Official Protocol Standards " (STD1) pour l'état de standardisation et le statut de ce protocole. La distribution de ce document est illimitée.

Copyright

Copyright © "Internet society" (1999) – tous droits réservés.

Note d'IESG

Ce document décrit un protocole d'accès à un annuaire qui fournit tant l'accès en lecture que l'accès pour mise à jour. L'accès de mise à jour exige une authentification sécurisée, mais ce document n'exige la mise en place d'aucun mécanisme d'authentification adéquat.

Selon RFC 2026, section 4.4.1, ce cahier des charges est approuvé par IESG comme norme proposée en dépit de cette limitation, pour les raisons suivantes :

- a. pour encourager la mise en place et le test d'interopérabilité de ces protocoles (avec ou sans l'accès de mise à jour) avant qu'ils soient déployés, et
- b. pour encourager le déploiement et l'utilisation de ces protocoles dans des applications à lecture seule. (par exemple applications où LDAPv3 est utilisé comme langage d'interrogation pour les annuaires qui sont mis à jour par un mécanisme sécurisé autre que LDAP), et
- c. pour éviter de retarder l'avancement et le déploiement d'autres protocoles standard d'Internet qui exigent la possibilité de questionner, mais pas de mettre à jour, des serveurs d'annuaire LDAPv3.

Les lecteurs sont avertis par la présente que jusqu'à ce que des mécanismes obligatoires d'authentification soient normalisés, les clients et les serveurs écrits selon ce cahier des charges

qui se servent de la fonctionnalité de mise à jour sont IMPROBABLEMENT INTEROPERABLE, ou PEUVENT INTEROPERER SEULEMENT SI L'AUTHENTIFICATION EST RÉDUITE À UN NIVEAU INADMISSIBLEMENT FAIBLE.

Les implanteurs sont découragés par la présente de déployer des clients ou des serveurs LDAPv3 qui mettent en œuvre la fonctionnalité de mise à jour, jusqu'à ce qu'une norme proposée pour l'authentification obligatoire dans LDAPv3 ait été approuvée et éditée comme RFC.

2. Résumé

LDAP est protocole allégé d'accès aux annuaires, défini dans [1], [2] et [3]. Ce document décrit un format pour un localisateur de ressources uniformes LDAP (LDAP URL). Le format décrit une opération de recherche LDAP à exécuter pour rechercher l'information à partir d'un annuaire LDAP. Ce document remplace le RFC 1959. Il met à jour le format URL de LDAP pour la version 3 de LDAP et clarifie comment les URL LDAP sont résolus. Ce document définit également un mécanisme d'extension pour les URL LDAP, de sorte que les futurs documents puissent étendre leur fonctionnalité, par exemple, pour permettre l'accès aux nouvelles extensions LDAPv3 dès qu'elles sont définies.

Les mots clés "DOIT", "PEUT", et "DEVRAIT" utilisés dans ce document doivent être interprétés comme décrit dans [6].

3. Définition d'URL

Un URL de LDAP commence par le préfixe protocolaire "ldap" et est défini par la grammaire suivante.

```

ldapurl      = scheme "://" [hostport] ["/"
                [dn ["?" [attributes] ["?" [scope]
                ["?" [filter] ["?" extensions]]]]]]
scheme       = "ldap"
attributes   = attrdesc *("," attrdesc)
scope        = "base" / "one" / "sub"
dn           = distinguishedName de la Section 3 de [1]
hostport     = hostport de la Section 5 de RFC 1738 [5]
attrdesc     = AttributeDescription de la Section 4.1.5 de [2]
filter       = filter de la Section 4 de [4]
extensions   = extension *("," extension)
extension    = ["!"] extype ["=" exvalue]
extype       = token / xtoken
exvalue      = LDAPString de la section 4.1.2 de [2]
token        = oid de la section 4.1 de [3]
xtoken       = ("X-" / "x-") token

```

Le préfixe "ldap" indique une entrée ou des entrées résidant dans le serveur LDAP fonctionnant sur la machine indiquée au numéro de port donné. Le port LDAP par défaut est le port TCP 389.

Si aucun port machine n'est donné, le client doit à priori connaître un serveur LDAP approprié à contacter.

Le "dn" est un nom différencié LDAP utilisant le format de chaîne de caractères décrit dans [1]. Il identifie l'objet de base de la recherche LDAP.

```

ldapurl      = scheme "://" [hostport] ["/"
                [dn ["?" [attributes] ["?" [scope]
                ["?" [filter] ["?" extensions]]]]]]
scheme       = "ldap"
attributes   = attrdesc *(", " attrdesc)
scope        = "base" / "one" / "sub"
dn           = distinguishedName de la Section 3 de [1]
hostport     = hostport de la Section 5 de RFC 1738 [5]
attrdesc     = AttributeDescription de la Section 4.1.5 de [2]
filter       = filter de la Section 4 de [4]
extensions   = extension *(", " extension)
extension    = ["!"] extype ["=" exvalue]
extype       = token / xtoken
exvalue      = LDAPString de la section 4.1.2 de [2]
token        = oid de la section 4.1 de [3]
xtoken       = ("X-" / "x-") token

```

Le préfixe "ldap" indique une entrée ou des entrées résidant dans le serveur LDAP fonctionnant sur la machine indiquée au numéro de port donné. Le port LDAP par défaut est le port TCP 389. Si aucun port machine n'est donné, le client doit à priori connaître un serveur LDAP approprié à contacter.

Le "dn" est un nom différencié LDAP utilisant le format de chaîne de caractères décrit dans [1]. Il identifie l'objet de base de la recherche LDAP.

La construction d'attributs est employée pour indiquer quels attributs de l'entrée ou des entrées devraient être retournés. Les différents noms "attrdesc" sont définis comme pour "AttributeDescription" dans [2]. Si la partie attribut est omise, tous les attributs d'utilisateur de l'entrée ou des entrées devraient être demandés (par exemple, en plaçant une liste NULLE dans le champ d'attributs "AttributeDescriptionList" dans la demande de recherche LDAP, ou (dans LDAPv3) en demandant le nom d'attribut spécial "*").

La construction d'une portée est employée pour indiquer la portée de la recherche à exécuter dans le serveur LDAP donné. Les portées permises sont "base" pour une recherche d'objet de base, "one" pour une recherche sur un niveau, ou "sub" pour une recherche de sous-arbre. Si la portée est omise, une portée de "base" est assumée.

Le filtre est utilisé pour indiquer le filtre de recherche à appliquer pendant la recherche aux entrées dans la portée indiquée. Il a le format indiqué dans [4]. Si le filtre est omis, un filtre "(objectClass=*)" est assumé.

La construction d'extensions fournit à l'URL de LDAP un mécanisme d'extensibilité, permettant aux capacités de l'URL d'être à l'avenir étendues. Les extensions sont une liste de paires de

"type=valeur" simplement séparées par des virgules, où la partie "=valeur" PEUT être omise pour des options ne l'exigeant pas. Chaque paire de "type=valeur" est une extension séparée. Ces extensions d'URL de LDAP ne sont pas nécessairement liées à aucun de ces mécanismes d'extension de LDAPv3. Les extensions peuvent être supportées ou non supportées par le client résolvant l'URL. Une extension préfixée avec le caractère '!' (ASCII 33) est critique. Une extension non préfixée avec le caractère '!' est non critique.

Si une extension est supportée par le client, le client DOIT obéir à l'extension si l'extension est critique. Le client DEVRAIT obéir aux extensions supportées qui sont non critiques.

Si une extension est non supportée par le client, le client NE DOIT PAS traiter l'URL si l'extension est critique. Si une extension non supportée est non critique, le client DOIT ignorer l'extension.

Si une extension critique ne peut pas être traitée avec succès par le client, le client NE DOIT PAS traiter l'URL. Si une extension non-critique ne peut pas être traitée avec succès par le client, le client DEVRAIT ignorer l'extension.

Les types d'extension préfixés par "X-" ou "x-" sont réservés pour l'usage dans des accords bilatéraux entre les parties communicantes. D'autres types d'extension DOIVENT être définis dans ce document, ou dans d'autres documents de normes.

Une extension d'URL de LDAP est définie dans ce document dans la prochaine section. D'autres documents ou une future version de ce document PEUVENT définir d'autres extensions.

Notez que tous caractères URL illégaux (par exemple, les espaces), caractères spéciaux d'URL (comme défini dans section 2.2 du RFC 1738) et le caractère réservé '?' (ASCII 63) apparaissant à l'intérieur d'un DN, d'un filtre, ou de tout autre élément d'un URL de LDAP DOIT être échappé en utilisant la méthode % décrite dans le RFC 1738 [5]. Si un caractère virgule ',' apparaît à l'intérieur d'une valeur d'extension, le caractère DOIT également être échappé en utilisant la méthode %.

4. l'Extension de "Bindname"

Cette section définit une extension d'URL de LDAP pour représenter le nom différencié à utiliser par un client lors de l'authentification à un annuaire LDAP pendant la résolution d'un URL de LDAP. Les clients PEUVENT implémenter cette extension.

Le type de l'extension est "bindname". La valeur de l'extension est le nom différencié de l'entrée de l'annuaire à authentifier, sous la même forme que celle décrite pour "dn" dans la grammaire ci-dessus. Le "dn" peut être la chaîne VIDE pour spécifier un accès non authentifié. L'extension peut être ou critique (préfixée par le caractère '!') ou non critique (non préfixée par le caractère '!').

Si l'extension de "bindname" est critique, le client résolvant l'URL DOIT s'authentifier à l'annuaire en utilisant le nom différencié donné et une méthode appropriée d'authentification. Notez que pour un nom différencié NUL, aucune liaison NE PEUT être exigée pour obtenir l'accès anonyme à l'annuaire. Si l'extension est non critique, le client PEUT se lier à l'annuaire en utilisant le nom différencié donné.

5. Traitement d'URL

Cette section décrit comment un URL de LDAP DEVRAIT être résolu par un client.

D'abord, le client obtient une connexion au serveur LDAP référencé dans l'URL, ou un serveur LDAP au choix du client si aucun serveur LDAP n'est explicitement référencé. Cette connexion PEUT être ouverte spécifiquement afin de résoudre l'URL ou le client PEUT réutiliser une connexion déjà ouverte. La connexion PEUT fournir la confidentialité, l'intégrité, ou d'autres services, par exemple, en utilisant TLS. L'utilisation des services de sécurité est à la discrétion du client si non spécifié dans l'URL.

Ensuite, le client s'authentifie au serveur LDAP. Cette étape est facultative, à moins que l'URL ne contienne une extension critique de "bindname" avec une valeur non nulle. Si une extension de "bindname" est donnée, le client procède selon la section ci-dessus.

Si une extension de "bindname" n'est pas indiquée, le client PEUT se lier à l'annuaire en utilisant un "dn" approprié et la méthode d'authentification de son propre choix (authentification NULLE y compris).

Ensuite, le client exécute l'opération de recherche LDAP indiquée dans l'URL. Des champs additionnels dans la demande de recherche du protocole LDAP, telle que le "sizelimit", "timelimit", "deref", et toute autre chose non indiqués ou par défaut dans la spécification de l'URL, PEUVENT être placés à la discrétion du client.

Une fois que la recherche s'est terminée, le client PEUT fermer la connexion au serveur LDAP, ou le client PEUT maintenir la connexion ouverte pour une utilisation future.

6. Exemples

Ce qui suit sont des exemples d'URL LDAP utilisant le format défini ci-dessus. Le premier exemple est un URL de LDAP se rapportant à l'université du Michigan, disponible à partir d'un serveur LDAP au choix du client :

```
ldap:///o=University%20of%20Michigan, c=US
```

Le prochain exemple est un URL de LDAP se rapportant à l'université du Michigan dans un serveur particulier de ldap :

```
ldap://ldap.itd.umich.edu/o=University%20of%20Michigan, c=US
```

Ces deux URL correspondent à une recherche d'objet de base de l'entrée "o=University of Michigan, c=US" à l'aide d'un filtre "(objectclass=*)", demandant tous les attributs.

L'exemple suivant est un URL de LDAP se rapportant seulement à l'attribut "postalAddress" de l'université du Michigan :

```
ldap://ldapitd.umich.edu/o=University%20of%20Michigan, c=US?postalAddress
```

L'opération de recherche correspondante LDAP est la même que dans l'exemple précédent, sauf que seul l'attribut adresse postale est demandé.

Le prochain exemple est un URL de LDAP se rapportant à l'ensemble des entrées trouvées en questionnant le serveur LDAP donné sur le port 6666 et en faisant une recherche de sous-arbre de l'université du Michigan pour n'importe quelle entrée avec un nom commun "Babs Jensen", recherchant tous les attributs :

```
ldap://host.com:6666/o=University%20of%20Michigan,
c=US??sub?(cn=Babs%20Jensen)
```

Le prochain exemple est un URL de LDAP se rapportant à tous les enfants de l'entrée "c=GB" :

```
ldap://ldap.itd.umich.edu/c=GB?objectClass?one
```

L'attribut "objectClass" est demandé pour être retourné avec les entrées, et le filtre par défaut "(objectclass=*)" est utilisé.

Le prochain exemple est un URL de LDAP pour rechercher l'attribut de courrier pour l'entrée LDAP nommée "o=Question?,c=US" donné ci-dessous, illustrant l'utilisation du mécanisme d'échappement sur le caractère réservé '?'.
LDAP

```
ldap://ldap.question.com/o=Question%3f, c=US?mail
```

Le prochain exemple illustre l'interaction entre les mécanismes de mise entre guillemets LDAP et URL.

```
ldap://ldap.netscape.com/o=Babsco,c=US??(int=%5c00%5c00%5c00%5c04)
```

Le filtre dans cet exemple utilise le mécanisme d'échappement de LDAP \ pour encoder trois zéro ou octets nuls dans la valeur. Dans LDAP, le filtre serait écrit comme (int=\00\00\00\04). Puisque le caractère \ doit être échappé dans un URL, les \ sont échappés par %5c dans le codage d'URL.

L'exemple final montre l'utilisation de l'extension "bindname" pour spécifier le "dn" qu'un client devrait utiliser pour l'authentification lors de la résolution de l'URL.

```
ldap:///??sub??bindname=cn=Manager%2co=Foo
ldap:///??sub?!bindname=cn=Manager%2co=Foo
```

Les deux URL sont identiques, sauf que le second marque l'extension de "bindname" comme critique. Notez l'utilisation de la méthode encodante % pour encoder la virgule dans valeur de nom différencié l'extension de "bindname".

7. Considérations Sécuritaires

Les considérations générales de sécurité d'URL discutées dans [5] sont appropriées pour les URL de LDAP.

L'utilisation des mécanismes de sécurité lors du traitement des URL de LDAP exige un soin particulier, puisque les clients peuvent rencontrer beaucoup de serveurs différents par l'intermédiaire d'URLs, et puisque les URL sont susceptibles d'être traités automatiquement, sans interposition d'utilisateur. Un client DEVRAIT avoir une stratégie de configuration d'utilisateur spécifiant sur quels serveurs se connecter pour utiliser quels mécanismes de sécurité, et NE DEVRAIT PAS établir de connexions qui sont contradictoires avec cette stratégie.

L'envoi de l'information d'authentification, quel que soit le mécanisme, peut violer les conditions d'intimité d'un utilisateur. En l'absence de stratégie spécifique permettant l'envoi d'information d'authentification à un serveur, un client devrait utiliser une connexion anonyme. (notez que les clients conformément aux caractéristiques précédentes d'URL de LDAP, où toutes les connexions sont anonymes et non protégées, sont conformes à cette spécification ; Ils ont simplement la stratégie de sécurité par défaut).

Quelques méthodes d'authentification, en particuliers mots de passe réutilisables envoyés au serveur, peuvent révéler une information facilement abusée au serveur distant ou aux écouteurs clandestins en transit, et ne devraient pas être utilisées dans un URL de traitement à moins que ce ne soit explicitement permis par la stratégie. La confirmation par l'utilisateur humain de l'utilisation d'information d'authentification est appropriée dans beaucoup de circonstances. L'utilisation des méthodes fortes d'authentification qui ne révèlent pas d'information sensible est bien préférable.

Le format d'URL de LDAP permet la spécification d'une opération de recherche arbitraire LDAP devant être exécutée lors de l'évaluation de l'URL de LDAP. En conséquence un URL de LDAP peut causer des résultats inattendus, par exemple, la recherche de grandes quantités de données, le déclenchement d'une recherche longévitable, etc... Les implications de sécurité d'une résolution d'un URL de LDAP sont identiques à ceux d'une résolution d'une requête de recherche de LDAP.

8. Remerciements

Le format d'URL de LDAP a été initialement défini à l'université du Michigan. Cette substance est basée sur un travail supporté par le "National Science Foundation" sous le numéro d'accord NCR-9416667. Le support de l'université du Michigan et du "National Science Foundation" est avec particulièrement reconnu.

Plusieurs personnes ont fait des commentaires valables sur ce document. En particulier RL "Bob" Morgan et Mark Wahl méritent des remerciements spéciaux pour leurs contributions.

9. Références

- [1] Wahl, M., Kille, S., and T. Howes, "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names", RFC 2253, December 1997.
- [2] Wahl, M., Howes, T., and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.
- [3] Wahl, M., Coulbeck, A., Howes, T. and S. Kille, "Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions", RFC 2252, December 1997.
- [4] Howes, T., "A String Representation of LDAP Search Filters", RFC 2254, December 1997.
- [5] Berners-Lee, T., Masinter, L. and M. McCahill, "Uniform Resource Locators (URL)," RFC 1738, December 1994.
- [6] Bradner, S., "Key Words for use in RFCs to Indicate Requirement Levels," RFC 2119, March 1997.

Adresses des Auteurs

Tim Howes
Netscape Communications Corp.
501 E. Middlefield Rd.
Mountain View, CA 94043
USA

Phone: +1 415 937-3419
EMail: howes@netscape.com

Mark Smith
Netscape Communications Corp.
501 E. Middlefield Rd.
Mountain View, CA 94043
USA

Phone: +1 415 937-3477
EMail: mcs@netscape.com

Copyright intégral

Copyright © The Internet Society (1999). Tous Droits Réservés.

Le document anglais original et les traductions de celui-ci peuvent être copiés et fournis à d'autres, et les travaux dérivés qui le commente ou l'explique ou facilite son implémentation peuvent être préparés, copiés, publiés ou distribués, en totalité ou en partie, sans aucune restriction tant que les observations ci-dessus sur le copyright et ce paragraphe sont inclus dans tous ces types de copies ou de travaux dérivés. Cependant, le document anglais original lui-même ne peut être modifié de quelque façon que ce soit, comme par exemple en retirant les observations de copyright ou les références à la Internet Society ou aux autres organismes de l'Internet, excepté comme l'exige le but du développement des standards Internet où dans un tel cas les procédures pour les copyrights définis dans le processus des Standards Internet doivent être suivies, ou alors comme l'exige une traduction dans une langue autre que l'anglais.

Les autorisations limitées accordées ci-dessus sont éternelles et ne pourront être révoquées par la Internet Society, ses successeurs ou ses repreneurs.

Ce document et les informations contenues ici sont fournis de façon " TELS QUELS " et les traducteurs, la Internet Society et la Internet Engineering Task Force déclinent toute garantie, explicites ou implicites, y compris mais pas seulement toute garantie que l'utilisation des informations de ce document ne violera pas des réglementations ou des garanties implicites commerciales ou physiques pour une application particulière.

L'édition des RFC est actuellement réalisée par l'Internet Society.