

Groupe de travail Réseau
Request for Comments : 2971
Catégorie : En cours de normalisation

T. Showalter, Mirapoint, Inc.
octobre 2000
Traduction Claude Brière de L'Isle

Extension ID à IMAP4

Statut de ce mémoire

Le présent document spécifie les bonnes pratiques actuelles de l'Internet pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright

Copyright (C) The Internet Society (2000). Tous droits réservés.

Résumé

Le protocole d'extension ID à la version 4 révision 1 du protocole d'accès au message Internet (IMAP4rev1, *Internet Message Access Protocol - Version 4rev1*) permet au serveur et au client d'échanger des informations d'identification sur leur mise en œuvre afin de faire des rapports plus complets sur les bogues et les statistiques d'utilisation.

1. Introduction

Le protocole IMAP4rev1 décrit dans la [RFC2060] fournit une méthode pour accéder aux mémorisations distantes de messagerie, mais il ne fournit aucune facilité pour annoncer quel programme un client ou serveur utilise pour fournir le service. Cela rend difficile aux mises en œuvre l'obtention de rapports complets sur les bogues des utilisateurs, car il est fréquemment difficile de savoir quel client ou serveur est en service.

De plus, certains sites peuvent souhaiter rassembler des statistiques d'utilisation sur la base des clients utilisés, mais dans un environnement où il est permis aux utilisateurs d'obtenir et conserver leurs propres clients, cela est difficile à accomplir.

La commande ID fournit une facilité pour annoncer les informations sur les programmes utilisés ainsi que les informations de contact (si des bogues devaient se produire).

2. Conventions utilisées dans ce document

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMETE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC2119].

Les conventions utilisées dans le présent document sont les mêmes que celles spécifiées dans la [RFC2060]. Dans les exemples, "C:" et "S:" indiquent les lignes envoyées respectivement par le client et par le serveur. Des sauts à la ligne ont été insérés pour faciliter la lecture.

3. Spécification

Le seul objet de l'extension ID est de permettre aux clients et serveurs d'échanger des informations sur leurs mises en œuvre pour les besoins de l'analyse statistique et la détermination des problèmes.

Les informations sont à soumettre à un serveur par tout client qui souhaite fournir des informations à caractère statistique, pourvu que le serveur annonce sa volonté de prendre les informations grâce à l'atome "ID" inclus dans la liste des capacités retournée par la commande CAPABILITY.

Les mises en œuvre NE DOIVENT PAS faire des changements de fonctionnement sur la base des données envoyées au titre de la commande ou la réponse ID. La commande ID est uniquement destinée à l'utilisateur humain, et n'est pas à utiliser pour améliorer les performances des clients ou serveurs.

Cela inclut, sans s'y limiter, ce qui suit :

Les serveurs NE DOIVENT PAS tenter de réparer des bogues des clients en utilisant les informations provenant de la

commande ID. Les clients NE DOIVENT PAS tenter de réparer les bogues des serveurs sur la base de la réponse à ID.

Les serveurs NE DOIVENT PAS fournir de dispositifs à un client ou optimiser par ailleurs pour un client particulier en utilisant les informations provenant de la commande ID. Les clients NE DOIVENT PAS fournir de dispositifs à un serveur ou optimiser par ailleurs pour un serveur particulier sur la base de la réponse à ID.

Les serveurs NE DOIVENT PAS refuser l'accès ou refuser le service à un client sur la base des informations provenant de la commande ID. Les clients NE DOIVENT PAS refuser de fonctionner ou limiter leur fonctionnement avec un serveur sur la base de la réponse à ID.

Raison : il est impératif que cette extension ne supprime pas le mécanisme CAPABILITY de IMAP avec une approche circonstancielle où les mises en œuvre devineraient les caractéristiques l'une de l'autre sur la base de qui elles prétendent être.

Les mises en œuvre NE DOIVENT PAS envoyer de fausses informations dans une commande ID.

Les mises en œuvre PEUVENT envoyer moins d'informations que ce qu'elles ont de disponible ou pas d'informations du tout. Un tel comportement peut être utile pour préserver la confidentialité de l'utilisateur. Voir les considérations pour la sécurité à la section 7.

3.1 Commande ID

Arguments : liste des paramètres du client ou NIL

Réponses : réponse FACULTATIVE non étiquetée : ID

Résultat : OK : informations d'identification acceptées
BAD : commande inconnue ou arguments invalides

Les informations d'identification de la mise en œuvre sont envoyées par le client avec la commande ID.

Cette commande est valide dans tous les états.

Les informations envoyées sont sous la forme d'une liste de paires champ/valeur. Les champs peuvent être toute chaîne IMAP4, et les valeurs peuvent être toute chaîne IMAP4 ou NIL. Une valeur de NIL indique que le client ne peut ou ne veut pas spécifier ces informations. Le client peut aussi envoyer NIL au lieu de la liste, indiquant qu'il veut n'envoyer aucune information, mais accepterait quand même une réponse du serveur.

Les champs disponibles sont définis au paragraphe 3.3.

Exemple :

```
C: a023 ID ("nom" "sodr" "version" "19.34" "vendeur" "Pink Floyd Music Limited")
S: * ID NIL
S: a023 OK ID terminé
```

3.2 Réponses à la commande ID

Contenu : liste des paramètres du serveur

En réponse à une commande ID produite par le client, le serveur répond avec une réponse étiquetée contenant les informations sur sa mise en œuvre. Le format est le même que celui de la liste du client.

Exemple :

```
C: a042 ID NIL
S: * ID ("nom" "Cyrus" "version" "1.5" "os" "sunos" "os-version" "5.5" "support-url" "mailto:cyrus-
bugs@andrew.cmu.fr")
S: a042 OK ID commande terminée
```

Un serveur DOIT envoyer une réponse ID étiquetée à une commande ID. Cependant, un serveur PEUT envoyer NIL à la place de la liste.

3.3 Valeurs de champ définies

Toute chaîne peut être envoyée comme un champ, mais ce qui suit est défini pour décrire certaines valeurs qui pourraient être envoyées. Les mises en œuvre ont toute liberté pour n'en envoyer aucune, ou pour les envoyer toutes. Les chaînes sont insensibles à la casse. Les chaînes de champ NE DOIVENT PAS faire plus de 30 octets. Les chaînes de valeur NE DOIVENT PAS faire plus de 1024 octets. Les mises en œuvre NE DOIVENT PAS envoyer plus de 30 paires champ-valeur.

nom : nom du programme

version : numéro de version du programme

os ; nom du système d'exploitation

os-version : version du système d'exploitation

vendeur : vendeur du client/serveur

support-url : URL à contacter pour l'assistance

adresse : adresse postale du contact/vendeur

date : date de réalisation du programme, spécifiée comme date-time dans IMAP4rev1

commande : commande utilisée pour lancer le programme

arguments : arguments fournis sur la ligne de commande, s'il en est

environnement : description de l'environnement, c'est-à-dire, variables de l'environnement UNIX ou réglages de registres Windows

Les mises en œuvre NE DOIVENT PAS utiliser les informations de contact pour soumettre des rapports automatiques d'erreurs. Les mise en œuvre peuvent inclure des informations d'une réponse d'ID dans un rapport préparé automatiquement, mais il leur est interdit d'envoyer le rapport sans l'autorisation de l'utilisateur.

Il est préférable de trouver le nom et la version du système d'exploitation sous-jacent au moment du démarrage dans les cas où cela est possible.

Les informations envoyées via une réponse à ID peuvent violer la confidentialité de l'utilisateur. Voir les considérations pour la sécurité à la section 7.

Les mises en œuvre NE DOIVENT PAS envoyer le même nom de champ plus d'une fois.

4. Syntaxe formelle

Cette syntaxe est destinée à augmenter la grammaire spécifiée dans la [RFC2060] afin de traiter la commande ID. Cette spécification utilise la notation de forme Backus-Naur augmenté (ABNF) telle qu'utilisée dans la [RFC2060].

```
command_any ::= "CAPABILITY" / "LOGOUT" / "NOOP" / x_command / id
                ;; ajoute la commande id à command_any dans la [RFC2060]
```

```
id ::= "ID" SPACE id_params_list
```

```
id_response ::= "ID" SPACE id_params_list
```

```
id_params_list ::= "(" #(string SPACE nstring) ")" / nil      ;; liste de paires champ valeur
```

```
response_data ::= "*" SPACE (resp_cond_state / resp_cond_bye / mailbox_data / message_data / capability_data /
                             id_response)
```

5. Utilisation de l'extension ID avec des pare-feu et autres intermédiaires

Il existe des mandataires, des pare-feu, et d'autres systèmes intermédiaires qui peuvent intercepter une session IMAP et apporter des changements aux données échangées dans la session. De tels intermédiaires ne sont pas anticipés par la conception du protocole IMAP4 et ne sont pas couverts par la norme IMAP4. Cependant, afin que la commande ID soit utile en présence de tels intermédiaires, ceux-ci ont besoin de tenir un compte particulier de la commande et de la réponse ID. En particulier, si un intermédiaire change une partie quelconque de la session IMAP, il doit aussi changer la commande ID pour annoncer sa présence.

Un pare-feu PEUT agir pour bloquer la transmission de champs d'informations spécifiques dans la commande et réponse ID dont il pense qu'ils révèlent des informations qui pourraient exposer à une faiblesse de la sécurité. Cependant, un pare-feu NE DEVRAIT PAS désactiver entièrement l'extension, lorsque présenté, et NE DEVRAIT PAS retirer inconditionnellement la liste de clients ou de serveurs.

Finalement, on devrait noter qu'un pare-feu, lorsque il traite une réponse CAPABILITY, NE DOIT PAS permettre que le nom des extensions dont le pare-feu n'a aucune connaissance soit retourné au client.

6. Références

- [RFC0822] D. Crocker, "Norme pour le [format des messages de texte](#) de l'ARPA-Internet", STD 11, août 1982. (*Obsolète, remplacée par la RFC5322*)
- [RFC2060] M. Crispin, "Protocole d'[accès au message Internet](#) - version 4rev1", décembre 1996. (*Obsolète, voir RFC3501*) (P.S.)
- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

7. Considérations pour la sécurité

Cette extension présente un danger de violation de la confidentialité des usagers si il en est fait un mauvais usage. Les clients et serveurs devraient notifier aux usagers qu'ils mettent en œuvre et activent la commande ID.

Il est très souhaitable que les mises en œuvre fournissent une méthode pour désactiver la prise en charge de ID, peut-être en n'envoyant pas du tout ID, ou en envoyant NIL comme argument à la commande ou réponse ID.

Les mises en œuvre doivent porter une extrême attention à l'ajout de champs envoyés au titre d'une commande ou réponse ID. Certains champs, incluant un numéro d'identifiant de processeur, une adresse Ethernet, ou autre identifiant unique (ou presque unique) permettent de retracer l'activité des usagers d'une façon qui viole leurs attentes de confidentialité.

Posséder les informations de mise en œuvre d'un client ou serveur particulier peut rendre plus facile à un attaquant d'obtenir un accès non autorisé par des failles dans la sécurité.

Comme cette commande inclut des données arbitraires et n'exige pas que l'utilisateur s'authentifie, les mises en œuvre de serveur sont averties de se garder contre l'envoi par un attaquant de données à mettre au rebut dans le but de remplir le journal d'événement de ID. En particulier, si un serveur enregistre naïvement chaque commande ID sur le disque sans l'inspecter, un attaquant peut simplement établir des milliers de connexions et envoyer quelques kilo octets de données aléatoires. Les serveurs doivent se garder contre cela. Les méthodes incluent de tronquer les réponses anormalement longues ; de colliger les réponses en ne mémorisant qu'une seule copie, puis en tenant un compteur du nombre de fois que la réponse a été vue ; de ne garder que les parties particulièrement intéressantes des réponses ; et de n'enregistrer les réponses que des usagers réellement connectés.

La sécurité est affectée par les pare-feu qui modifient le flux de protocole IMAP ; voir la section 5, "Utilisation de l'extension ID avec des pare-feu et autres intermédiaires", pour plus d'informations.

8. Adresse de l'auteur

Tim Showalter
Mirapoint, Inc.
909 Hermosa Ct.
Sunnyvale, CA 94095
USA
mél : tjs@mirapoint.com

9. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2000). Tous droits réservés.

Ce document et les traductions de celui-ci peuvent être copiés et diffusés, et les travaux dérivés qui commentent ou expliquent autrement ou aident à sa mise en œuvre peuvent être préparés, copiés, publiés et distribués, partiellement ou en totalité, sans restriction d'aucune sorte, à condition que l'avis de copyright ci-dessus et ce paragraphe soit inclus sur toutes ces copies et œuvres dérivées. Toutefois, ce document lui-même ne peut être modifié en aucune façon, par exemple en supprimant le droit d'auteur ou les références à l'Internet Society ou d'autres organisations Internet, sauf si c'est nécessaire à l'élaboration des normes Internet, auquel cas les procédures pour les droits de reproduction définis dans les processus des normes pour l'Internet doivent être suivies, ou si nécessaire pour le traduire dans des langues autres que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Société Internet, ses successeurs ou ayants droit.

Ce document et les renseignements qu'il contient sont fournis "TELS QUELS" et l'INTERNET SOCIETY et l'INTERNET ENGINEERING TASK FORCE déclinent toute garantie, expresse ou implicite, y compris mais sans s'y limiter, toute garantie que l'utilisation de l'information ici présente n'enfreindra aucun droit ou aucune garantie implicite de commercialisation ou d'adaptation à un objet particulier.

Remerciement

Le financement de la fonction d'éditeur des RFC est actuellement fourni par la Internet Society.