Groupe de travail Réseau
Request for Comments : 2384
Catégorie : En cours de normalisation

R. Gellens, QUALCOMM Incorporated
août 1998
Traduction Claude Brière de L'Isle

Schéma d'URL POP

1. Introduction

La [RFC1939] présente un protocole d'accès de messagerie largement déployé. De nombreux programmes accèdent aux mémorisations de message de POP3, et ont donc besoin des informations de configuration de POP3. Comme il y a plusieurs éléments de configuration qui sont exigés afin d'accéder à une boîte aux lettres, il est pratique d'avoir une seule représentation de chaîne.

Une boîte aux lettres POP3 (comme une boîte aux lettres de la [RFC2060]) est une ressource du réseau, et les URL sont une représentation généralisée des ressources du réseau qui est largement utilisée.

Un moyen de spécifier une boîte aux lettres POP3 comme un URL sera vraisemblablement utile dans de nombreux programmes et protocoles. La [RFC2244] est un cas dans lequel est nécessaire une encapsulation des éléments requis pour l'accès aux services du réseau. Par exemple, une mémorisation de message de la [RFC2060] est normalement spécifiée dans les ensembles de données du protocole ACAP comme relevant de la [RFC2192].

Le présent mémoire définit un schéma d'URL pour référencer une boîte aux lettres POP.

2. Conventions utilisées dans le document

Les mots clés "DOIT", "NE DOIT PAS", "DEVRAIT", "NE DEVRAIT PAS", et "PEUT" dans le présent document sont à interpréter comme défini dans "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence" [RFC2119].

3. Schéma POP

Le schéma d'URL POP désigne un serveur POP, et facultativement un numéro d'accès, un mécanisme d'authentification, un identifiant d'authentification, et/ou un identifiant d'autorisation.

L'URL POP suit la syntaxe commune de schéma Internet telle que définie dans la [RFC1738] sauf que les mots de passe en texte clair ne sont pas permis. Si :<accès> est omis, l'accès par défaut est 110.

L'URL POP est décrit à la Section 8 en utilisant l'ABNF de la [RFC2234].

Un URL POP est de la forme générale :

pop://<usager>;auth=<auth>@<hôte>:<accès>

Où <usager>, <hôte>, et <accès> sont comme défini dans la [RFC1738], et certains des éléments, ou tous, sauf "pop://" et <hôte>, peuvent être omis.

4. Nom d'usager POP et mécanisme d'authentification

On peut fournir une autorisation (à quelle boîte aux lettres accéder) et une identité (qu'on appellera "nom d'utilisateur" pour simplifier) d'authentification (à quel mot de passe appliquer la vérification) et/ou un nom de mécanisme d'authentification. Ils sont utilisés dans une commande "USER", "APOP", "AUTH" de la [RFC1734], ou dans une commande d'extension qui établit la connexion avec le serveur POP. Si l'URL ne fournit pas d'identifiant d'authentification, le programme qui interprète l'URL POP DEVRAIT en demander un à l'usager.

Un mécanisme d'authentification peut être exprimé en ajoutant ";AUTH=<enc- auth-type>" à la fin du nom d'utilisateur. Si le nom du mécanisme d'authentification n'est pas précédé d'un "+", c'est un mécanisme POP SASL de la [RFC2222]. Si il est précédé d'un "+", c'est soit un mécanisme "APOP", soit un mécanisme d'extension.

Lorsque un <enc-auth-type> est spécifié, le client DEVRAIT demander des accréditifs appropriés à ce mécanisme et utiliser la commande "AUTH", "APOP", ou la commande d'extension au lieu de la commande "USER". Si aucun nom d'utilisateur n'est spécifié, il DEVRAIT en être obtenu un du mécanisme, ou il DEVRAIT en être demandé un à l'usager, selon le cas approprié.

La chaîne ";AUTH=*" indique que le client DEVRAIT choisir un mécanisme d'authentification approprié. Il PEUT utiliser tout mécanisme pris en charge par le serveur POP.

Si un <enc-auth-type> autre que ";AUTH=*" est spécifié, le client NE DEVRAIT PAS utiliser un mécanisme différent sans la permission explicite de l'usager.

Si un nom d'utilisateur est inclus sans aucun mécanisme d'authentification, ";AUTH=*" est alors supposé.

Comme des URL peuvent facilement venir de sources qui ne sont pas de confiance, il faut faire attention quand on résout un URL qui exige ou demande n'importe quelle sorte d'authentification. Si les accréditifs d'authentification sont fournis par le mauvais serveur, cela peut compromettre la sécurité du compte de l'usager. Le programme qui résout l'URL devrait s'assurer dans ce cas qu'il satisfait au moins un des critères suivants :

(1) L'URL vient d'une source de confiance, telle qu'un serveur de référence que le client a validé et auquel il accorde sa confiance conformément à la politique du site. Noter que l'entrée de l'URL par l'usager peut compter ou non comme source de confiance, selon le niveau d'expérience de l'usager et la politique du site.

(2) Une politique locale explicite du site permet au client de se connecter au serveur dans l'URL. Par exemple, si le client connaît le nom de domaine du site, la politique du site impose que tout nom d'hôte se terminant dans ce domaine soit de confiance.

(3) L'usager confirme que la connexion à ce nom de domaine avec les accréditifs et/ou mécanismes spécifiés est permise.

(4) Un mécanisme est utilisé pour valider le serveur avant de passer des accréditifs de client potentiellement compromettants.

(5) Un mécanisme d'authentification est utilisé qui ne révèle pas au serveur d'informations qui pourraient être utilisées pour compromettre de futures connexions.

Un URL contenant ";AUTH=*" devrait être traité avec une attention supplémentaire car il peut retomber sur un mécanisme de sécurité plus faible. En fait, il est déconseillé aux clients d'utiliser un mot de passe en clair comme réponse par défaut avec ";AUTH=*" à moins que la connexion n'ait un chiffrement fort (par exemple une clé d'une longueur supérieure à 56 bits).

Noter que si des caractères non sûrs ou réservés comme " " ou ";" sont présents dans le nom d'utilisateur ou le mécanisme d'authentification, ils DOIVENT être codés comme décrit dans la [RFC1738].

5. URL POP relatifs

Les URL POP relatifs ne sont pas permis.

6. Considérations d'internationalisation

Comme les caractères à 8 bits ne sont pas permis dans les URL, les caractères de la [RFC2279] sont codés comme exigé par la spécification des URL [RFC1738].

7. Exemples

Les exemples suivants démontrent comment un programme client POP peut traduire divers URL POP en une série de commandes POP. Les commandes envoyées du client au serveur sont précédées de "C:", et les réponses envoyées du serveur au client sont précédées de "S:".

L'URL <pop://rg@mailsrv.qualcomm.com> résulte en les commandes client suivantes :

```
<request password from user>
<connect to mailsrv.qualcomm.com, port 110>
S: +OK POP3 server ready <1896.697170952@mailsrv.qualcomm.com>
C: USER rg
S: +OK
C: PASS secret
S: +OK rg's mailbox has 2 messages (320 octets)
```

L'URL <pop://rg;AUTH=+APOP@mail.eudora.com:8110> résulte en les commandes client suivantes :

```
<client requests password from user>
<connect to mail.eudora.com, port 8110>
S: +OK POP3 server ready <1896.697170952@mail.eudora.com>
C: APOP rg c4c9334bac560ecc979e58001b3e22fb
S: +OK mailbox has 1 message (369 octets)
```

L'URL <pop://baz;AUTH=SCRAM-MD5@foo.bar> résulte en les commandes client suivantes :

```
<connect to foo.bar, port 110>
S: +OK POP3 server ready <1896.697170952@foo.bar>
C: AUTH SCRAM-
    MD5AGNocmlzADx0NG40UGFiOUhCMEFtL1FMWEI3MmVnQGVsZWFub3IuaW5ub3NvZnQuY29tPg==
S: + dGVzdHNhbHQBAAAAaW1hcEBlbGVhbm9yLmlubm9zb2Z0LmNvbQBq
    aGNOWmxSdVBiemlGcCt2TFYrTkN3
C: AQAAAMg9jU8CeB4KOfk7sUhSQPs=
S: + U0odqYw3B7XIIW0oSz65OQ==
C:
S: +OK mailbox has 1 message (369 octets)
```

8. ABNF pour le schéma d'URL POP

Le schéma d'URL POP est décrit en utilisant la [RFC2234] :

```
achar          = uchar / "&" / "=" / "~"          ; voir la définition de "uchar" dans la [RFC1738]
auth           = ";AUTH=" ( "*" / enc-auth-type )
enc-auth-type  = enc-sasl / enc-ext
enc-ext        = "+" ("APOP" / 1*achar)           ; APOP ou nom codé de mécanisme d'extension
enc-sasl       = 1*achar                          ; version codée de "auth_type" de la [RFC2222]
enc-user       = 1*achar                          ; version codée de la boîte aux lettres de la [RFC1939]
pop-url        = "pop://" server
server         = [user-auth "@"] hostport         ; voir la définition de "hostport" dans la [RFC1738]
user-auth      = enc-user [auth]
```

9. Considérations pour la sécurité

Les considérations pour la sécurité exposées dans les [RFC1939] et [RFC1738] sont pertinentes pour celle-ci. Les considérations pour la sécurité qui se rapportent à l'authentification des URL sont exposées à la section 4 du présent document.

De nombreux clients de messagerie électronique mémorisent le mot de passe en clair pour une utilisation ultérieure après s'être connecté à un serveur POP. De tels clients NE DOIVENT PAS utiliser un mot de passe mémorisé en réponse à un URL POP sans permission explicite de la part de l'usager de fournir ce mot de passe au nom d'hôte spécifié.

10. Remerciements

Le présent document a fait beaucoup d'emprunts à la spécification de Chris Newman [RFC2192] et s'est efforcé de suivre les conseils de la [RFC2718].

11. Références

[RFC1734] J. Myers, "Commande POP3 AUTHentification", décembre 1994. *(P.S., remplacée par la RFC5034)*

[RFC1738] T. Berners-Lee et autres, "Localisateurs uniformes de ressource (URL)", décembre 1994. *(P.S),(Obsolète, voir les RFC4248 et 4266)*

[RFC1939] J. Myers, M. Rose, "Protocole Post Office - version 3", mai 1996. (*MàJ par* RFC1957, RFC2449) (STD0053)

[RFC2060] M. Crispin, "Protocole d'accès au message Internet - version 4rev1", décembre 1996. *(Remplace* RFC1730) (*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.

[RFC2192] C. Newman, "Schéma d'URL IMAP", septembre 1997. (*Obsolète, voir* RFC5092) *(P.S.)*

[RFC2222] J. Myers, "Authentification simple et couche de sécurité (SASL)", octobre 1997. *(P.S.)* (*MàJ par* RFC2444) (*Obsolète, voir* RFC4422, RFC4752)

[RFC2234] D. Crocker et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", novembre 1997. (*Obsolète, voir* RFC5234)

[RFC2244] C. Newman, J. G. Myers, "ACAP – Protocole d'accès à la configuration d'application", novembre 1997. *(P.S.)*

[RFC2279] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", janvier 1998. (*Obsolète, voir* RFC3629) *(D.S.)*

[RFC2718] L. Masinter, H. Alvestrand, D. Zigmond et R. Petke, "Lignes directrices pour les nouveaux schémas d'URL", novembre 1999. (*Obsolète, voir* RFC4395) *(Information)*

12. Adresse de l'auteur

Randall Gellens
QUALCOMM Incorporated
6455 Lusk Blvd.
San Diego, CA 92121-2779
U.S.A.
téléphone : +1 619 651 5115
fax : +1 619 651 5334
mél : Randy@Qualcomm.com

13. Déclaration complète de droits de reproduction