

IMAP4 Login Referrals

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1997). All Rights Reserved.

1. Abstract

When dealing with large amounts of users and many IMAP4 [RFC-2060] servers, it is often necessary to move users from one IMAP4 server to another. For example, hardware failures or organizational changes may dictate such a move.

Login referrals allow clients to transparently connect to an alternate IMAP4 server, if their home IMAP4 server has changed.

A referral mechanism can provide efficiencies over the alternative 'proxy method', in which the local IMAP4 server contacts the remote server on behalf of the client, and then transfers the data from the remote server to itself, and then on to the client. The referral mechanism's direct client connection to the remote server is often a more efficient use of bandwidth, and does not require the local server to impersonate the client when authenticating to the remote server.

2. Conventions used in this document

In examples, "C:" and "S:" indicate lines sent by the client and server respectively.

A home server, is an IMAP4 server that contains the user's inbox.

A remote server is a server that contains remote mailboxes.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC-2119].

3. Introduction and Overview

IMAP4 servers that support this extension MUST list the keyword LOGIN-REFERRALS in their CAPABILITY response. No client action is needed to invoke the LOGIN-REFERRALS capability in a server.

A LOGIN-REFERRALS capable IMAP4 server SHOULD NOT return a referral to a server that will return a referral. A client MUST NOT follow more than 10 levels of referral without consulting the user.

A LOGIN-REFERRALS response code MUST contain as an argument a valid IMAP server URL as defined in [IMAP-URL].

A home server referral consists of either a tagged NO or OK, or an untagged BYE response that contains a LOGIN-REFERRALS response code.

Example: A001 NO [REFERRAL IMAP://user;AUTH=*@SERVER2/] Remote Server

NOTE: user;AUTH=* is specified as required by [IMAP-URL] to avoid a client falling back to anonymous login.

4. Home Server Referrals

A home server referral may be returned in response to an AUTHENTICATE or LOGIN command, or it may appear in the connection startup banner. If a server returns a home server referral in a tagged NO response, that server does not contain any mailboxes that are accessible to the user. If a server returns a home server referral in a tagged OK response, it indicates that the user's personal mailboxes are elsewhere, but the server contains public mailboxes which are readable by the user. After receiving a home server referral, the client can not make any assumptions as to whether this was a permanent or temporary move of the user.

4.1. LOGIN and AUTHENTICATE Referrals

An IMAP4 server MAY respond to a LOGIN or AUTHENTICATE command with a home server referral if it wishes to direct the user to another IMAP4 server.

Example: C: A001 LOGIN MIKE PASSWORD
S: A001 NO [REFERRAL IMAP://MIKE@SERVER2/] Specified user
is invalid on this server. Try SERVER2.

Example: C: A001 LOGIN MATTHEW PASSWORD
S: A001 OK [REFERRAL IMAP://MATTHEW@SERVER2/] Specified user's personal mailboxes located on Server2, but public mailboxes are available.

Example: C: A001 AUTHENTICATE GSSAPI
<authentication exchange>
S: A001 NO [REFERRAL IMAP://user;AUTH=GSSAPI@SERVER2/] Specified user is invalid on this server. Try SERVER2.

4.2. BYE at connection startup referral

An IMAP4 server MAY respond with an untagged BYE and a REFERRAL response code that contains an IMAP URL to a home server if it is not willing to accept connections and wishes to direct the client to another IMAP4 server.

Example: S: * BYE [REFERRAL IMAP://user;AUTH=*@SERVER2/] Server not accepting connections. Try SERVER2

5. Formal Syntax

The following syntax specification uses the augmented Backus-Naur Form (BNF) as described in [ABNF].

This amends the "resp_text_code" element of the IMAP4 grammar described in [RFC-2060]

```
resp_text_code =/ "REFERRAL" SPACE <imapurl>  
; See [IMAP-URL] for definition of <imapurl>  
; See [RFC-2060] for base definition of resp_text_code
```

6. Security Considerations

The IMAP4 login referral mechanism makes use of IMAP URLs, and as such, have the same security considerations as general internet URLs [RFC-1738], and in particular IMAP URLs [IMAP-URL].

A server MUST NOT give a login referral if authentication for that user fails. This is to avoid revealing information about the user's account to an unauthorized user.

With the LOGIN-REFERRALS capability, it is potentially easier to write a rogue 'password catching' server that collects login data and then refers the client to their actual IMAP4 server. Although referrals reduce the effort to write such a server, the referral response makes detection of the intrusion easier.

7. References

[RFC-2060], Crispin, M., "Internet Message Access Protocol - Version 4rev1", RFC 2060, December 1996.

[IMAP-URL], Newman, C., "IMAP URL Scheme", RFC 2192, Innosoft, September 1997.

[RFC-1738], Berners-Lee, T., Masinter, L. and M. McCahill, "Uniform Resource Locators (URL)", RFC 1738, December 1994.

[RFC-2119], Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[ABNF], DRUMS working group, Dave Crocker Editor, "Augmented BNF for Syntax Specifications: ABNF", Work in Progress.

8. Acknowledgments

Many valuable suggestions were received from private discussions and the IMAP4 mailing list. In particular, Raymond Cheng, Mark Crispin, Mark Keasling Chris Newman and Larry Osterman made significant contributions to this document.

9. Author's Address

Mike Gahrns
Microsoft
One Microsoft Way
Redmond, WA, 98072

Phone: (206) 936-9833
EMail: mikega@microsoft.com

10. Full Copyright Statement

Copyright (C) The Internet Society (1997). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."