Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 24, 2014

C. Newman
Oracle

October 21, 2013

IMAP UNAUTHENTICATE for Connection Reuse
draft-newman-imap-unauth-00.txt

Abstract

This specification extends the Internet Message Access Protocol (IMAP) to allow an administrative client to reuse the same IMAP connection on behalf of multiple IMAP user identities.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 24, 2014.

Table of Contents

1. Introduction

Modern IMAP [RFC3501] server deployments often have peer systems with administrative privilege that perform actions on behalf of IMAP end-users. For example, a voice mail gateway can use IMAP to store a user's voicemail and mark that voicemail as \Seen when the user listens to it via the phone interface. These systems can issue the IMAP AUTHENTICATE command with administrative credentials to act on behalf of other users. However, with the IMAP base specification, these specialized IMAP clients must close the connection and create a new connection for each user. For efficiency reasons, it is desirable for these clients to reuse the same connection, particularly if SSL has been negotiated. This specification proposes the UNAUTHENTICATE command to achieve this goal.

The IMAP state machine described in section 3 of RFC 3501 does not have a transition from authenticated or selected state to not authenticated state. The UNAUTHENTICATE command adds a transition from authenticated or selected state to not authenticated state.

2. Conventions Used in This Document

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 [RFC2119].

3. UNAUTHENTICATE Command

Arguments: None

Responses: no specific response for this command

Result: OK - completed, now in not authenticated state
BAD - command unknown or arguments invalid

This command directs the server to reset all connection state, except for state at the TLS [RFC5465] layer. Upon completion, the server connection is placed in not authenticated state. This represents transition 7 in the State Machine Diagram (Section 5).

If a mailbox was selected, the mailbox ceases to be selected but no expunge event is generated. If a SASL [RFC4422] security layer was active, it terminates immediately after the server sends the CRLF following the OK response. For the client, it terminates immediately after the CRLF following the UNAUTHENTICATE command.

After sending this command, the client is free to issue a new AUTHENTICATE or LOGIN command as permitted based on the server's capabilities. If no SASL security layer was active, the client is permitted to pipeline the UNAUTHENTICATE command with a subsequent AUTHENTICATE command. If the IMAP server also advertises SASL-IR [RFC4959], this permits an administrative client to re-authenticate in one round trip. Because of this pipelining optimization, a server advertising UNAUTHENTICATE is not permitted to respond to the UNAUTHENTICATE command with a NO response if it is unable to reset state associated with the connection. Servers MAY close the connection with an untagged BYE response if this preferably rare situation occurs.

The IMAP ID [RFC2971] command provides properties about the client primarily for use in server log or audit files. Because IMAP ID is not related to application authentication or user identity in any way and caching it for the duration of the client connection can be useful, the interaction between IMAP ID and the UNAUTHENTICATE command is implementation defined. For example, a compliant server MAY discard cached IMAP ID information in response to an UNAUTHENTICATE command.

4. Interactions

This section describes interactions between this extension and other IMAP extensions or usage models.

4.1. Stateful Extensions

This lists some IMAP extensions that have connection state that MUST be reset if both the specified extension is advertised and the UNAUTHENTICATE command is advertised and used. This list may not be complete; the requirement to reset connection state applies to all current and future extensions except STARTTLS and ID.

- Cached identity information, such a group memberships, that are used to evaluate access control lists [RFC4314] MUST be reset.

- CONDSTORE servers [RFC4551] MUST behave as if no CONDSTORE enabling command had been issued after an UNAUTHENTICATE command is issued.

- If IMAP COMPRESS [RFC4978] is active, the compression layer terminates after the server sends the CRLF following the OK response and after the client sends the CRLF following the UNAUTHENTICATE command. In the event it matters, the compression layer terminates before a SASL layer terminates.

- Any extensions enabled by the IMAP ENABLE [RFC5161] command cease to be enabled when the UNAUTHENTICATE command is issued. This includes, but is not limited to, CONDSTORE [RFC4551], QRESYNC [RFC5162], METADATA [RFC5464], METADATA-SERVER [RFC5464] and UTF8=ACCEPT [RFC6855].

- A server advertising SEARCHRES [RFC5182] discards any saved search results so that '$' subsequently represents the empty set.

- A server advertising LANGUAGE [RFC5255] will revert to the "i-default" language.

- When a server advertises CONTEXT=SEARCH or CONTEXT=SORT [RFC5267], the UNAUTHENTICATE command includes an implicit CANCELUPDATE for all server contexts.

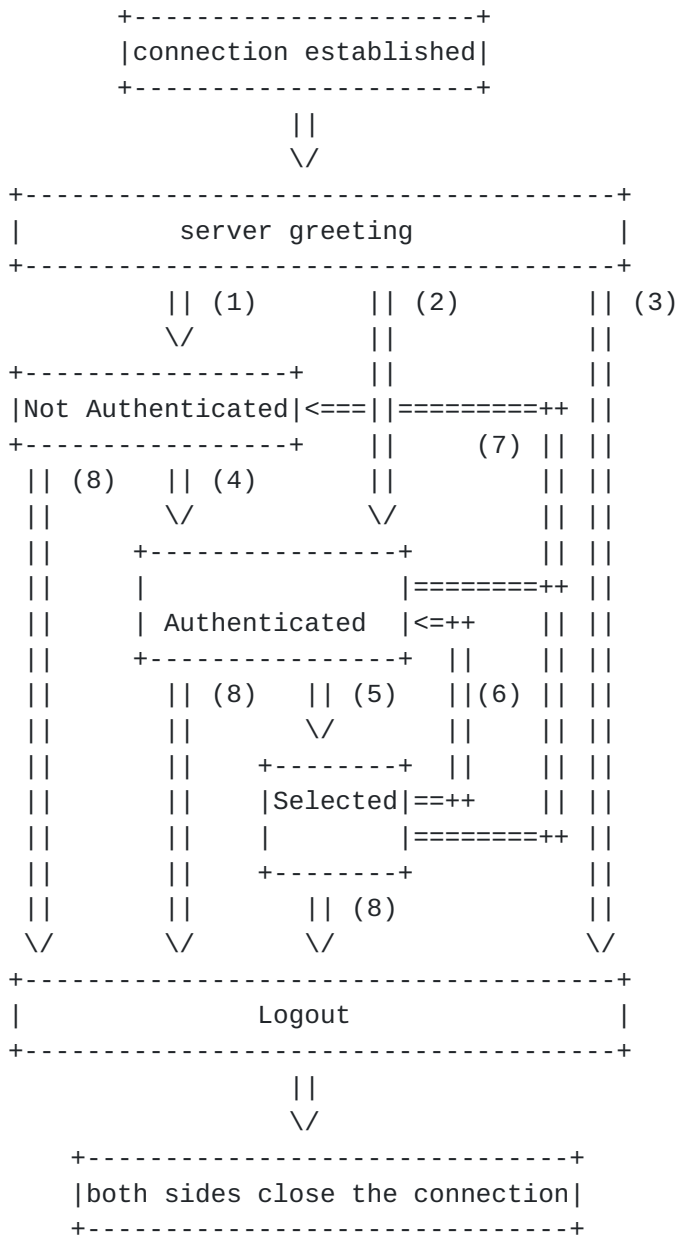
- When a server advertises NOTIFY [RFC5465], the UNAUTHENTICATE command cancels server state related to the NOTIFY command and reverts to default IMAP base-specification behavior for notifications.

4.2. Client Certificates, SASL EXTERNAL and imaps

When a TLS [RFC5246] security layer is negotiated either via the STARTTLS command or use of the imaps port [RFC6186], IMAP servers MAY be configured to request a client certificate and IMAP clients MAY provide one. Client credentials at the TLS layer do not normally impact the application layer without use of the SASL EXTERNAL mechanism [RFC4422] in an IMAP AUTHENTICATE command that directs to the server to use the provided client certificate to authenticate as the specified IMAP user. The UNAUTHENTICATE command breaks any application-level binding of the TLS client credentials but does not discard the client credentials. As a result, an administrative client may use a client certificate with administrative privilege to act on behalf of multiple IMAP users in the same connection via the EXTERNAL mechanism and the UNAUTHENTICATE command.

Some server implementations using the imaps port will request and use a TLS client certificate to authenticate immediately as the default IMAP identity associated with that certificate. These implementations indicate this behavior by using the PREAUTH greeting as indicated by transition 2 in the State Machine Diagram (Section 5). As a result, TLS client certificates can not be used for administrative authentication with the imaps port unless the UNAUTHENTICATE command is also advertised. In that case, an administrative client can respond to the PREAUTH greeting with an UNAUTHENTICATE command and then issue an AUTHENTICATE EXTERNAL command.

5. Revised State Machine



Revised IMAP state machine transitions:

1. connection without pre-authentication (OK greeting)

2. pre-authenticated connection (PREAUTH greeting)

3. rejected connection (BYE greeting)

4. successful LOGIN or AUTHENTICATE command

5. successful SELECT or EXAMINE command

6. CLOSE, UNSELECT [RFC3691] or failed SELECT or EXAMINE command

7. UNAUTHENTICATE command

8. LOGOUT command, server shutdown, or connection closed

6. Formal Syntax

The following syntax specification uses the Augmented Backus-Naur Form (ABNF) as described in [RFC5234]. Amended terms are defined in [RFC3501].

```
capability     =/ "UNAUTHENTICATE"

command-auth   =/ "UNAUTHENTICATE"

command-select =/ "UNAUTHENTICATE"
```

7. IANA Considerations

The IANA shall add the UNAUTHENTICATE capability to the IMAP4 Capabilities Registry.

8. Security Considerations

The original IMAP state machine was designed to allow a server implementation approach where each IMAP authentication identity matches an operating system identity and the server revokes all administrative privilege onces authentication completes. This extension is not compatible with that implementation approach. However, that approach has significant performance costs on Unix systems, and this extension is designed for environments where efficiency is a relatively high priority deployment goal. So this extension is appropriate for some deployments but may not be appropriate for the most security sensitive environments.

IMAP server implementations are complicated and can retain a lot of state related to an authenticated user. Server implementers need to take care to reset all server state such that authentication as a subsequent user does not inherit any data or privileges from the previous user. State data associated with a user can include cached identity information such as group membership used to evaluate access control lists [RFC4314], active notifications [RFC5465], access to

per-user data such as flags, etc.

IMAP server systems are often deployed in a two-tier model where a server-side IMAP proxy routes to an IMAP back-end which handles all connections for a subset of possible users. Some IMAP proxies enter a pass-through mode after authentication. The UNAUTHENTICATE command, if enabled, would allow a client to bypass any security restrictions present in the proxy layer but not in the back-end server layer on a subsequent authentication. As a result, IMAP server implementations of this extension MUST provide a way to disable it when it is not needed. Use of an IMAP proxy that processes the UNAUTHENTICATE command at the proxy layer eliminates this concern.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, March 2003.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

9.2. Informative References

[RFC2971] Showalter, T., "IMAP4 ID extension", RFC 2971, October 2000.

[RFC3691] Melnikov, A., "Internet Message Access Protocol (IMAP) UNSELECT command", RFC 3691, February 2004.

[RFC4422] Melnikov, A. and K. Zeilenga, "Simple Authentication and Security Layer (SASL)", RFC 4422, June 2006.

[RFC4314] Melnikov, A., "IMAP4 Access Control List (ACL) Extension", RFC 4314, December 2005.

[RFC4551] Melnikov, A. and S. Hole, "IMAP Extension for Conditional STORE Operation or Quick Flag Changes Resynchronization", RFC 4551, June 2006.

[RFC4959] Siemborski, R. and A. Gulbrandsen, "IMAP Extension for Simple Authentication and Security Layer (SASL) Initial

Client Response", RFC 4959, September 2007.

[RFC4978] Gulbrandsen, A., "The IMAP COMPRESS Extension", RFC 4978, August 2007.

[RFC5161] Gulbrandsen, A. and A. Melnikov, "The IMAP ENABLE Extension", RFC 5161, March 2008.

[RFC5162] Melnikov, A., Cridland, D., and C. Wilson, "IMAP4 Extensions for Quick Mailbox Resynchronization", RFC 5162, March 2008.

[RFC5182] Melnikov, A., "IMAP Extension for Referencing the Last SEARCH Result", RFC 5182, March 2008.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5255] Newman, C., Gulbrandsen, A., and A. Melnikov, "Internet Message Access Protocol Internationalization", RFC 5255, June 2008.

[RFC5267] Cridland, D. and C. King, "Contexts for IMAP4", RFC 5267, July 2008.

[RFC5464] Daboo, C., "The IMAP METADATA Extension", RFC 5464, February 2009.

[RFC5465] Gulbrandsen, A., King, C., and A. Melnikov, "The IMAP NOTIFY Extension", RFC 5465, February 2009.

[RFC6186] Daboo, C., "Use of SRV Records for Locating Email Submission/Access Services", RFC 6186, March 2011.

[RFC6855] Resnick, P., Newman, C., and S. Shen, "IMAP Support for UTF-8", RFC 6855, March 2013.

Appendix A. Design Considerations

The author deliberately choose to add a separate UNAUTHENTICATE command instead of allowing the LOGIN or AUTHENTICATE commands to be issued when the connection is in a state other than unauthenticated state. The primary reason for this choice is because the code that transitions from not authenticated state to authenticated state in a server is often the most security sensitive code as it needs to assume and handle unconditionally hostile attackers. That sensitive code is simpler if it only handles a single server state

(unauthenticated) and the state transition is as simple as possible. Smaller and simpler code is easier to audit and write in a secure way.

A secondary reason to have a separate command is that it is simpler to enable or disable the feature with that design. See the discussion in the security considerations section recommending implementations provide a way to disable this extension.

Appendix B. Acknowledgements

TBD

Author's Address

Chris Newman
Oracle
440 E. Huntington Dr., Suite 400
Arcadia, CA 91006
US

Email: chris.newman@oracle.com