Protocolo IMAP

Martín López de Ipiña, Alex Rivas Machin, Borja Gomez Calvo

El protocolo IMAP (Internet Message Access Protocol) es un estándar de Internet diseñado para permitir a los clientes de correo electrónico acceder a mensajes almacenados en un servidor remoto. A diferencia de otros protocolos de correo, IMAP está específicamente optimizado para gestionar correos en el servidor, permitiendo a los usuarios:

- Acceder a su correo desde múltiples dispositivos
- Mantener los mensajes sincronizados entre dispositivos
- Trabajar con mensajes sin necesidad de descargarlos completamente
- Gestionar carpetas y estructuras organizativas en el servidor
- Realizar búsquedas en el servidor sin descargar todo el buzón

IMAP opera por defecto en el puerto 143 para conexiones no cifradas y en el puerto 993 para conexiones seguras (IMAPS). La versión actual más utilizada es IMAP4rev1, definida en el RFC 3501. RFC 9051 IMAP4rev2 (2021)

CAPABILITY en IMAP

Este mecanismo permite al cliente descubrir exactamente qué características y extensiones están disponibles en el servidor antes de intentar utilizarlas.

Cuando un cliente IMAP envía el comando CAPABILITY, el servidor responde con una lista completa de sus capacidades:

C: A001 CAPABILITY
S: * CAPABILITY IMAP4rev1 STARTTLS AUTH=PLAIN AUTH=LOGIN IDLE NAMESPACE QUOTA
S: A001 OK CAPABILITY completado

Esta respuesta proporciona la siguiente información:

- La versión del protocolo soportada (IMAP4rev1)
- Soporte para establecer conexiones seguras (STARTTLS) bajo conexión segura
- Métodos de autenticación disponibles (AUTH=PLAIN, AUTH=LOGIN)
- Extensiones adicionales que permiten funcionalidades avanzadas (IDLE, NAMESPACE, QUOTA)

El comando CAPABILITY puede ser utilizado en cualquier momento de la sesión, incluso después de la autenticación, ya que algunas capacidades pueden depender del usuario autenticado.

Mecanismos de Autenticación en IMAP

IMAP ofrece un sistema de autenticación que soporta diversos métodos:

LOGIN básico: Proporciona un método simple pero menos seguro:

C: A002 LOGIN usuario contraseña
S: A002 OK LOGIN completado

AUTHENTICATE: Permite usar mecanismos SASL (Simple Authentication and Security Layer):

C: A003 AUTHENTICATE PLAIN
S: +
C: dXNlcm5hbWUAcGFzc3dvcmQ= (codificación Base64 de "usuario\0contraseña")
S: A003 OK Autenticación exitosa

STARTTLS: Permite establecer una conexión cifrada antes de enviar las credenciales:

C: A004 STARTTLS
S: A004 OK Comenzando negociación TLS

El proceso de autenticación en IMAP está diseñado para ser extensible, permitiendo que nuevos métodos sean implementados según evolucionen los estándares de seguridad.

Comparación con POP3

POP3 (Post Office Protocol versión 3) ofrece funcionalidades similares a IMAP pero con un enfoque diferente:

Aspecto	IMAP	POP3
Equivalente a CAPABILITY	Comando CAPABILITY, integrado desde el inicio en el protocolo	Comando CAPA, añadido posteriormente como extensión
Autenticación	Múltiples mecanismos a través de SASL, con soporte nativo para diversos métodos SASL - rfc 5034	Principalmente USER/PASS, con APOP para desafío-respuesta. AUTH añadido posteriormente
Seguridad	Diseñado con mayor énfasis en seguridad desde su concepción No me parece acertada esta afirmación	Inicialmente menos enfocado en seguridad, mejorado con extensiones

Mejoras de Seguridad en IMAP

IMAP4rev1 incorpora diversas medidas de seguridad diseñadas para proteger tanto la información de autenticación como el contenido de los mensajes:

Protección contra Accesos No Autorizados

- Implementación obligatoria de TLS_RSA_WITH_RC4_128_MD5 y recomendación para TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- Mensajes de error diseñados para no revelar información sensible (no especifican si falló el usuario o la contraseña)
- Configuración de limitaciones o retrasos en intentos de autenticación fallidos
- Verificación estricta de identidad del servidor durante negociaciones TLS

Autenticación Robusta

- Soporte extensible para diversos mecanismos mediante el framework SASL
- Comando AUTHENTICATE para implementar métodos avanzados de autenticación
- Implementación obligatoria del mecanismo AUTH=PLAIN
- Recomendación de implementar mecanismos que no utilicen contraseñas en texto plano (como GSSAPI)
- Capacidad LOGINDISABLED que previene el uso del comando LOGIN cuando no hay protección

Conexiones Seguras

- Comando STARTTLS para iniciar una negociación TLS antes de intercambiar credenciales
- Verificación del nombre de host contra el certificado del servidor para evitar ataques man-in-the-middle
- Capacidad de anunciar automáticamente nuevas capacidades tras establecer una conexión TLS
- Recomendación explícita de no utilizar contraseñas en texto plano sin protección de la conexión

Bibliografía

RFC 3501: https://www.rfc-editor.org/rfc/rfc3501.html

pruebas de conexiones seguras con IMAP, capturas con Wireshark.