

Contenido

[Pregunta:](#)

Pregunta:

¿Qué los diversos códigos del HTTP de respuesta significan?

Entorno: Dispositivo de seguridad de la red de Cisco (WSA) que funciona con cualquier versión de AsyncOS

El HTTP tiene siempre un pedido de cliente y una respuesta del servidor. Las respuestas del servidor son clasificadas por un código numérico de la respuesta. Los códigos de la respuesta indican las razones detrás de los pedidos de HTTP acertados y fallados.

Para la información detallada completa con respecto a los códigos del HTTP de respuesta, vea por favor el RFC 2616 (HTTP), la [sección 10](#).

Abajo están los detalles con respecto al código más común de la respuesta que usted es probable ejecutarse en:

códigos 1xx: Informativo

100 continúan: Visto típicamente con respecto al protocolo ICAP. Ésta es una respuesta informativa que nos deja el cliente saber que puede continuar enviando los datos. Con respecto a los servicios ICAP (tales como exploración del virus), el servidor puede querer solamente ver la primera cantidad x de bytes. Cuando se hace que analiza el primer conjunto de los bytes y no detectó un virus, enviará 100 continúa dejando al cliente saber para enviar el resto del objeto.

códigos 2xx: Acertado

AUTORIZACIÓN 200: El código más común de la respuesta. Esto significa que la petición es acertada sin ningún tipo de problema.

códigos 3xx: Cambio de dirección

302 encontrado: Esto es un cambio de dirección temporal. Dan instrucciones al cliente para hacer un nuevo pedido el objeto especificado en la ubicación: encabezado.

304 no modificado: Esto está en respuesta a un **GIMS** (If-modified-since GET). Éste es literalmente un HTTP estándar GET que incluye el **If-modified-since de la** encabezado: **<date>**. Esta encabezado dice a servidor que el cliente tiene una copia del objeto solicitado en él está caché local e incluida es la fecha que el objeto fue traído. Si el objeto se ha modificado desde la esa fecha, el servidor responderá con una AUTORIZACIÓN 200 y una copia nueva del objeto. Si el objeto no ha cambiado puesto que la fecha traída, el servidor devolverá una respuesta no modificada 304.

307 temporal reorienta: A todos los efectos, tiene el mismo significado que los 302. Si se

descubren otros detalles, este artículo puede ser actualizado.

códigos 4xx: Error del cliente

Mala petición 400: Esto significa que algo en el pedido de HTTP no es sintaxis correcto siguiente. Las posibles causas podrían ser debido a las encabezados múltiples que estaban en la misma línea, los espacios en una encabezado, ningún HTTP/1.1 en URI, tan adelante. [El RFC 2616](#) se debe referir para la sintaxis adecuada.

401 desautorizado: El objeto pedido requiere la autenticación para ser accedido. Los 401 se utiliza para la autenticación a un servidor Web del destino. Al usar el dispositivo de seguridad de la red de Cisco (WSA) en el modo transparente, 401 se devuelve al cliente cuando la autenticación se habilita en el proxy. Esto es porque la aplicación es spoofing sí mismo como si fuera el OCS (servidor contenido del origen).

Los métodos de autenticación disponibles se especifican en una **WWW-autenticidad:** Encabezado del HTTP de respuesta. Esto dirá a cliente independientemente de si este servidor está pidiendo el NTLM, básico, u otros métodos de autenticación.

403 prohibido: Niegan el cliente de acceder el objeto solicitado. Hay muchas causas para porqué un servidor puede negar el acceso a un objeto. Típicamente, el servidor incluirá una cierta clase de descripción de la causa dentro de los datos HTTP (respuesta HTML).

404 no encontrado: El objeto solicitado no existe en el servidor.

Autenticación de representación 407 requerida: Éste es lo mismo que 401, salvo que está específicamente para la autenticación a un proxy, no el OCS. Se envía esto solamente si la petición fue enviada explícitamente al proxy. 407 no se pueden enviar a un cliente mientras que usan WSA como proxy transparente, como el cliente no sabe que existe el proxy. Si éste es el caso, el cliente muy probablemente FIN o RST el socket TCP.

En vez de usar WWW-autentique: encabezados para especificar qué métodos de autenticación están disponibles, la proxy-**autenticidad:** se utiliza la encabezado.

códigos 5xx: Error del servidor

Error de servidor interno 500: Error del Servidor genérico

Gateway del malo 502: Usted verá típicamente esto al usar el WSA como proxy, donde está respondiendo el gateway incorrectamente.

Servicio 503 inasequible: Esto se envía típicamente cuando el OCS está estando sobre estorbado. Intentar la petición otra vez en otro momento debe ser acertado.

Descanso de 504 gateways: 504 serán enviados si WSA no recibió una respuesta de su gateway.