

# 不同的HTTP響應代碼是什麼意思？

## 目錄

[問題：](#)

## 問題：

不同的HTTP響應代碼是什麼意思？

**環境：**運行任何AsyncOS版本的思科網路安全裝置(WSA)

HTTP總是有客戶端請求和伺服器響應。伺服器響應由數字響應代碼分類。響應代碼指示HTTP請求成功和失敗的原因。

有關HTTP響應代碼的完整詳細資訊，請參閱RFC 2616(HTTP) [第10節](#)。

下面是有關您可能遇到的最常見響應代碼的詳細資訊：

**1xx碼：**資訊

**100繼續：**通常出現在ICAP協定中。這是一個資訊性響應，告知客戶端可以繼續傳送資料。關於ICAP服務（如病毒掃描），伺服器可能只希望看到前x個位元組。當掃描完第一組位元組並且沒有檢測到病毒時，它將傳送100 Continue以讓客戶端知道傳送對象的其餘部分。

**2xx碼：**成功

**200確定：**最常見的響應代碼。這表示請求成功而沒有任何問題。

**3xx代碼：**重新導向

**找到302個：**這是臨時重新導向。指示客戶端對Location:標題。

**304未修改：**這是對GIMS(GET If-modified-since)的響應。這實際上是一個標準的HTTP GET，其中包括If-modified-since:<日期>。此標頭告訴伺服器，客戶端的本地快取中有一個請求的對象的副本，其中包括提取該對象的日期。如果在該日期後修改了對象，伺服器將以200 OK和對象的新副本進行響應。如果自獲取日期以來對象未更改，伺服器將發回304 Not Modified響應。

**307臨時重新導向：**無論出於什麼目的，它都與302具有相同的含義。如果發現了更多細節，本文可以進行更新。

**4xx代碼：**客戶端錯誤

**400錯誤請求：**這表示HTTP要求中的內容未遵循正確的語法。可能的原因可能是同一行上有多個報頭、報頭中有空格、URI中沒有HTTP/1.1等等。 [應引用RFC 2616](#)以取得適當的語法。

**401未授權：**請求的對象需要身份驗證才能訪問。401用於對目標Web伺服器進行身份驗證。在透明

模式下使用思科網路安全裝置(WSA)時，在代理上啟用驗證時，會將401傳送回客戶端。這是因為裝置正在偽裝，就好像它是OCS ( 源內容伺服器 )。

**www-authenticate**中指定了可用的身份驗證方法：HTTP響應報頭。這將告知客戶端此伺服器是否請求NTLM、基本或其他身份驗證方法。

**403禁止**:拒絕客戶端訪問請求的對象。導致伺服器拒絕訪問對象的原因有很多。通常，伺服器會在HTTP資料 ( HTML響應 ) 中包含某種原因說明。

**未找到404**:伺服器上不存在請求的對象。

**需要407代理驗證**:這與401相同，不同之處在於它專門用於代理的身份驗證，而不是OCS。僅當請求被明確傳送到代理時才傳送此消息。將WSA用作透明代理時，無法將407傳送到客戶端，因為客戶端不知道該代理存在。如果是這種情況，使用者端很可能使用FIN或RST進行TCP套接字。

而不使用**www-authenticate**:標頭指定可用的驗證方法，**proxy-authenticate**:使用報頭。

**5xx代碼**:伺服器錯誤

**500內部伺服器錯誤**:通用伺服器故障

**502錯誤的網關**:當使用WSA作為代理時，通常會出現這種情況，因為網關的響應不正確。

**503服務不可用**:這通常在OCS過度保留時傳送。稍後再次嘗試請求應該成功。

**504網關超時**:如果WSA沒有從其網關收到響應，則將傳送504。