ماذا تعني رموز إستجابة HTTP المختلفة؟

المحتويات

سؤال:

ماذا تعني رموز إستجابة HTTP المختلفة؟

البيئة: تشغيل جهاز أمان الويب (WSA) من Cisco لأي إصدار من AsyncOS

يحتوي HTTP دائما على طلب عميل واستجابة خادم. يتم تصنيف استجابات الخادم بواسطة رمز إستجابة رقمي. تشير رموز الاستجابة إلى الأسباب وراء طلبات HTTP الناجحة والفاشلة.

للحصول على معلومات تفصيلية كاملة حول رموز الاستجابة لبروتوكول HTTP، يرجى مراجعة (HTTP RFC 2616)، القسم 10.

فيما يلي تفاصيل حول رمز الاستجابة الأكثر شيوعا الذي من المحتمل أن تواجهها:

رموز **xx**: إعلامية

100 متابعة: ينظر إليها عادة فيما يتعلق ببروتوكول ICAP. هذه إستجابة إعلامية لنعلم العميل أنه يمكنه الاستمرار في إرسال البيانات. فيما يتعلق بخدمات ICAP (مثل الكشف عن الفيروسات)، قد يحتاج الخادم فقط إلى رؤية أول كمية س من وحدات البايت. عند الانتهاء من مسح المجموعة الأولى من وحدات البايت وعدم اكتشاف فيروس، سيتم إرسال 100 متابعة إلى العميل ليعلم بإرسال بقية الكائن.

رموز **2xx**: ناجحة

200 OK: رمز الاستجابة الأكثر شيوعا. وهذا يعني أن الطلب ناجح دون أية مشاكل.

رموز 3xx: إعادة التوجيه

302 وجدت: هذا إعادة توجيه مؤقتة. تم توجيه العميل إلى تقديم طلب جديد للكائن المحدد في الموقع: الرأس.

304 غير معدل: يأتي هذا إستجابة ل GET if-modified-since) **GIMS**). هذا هو حرفيا HTTP GET القياسي الذي يتضمن الرأس **If-modified-since: <date>**. يخبر هذا الرأس الخادم بأن العميل لديه نسخة من الكائن المطلوب في ذاكرة التخزين المؤقت المحلية الخاصة به، ويتم تضمينه هو التاريخ الذي تم فيه إحضار الكائن. إذا تم تعديل الكائن منذ ذلك التاريخ، سيستجيب الخادم مع 200 OK ونسخة جديدة من الكائن. إذا لم يتم تغيير الكائن منذ تاريخ الإحضار، سيقوم الخادم بإرسال إستجابة 304 غير معدلة.

307 إعادة التوجيه المؤقتة: بالنسبة لجميع المقاصد والأغراض، فإنها تحمل نفس المعنى الذي تحمله المادة 302. إذا اكتشفت تفاصيل اضافية، يمكن تحديث هذه المقالة.

رموز 4xx: خطأ العميل

400 طلب غير صحيح: هذا يعني أن شيء في طلب HTTP لا يتبع بناء جملة صحيح. قد يرجع السبب المحتمل إلى

وجود رؤوس متعددة على نفس السطر، المسافات في الرأس، بدون HTTP/1.1 في URI، وهكذا. يجب الإشارة إلى RFC 2616 لصياغة صحيحة.

401 غير مصرح به: يتطلب الكائن المطلوب المصادقة من أجل الوصول إليه. يستخدم 401 للمصادقة على خادم ويب الوجهة. عند إستخدام جهاز أمان الويب (WSA) من Cisco في الوضع الشفاف، يتم إرسال رقم 401 مرة أخرى إلى العميل عند تمكين المصادقة على الوكيل. وذلك لأن الجهاز ينتحل نفسه كما لو كان هو OCS (خادم المحتوى الأصلي).

يتم تحديد طرق المصادقة المتاحة في **www-authenticate**: رأس إستجابة HTTP. سيخبر هذا العميل ما إذا كان هذا الخادم يطلب NTLM أو الأساليب الأساسية أو غيرها من طرق المصادقة أم لا.

403 ممنوع: تم رفض العميل من الوصول إلى الكائن المطلوب. هناك العديد من الأسباب التي قد تؤدي إلى رفض الخادم للوصول إلى كائن. بشكل نموذجي، سيتضمن الخادم نوعا من وصف السبب ضمن بيانات HTTP (إستجابة HTML).

404 غير موجود: الكائن المطلوب غير موجود على الخادم.

407 مطلوب مصادقة الوكيل: وهذا هو نفسه كما هو الحال في 401، باستثناء أنه مخصص للمصادقة على وكيل، وليس لمصادقة OCS. ويتم إرسال هذا فقط إذا تم إرسال الطلب بشكل صريح إلى الوكيل. لا يمكن إرسال رقم 407 إلى عميل أثناء إستخدام WSA كوكيل شفاف، نظرا لأن العميل لا يعرف وجود الوكيل. إذا كان هذا هو الحال، فمن المرجح أن يقوم العميل بإعادة التوجيه أو إعادة التوجيه (RST) لمقبس بروتوكول التحكم في الإرسال (TCP).

بدلا من إستخدام مصادقة www: الرؤوس لتحديد طرق المصادقة المتاحة، يتم إستخدام الرأس **Proxy-authenticate**.

رموز 5xx: خطأ في الخادم

خطأ في الخادم الداخلي 500: فشل الخادم العام

عبارة 502 غير صحيحة: سترى ذلك عادة عند إستخدام WSA كوكيل، حيث تستجيب البوابة بشكل غير صحيح.

الخدمة 503 غير متوفرة: يتم إرسال هذا عادة عندما يكون OCS مرهونا فوق الحد. يجب أن تكون محاولة إجراء الطلب مرة أخرى في وقت لاحق ناجحة.

مهلة البوابة 504: سيتم إرسال 504 إذا لم يستلم WSA إستجابة من البوابة الخاصة به.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).