Wat betekenen de verschillende HTTP-responscodes?

Inhoud

Vraag:

Wat betekenen de verschillende HTTP-responscodes?

Milieu: Cisco Web Security Appliance (WSA) met alle AsyncOS-versie

HTTP heeft altijd een client-aanvraag en een server-respons. De serverreacties worden geclassificeerd door een numerieke responscode. De responscodes geven de redenen aan achter succesvolle en mislukte HTTP-verzoeken.

Zie RFC 2616 (HTTP), sectie 10 voor meer informatie over HTTP-responscodes.

Hieronder zie je details over de meest voorkomende responscode waarmee je waarschijnlijk zal werken:

1x-codes: informatief

100 Doorgaan: Gewoonlijk gezien met betrekking tot het ICAP-protocol. Dit is een informatieve reactie die de klant laat weten dat hij gegevens kan blijven versturen. Wat de ICAP services (zoals het scannen van virussen) betreft, kan het zijn dat de server alleen de eerste x hoeveelheid bytes wil zien. Wanneer de eerste reeks bytes is gescand en geen virus heeft gedetecteerd, wordt een 100 Doorgaan om de client te laten weten de rest van het object te verzenden.

2x-codes: succesvol

200 OK: De meest voorkomende responscode. Dit betekent dat het verzoek zonder problemen succesvol is.

3xx-codes: omleiding

302 gevonden: Dit is een tijdelijke omleiding. De client is geïnstrueerd een nieuw verzoek in te dienen voor het object dat in de locatie is gespecificeerd: kopbal.

Niet gewijzigd: Dit is een reactie op een **GIMS** (ALS-aangepast-sindsdien). Dit is letterlijk een standaard HTTP GET dat de header **As-Modified-sens** bevat**: <datum>.** Deze header vertelt de server dat de client een kopie heeft van het gevraagde object in het lokale cache en dat het onderdeel is opgenomen is de datum waarop het object is opgehaald. Als het object sinds die datum is aangepast, reageert de server op 200 OK en een nieuwe kopie van het object. Als het object niet is veranderd sinds de opgehaalde datum, stuurt de server een 304 Not Modified

Response terug.

307 Tijdelijke omleiding: Het heeft in alle opzichten dezelfde betekenis als het artikel 302. Indien verdere details worden ontdekt, kan dit artikel worden aangepast.

4xx-codes: Clientfout

400 Slecht verzoek: Dit betekent dat het iets in het HTTP-verzoek niet de juiste syntaxis volgt. Mogelijke oorzaken zouden te wijten kunnen zijn aan meerdere kopregels op dezelfde regel, spaties in een header, geen HTTP/1.1 in de URI, enzovoort. RFC 2616 dient te worden verwezen naar de juiste syntaxis.

401 Niet-geautoriseerd: Het gevraagde object vereist authenticatie om toegang te krijgen. De 401 wordt gebruikt voor authenticatie aan een doelwebserver. Wanneer u het Cisco Web Security Appliance (WSA) in transparante modus gebruikt, wordt een 401 teruggestuurd naar de client wanneer verificatie op de proxy is ingeschakeld. Dit komt doordat het apparaat zichzelf afwerpt alsof het een OCS-server (oorsprongsinhoudsserver) is.

De beschikbare methoden voor echtheidscontrole worden gespecificeerd in een **www-echt**: HTTP-responsheader. Dit zal de client vertellen of deze server al dan niet om NTLM, basismethoden of andere methoden van authenticatie vraagt.

403 Verboden: De client heeft geen toegang tot het gevraagde object. Er zijn veel oorzaken waarom een server toegang tot een object kan ontkennen. Meestal zal de server een beschrijving van de oorzaak bevatten in de HTTP gegevens (HTML-respons).

Niet gevonden: Het gevraagde object bestaat niet op de server.

Vereiste proxy-verificatie: Dit is hetzelfde als een 401, behalve dat het specifiek is voor authenticatie aan een volmacht, niet de OCS. Dit verzoek wordt alleen verzonden indien het expliciet aan de volmacht is toegezonden. Een 407 kan niet naar een cliënt worden verzonden terwijl WSA als transparante volmacht wordt gebruikt, aangezien de cliënt niet weet dat de volmacht bestaat. Als dit het geval is, zal de client waarschijnlijk FIN of RST de TCP socket openen.

In plaats van www-echt te gebruiken: Kop om te specificeren welke authenticatiemethoden beschikbaar zijn, **proxy-echt**: header wordt gebruikt.

5x-codes: Serverfout

500 interne serverfout: Generic Server-storing

Slechte gateway: U ziet dit doorgaans bij gebruik van de WSA als een proxy, waarbij de gateway niet correct reageert.

503 Niet beschikbaar: Dit wordt doorgaans verzonden wanneer de OCS wordt overbelast. Het is een succes om op een later tijdstip opnieuw een verzoek in te dienen.

Time-out gateway 504: Er wordt een 504 verzonden indien WSA geen antwoord van zijn gateway heeft ontvangen.