Qual è il significato dei diversi codici di risposta HTTP?

Sommario

Domanda:

Qual è il significato dei diversi codici di risposta HTTP?

Ambiente: appliance Cisco Web Security (WSA) con qualsiasi versione di AsyncOS

HTTP dispone sempre di una richiesta client e di una risposta server. Le risposte del server sono classificate da un codice di risposta numerico. I codici di risposta indicano i motivi delle richieste HTTP riuscite e non riuscite.

Per informazioni dettagliate complete sui codici di risposta HTTP, vedere la RFC 2616 (HTTP), sezione 10.

Di seguito sono riportati i dettagli relativi al codice di risposta più comune che si prevede di utilizzare:

Codici 1xx: Informativo

100 Continue: generalmente visto in relazione al protocollo ICAP. Si tratta di una risposta informativa che informa il client che può continuare a inviare dati. Per quanto riguarda i servizi ICAP (ad esempio la scansione antivirus), il server potrebbe voler vedere solo la prima x quantità di byte. Al termine della scansione del primo set di byte e quando non è stato rilevato alcun virus, viene inviato il messaggio 100 Continue per informare il client di inviare il resto dell'oggetto.

Codici 2xx: validi

200 OK: il codice di risposta più comune. Ciò significa che la richiesta è stata completata senza alcun problema.

Codici 3xx: Reindirizzamento

302 Trovato: questo è un reindirizzamento temporaneo. Al client viene richiesto di effettuare una nuova richiesta per l'oggetto specificato nell'intestazione Location:.

304 Non modificato: questo è in risposta a un GIMS (GET If-Modified-Since). Si tratta letteralmente di un HTTP GET standard che include l'intestazione If-modified-Since: <data>. Questa intestazione indica al server che il client dispone di una copia dell'oggetto richiesto nella

cache locale e indica la data in cui l'oggetto è stato recuperato. Se l'oggetto è stato modificato dopo tale data, il server risponderà con 200 OK e una nuova copia dell'oggetto. Se l'oggetto non è stato modificato dopo la data di recupero, il server restituirà una risposta 304 Non modificato.

307 Temporary Redirect: A tutti gli effetti, ha lo stesso significato di 302. Se vengono individuati ulteriori dettagli, è possibile aggiornare questo articolo.

Codici 4xx: Errore del client

400 Richiesta non valida: ciò significa che qualcosa nella richiesta HTTP non segue la sintassi corretta. Le possibili cause possono essere dovute alla presenza di più intestazioni sulla stessa riga, di spazi in un'intestazione, di HTTP/1.1 nell'URI e così via. Per la sintassi corretta, fare riferimento alla RFC 2616.

401 Non autorizzato: per accedere all'oggetto richiesto è necessaria l'autenticazione. Il modello 401 viene utilizzato per l'autenticazione su un server Web di destinazione. Quando si utilizza l'appliance Cisco Web Security (WSA) in modalità trasparente, quando l'autenticazione è abilitata sul proxy, viene inviato al client un file 401. Questo accade perché l'accessorio viene sottoposto a spoofing come se si trattasse di OCS (source content server).

I metodi di autenticazione disponibili sono specificati in un'intestazione di risposta www-authenticate: HTTP. In questo modo il client saprà se il server richiede NTLM, standard o altri metodi di autenticazione.

403 Accesso negato: al client è negato l'accesso all'oggetto richiesto. Le cause che possono impedire l'accesso a un oggetto possono essere molteplici. In genere, il server include una sorta di descrizione della causa all'interno dei dati HTTP (risposta HTML).

404 Non trovato: l'oggetto richiesto non esiste nel server.

407 Autenticazione proxy richiesta: è la stessa di 401, ad eccezione del fatto che è specificamente per l'autenticazione a un proxy, non OCS. Questo viene inviato solo se la richiesta è stata inviata esplicitamente al proxy. Impossibile inviare un 407 a un client quando si utilizza WSA come proxy trasparente, in quanto il client non è a conoscenza dell'esistenza del proxy. In questo caso, è molto probabile che il client rilevi il socket TCP tramite FIN o RST.

Anziché utilizzare le intestazioni www-authenticate: per specificare i metodi di autenticazione disponibili, viene utilizzata l'intestazione proxy-authentication:.

Codici 5xx: Errore del server

500 Errore interno del server: errore generico del server

502 Bad Gateway: in genere ciò si verifica quando si utilizza il WSA come proxy, in cui il gateway risponde in modo errato.

503 Servizio non disponibile: in genere viene inviato quando OCS è sovraccaricato. Tentativo di

ripetere la richiesta in un secondo momento dovrebbe avere esito positivo.

504 Gateway Timeout: verrà inviato un 504 se WSA non ha ricevuto una risposta dal gateway.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).