Was bedeuten die verschiedenen HTTP-Antwortcodes?

Inhalt

Frage:

Was bedeuten die verschiedenen HTTP-Antwortcodes?

Umgebung: Cisco Web Security Appliance (WSA) mit AsyncOS-Version

HTTP verfügt immer über eine Clientanforderung und eine Serverantwort. Die Serverantworten werden durch einen numerischen Antwortcode klassifiziert. Antwortcodes geben die Gründe für erfolgreiche und fehlgeschlagene HTTP-Anfragen an.

Ausführliche Informationen zu HTTP-Antwortcodes finden Sie in RFC 2616 (HTTP), Abschnitt 10.

Im Folgenden finden Sie einige Details zum häufigsten Antwortcode, mit dem Sie wahrscheinlich arbeiten werden:

1xx-Codes: Informativ

100 Weiter: Typisch für das ICAP-Protokoll. Dies ist eine informative Antwort, die den Client darauf hinweist, dass er weiterhin Daten senden kann. Bei ICAP-Diensten (z. B. Virenscans) möchte der Server möglicherweise nur die erste x Bytemenge sehen. Wenn der erste Bytesatz gescannt wird und kein Virus erkannt wurde, sendet er einen 100 Continue-Befehl, um den Client darüber zu informieren, den Rest des Objekts zu senden.

2xx-Codes: Erfolgreich

200 OK: Der häufigste Antwortcode. Dies bedeutet, dass die Anfrage ohne Probleme erfolgreich war.

3xx-Codes: Umleitung

302 gefunden: Dies ist eine vorübergehende Umleitung. Der Client wird angewiesen, eine neue Anforderung für das in Location: Header.

304 Nicht geändert: Dies ist eine Reaktion auf ein **GIMS** (GET If-modified-Since). Dies ist buchstäblich ein Standard-HTTP GET, das den Header **If-modified-Since** enthält**: <Datum>** Dieser Header teilt dem Server mit, dass der Client eine Kopie des angeforderten Objekts im lokalen Cache hat und dass es sich dabei um das Datum handelt, an dem das Objekt abgerufen wurde. Wenn das Objekt seit diesem Datum geändert wurde, antwortet der Server mit einem 200 OK und einer neuen Kopie des Objekts. Wenn das Objekt seit dem abgerufenen Datum nicht geändert

wurde, sendet der Server eine 304 Not Modified-Antwort zurück.

307 Temporäre Umleitung: Sie hat im Grunde dieselbe Bedeutung wie die 302. Wenn weitere Details entdeckt werden, kann dieser Artikel aktualisiert werden.

4xx-Codes: Client-Fehler

400 Bad Request: Das bedeutet, dass das Objekt in der HTTP-Anfrage nicht der richtigen Syntax entspricht. Mögliche Ursachen können darin liegen, dass mehrere Header sich auf derselben Zeile befinden, Leerzeichen in einem Header, keine HTTP/1.1 im URI usw. Auf RFC 2616 sollte zur korrekten Syntax verwiesen werden.

401 Nicht autorisiert: Für den Zugriff auf das angeforderte Objekt ist eine Authentifizierung erforderlich. Der 401 wird für die Authentifizierung zu einem Ziel-Webserver verwendet. Wenn die Cisco Web Security Appliance (WSA) im transparenten Modus verwendet wird, wird eine 401-Appliance an den Client zurückgesendet, wenn die Authentifizierung auf dem Proxy aktiviert ist. Dies liegt daran, dass sich die Appliance selbst als OCS (Ursprungsinhaltsserver) getäuscht hat.

Die verfügbaren Authentifizierungsmethoden werden in einem **www-authentication** angegeben: HTTP-Antwortheader Dadurch wird dem Client mitgeteilt, ob dieser Server NTLM, einfache oder andere Authentifizierungsmethoden anfordert.

403 Verboten: Dem Client wird der Zugriff auf das angeforderte Objekt verweigert. Es gibt viele Gründe, warum ein Server den Zugriff auf ein Objekt verweigern kann. Normalerweise enthält der Server eine Beschreibung der Ursache in den HTTP-Daten (HTML-Antwort).

404 Nicht gefunden: Das angeforderte Objekt ist auf dem Server nicht vorhanden.

407-Proxy-Authentifizierung erforderlich: Dies entspricht dem 401, mit der Ausnahme, dass es speziell für die Authentifizierung eines Proxys und nicht des OCS bestimmt ist. Diese wird nur gesendet, wenn die Anforderung explizit an den Proxy gesendet wurde. Ein 407 kann nicht an einen Client gesendet werden, wenn WSA als transparenter Proxy verwendet wird, da der Client nicht weiß, dass der Proxy vorhanden ist. Ist dies der Fall, wird der Client höchstwahrscheinlich den TCP-Socket FIN oder RST.

Anstelle von www-authentication: Header, um anzugeben, welche Authentifizierungsmethoden verfügbar sind, **authentifiziert** der **Proxy**: Header wird verwendet.

5xx-Codes: Serverfehler

500 interner Serverfehler: Generischer Serverfehler

502 Schlechtes Gateway: In der Regel wird dies angezeigt, wenn die WSA als Proxy verwendet wird, wo das Gateway falsch reagiert.

503 Service nicht verfügbar: Diese wird in der Regel gesendet, wenn der OCS überlastet ist. Der Versuch, die Anforderung zu einem späteren Zeitpunkt erneut durchzuführen, sollte erfolgreich sein.

504-Gateway-Timeout: Wenn die WSA keine Antwort vom Gateway erhalten hat, wird eine 504 gesendet.