Troubleshooting am LoadMaster: Logs, L7-Debug und TCP-Dump



WISSEN
Alles zum Kemp LoadMaster mit Microsoft-Brille: Exchange, SharePoint, ADFS, RDS, Eigenentwicklungen und Kerberos an einem Ort.
› **Kemp LoadMaster**

BERATUNG
Seit Stunden 503 und niemand weiß, warum? Wir lesen mit dir Logs, Traces und Mitschnitte, bis der Schuldige feststeht.
› **Beratung zum Kemp LoadMaster**

SCHULUNG
Fehlersuche am LoadMaster im Labor üben: kaputte Health Checks, KCD-Fehler, TLS-Abbrüche, alles mit Absicht kaputt gemacht.
› **Kemp-LoadMaster-Schulung**

Der Anruf kommt immer zur selben Uhrzeit: kurz bevor du nach Hause wolltest. „OWA geht nicht.“ Mehr Information gibt es nicht, und mehr wird es auch nicht geben, denn die Person am anderen Ende hat inzwischen einen Screenshot gemacht, der zu achtzig Prozent aus Taskleiste besteht. Irgendwo darauf ist ein 403 zu erkennen. Oder ein 503. Oder eine Zertifikatswarnung. Sicher ist nur eines: Bis zum Ende des Gesprächs wird der LoadMaster schuld sein. Er ist neu im Haus, er steht in der Mitte, und Dinge in der Mitte bekommen bekanntlich von beiden Seiten Schläge ab.

Manchmal ist er tatsächlich schuld. Ein Edge Security Pack, das einen Pfad nicht kennt, eine WAF-Regel, die ein Exchange-Formular für einen Angriff hält, ein Health Check, der alle Server für tot erklärt, ein Keytab mit dem falschen Verschlüsselungstyp. Mindestens genauso oft aber ist der LoadMaster nur der Bote, der eine schlechte Nachricht des IIS weiterreicht, und die eigentliche Ursache sitzt auf dem Exchange-Server, im Active Directory oder in einer Eigenentwicklung, die seit dem letzten Update Host-Header anders interpretiert.

Dieser Beitrag aus der Serie zum Kemp LoadMaster beschreibt einen systematischen Fehlerweg. Nicht als Nacherzählung der Herstellerdoku, sondern als Reihenfolge, die in der Praxis Zeit spart: zuerst klären, wer geantwortet hat, dann das richtige Log lesen, erst danach zu den schweren Werkzeugen L7-Debug und TCP-Dump greifen. Am Ende steht eine Fehlerbild-Tabelle für die Klassiker, die dir in Microsoft-Umgebungen immer wieder begegnen.

FAKTEN · Das Wichtigste in 30 Sekunden

Erste Frage immer: Hat der LoadMaster selbst geantwortet oder der Real Server? Die Antwort-

Header verraten es meist in Sekunden.

Das System Message File ist das Hauptlog des LoadMasters. Dort landen auch die Ausgaben des L7-Debugs.

ESP schreibt eigene Logs (Connection, Security, User), die WAF ein eigenes Event Log. Beide findest du nicht im System Message File.

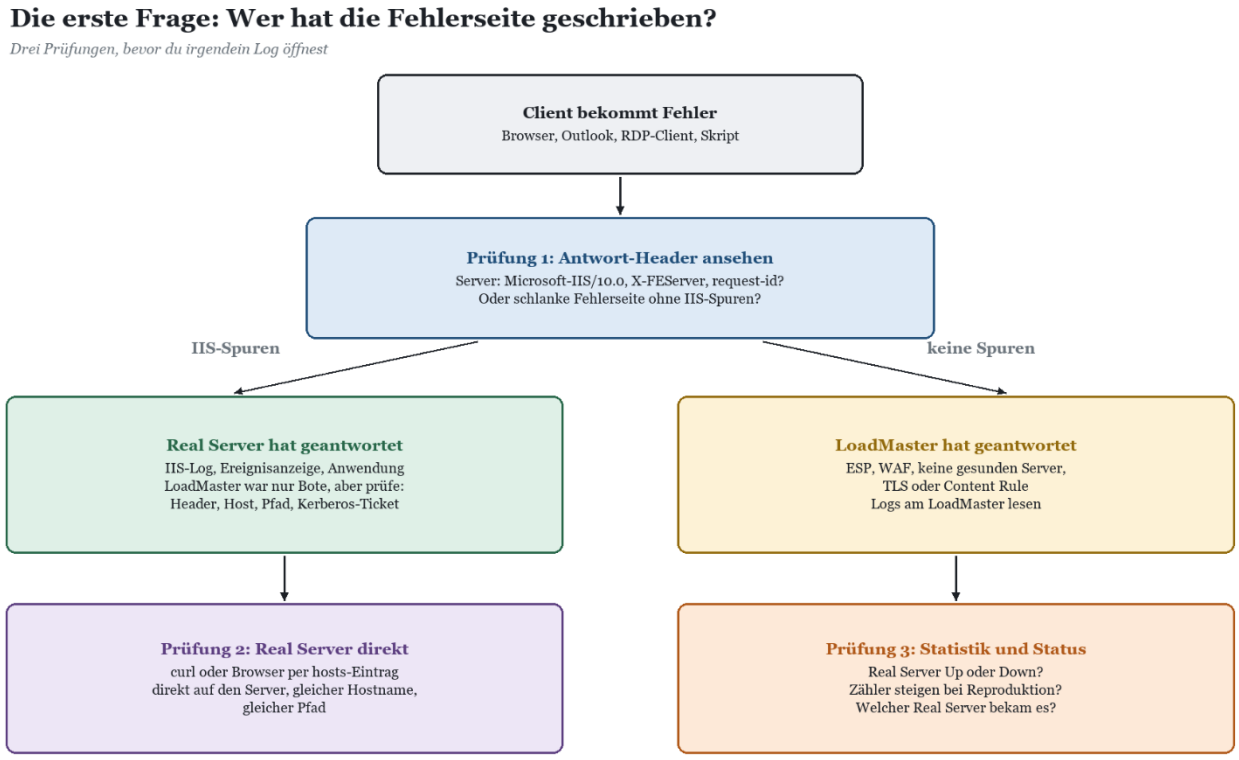
Extended L7 Debug arbeitet je Virtual Service und lässt sich auf eine einzelne Client-IP einschränken. Das globale L7-Debug ist der Vorschlaghammer.

Der TCP-Dump in der WUI stoppt standardmäßig nach 10.000 Paketen oder 30 MB. Kurz und gezielt mitschneiden, nicht „mal laufen lassen“.

Die erste Frage: Wer hat eigentlich geantwortet?

Ein Layer-7-Virtual-Service ist ein vollwertiger Reverse Proxy. Der Client spricht mit dem LoadMaster, der LoadMaster spricht mit dem Real Server, und dazwischen hat der LoadMaster jede Menge Gelegenheiten, selbst eine Antwort zu erzeugen: Die WAF blockt, das ESP verlangt eine Anmeldung oder verweigert einen Pfad, kein Real Server ist gesund, eine Content Rule leitet um, der TLS-Handshake scheitert schon vor dem ersten Byte HTTP. Für den Client sehen all diese Fälle gleich aus: eine Fehlermeldung von „dem Server“.

Genau deshalb ist die wichtigste Minute einer Fehlersuche die, in der du herausfindest, wer die Fehlerseite geschrieben hat. Danach weißt du, ob du die nächste Stunde in den Logs des LoadMasters oder in der Ereignisanzeige des Windows-Servers verbringst. Wer diese Minute überspringt, sucht im Zweifel an der falschen Stelle sehr gründlich.



Skizze: Header-Namen beispielhaft für Exchange und IIS; Eigenentwicklungen haben eigene Spuren

Antwort-Header lesen statt Screenshots deuten

Öffne die Entwicklertools des Browsers, Reiter Netzwerk, und sieh dir die fehlerhafte Antwort an. Ein IIS hinterlässt Spuren: den Header Server mit Microsoft-IIS und Versionsnummer, oft X-

Powered-By, bei Exchange zusätzlich X-FEServer und request-id, bei SharePoint SPRequestGuid. Fehlen alle diese Spuren und die Fehlerseite ist auffällig schlicht, hat mit hoher Wahrscheinlichkeit der LoadMaster selbst geantwortet. Bei Eigenentwicklungen lohnt es sich, einmal im Normalbetrieb nachzusehen, welche Header die Anwendung setzt, damit du im Störfall vergleichen kannst.

Vorsicht bei Umgebungen, in denen Content Rules Header wie Server oder X-Powered-By aus Sicherheitsgründen entfernen. Dann fehlen die Spuren auch bei echten IIS-Antworten. Lege dir für solche Fälle einen eigenen, harmlosen Header an, den der Real Server immer setzt, etwa den Namen des Knotens. Im Störfall ist das Gold wert.

```
curl -sk -o /dev/null -D - https://mail.contoso.de/owa/
curl -sk -o /dev/null -D - --resolve mail.contoso.de:443:10.0.20.11
https://mail.contoso.de/owa/
```

Die zweite Zeile ist der Trick, der viele Diskussionen beendet: Du sprichst denselben Hostnamen mit demselben Pfad an, aber direkt auf dem Real Server, am LoadMaster vorbei. curl ist auf aktuellen Windows-Versionen an Bord. Liefert der Server direkt dieselbe Fehlermeldung, ist der LoadMaster aus dem Schneider. Funktioniert es direkt, aber nicht über den LoadMaster, ist er zumindest Mitwisser.

Statistiken als Lügendetektor

Die Statistiken des LoadMasters zeigen live, wie viele Verbindungen und Requests je Virtual Service und je Real Server ankommen. Das klingt banal, beantwortet aber zwei Fragen, die in der Fehlersuche ständig auftauchen. Erstens: Kommt der Client überhaupt beim LoadMaster an? Bleiben die Zähler beim Reproduzieren stehen, liegt das Problem davor, also bei DNS, Firewall, NAT oder einem Client, der an eine alte Adresse geht. Zweitens: Welcher Real Server bekommt die Anfragen? Wenn nur einer von dreien Fehler produziert, siehst du über die Statistik, ob die betroffenen Benutzer gerade an genau diesem hängen.

Daneben ist die Übersicht der Virtual Services selbst ein schneller Blick wert: Status des Virtual Service, Status jedes Real Servers. Ein Real Server, der rot ist, ist für den LoadMaster tot, egal, was der Server selbst davon hält. Warum ein Health Check einen gesunden Server für tot oder, noch tückischer, einen kranken für gesund hält, ist Thema des Beitrags Health Checks, die wirklich prüfen: warum „Port 443 offen“ nicht reicht.

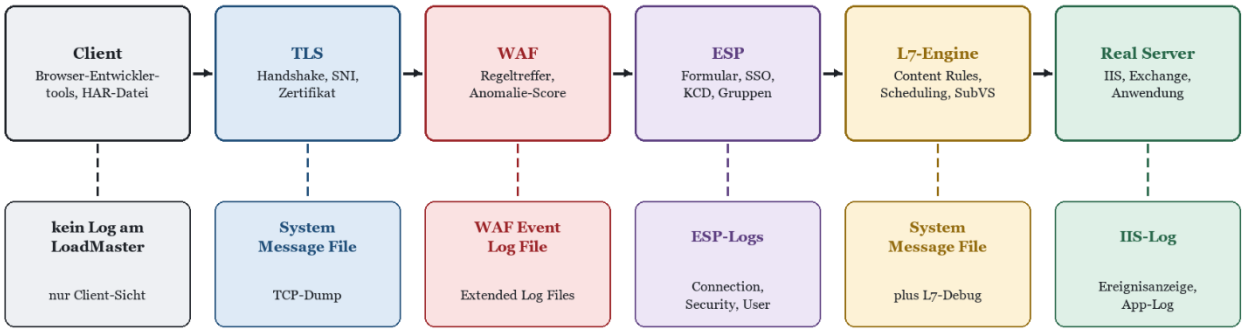
> **TIPP · Notiere die Uhrzeit, bevor du reproduzierst**
>
> Alle Logs dieses Beitrags sind zeitbasiert. Wenn du weißt, dass der Fehler um 14:32:10 auftrat, findest du die passenden Zeilen in Sekunden. Prüfe einmalig, dass der LoadMaster per NTP dieselbe Uhrzeit wie deine Domänencontroller hat. Abweichende Uhren machen Korrelation zur Geduldsprobe und Kerberos zum Totalausfall.

Die Logs des LoadMasters: welches Buch für welche Frage

Der LoadMaster führt nicht ein Log, sondern mehrere, und sie sind über zwei Stellen in der WUI verteilt. Unter System Configuration, Logging Options, System Log Files liegen die Systemlogs. Die Logs des Edge Security Pack und die WAF-Auswertungen findest du zusätzlich unter Extended Log Files. Wer das nicht weiß, sucht den ESP-Fehler eine halbe Stunde im System Message File und kommt zu dem Schluss, dass es keinen gibt.

Die Logkarte: Jede Station schreibt in ein anderes Buch

Ein Request durchläuft den LoadMaster in Etappen. Suche dort, wo er stecken geblieben ist



Querschnitt über alle Stationen

- Statistiken: Verbindungen und Requests je Virtual Service und Real Server, live.
- Audit Log File: wer hat wann per WUI oder API etwas geändert? (Antwort auf „Wir haben nichts gemacht“)
- Syslog: alles oben, nur länger aufbewahrt und mit Zeitstempel neben den Windows-Logs.
- TCP-Dump: die einzige Quelle, die nicht interpretiert, sondern nur mitschreibt.

Skizze: Reihenfolge vereinfacht; welche Stationen aktiv sind, hängt vom Virtual Service ab

Log	Was drinsteht	Typische Frage
System Message File	Ereignisse des Betriebssystems und der LoadMaster-Dienste, Zustandswechsel von Real Servern, TLS-Fehler, bei aktivem L7-Debug die Debug-Ausgabe	Warum ist der Server rot? Warum bricht die Verbindung ab?
Warning Message File	Warnungen aus dem Betrieb	Gibt es Auffälligkeiten seit dem Update?
Boot.msg File	Startinformationen inklusive Firmware-Version	Was lief beim letzten Neustart?
Audit Log File	Jede Aktion eines Benutzers über WUI oder API, sofern Session Management aktiv ist	Wer hat gestern um 17 Uhr den Virtual Service geändert?
ESP Connection Log	Verbindungen zu ESP-geschützten Diensten	Kam der Client bis zum ESP?
ESP Security Log	Fehlgeschlagene Anmeldungen und sicherheitsrelevante Ereignisse	Warum wird der Benutzer abgewiesen?
ESP User Log	Erfolgreiche Anmeldungen, Abmeldungen, angefragte URLs	Wer war wann wo drin?
WAF Event Log File	Zuletzt ausgelöste WAF-Regeln	Welche Regel blockt das Formular?
WAF Debug Log File	Debug-Traces der WAF, nur bei aktivem WAF-Debug	Nur mit dem Support

System Message File: das Hauptbuch

Das System Message File ist die erste Anlaufstelle, wenn der LoadMaster selbst etwas falsch zu machen scheint. Hier siehst du, wann ein Real Server als down markiert wurde und wann er zurückkam, hier landen Fehlermeldungen der Layer-7-Engine und, sobald du es einschaltest, die Ausgabe des L7-Debugs. Die WUI zeigt die Datei im Browser an, und bei einem gut besuchten LoadMaster ist das eine lange Rolle Papier. Filtere im Browser mit der Suchfunktion nach der Adresse des Real Servers, des Virtual Service oder der Client-IP.

Über Save Logs lädst du alle Logs als komprimiertes Archiv herunter. Das ist der Weg, wenn du in Ruhe mit einem Editor arbeiten oder den Progress-Support einbinden willst. Clear Logs leert das Warning und das System Message File. Das ist praktisch vor einer gezielten Reproduktion, aber denk daran, dass damit auch die Geschichte der letzten Tage weg ist. Wenn du den LoadMaster per Syslog an ein zentrales System angebunden hast, ist das egal. Wenn nicht, solltest du das ändern, bevor du es brauchst; wie das geht, steht im Beitrag Monitoring, Syslog und SNMP: den LoadMaster ins Monitoring holen.

ESP-Logs: wo Anmeldungen sterben

Sobald ein Virtual Service mit dem Edge Security Pack vorauthentifiziert, gibt es eine zweite Wahrheit neben dem IIS-Log: Der Benutzer hat sich am LoadMaster angemeldet, nicht am Exchange-Server. Scheitert das, sieht der Real Server davon nichts. Das ESP Security Log zeigt fehlgeschlagene Anmeldungen, das User Log die erfolgreichen samt angefragter URL, das Connection Log die Verbindungen. Die Logs sind persistent und überstehen einen Neustart.

Eine Eigenheit solltest du kennen: Wenn du die ESP-Logs an einen Remote-Syslog senden willst, schaltest du die lokale Protokollierung der Extended ESP Logs ab. Beides gleichzeitig, lokal und remote, unterstützen aktuelle Firmware-Versionen laut Progress nicht mehr. Wer also auf der WUI nach ESP-Logs sucht und nichts findet, sollte zuerst prüfen, ob sie nicht längst ins SIEM fließen. Für tiefere Analysen gibt es in den ESP-Optionen zusätzlich SSOMGR-Debug-Traces, die den Single-Sign-On-Manager gesprächig machen. Wie ESP, SSO-Domänen und Vorauthentifizierung zusammenspielen, beschreibt Edge Security Pack: Vorauthentifizierung, SSO-Domänen und der TMG-Ersatz.

AUS DER PRAXIS · Der Benutzer, den es nicht gab

In einer Verwaltung meldeten sich nach einer Umstellung einzelne Benutzer nicht mehr an OWA an, andere schon. Das IIS-Log war leer, also „kam nichts an“. Das ESP Security Log zeigte dagegen für jeden Fehlversuch dieselbe Meldung: Benutzer nicht gefunden. Ursache war das Format des Anmeldenamens. Die SSO-Domäne erwartete den UPN, die betroffenen Benutzer tippten aus Gewohnheit Domäne und Benutzername. Fünf Minuten Log lesen, statt zwei Tage Exchange-Server neu starten.

WAF-Logs: wenn die Firewall Exchange für einen Angreifer hält

Die Web Application Firewall blockt standardmäßig mit einem 403, und dieser 403 kommt vom LoadMaster, nicht vom IIS. Das WAF Event Log File zeigt, welche Regel zugeschlagen hat, mit Regel-ID, betroffenem Pfad und Client. Der Button erscheint in der WUI übrigens nur, wenn es überhaupt Einträge gibt. Wer ihn nicht findet, hat also entweder keine WAF-Treffer oder sucht am falschen Virtual Service.

Klassiker in Microsoft-Umgebungen sind große POST-Requests bei ActiveSync und EWS, Base64-Blöcke in OWA-Anhängen, die verdächtig nach Code aussehen, und SharePoint-Formulare mit Feldnamen, die eine Regel für SQL hält. Die Lösung ist nie, die WAF auszuschalten, sondern die Regel für genau diesen Pfad gezielt zu entschärfen. Wie du das ohne Fehlalarm-Hölle hinbekommst, steht in Web Application Firewall und Geoblocking am LoadMaster: Schutz ohne Fehlalarm-Hölle.

WARNUNG · Logs enthalten personenbezogene Daten

ESP User Log, WAF-Log, L7-Debug und TCP-Dump enthalten Benutzernamen, Client-IPs, URLs und je nach Einstellung auch Header mit Cookies oder Tokens. Bevor du ein Archiv an den Support oder einen Dienstleister gibst, kläre den Weg mit dem Datenschutz und schwärze, was nicht gebraucht

wird. Und lösche die Dateien danach auch wieder, statt sie im Downloads-Ordner zu archivieren.

L7-Debug: das Mikroskop mit Nebenwirkungen

Wenn die normalen Logs nur sagen, dass etwas schiefging, aber nicht warum, ist das L7-Debug die nächste Stufe. Es schreibt zusätzliche Informationen über die Verarbeitung von Layer-7-Verbindungen ins System Message File: welcher Real Server gewählt wurde, welche Content Rule gegriffen hat, an welcher Stelle eine Verbindung beendet wurde. Es gibt zwei Ausprägungen, und der Unterschied ist für den Produktivbetrieb entscheidend.

Global oder je Virtual Service

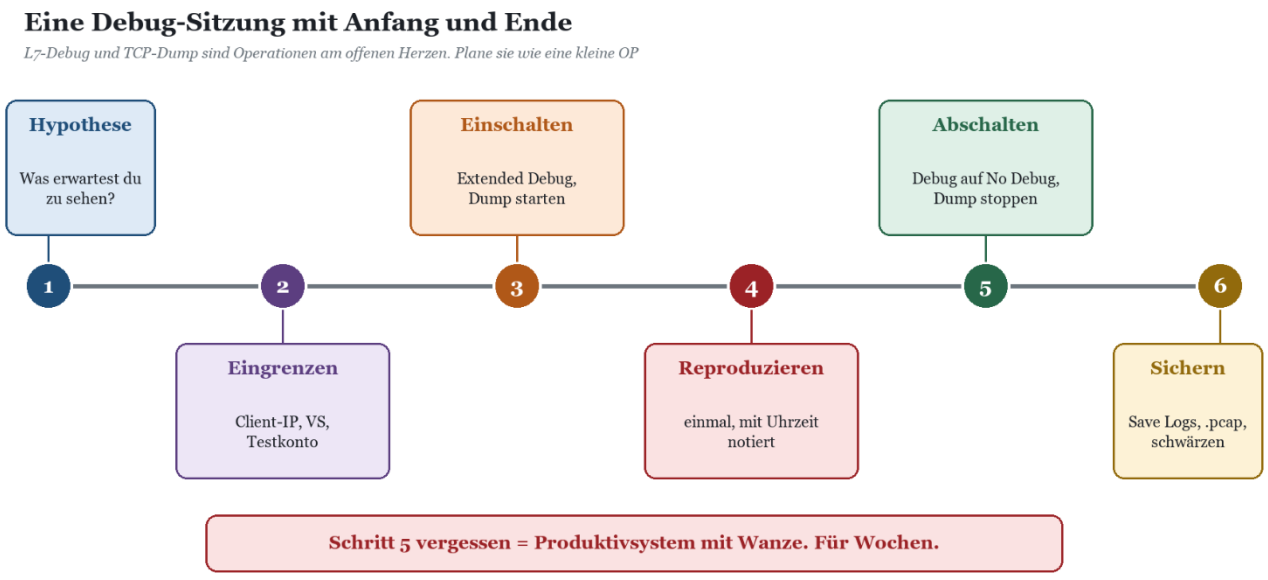
Die globale Option Enable L7 Debug Traces findest du unter System Configuration, Logging Options, System Log Files, Debug Options. Sie gilt für alle Layer-7-Verbindungen des gesamten LoadMasters. Auf einer Appliance, die Exchange, SharePoint und drei Eigenentwicklungen gleichzeitig bedient, erzeugst du damit in Minuten eine Logflut, in der du deinen einen Testlauf suchen darfst. Progress weist ausdrücklich darauf hin, dass die Option zusätzliche Ressourcen kostet und Autorisierungsparameter sichtbar machen kann.

Deutlich feiner ist das Extended L7 Debug. Du aktivierst es einmalig in denselben Debug Options, danach bekommt jeder Virtual Service im Bearbeitungsdialog einen Abschnitt Extended Debug. Dort wählst du die Stufe und kannst optional eine einzelne Client-Adresse angeben. Dann wird nur der Verkehr dieses einen Clients protokolliert, also deines Test-PCs. SubVS erben die Einstellung, du kannst aber auch gezielt nur einen SubVS debuggen. Die globale Option hat Vorrang: Ist sie an, nützt die feine Einstellung nichts.

Stufe	Was protokolliert wird	Wann sinnvoll
No Debug	Nichts zusätzlich, Standard für alle Virtual Services und SubVS	Immer, außer jetzt gerade
Call Tracing	Grundlegende Ablaufinformation der wichtigsten Schritte	Erster Blick: wohin geht der Request, wo endet er?
Full Debug	Alle verfügbaren Debug-Ausgaben, entspricht der globalen Option für diesen VS	Wenn Call Tracing nicht reicht
Full Debug + HTTP Headers	Zusätzlich die HTTP-Header, also potenziell Cookies, Authorization-Header und Tokens	Header-Probleme, Kerberos, Content Rules; nur kurz

WICHTIG · Debug ist ein Zustand, kein Ereignis

Das L7-Debug schaltet sich nicht von selbst ab. Wer es freitags einschaltet und montags vergisst, betreibt ab dann einen LoadMaster, der still Header mit Anmeldeinformationen ins Log schreibt und dafür Leistung verbrennt. Stelle die Stufe direkt nach der Reproduktion zurück auf No Debug und deaktiviere bei Bedarf auch das Extended Debug wieder. Ein Eintrag im Änderungsprotokoll schadet nicht, das Audit Log File führt ohnehin Buch.



Skizze: Ablauf für eine geplante Fehlersuche; im Störfall genauso, nur schneller

Was du im Trace suchst

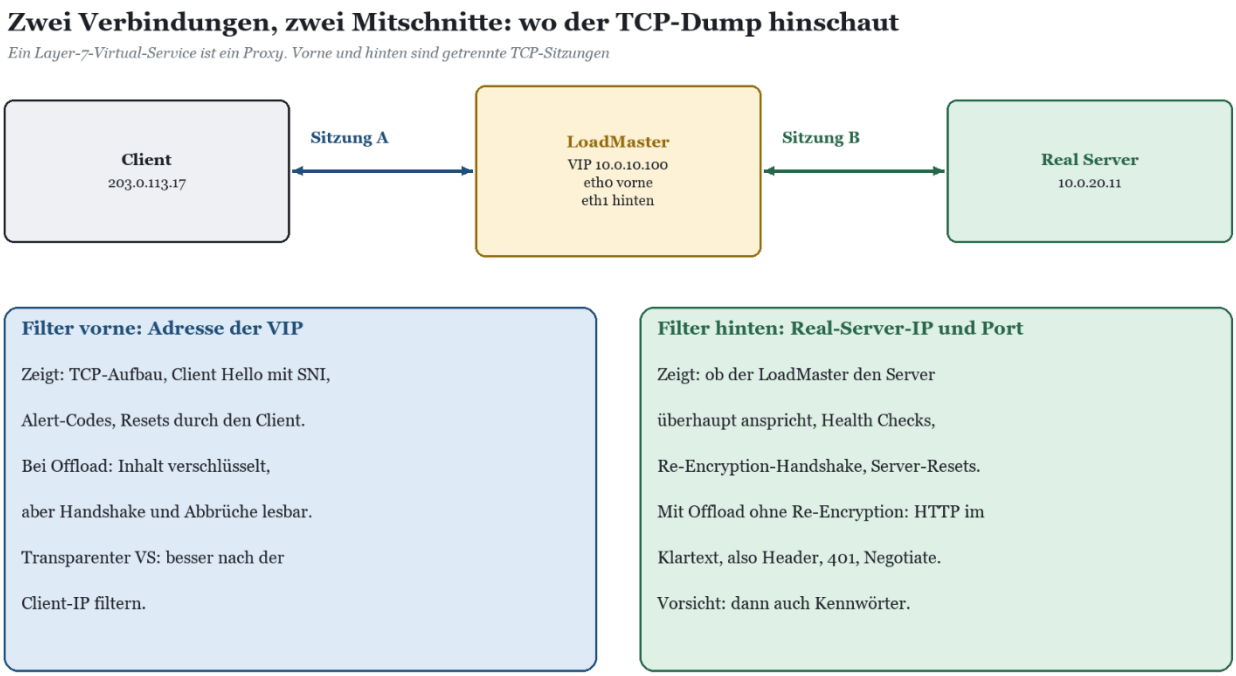
Ein L7-Trace ist kein Roman, sondern eine Abfolge technischer Zeilen. Du liest ihn mit einer Frage im Kopf. Wird überhaupt ein Real Server ausgewählt, und welcher? Greift eine Content Rule, die du nicht erwartet hast, etwa eine Umleitung, die den Pfad verändert? Schickt der Real Server einen 401 mit Negotiate zurück, obwohl das ESP eigentlich per KCD ein Ticket mitliefern sollte? Kommt vom Server ein Reset, oder beendet der LoadMaster selbst die Verbindung? Mit der Stufe Full Debug + HTTP Headers siehst du außerdem, ob der Host-Header beim Real Server so ankommt, wie die Anwendung ihn erwartet. Gerade bei Eigenentwicklungen, die auf http.sys-Reservierungen mit festem Hostnamen hören, ist das eine häufige Ursache.

Wenn der Trace zeigt, dass der Server mit 401 und WWW-Authenticate: Negotiate antwortet und danach ein NTLM-Austausch beginnt, hast du nebenbei ein Thema gefunden, das in vielen Umgebungen niemandem auffällt. Mehr dazu in NTLM, NTLM-Proxy und der Kerberos-Fallback, den keiner bemerkt.

TCP-Dump in der WUI: die Zeugin, die nicht lügt

Logs interpretieren. Ein Mitschnitt nicht. Wenn sich LoadMaster-Log, IIS-Log und Anwenderaussage widersprechen, ist der TCP-Dump die Instanz, die klärt, was tatsächlich auf der Leitung war. Der LoadMaster bringt dafür eine Mitschnittfunktion in der WUI mit, du brauchst also weder SSH noch ein separates Gerät am Spiegelport. Laut aktueller Progress-Dokumentation liegt sie unter System Configuration, Troubleshooting; ältere Anleitungen verorten sie bei den Debug Options der Logging Options. Je nach Firmware findest du sie an der einen oder anderen Stelle.

Die Bedienung ist schlicht: Interface wählen oder alle, optional Adresse und Port als Filter, Start, reproduzieren, Stop, Download. Heraus kommt eine .pcap-Datei, die du in Wireshark öffnest. Weitere tcpdump-Optionen sind laut Progress nur über die API erreichbar.



Skizze: Adressen aus Dokumentations- und Beispielbereichen; Interfaces je nach Bereitstellung

Richtig filtern: vorne, hinten oder beides

Weil ein Layer-7-Virtual-Service ein Proxy ist, gibt es zwei getrennte TCP-Verbindungen: Client zu LoadMaster und LoadMaster zu Real Server. Die Frage, wo du mitschneidest, ist die Frage, welche Hälfte du verdächtigst. Für nicht transparente Virtual Services empfiehlt Progress, nach der Adresse des Virtual Service zu filtern; bei transparenten Diensten ist die Client-IP der bessere Filter, weil sie auf beiden Seiten auftaucht. Was Transparenz und SNAT dabei mit den Adressen anstellen, erklärt Client-IP sichtbar machen: Transparenz, SNAT und X-Forwarded-For.

Verdacht	Filter	Worauf du in Wireshark achtest
TLS-Handshake scheitert beim Client	Adresse der VIP, Port 443	Client Hello mit SNI, Server Hello, Alert-Nachricht und deren Code
Real Server antwortet nicht	Adresse des Real Servers	SYN ohne SYN-ACK, Retransmissions, Reset vom Server
Re-Encryption scheitert	Real Server, Port 443	Handshake LoadMaster zu Server: Protokollversion, Cipher, Alert
Health Check lügt	Real Server, Port des Checks	Was fragt der Check an, was antwortet der Server wirklich?
Verbindungen brechen nach Minuten ab	Client-IP oder VIP	Zeitpunkt des FIN oder RST, Leerlaufzeit davor, wer beendet?
Kerberos zum DC	Adresse des DC, Port 88	TGS-REQ, KRB-ERROR mit Fehlercode, angefragter SPN

Grenzen, die man kennen sollte

Der Mitschnitt stoppt standardmäßig nach 10.000 Paketen oder 30 MB, je nachdem, was zuerst eintritt. Lauschst du auf zwei Interfaces, teilen sich beide den Speicher. Das reicht für eine gezielte Reproduktion locker, für „lass mal über Nacht laufen“ dagegen nicht. Wer über die API mehr Pakete erzwingt, schreibt nach Progress-Angaben in ein sehr kleines temporäres Verzeichnis. Läuft das voll, ist die WUI weg. Das ist die Sorte Fehlersuche, nach der man zwei Probleme hat.

Und dann ist da TLS. Vorne ist der Verkehr verschlüsselt, mit Re-Encryption auch hinten. Den Handshake, die SNI, die Zertifikatskette des Servers und den Alert-Code siehst du trotzdem, und genau das brauchst du bei Handshake-Fehlern. Den HTTP-Inhalt siehst du nur auf der Rückseite, wenn der LoadMaster per Offload unverschlüsselt zum Server spricht. Wenn du den Inhalt brauchst, ist das L7-Debug mit Headern meist das einfachere Werkzeug.

WARNUNG · Klartext heißt Klartext

Ein Mitschnitt der Rückseite bei reinem Offload enthält Formular-Anmeldungen, Basic-Auth-Header und Cookies im Klartext. Behandle die .pcap-Datei wie ein Kennwort-Export: kurz aufbewahren, nicht per Mail verschicken, nach der Analyse löschen. Teste wenn möglich mit einem eigenen Testkonto statt mit dem Konto der Geschäftsführung, das gerade „ganz dringend“ nicht geht.

Fehlerbilder und die erste Prüfung

Die folgende Tabelle ist kein Ersatz für Nachdenken, aber ein guter Startpunkt. Sie sortiert die Fehler, die vor Exchange, SharePoint, ADFS, RDS und Eigenentwicklungen am häufigsten auftauchen, nach dem, was der Client sieht, und nennt die Prüfung, die in der Praxis am schnellsten Klarheit bringt.

Fehlerbild	Wer antwortet meist?	Erste Prüfung	Typische Ursache
403 ohne IIS-Header	LoadMaster	WAF Event Log, dann ESP Security Log	WAF-Regel, Pfad nicht in den erlaubten virtuellen Verzeichnissen des ESP, Host nicht erlaubt
403.x mit IIS-Header	Real Server	IIS-Log mit Substatus	IP-Beschränkung, SSL-Pflicht, Berechtigung im Dateisystem
503, kein Server verfügbar	LoadMaster	Status der Real Server, System Message File	Alle Real Server down: Health Check falsch, Server wirklich weg, Wartung vergessen
503 mit IIS-Header	Real Server	IIS-Log, HTTPERR-Log, Anwendungspool	Anwendungspool gestoppt, http.sys-Warteschlange voll
Anmeldeschleife oder 401	Real Server nach ESP	ESP Logs, L7-Debug mit Headern, Ereignis 4769 am DC	KCD scheitert, SPN fehlt, falscher Verschlüsselungstyp
Kerberos-Fehler am DC	Domänencontroller	Ereignis 4769: Fehlercode, Ticket-Verschlüsselung	RC4-Keytab gegen AES-only-Domäne, Delegation unvollständig, Uhrzeit
TLS-Fehler im Browser	LoadMaster	Zertifikat am VS, TCP-Dump vorne	Falsches Zertifikat für die SNI, Zwischenzertifikat fehlt, Cipher Set zu streng
502 oder Abbruch nach Handshake	LoadMaster zum Server	TCP-Dump hinten, System Message File	Re-Encryption: Server spricht anderes TLS, Zertifikat am Server abgelaufen
Nur ein Teil der Benutzer betroffen	unklar	Statistik je Real Server, Persistence	Ein kranker Real Server, den der Health Check für gesund hält

403 vom LoadMaster: WAF oder ESP

Ein 403 ohne IIS-Spuren hat fast immer zwei Verdächtige. Die WAF blockt einen Request, der ihr verdächtig vorkommt, und das WAF Event Log nennt die Regel. Das ESP verweigert einen Pfad

oder Host, der nicht in seiner Positivliste steht: Ein Virtual Service mit ESP lässt nur die virtuellen Hosts und virtuellen Verzeichnisse durch, die du ausdrücklich erlaubt hast. Nach einem Exchange-Update, das einen neuen Pfad mitbringt, oder bei einer Eigenentwicklung, die plötzlich unter /api/v2/ antwortet, ist genau diese Liste der Schuldige. Prüfe sie, bevor du den Real Server verdächtigst.

503: keine gesunden Real Server

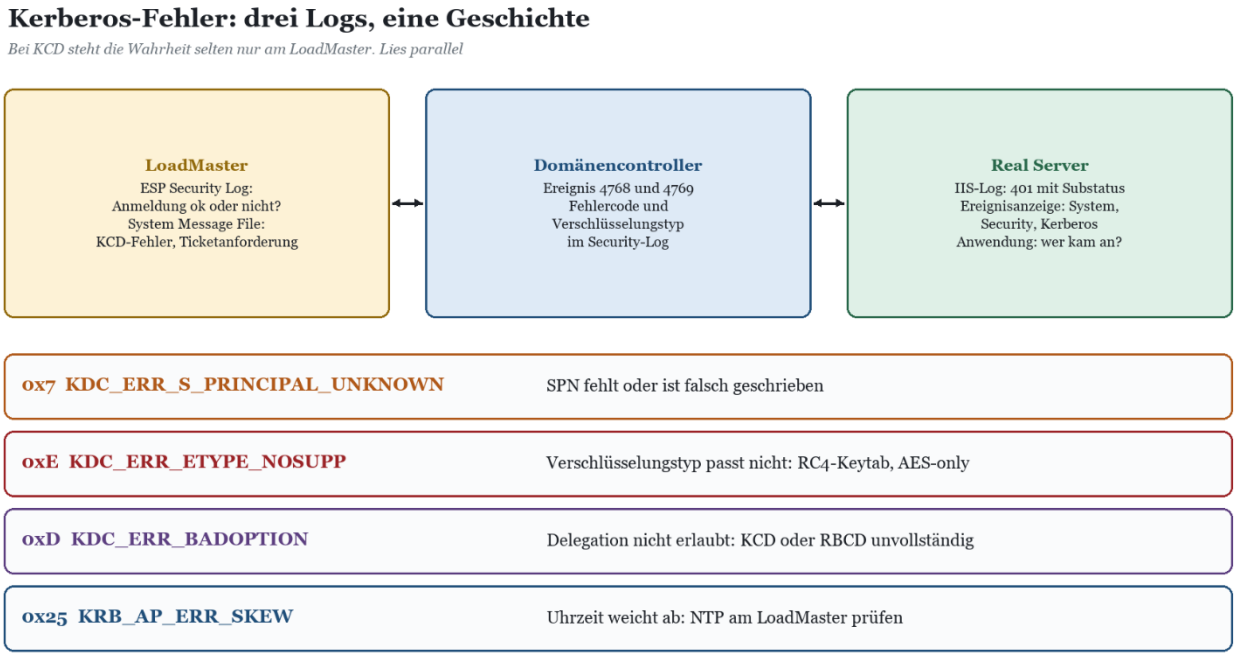
Wenn der LoadMaster keinen verfügbaren Real Server hat, kann er den Request nirgends hinschicken und antwortet selbst mit 503. Die Frage ist also nie „warum 503?“, sondern „warum sind alle Server down?“. Der Status in der Übersicht der Virtual Services und die Zustandswechsel im System Message File sagen dir, seit wann. Dann prüfst du den Health Check: Welche URL fragt er an, mit welchem Host-Header, welchen Statuscode erwartet er? Ein Check auf eine Seite, die nach einem Update eine Umleitung liefert, erklärt einen kompletten Ausfall, obwohl alle Server kerngesund sind. Den umgekehrten Fall, den kranken Server mit grünem Status, entdeckst du über die Statistik und den direkten Test am Real Server.

TIPP · Freundliche 503 statt nackter Fehlerseite

Der LoadMaster kann für den Fall, dass kein Real Server verfügbar ist, eine Umleitung oder eine eigene Fehlermeldung ausliefern. Eine Wartungsseite mit Telefonnummer reduziert die Anrufe im Störfall erheblich. Und sie hat einen Nebeneffekt für dich: Wer diese Seite sieht, hat eindeutig den LoadMaster erreicht, und alle Real Server sind down.

Kerberos-Fehler: parallel lesen

Kerberos Constrained Delegation am LoadMaster bedeutet, dass der LoadMaster im Namen des Benutzers ein Service-Ticket für den Real Server anfordert. Scheitert das, sieht der Benutzer eine Anmeldeschleife oder einen 401, und das ESP Security Log meldet bestenfalls, dass die Delegation nicht klappte. Die eigentliche Begründung steht am Domänencontroller: Ereignis 4769 im Security-Log mit Fehlercode, angefragtem SPN und Verschlüsselungstyp. Wer die drei Quellen nebeneinanderlegt, LoadMaster, DC und Real Server, ist meist nach zehn Minuten fertig. Wer nur am LoadMaster sucht, ist es nach zehn Stunden noch nicht.



Skizze: häufige Kerberos-Fehlercodes aus Ereignis 4769; Liste nicht vollständig

Der Fehlercode 0xE, KDC_ERR_ETYPE_NOSUPP, ist in Domänen, die RC4 abgeschaltet haben, der Dauerbrenner: Das Keytab des LoadMasters enthält nur einen RC4-Schlüssel, die Domäne verlangt AES. Die Geschichte dieses Fehlers erzählt Die RC4-Falle: KCD-Keytab trifft AES-only-Domäne. Fehlt der SPN oder ist er doppelt vergeben, hilft SPN-Probleme hinter dem Load Balancer: ein Name, mehrere Server, und für die Einrichtung von KCD und RBCD selbst gibt es Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten. Die Grundlagen zu Tickets, Delegation und Verschlüsselungstypen aus Microsoft-Sicht sammelt der Bereich Microsoft Kerberos.

FAKTEN · Ereignis 4769 richtig lesen

Ereignis 4769 protokolliert Anforderungen von Service-Tickets am Domänencontroller. Interessant sind das Feld Failure Code und die Ticket Encryption Type. 0x17 steht für RC4, 0x12 für AES256. Wenn erfolgreiche Tickets mit 0x17 ausgestellt werden, obwohl du AES-only planst, hast du ein Problem, das erst beim nächsten Härtungsschritt explodiert. Damit das Ereignis erscheint, muss die Überwachung der Kerberos-Dienstickets aktiviert sein.

TLS-Handshake: vorne oder hinten?

Bei TLS-Fehlern lautet die erste Frage: Scheitert der Handshake zwischen Client und LoadMaster oder zwischen LoadMaster und Real Server? Zeigt der Browser eine Zertifikatswarnung oder bricht er mit einem Protokollfehler ab, liegt es vorne: falsches Zertifikat für den angefragten Hostnamen, eine fehlende Zwischenzertifizierungsstelle oder ein Cipher Set, das ältere Clients aussperrt. Ein Mitschnitt auf der VIP zeigt das Client Hello mit SNI und den Alert, den eine Seite schickt. Kommt der Browser dagegen sauber durch und erst danach kommt ein Fehler, liegt das Problem bei Re-Encryption hinten, etwa weil der Real Server nach einer Härtung nur noch TLS 1.3 spricht oder sein Zertifikat abgelaufen ist. Die Hintergründe zu Offload, Re-Encryption und Zertifikatsketten stehen in TLS-Offload, Re-Encryption und Zertifikate: PKI trifft LoadMaster.

FAQ: Troubleshooting am Kemp LoadMaster

Woran erkenne ich, ob der LoadMaster oder der Real Server geantwortet hat?

An den Antwort-Headern. IIS, Exchange und SharePoint setzen typische Header wie Server, X-FEServer oder SPRequestGuid. Fehlen diese und die Fehlerseite ist schlicht, war es meist der LoadMaster. Zur Gegenprobe sprichst du den Real Server mit curl und --resolve direkt an.

Wo finde ich die ESP-Logs?

Nicht im System Message File, sondern unter den Extended Log Files in den Logging Options. Werden die ESP-Logs an einen Remote-Syslog gesendet, ist die lokale Protokollierung abgeschaltet, dann suchst du im Syslog-System.

Darf ich das L7-Debug im Produktivbetrieb einschalten?

Kurz und gezielt ja, am besten als Extended L7 Debug auf einem Virtual Service und auf deine Test-Client-IP eingeschränkt. Das globale L7-Debug kostet Leistung, flutet das Log und kann Anmeldeinformationen sichtbar machen. Danach sofort zurück auf No Debug.

Warum sehe ich im TCP-Dump keinen HTTP-Inhalt?

Weil die Verbindung verschlüsselt ist. Vorne siehst du immer nur TLS, hinten nur dann Klartext, wenn der LoadMaster ohne Re-Encryption zum Server spricht. Für Header ist das L7-Debug mit der Stufe Full Debug + HTTP Headers meist der einfachere Weg.

Wie lange läuft ein TCP-Dump in der WUI?

Bis du ihn stoppst, höchstens aber bis 10.000 Pakete oder 30 MB erreicht sind. Beim Mitschnitt auf zwei Interfaces teilen sich beide den Speicher. Für längere Mitschnitte ist ein Spiegelport oder eine Messung am Server sinnvoller.

Der LoadMaster liefert 503, aber die Server laufen. Was nun?

Dann hält der Health Check die Server für tot. Prüfe URL, Host-Header und erwarteten Statuscode des Checks und sieh im System Message File nach, seit wann die Server down sind. Häufig liefert die geprüfte Seite nach einem Update eine Umleitung statt 200.

Wie finde ich heraus, wer eine Einstellung geändert hat?

Im Audit Log File. Es protokolliert Aktionen über WUI und API, setzt aber voraus, dass Session Management aktiviert ist. Ohne das bleibt nur die Erinnerung der Kolleginnen und Kollegen, und die ist im Störfall erfahrungsgemäß lückenhaft.

Was schicke ich dem Progress-Support?

Das Archiv aus Save Logs, eine Beschreibung mit Uhrzeit der Reproduktion, die betroffene Client-IP und bei Bedarf eine .pcap-Datei. Schwärze vorher, was personenbezogen ist, und kläre den Versand mit dem Datenschutz.

Fazit: Erst den Täter bestimmen, dann die Spuren sichern

Troubleshooting am LoadMaster ist weniger eine Frage der Werkzeuge als der Reihenfolge. Wer zuerst klärt, ob der LoadMaster oder der Real Server geantwortet hat, spart sich die Hälfte der Suche. Danach liest du das Log, das zur Station passt: System Message File für Real-Server-Status und Layer-7-Engine, ESP-Logs für Anmeldungen, WAF Event Log für 403 ohne IIS-Spuren, Ereignis 4769 am Domänencontroller für alles mit Kerberos. Erst wenn die Logs nicht reichen, kommen Extended L7 Debug und TCP-Dump, gezielt auf einen Virtual Service und eine Client-IP, mit festem Anfang und festem Ende.

Der Rest ist Vorbereitung: NTP am LoadMaster, Syslog an ein zentrales System, ein eigener Header für den Knotennamen, ein Testkonto, das niemandem gehört, und eine Wartungsseite für den 503. Dann ist der nächste Anruf kurz vor Feierabend zwar immer noch lästig, aber er dauert zwanzig Minuten statt einen Abend. Und der LoadMaster bekommt nur noch dann die Schuld, wenn er sie auch verdient hat.

TIPP · Unterstützung bei der Fehlersuche

Wenn ein Fehler sich hartnäckig zwischen LoadMaster, Active Directory und Exchange versteckt, hilft die Beratung zum Kemp LoadMaster. Wer den Fehlerweg mit dem eigenen Team an absichtlich kaputten Laborumgebungen üben möchte, findet das in der Kemp-LoadMaster-Schulung.

WEITERLESEN · Weiter im Thema

› Health Checks, die wirklich prüfen: warum „Port 443 offen“ nicht reicht
› Edge Security Pack: Vorauthentifizierung, SSO-Domänen und der TMG-Ersatz
› Die RC4-Falle: KCD-Keytab trifft AES-only-Domäne
› Web Application Firewall und Geoblocking am LoadMaster: Schutz ohne Fehlalarm-Hölle
› Monitoring, Syslog und SNMP: den LoadMaster ins Monitoring holen
› TLS-Offload, Re-Encryption und Zertifikate: PKI trifft LoadMaster