Monitoring, Syslog und SNMP: den LoadMaster ins Monitoring holen



Skizze: vier Kanäle, über die der LoadMaster Auskunft gibt

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

BERATUNG
Dein LoadMaster läuft, aber keiner merkt, wenn er es nicht mehr tut? Wir bauen mit dir Syslog, SNMP und Alarmierung, die nur dann klingelt, wenn es zählt.
› **Beratung zum Kemp LoadMaster**

SCHULUNG
Betrieb und Monitoring im Labor üben: Real Server abschießen, HA-Wechsel provozieren, Alarme auswerten. Absichtlich, nicht nachts um drei.
› **Kemp-LoadMaster-Schulung**

Es gibt zwei Arten, von einem Ausfall zu erfahren. Die eine ist eine Meldung im Monitoring, nüchtern, mit Zeitstempel, zehn Minuten bevor jemand etwas merkt. Die andere ist der Anruf aus dem Vorzimmer, warum Outlook seit dem Mittagessen „so komisch“ ist. Die zweite Variante ist erstaunlich verbreitet, denn sie funktioniert ohne jede Konfiguration. Sie hat nur einen Haken: Sie meldet grundsätzlich zu spät, und sie meldet nie, was eigentlich kaputt ist.

Der LoadMaster ist in diesem Spiel ein besonders verschwiegener Kandidat. Er weiß genau, welcher Real Server seit drei Stunden aus dem Pool geflogen ist, dass der Standby-Knoten nicht mehr synchronisiert, dass das Zertifikat für den Exchange-Namespace in elf Tagen abläuft und wer gestern Nachmittag eine Content Rule geändert hat. Er schreibt das alles brav in sein lokales Log. Und dort bleibt es, bis ein Firmware-Update oder ein voller Puffer es gnädig entsorgt. Zwischen „der LoadMaster weiß es“ und „du weißt es“ liegen Syslog, SNMP und E-Mail-Benachrichtigungen, und genau die richtest du in vielen Umgebungen erst nach dem ersten peinlichen Ausfall ein.

Dieser Beitrag aus der Serie zum Kemp LoadMaster erklärt, welche Kanäle der LoadMaster anbietet, wie du sie in eine Microsoft-lastige Umgebung mit SIEM und klassischem Monitoring einhängst und vor allem, welche Ereignisse wirklich jemanden wecken sollten. Denn das zweithäufigste Monitoring-Problem nach „gar keins“ ist „zu viel“: ein Postfach mit 4.000 ungelesenen Alarmen, die alle auf eine Regel zeigen, die längst niemand mehr liest.

FAKTEN · Das Wichtigste in 30 Sekunden

Der LoadMaster sendet Syslog nach RFC 5424 an bis zu zehn Ziele. Jedes Ziel bekommt eine Severity und hört alles ab dieser Stufe aufwärts.

Für Syslog stehen UDP, TCP und TLS zur Wahl. Für ein SIEM, das Sicherheitsereignisse auswerten soll, ist UDP die schlechteste Wahl.

SNMP ist ab Werk aus, Traps ebenfalls. Mit SNMPv3 nutzt du SHA und AES, MD5 und DES gelten auch beim Hersteller als veraltet.

E-Mail-Benachrichtigungen kennen sechs Stufen mit eigenen Empfängerlisten. Wer bei Error eingetragen ist, bekommt automatisch auch Critical und Emergency.

Kein Kanal ersetzt die Außensicht: Ein Check gegen den Virtual Service mit Zertifikatsprüfung fängt Fehler, die der LoadMaster selbst für völlig normal hält.

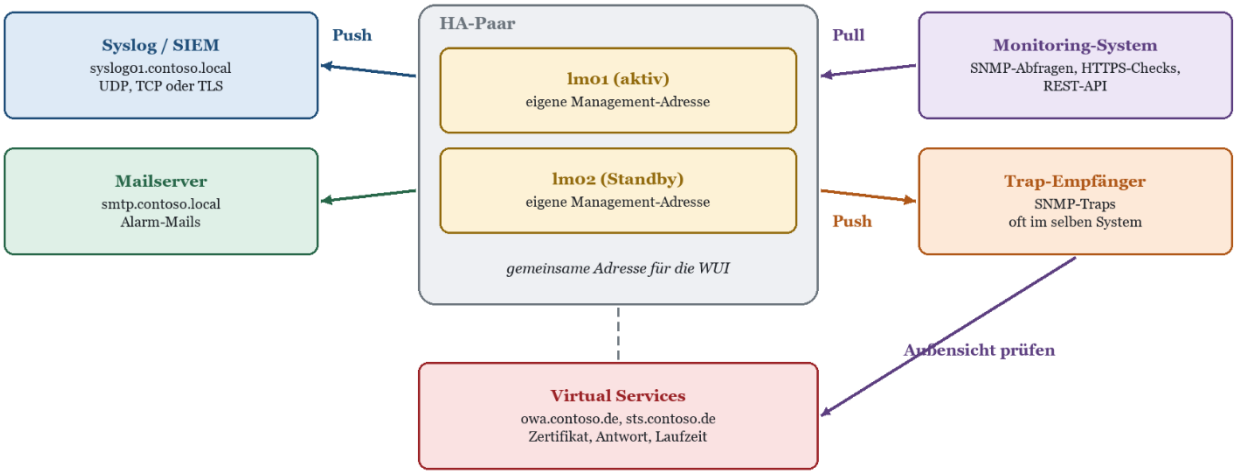
Vier Kanäle, ein Gerät: was der LoadMaster von sich gibt

Bevor du irgendetwas konfigurierst, lohnt der Blick auf das Prinzip. Der LoadMaster kennt zwei Richtungen. Bei Syslog, SNMP-Traps und E-Mail meldet er sich von selbst, sobald etwas passiert. Das ist Push. Bei SNMP-Abfragen und bei der REST-API fragt dein Monitoring-System regelmäßig nach, wie es ihm geht. Das ist Pull. Beides hat seinen Platz, und beides hat eine Schwäche, die das jeweils andere ausgleicht.

Push ist schnell und kennt den Grund: „Real Server 10 im Virtual Service Exchange-HTTPS ist down“ steht im Syslog, sobald es passiert. Push hat aber ein fundamentales Problem: Ein Gerät, das tot ist, meldet nichts mehr. Ein abgestürzter LoadMaster schickt keine letzte Syslog-Nachricht mit Entschuldigung. Pull dagegen merkt genau das, weil die Antwort ausbleibt, weiß aber nur, was es abfragt. Ein vernünftiges Monitoring kombiniert also beides: Pull für „lebt er noch und wie geht es ihm“, Push für „was genau ist passiert“.

Wer redet mit wem: die Monitoring-Architektur um ein HA-Paar

Push-Kanäle gehen vom LoadMaster weg, Pull-Kanäle kommen von außen



Merksätze zur Skizze

- SNMP fragst du an beiden Knoten einzeln ab, sonst weißt du nie, wer gerade spricht.
- Syslog und Mail kommen je nach Knoten von dessen Adresse. Der Filter im SIEM muss beide kennen.
- Die Außensicht auf den Virtual Service ersetzt keiner der vier Kanäle. Sie ergänzt sie.

Skizze: Namen aus der Beispieldomäne; Adressen und Ports abhängig von deiner Umgebung

Kanal	Richtung	Stärke	Schwäche	Typischer

				Empfänger
Syslog	Push	Detailreich, jede Meldung mit Zeitstempel und Hostname, ideal für Korrelation	Totes Gerät schweigt, UDP verliert still	SIEM, zentraler Syslog-Server
SNMP-Abfrage	Pull	Erkennt Ausfälle, liefert Zähler und Zustände über die MIBs	Nur so schlau wie die abgefragten OIDs, kostet laut Hersteller spürbar Leistung	Netzwerk- und Server-Monitoring
SNMP-Trap	Push	Sofortige Meldung wichtiger Ereignisse an das Monitoring	Ab Werk aus, UDP-basiert, braucht MIB-Import zum Übersetzen	Trap-Empfänger im Monitoring
E-Mail	Push	Ohne weitere Infrastruktur nutzbar, sechs Stufen mit eigenen Empfängern	Postfächer sind kein Alarmsystem, Mailserver kann selbst betroffen sein	Team-Postfach, Ticketsystem
REST-API	Pull	Statistik und Konfiguration maschinenlesbar, gut für Skripte	Eigenbau, Zugangsdaten müssen sicher verwahrt werden	PowerShell-Skript, Monitoring-Plug-in

Warum die Außensicht trotzdem Pflicht bleibt

Alle vier Kanäle beschreiben die Welt aus Sicht des LoadMasters. Und der hält manches für gesund, was für deine Benutzerinnen und Benutzer längst kaputt ist. Ein Health Check, der nur prüft, ob Port 443 offen ist, meldet einen Exchange-Server als gesund, dessen OWA-Anwendungspool seit Stunden nur noch Fehlerseiten produziert. Ein abgelaufenes Zertifikat am Virtual Service ist für den LoadMaster kein Fehler, er liefert es einfach weiter aus. Warum der Health Check selbst der erste Ansatzpunkt ist, erklärt Health Checks, die wirklich prüfen: warum „Port 443 offen“ nicht reicht.

Deshalb gehört zu jedem wichtigen Virtual Service mindestens ein synthetischer Check aus deinem Monitoring-System: HTTPS-Abruf auf den echten Namen, zum Beispiel owa.contoso.de, mit Prüfung von Statuscode, einem Stück erwartetem Inhalt und der Restlaufzeit des Zertifikats. Wenn möglich von einem Standort außerhalb des eigenen Netzes, damit auch Firewall, DNS und Internetanbindung mitgeprüft werden. Das ist der Teil des Monitorings, der dem Vorzimmer-Anruf am nächsten kommt, nur zehn Minuten früher.

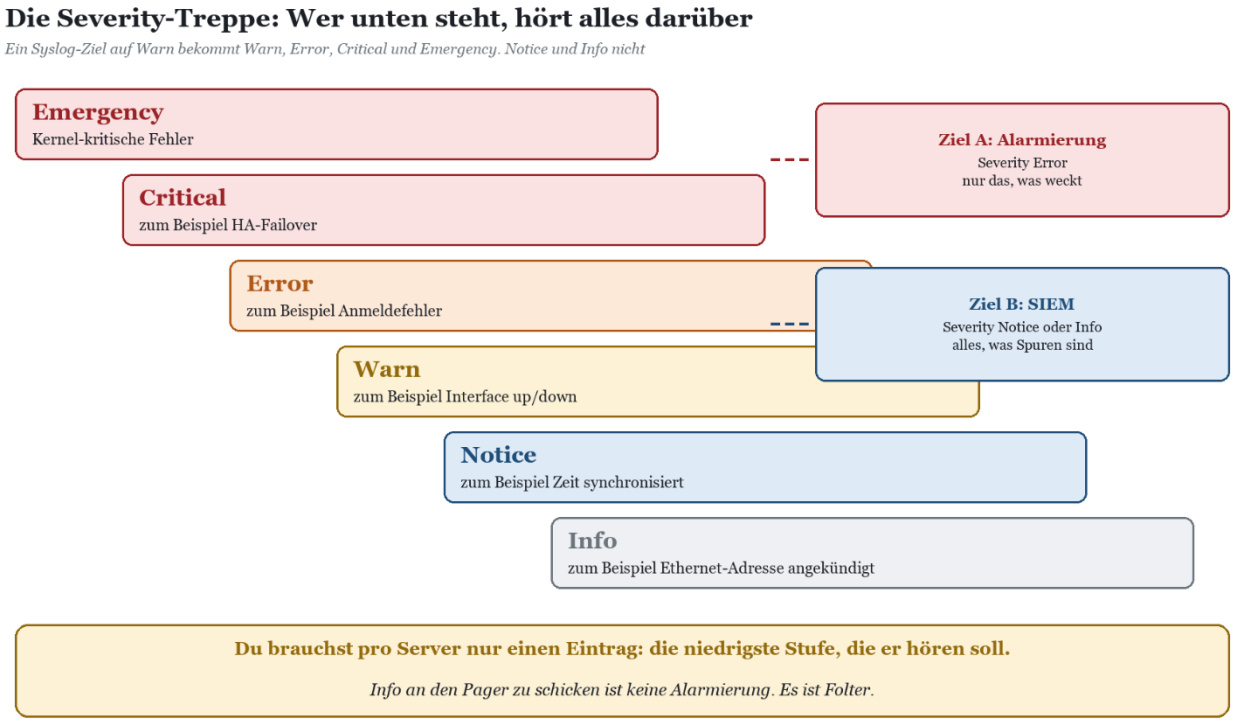
> **TIPP · Knotenname im Antwort-Header**
>
> Wenn du per Content Rule einen eigenen Header mit dem Namen des antwortenden Real Servers setzt, kann der synthetische Check ihn mitprotokollieren. Dann siehst du im Verlauf, ob plötzlich alle Anfragen auf einem einzigen Server landen. Das ist oft der erste Hinweis darauf, dass seine Kollegen still aus dem Pool gefallen sind.

Kemp Syslog an zentralen Server oder SIEM

Syslog ist der wichtigste Kanal, weil er am meisten erzählt. Der LoadMaster erzeugt Meldungen im Format nach RFC 5424, also mit vollständigem Zeitstempel und dem Hostnamen des Geräts. Lokal speichert er sie ohnehin. Die Kunst besteht darin, sie rechtzeitig dorthin zu schicken, wo sie länger leben als bis zum nächsten Neustart und wo sie neben den Logs von Domänencontrollern, Exchange und Firewall liegen.

Ziele, Stufen und die Treppe nach oben

In den Syslog-Optionen der WUI trägst du die Adresse eines Syslog-Hosts ein, wählst eine Severity und fügst ihn hinzu. Bis zu zehn Ziele sind möglich. Die Severity wirkt wie eine Treppe: Ein Ziel mit Warn erhält Warn und alles Wichtigere, also Error, Critical und Emergency. Du brauchst pro Ziel deshalb nur einen einzigen Eintrag mit der niedrigsten Stufe, die es hören soll. Trägst du dieselbe Adresse noch einmal ein, ersetzt das den vorhandenen Eintrag. Und gelöscht wird ein Ziel, indem du seine Severity auf None setzt, was beim ersten Mal ungefähr so intuitiv ist wie ein Notausgang hinter einer Tür mit der Aufschrift „Abstellraum“.



Skizze: Stufen und Beispiele nach der Beschreibung der Syslog-Optionen in der LoadMaster-WUI

Stufe	Beispiel laut Hersteller	Wofür du sie nutzt
Emergency	Kernel-kritische Fehler	Nur im Paket mit allem darüber relevant
Critical	HA-Failover	Untergrenze für Alarmierung außerhalb der Geschäftszeit
Error	Anmeldefehler	Untergrenze für ein Alarm- oder Ticketziel
Warn	Interface up oder down	Sinnvoll für Betriebsüberwachung tagsüber
Notice	Zeit synchronisiert	Untergrenze für ein SIEM mit Speicherbedarf im Blick
Info	Lokal angekündigte Ethernet-Adresse	SIEM oder Archiv, wenn du wirklich alles willst

Die Beispiele zeigen ein Detail, das gern übersehen wird: Ein Anmeldefehler ist Error, ein HA-Wechsel Critical. Welche Stufe ein „Real Server down“ bekommt, solltest du nicht raten, sondern ausprobieren. Nimm im Wartungsfenster einen Real Server aus dem Pool oder stoppe auf ihm den IIS und schau nach, mit welcher Severity und welchem Text die Meldung im Syslog ankommt. Danach baust du die Filterregel im SIEM auf diesen Text, nicht auf deine Vermutung.

UDP, TCP oder TLS: Transport mit Folgen

Klassisch geht Syslog per UDP an Port 514. Das ist schnell, einfach und hat die charmante Eigenschaft, Nachrichten ohne jede Rückmeldung zu verlieren, wenn Netz oder Empfänger kurz

ausgelastet sind. Für eine reine Betriebsübersicht ist das verschmerzbar. Für ein SIEM, das Anmeldeversuche am Edge Security Pack oder Treffer der WAF auswerten soll, ist es eine Einladung zu Lücken in genau den Minuten, in denen es spannend wird.

Der LoadMaster bietet deshalb neben UDP auch TCP und TLS an. Neuere Firmware hat dafür eine eigene Auswahl des Protokolls. In älteren Ständen hing das Verhalten am Port: ohne eigene Angabe UDP 514, Port 601 bedeutete TCP, jeder andere Port verschlüsseltes TCP. Prüfe auf deinem Gerät, welche Variante deine Firmware zeigt, statt dich auf ein altes Handbuch zu verlassen. Bei TLS kann der LoadMaster zusätzlich prüfen, ob der Name oder die Adresse, über die er den Syslog-Server anspricht, im Zertifikat steht. Diese Prüfung ist ab Werk aus. Schalte sie ein, sobald dein Syslog-Server ein Zertifikat aus deiner internen PKI mit passendem Subject Alternative Name hat.

Transport	Zuverlässigkeit	Vertraulichkeit	Empfehlung
UDP	Keine Zustellbestätigung, Verluste bleiben unbemerkt	Klartext im Netz	Nur für unkritische Betriebsmeldungen im eigenen Management-Netz
TCP	Verbindungsorientiert, Verluste werden seltener	Klartext im Netz	Brauchbar im getrennten Management-Netz
TLS	Wie TCP	Verschlüsselt, auf Wunsch mit Prüfung des Servernamens	Standard für SIEM und alles über Netzgrenzen hinweg

WARNUNG · Was im Syslog steht, ist manchmal ziemlich persönlich

Anmeldemeldungen des ESP enthalten Benutzernamen, WAF-Meldungen Client-Adressen und Teile von Anfragen. Damit sind die Logs personenbezogene Daten. Kläre Speicherdauer, Zugriffsrechte und Zweck mit dem Datenschutz und, in Verwaltungen und vielen Unternehmen, mit dem Personal- oder Betriebsrat, bevor das SIEM jahrelang alles aufhebt. Ein Log, das niemand lesen darf, ist zwar sicher, aber auch ziemlich sinnlos.

Präfix, Zeit und Hostname: damit das SIEM weiß, wer spricht

Zwei Details entscheiden, ob du später im SIEM sauber suchen kannst. Erstens die Zeit. Ein LoadMaster ohne NTP läuft gemächlich vor oder nach, und dann liegen seine Meldungen zum HA-Wechsel drei Minuten neben den Ereignissen der Exchange-Server. Korrelation wird so zu Kaffeesatzlesen. Trag als NTP-Quelle dieselben Server ein, die auch deine Domänencontroller nutzen, oder gleich die Domänencontroller selbst.

Zweitens die Herkunft. Der Hostname steht in jeder Meldung, aber ein Name wie lm01 sagt im SIEM wenig, wenn es drei Standorte mit je einem lm01 gibt. Der LoadMaster kennt dafür ein frei wählbares Präfix von bis zu 80 Zeichen, das vor jede Syslog-Meldung gesetzt wird. Ein Präfix wie LM-DMZ-FFM macht im SIEM aus einer anonymen Zeile eine eindeutige Quelle, auch wenn jemand später die Hostnamen vereinheitlicht.

ESP- und WAF-Logs: die eigentlich spannenden Meldungen

Edge Security Pack und Web Application Firewall führen eigene Logs, die nicht im allgemeinen System Message File landen. Gerade sie interessieren das SIEM aber am meisten: gescheiterte Anmeldungen vor OWA, Kontosperrungen durch Passwort-Spraying, WAF-Treffer gegen die Exchange-Pfade. Beide lassen sich an einen Remote-Syslog weitergeben. Beachte dabei, dass die lokale Protokollierung der ESP-Logs abgeschaltet wird, wenn du sie an einen entfernten Syslog sendest. Wer danach am LoadMaster im lokalen Log sucht, findet dort nichts und zweifelt an

seinem Verstand. Wo die einzelnen Logs liegen und wie du sie im Störfall liest, beschreibt Troubleshooting am LoadMaster: Logs, L7-Debug und TCP-Dump.

Für die Korrelation im SIEM ist außerdem die echte Client-Adresse entscheidend. Arbeitet der Virtual Service ohne Transparenz, sehen die IIS-Logs und die Windows-Ereignisse nur die Adresse des LoadMasters. Dann ist das LoadMaster-Log die einzige Stelle, an der die ursprüngliche Adresse steht, und dein SIEM muss beide Quellen zusammenführen. Wie du die Client-IP bis zum Server durchreichst, steht in Client-IP sichtbar machen: Transparenz, SNAT und X-Forwarded-For.

Anbindung an Microsoft Sentinel und andere SIEM-Systeme

Windows Server bringt keinen eigenen Syslog-Empfänger mit. In Microsoft-Umgebungen führt der Weg deshalb meist über einen kleinen Linux-Server, der Syslog annimmt und weiterleitet. Für Microsoft Sentinel ist das der Azure Monitor Agent auf einem Linux-Forwarder, der Syslog in einen Log-Analytics-Arbeitsbereich schreibt. Bei anderen SIEM-Systemen übernimmt ein Kollektor des Herstellers dieselbe Rolle. Der Ablauf ist immer gleich: LoadMaster sendet an den Kollektor, Kollektor normalisiert und leitet weiter, das SIEM parst die Felder.

Der aufwendigste Teil ist das Parsen. Die Meldungen des LoadMasters sind nicht in einem standardisierten Sicherheitsformat wie CEF gehalten, sondern Text. Plane daher Zeit für eigene Parser oder Abfragen ein, die aus der Textzeile Virtual Service, Real Server, Benutzername und Client-Adresse extrahieren. Wer das überspringt, hat am Ende ein SIEM, das alles speichert und nichts versteht.

AUS DER PRAXIS · Das SIEM, das nie etwas fand

In einer Verwaltung lief das LoadMaster-Syslog seit zwei Jahren per UDP ins SIEM. Als ein Passwort-Spraying gegen OWA aufgearbeitet werden sollte, stellte sich heraus, dass der Kollektor die Zeilen zwar annahm, aber einer generischen Quelle ohne Parser zuordnete. Zwei Jahre Logs, null durchsuchbare Felder. Die eigentliche Arbeit war danach nicht die Technik, sondern eine Stunde mit fünf Testanmeldungen, die zeigte, welche Zeile was bedeutet.

SNMP: Abfragen, Traps und die MIBs

SNMP ist das Werkzeug der klassischen Monitoring-Systeme. Sie fragen in festen Abständen Werte ab, zeichnen Verläufe auf und schlagen Alarm, wenn ein Wert eine Schwelle reißt oder eine Antwort ausbleibt. Am LoadMaster ist SNMP ab Werk ausgeschaltet. Die WUI warnt beim Einschalten ausdrücklich vor einem spürbaren Leistungseinfluss. Das ist kein Grund, darauf zu verzichten, aber ein guter Grund, das Abfrageintervall nicht auf zehn Sekunden zu stellen und nicht jede verfügbare Tabelle bei jedem Durchlauf komplett zu laden.

v2c oder v3: Community ist kein Kennwort

Mit SNMP v1 und v2c identifiziert sich dein Monitoring über eine Community, die im Klartext über das Netz geht. Die Voreinstellung lautet, wie bei so vielen Geräten, public. Wer sie so lässt, hat nicht SNMP eingerichtet, sondern einen öffentlichen Aushang. Schränke bei v2c mindestens die zugelassenen SNMP-Clients auf die Adressen deines Monitorings ein, denn ohne Eintrag nimmt der LoadMaster Anfragen von jedem Host an.

Besser ist SNMPv3. Dort gibt es Benutzer, ein Authentifizierungskennwort mit mindestens acht Zeichen und optional Verschlüsselung. Als Authentifizierung bietet der LoadMaster MD5 und SHA an, als Verschlüsselung DES und AES. Der Hersteller selbst nennt MD5 und DES veraltet. Die Entscheidung ist also schnell getroffen: SHA und AES, mit eingeschalteter Privacy. Beachte, dass mit SNMPv3 die Felder für Community und SNMP-Clients verschwinden. Den Zugriff beschränkst du dann zusätzlich über die Firewall vor der Management-Schnittstelle.

Merkmal	SNMP v2c	SNMPv3
Identifikation	Community, ab Werk public	Benutzername und Kennwort
Schutz der Daten	Keiner, alles im Klartext	Authentifizierung mit SHA, Verschlüsselung mit AES
Zugriffsbeschränkung am Gerät	Liste der SNMP-Clients	Benutzer, zusätzlich Firewall
Einsatz	Nur im abgeschotteten Management-Netz	Standard für neue Installationen
Typischer Fehler	public bleibt public	MD5 und DES aus Bequemlichkeit

MIBs: ohne Wörterbuch nur Zahlenkolonnen

Damit dein Monitoring-System mit den Antworten etwas anfangen kann, braucht es die MIB-Dateien des LoadMasters. Der Hersteller liefert vier: ONE4NET-MIB für die Enterprise-Kennung, IPVS-MIB für die Statistik der Virtual Services, B-100-MIB für Konfigurationsdaten und CERTS-MIB für Informationen zu den TLS-Zertifikaten. Importiere alle vier, bevor du Sensoren anlegst. Ohne sie siehst du OIDs wie lange Telefonnummern und musst raten, welche davon der Zustand eines Real Servers ist.

Gängige Systeme wie Checkmk, Zabbix, PRTG oder System Center Operations Manager unterscheiden sich in der Bedienung, nicht im Prinzip. Du legst den LoadMaster als SNMP-Gerät an, importierst die MIBs, wählst die Werte aus und definierst Schwellen. Manche Systeme bringen fertige Vorlagen für den LoadMaster mit, andere nicht. Prüfe fertige Vorlagen trotzdem kritisch, denn sie stammen oft aus der Zeit, als das Gerät noch anders hieß, und fragen gern Werte ab, die niemand braucht, während der wichtigste fehlt.

Was du abfragst	Warum	Sinnvolle Schwelle
Erreichbarkeit beider Knoten	Erkennt ausgefallenen Standby, den kein Benutzer bemerkt	Sofort, nach zwei verpassten Abfragen
Zustand je Real Server	Erkennt Server, die still aus dem Pool fallen	Einzelner Server: Ticket; alle Server eines VS: Alarm
Verbindungen je Virtual Service	Zeigt Lastspitzen und plötzliche Einbrüche	Abweichung vom üblichen Verlauf statt fester Zahl
CPU und Arbeitsspeicher	Sizing-Grenzen werden sichtbar, bevor es knirscht	Dauerhaft über 80 Prozent über längere Zeit
Zertifikate aus CERTS-MIB	Ergänzt den externen Zertifikatscheck	Staffel ab 90 Tagen
Schnittstellen	Erkennt Link-Verlust in Bond- oder HA-Netzen	Jeder Statuswechsel

Traps: wenn der LoadMaster selbst anruft

Traps sind die Push-Variante von SNMP. Sind sie eingeschaltet und ist mindestens ein Empfänger eingetragen, meldet der LoadMaster wichtige Ereignisse zum Gerät, zu Virtual Services und zu Real Servern von sich aus. Auch Traps sind ab Werk aus. Für die Empfänger gibt es zwei Listen: Trap Sink1 für SNMPv1-Traps, Trap Sink2 für SNMPv2-Traps, jeweils mit Leerzeichen getrennte Adressen. Moderne Monitoring-Systeme verstehen v2-Traps besser, trag dein System also dort ein.

Im HA-Betrieb erscheint zusätzlich eine Option, die Traps von der gemeinsamen Adresse statt von der Adresse des gerade aktiven Knotens zu senden. Das klingt praktisch, ist aber eine Geschmacksfrage: Mit der gemeinsamen Adresse landen alle Traps an einem Objekt im

Monitoring, dafür weißt du nicht mehr direkt, welcher Knoten sie geschickt hat. Mit der Knotenadresse siehst du das sofort, musst aber beide Knoten als Trap-Quelle anlegen. Wir empfehlen die Knotenadresse, weil nach einem Failover genau die Frage „wer ist jetzt aktiv“ zählt.

WICHTIG · Traps sind UDP und damit ein Versprechen ohne Garantie

Ein Trap, der unterwegs verloren geht, ist weg. Es gibt keine Wiederholung und keinen Hinweis. Verlass dich bei kritischen Zuständen deshalb nie allein auf den Trap. Die regelmäßige Abfrage des Zustands ist das Sicherheitsnetz, der Trap nur die Abkürzung.

E-Mail-Benachrichtigungen und die Ereignisse, die wirklich zählen

E-Mail: einfach, aber kein Alarmsystem

Die E-Mail-Benachrichtigung ist der Kanal für alle, die noch kein Monitoring-System haben, und ein gutes Zusatznetz für alle anderen. In den E-Mail-Optionen trägst du den SMTP-Server als FQDN oder Adresse ein, den Port, eine Absenderadresse und bei Bedarf ein Kennwort. Für die Verbindungssicherheit stehen keine Verschlüsselung, STARTTLS wenn verfügbar, erzwungenes STARTTLS und SSL/TLS zur Wahl. Nimmst du einen FQDN, braucht der LoadMaster einen funktionierenden DNS-Server, was nach einem DNS-Umbau gern vergessen wird.

Die Empfänger ordnest du sechs Stufen zu, jede mit eigener, kommagetrennter Liste. Auch hier gilt die Treppe: Wer bei Error steht, bekommt Critical und Emergency automatisch mit. Ein Testversand an alle Empfänger ist direkt in der WUI möglich. Nutze ihn nach jeder Änderung am Mailserver, nicht erst, wenn du die erste echte Warnung vermisst.

Steht der LoadMaster vor Exchange, liegt der Gedanke nahe, Exchange auch als Mailserver für die Benachrichtigungen zu nutzen. Das ist in Ordnung, solange du dir der Ironie bewusst bist: Fällt Exchange aus, kann der LoadMaster dir genau das nicht mehr mitteilen. Für Alarme, die einen Exchange-Ausfall betreffen, brauchst du einen zweiten Weg, etwa das Monitoring-System mit eigenem Versand oder einen SMS-Gateway. Wie du einen sauberen Empfangsconnector für Geräte-Mails auf Exchange einrichtest und warum dabei die Absender-IP zählt, erklärt SMTP über den LoadMaster: Relay, Empfangsconnectors und die echte Absender-IP.

Einstellung	Empfehlung	Warum
SMTP-Server	Interner Relay mit eigenem Empfangsconnector	Geräte-Mails sauber getrennt von Benutzerverkehr, Relay-Berechtigung nur für die LoadMaster-Adressen
Verbindungssicherheit	STARTTLS oder SSL/TLS	Alarm-Mails enthalten Hostnamen und Zustände
Absender	Eigene Adresse je Gerät oder Standort	Mailregeln und Tickets lassen sich zuordnen
Empfänger Error und höher	Team-Postfach oder Ticketsystem, nicht Einzelpersonen	Urlaub, Krankheit und Kündigung gibt es auch in der IT
Empfänger Info	Niemand	Wer Info per Mail abonniert, filtert sie nach drei Tagen weg

Welche Ereignisse wirklich jemanden wecken sollten

Jetzt der Teil, an dem die meisten Monitoring-Projekte scheitern: die Auswahl. Technisch kannst du dir alles schicken lassen. Organisatorisch erträgt ein Team nur eine Handvoll Alarme pro Woche, bevor es anfängt, sie zu ignorieren. Und ein ignorierter Alarm ist schlimmer als gar keiner,

weil er das gute Gefühl erzeugt, es sei ja überwacht. Die folgende Pyramide teilt die Ereignisse danach ein, wie schnell jemand handeln muss.



Skizze: Schwellenwerte sind Vorschläge; dein Betriebsmodell entscheidet über die Grenzen

Ereignis	Erkennen über	Dringlichkeit	Erste Reaktion
Alle Real Server eines Virtual Service down	Syslog, Trap, SNMP-Zustand, externer Check	Sofort	Server prüfen, Health Check prüfen, ggf. Wartungsseite
Einzelner Real Server down	Syslog, SNMP-Zustand	Heute	Ursache auf dem Server klären, Redundanz ist reduziert
HA-Wechsel	Syslog Critical, Trap, Erreichbarkeit beider Knoten	Heute	Grund des Failovers klären, Standby wieder herstellen
Standby-Knoten nicht erreichbar	SNMP-Abfrage des Knotens	Heute	Redundanz ist weg, obwohl alles grün aussieht
Zertifikat läuft ab	Externer Check, CERTS-MIB	Gestaffelt ab 90 Tagen	Erneuerung anstoßen, Tausch am LoadMaster planen
Lizenz oder Subscription läuft aus	WUI-Hinweis, Kalender, Kemp 360 Central	Gestaffelt	Verlängerung anstoßen, bevor Funktionen fehlen
Häufung von Anmeldefehlern am ESP	SIEM-Regel auf Syslog	Je nach Umfang	Konten prüfen, Quelladressen bewerten
Konfigurationsänderung	Syslog, Audit Log	Nur speichern	Nachvollziehbarkeit, keine Alarmierung

Real Server down: der häufigste und am meisten unterschätzte Alarm

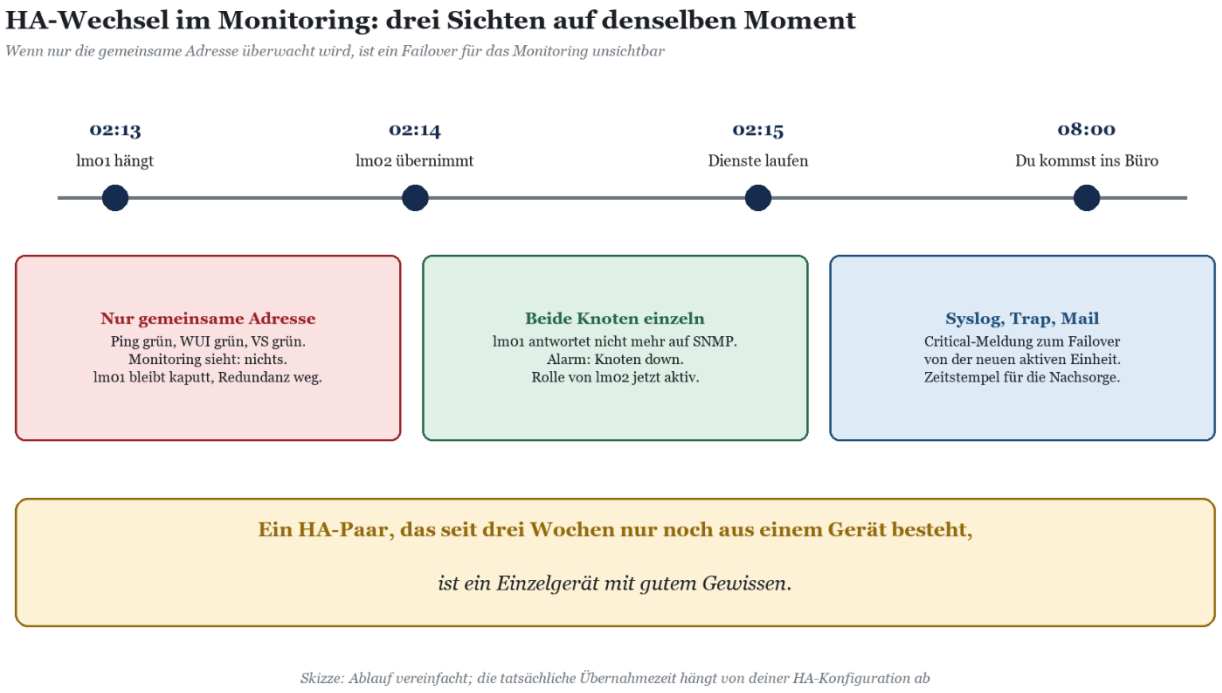
Wenn ein einzelner Real Server aus dem Pool fällt, merkt das niemand. Genau dafür hast du ja einen Load Balancer. Das Problem ist die Gewöhnung. Der Server bleibt draußen, weil der Alarm nur „Warnung“ hieß, und wenn drei Wochen später der zweite Server beim Patchday neu startet, ist plötzlich der ganze Dienst weg. Aus Sicht der Benutzerinnen und Benutzer ist das ein

Totalausfall aus heiterem Himmel. Aus Sicht des Monitorings war es eine Ansage mit drei Wochen Vorlauf.

Behandle deshalb „ein Real Server down“ nicht als Alarm, sondern als Ticket mit Fälligkeit, und „letzter gesunder Real Server“ als Alarm. Viele Monitoring-Systeme können das über eine Regel auf die Zahl gesunder Server je Virtual Service abbilden. Und achte auf das Gegenteil: Ein Health Check, der alle fünf Minuten zwischen up und down wechselt, erzeugt eine Flut, die das Team schnell abstumpft. Flattern ist ein eigenes Symptom, meist für einen zu strengen oder zu ungeduldigen Check.

HA-Wechsel: der Ausfall, den keiner sieht

Ein Failover im HA-Paar ist der Moment, in dem die Hochverfügbarkeit funktioniert hat und zugleich aufgebraucht ist. Der Dienst läuft weiter, die Benutzer merken nichts, und genau deshalb merkt es auch sonst niemand. Wird nur die gemeinsame Adresse überwacht, ist für das Monitoring alles grün, während der ehemals aktive Knoten in einer Ecke des Rechenzentrums vor sich hin hängt.

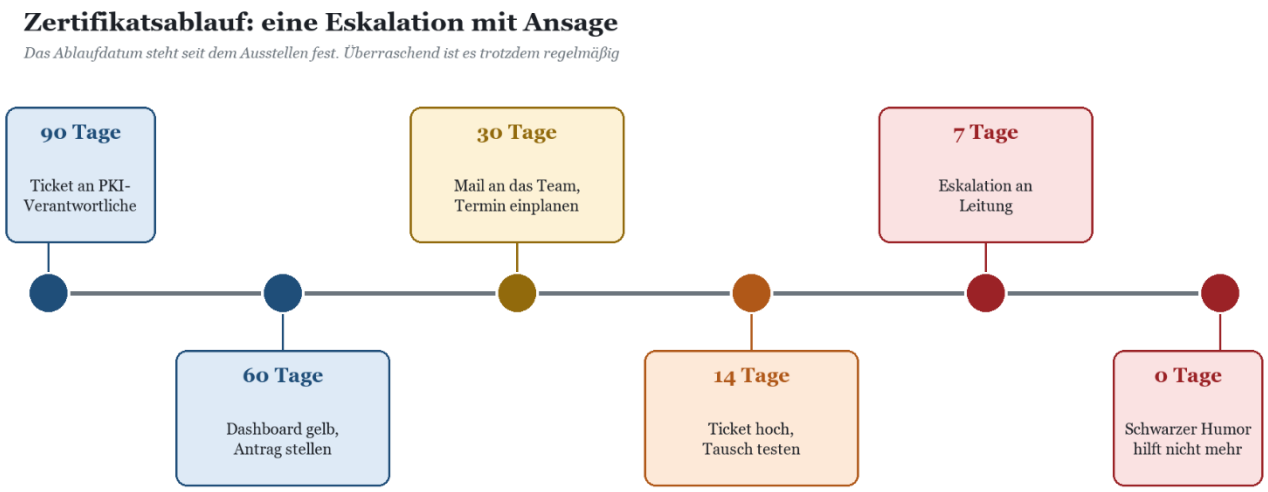


Skizze: Ablauf vereinfacht; die tatsächliche Übernahmezeit hängt von deiner HA-Konfiguration ab

Überwache deshalb immer beide Knoten über ihre eigenen Management-Adressen, und lass dir den Wechsel selbst über Syslog oder Trap melden. Die Meldung zum Failover hat laut Hersteller die Stufe Critical und kommt damit auch bei einem strengen Alarmziel an. Was einen Failover auslösen kann und wie du ihn kontrolliert testest, steht in HA-Paar, Failover und Konfig-Sync: zwei LoadMaster, ein Gedanke.

Zertifikatsablauf: die vorhersehbarste Überraschung der IT

Ein Zertifikat hat ein Ablaufdatum, das seit dem Tag seiner Ausstellung bekannt ist. Trotzdem gehört „Zertifikat abgelaufen“ zu den häufigsten Ursachen für Ausfälle von Exchange, ADFS und RD Gateway. Der Grund ist schlicht organisatorisch: Das Zertifikat wurde vor einem oder zwei Jahren von jemandem eingespielt, der inzwischen andere Aufgaben hat, und das Ablaufdatum stand in dessen Kalender.



Skizze: Vorschlag für Schwellen; geprüft wird das Zertifikat, das der Virtual Service ausliefert

Der verlässlichste Weg ist der externe Check auf den Virtual Service. Er prüft genau das Zertifikat, das Clients sehen, inklusive Kette. Ergänzend liefert die CERTS-MIB Zertifikatsinformationen direkt vom LoadMaster, was auch Zertifikate erfasst, die nur für Re-Encryption oder interne Dienste im Einsatz sind. Vergiss dabei die Zertifikate auf den Real Servern nicht: Bei Re-Encryption baut der LoadMaster selbst eine TLS-Verbindung zum Server auf, und dessen Zertifikat läuft genauso ab. Welche Zertifikate an welcher Stelle sitzen, beschreibt TLS-Offload, Re-Encryption und Zertifikate: PKI trifft LoadMaster.

TIPP · Kürzere Laufzeiten, mehr Wechsel

Die Laufzeiten öffentlicher TLS-Zertifikate werden in den kommenden Jahren schrittweise verkürzt. Was heute einmal im Jahr passiert, passiert bald mehrmals. Ein Zertifikatsmonitoring mit Staffelung ist dann keine Kür mehr, sondern die Voraussetzung dafür, dass der Tausch per API automatisiert werden kann, ohne dass jemand ihn vergisst. Wie das per PowerShell aussieht, zeigt Automatisierung per REST-API und PowerShell.

Lizenz und Subscription: der Ausfall per Kalender

Läuft eine Testlizenz oder Subscription ab, zeigt der LoadMaster das im Bereich der Lizenzinformationen der WUI an. Das ist ehrlich, hilft aber nur, wenn jemand regelmäßig hineinschaut. Gehören deine Geräte zu einer über Kemp 360 Central verwalteten Lizenzierung, prüft jeder LoadMaster seine Lizenz täglich. Scheitert die Prüfung, beginnt eine Schonfrist von 30 Tagen, und ab dem 20. Tag ohne Kontakt verschickt Central täglich eine Mail, sofern SMTP eingerichtet ist. Spätestens das ist ein Grund, die Mail-Einstellungen in Central nicht zu überspringen.

Für alle anderen gilt: Das Ablaufdatum gehört in den Kalender eines Teams, nicht einer Person, mit Erinnerung drei Monate vorher. Beschaffung in Mittelstand und Verwaltung dauert selten kürzer. Welche Editionen und Lizenzmodelle es gibt, erklärt Editionen, Lizenzierung und Sizing: welcher LoadMaster für welchen Laden.

Viele LoadMaster, ein Blick: Kemp 360 Central

Ab einer Handvoll Geräten oder mehreren Standorten wird das Einrichten von Syslog, SNMP und Mail pro Gerät mühsam. Kemp 360 Central sammelt Syslog der angebundenen LoadMaster ein

und stellt beim ersten Kontakt die passenden Syslog-Optionen am Gerät selbst ein. Dazu kommen zentrale Übersichten über Zustände, Firmware-Stände und Lizenzen. Es ersetzt dein SIEM oder dein Rechenzentrums-Monitoring nicht, aber es ist der natürliche Ort für die LoadMaster-spezifische Sicht. Mehr dazu in Kemp 360 Central und Global Server Load Balancing für mehrere Standorte.

WARNUNG · Syslog-Ziele nach dem Einbinden in Central prüfen

Weil Central beim ersten Kontakt Syslog-Optionen am LoadMaster setzt, solltest du danach kontrollieren, ob deine bisherigen Ziele noch so eingetragen sind, wie du sie geplant hast. Die Grenze von zehn Zielen gilt weiterhin, und ein vergessener Eintrag fällt erst auf, wenn das SIEM plötzlich still ist.

Vom ersten Syslog bis zum Alarmplan: so führst du es ein

Monitoring wird selten an einem Stück fertig. Ein pragmatischer Ablauf in fünf Schritten hat sich in mittelständischen Umgebungen und Verwaltungen bewährt, weil er nach jedem Schritt schon einen Nutzen bringt.

- **Zeit und Namen.** NTP auf allen LoadMastern, sinnvolle Hostnamen und ein Syslog-Präfix je Gerät. Ohne das ist jeder weitere Schritt halb so viel wert.
- **Syslog ins Archiv.** Ein Ziel auf Notice oder Info per TLS an den zentralen Syslog-Server oder SIEM-Kollektor, ESP- und WAF-Logs inklusive. Parser für die wichtigsten Meldungen.
- **Erreichbarkeit und Zustand.** SNMPv3 mit SHA und AES, beide Knoten einzeln, Zustand der Real Server und Erreichbarkeit als erste Sensoren.
- **Außensicht.** Synthetischer HTTPS-Check je wichtigem Namespace mit Zertifikatsprüfung.
- **Alarmplan.** Für jedes Ereignis aus der Tabelle festlegen, wer wann wie benachrichtigt wird. Danach die Tests: Real Server stoppen, Failover auslösen, Testmail senden.

FAKTEN · Testfälle für die Abnahme

Ein Real Server wird im Wartungsfenster gestoppt: Syslog-Meldung, SNMP-Zustand und Ticket erscheinen. Der letzte Real Server wird gestoppt: Alarm erscheint. Ein Failover wird ausgelöst: Critical-Meldung, Trap und Erreichbarkeitsalarm des ehemals aktiven Knotens erscheinen. Ein Testversand an alle Mail-Empfänger kommt an. Ein Monitoring, das nie getestet wurde, ist eine Behauptung.

Wenn du den Alarmplan mit deinem Team gemeinsam erarbeiten oder die Integration in SIEM und Monitoring absichern möchtest, unterstützt dich die Beratung zum Kemp LoadMaster. Wer Failover, Real-Server-Ausfälle und Alarme lieber einmal in Ruhe im Labor erlebt, statt zum ersten Mal im Ernstfall, findet das in der Kemp-LoadMaster-Schulung.

FAQ: Monitoring, Syslog und SNMP am Kemp LoadMaster

Wie viele Syslog-Ziele kann ich am LoadMaster eintragen?

Bis zu zehn einzelne Adressen. Jedes Ziel bekommt eine Severity und erhält alle Meldungen ab dieser Stufe aufwärts. Mehrere Einträge für dasselbe Ziel sind deshalb unnötig.

Welche Severity sollte ich für das SIEM wählen?

Für ein SIEM ist Notice ein guter Startpunkt, Info, wenn du auch Routinemeldungen brauchst und der Speicher es hergibt. Für ein Alarmziel reicht Error oder Critical.

Kann der LoadMaster Syslog verschlüsselt senden?

Ja, per TLS. Zusätzlich lässt sich prüfen, ob Name oder Adresse des Syslog-Servers im Zertifikat stehen. Diese Prüfung ist ab Werk aus und sollte bei einem Zertifikat aus der internen PKI eingeschaltet werden.

Warum finde ich die ESP-Logs nicht mehr lokal?

Weil sie an einen Remote-Syslog weitergeleitet werden. In diesem Fall ist die lokale Protokollierung der ESP-Logs abgeschaltet, und du suchst im Syslog-System.

Brauche ich SNMP, wenn ich schon Syslog habe?

Ja. Syslog meldet, was passiert, aber ein ausgefallenes Gerät meldet nichts mehr. Die regelmäßige SNMP-Abfrage erkennt genau diesen Fall und liefert Verläufe für Last und Zustand.

Welche SNMP-Version sollte ich verwenden?

SNMPv3 mit SHA für die Authentifizierung und AES für die Verschlüsselung. MD5 und DES bietet der LoadMaster an, der Hersteller bezeichnet sie aber selbst als veraltet. v2c nur im abgeschotteten Management-Netz und nie mit der Community public.

Welche MIBs brauche ich?

ONE4NET-MIB, IPVS-MIB, B-100-MIB und CERTS-MIB. Importiere alle vier in dein Monitoring-System, bevor du Sensoren anlegst.

Soll ich im HA-Paar die gemeinsame Adresse oder die Knoten überwachen?

Beides, aber die Knoten sind wichtiger. Nur über die einzelnen Management-Adressen erkennst du, dass der Standby-Knoten ausgefallen ist, während der Dienst weiterläuft.

Warnt der LoadMaster selbst vor ablaufenden Zertifikaten?

Verlass dich nicht darauf. Prüfe das ausgelieferte Zertifikat mit einem externen Check gegen den Virtual Service und ergänze die CERTS-MIB per SNMP für die übrigen Zertifikate.

Kann ich Exchange als Mailserver für die Benachrichtigungen nutzen?

Ja, über einen eigenen Empfangsconnector mit Relay-Berechtigung für die LoadMaster-Adressen. Für Alarme, die Exchange selbst betreffen, brauchst du aber einen zweiten Benachrichtigungsweg.

Fazit: Ein LoadMaster, der redet, ist ein LoadMaster, dem du vertrauen kannst

Der LoadMaster weiß in jedem Moment, wie es deinen Diensten geht. Ob du es auch weißt, hängt an einer Stunde Konfiguration und einem Nachmittag Nachdenken. Syslog per TLS an das SIEM, mit Präfix und sauberer Zeit, liefert die Spuren. SNMPv3 auf beide Knoten liefert Zustand und Verläufe und merkt, wenn ein Gerät schweigt. Traps und Mails sind die Abkürzung, nicht das Netz. Und der synthetische Check von außen prüft, was am Ende zählt: ob Benutzerinnen und Benutzer ihre Anwendung erreichen.

Der eigentliche Gewinn liegt aber in der Auswahl. Wenige Alarme, die alle bedeuten, dass jemand handeln muss, sind wertvoller als hundert, die alle bedeuten, dass etwas irgendwie anders ist. Real Server down als Ticket, der letzte Server als Alarm, HA-Wechsel und Zertifikate mit Vorlauf, der Rest ins Archiv. Dann klingelt das Telefon aus dem Vorzimmer nur noch, wenn jemand fragen möchte, warum es so ruhig geworden ist.

WEITERLESEN · Weiter im Thema

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

› Kemp 360 Central und Global Server Load Balancing für mehrere Standorte

› Client-IP sichtbar machen: Transparenz, SNAT und X-Forwarded-For
› Health Checks, die wirklich prüfen: warum „Port 443 offen“ nicht reicht
› HA-Paar, Failover und Konfig-Sync: zwei LoadMaster, ein Gedanke
› TLS-Offload, Re-Encryption und Zertifikate: PKI trifft LoadMaster