Kemp 360 Central und Global Server Load Balancing für mehrere Standorte



Skizze: zentrale Verwaltung und DNS-basierte Verteilung über zwei Rechenzentren

WISSEN

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

› **Kemp LoadMaster**

BERATUNG

Zweiter Standort, GSLB oder doch nur ein sauberes Runbook? Wir rechnen mit dir durch, was dein Ausfallszenario wirklich braucht, und bauen es dann auch.

› **Beratung zum Kemp LoadMaster**

SCHULUNG

Delegation, GEO-Cluster und Failure Delay im Labor üben, wo ein Standortausfall nur ein Mausklick ist und kein Wochenende.

› **Kemp-LoadMaster-Schulung**

Irgendwann kommt in jedem mittelständischen Unternehmen und in jeder Verwaltung die Frage aus der Geschäftsführung oder vom Informationssicherheitsbeauftragten: Was passiert eigentlich, wenn das Rechenzentrum abbrennt? Die ehrliche Antwort lautet meist: Dann haben wir einen zweiten Serverraum im Nachbargebäude, in dem ein paar Hosts stehen, auf die Veeam repliziert. Und dann? Dann ändert jemand den DNS-Eintrag. Wer? Der Kollege, der weiß, wo das Kennwort für das Provider-Portal liegt. Und wenn der im Urlaub ist? Stille.

Genau in diese Stille fallen zwei Werkzeuge aus dem Kemp-Kosmos. Kemp 360 Central verwaltet viele LoadMaster an einer Stelle: Backups, Firmware, Lizenzen, Überblick. Die GEO-Funktion des LoadMasters, also Global Server Load Balancing, beantwortet DNS-Anfragen abhängig davon, welcher Standort gerade lebt. Beides klingt nach Konzern-Rechenzentrum mit eigenem Netzwerkteam. Beides kann aber auch im Mittelstand sinnvoll sein, wenn man weiß, wofür. Und beides kann auch völlig überdimensioniert sein, wenn ein geübter manueller Schwenk dasselbe leistet.

Dieser Beitrag aus der Serie zum Kemp LoadMaster erklärt dir, was Kemp 360 Central tatsächlich übernimmt und was nicht, wie kemp gslb mit der GEO-Funktion funktioniert, wie du eine Teilzone sauber delegierst und wo es in der Praxis knallt: bei Health Checks, die den falschen Standort für tot erklären, bei TTLs, die niemanden interessieren, und bei Exchange, das sich von schnellem DNS allein nicht retten lässt. Am Ende steht eine ehrliche Entscheidungshilfe, wann sich das lohnt.

FAKTEN · Das Wichtigste in 30 Sekunden

Kemp 360 Central ist eine Verwaltungs- und Überwachungsplattform für mehrere LoadMaster. Sie liegt nicht im Datenpfad. Fällt sie aus, balancieren die LoadMaster weiter.

Central speichert Firmware, Vorlagen und Backups in einem Global Repository, sichert LoadMaster zeitgesteuert und aktualisiert Firmware auf mehreren Geräten. Wiederherstellungen lassen sich laut Hersteller nicht planen, sie bleiben Handarbeit.

Bei Pooled oder Metered Licensing beziehen die LoadMaster ihre Lizenz von Kemp 360 Central. Pooled und Metered schließen sich gegenseitig aus.

GEO gibt es als eigenständiges GEO-Produkt oder als GSLB-Funktion auf dem LoadMaster. GEO ist autoritativer DNS-Server für die Namen, die du ihm überträgst, und beantwortet A- und AAAA-Anfragen.

Verteilverfahren laut Dokumentation: Round Robin, Weighted Round Robin, Fixed Weighted, Real Server Load, Location Based, Proximity und All Available.

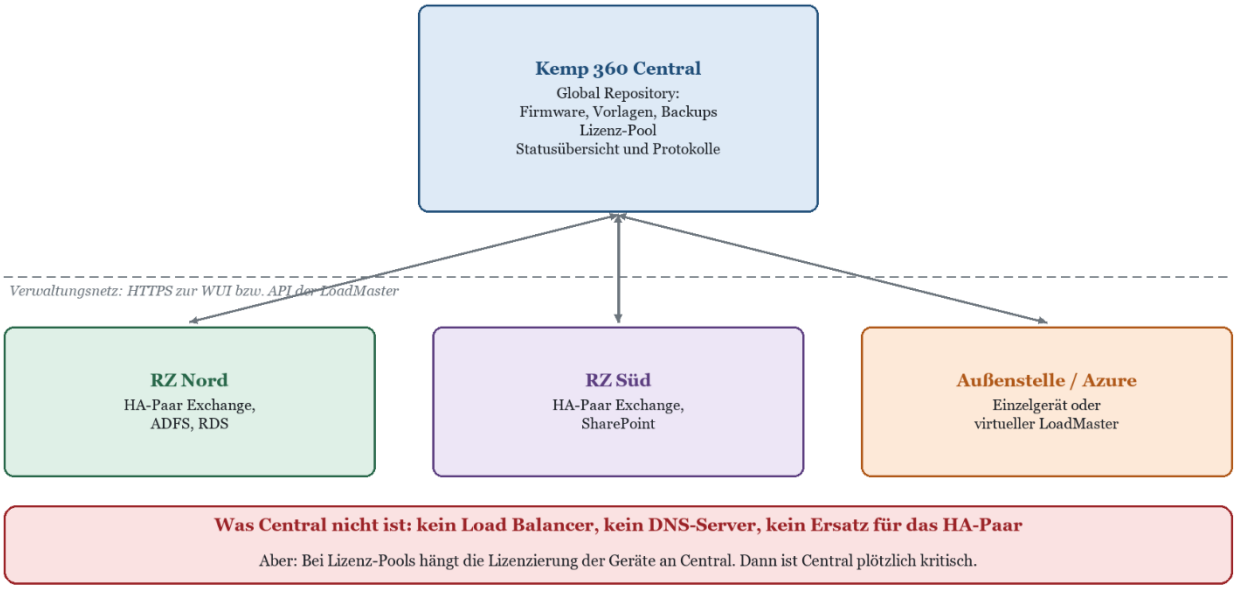
Failure Delay verzögert den Standortwechsel um eine einstellbare Zahl von Minuten. Erst dann wird der Site Recovery Mode verfügbar: Automatic oder Manual.

Kemp 360 Central: der Hausmeister für viele LoadMaster

Solange du ein HA-Paar betreibst, brauchst du keine zentrale Verwaltung. Du hast eine Weboberfläche, eine Konfiguration und ein Backup, und die Synchronisation zwischen den beiden Knoten erledigt das Paar selbst. Wie das funktioniert, beschreibt HA-Paar, Failover und Konfig-Sync: zwei LoadMaster, ein Gedanke. Spannend wird es ab dem dritten, vierten, fünften Gerät: zwei HA-Paare in zwei Rechenzentren, ein virtueller LoadMaster in Azure, vielleicht noch ein Einzelgerät in einer Außenstelle. Dann merkst du, dass jedes Gerät eine eigene kleine Insel ist, mit eigenem Firmware-Stand, eigenem Backup-Zeitplan und eigener Meinung darüber, wann das Zertifikat abläuft.

Kemp 360 Central: eine Konsole, viele LoadMaster

Central steht neben dem Datenpfad, nicht in ihm. Fällt Central aus, balancieren die LoadMaster einfach weiter



Skizze: vereinfachte Architektur; Funktionsumfang abhängig von Abonnement und Version

Was Central übernimmt: Backup, Firmware, Vorlagen, Überblick

Kemp 360 Central ist eine virtuelle Appliance, die du im Verwaltungsnetz betreibst und der du deine LoadMaster bekannt machst. Danach siehst du alle Geräte in einer Liste mit Status, Firmware-Stand und Lizenz. Die drei Funktionen, die im Alltag am meisten bringen, sind unspektakulär und gerade deshalb wertvoll:

- **Zeitgesteuerte Backups.** Central erzeugt Sicherungsarchive der LoadMaster-Konfiguration und auf Wunsch der Zertifikate, legt sie zentral ab und kann sie auf einen LoadMaster zurückspielen. Die Sicherung liegt damit endlich außerhalb des Geräts, das sie betrifft.
- **Firmware aus einem Repository.** Firmware wird einmal ins Global Repository geladen und dann auf einzelne Geräte oder Gruppen verteilt, auf Wunsch auch zeitgesteuert. Bei HA-Paaren planst du das Update laut Hersteller auf den einzelnen Knoten, nicht auf der gemeinsamen Adresse. Das ist richtig so, denn genau dort willst du Kontrolle über die Reihenfolge.
- **Vorlagen.** Konfigurationsvorlagen, etwa die Kemp-Templates für Exchange oder ADFS, liegen ebenfalls im Repository und lassen sich auf LoadMaster hochladen. Das sorgt dafür, dass alle Geräte mit demselben Stand der Vorlagen arbeiten.
- **Überblick und Protokolle.** Status der Geräte und Virtual Services, Syslog-Sammlung der verwalteten LoadMaster, Nutzungsberichte. Kein Ersatz für ein richtiges Monitoring, aber ein guter zweiter Blick.

WICHTIG · Planung braucht Abstand

Geplante Aufgaben in Central dürfen laut Herstellerdokumentation nicht innerhalb einer Stunde zueinander liegen. Wer Backup um 02:00 und Firmware-Update um 02:30 plant, bekommt eine Fehlermeldung statt eines Wartungsfensters. Leg dir einen festen Takt zurecht, zum Beispiel Backup täglich um 01:00, Updates nur nach Freigabe und nie in derselben Stunde.

Lizenz-Pools: bequem, aber Central wird zur Abhängigkeit

Neben der klassischen Einzellizenz pro Gerät kennt Progress Abonnement-Modelle, bei denen die LoadMaster ihre Lizenz von Kemp 360 Central beziehen. Beim Pooled Licensing kaufst du eine feste Kapazität und verteilst sie auf Geräte. Wird ein virtueller LoadMaster abgebaut, holst du seine Lizenz in Central zurück, und sie steht dem nächsten Gerät zur Verfügung. Beim Metered Licensing wird die tatsächliche Nutzung gemessen und abgerechnet. Beides gleichzeitig geht laut Hersteller nicht.

Der Haken ist architektonisch, nicht kaufmännisch: Sobald die Lizenzen am zentralen Server hängen, ist Central kein netter Zusatz mehr, sondern Teil der Betriebsfähigkeit. Progress sieht deshalb für Metered-Umgebungen ein HA-Paar aus zwei Central-Instanzen vor, die dieselbe Version haben müssen. Für den Mittelstand heißt das: Wenn du dich für ein Pool-Modell entscheidest, betreibst du Central mit derselben Sorgfalt wie einen Domänencontroller. Backup, Monitoring, Firmware-Pflege, Notfallplan. Welche Edition und welches Lizenzmodell zu deinem Bestand passt, sortiert Editionen, Lizenzierung und Sizing: welcher LoadMaster für welchen Laden.

Aspekt	Einzellizenz pro Gerät	Pooled Licensing	Metered Licensing
Lizenz liegt	auf dem LoadMaster	in Central, an Geräte verteilt	in Central, nach Nutzung abgerechnet
Rolle von Central	optional, Komfort	betriebsrelevant	betriebsrelevant
Neues Gerät	Lizenz bestellen und	aus dem Pool ziehen	aus Central lizenzieren

ausrollen	aktivieren		
Gerät abbauen	Lizenz bleibt am Gerät	Lizenz zurück in den Pool	Nutzung endet
Passt typischerweise	zwei bis vier feste Geräte	viele virtuelle Geräte, wechselnder Bestand	Dienstleister, stark schwankende Nutzung

WARNUNG · Central nie nur als einzige Kopie betreiben

Das klassische Eigentor: Central läuft als einzelne virtuelle Maschine auf demselben Cluster wie alles andere, und das Backup von Central liegt auf Central. Fällt der Cluster aus, sind die LoadMaster-Backups weg, genau in dem Moment, in dem du sie brauchst. Exportiere die Sicherungen zusätzlich auf ein Ziel am anderen Standort, und sichere Central selbst. Laut Hersteller enthält die Central-Sicherung weder Protokolldaten noch die Firmware-Dateien aus dem Repository. Die musst du im Notfall neu besorgen.

Monitoring: Central ist Ergänzung, nicht Ersatz

Central zeigt dir, ob Geräte und Virtual Services grün sind, und sammelt Protokolle. Das ist praktisch für den schnellen Blick. Wer aber ohnehin PRTG, Checkmk, Zabbix oder System Center Operations Manager betreibt, sollte die LoadMaster dort per SNMP und Syslog einbinden, damit Alarme in denselben Bereitschaftsprozess laufen wie alles andere. Eine zweite Alarmkonsole, die nur einer kennt, ist im Ernstfall keine Hilfe. Wie du das aufsetzt, steht in Monitoring, Syslog und SNMP: den LoadMaster ins Monitoring holen.

TIPP · Wann sich Central im Mittelstand lohnt

Als Faustregel: Ab drei unabhängigen Geräten oder Paaren, ab zwei Standorten oder sobald du virtuelle LoadMaster häufig auf- und abbaust, lohnt sich der Blick auf Central. Bei einem einzigen HA-Paar ersetzt ein Skript, das nachts die Konfiguration sichert, den Großteil des Nutzens. Wie das aussieht, zeigt Automatisierung per REST-API und PowerShell. Prüfe außerdem, ob Central in deinem Abonnement enthalten ist. Laut Hersteller ist es nur in bestimmten Abonnements verfügbar.

Kemp GSLB mit GEO: DNS als Verkehrspolizist

Ein normaler Virtual Service verteilt Verbindungen auf Real Server. Er hat eine virtuelle IP-Adresse, und der Client verbindet sich mit dieser Adresse. Was aber, wenn der ganze Standort mit dieser Adresse weg ist? Dann hilft dir kein noch so schlauer Virtual Service, denn niemand kommt mehr bis zu ihm durch. Die Lösung muss eine Ebene früher ansetzen: bei der Frage, welche Adresse der Client überhaupt bekommt. Und diese Frage beantwortet DNS.

Was GEO eigentlich macht

Die GEO-Funktion macht den LoadMaster zu einem autoritativen DNS-Server für eine Handvoll Namen. Für jeden Namen, im Kemp-Sprachgebrauch ein FQDN, hinterlegst du mehrere Ziele, typischerweise die virtuellen IP-Adressen der Exchange-Dienste in zwei Rechenzentren. Kommt eine DNS-Anfrage, prüft GEO, welche Ziele gesund sind, wählt nach dem eingestellten Verfahren eines aus und antwortet mit dessen Adresse. Seit Firmware 7.2.53 kann GEO zusätzlich TXT-, CNAME- und MX-Einträge zu einem FQDN liefern. Den Inhalt der Pakete sieht GEO nie. Es ist ein Wegweiser, kein Türsteher.

Daraus folgt eine Eigenschaft, die man sich nicht oft genug klarmachen kann: GSLB wirkt nur bei der nächsten Namensauflösung. Ein Client, der schon verbunden ist, bleibt bei seinem Ziel, bis die Verbindung abbricht. Ein Resolver, der die Antwort zwischengespeichert hat, liefert sie weiter aus,

bis die TTL abgelaufen ist. GSLB ist also schnell im Sinne von Minuten, nicht im Sinne von Sekunden. Wer Sekunden braucht, braucht ein HA-Paar am Standort, und das bleibt auch mit GSLB Pflicht.

Ebene	Werkzeug	schützt vor	Umschaltzeit (Größenordnung)
Server	Virtual Service mit Health Check	Ausfall eines Real Servers	Sekunden
Gerät	HA-Paar	Ausfall eines LoadMasters	Sekunden
Standort	GSLB mit GEO	Ausfall eines Rechenzentrums	Minuten, abhängig von TTL und Delay
Standort, manuell	DNS-Schwenk nach Runbook	Ausfall eines Rechenzentrums	so lange, bis jemand handelt

Verteilverfahren: welches für welchen Zweck

GEO bietet sieben Verfahren. Für den typischen Mittelständler mit zwei Standorten in derselben Stadt oder demselben Bundesland sind die meisten davon akademisch. Proximity und Location Based verteilen nach Herkunft des Clients, was bei zwei Rechenzentren im selben Postleitzahlenbereich herzlich egal ist. Interessant sind fast immer zwei: Fixed Weighted für aktiv/passiv und Round Robin oder Weighted Round Robin für aktiv/aktiv.

Verfahren	Prinzip	Typischer Einsatz im Mittelstand
Fixed Weighted	immer das Ziel mit dem höchsten Gewicht, bei Ausfall das nächste	aktiv/passiv: Hauptstandort plus Ausweichstandort. Der Klassiker.
Round Robin	Ziele der Reihe nach	aktiv/aktiv bei gleich starken Standorten
Weighted Round Robin	Reihe nach Gewicht, schwere Ziele öfter	aktiv/aktiv mit kleinerem Zweitstandort
Real Server Load	Standort mit der geringsten Last laut LoadMaster-Statistik	selten, setzt Cluster mit LoadMaster-Anbindung voraus
Location Based	nach Land, Kontinent oder IP-Bereich des Clients	interne Netze gezielt an den nahen Standort, Rest an den Hauptstandort
Proximity	geografisch nächstes Ziel nach Koordinaten	internationale Standorte, im Mittelstand selten
All Available	alle gesunden Ziele in einer Antwort	Sonderfälle, Client wählt selbst

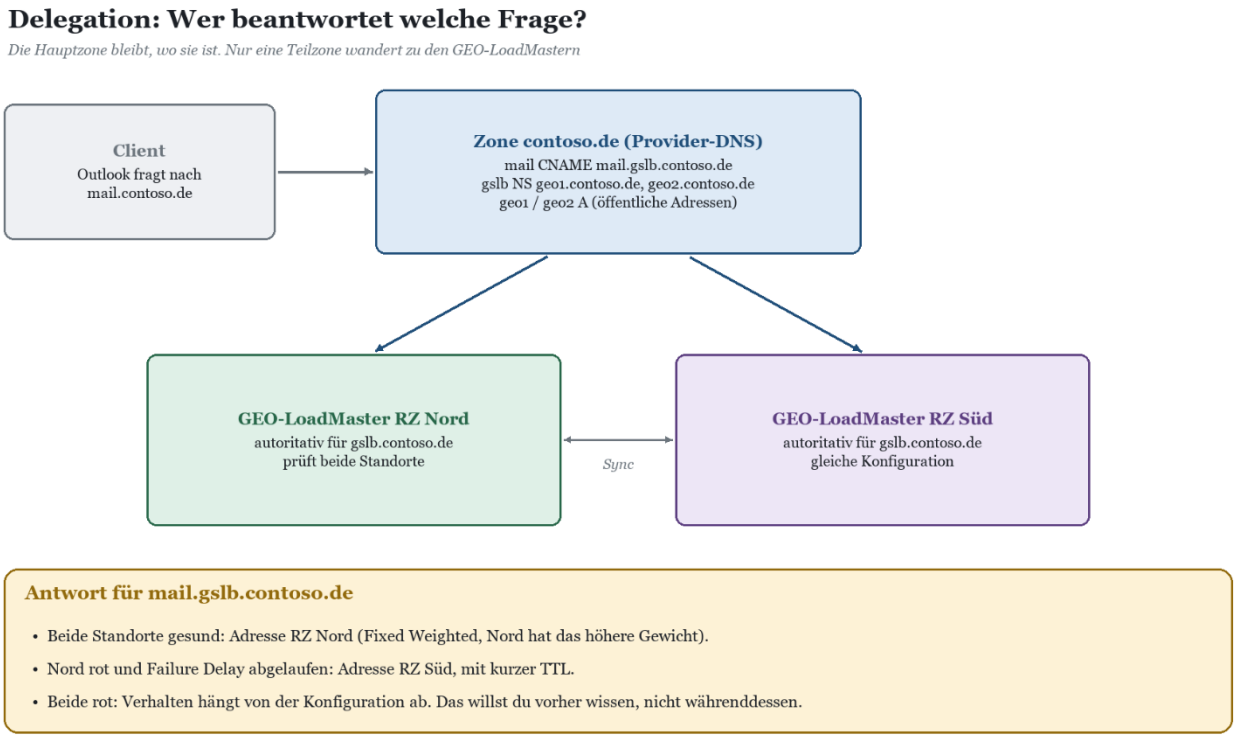
FAKTEN · Stickiness, das DNS-Gegenstück zur Persistence

GEO kann sich merken, welcher Client welche Antwort bekommen hat, und ihm bei der nächsten Anfrage dieselbe liefern. Laut Hersteller wird diese Tabelle geleert, wenn ein Standort ausfällt. Beachte, dass GEO die Adresse des anfragenden Resolvers sieht, nicht die des Clients dahinter. Bei einem zentralen DNS-Server für das ganze Unternehmen klebt also das ganze Unternehmen am selben Standort. Mehr zu Persistence auf Verbindungsebene findest du in Persistence und Scheduling: wer hängt an welchem Server und warum.

Delegation der Zone: der Teil, vor dem alle Angst haben

Damit GEO Anfragen beantworten kann, muss die Anfrage bei GEO ankommen. Dazu delegierst du einen Teil deines Namensraums an die GEO-LoadMaster. Bewährt hat sich eine eigene Teilzone, zum Beispiel gslb.contoso.de, die beim Provider per NS-Eintrag an zwei GEO-Instanzen

übertragen wird, je eine pro Standort. Die eigentlichen Dienstnamen bleiben in der Hauptzone und zeigen per CNAME in die Teilzone: mail.contoso.de wird zu mail.gslb.contoso.de. Die Hauptzone bleibt, wo sie ist, das Risiko bleibt klein.



Skizze: Beispielzone contoso.de; Namen frei gewählt, Glue-Records beim Provider je nach Aufbau nötig

Warum nicht gleich die ganze Zone an GEO geben? Weil GEO ein Spezialist ist, kein vollwertiger DNS-Server für deine MX-, SPF-, DKIM-, DMARC- und Autodiscover-Einträge. Und weil du bei einem Fehler in der Delegation dann nicht nur Exchange verlierst, sondern alles. Kemp selbst dokumentiert für eine Firmware-Version außerdem ein bekanntes Problem: Wer nachträglich einen Zone Name in GEO einträgt, nachdem bereits funktionierende FQDNs existieren, riskiert, dass GEO für einige davon nicht mehr antwortet. Entscheide dich also vor dem ersten FQDN, ob du mit Zone Name arbeitest, und prüfe die Release Notes deines Firmware-Stands.

WARNUNG · CNAME auf der Zonenspitze geht nicht

Du kannst contoso.de selbst nicht per CNAME in die GSLB-Teilzone zeigen lassen, das verbietet der DNS-Standard. Für Dienste auf der Zonenspitze brauchst du andere Wege. Für Exchange ist das selten ein Problem, weil mail.contoso.de und autodiscover.contoso.de ohnehin eigene Namen sind. Bei Eigenentwicklungen, die zwingend unter der nackten Domäne laufen sollen, wird es dagegen knifflig.

Und intern? Split-Brain-DNS mit Active Directory

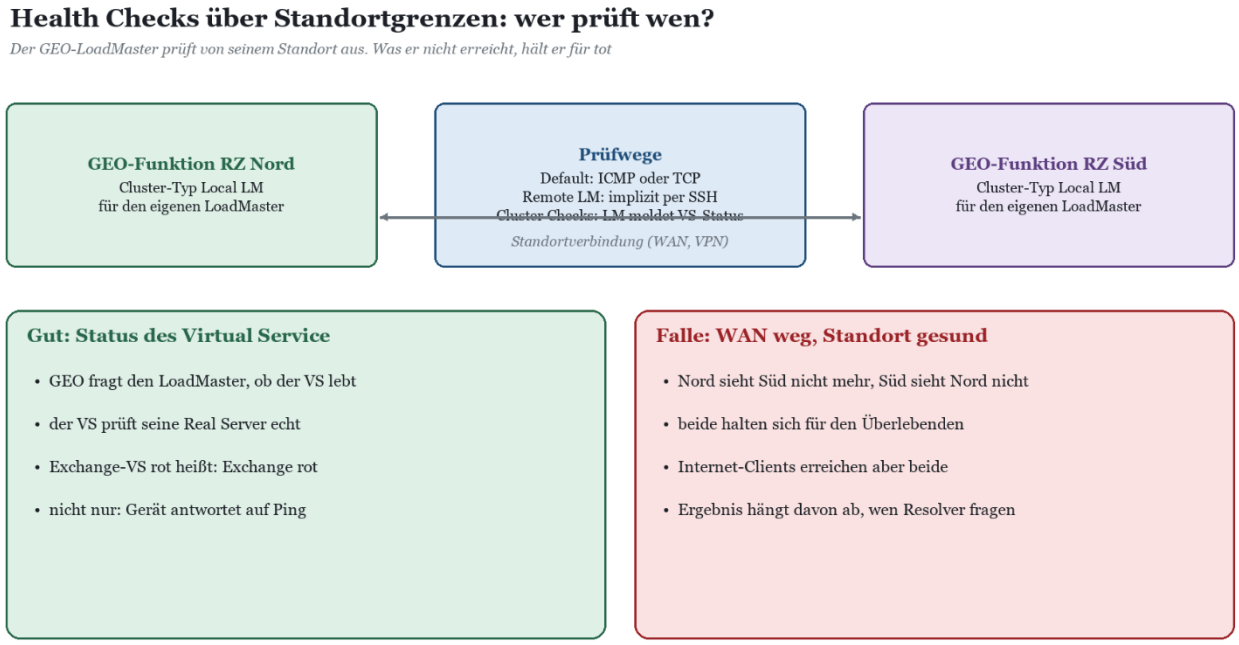
Die meisten Microsoft-Umgebungen betreiben Split-Brain-DNS: Intern beantworten die Domänencontroller contoso.de mit internen Adressen, extern der Provider mit öffentlichen. Wenn GSLB auch intern greifen soll, brauchst du in der AD-integrierten Zone ebenfalls eine Delegation von gslb.contoso.de auf die internen Adressen der GEO-Instanzen, und die GEO-Ziele brauchen interne Adressen. GEO kennt dafür die Unterscheidung zwischen öffentlichen und privaten Zielen und kann je nach Herkunft der Anfrage passende Adressen liefern. Das ist der Teil, an dem die meisten Projekte länger dauern als geplant, weil plötzlich drei Teams beteiligt sind: Netzwerk, AD und Provider.

TIPP · DNS-Server-Cache beim Testen leeren

Nach jeder Änderung an GEO liefern deine Domänencontroller die alte Antwort aus dem Cache, bis die TTL abläuft. Beim Testen leerst du den Cache mit Clear-DnsServerCache auf den DNS-Servern und mit Clear-DnsClientCache auf dem Testclient. Kemp empfiehlt für die Fehlersuche zusätzlich, die Stickiness vorübergehend auf null zu setzen.

Health Checks über Standorte und der Failover, der nicht flattern darf

GSLB ist exakt so gut wie seine Gesundheitsprüfung. Ein GEO, das nur pingt, schickt fröhlich Clients an einen Standort, dessen Exchange-Server seit einer Stunde keine Postfächer mehr bereitstellen, weil der LoadMaster dort brav auf ICMP antwortet. Die Prüfungen laufen dabei immer vom LoadMaster aus. Was der GEO-LoadMaster nicht erreichen kann, gilt als ausgefallen, und genau darin steckt die interessanteste Falle dieses Themas.



Skizze: Cluster-Typen nach Herstellerdokumentation; Prüfungen erfolgen vom LoadMaster aus

Cluster-Typen und was sie wirklich prüfen

In GEO fasst du die Ziele eines Standorts in Clustern zusammen. Der Cluster-Typ bestimmt, wie GEO prüft. Default ist ein generischer Cluster, der nicht mit einem LoadMaster spricht und nur ICMP oder TCP-Verbindungen nutzt. Remote LM prüft einen entfernten LoadMaster implizit über SSH. Local LM steht für den LoadMaster, auf dem GEO selbst läuft. Mit Cluster Checks fragt GEO den LoadMaster, welche Virtual Services gesund sind, statt nur das Gerät anzupingen.

Der Unterschied ist entscheidend. Prüft GEO nur das Gerät, fällt alles dahinter erst dann aus, wenn das Gerät weg ist. Prüft GEO den Status des Virtual Service, und prüft der Virtual Service seine Real Server ernsthaft, dann pflanzt sich ein Exchange-Ausfall bis in die DNS-Antwort fort. Das funktioniert aber nur, wenn die Health Checks am Virtual Service selbst etwas taugen. Für Exchange heißt das: die healthcheck.htm der einzelnen Protokolle, nicht ein offener Port 443. Wie man das richtig macht, steht in Health Checks, die wirklich prüfen: warum „Port 443 offen“ nicht reicht.

Prüfweg	prüft	erkennt Exchange-Ausfall?	Bewertung

ICMP auf VIP	Gerät oder Adresse antwortet	nein	nur als Notlösung
TCP auf VIP:443	Port nimmt Verbindungen an	nein, der LoadMaster nimmt immer an	trügerisch
Cluster Checks am LoadMaster	Status des Virtual Service	ja, wenn der VS gut prüft	empfohlen
Remote LM	entfernter LoadMaster per SSH	indirekt	sinnvoll bei mehreren GEO-Instanzen

FAKTEN · Resource Check Parameters

Wie oft und wie geduldig GEO prüft, legen drei globale Werte fest: Prüfintervall, Verbindungs-Timeout und Zahl der Wiederholungen. Die aktuelle Herstellerdokumentation nennt als Vorgabe 120 Sekunden Intervall, 20 Sekunden Timeout und zwei Wiederholungen. Ein Ziel, das gar nicht antwortet, braucht damit nach der Formel (Wiederholungen plus eins) mal Timeout bis zu einer Minute pro Prüfdurchgang, bevor es als ausgefallen gilt. Ein Ziel, das aktiv ablehnt, fällt schneller auf.

Failure Delay und Site Recovery Mode

Nichts ist schlimmer als ein Standortwechsel wegen eines Neustarts. Ein Exchange-Knoten bootet nach dem Patchday, der Virtual Service ist für zwei Minuten rot, GEO schwenkt alle Clients ins Ausweichrechenzentrum, das gar nicht für die volle Last ausgelegt ist, und fünf Minuten später wieder zurück. Dagegen hilft Failure Delay. Du findest es in der FQDN-Konfiguration im Abschnitt Site Failure Handling. Es legt in Minuten fest, wie lange GEO wartet, bevor es einen Standort als ausgefallen betrachtet. Erholt sich der Standort in dieser Zeit, passiert nichts.

Erst wenn ein Failure Delay gesetzt ist, erscheint der Site Recovery Mode. Automatic nimmt einen wieder gesunden Standort automatisch zurück in die Verteilung. Manual deaktiviert das Ziel nach einem Ausfall administrativ, und es kommt erst zurück, wenn jemand es freigibt und der Health Check grün ist. Kemp empfiehlt für Exchange über mehrere Standorte ausdrücklich beides: Failure Delay einschalten und Manual als Recovery Mode. Der Grund ist simpel. Der Rückweg ist bei Exchange fast immer heikler als der Hinweg, weil die Datenbanken nach einem Standortausfall nicht automatisch wieder am Hauptstandort aktiv sind.



AUS DER PRAXIS · Das Pingpong-Wochenende

Typischer Verlauf: GSLB mit Round Robin über zwei Standorte, kein Failure Delay, Recovery automatisch. Am Samstag ist die Standortverbindung instabil. Der Health Check vom einen zum anderen Standort kippt alle paar Minuten. GEO nimmt den Standort raus, wieder rein, wieder raus. Clients landen abwechselnd hier und dort, Outlook verbindet sich neu, ActiveSync-Geräte synchronisieren alles noch einmal, und die Helpdesk-Tickets am Montag lauten alle: E-Mail war am Wochenende irgendwie komisch. Die Lösung war am Ende unspektakulär: Failure Delay, Manual Recovery und ein Health Check auf den Status des Virtual Service statt auf eine Adresse hinter dem VPN.

Die Split-Brain-Falle bei abgerissener Standortverbindung

Zwei GEO-Instanzen, je eine pro Standort, synchronisieren ihre Konfiguration und sind beide autoritativ für die Teilzone. Was passiert, wenn die Verbindung zwischen den Standorten reißt, beide Standorte aber für sich gesund und aus dem Internet erreichbar sind? Nord sieht Süd nicht mehr und hält Süd für tot. Süd denkt dasselbe über Nord. Jede Instanz antwortet nur noch mit dem eigenen Standort. Welche Antwort ein Client bekommt, hängt davon ab, welchen der beiden Nameserver sein Resolver gerade fragt. Für zustandslose Webanwendungen ist das harmlos. Für Exchange mit einer DAG, deren Datenbanken aktiv nur an einem Standort laufen, bedeutet es: Die Hälfte der Clients landet am falschen Ende und wird per Proxy über eine Verbindung geschickt, die gerade nicht existiert.

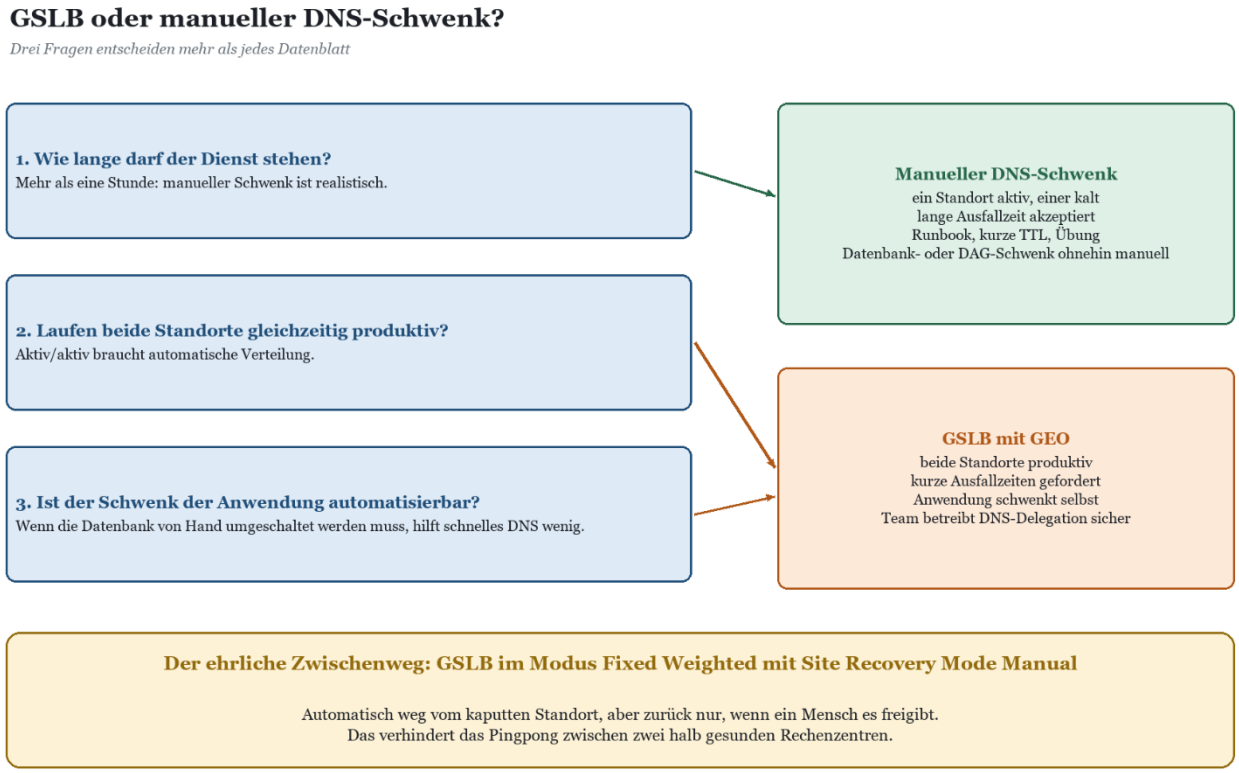
Ein Allheilmittel gibt es nicht, aber gute Gegenmittel. Prüfe die Standorte möglichst über dieselben Wege, über die auch Clients kommen, also über die öffentlichen Adressen, nicht über das interne VPN. Nutze Fixed Weighted statt Round Robin, wenn die Anwendung ohnehin nur an einem Standort wirklich aktiv ist. Und dokumentiere, was in diesem Fall passieren soll. Die Microsoft-Dokumentation zur Standortausfallsicherheit von Exchange Server beschreibt ausführlich, wie Namensräume und DAG zusammenspielen. Die Kemp-Seite beschreibt die DNS-Seite. Zusammen gelesen ergibt sich ein Bild. Wie die Exchange-Dienste am LoadMaster selbst aufgebaut sind, findest du in Exchange Server hinter dem LoadMaster: Templates, Namespaces, Health Checks.

WARNUNG · Schnelles DNS rettet keine Datenbank

GSLB schwenkt Clients, nicht Daten. Wenn am Ausweichstandort die Exchange-Datenbanken, das SQL-Cluster von SharePoint oder der Dateiserver der Eigenentwicklung erst manuell aktiviert werden müssen, landen die Clients dort pünktlich vor einer verschlossenen Tür. Der Standortwechsel der Anwendung muss vor oder mit dem DNS-Schwenk passieren. Bei ADFS zusätzlich die Frage: Ist die Farm am Ausweichstandort überhaupt Mitglied derselben Farm und kann sie Token signieren?

Lohnt sich das? GSLB gegen den guten alten DNS-Schwenk

Jetzt der unbequeme Teil. Viele mittelständische Umgebungen haben einen zweiten Standort, der im Normalbetrieb wenig tut. Die Anwendungen laufen aktiv/passiv, die Datenbanken werden repliziert, der Schwenk ist ein Projekt für einen Nachmittag. In diesem Szenario löst GSLB ein Problem, das du nicht hast: Es schwenkt in Minuten etwas, für dessen Schwenk die Anwendung ohnehin eine Stunde braucht. Ein gut vorbereiteter manueller DNS-Schwenk leistet hier dasselbe, kostet keinen zusätzlichen Betriebsaufwand und hat einen unschätzbaren Vorteil: Ein Mensch entscheidet, ob der Standort wirklich tot ist.



Skizze: Entscheidungshilfe als Orientierung, keine Sizing-Regel

Wann der manuelle Schwenk reicht

Der manuelle Schwenk ist kein Armutszeugnis, sondern in vielen Häusern die richtige Antwort. Er reicht, wenn diese Bedingungen zusammenkommen:

- Die vereinbarte Wiederanlaufzeit liegt bei einer Stunde oder mehr.
- Der Zweitstandort ist passiv, und die Anwendung muss dort ohnehin von Hand aktiviert werden.
- Die TTL der betroffenen Einträge ist dauerhaft kurz, etwa fünf Minuten, und nicht erst dann, wenn es brennt. Eine TTL von einem Tag lässt sich im Notfall nicht mehr verkürzen.

- Es gibt ein Runbook mit den exakten Einträgen, alten und neuen Adressen, und mindestens zwei Personen haben Zugang zum DNS beim Provider und zur internen Zone.
- Der Schwenk wurde mindestens einmal im Jahr wirklich geübt, nicht nur besprochen.

Der letzte Punkt ist der wichtigste. Wer den Schwenk automatisiert, testet ihn implizit bei jedem Health Check. Wer ihn manuell macht, testet ihn nur, wenn er ihn übt. Ein Runbook, das seit drei Jahren niemand ausgeführt hat, beschreibt mit hoher Wahrscheinlichkeit eine Umgebung, die es nicht mehr gibt. Mit kurzen TTLs und einem PowerShell-Skript für die interne Zone und einem für die API des Providers kommt man übrigens schon sehr weit.

Wann GSLB sich lohnt

GSLB spielt seine Stärken aus, wenn beide Standorte gleichzeitig produktiv arbeiten und die Anwendung selbst den Standortwechsel verkraftet. Beispiele sind zustandslose Webanwendungen und Eigenentwicklungen mit replizierter Datenbank, RD-Gateway-Farmen an zwei Standorten, Always On VPN mit Einwahlknoten in beiden Rechenzentren oder Exchange mit einer DAG, deren aktive Kopien auf beide Standorte verteilt sind und die per Datacenter Activation Coordination sauber konfiguriert ist. Ebenfalls ein Kandidat: eine hybride Umgebung mit einem Standort im eigenen Rechenzentrum und einem in Azure. Was dabei zu beachten ist, beschreibt LoadMaster in Azure und hybriden Umgebungen.

Kriterium	Manueller DNS-Schwenk	GSLB mit GEO
Umschaltzeit	bis jemand reagiert, plus TTL	Prüfdauer plus Failure Delay plus TTL
Fehlalarme	praktisch ausgeschlossen, ein Mensch entscheidet	möglich, gegen Flattern hilft Failure Delay
Betriebsaufwand	Runbook pflegen und üben	GEO-Konfiguration, Delegation, Monitoring, Sync
Aktiv/aktiv	nicht sinnvoll	ja
Abhängigkeiten	Zugang zum Provider-DNS	Delegation, erreichbare GEO-Instanzen an beiden Standorten
Typischer Fehler	Runbook veraltet, Kennwort fehlt	Health Check prüft das Falsche
Geeignet für	aktiv/passiv mit manuellem Anwendungsschwenk	aktiv/aktiv oder automatischer Anwendungsschwenk

CHECKLISTE · Bevor du GSLB einführst

Gibt es eine schriftliche Anforderung an die Wiederanlaufzeit pro Dienst?

Schwenkt die Anwendung am Ausweichstandort ohne Handarbeit, oder wartet sie auf einen Menschen?

Steht an jedem Standort ein HA-Paar, oder ersetzt GSLB versehentlich die Hochverfügbarkeit vor Ort?

Sind die Health Checks der Virtual Services aussagekräftig, bevor GEO sich auf sie verlässt?

Darf und kann jemand die Teilzone beim Provider und im Active Directory delegieren?

Ist der Ausweichstandort für die volle Last ausgelegt, oder nur für einen Notbetrieb?

Gibt es einen Testtermin, an dem ein Standort wirklich abgeschaltet wird?

Ein pragmatischer Mittelweg

Zwischen Vollautomatik und Handbetrieb liegt eine Variante, die sich in der Praxis häufig bewährt: GSLB mit Fixed Weighted, Failure Delay und Site Recovery Mode Manual. Im Normalbetrieb

bekommt jeder Client den Hauptstandort. Fällt er für länger als die eingestellte Wartezeit aus, schwenkt GEO automatisch, und zwar ohne dass jemand nachts das Provider-Portal suchen muss. Zurück geht es erst, wenn ein Mensch die Rückkehr freigibt. Das kombiniert die Geschwindigkeit der Automatik mit der Urteilskraft eines Menschen, der weiß, dass am Hauptstandort zwar wieder Strom ist, aber die Datenbanken noch am Ausweichstandort laufen.

TIPP · Firmware-Updates an GEO-Instanzen

Beide GEO-Instanzen sind autoritativ für dieselbe Teilzone. Aktualisiere sie nacheinander, nie gleichzeitig, und prüfe nach jedem Update mit Resolve-DnsName gegen genau diese Instanz, ob sie antwortet. Wie du Updates allgemein ohne Herzrasen planst, beschreibt Firmware-Updates, Backup und Notfallplan: LoadMaster-Betrieb ohne Herzrasen.

Ob dein Ausfallszenario GSLB, Central, beides oder keins von beidem braucht, lässt sich selten am Schreibtisch entscheiden, sondern am besten mit einem Blick auf die Anwendungen und ihre Abhängigkeiten. Dabei unterstützt dich die Beratung zum Kemp LoadMaster. Wer Delegation, Cluster und Failover erst gefahrlos ausprobieren will, übt das in der Kemp-LoadMaster-Schulung.

FAQ: Kemp 360 Central und GSLB

Brauche ich Kemp 360 Central, um GSLB zu nutzen?

Nein. GEO ist eine Funktion des LoadMasters beziehungsweise ein eigenständiges GEO-Produkt und wird am Gerät konfiguriert. Central ist eine Verwaltungsplattform für mehrere Geräte und hat mit der DNS-Verteilung nichts zu tun.

Was passiert mit dem Datenverkehr, wenn Kemp 360 Central ausfällt?

Nichts, die LoadMaster arbeiten weiter. Kritisch wird ein Ausfall von Central nur, wenn die Geräte ihre Lizenz aus einem Pool oder per Metered Licensing von Central beziehen. Dann gehört Central in dein Hochverfügbarkeits- und Backupkonzept.

Kann Kemp 360 Central Backups auch automatisch zurückspielen?

Backups lassen sich zeitgesteuert anlegen und auf einen LoadMaster zurückspielen. Eine geplante Wiederherstellung sieht der Hersteller nicht vor. Das ist auch gut so.

Welches GEO-Verfahren nehme ich für aktiv/passiv?

Fixed Weighted. GEO liefert immer das Ziel mit dem höchsten Gewicht und weicht erst bei dessen Ausfall auf das nächste aus.

Muss ich meine ganze Domäne an den LoadMaster delegieren?

Nein, und du solltest es auch nicht. Delegiere eine Teilzone wie gslb.contoso.de und lass die Dienstnamen per CNAME dorthin zeigen. Die Hauptzone mit MX, SPF und Co. bleibt beim Provider.

Wie schnell schwenkt GSLB?

Die Summe aus Prüfdauer, Failure Delay und TTL, plus dem Eigenleben der Clients. In der Praxis bewegt sich das im Bereich von Minuten. Wer Sekunden braucht, löst das mit einem HA-Paar am Standort, nicht mit DNS.

Ersetzt GSLB das HA-Paar?

Nein. GSLB schützt vor dem Ausfall eines Standorts, das HA-Paar vor dem Ausfall eines Geräts. Ohne HA-Paar würde jeder Neustart eines LoadMasters zum Standortwechsel führen.

Warum empfiehlt Kemp für Exchange den Site Recovery Mode Manual?

Weil die Rückkehr zum Hauptstandort bei Exchange davon abhängt, wo die Datenbanken aktiv sind. Manual verhindert, dass Clients zurückgeschickt werden, bevor ein Administrator die Datenbanken zurückgeschwenkt hat.

Funktioniert GSLB auch für interne Clients?

Ja, wenn die AD-integrierte Zone die Teilzone ebenfalls an die GEO-Instanzen delegiert und die Ziele interne Adressen haben. GEO unterscheidet dafür öffentliche und private Ziele.

Reicht ein Health Check per Ping auf die virtuelle IP?

Nein. Der LoadMaster antwortet auf Ping, auch wenn alle Real Server dahinter tot sind. Lass GEO den Status des Virtual Service abfragen, und sorge dafür, dass dieser seine Real Server sinnvoll prüft.

Ab wann lohnt sich Kemp 360 Central für den Mittelstand?

Als Faustregel ab drei unabhängigen Geräten oder Paaren, ab mehreren Standorten oder bei häufig wechselndem Bestand an virtuellen LoadMastern. Bei einem HA-Paar reicht meist ein Skript, das die Konfiguration sichert.

Fazit: Erst die Anwendung, dann das DNS

Kemp 360 Central ist der Hausmeister, den du ab einer gewissen Zahl von LoadMastern wirklich willst: Backups außerhalb des Geräts, Firmware aus einer Hand, Lizenzen im Pool und ein Überblick, der nicht in fünf Browser-Tabs verteilt ist. Mit dem Pool kommt aber Verantwortung, denn dann ist Central kein Komfort mehr, sondern Infrastruktur. Bei einem einzelnen HA-Paar ist es eher Luxus.

GSLB mit GEO ist ein scharfes Werkzeug für ein klar umrissenes Problem: einen Standortausfall automatisch und in Minuten zu überbrücken. Es funktioniert hervorragend, wenn die Anwendung mitspielt, die Health Checks ehrlich sind und Failure Delay das Flattern verhindert. Es ist verschwendete Mühe, wenn am Ausweichstandort erst jemand die Datenbank von Hand starten muss. Dann reicht ein geübter manueller Schwenk mit kurzer TTL, und der Rest der Energie geht besser in die Übung. Denn das Rechenzentrum brennt nicht nach Ankündigung, aber immer dann, wenn der Kollege mit dem Provider-Kennwort gerade in den Bergen ist.

WEITERLESEN · Weiter im Thema

› HA-Paar, Failover und Konfig-Sync: zwei LoadMaster, ein Gedanke
› Monitoring, Syslog und SNMP: den LoadMaster ins Monitoring holen
› Editionen, Lizenzierung und Sizing: welcher LoadMaster für welchen Laden
› Health Checks, die wirklich prüfen: warum „Port 443 offen“ nicht reicht
› Exchange Server hinter dem LoadMaster: Templates, Namespaces, Health Checks
› LoadMaster in Azure und hybriden Umgebungen