Firmware-Updates, Backup und Notfallplan: LoadMaster-Betrieb ohne Herzrasen



Skizze: die vier Phasen eines entspannten Firmware-Updates

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

BERATUNG
Firmware seit drei Jahren nicht angefasst, Backup unklar, Notfallplan nur im Kopf? Wir bringen deinen LoadMaster mit dir auf Stand, inklusive Rückweg.
› **Beratung zum Kemp LoadMaster**

SCHULUNG
Update, Failover und Restore im Labor üben, bis es langweilig wird. Langweilig ist im Betrieb das höchste Lob.
› **Kemp-LoadMaster-Schulung**

Es gibt LoadMaster, die seit ihrer Installation keine neue Firmware gesehen haben. Sie laufen stabil, still und zuverlässig, und niemand traut sich, sie anzufassen. Das Argument klingt vernünftig: „Never touch a running system." Es stimmt nur leider nicht für ein Gerät, das per Definition im Internet steht, TLS terminiert und vor Exchange, ADFS oder dem RD Gateway die erste Tür ist. Für so ein Gerät heißt der Satz eigentlich: „Never touch a running system, until someone else does." Und dieser Jemand fragt nicht nach einem Wartungsfenster.

Die Angst vor dem Update ist trotzdem nicht unbegründet. Wer schon einmal um 22 Uhr vor einem LoadMaster saß, der nach dem Neustart nicht mehr antwortet, während die Fachabteilung ab sechs Uhr Mails erwartet, kennt das Herzrasen. Nur liegt die Ursache fast nie im Update selbst. Sie liegt im fehlenden Backup, im nicht gelesenen Hinweis in den Release Notes, im HA-Paar, das in Wahrheit seit Wochen nicht mehr synchron war, und im fehlenden Plan B.

Dieser Beitrag aus der Serie zum Kemp LoadMaster nimmt dir das Herzrasen ab, soweit das ein Text kann. Du erfährst, welche Release-Kanäle es gibt und welchen du willst, wie du Release Notes mit Microsoft-Brille liest, wie das Update im HA-Paar sauber abläuft und wo der Rückweg endet. Danach geht es um das, was die meisten erst nach dem ersten Ernstfall einrichten: Konfigurationssicherung, die Lücken im Backup, die Wiederherstellung auf eine frische Instanz und den Notbetrieb per DNS, wenn gar kein LoadMaster mehr da ist.

FAKTEN · Das Wichtigste in 30 Sekunden

Progress pflegt zwei aktive Release-Kanäle: Long Term Support Feature (LTSF) und General Availability (GA). Für den Produktivbetrieb empfiehlt der Hersteller LTSF, es sei denn, du brauchst eine Funktion oder Korrektur, die es nur im GA-Zweig gibt.

Im HA-Paar aktualisierst du zuerst die passive Einheit, startest sie neu und aktualisierst dann die aktive. Deren Neustart löst den einzigen Failover aus.

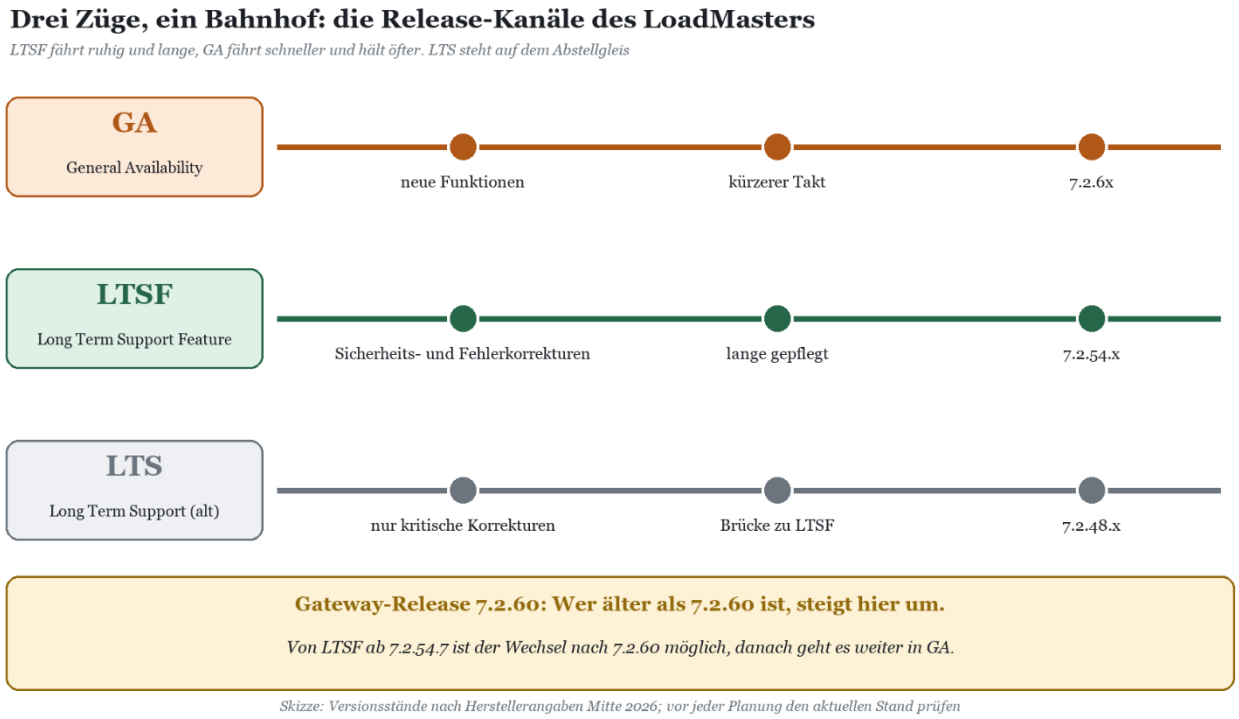
Der LoadMaster hält genau ein vorheriges Firmware-Image vor. Ein Rücksprung ist also möglich, aber nur einen Schritt weit, und bestimmte Downgrades sind ausdrücklich verboten.

Das Konfigurationsbackup enthält weder Zertifikate noch Lizenz. Beides sicherst du getrennt.

Automatische Backups gehen täglich oder wöchentlich per SCP, SFTP oder FTP an ein Ziel außerhalb des Geräts. Im HA-Paar wird nur die aktive Einheit gesichert.

Release-Kanäle und Release Notes: erst lesen, dann klicken

Wer aus der Microsoft-Welt kommt, kennt das Prinzip aus Windows Server: Long-Term Servicing Channel für Server, die Ruhe brauchen, und schnellere Kanäle für alle, die neue Funktionen wollen. Progress macht beim LoadMaster etwas ganz Ähnliches, nur mit anderen Abkürzungen. Und wie bei Microsoft gilt: Der Kanal ist eine Entscheidung, keine Voreinstellung, die man irgendwann zufällig vorfindet.



Skizze: Versionsstände nach Herstellerangaben Mitte 2026; vor jeder Planung den aktuellen Stand prüfen

GA, LTSF und das alte LTS im Vergleich

Der GA-Zweig bekommt neue Funktionen zuerst. Mitte 2026 stand er bei Version 7.2.63, der LTSF-Zweig bei 7.2.54 mit fortlaufenden Wartungsständen. LTSF sammelt die Funktionen eines bereits gereiften Standes und bekommt danach vor allem Sicherheits- und Fehlerkorrekturen. Daneben existiert noch der ältere LTS-Zweig 7.2.48, der nur noch kritische Fehler und Sicherheitslücken behandelt und als Brücke zu LTSF gedacht ist. Er enthält zum Beispiel noch die alte, abgekündigte WAF-Engine. Wer dort steht, hat einen Umzug vor sich, keinen Wartungsstand.

Kanal	Zweig (Mitte 2026)	Was kommt hinein	Passt für	Haken

LTSF	7.2.54.x	Sicherheits- und Fehlerkorrekturen auf einem gereiften Funktionsstand	Die meisten Produktivumgebungen vor Exchange, ADFS, RDS	Neue Funktionen kommen erst mit dem nächsten LTSF-Zweig
GA	7.2.6x	Neue Funktionen, Korrekturen, Sicherheitsupdates	Wenn du eine konkrete neue Funktion oder Korrektur brauchst	Kürzerer Takt, mehr Updates, weniger Felderfahrung pro Version
LTS (alt)	7.2.48.x	Nur noch kritische Fehler und Sicherheitslücken	Übergang von sehr alten Ständen	Alte WAF-Engine, keine neuen Funktionen

WICHTIG · Versionsnummern veralten schneller als dieser Artikel

Die genannten Stände sind eine Momentaufnahme. Maßgeblich ist die Herstellerseite mit der Empfehlung, welche Version gerade für den Produktivbetrieb vorgesehen ist. Prüfe sie vor jeder Planung, nicht erst am Abend des Wartungsfensters.

Upgrade-Pfade und Gateway-Releases

Nicht jede Version springt direkt auf jede andere. Progress definiert sogenannte Gateway-Releases, über die du umsteigen musst. Ein Beispiel aus der aktuellen Dokumentation: Stände bis einschließlich 7.2.59.4 gehen zuerst auf 7.2.60.0, erst von dort ist jede spätere Version erreichbar. Wer im LTSF-Zweig ab 7.2.54.7 steht, kann ebenfalls nach 7.2.60 wechseln. Für ein Gerät, das drei Jahre nicht aktualisiert wurde, bedeutet das oft zwei Updates mit zwei Neustarts. Das ist kein Drama, gehört aber in die Planung des Wartungsfensters, damit aus einer Stunde nicht drei werden.

Release Notes mit Microsoft-Brille lesen

Release Notes von Load Balancern sind selten Lesevergnügen. Sie bestehen aus einer langen Liste von Korrekturen mit internen Nummern, und der eine Satz, der deinen Exchange-Namespace betrifft, steht zwischen zwei Einträgen zu Funktionen, die du nie benutzt hast. Statt alles zu lesen, suchst du gezielt.

Suchbegriff	Warum er dich betrifft
Upgrade Path, Gateway	Ob du direkt springen darfst oder einen Zwischenstand brauchst
Known Issues	Was nach dem Update bekanntermaßen nicht funktioniert, mit Workaround
CVE, Security	Wie dringend das Update ist und ob die Lücke deine Konfiguration betrifft
ESP, SSO, KCD, LDAP	Vorauthentifizierung vor OWA, ECP und SharePoint, Kerberos-Delegation
TLS, Cipher, OpenSSL	Geänderte Standard-Cipher können ältere Clients oder Real Server aussperren
WAF, OWASP	Regelwerk und Engine ändern sich, False Positives sind möglich
Deprecated, Removed	Funktionen, die mit diesem Stand verschwinden oder bald verschwinden
Hyper-V, Azure, VMware	Plattformspezifische Hinweise zu Treibern, Images und Integration

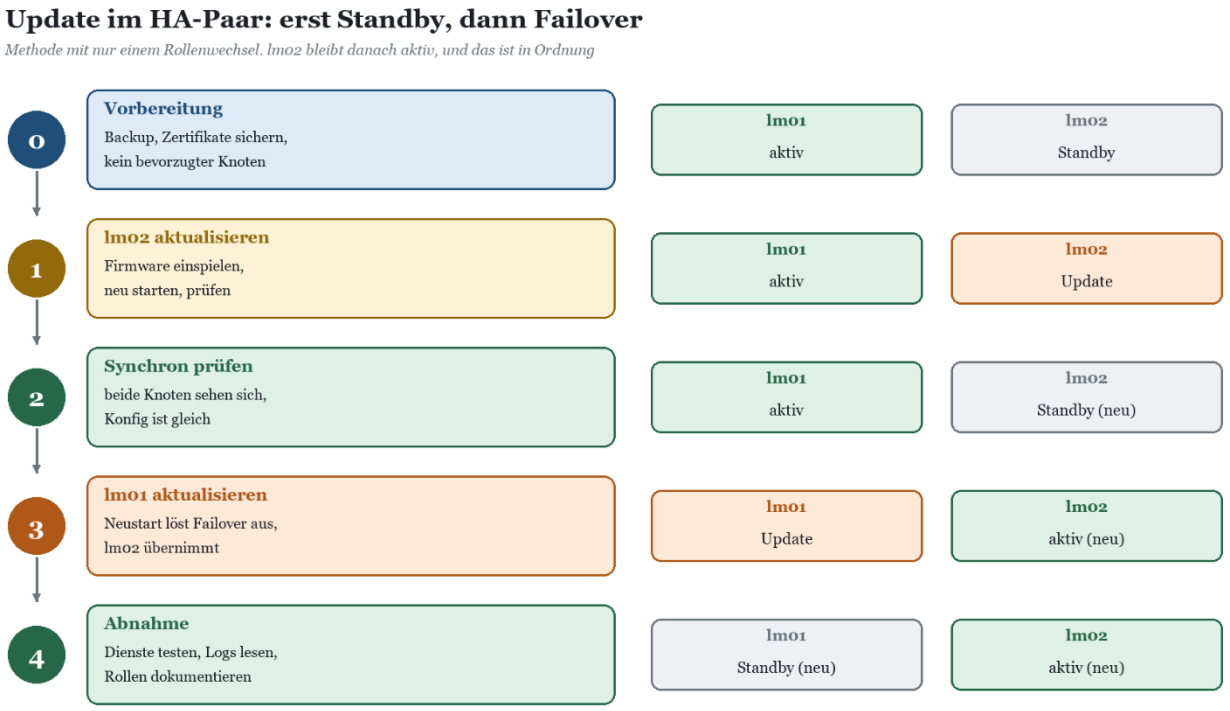
AUS DER PRAXIS · Die Cipher-Überraschung

Ein typisches Bild: Nach dem Update eines LoadMasters vor einer Eigenentwicklung auf einem älteren Windows Server melden alle Health Checks plötzlich „down“. Ursache war ein geändertes Cipher-Verhalten für die Re-Encryption zum Real Server, das in den Release Notes dokumentiert

war. Gelesen hatte es niemand. Die Lösung dauerte zehn Minuten, die Suche danach zwei Stunden. Wie Cipher-Sets und Re-Encryption zusammenhängen, steht in TLS-Offload, Re-Encryption und Zertifikate: PKI trifft LoadMaster.

Das Update im HA-Paar: erst Standby, dann Failover

Ein HA-Paar ist die beste Versicherung gegen ein misslungenes Update, wenn du es richtig benutzt. Die Idee ist einfach: Einer arbeitet, während der andere operiert wird. Danach wird getauscht. Damit das klappt, muss das Paar vorher gesund sein. Ein HA-Paar, dessen Standby seit Wochen nicht synchronisiert, ist während des Updates kein Paar, sondern ein Einzelgerät mit einem Zuschauer. Wie Synchronisation und Rollen funktionieren, erklärt HA-Paar, Failover und Konfig-Sync: zwei LoadMaster, ein Gedanke.



Skizze: Ablauf nach der Herstellerempfehlung; Zugriff auf die Knoten je nach HA-Aufbau über gemeinsame oder eigene Adresse

Vorbereitung: der bevorzugte Knoten muss weg

In den HA-Parametern lässt sich festlegen, dass eine Einheit bevorzugt aktiv sein soll. Das ist im Alltag bequem, beim Update aber hinderlich: Kommt der bevorzugte Knoten nach seinem Neustart zurück, holt er sich die Rolle sofort zurück, und du hast einen Failover mehr, als du wolltest, womöglich auf eine Einheit, die noch gar nicht fertig ist. Der Hersteller empfiehlt deshalb, vor dem Update die Option „Switch to Preferred Server“ unter System Configuration > HA Parameters auf „No Preferred Host“ zu stellen. Notiere dir den alten Wert, damit du ihn danach bewusst wieder setzen oder bewusst weglassen kannst.

Der Ablauf in fünf Schritten

- **Vorher sichern.** Konfigurationsbackup und Zertifikatsbackup ziehen, Lizenzdaten bereithalten, Firmware-Datei herunterladen und Prüfsumme kontrollieren, falls der Hersteller eine angibt.

- **Passive Einheit aktualisieren.** Firmware unter System Configuration > System Administration > Update Software hochladen, Update starten, nach Abschluss neu starten. Der Dienst läuft währenddessen auf der aktiven Einheit weiter.
- **Zustand prüfen.** Ist die aktualisierte Einheit wieder im Paar sichtbar, als Standby markiert und synchron? Erst dann geht es weiter. Ist sie es nicht, hast du jetzt noch alle Optionen.
- **Aktive Einheit aktualisieren.** Dasselbe auf der aktiven Einheit. Mit ihrem Neustart übernimmt die bereits aktualisierte Einheit. Das ist der einzige Failover im ganzen Ablauf.
- **Abnahme.** Virtual Services, Health Checks und Anmeldungen testen, Syslog lesen, neue Rollen dokumentieren.

Am Ende ist die ehemals passive Einheit aktiv. Das ist bei dieser Methode Absicht und in den meisten Umgebungen völlig egal. Wenn es dir nicht egal ist, etwa weil dein Monitoring oder deine Dokumentation fest von einer bestimmten aktiven Einheit ausgeht, gibt es die Alternative: aktive Einheit zuerst aktualisieren, dann manuell auf die passive umschalten, die zweite Einheit aktualisieren und zurückschalten. Das kostet einen zweiten Failover. Ehrlicher ist es meist, Monitoring und Dokumentation so zu bauen, dass sie mit beiden Rollenverteilungen leben können.

WARNUNG · Gemischte Firmware ist ein Zustand, kein Ziel

Zwischen Schritt 2 und Schritt 4 laufen beide Einheiten mit unterschiedlicher Firmware. Das ist für die Dauer des Updates vorgesehen, aber nicht für die nächsten drei Wochen. Ändere in dieser Zeit keine Konfiguration und beende das Update im selben Wartungsfenster. Wer nach Schritt 2 „morgen weitermacht“, hat ein Paar, bei dem unklar ist, was ein Failover in der Nacht anrichtet.

Was ein Failover für Exchange, ADFS und RDS bedeutet

Ein Failover ist kurz, aber nicht unsichtbar. Bestehende TCP-Verbindungen und Persistenz-Informationen überleben ihn je nach Konfiguration nicht. Für die Microsoft-Dienste heißt das:

Dienst	Was Benutzerinnen und Benutzer merken	Empfehlung
Exchange (OWA, Outlook, ActiveSync)	Outlook verbindet sich neu, OWA meist unbemerkt, mit ESP-Vorauthentifizierung ggf. erneute Anmeldung	Wartungsfenster außerhalb der Kernzeit, ESP-Sitzungsdauer berücksichtigen
SMTP	Eingehende Verbindungen brechen ab, sendende Server versuchen es erneut	Unkritisch, SMTP ist auf Wiederholung gebaut
ADFS und WAP	Laufende Anmeldungen schlagen fehl, bestehende Tokens bleiben gültig	Nicht zur Hauptanmeldezeit am Morgen
RD Gateway	Bestehende Sitzungen über das Gateway trennen sich und müssen neu aufgebaut werden	Das schmerzt am meisten. Ankündigen und nachts machen
SharePoint	Einzelne Seitenaufrufe scheitern, Neuladen hilft	Unkritisch, außer bei großen Uploads

Rollback: der Rückweg und wo er endet

Der LoadMaster behält nach einem Update das vorherige Firmware-Image. Unter System Configuration > System Administration > Update Software zeigt er die gespeicherte vorherige Version an und bietet die Schaltfläche „Restore Software“ an. Nach dem Zurückspielen startet das Gerät neu. Das klingt nach einem Netz mit doppeltem Boden, hat aber drei Einschränkungen, die du kennen musst, bevor du sie brauchst.

- **Nur ein Schritt zurück.** Es gibt genau ein vorheriges Image. Wer zwei Updates hintereinander einspielt, etwa über ein Gateway-Release, kommt per Knopfdruck nur auf das Gateway-Release zurück, nicht auf den Ausgangsstand.
- **Konfiguration mit Zeitstempel.** Beim Rücksprung landet die Konfiguration auf dem Stand zum Zeitpunkt des Updates. Alles, was du nach dem Update geändert hast, ist weg. Hast du Änderungen gemacht, gehört nach dem Rücksprung das passende Backup dazu.
- **Verbotene Downgrades.** Der Hersteller warnt ausdrücklich davor, von 7.2.36 oder neuer auf einen Stand unter 7.2.36 zurückzugehen: Das Gerät wird unerreichbar und lässt sich nicht wiederherstellen. Außerdem verweigert ein LoadMaster ab 7.2.62 den Wechsel auf Stände vor 7.2.61.1. Prüfe vor jedem Downgrade die Hinweise zur Zielversion.

TIPP · Der Hypervisor-Snapshot ist kein Restore

Bei virtuellen LoadMastern unter Hyper-V oder VMware liegt der Gedanke nahe, vor dem Update einfach einen Snapshot zu ziehen. Der Hersteller stellt aber klar, dass Snapshots nicht geeignet sind, einen LoadMaster in einen funktionierenden Zustand zurückzuversetzen. Lizenzbindung, HA-Zustand und Gerätezustand passen danach nicht zusammen. Der saubere Rückweg führt über „Restore Software“ und das Konfigurationsbackup.

Wartungsfenster: kurz planen, lang reservieren

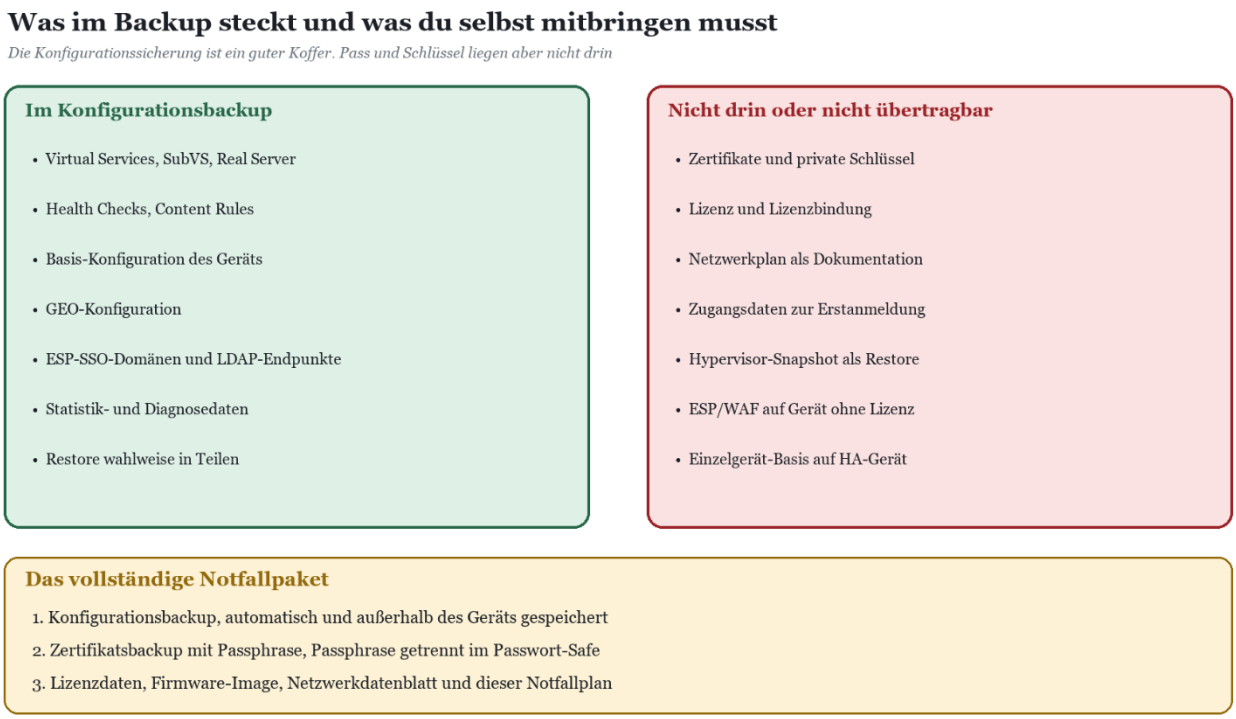
Ein Firmware-Update im HA-Paar dauert in der Praxis selten länger als eine halbe Stunde. Reserviere trotzdem zwei. Die Zeit brauchst du nicht für das Update, sondern für die Abnahme und für den Fall, dass du zurück musst. Ein Rollback mit Backup-Restore, erneutem Test und Kontrolle beider Knoten frisst schnell eine Stunde. Wenn das Wartungsfenster dann schon vorbei ist, beginnt das Herzrasen, das dieser Artikel verhindern will.

Zeitpunkt	Was passiert
Eine Woche vorher	Release Notes lesen, Kanal und Zielversion festlegen, Upgrade-Pfad prüfen, Wartungsfenster ankündigen, Labor- oder Testgerät aktualisieren, falls vorhanden
Ein Tag vorher	Backup und Zertifikatsbackup ziehen und Wiederherstellbarkeit prüfen, HA-Zustand kontrollieren, Firmware-Datei bereitlegen, Notfallplan ausdrucken
Im Fenster, Minute 0	Bevorzugten Knoten deaktivieren, aktuellen Stand dokumentieren
Minute 5 bis 30	Passive Einheit aktualisieren und prüfen, aktive Einheit aktualisieren
Minute 30 bis 60	Abnahme mit Testliste, Syslog lesen, Monitoring prüfen
Danach	HA-Einstellung wiederherstellen, neues Backup ziehen, Dokumentation aktualisieren

Wenn du mehrere LoadMaster oder Standorte betreibst, lohnt sich ein zentraler Blick auf die Firmware-Stände. Kemp 360 Central zeigt sie gesammelt an und kann Updates auf ausgewählten Geräten anstoßen. Mehr dazu in Kemp 360 Central und Global Server Load Balancing für mehrere Standorte.

Konfigurationssicherung: was drin ist und was fehlt

Das Backup des LoadMasters ist ein unscheinbarer Knopf mit großer Wirkung. Er erzeugt eine Datei, mit der du ein Gerät in Minuten auf einen bekannten Stand bringst. Vorausgesetzt, du hast die Datei noch, wenn das Gerät nicht mehr da ist. Ein Backup, das ausschließlich auf dem LoadMaster selbst oder auf dem Rechner der Kollegin liegt, die seit letztem Jahr in Elternzeit ist, ist ein schöner Gedanke, aber keine Sicherung.



Skizze: Inhalte nach Herstellerdokumentation zusammengefasst; Details abhängig von Firmware-Stand und Lizenz

Manuelles Backup vor jeder Änderung

Unter System Configuration > System Administration > Backup/Restore erzeugst du die Sicherungsdatei auf Knopfdruck. Sie enthält die Konfiguration der Virtual Services, die lokalen Geräteeinstellungen und Statistik- sowie Diagnosedaten. Beim Zurückspielen kannst du auswählen, welche Teile du wiederherstellst: VS Configuration, LoadMaster Base Configuration, GEO Configuration und ESP SSO Configuration. Letztere bringt SSO-Domänen, LDAP-Endpunkte und Bildsätze für Anmeldeformulare zurück, aber nicht die Virtual Services selbst. Die brauchen zusätzlich die VS Configuration.

Die Faustregel ist einfach: Vor jedem Update, vor jeder größeren Änderung und nach jeder erfolgreichen Änderung ziehst du ein Backup. Der Dateiname bekommt Datum, Gerät und Anlass, zum Beispiel lm01-2026-10-28-vor-update. Drei Monate später weißt du sonst nicht mehr, welche der elf Dateien mit Namen „backup“ die richtige ist.

Automatisches Backup an ein Ziel außerhalb des Geräts

Auf derselben Seite lässt sich ein automatisches Backup einschalten. Der LoadMaster schickt die Sicherung dann täglich oder wöchentlich zu einer festen Uhrzeit an einen entfernten Server. Zur Wahl stehen FTP, SCP und SFTP. FTP ist unverschlüsselt und hat in einer Umgebung, in der die Datei die komplette Veröffentlichung deiner Exchange- und ADFS-Infrastruktur beschreibt, nichts verloren. Für SCP und SFTP hinterlegst du einen privaten Schlüssel. Ein Test-Knopf prüft die Einstellungen, das Ergebnis steht im System Message File.

Methode	Verschlüsselt	Anmeldung	Bewertung
FTP	Nein	Benutzer und Kennwort	Nur im Labor. Datei und Kennwort gehen im Klartext über das Netz
SCP	Ja	Benutzer und privater Schlüssel	Gut, wenn ein SSH-Ziel vorhanden ist
SFTP	Ja	Benutzer und privater Schlüssel	Empfehlung. Unter Windows Server mit dem integrierten OpenSSH-Server als Ziel umsetzbar

TIPP · SFTP-Ziel auf Windows Server

Windows Server bringt seit Version 2019 einen OpenSSH-Server als optionales Feature mit, ab Windows Server 2025 ist er bereits installiert und muss nur aktiviert werden. Ein eigener Benutzer nur für die Backups, ein eigenes Verzeichnis und eine Firewall-Regel, die nur die Management-Adressen der LoadMaster zulässt, ergeben ein sauberes Backup-Ziel ohne Zusatzsoftware. Das Verzeichnis gehört anschließend in deine reguläre Datensicherung, sonst hast du nur das Problem verschoben. Wer die Sicherung lieber per Skript zieht, findet den Weg in Automatisierung per REST-API und PowerShell.

FAKTEN · Backup im HA-Paar

Im HA-Paar sichert das automatische Backup nur die Konfiguration der aktiven Einheit. Die passive Einheit spiegelt sie ohnehin. Beim Wiederherstellen gilt aber: Eine Basis-Konfiguration eines Einzelgeräts lässt sich nicht auf ein HA-Gerät zurückspielen und umgekehrt. Die Virtual-Service-Konfiguration ist davon nicht betroffen.

Zertifikate: das eigene Backup mit Passphrase

Die Konfigurationssicherung enthält keine Zertifikate und keine privaten Schlüssel. Für sie gibt es im Zertifikatsbereich der WUI eine eigene Sicherung, die mit einer Passphrase verschlüsselt wird. Das ist sicherheitlich richtig, organisatorisch aber eine Falle: Ohne Passphrase ist die Datei wertlos, und die Passphrase steht erfahrungsgemäß nirgendwo. Lege sie im Passwort-Safe des Teams ab, nicht in der Datei daneben. Für Zertifikate aus der internen PKI kannst du dir zur Not ein neues ausstellen lassen. Für öffentliche Zertifikate vor Exchange und ADFS bedeutet ein verlorener Schlüssel einen neuen Antrag, und das am Tag des Ausfalls. Wo welche Zertifikate am LoadMaster sitzen, beschreibt TLS-Offload, Re-Encryption und Zertifikate: PKI trifft LoadMaster.

Nach jedem Zertifikatstausch gehört ein neues Zertifikatsbackup dazu. Die Sicherung vom letzten Jahr enthält das abgelaufene Zertifikat, und das hilft dir im Notfall genau so viel wie gar keins.

Lizenz und Netzwerk: das, was keiner sichert

Auch die Lizenz steckt nicht im Backup. Sie hängt an der Instanz und wird über die Lizenzverwaltung des Herstellers aktiviert, online mit dem Herstellerkonto oder offline über eine Lizenzdatei. Für eine neue Instanz brauchst du also Zugang zum Herstellerkonto, die Zuordnung der Lizenz und im Zweifel den Herstellersupport, um eine Lizenz von einer defekten auf eine neue Instanz zu übertragen. Welche Modelle es gibt und was eine Subscription bedeutet, steht in Editionen, Lizenzierung und Sizing: welcher LoadMaster für welchen Laden.

Das Netzwerk ist ein Sonderfall. Teile davon stecken in der Basis-Konfiguration, aber bevor du überhaupt etwas zurückspielen kannst, braucht die neue Instanz eine erreichbare Management-Adresse, die du an der Konsole vergibst. Dazu kommen Dinge, die außerhalb des LoadMasters liegen: VLAN-Zuordnung der virtuellen Netzwerkkarten im Hyper-V oder im vSwitch, Firewall-Regeln und NAT, die auf bestimmte Adressen zeigen, statische Routen und MAC-Adressfilter. Ein einseitiges Netzwerkdatenblatt pro LoadMaster mit Adressen, Masken, Gateways, VLANs, Interfaces und HA-Adressen ist im Ernstfall Gold wert.

Was	Im Konfigurationsbackup	Wie du es sicherst
Virtual Services, SubVS, Real Server, Content Rules	Ja	Konfigurationsbackup
Basis-Einstellungen des Geräts	Ja, nur auf gleichartiges	Konfigurationsbackup

	Gerät	
ESP-SSO-Domänen, LDAP-Endpunkte	Ja	Konfigurationsbackup, Restore-Option ESP SSO
Zertifikate und private Schlüssel	Nein	Zertifikatsbackup mit Passphrase
Lizenz	Nein	Herstellerkonto, Lizenzdaten, Supportkontakt
Management-Erstzugang, Hypervisor-Netz	Nein	Netzwerkdatenblatt
Kerberos-Konto und Keytab für KCD	Teilweise	Dokumentation, Keytab sicher verwahren
Firmware-Image	Nein	Installierte Version als Datei ablegen

Gerade die Kerberos-Seite verdient einen Moment Aufmerksamkeit. Wer am LoadMaster KCD nutzt, hat im Active Directory ein Dienstkonto mit Delegationsrechten und SPNs, und der LoadMaster braucht dessen Schlüssel. Beides überlebt den Verlust des LoadMasters im AD, aber du musst wissen, wie es zusammengehört. Die Details stehen in Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten.

Wenn es doch knallt: Wiederherstellung und Notbetrieb per DNS

Irgendwann ist der LoadMaster einfach weg. Hardware defekt, VM gelöscht, Datastore kaputt, Update gescheitert und kein Rückweg mehr. Dann gibt es zwei Wege: eine neue Instanz aus dem Backup aufbauen oder die Dienste vorübergehend ganz ohne LoadMaster betreiben. Oft brauchst du beides nacheinander.

Wiederherstellung auf eine neue Instanz



Skizze: Reihenfolge als Empfehlung; Details je nach Plattform (Hardware, Hyper-V, VMware, Azure)

Die Reihenfolge ist entscheidend. Zuerst stellst du eine neue Instanz auf derselben Plattform bereit und bringst sie auf den Firmware-Stand, aus dem das Backup stammt, nicht auf den neuesten. Dann vergibst du an der Konsole eine Management-Adresse. Bevor du die Konfiguration einspielst, aktivierst du die Lizenz. Das ist kein Formalismus: Eine Konfiguration mit ESP-fähigen Virtual

Services lässt sich nur auf ein Gerät zurückspielen, das für ESP lizenziert ist, und eine WAF-Konfiguration nur auf eins mit WAF-Lizenz. Erst dann folgen Konfiguration und Zertifikate.

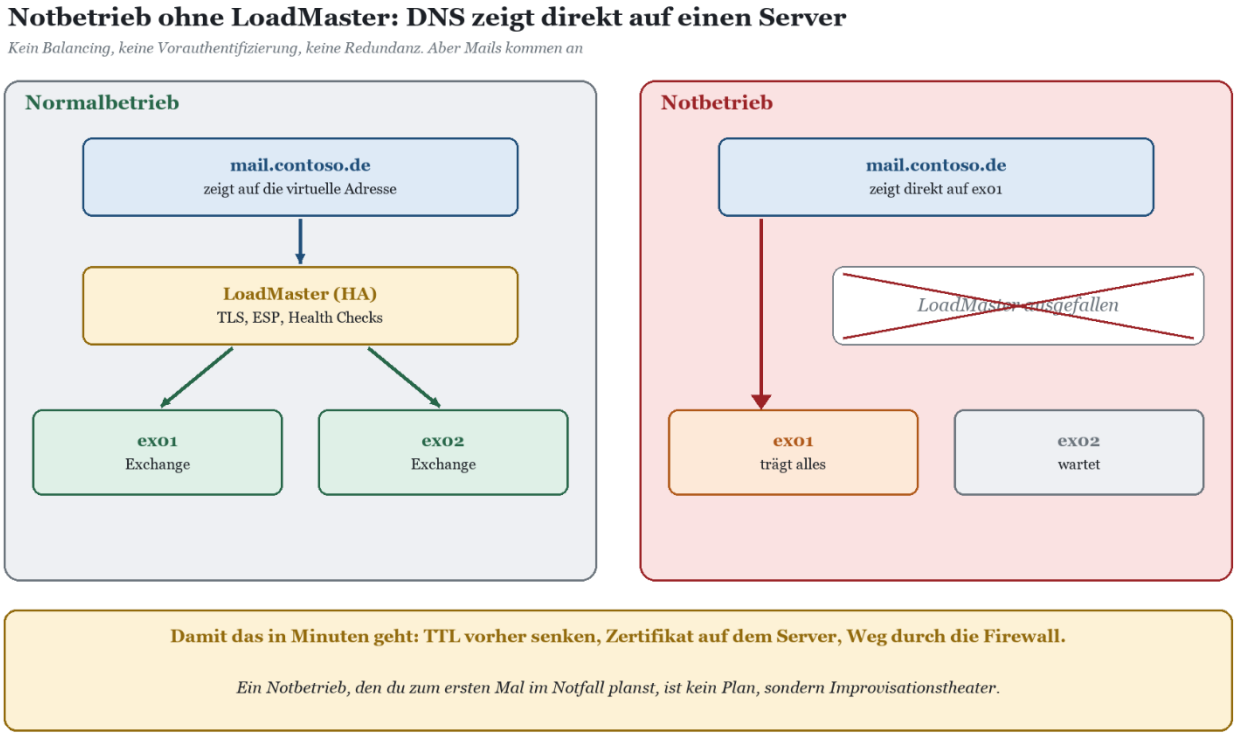
WARNUNG · Doppelte Adressen beim Paralleltest

Wenn du die Wiederherstellung testest, während die alte Instanz noch läuft, und dabei die Basis-Konfiguration einspielst, übernimmt die neue Instanz auch deren Netzwerkeinstellungen. Zwei Geräte mit derselben virtuellen Adresse im selben Netz sind ein hervorragender Weg, Exchange für alle unerreichbar zu machen. Teste Restores in einem isolierten Netz oder spiele dort nur die VS-Konfiguration ein.

Nach dem Restore kommt die Abnahme wie nach einem Update, ergänzt um die Dinge, die nicht im Backup stecken: Syslog-Ziele erreichen ihre Empfänger, das Monitoring kennt die neue Instanz, Kerberos-Delegation funktioniert, Firewall-Regeln passen zu möglicherweise neuen MAC-Adressen. Wie du die neue Instanz wieder ins Monitoring holst, beschreibt Monitoring, Syslog und SNMP: den LoadMaster ins Monitoring holen. Bei einem HA-Paar baust du zuerst eine Einheit auf, bringst die Dienste in Betrieb und koppelst die zweite danach dazu.

Notbetrieb ohne LoadMaster per DNS

Wenn gar kein LoadMaster mehr da ist und die Wiederherstellung dauert, bleibt der älteste Trick der Welt: DNS-Namen direkt auf einen Server zeigen lassen. Statt auf die virtuelle Adresse am LoadMaster zeigt mail.contoso.de dann intern auf ex01 und extern über die Firewall-Veröffentlichung auf denselben Server. Das ist kein Load Balancing, keine Redundanz und keine Vorauthentifizierung. Aber Postfächer sind erreichbar, und das ist am Tag des Ausfalls die einzige Kennzahl, die interessiert.



Skizze: Beispielnamen aus contoso.de; intern und extern gelten ggf. getrennte DNS-Zonen

Damit das im Ernstfall in Minuten statt Stunden geht, musst du es vorher vorbereiten. Die folgenden Punkte entscheiden, ob der Notbetrieb trägt.

Dienst	Notbetrieb per DNS	Vorbereitung	Stolperstein

Exchange	Namespace auf einen Postfachserver	Zertifikat mit allen Namen auf jedem Server, nicht nur am LoadMaster	Mit TLS-Offload liegt das öffentliche Zertifikat oft nur am LoadMaster
SMTP eingehend	MX bzw. Firewall-NAT auf einen Server	Empfangsconnector für anonyme Mails auf dem Zielserver	Connector unterscheidet ggf. nach Quell-IP des LoadMasters
ADFS	sts.contoso.de auf einen ADFS- bzw. WAP-Server	SSL-Zertifikat auf allen Farmknoten	Ohne WAP wäre ADFS direkt im Internet, nur extern über WAP
RDS	Gateway-Name auf einen RD Gateway-Server	Zertifikat und Ressourcenrichtlinien auf jedem Gateway	Connection Broker braucht den Namen der Farm, nicht des Servers
SharePoint	Webanwendung auf einen Webfrontend-Server	Bindung und Zertifikat im IIS je Server	Mit Kerberos SPN am Dienstkonto, nicht am Server prüfen
Eigenentwicklungen	Name auf einen Server	Zertifikat und Bindung je Server	Sitzungen ohne Persistenz, In-Memory-Session ist dann egal

WICHTIG · Notbetrieb heißt bewusst auf Schutz verzichten

Am LoadMaster hängen oft Vorauthentifizierung mit ESP, WAF-Regeln und Geoblocking. Im DNS-Notbetrieb fällt all das weg, und OWA steht direkt im Internet. Für eine Nacht kann das die richtige Entscheidung sein, sie gehört aber in den Notfallplan, mit Namen der Person, die sie trifft, und einer Frist. Interne Dienste per DNS umzuleiten ist unproblematisch. Externe Veröffentlichungen ohne Vorauthentifizierung sind ein Risiko auf Zeit. Was ESP schützt, beschreibt Edge Security Pack: Vorauthentifizierung, SSO-Domänen und der TMG-Ersatz.

Zwei Details machen den Unterschied zwischen fünf Minuten und fünf Stunden. Erstens die TTL: Steht der A-Record auf 24 Stunden, nutzen Clients und Resolver die alte Adresse bis morgen weiter. Eine TTL von fünf bis fünfzehn Minuten für veröffentlichte Namen ist ein vernünftiger Kompromiss. Zweitens Kerberos: Läuft die Anmeldung über ein gemeinsames Dienstkonto mit SPN, etwa die Alternate Service Account Credential bei Exchange, funktioniert Kerberos auch direkt am Server, solange der Name gleich bleibt. Wer stattdessen die SPNs am Computerkonto registriert hat, sollte das vorher klären. Hintergründe stehen in SPN-Probleme hinter dem Load Balancer: ein Name, mehrere Server.

AUS DER PRAXIS · Der Notbetrieb, der nie geübt wurde

Ein typischer Verlauf: Der LoadMaster einer Verwaltung fällt nach einem Stromausfall aus, das Team stellt mail.contoso.de auf einen Exchange-Server um. Intern geht alles. Extern zeigt jedes Smartphone eine Zertifikatswarnung, denn das öffentliche Zertifikat lag nur am LoadMaster, auf den Exchange-Servern war das selbst signierte Standardzertifikat gebunden. Der Export vom LoadMaster war nicht mehr möglich, das Zertifikatsbackup hatte keine bekannte Passphrase. Ein neues Zertifikat kam am Nachmittag. Seitdem ist das öffentliche Zertifikat auf allen Exchange-Servern gebunden, auch wenn der LoadMaster es nicht braucht.

Die Checkliste für den Kühlschrank

Alles zusammen passt auf eine Seite. Druck sie aus und häng sie dorthin, wo du sie um 22 Uhr im Wartungsfenster findest.

CHECKLISTE · Firmware-Update, Backup und Notfallplan

Vor dem Update: Kanal und Zielversion festgelegt, Release Notes nach Upgrade-Pfad, Known Issues, TLS, ESP und WAF durchsucht, Wartungsfenster angekündigt.

Sicherung: Konfigurationsbackup gezogen und außerhalb des Geräts abgelegt, Zertifikatsbackup mit Passphrase im Passwort-Safe, Lizenzdaten und Herstellerkonto erreichbar.

HA-Paar: beide Einheiten sichtbar und synchron, bevorzugter Knoten deaktiviert, alter Wert notiert.

Update: erst passive Einheit, Neustart, Kontrolle, dann aktive Einheit. Kein Konfigurationswechsel zwischendurch, Update im selben Fenster abschließen.

Abnahme: Testliste für Exchange, ADFS, RDS, SharePoint abgearbeitet, Syslog gelesen, Monitoring grün.

Danach: HA-Einstellung zurück, neues Backup, Dokumentation und Firmware-Stand aktualisiert.

Rückweg: Restore Software kennt nur einen Schritt zurück. Verbotene Downgrades geprüft.

Dauerhaft: automatisches Backup per SFTP aktiv und getestet, Netzwerkdatenblatt aktuell, Zertifikate auch auf den Real Servern, TTL der veröffentlichten Namen kurz, DNS-Notbetrieb mindestens einmal im Jahr geübt.

Wenn du die Checkliste auf deine Umgebung zuschneiden, ein überfälliges Update mit Gateway-Release begleiten lassen oder den Notbetrieb einmal durchspielen möchtest, hilft dir die Beratung zum Kemp LoadMaster. Wer Update, Failover und Restore lieber einmal gefahrlos im Labor erleben will, findet das in der Kemp-LoadMaster-Schulung.

FAQ: Firmware-Update, Backup und Notfallplan am Kemp LoadMaster

Welchen Release-Kanal sollte ich für den Produktivbetrieb wählen?

In den meisten Fällen LTSF. Der Hersteller empfiehlt ihn für Produktivumgebungen, solange du keine Funktion oder Korrektur brauchst, die nur im GA-Zweig enthalten ist.

Wie oft sollte ich die Firmware aktualisieren?

Sicherheitsupdates zeitnah, besonders bei Lücken in der Verwaltungsoberfläche oder im Datenpfad. Für Funktionsupdates reicht ein geplanter Takt, etwa zwei- bis viermal im Jahr.

Welche Einheit aktualisiere ich im HA-Paar zuerst?

Die passive. Nach ihrem Neustart und einer Kontrolle folgt die aktive Einheit, deren Neustart den einzigen Failover auslöst.

Warum soll ich den bevorzugten Knoten vor dem Update deaktivieren?

Weil der bevorzugte Knoten sich nach seinem Neustart sonst sofort die aktive Rolle zurückholt. Das verursacht zusätzliche Failover und kann eine unfertige Einheit aktiv machen.

Kann ich ein Firmware-Update rückgängig machen?

Ja, über „Restore Software“ auf die zuletzt installierte Version. Es gibt aber nur einen Schritt zurück, Änderungen nach dem Update gehen verloren, und manche Downgrades sind ausdrücklich nicht erlaubt.

Enthält das Backup meine Zertifikate?

Nein. Zertifikate und private Schlüssel sicherst du separat mit einer Passphrase. Auch die Lizenz ist nicht im Konfigurationsbackup enthalten.

Reicht ein Snapshot der virtuellen Maschine als Backup?

Nein. Der Hersteller schließt Hypervisor-Snapshots als Methode zur Wiederherstellung eines funktionierenden LoadMasters aus. Nutze das Konfigurationsbackup.

Welche Übertragungsmethode sollte ich für automatische Backups nutzen?

SFTP oder SCP mit privatem Schlüssel. FTP überträgt Datei und Kennwort unverschlüsselt.

Kann ich ein Backup eines HA-Paars auf ein Einzelgerät zurückspielen?

Die Virtual Services ja, die Basis-Konfiguration nicht. Sie lässt sich nur zwischen gleichartigen Geräten übertragen, also Einzelgerät zu Einzelgerät oder HA zu HA.

Wie betreibe ich Exchange, wenn der LoadMaster komplett ausfällt?

Indem du die DNS-Namen und die Firewall-Veröffentlichung direkt auf einen Exchange-Server zeigen lässt. Das setzt voraus, dass das passende Zertifikat auf dem Server gebunden ist und die TTL kurz genug ist. Einzelheiten zur Veröffentlichung stehen in Exchange Server hinter dem LoadMaster: Templates, Namespaces, Health Checks.

Fazit: Langweilige Updates sind gute Updates

Ein Firmware-Update am LoadMaster ist kein Abenteuer, sondern ein Handgriff, wenn das Drumherum stimmt. Der richtige Kanal, ein Blick in die Release Notes, ein Backup mit Zertifikaten und bekannter Passphrase, ein gesundes HA-Paar ohne bevorzugten Knoten und ein Wartungsfenster mit Luft: Dann ist das Update nach einer halben Stunde erledigt, und der spannendste Moment ist die Frage, ob jemand den Failover überhaupt bemerkt hat.

Der eigentliche Wert liegt aber im Teil, den du hoffentlich nie brauchst. Ein automatisches Backup außerhalb des Geräts, ein Netzwerkdatenblatt, Zertifikate auf den Real Servern und ein geübter DNS-Notbetrieb verwandeln den Totalausfall von einer Katastrophe in eine unangenehme Nacht. Und eine unangenehme Nacht, nach der am Morgen alle Mails da sind, ist im Betrieb so etwas wie ein Kompliment.

WEITERLESEN · Weiter im Thema

› HA-Paar, Failover und Konfig-Sync: zwei LoadMaster, ein Gedanke
› Automatisierung per REST-API und PowerShell
› TLS-Offload, Re-Encryption und Zertifikate: PKI trifft LoadMaster
› Kemp 360 Central und Global Server Load Balancing für mehrere Standorte
› Monitoring, Syslog und SNMP: den LoadMaster ins Monitoring holen
› Editionen, Lizenzierung und Sizing: welcher LoadMaster für welchen Laden