Kemp LoadMaster in Microsoft-Umgebungen: Praxiswissen für Admins

Der Kemp LoadMaster ist in vielen deutschen Rechenzentren das, was der Türsteher für den Club ist: Jeder muss an ihm vorbei, keiner redet über ihn – bis er jemanden nicht reinlässt. Dann steht plötzlich die halbe IT-Abteilung vor der Tür und diskutiert, warum Outlook seit dem Zertifikatstausch nur noch Passwortabfragen produziert.

Dieser Kompetenzbereich schließt die Lücke, die zwischen der Dokumentation von Progress Kemp und Microsoft Learn klafft. Kemp erklärt dir sehr ordentlich, welcher Knopf wo sitzt. Microsoft erklärt dir sehr ordentlich, wie Exchange, SharePoint und ADFS funktionieren. Was dir keiner erklärt: was passiert, wenn beides aufeinandertrifft. **Genau da setzen die Artikel hier an** – deutschsprachig, aus echten Projekten und mit einer klaren Microsoft-Brille.

WISSEN
30 Fachartikel
Von Virtual Service bis KCD: alles, was hinter dem LoadMaster schiefgehen kann – und wie du es geraderückst.
Zur Themenübersicht

BERATUNG
Kemp-Beratung
Konfiguration prüfen, Kerberos zum Laufen bringen, Exchange und Co. sauber veröffentlichen.
Zur Beratungsseite

SCHULUNG
Kemp-Schulung
Ein Tag online für Microsoft-Administratorinnen und -Administratoren, mit echten Übungen.
Zur Schulungsseite

Faktenkasten: Kemp LoadMaster auf einen Blick

- **Was:** Application Delivery Controller (Load Balancer mit Layer-7-Funktionen), heute Teil des Produktportfolios von Progress
- **Formen:** Hardware-Appliance, virtueller LoadMaster für Hyper-V und VMware, Images für Azure und AWS
- **Edge Security Pack (ESP):** Reverse Proxy, Vorauthentifizierung, Single Sign-on, AD- und RADIUS-Anbindung, Kerberos Constrained Delegation – laut Hersteller in allen LoadMaster-Modellen enthalten
- **Typische Einsatzorte:** Exchange Server, SharePoint Server, ADFS, Remote Desktop Services, Eigenentwicklungen und Hersteller-APIs
- **Historischer Hintergrund:** ESP wurde ausdrücklich als Ersatz für Microsofts eingestellten Forefront TMG positioniert

Warum der LoadMaster ein eigenes Thema verdient

Ein Load Balancer klingt nach Infrastruktur-Klempnerei: Verkehr rein, Verkehr auf zwei Server verteilen, fertig. In Microsoft-Umgebungen stimmt das ungefähr so wie „ein Auto bringt dich von A nach B“. Es stimmt – solange niemand nach Bremsen fragt.

Der LoadMaster sitzt an der empfindlichsten Stelle deiner Umgebung: Er terminiert TLS, entscheidet über Authentifizierung, schreibt Header um, fängt Angriffe ab und verteilt

Verbindungen an Server, deren Eigenheiten er kennen muss. Jede dieser Aufgaben hat Microsoft-spezifische Fallstricke, und die meisten fallen erst auf, wenn ein Benutzer anruft.

Der LoadMaster als Türsteher vor deinen Microsoft-Diensten

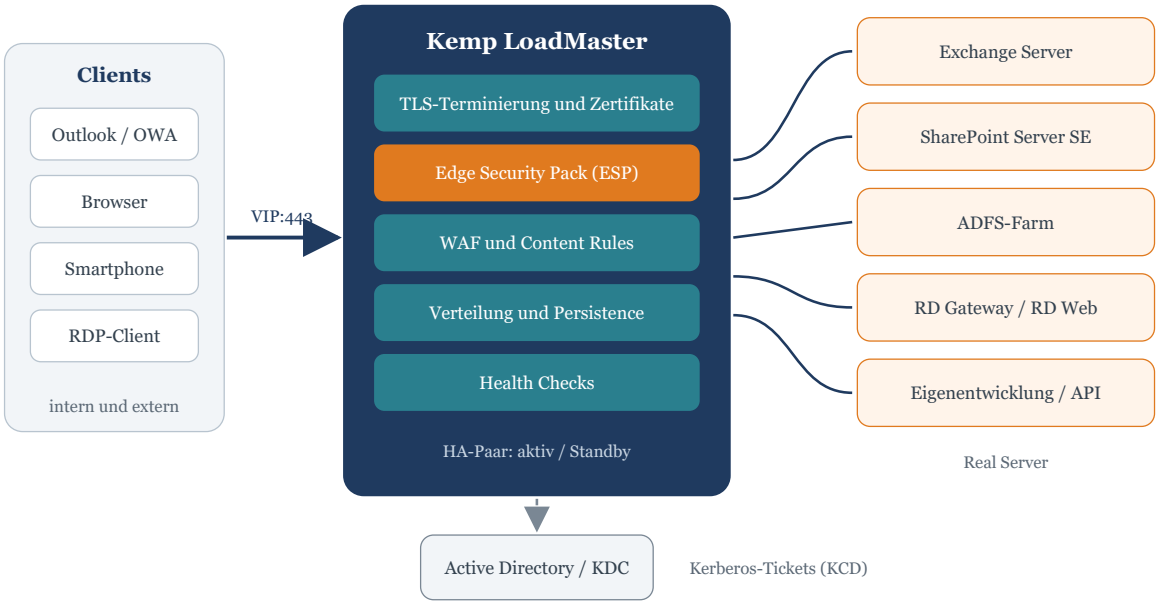


Abbildung 1: Der LoadMaster zwischen Clients, Microsoft-Diensten und Active Directory

Die Skizze zeigt, warum der LoadMaster so viel Einfluss hat: Alles, was von außen (und oft auch von innen) auf Exchange, SharePoint oder ADFS zugreift, läuft durch ein einziges Gerät – und dieses Gerät spricht mit dem Active Directory, wenn Kerberos-Delegation im Spiel ist. Fällt eine dieser Schichten falsch aus, sieht der Benutzer nur „geht nicht“.

Die fünf Aufgaben des LoadMasters in Microsoft-Umgebungen

Aufgabe	Was dabei passiert	Typischer Microsoft-Stolperstein
Verteilen	Verbindungen auf mehrere Real Server, mit oder ohne Persistence	Persistence dort, wo sie nicht nötig ist, oder Quell-IP-Persistence hinter einem NAT
Prüfen	Health Checks entscheiden, welcher Server Verkehr bekommt	TCP-Check meldet „gesund“, obwohl der Exchange-Dienst längst hängt
Verschlüsseln	TLS-Terminierung, Re-Encryption, Zertifikate, Cipher-Sets	Zertifikat nur auf einer Seite erneuert, oder Alt-Clients ohne SNI
Authentifizieren	Vorauthentifizierung per ESP, SSO, KCD zum Server	SPN, Delegation, RC4/AES – der Klassiker schlechthin
Schützen	WAF, Content Rules, Geoblocking, Header-Härtung	WAF blockiert Outlook im Web, SNAT macht SMTP zum offenen Relay

Aus der Praxis: „Wir haben nichts geändert“

Ein Mittelständler meldet: Seit Montag fragt Outlook ständig nach dem Passwort. Geändert habe man nichts. Nach einer halben Stunde stellt sich heraus: Am Wochenende wurde das Exchange-Zertifikat erneuert – auf den Exchange-Servern. Der LoadMaster präsentiert weiter das alte, das inzwischen abgelaufen ist, und Re-Encryption zum Backend klappt nur noch mit Glück.

Die Lehre: Beim LoadMaster gibt es kein „nichts geändert“. Es gibt nur „an der anderen Seite etwas geändert“. Mehr dazu in TLS-Offload, Re-Encryption und Zertifikate: PKI trifft LoadMaster.

Kerberos hinter dem LoadMaster: die Königsdisziplin

Wenn es eine Disziplin gibt, an der LoadMaster-Projekte regelmäßig scheitern, dann ist es Kerberos. Das liegt nicht am LoadMaster, sondern daran, dass Kerberos Namen ernst nimmt: Der Client fordert ein Ticket für den Namen an, den er sieht – also für den Namen des Virtual Service, nicht für den Server dahinter. Wer das verinnerlicht hat, hat die halbe Miete. Die Grundlagen dazu findest du im Kerberos-Kompetenzbereich.

Richtig spannend wird es, wenn der LoadMaster selbst die Authentifizierung übernimmt. Mit dem Edge Security Pack meldet sich der Benutzer am LoadMaster an – per Formular, Zertifikat oder SAML –, und der LoadMaster besorgt sich per **Kerberos Constrained Delegation (KCD)** im Namen des Benutzers ein Ticket für den eigentlichen Server. Das ist elegant, weil der Client kein Kerberos können muss. Es ist aber auch die Stelle, an der die meisten Stunden verbrannt werden.

Kerberos Constrained Delegation am LoadMaster

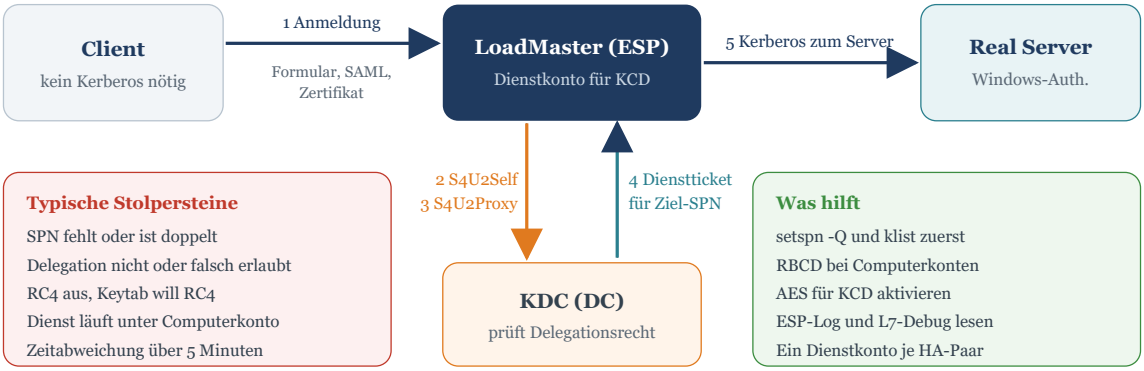


Abbildung 2: So holt sich der LoadMaster per KCD ein Ticket im Namen des Benutzers

Achtung: Die RC4-Falle

Viele Domänen sind inzwischen gehärtet und erlauben nur noch AES für Kerberos. Ein LoadMaster, der für KCD noch RC4 anfordert, bekommt dann vom Domänencontroller eine Absage – Fehlerbild „Verschlüsselungstyp nicht unterstützt“. Die Lösung liegt meist in einer AES-Option für KCD am LoadMaster und sauber gesetzten Verschlüsselungstypen am Dienstkonto.

> Weil Microsoft RC4 für Kerberos schrittweise abkündigt, trifft das früher oder später jede Umgebung. Details in Die RC4-Falle: KCD-Keytab trifft AES-only-Domäne.

Ein zweiter Klassiker: Dienste, die unter dem **Computerkonto** laufen statt unter einem Dienstkonto. Klassische KCD wird dann unhandlich, weil die Delegation am Konto des LoadMasters gepflegt werden muss und das Zielkonto je Server anders heißt. Hier ist **resource-based constrained delegation (RBCD)** die sauberere Lösung: Der Zielserver erlaubt selbst, wer an ihn delegieren darf. Wie das konkret geht, steht in Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten.

Szenario	Empfehlung	Weiterlesen
Client spricht Kerberos, LoadMaster reicht durch	SPN auf den VIP-Namen, gemeinsames Dienstkonto oder ASA	SPN-Probleme hinter dem Load Balancer: ein Name, mehrere Server
LoadMaster authentifiziert, Server will Kerberos	ESP mit KCD, AES aktivieren	Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten
Server laufen unter Computerkonten	RBCD statt klassischer KCD	Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten
Kerberos ist zu aufwendig, Lösung läuft bald aus	NTLM-Proxy prüfen, Nachteile kennen	NTLM, NTLM-Proxy und der Kerberos-Fallback, den keiner bemerkt
Externe Benutzer mit Entra ID und MFA	SAML/OIDC zum Client, KCD zum Server	SAML, OIDC und Entra ID: der LoadMaster als moderner Identitätsvermittler

Microsoft-Workloads hinter dem LoadMaster

Jeder Microsoft-Dienst hat seine eigene Persönlichkeit. Exchange ist seit Version 2013 erstaunlich pflegeleicht, solange du ihm die richtigen Health Checks gönnst. SharePoint ist sensibel bei Namen und Authentifizierung. ADFS will SNI und hat eine eigene Probe-Seite. Und SMTP ist der Kandidat, bei dem ein falsch gesetzter Haken aus deinem Mailserver ein offenes Relay macht.

Workload	Worauf es ankommt	Artikel
Exchange Server	Protokollspezifische Health Checks, keine Persistence nötig, Namespaces planen	Exchange Server hinter dem LoadMaster: Templates, Namespaces, Health Checks
SMTP	Quell-IP für Empfangsconnectors, SNAT vs. Transparenz	SMTP über den LoadMaster: Relay, Empfangsconnectors und die echte Absender-IP

Workload	Worauf es ankommt	Artikel
SharePoint Server SE	AAM, Kerberos mit gemeinsamem Dienstkonto, Health Check mit Anmeldung	SharePoint Server Subscription Edition hinter dem LoadMaster
ADFS und WAP	SNI, /adfs/probe, Client-IP für Extranet Lockout	ADFS und Web Application Proxy mit dem LoadMaster: Farm, Probe, SNI
Remote Desktop Services	RD Gateway mit UDP, Persistence, Connection Broker	Remote Desktop Services: RD Gateway, RD Web und Connection Broker balancieren
Eigenentwicklungen	Windows-Authentifizierung, http.sys, Health-Endpunkt	IIS-Eigenentwicklungen und http.sys-Dienste veröffentlichen

> **Tipp: Templates sind ein Anfang, kein Ende**
> Kemp liefert für viele Microsoft-Workloads fertige Templates. Nimm sie – aber lies hinterher, was sie eingestellt haben. Templates kennen deine Namespaces nicht, deine Authentifizierung nicht und deine Zertifikate schon gar nicht. Ein Template ist wie ein Fertigteilhaus: Steht schnell, aber die Steckdosen musst du trotzdem selbst setzen.

Security am Rand: mehr als nur verteilen

Weil der LoadMaster ohnehin jede Anfrage sieht, ist er der natürliche Ort für Schutzmaßnahmen: Vorauthentifizierung, bevor überhaupt ein Paket deinen Exchange erreicht, eine Web Application Firewall, Geoblocking gegen automatisierte Angriffe und Content Rules, die verräterische Header entfernen. Das funktioniert hervorragend – wenn du die Microsoft-Dienste dahinter kennst. Sonst blockiert die WAF fröhlich die eigene Belegschaft.

- Vorauthentifizierung und Zwei-Faktor: MFA vor OWA, ECP und Co.: Zwei-Faktor am LoadMaster
- WAF und Geoblocking ohne Fehlalarm-Hölle: Web Application Firewall und Geoblocking am LoadMaster: Schutz ohne Fehlalarm-Hölle
- Header umschreiben, Pfade umleiten: Content Rules: Header umschreiben, Pfade umleiten, Dinge verstecken
- Wer war das eigentlich? Client-IP sichtbar machen: Client-IP sichtbar machen: Transparenz, SNAT und X-Forwarded-For

Betrieb: damit der Türsteher nicht einschläft

Ein LoadMaster läuft oft jahrelang unauffällig – und genau das ist das Problem. Firmware wird nicht aktualisiert, das HA-Paar wurde nie umgeschaltet, das letzte Backup liegt auf dem Laptop eines ehemaligen Kollegen. Dann kommt der Tag, an dem eine Sicherheitslücke ein Update erzwingt, und alle hoffen, dass es gut geht.

Gut zu wissen: Die Betriebs-Checkliste in fünf Punkten

- Firmware-Kanal bewusst wählen und Updates einplanen statt aussitzen
- HA-Failover mindestens einmal im Jahr testen, nicht nur im Ernstfall
- Konfigurationsbackup automatisieren und außerhalb des LoadMasters ablegen
- Zertifikatsabläufe überwachen – auf dem LoadMaster und auf den Real Servern
- Syslog ins zentrale Monitoring, damit ein toter Real Server nicht erst dem Benutzer auffällt

Alle Themen im Überblick

Die 30 Fachartikel dieses Kompetenzbereichs sind in fünf Themenbereiche gegliedert. Du kannst vorne anfangen und dich durcharbeiten – oder direkt dort einsteigen, wo es gerade brennt.

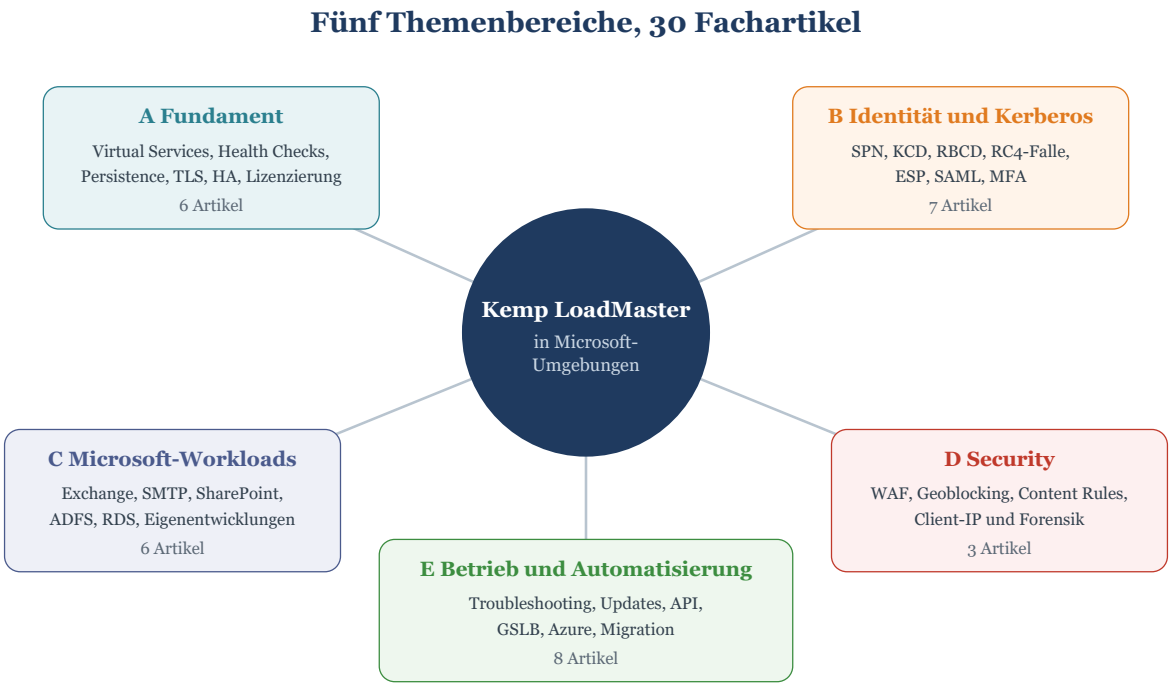


Abbildung 3: Die fünf Themenbereiche des Kemp-Kompetenzbereichs

A – Fundament

- Virtual Service, Real Server, SubVS: das Grundvokabular des LoadMasters
- Health Checks, die wirklich prüfen: warum „Port 443 offen“ nicht reicht
- Persistence und Scheduling: wer hängt an welchem Server und warum
- TLS-Offload, Re-Encryption und Zertifikate: PKI trifft LoadMaster
- HA-Paar, Failover und Konfig-Sync: zwei LoadMaster, ein Gedanke
- Editionen, Lizenzierung und Sizing: welcher LoadMaster für welchen Laden

B – Identität und Kerberos

- SPN-Probleme hinter dem Load Balancer: ein Name, mehrere Server
- Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten

- Die RC4-Falle: KCD-Keytab trifft AES-only-Domäne
- NTLM, NTLM-Proxy und der Kerberos-Fallback, den keiner bemerkt
- Edge Security Pack: Vorauthentifizierung, SSO-Domänen und der TMG-Ersatz
- SAML, OIDC und Entra ID: der LoadMaster als moderner Identitätsvermittler
- MFA vor OWA, ECP und Co.: Zwei-Faktor am LoadMaster

C – Microsoft-Workloads

- Exchange Server hinter dem LoadMaster: Templates, Namespaces, Health Checks
- SMTP über den LoadMaster: Relay, Empfangsconnectors und die echte Absender-IP
- SharePoint Server Subscription Edition hinter dem LoadMaster
- ADFS und Web Application Proxy mit dem LoadMaster: Farm, Probe, SNI
- Remote Desktop Services: RD Gateway, RD Web und Connection Broker balancieren
- IIS-Eigenentwicklungen und http.sys-Dienste veröffentlichen

D – Security

- Web Application Firewall und Geoblocking am LoadMaster: Schutz ohne Fehlalarm-Hölle
- Content Rules: Header umschreiben, Pfade umleiten, Dinge verstecken
- Client-IP sichtbar machen: Transparenz, SNAT und X-Forwarded-For

E – Betrieb und Automatisierung

- Troubleshooting am LoadMaster: Logs, L7-Debug und TCP-Dump
- Monitoring, Syslog und SNMP: den LoadMaster ins Monitoring holen
- Firmware-Updates, Backup und Notfallplan: LoadMaster-Betrieb ohne Herzrasen
- Automatisierung per REST-API und PowerShell
- Kemp 360 Central und Global Server Load Balancing für mehrere Standorte
- LoadMaster in Azure und hybriden Umgebungen
- Migration von Windows NLB, IIS ARR oder TMG-Erbe auf den LoadMaster
- Entscheidungshilfe: LoadMaster, Entra Application Proxy, Azure Application Gateway oder Reverse Proxy?

LoadMaster oder etwas anderes?

Nicht jede Umgebung braucht einen LoadMaster, und nicht jede Umgebung, die einen hat, braucht ihn noch. Wer nur eine einzelne Webanwendung mit Entra ID veröffentlichen will, ist mit dem Entra Application Proxy oft schneller am Ziel. Wer dagegen Exchange mit SMTP, mehrere On-Premises-Dienste und Kerberos-Delegation unter einen Hut bringen muss, kommt an einem richtigen Application Delivery Controller kaum vorbei.

Anforderung	LoadMaster	Entra Application Proxy	Azure Application Gateway
On-Premises-Webdienste veröffentlichen	ja	ja	eingeschränkt, über Netzanbindung
Layer-4-Protokolle wie SMTP	ja	nein	nein
Kerberos-Delegation zum Server	ja (KCD)	ja (KCD)	nein
Lastverteilung im eigenen Rechenzentrum	ja	nein	nein
Betrieb einer eigenen Appliance	ja, inklusive Updates	nein, Connector genügt	nein, Azure-Dienst

Die ausführliche Abwägung mit allen Kriterien findest du in Entscheidungshilfe: LoadMaster, Entra Application Proxy, Azure Application Gateway oder Reverse Proxy?. Und wenn du von Windows NLB, IIS ARR oder einem TMG-Erbe kommst: Migration von Windows NLB, IIS ARR oder TMG-Erbe auf den LoadMaster.

Beratung und Schulung

Manchmal reicht ein Artikel nicht, weil das Problem nicht im Artikel steht, sondern in deiner Umgebung. Dann schauen wir gemeinsam drauf: Konfiguration prüfen, Kerberos-Strecke aufbauen, Exchange sauber veröffentlichen oder eine Migration von Altlasten planen. Alles dazu auf der Beratungsseite zum Kemp LoadMaster.

Wenn dein Team den LoadMaster selbst sicher beherrschen soll, gibt es die eintägige Kemp-LoadMaster-Schulung für Microsoft-Administratoren – online, praxisnah und mit Übungen an echten Szenarien.

Häufige Fragen zum Kemp LoadMaster

Brauche ich für Exchange überhaupt noch einen Load Balancer?

Sobald du mehr als einen Exchange-Server hast und Ausfälle nicht per Hand umschalten willst: ja. Exchange selbst bringt keine Lastverteilung für Clientverbindungen mit. Seit Exchange 2013 ist die Aufgabe des Load Balancers aber deutlich einfacher geworden, weil keine Sitzungsbindung mehr nötig ist.

Layer 4 oder Layer 7 – was ist besser?

Layer 4 ist einfacher und schneller, sieht aber nicht in den Verkehr hinein. Layer 7 terminiert TLS und kann dadurch protokollspezifisch prüfen, Header umschreiben und vorauthentifizieren. Für Exchange und SharePoint ist Layer 7 meist die bessere Wahl, für SMTP oft Layer 4.

Was ist das Edge Security Pack und muss ich es extra kaufen?

ESP bündelt Reverse-Proxy-, Authentifizierungs- und SSO-Funktionen des LoadMasters. Laut Hersteller ist es in allen LoadMaster-Modellen enthalten. Welche Funktionen deine Edition im Detail bietet, prüfst du am besten in der aktuellen Progress-Übersicht.

Warum funktioniert Kerberos hinter dem LoadMaster nicht?

In neun von zehn Fällen liegt es am SPN: Der Client fragt nach einem Ticket für den VIP-Namen, und dieser SPN fehlt, ist doppelt vergeben oder hängt am falschen Konto. Der zehnte Fall ist meist die RC4/AES-Frage bei KCD.

Kann der LoadMaster den Web Application Proxy für ADFS ersetzen?

Technisch kann er ADFS veröffentlichen und vorauthentifizieren. Ob das ein vollwertiger Ersatz ist, hängt von deinen Anforderungen an Extranet Lockout, Gerätebindung und Support ab. Die Abwägung steht in ADFS und Web Application Proxy mit dem LoadMaster: Farm, Probe, SNI.

Wie bekomme ich die echte Client-IP in meine IIS-Logs?

Entweder über den Transparenz-Modus, der Routing-Anforderungen mit sich bringt, oder über den Header X-Forwarded-For, den du im IIS-Logging als zusätzliches Feld aufnimmst. Details in Client-IP sichtbar machen: Transparenz, SNAT und X-Forwarded-For.

Reicht die kostenlose Edition des LoadMasters?

Für Labor, Tests und kleine Umgebungen oft ja. Für produktive Umgebungen mit Hochverfügbarkeit, Support-Anspruch und vollem Funktionsumfang solltest du die Grenzen der freien Edition genau prüfen. Mehr in Editionen, Lizenzierung und Sizing: welcher LoadMaster für welchen Laden.

Wie aktualisiere ich ein HA-Paar ohne Ausfall?

Erst den Standby-Knoten aktualisieren, dann bewusst umschalten, dann den zweiten Knoten. Vorher Backup, Release Notes lesen und ein Wartungsfenster einplanen. Die Schritt-für-Schritt-Anleitung steht in Firmware-Updates, Backup und Notfallplan: LoadMaster-Betrieb ohne Herzrasen.

Wie geht es weiter?

WISSEN

Einstieg

Fang mit dem Grundvokabular an – oder spring direkt zum Kerberos-Kapitel.

Virtual Service, Real Server, SubVS

BERATUNG

Hilfe holen

Wenn es brennt oder du eine zweite Meinung zu deiner Konfiguration willst.

Zur Kemp-Beratung

SCHULUNG

Team fit machen

Ein Tag, vier Blöcke, viele Übungen – speziell für Microsoft-Admins.

Zur Kemp-Schulung