SharePoint Server Subscription Edition hinter dem LoadMaster



WISSEN

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

› **Kemp LoadMaster**

BERATUNG

SharePoint-Farm hinter dem LoadMaster neu aufbauen, Kerberos geradeziehen oder die Suche wieder zum Laufen bringen? Wir schauen gemeinsam drauf.

› **Beratung zum Kemp LoadMaster**

SCHULUNG

Virtual Services, Health Checks und Persistenz für Microsoft-Workloads im Labor durchspielen, bevor es die Produktion tut.

› **Kemp-LoadMaster-Schulung**

SharePoint hinter einem Load Balancer hat einen Ruf, den es eigentlich nicht verdient. Im Vergleich zu Exchange ist SharePoint Server Subscription Edition geradezu pflegeleicht: ein paar Front-End-Server, ein HTTPS-Name, fertig. Und trotzdem landen SharePoint-Farmen verlässlich auf dem Tisch, wenn es um Load-Balancer-Probleme geht. Nicht, weil der LoadMaster etwas falsch macht, sondern weil SharePoint eine sehr feste Meinung darüber hat, wie es heißt, wer es aufruft und wie man sich bei ihm anmeldet. Der Load Balancer steht genau zwischen diesen drei Meinungen und bekommt dafür die Schuld.

Die Klassiker kennst du vielleicht: Links, die plötzlich auf http zeigen. Kerberos, das auf einem Server funktioniert und auf dem anderen nicht. Ein Health Check, der jeden Server für tot erklärt, weil SharePoint höflich mit 401 antwortet. Und die Suche, die seit dem Umbau nur noch Anmeldeseiten indexiert. Das ist ungefähr so, als würdest du eine Bibliothek katalogisieren und am Ende vierzigtausend Karteikarten mit der Aufschrift „Bitte klingeln“ haben.

Dieser Beitrag gehört zur Serie rund um den Kemp LoadMaster und schließt die Lücke zwischen dem Deployment Guide von Progress Kemp und den SharePoint-Seiten auf Microsoft Learn. Es geht um alternative Zugriffszuordnungen und Host-Header-Websitesammlungen, um Kerberos mit gemeinsamem Dienstkonto, um Health Checks, die mit Anmeldung umgehen können, um die ewige Frage nach der Persistenz, um Office Online Server als eigenen Virtual Service und um den Distributed Cache, der von alledem herrlich unbeeindruckt bleibt. Wer tiefer in SharePoint selbst einsteigen will, findet die Grundlagen auf der Themenseite SharePoint.

FAKTEN · Das Wichtigste in sechs Sätzen

SharePoint SE braucht für die Anmeldung keine Sitzungsaffinität, weil Anmeldetoken im Distributed Cache liegen und damit auf jedem Front-End gültig sind.

Office Online Server dagegen will Client-Affinität; er gehört in einen eigenen Virtual Service mit eigenem Namen, eigenem Zertifikat und Persistenz.

Wer TLS am LoadMaster beendet, muss SharePoint das per alternativer Zugriffszuordnung oder, bei Host-Header-Websitesammlungen, per Header Front-End-Https: On mitteilen; Microsoft unterstützt das, empfiehlt aber Re-Encryption.

Kerberos klappt hinter dem LoadMaster gut, weil alle Server einer Web-App denselben Anwendungspool-Account nutzen; der SPN gehört genau an dieses Konto.

Ein Health Check ohne Anmeldung bekommt von SharePoint 401 oder eine Umleitung zur Anmeldung; wie du das wertest, entscheidet über die Aussagekraft.

Office Online Server erreicht am 31. Dezember 2026 sein Supportende, also in wenigen Wochen. Plane den Virtual Service mit diesem Datum im Kopf.

Namen, Zonen und Schemata: AAM und Host-Header-Websitesammlungen

SharePoint baut jeden Link, den es ausliefert, selbst zusammen. Dafür muss es wissen, unter welcher Adresse der Browser es gerade erreicht hat. Bei einem direkten Zugriff ist das trivial. Hinter einem LoadMaster mit TLS-Offload aber kommt beim Server eine Anfrage an http://sharepoint.contoso.de an, obwohl der Benutzer https://sharepoint.contoso.de getippt hat. Wenn SharePoint davon nichts weiß, liefert es Links mit http aus. Der Browser folgt, der LoadMaster leitet um, Formulare verlieren ihre Daten und Office-Clients bekommen Gemischtinhalt-Warnungen in einem Tonfall, den man sonst nur von Steuerbescheiden kennt.

Pfadbasierte Web-Apps: alternative Zugriffszuordnungen

Bei klassischen, pfadbasierten Web-Apps regeln alternative Zugriffszuordnungen, kurz AAM, das Problem. Jede Web-App hat bis zu fünf Zonen: Default, Intranet, Internet, Custom und Extranet. Jede Zone hat eine öffentliche URL, also die Adresse, die SharePoint in Links schreibt, und beliebig viele interne URLs, also Adressen, unter denen Anfragen ankommen dürfen. Bei TLS-Offload trägst du als öffentliche URL https://sharepoint.contoso.de ein und ergänzt eine interne URL http://sharepoint.contoso.de in derselben Zone. Kommt die Anfrage per http vom LoadMaster, ordnet SharePoint sie der Zone zu und schreibt trotzdem https in die Links. Die IIS-Bindung auf Port 80 muss dazu natürlich existieren.

Mit Re-Encryption entfällt dieser Trick: Der LoadMaster spricht https mit den Servern, interne und öffentliche URL sind identisch, und SharePoint merkt vom Load Balancer gar nichts. Genau deshalb ist das der Weg, den du für eine neue Farm wählen solltest. Für SharePoint SE kommt hinzu, dass die Edition TLS 1.3 und SNI-basierte IIS-Bindungen unterstützt. Wenn du Bindungen mit SNI anlegst, muss der LoadMaster beim Re-Encrypt den richtigen Servernamen mitschicken, sonst bekommt er ein Zertifikat, das nicht passt, oder gar keins. Prüfe das im Testaufbau, bevor du es in der Produktion herausfindest.

Host-Header-Websitesammlungen: keine AAM, dafür ein Header

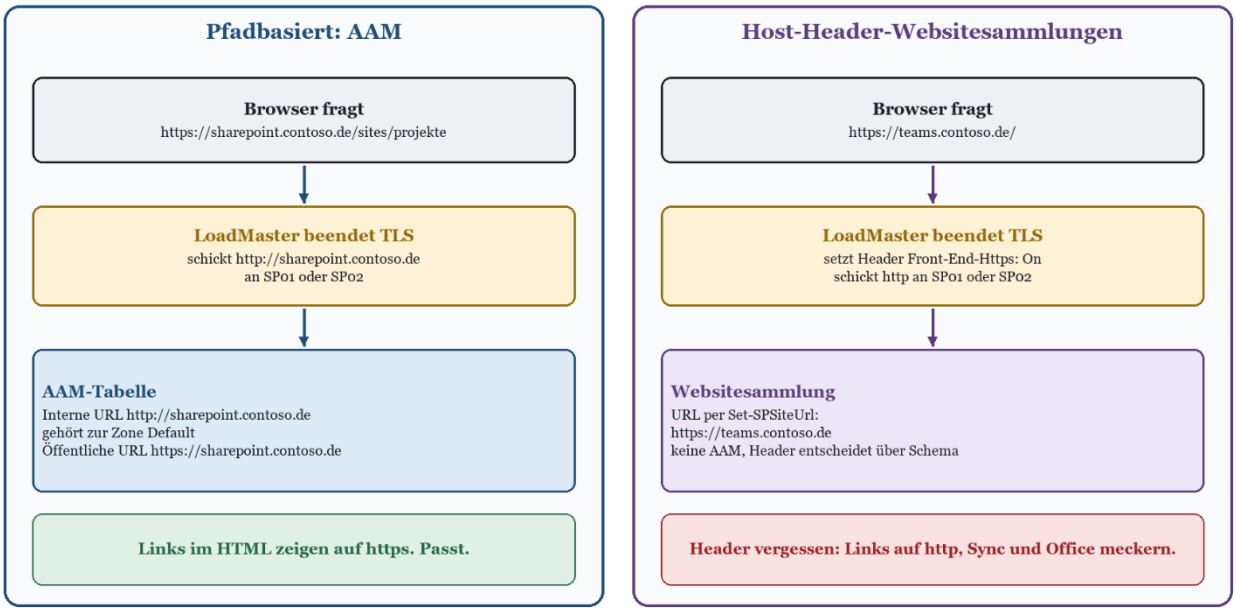
Microsoft empfiehlt seit Jahren Host-Header-Websitesammlungen, also viele Websitesammlungen mit eigenen Hostnamen in einer einzigen Web-App. Das spart Anwendungspools, Arbeitsspeicher und Nerven. Der Haken: Für diese Sammlungen gelten keine AAM. Ihre URLs setzt du per Set-SPSiteUrl, auf Wunsch auch je Zone. Und woher weiß SharePoint dann, dass vor dem LoadMaster

eigentlich https war? Microsoft beantwortet das in der Dokumentation zur Architektur von Host-Header-Websitesammlungen eindeutig: Das TLS-beendende Gerät muss den Header Front-End-Https: On in jede Anfrage einfügen. SharePoint baut dann Links mit https. Gleich danach steht der Satz, den man gern überliest: TLS-Terminierung außerhalb des Servers ist unterstützt, aber nicht empfohlen, weil der Verkehr zwischen Proxy und Webserver unverschlüsselt läuft.

Am LoadMaster setzt du diesen Header mit einer Content Rule, die beim Weiterleiten an den Real Server einen Header ergänzt. Wie das im Detail geht und wie du prüfst, ob die Regel greift, steht im Beitrag Content Rules: Header umschreiben, Pfade umleiten, Dinge verstecken.

Woher SharePoint weiß, wie es heißt

Pfadbasierte Web-App mit AAM gegen Host-Header-Websitesammlungen, beide hinter TLS-Offload



Skizze: Prinzip; mit Re-Encryption entfällt das Umschreiben des Schemas

Aspekt	Pfadbasiert mit AAM	Host-Header-Websitesammlungen
Namen je Web-App	einer je Zone	beliebig viele
URL-Verwaltung	Zentraladministration, AAM-Tabelle	Set-SPSiteUrl in PowerShell
TLS-Offload	interne http-URL zur https-Zone	Header Front-End-Https: On
Re-Encryption	nichts weiter zu tun	nichts weiter zu tun
Zertifikat am VS	Name der Web-App	Platzhalter oder SAN mit allen Namen
SPN für Kerberos	einer je Name	einer je Hostname
Typischer Fehler	öffentliche URL mit http	Header fehlt, Links auf http

WARNUNG · Default-Zone ist nicht verhandelbar

Die Zone Default ist für SharePoint mehr als ein Name. Benachrichtigungen, E-Mail-Links, Workflows und vor allem die Suche richten sich nach ihr. Die Default-Zone muss Windows-Authentifizierung anbieten, sonst kann der Crawler nicht crawlen. Wer die Default-Zone für die Internetveröffentlichung mit Vorauthentifizierung am LoadMaster umbaut, legt damit die Grundlage für das Praxisbeispiel weiter unten. Lege für externe Zugriffe lieber eine zusätzliche Zone an.

Kerberos mit gemeinsamem Dienstkonto: der freundlichste Fall

Kerberos hinter einem Load Balancer ist ein Dauerbrenner, weil der Client ein Ticket für den Namen des VIP anfordert und dieses Ticket dann auf irgendeinem Server landet, der es entschlüsseln können muss. Bei SharePoint ist das ausnahmsweise gut gelöst: Eine Web-App läuft auf allen Servern der Farm im selben Anwendungspool mit demselben Domänenkonto. SharePoint sorgt selbst dafür, dass das so bleibt. Außerdem schaltet SharePoint die Kernelmodus-Authentifizierung im IIS ab, sodass das Ticket mit dem Schlüssel des Anwendungspool-Kontos entschlüsselt wird und nicht mit dem des Computerkontos.

Daraus folgt eine einzige Regel: Der SPN HTTP/sharepoint.contoso.de gehört an das Anwendungspool-Konto, zum Beispiel svc-sp-content, und an kein anderes Konto im ganzen Wald. Bei Host-Header-Websitesammlungen kommt für jeden Hostnamen ein eigener SPN an dasselbe Konto. Das Grundprinzip und die typischen Fehlerbilder, wenn ein Name auf mehrere Server zeigt, erklärt der Beitrag SPN-Probleme hinter dem Load Balancer: ein Name, mehrere Server. Die Kerberos-Seite der Medaille mit Tickets, Verschlüsselungstypen und Delegierung findest du auf der Themenseite Microsoft Kerberos.

Wo es trotzdem knallt

- **Doppelte SPNs.** Irgendwer hat HTTP/sharepoint.contoso.de vor Jahren an das Computerkonto des ersten Servers gehängt. Der KDC findet zwei Konten und liefert gar kein Ticket. setspn -X findet so etwas in Sekunden.
- **CNAME statt A-Eintrag.** Manche Clients bauen den SPN aus dem kanonischen Namen. Zeigt sharepoint.contoso.de per CNAME auf lb-vip01.contoso.local, fragt der Client unter Umständen nach dem falschen SPN. Ein A-Eintrag für den VIP-Namen erspart dir das.
- **Unterschiedliche Konten je Web-App mit gleichem Namen.** Zwei Web-Apps, ein Hostname, verschiedene Ports oder Pfade: Kerberos kennt nur einen SPN je Name. Das geht nicht gut.
- **Leise Rückfälle auf NTLM.** Funktioniert Kerberos nicht, fällt Windows still auf NTLM zurück, und alles scheint zu laufen. Bis die erste Delegierung an SQL Reporting Services oder einen Webservice im Backend fehlschlägt.

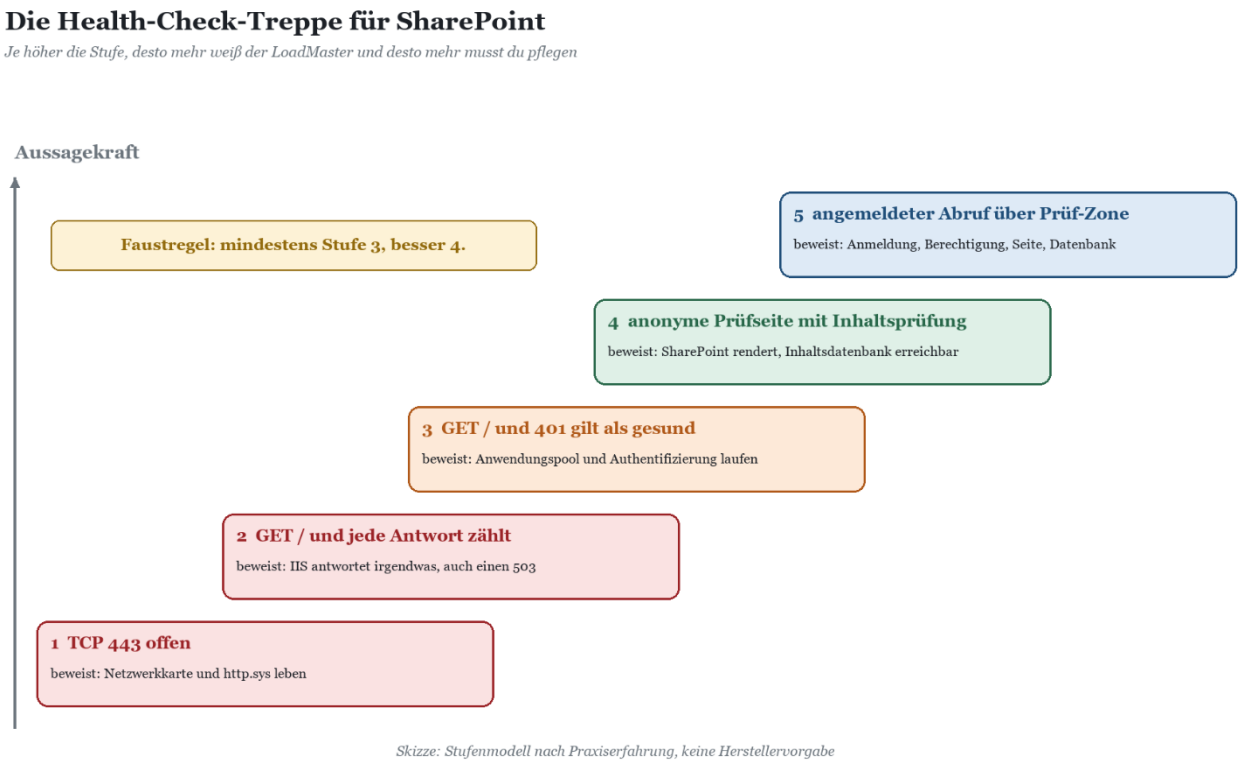
Zum letzten Punkt lohnt der Blick in den Beitrag NTLM, NTLM-Proxy und der Kerberos-Fallback, den keiner bemerkt. NTLM ist verbindungsorientiert: Die Anmeldung gilt für genau eine TCP-Verbindung. Ein Layer-7-Load-Balancer, der Verbindungen verschiedener Clients zum Server bündelt, zerlegt das. Der LoadMaster hält Client- und Serververbindung standardmäßig eins zu eins zusammen; wenn du mit Optionen zur Verbindungsoptimierung experimentierst, teste NTLM-Clients danach ausdrücklich.

> **TIPP · Kerberos prüfen, bevor die Benutzer es tun**
>
> Melde dich an einem Client an, öffne die Seite über den VIP und sieh mit klist nach, ob ein Ticket für HTTP/sharepoint.contoso.de existiert. Dann zwingst du den LoadMaster per Real-Server-Deaktivierung auf den jeweils anderen Server und wiederholst den Test. Kerberos, das nur auf einem Server funktioniert, ist fast immer ein SPN- oder Kontoproblem, nie ein Problem des Load Balancers.

Health Checks und Persistenz: was der LoadMaster wissen muss

SharePoint ist bei anonymen Anfragen konsequent. Eine Web-App mit Windows-Authentifizierung antwortet auf GET / mit 401 und dem Hinweis, wie man sich anmeldet. Eine Web-App mit mehreren Anmeldeanbietern oder SAML schickt eine Umleitung zur Anmeldeseite. Ein Health Check, der stur auf 200 wartet, erklärt damit jeden Server für tot, und der Virtual Service ist leer. Die übliche Reaktion im Betrieb ist, den Check auf „TCP-Port offen“ zurückzudrehen, und dann ist

man wieder bei einem Load Balancer, der einen abgestürzten Anwendungspool fröhlich mit Benutzern füttert, weil http.sys ja noch auf Port 443 lauscht. Warum das grundsätzlich nicht reicht, steht im Beitrag Health Checks, die wirklich prüfen: warum „Port 443 offen“ nicht reicht.



Skizze: Stufenmodell nach Praxiserfahrung, keine Herstellervorgabe

Health Checks mit Anmeldung

Einen Kerberos- oder NTLM-Handshake kann der Health Check des LoadMasters nicht führen. Er kann aber eine URL abrufen, eigene Header mitschicken und die Antwort auf Statuscode und Inhalt prüfen. Daraus ergeben sich drei brauchbare Varianten. Die erste: Du wertest die 401 als Lebenszeichen, sofern deine Firmware erlaubt, abweichende Statuscodes als gültig zu definieren. Das beweist, dass Anwendungspool und Authentifizierung antworten, aber nicht, dass die Inhaltsdatenbank erreichbar ist. Die zweite: eine anonyme Prüfseite, etwa eine kleine Websitesammlung mit anonymem Lesezugriff in einer eigenen Zone, deren Seite einen festen Text enthält, auf den der Check prüft. Die dritte: eine interne Prüf-Zone mit Standardauthentifizierung und einem Monitoring-Konto, das nur auf diese eine Websitesammlung lesen darf; der LoadMaster schickt dann einen Authorization-Header mit.

Variante	Was sie beweist	Aufwand	Haken
TCP 443	Port offen	keiner	erkennt keinen toten Anwendungspool
GET / mit 401 als gültig	IIS, Pool, Authentifizierung	gering	Datenbankausfall bleibt unbemerkt
Anonyme Prüfseite mit Textprüfung	Rendering und Inhaltsdatenbank	mittel	anonymer Zugriff muss bewusst und eng begrenzt sein
Prüf-Zone mit Standardauthentifizierung	Anmeldung, Berechtigung, Datenbank	höher	Kennwort steht in der LoadMaster-Konfiguration

WARNUNG · Prüf-Konten sind Konten

Ein Monitoring-Konto mit Standardauthentifizierung liegt im Klartext-Base64 in der Konfiguration

jedes Health Checks und in jedem Backup des LoadMasters. Gib ihm keine Rechte außer Lesen auf der Prüf-Websitesammlung, verbiete die interaktive Anmeldung, nimm es aus privilegierten Gruppen heraus und lass die Prüf-Zone ausschließlich über das interne Netz erreichbar sein. Wer stattdessen das Farmkonto einträgt, hat eine sehr kurze Geschichte für das nächste Audit.

Persistenz: ja, nein oder lieber nicht

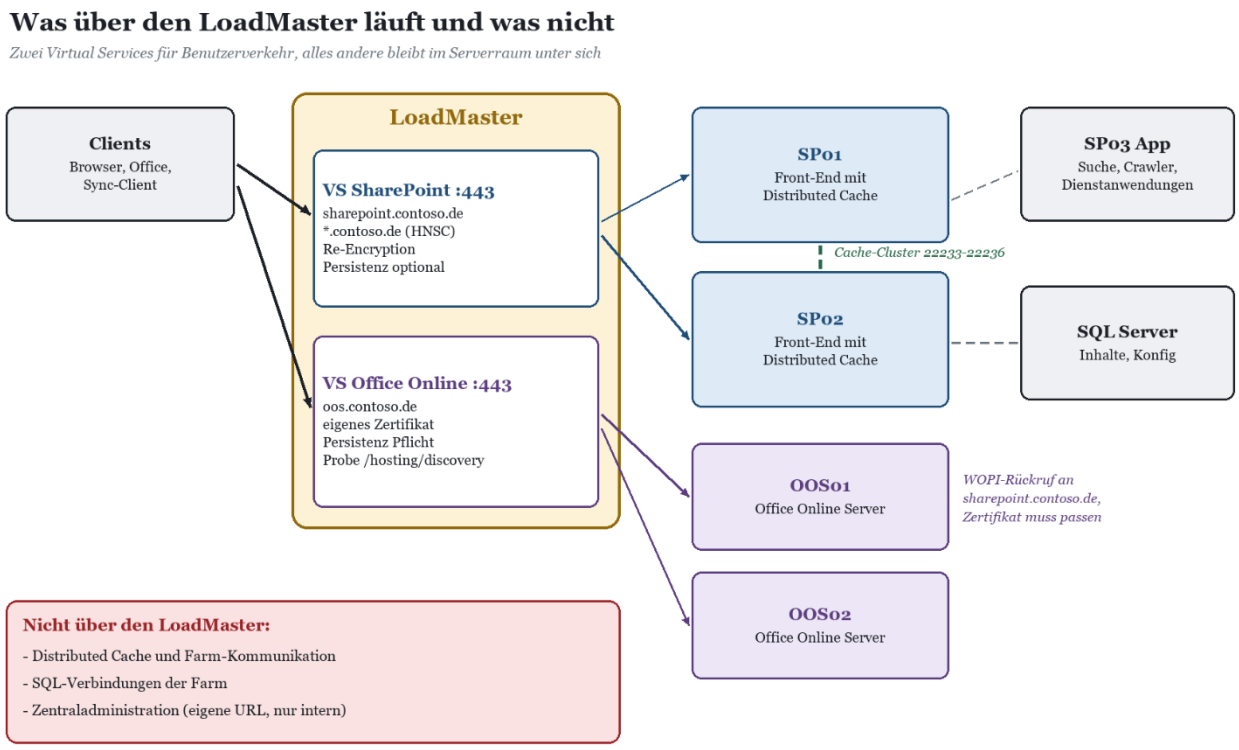
Seit SharePoint 2013 liegen die Anmeldetoken, die FedAuth-Cookies und der Login-Token-Cache im Distributed Cache. Ein Benutzer, der sich an SP01 angemeldet hat, ist damit auch an SP02 angemeldet. Microsoft hat damit die Pflicht zur Sitzungsaffinität für SharePoint selbst abgeschafft. In der Praxis gibt es trotzdem Gründe, sie einzuschalten: ältere Lösungen von Drittanbietern mit Sitzungszustand im Arbeitsspeicher, Upload-Szenarien über langsame Leitungen und Farmen, deren Distributed Cache nicht so stabil ist, wie er sein sollte. Persistenz kaschiert dann Probleme, statt sie zu lösen, aber manchmal ist Kaschieren genau das, was am Freitagnachmittag gebraucht wird.

Szenario	Empfehlung	Begründung
Reine SharePoint-SE-Farm, Windows-Anmeldung	keine Persistenz	Token im Distributed Cache
SAML über ADFS oder Entra ID	keine Persistenz, optional Cookie	FedAuth gilt farmweit, Cookie glättet Neuanmeldungen
Drittanbieter mit Sitzungszustand	Cookie-Persistenz	Hersteller fragen, nicht raten
Viele Clients hinter einer NAT-Adresse	keine Persistenz auf Quell-IP	sonst landet die ganze Zentrale auf einem Server
Crawler über den VIP	gar nicht erst über den VIP	siehe Praxisbeispiel
Office Online Server	Persistenz erforderlich	Microsoft verlangt Client-Affinität

Welche Persistenzmodi der LoadMaster kennt und warum Quell-IP-Persistenz hinter Proxys und NAT eine schlechte Idee ist, steht ausführlich im Beitrag Persistence und Scheduling: wer hängt an welchem Server und warum.

Distributed Cache: unbeeindruckt und bitte auch unberührt

Der Distributed Cache läuft zwischen den Farmservern auf eigenen Ports, standardmäßig 22233 bis 22236, und hat mit dem LoadMaster schlicht nichts zu tun. Er braucht keinen VIP, keinen Health Check und keine Persistenz. In SharePoint SE bringt SharePoint den Cache-Dienst selbst mit, statt auf ein separat installiertes AppFabric zu setzen. Der LoadMaster beeinflusst ihn trotzdem indirekt: Wer ohne Persistenz arbeitet, verlässt sich darauf, dass der Cache gesund ist. Ein Cache-Host, der beim Patchen unsauber aus dem Cluster genommen wurde, äußert sich dann als „Benutzer müssen sich ständig neu anmelden“, und der erste Verdacht fällt wie immer auf den Load Balancer.



Skizze: vereinfachte Farm, Namen fiktiv; gestrichelt = Verkehr ohne LoadMaster

WICHTIG · Server in Wartung schicken

Bevor du einen SharePoint-Server patchst, nimm ihn am LoadMaster aus dem Virtual Service, warte, bis die Verbindungen ausgelaufen sind, und fahre erst dann den Distributed Cache auf diesem Host geordnet herunter. Die Reihenfolge rückwärts ist die Version mit Anrufen aus der Fachabteilung.

Office Online Server als eigener Virtual Service

Office Online Server, kurz OOS, rendert und bearbeitet Word-, Excel- und PowerPoint-Dateien im Browser. SharePoint spricht mit ihm über WOPI: Der Browser lädt die Bearbeitungsoberfläche von oos.contoso.de, der OOS-Server holt sich die Datei per Rückruf von sharepoint.contoso.de. Daraus folgen zwei Dinge. Erstens braucht OOS einen eigenen Namen und damit einen eigenen Virtual Service. Zweitens muss jeder OOS-Server den SharePoint-Namen auflösen und erreichen können, und zwar über einen Weg, auf dem das Zertifikat passt.

Microsoft beschreibt in der Planung für Office Online Server, was der Load Balancer können sollte: Layer-7-Routing, Client- oder Front-End-Affinität und TLS-Offload. Die Affinität ist kein Luxus, denn Bearbeitungssitzungen und vor allem Excel-Arbeitsmappen leben im Speicher des OOS-Servers, der sie geöffnet hat. Ohne Persistenz springt der Browser zwischen Servern hin und her, und die Sitzung zerfällt. Zwischen den OOS-Servern läuft außerdem Port 809 für die farminterne Kommunikation, der nicht über den LoadMaster geht, aber in der Firewall offen sein muss.

Einstellung	VS SharePoint	VS Office Online Server
Name	sharepoint.contoso.de, ggf. weitere	oos.contoso.de
Persistenz	nicht erforderlich	erforderlich, Cookie oder Quell-IP
Health Check	Prüfseite oder 401 als gültig	/hosting/discovery liefert XML
TLS	Re-Encryption empfohlen	Offload möglich, dann OOS-Farm

		entsprechend einrichten
Zugriff von außen	eigene Zone, ggf. Vorauthentifizierung	nur mit SharePoint zusammen
Supportende	Modern Lifecycle, solange aktuell	31. Dezember 2026

WICHTIG · Supportende Office Online Server

Microsoft hat im Oktober 2025 angekündigt, dass Office Online Server am 31. Dezember 2026 ohne erweiterte Supportphase ausläuft. SharePoint SE selbst bleibt unterstützt, die Browserbearbeitung von Office-Dateien entfällt dann ohne Ersatz im lokalen Rechenzentrum. Baue den OOS-Virtual-Service heute so, dass du ihn Anfang 2027 mit einem Klick deaktivieren kannst, und kläre vorher, was die Benutzer statt der Vorschau sehen sollen.

TIPP · Der Discovery-Endpunkt ist dein Health Check

Office Online Server liefert unter /hosting/discovery ein XML-Dokument mit seinen Fähigkeiten aus, anonym und schnell. Prüfe am LoadMaster auf Status 200 und auf einen festen Textbestandteil wie wopi-discovery. Das ist einer der seltenen Fälle, in denen ein Microsoft-Produkt dir den perfekten Health Check schenkt.

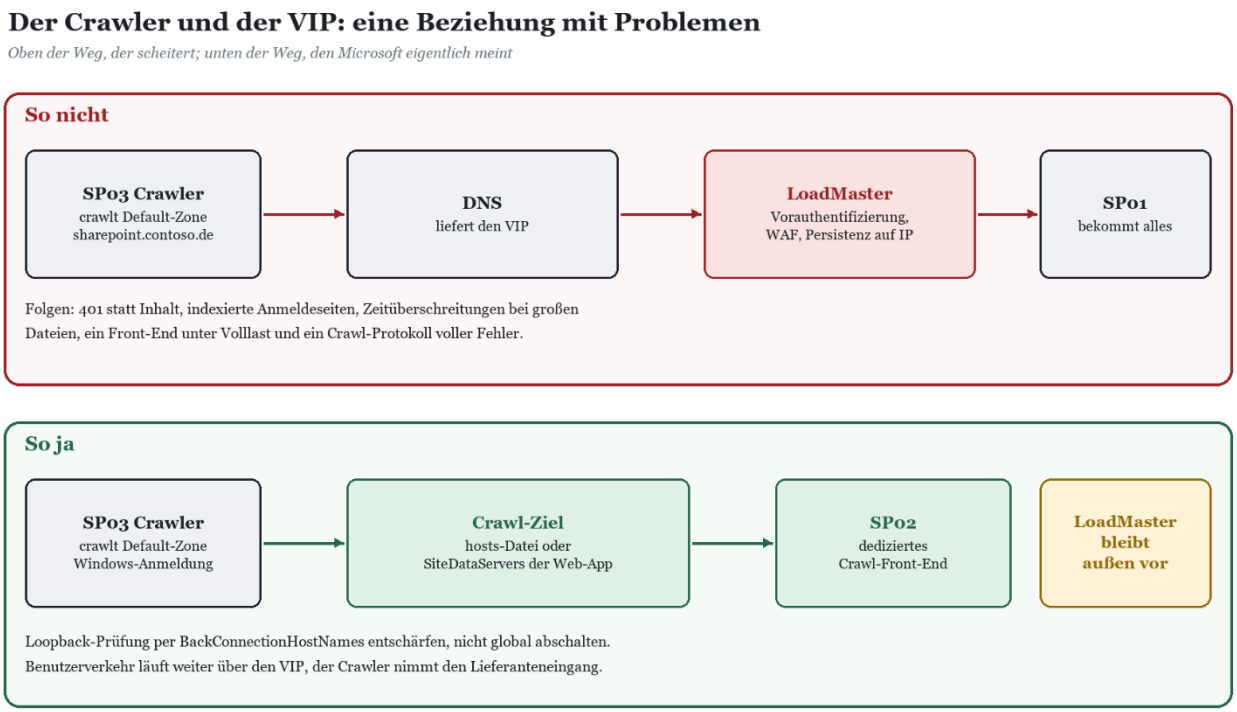
Praxisfall: Die Suche crawlt über den VIP und scheitert

AUS DER PRAXIS · Nach dem Umbau findet die Suche nur noch Anmeldeseiten

Eine Verwaltung mit rund 900 Benutzerinnen und Benutzern zieht ihre SharePoint-SE-Farm hinter einen neuen LoadMaster. Der Virtual Service bekommt Vorauthentifizierung für den Zugriff von außen, eine Web Application Firewall und Quell-IP-Persistenz, weil das im alten Load Balancer auch so war. Am Montag sind die Suchergebnisse merkwürdig. Am Dienstag liefert die Suche nach „Haushalt“ zweihundert Treffer, alle mit dem Titel der Anmeldeseite. Am Mittwoch ist das Crawl-Protokoll rot.

Die Ursache ist eine Kette, die man in vielen Farmen findet. Der Crawler auf dem Anwendungsserver crawlt die Default-Zone unter sharepoint.contoso.de. DNS liefert den VIP. Der Crawler landet damit am LoadMaster, genau wie ein Benutzer. Ab hier geht in dieser Farm alles schief, was schiefgehen kann:

- **Vorauthentifizierung.** Der Crawler kann keine Formularanmeldung. Er bekommt das HTML der Anmeldeseite mit Status 200 und indexiert es pflichtbewusst. Zweihundertmal.
- **Web Application Firewall.** Der Crawler stellt Tausende Anfragen pro Minute, ruft Listenansichten mit langen Abfragezeichenfolgen ab und lädt Office-Dateien herunter. Für eine WAF sieht das aus wie ein Angriff, und sie handelt entsprechend.
- **Quell-IP-Persistenz.** Alle Crawl-Anfragen kommen von einer Adresse und landen damit auf demselben Front-End. SP01 läuft unter Volllast, SP02 langweilt sich, die Benutzer auf SP01 leiden mit.
- **Zeitüberschreitungen.** Große Dateien brauchen länger als das Idle-Timeout des Virtual Service. Der Crawler meldet Fehler, die niemand mit dem LoadMaster verbindet.



Skizze: Prinzip, Namen fiktiv

Die Lösung: Crawler am LoadMaster vorbeischicken

Microsoft ist bei diesem Thema eindeutig: Der Crawler soll nicht durch den Load Balancer, sondern direkt auf ein oder mehrere Front-Ends. Dafür gibt es zwei Wege. Der klassische ist ein Eintrag in der hosts-Datei des Crawl-Servers, der sharepoint.contoso.de auf die IP-Adresse eines bestimmten Front-Ends zeigt, oder auf den Crawl-Server selbst, wenn dort die Web-App läuft. Der elegantere ist die Eigenschaft SiteDataServers der Web-App, mit der du per PowerShell festlegst, welche Server der Crawler für eine Web-App verwendet. In beiden Fällen gilt: Das Zertifikat auf dem Ziel-Server muss zum Namen passen, und die Default-Zone muss Windows-Authentifizierung anbieten.

Zeigt der Name auf den Server selbst, schlägt die Loopback-Prüfung von Windows zu: NTLM-Anmeldungen an einen lokalen Dienst unter einem fremden Namen werden abgewiesen. Statt die Prüfung global per DisableLoopbackCheck abzuschalten, trägst du die betroffenen Namen in BackConnectionHostNames ein. Das ist der Unterschied zwischen einer Tür, die du für einen Gast öffnest, und einer Tür, die du aushängst.

Symptom im Crawl-Protokoll	Wahrscheinliche Ursache	Abhilfe
Zugriff verweigert, 401	Crawler landet an Vorauthentifizierung oder Kerberos-SPN fehlt	Crawl-Ziel direkt, SPN prüfen
Treffer zeigen nur Anmeldeseite	Formularanmeldung am VIP liefert 200 mit Login-HTML	Crawler am VIP vorbei, Default-Zone ohne Vorauthentifizierung
Zeitüberschreitung bei großen Dateien	Idle-Timeout am Virtual Service	Crawl-Ziel direkt
Viele 403 oder Verbindungsabbrüche	WAF-Regeln oder Ratenbegrenzung	Crawler nicht über WAF führen
Ein Front-End unter Volllast beim Crawl	Quell-IP-Persistenz	dediziertes Crawl-Ziel
401 nur bei Ziel = eigener	Loopback-Prüfung	BackConnectionHostNames

Server		

TIPP · Vorauthentifizierung gehört in eine eigene Zone

Wenn du SharePoint mit Vorauthentifizierung am LoadMaster ins Internet bringst, erweitere die Web-App um eine Zone Internet mit eigenem Namen, etwa extranet.contoso.de, und lege die Vorauthentifizierung nur auf deren Virtual Service. Die Default-Zone bleibt intern, mit Windows-Anmeldung, für Benutzer im Netz und den Crawler. Wie Vorauthentifizierung und SSO-Domänen am LoadMaster funktionieren, erklärt der Beitrag Edge Security Pack: Vorauthentifizierung, SSO-Domänen und der TMG-Ersatz.

TLS: Offload, Bridging oder durchreichen

Für SharePoint SE sind alle drei Varianten technisch möglich. Reines Durchreichen auf Layer 4 ist am einfachsten, verschenkt aber Content Rules, Header und eine vernünftige Prüfung. Offload mit http zum Server funktioniert mit AAM und dem Header Front-End-Https: On, ist laut Microsoft aber nicht empfohlen. Re-Encryption kombiniert Sichtbarkeit am LoadMaster mit verschlüsselter Strecke bis zum Server und ist deshalb der Standard, den du für neue Farmen wählen solltest. Zertifikatsketten, Re-Encryption und die PKI-Seite des Themas behandelt der Beitrag TLS-Offload, Re-Encryption und Zertifikate: PKI trifft LoadMaster.

FAQ: Häufige Fragen zu Kemp und SharePoint

Gibt es ein Kemp-Template für SharePoint SE?

Progress Kemp bietet Templates und einen Deployment Guide für SharePoint 2019 mit Varianten für HTTP, HTTPS, Offload und Re-Encryption, getrennt für Benutzerportal und Zentraladministration. Für SharePoint SE passen sie als Ausgangspunkt, weil sich am HTTP-Verhalten nichts Grundlegendes geändert hat. Health Check und Persistenz solltest du trotzdem bewusst nachschärfen.

Muss ich für SharePoint SE Persistenz einschalten?

Nein. Anmeldetoken liegen im Distributed Cache und gelten auf jedem Front-End. Persistenz brauchst du nur für Lösungen von Drittanbietern mit Sitzungszustand und für Office Online Server.

Gehört die Zentraladministration hinter den LoadMaster?

In der Regel nicht. Sie läuft auf einem oder zwei Servern, wird nur von Administratorinnen und Administratoren genutzt und sollte ohnehin nicht aus dem Benutzernetz erreichbar sein. Wenn du sie trotzdem balancierst, dann in einem eigenen Virtual Service mit eigenem Namen und Zugriffsbeschränkung.

Warum zeigt SharePoint hinter dem LoadMaster Links mit http an?

Weil TLS am LoadMaster endet und SharePoint davon nichts weiß. Bei pfadbasierten Web-Apps fehlt die interne http-URL in der https-Zone der AAM, bei Host-Header-Websitesammlungen fehlt der Header Front-End-Https: On. Mit Re-Encryption tritt das Problem gar nicht auf.

Warum funktioniert Kerberos nur auf einem der beiden Server?

Fast immer liegt ein SPN am falschen Konto oder doppelt vor, oder auf einem Server läuft der Anwendungspool unter einem anderen Konto. Der LoadMaster beteiligt sich an Kerberos nicht, solange du keine Vorauthentifizierung mit Delegierung einsetzt.

Darf die Suche über den VIP crawlen?

Sie darf, sollte aber nicht. Führe den Crawler per hosts-Datei oder SiteDataServers direkt auf ein Front-End. Das entlastet die Benutzer-Server, umgeht Vorauthentifizierung, WAF und Persistenz und macht Crawl-Fehler wieder eindeutig.

Was passiert mit dem OOS-Virtual-Service nach dem 31. Dezember 2026?

Technisch läuft er weiter, solange die Server laufen. Sicherheitsupdates gibt es dann aber keine mehr. Plane, wie du OOS aus SharePoint abmeldest und den Virtual Service stilllegst, statt ihn als unbeaufsichtigten Altbestand im Internet stehen zu lassen.

Fazit: SharePoint ist nett zum LoadMaster, wenn man es lässt

SharePoint Server Subscription Edition stellt an einen Load Balancer überschaubare Anforderungen: keine Persistenz für die Anmeldung, ein gemeinsames Dienstkonto für Kerberos, saubere Namen. Die Probleme entstehen an den Stellen, an denen Annahmen aufeinanderprallen: TLS endet woanders, als SharePoint glaubt; ein Health Check erwartet 200, wo SharePoint höflich 401 sagt; der Crawler nimmt denselben Weg wie die Benutzer und läuft dabei in Vorauthentifizierung, WAF und Persistenz. Office Online Server bekommt seinen eigenen Virtual Service mit Affinität, wenigstens noch bis Jahresende. Und der Distributed Cache bleibt, wo er hingehört: zwischen den Servern, unbeeindruckt vom LoadMaster und im Idealfall auch unbeachtet von ihm.

Wer diese Punkte einmal sauber aufsetzt, hat eine Farm, bei der niemand weiß, dass ein LoadMaster davorsteht. Das ist das höchste Lob, das ein Load Balancer bekommen kann. Er wird es nicht hören, aber du schläfst besser.

TIPP · Unterstützung bei Planung und Umsetzung

Wenn du eine SharePoint-SE-Farm hinter dem LoadMaster neu aufbaust, Kerberos und Suche geradeziehen oder den Abschied von Office Online Server planen willst, hilft dir die Beratung zum Kemp LoadMaster. Wer Virtual Services, Health Checks und Persistenz mit dem eigenen Team im Labor durchspielen möchte, findet das in der Kemp-LoadMaster-Schulung.

WEITERLESEN · Weiter im Thema

› SPN-Probleme hinter dem Load Balancer: ein Name, mehrere Server
› Persistence und Scheduling: wer hängt an welchem Server und warum
› TLS-Offload, Re-Encryption und Zertifikate: PKI trifft LoadMaster
› Health Checks, die wirklich prüfen: warum „Port 443 offen“ nicht reicht
› SharePoint