Exchange Server hinter dem LoadMaster: Templates, Namespaces, Health Checks



WISSEN

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

› Kemp LoadMaster

BERATUNG

Exchange SE hinter dem LoadMaster neu aufbauen oder ein gewachsenes Setup aufräumen? Wir schauen mit dir auf Namespaces und Health Checks.

› Beratung zum Kemp LoadMaster

SCHULUNG

Templates importieren, SubVS bauen, healthcheck.htm verstehen und einen Exchange gezielt in Wartung schicken, im Labor statt in Produktion.

› Kemp-LoadMaster-Schulung

Exchange hinter einem Load Balancer ist eines dieser Themen, bei denen jeder glaubt, es sei erledigt, bis der erste Server in Wartung geht. Virtuelle IP anlegen, zwei Real Server eintragen, Port 443, fertig. Läuft ja. Und dann bootet ein Server nach dem Patchday, der IIS ist schon oben, die Exchange-Dienste noch nicht, und der LoadMaster schickt fröhlich jede zweite Outlook-Verbindung in ein schwarzes Loch. Der Port war offen. Der Health Check war grün. Die Benutzer waren es nicht.

Der Grund ist simpel: Exchange sieht von außen aus wie eine Webseite, besteht aber aus einem halben Dutzend Protokollen, die sich nur zufällig Port und Hostnamen teilen. OWA, ECP, MAPI über HTTP, EWS, ActiveSync, Autodiscover, das Offline-Adressbuch und für Nostalgiker noch Outlook Anywhere. Jedes davon hat einen eigenen Anwendungspool, kann einzeln ausfallen und hat eigene Vorstellungen davon, wie lange eine Verbindung offen bleiben darf. Ein Load Balancer, der das nicht weiß, verteilt Verkehr. Einer, der es weiß, verteilt Verfügbarkeit.

Dieser Beitrag gehört zur Serie rund um den Kemp LoadMaster und richtet sich an dich, wenn du Exchange Server Subscription Edition oder noch Exchange 2019 hinter einem Progress Kemp LoadMaster betreibst oder dorthin umziehst. Es geht um die Entscheidung zwischen Layer 4 und Layer 7, um das Namensmodell, um die Exchange-Templates von Kemp, um protokollspezifische Health Checks mit healthcheck.htm und um die drei Klassiker, bei denen es in der Praxis knallt: Autodiscover, MAPI über HTTP und ActiveSync. Wenn dir Begriffe wie Virtual Service, Real Server

und SubVS noch nicht flüssig über die Lippen gehen, lies vorher den Beitrag Virtual Service, Real Server, SubVS: das Grundvokabular des LoadMasters.

FAKTEN · Das Wichtigste in fünf Sätzen

Seit Exchange 2013 braucht der Client-Zugriff keine Sitzungsaffinität mehr; Microsoft empfiehlt für Exchange 2016, 2019 und SE einen einzigen Namespace mit Layer-7-Lastverteilung ohne Persistenz.

Layer 7 erlaubt einen Health Check je Protokoll; Layer 4 kann pro virtueller IP nur einen Pfad prüfen und nimmt im Fehlerfall den ganzen Server für alle Protokolle heraus.

Jedes virtuelle Verzeichnis liefert unter /<verzeichnis>/healthcheck.htm einen HTTP-Status 200, solange Managed Availability das Protokoll für gesund hält, und hört damit auf, wenn du den Server per Komponentenstatus in Wartung schickst.

Progress Kemp stellt fertige Exchange-Templates bereit, die einen Virtual Service mit SubVS je Protokoll samt passenden Health Checks anlegen; du musst sie trotzdem verstehen und nachschärfen.

Seit Exchange 2019 CU14 ist Extended Protection standardmäßig aktiv, und damit ist TLS-Offloading ohne Re-Encryption für Exchange keine Option mehr.

Layer 4 oder Layer 7: wie viel der LoadMaster von Exchange verstehen muss

Bevor du dich mit Templates beschäftigst, lohnt ein Blick darauf, was Exchange vom Load Balancer überhaupt noch verlangt. Die Antwort ist erfreulich kurz: erstaunlich wenig. Seit Exchange 2013 ist der Client-Zugriffsdienst zustandslos. Er authentifiziert die Anfrage, findet heraus, auf welchem Server das Postfach gerade aktiv ist, und leitet per Proxy dorthin weiter. Ob die nächste Anfrage desselben Benutzers auf einem anderen Server landet, ist Exchange egal. Microsoft schreibt das für Exchange 2016 und 2019 ausdrücklich so: Sitzungsaffinität am Load Balancer ist nicht mehr erforderlich.

Exchange SE ist Exchange 2019 mit neuer Lizenz

Für dieses Thema gibt es zwischen Exchange 2019 und Exchange Server Subscription Edition keinen Unterschied, der dem LoadMaster auffallen würde. Exchange SE ist seit dem 1. Juli 2025 allgemein verfügbar, die RTM-Version war codegleich mit Exchange 2019 CU15, und das In-Place-Upgrade von CU14 oder CU15 ist unterstützt. Neu sind Lizenzmodell und Lebenszyklus: SE folgt der Modern Lifecycle Policy und bleibt unterstützt, solange du aktuell bleibst. Exchange 2016 und 2019 haben ihr Supportende dagegen am 14. Oktober 2025 erreicht. Wenn du heute, Ende 2026, noch Exchange 2019 betreibst, ist das Load Balancing dein kleinstes Problem, aber die Konfiguration am LoadMaster kannst du beim Upgrade auf SE unverändert stehen lassen.

Layer 4: schnell, ehrlich, ahnungslos

Ein Layer-4-Virtual-Service sieht nur IP-Adressen und Ports. Der TLS-Verkehr läuft verschlüsselt durch, der LoadMaster weiß nicht, ob gerade OWA oder ActiveSync vorbeikommt. Das ist schnell und unkompliziert, Zertifikate liegen nur auf den Exchange-Servern, und die Client-IP-Adresse kommt ohne Umwege am Server an, wenn das Routing passt. Der Haken liegt beim Health Check: Ein Layer-4-Dienst kann zwar per HTTPS eine URL abfragen, aber eben nur eine pro Virtual Service. Also prüfst du stellvertretend /owa/healthcheck.htm und hoffst, dass MAPI, EWS und ActiveSync sich genauso fühlen wie OWA. Spoiler: Tun sie nicht immer.

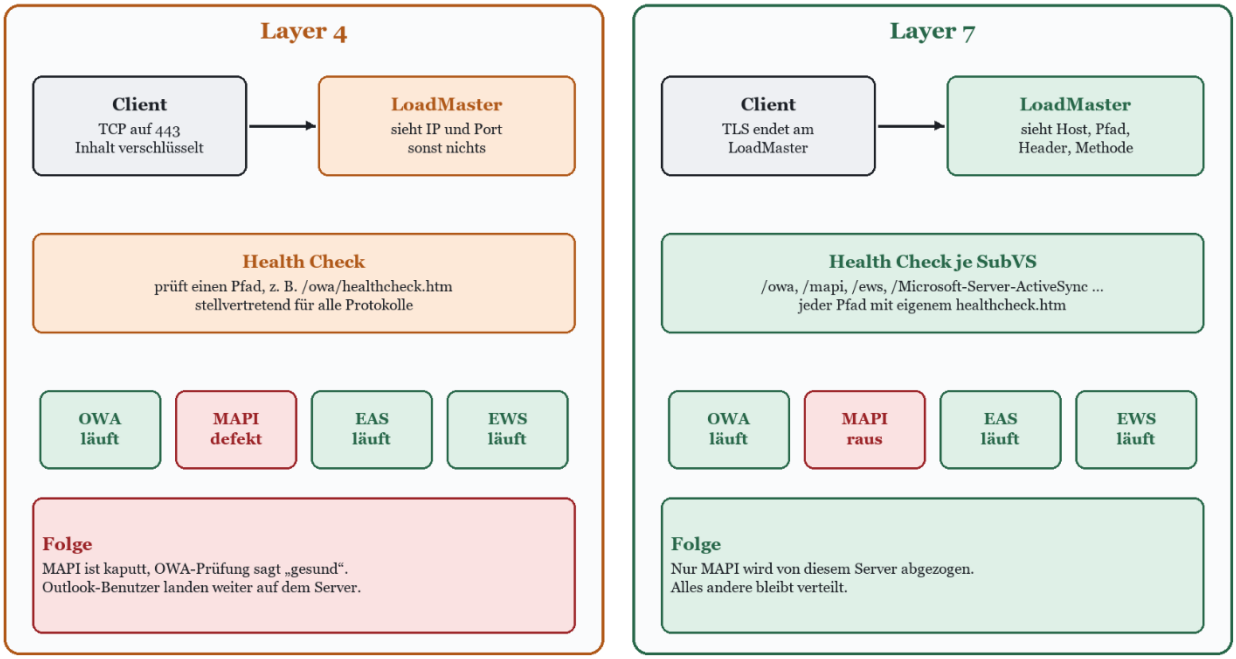
Layer 7: der LoadMaster liest mit

Bei Layer 7 terminiert der LoadMaster die TLS-Verbindung, sieht Hostnamen, Pfad und Header und kann anhand des Pfads entscheiden, in welchen SubVS eine Anfrage gehört. Jeder SubVS hat

eigene Real Server und einen eigenen Health Check. Fällt auf einem Server nur der Anwendungspool für MAPI aus, verschwindet dieser Server ausschließlich aus dem MAPI-SubVS. OWA, EWS und ActiveSync laufen dort weiter. Genau das meint Microsoft mit „Health Check je Protokoll“, und genau deshalb ist ein einzelner Namespace mit Layer 7 ohne Sitzungsaffinität die Empfehlung aus Redmond.

Layer 4 gegen Layer 7: was der LoadMaster sieht

Links ein verschlossener Umschlag, rechts ein geöffneter Brief



Skizze: vereinfachte Darstellung, Server und Pfade fiktiv

Kriterium	Layer 4	Layer 7 mit SubVS
Health Check	ein Pfad je virtueller IP	ein Pfad je Protokoll
Ausfall eines Protokolls	ganzer Server raus oder unentdeckt	nur dieses Protokoll raus
TLS	durchgereicht, Zertifikat nur auf Exchange	am LoadMaster beendet, zum Server erneut verschlüsselt
Content Rules, Header, ESP, WAF	nicht möglich	möglich
Client-IP am Server	sichtbar bei transparenter Weiterleitung	über X-Forwarded-For oder Transparenz
Rechenlast am LoadMaster	gering	höher, Sizing beachten
Typischer Einsatz	kleine Umgebungen, SMTP, Notlösung	Standard für HTTPS vor Exchange

WARNUNG · Extended Protection verträgt kein reines Offloading

Exchange 2019 ab CU14 und Exchange SE aktivieren Extended Protection standardmäßig. Dabei bindet der Server die Windows-Authentifizierung an die TLS-Verbindung, die er selbst sieht. Endet TLS am LoadMaster und geht unverschlüsselt per HTTP weiter, bricht das. Microsoft unterstützt mit Extended Protection kein SSL-Offloading, sondern nur SSL-Bridging, also Re-Encryption, und das nur, wenn LoadMaster und Exchange-Server dasselbe Zertifikat verwenden. Templates mit reinem

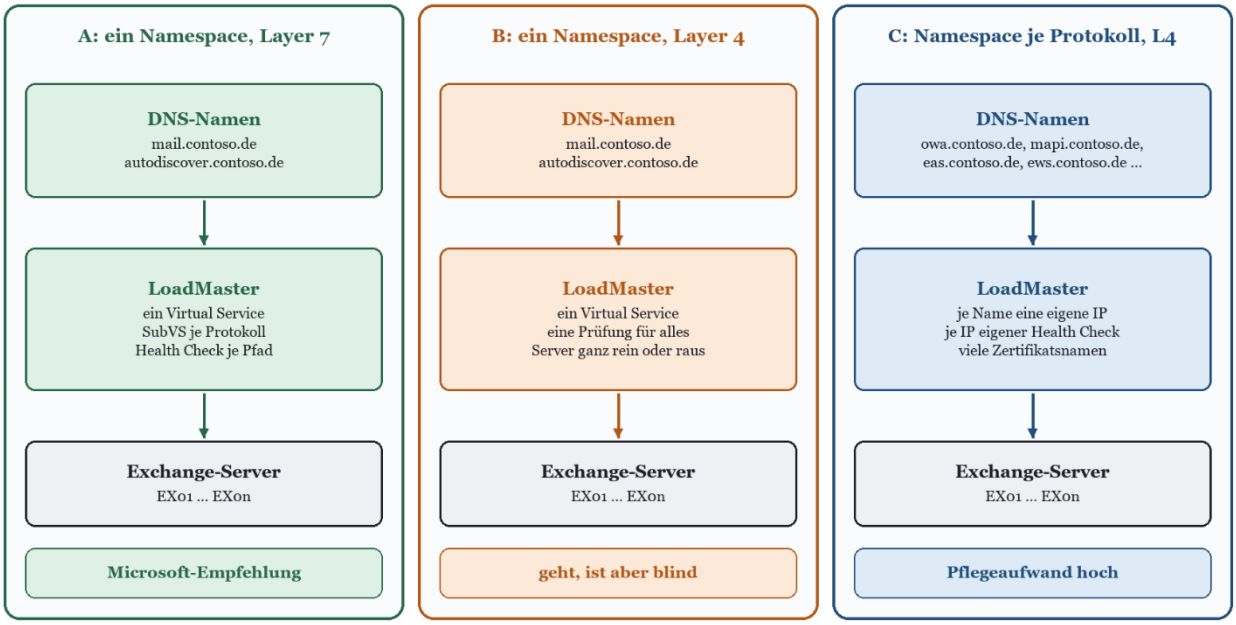
Offloading sind für aktuelle Exchange-Versionen deshalb die falsche Wahl. Details zu Zertifikaten und Re-Encryption stehen im Beitrag TLS-Offload, Re-Encryption und Zertifikate: PKI trifft LoadMaster.

Ein Namespace oder getrennte Namespaces: das Namensmodell entscheidet mit

Namespaces sind bei Exchange die DNS-Namen, unter denen Clients die Dienste erreichen. Das klingt nach Kosmetik, ist aber Architektur, denn der Namespace bestimmt, wie viele virtuelle IP-Adressen, Zertifikatsnamen und Health Checks du brauchst. Microsoft beschreibt im Kern drei Varianten, und der LoadMaster kann alle drei.

Drei Namensmodelle für denselben Exchange

Wie viele Namen du brauchst, hängt davon ab, wie klug dein Load Balancer ist



Skizze: Namensmodelle nach Microsoft-Lesart, Beispieldomäne contoso.de

Variante A: ein Namespace, Layer 7

Ein Name wie mail.contoso.de für OWA, ECP, MAPI, EWS, ActiveSync, OAB und Outlook Anywhere, dazu autodiscover.contoso.de. Beide Namen zeigen auf dieselbe virtuelle IP, der LoadMaster sortiert per Content Rule nach Pfad in die SubVS. Ein Zertifikat mit zwei Namen genügt, die virtuellen Verzeichnisse auf allen Exchange-Servern tragen dieselben internen und externen URLs. Das ist die Variante, die du ohne guten Grund wählen solltest. Sie ist auch die Variante, auf der die Kemp-Templates aufbauen.

Variante B: ein Namespace, Layer 4

Gleiche Namen, aber der LoadMaster reicht nur TCP durch. Funktioniert, ist aber blind für einzelne Protokolle. Sinnvoll höchstens, wenn der LoadMaster aus Lizenz- oder Leistungsgründen kein Layer 7 machen soll oder du übergangsweise eine alte Konfiguration weiterbetreibst. Plane in diesem Fall wenigstens den aussagekräftigsten Pfad als Health Check ein, in den meisten Umgebungen ist das heute MAPI über HTTP, weil Outlook dort die meisten Benutzer erzeugt.

Variante C: ein Namespace je Protokoll, Layer 4

Der Klassiker aus der Zeit, als Load Balancer teuer und dumm waren: owa.contoso.de, mapi.contoso.de, eas.contoso.de, ews.contoso.de und so weiter, jeder Name mit eigener virtueller IP und eigenem Layer-4-Health-Check auf den passenden Pfad. Damit bekommst du die Protokolltrennung von Layer 7, ohne TLS am LoadMaster aufzubrechen. Du bezahlst mit einem Zertifikat voller Namen, vielen DNS-Einträgen, vielen öffentlichen IP-Adressen und einer Exchange-Konfiguration, bei der jedes virtuelle Verzeichnis eine andere URL hat. Wer das heute neu baut, hat entweder einen sehr guten Grund oder einen sehr alten Projektplan.

Merkmal	A: 1 Name, L7	B: 1 Name, L4	C: n Namen, L4
Virtuelle IP-Adressen	eine	eine	eine je Protokoll
Namen im Zertifikat	2 (mail, autodiscover)	2	6 bis 9
Health Check je Protokoll	ja	nein	ja
TLS am LoadMaster	ja, Re-Encryption	nein	nein
ESP, WAF, Content Rules	ja	nein	nein
Pflegeaufwand Exchange-URLs	gering	gering	hoch
Empfehlung	Standard	Notlösung	Altlast oder Sonderfall

Split-DNS: intern derselbe Name

Damit ein einzelner Namespace funktioniert, muss mail.contoso.de intern auf die interne virtuelle IP des LoadMasters zeigen und extern auf die öffentliche Adresse vor der Firewall. Wer intern direkt auf einen Exchange-Server auflöst, umgeht den LoadMaster und wundert sich, warum die Wartung eines Servers plötzlich doch Outlook-Profile betrifft. Ebenso gehört die Autodiscover-SCP im Active Directory auf den gemeinsamen Namen, nicht auf den Server-FQDN, den das Setup dort gern hinterlässt. Dazu gleich mehr im Praxisteil.

TIPP · Eine Schreibweise für alle URLs

Setze InternalUrl und ExternalUrl aller virtuellen Verzeichnisse auf denselben Namen und prüfe das per PowerShell auf jedem Server. Ein einziger Server, auf dem noch https://ex02.contoso.local/ews/exchange.asmx eingetragen ist, reicht, damit Outlook gelegentlich am LoadMaster vorbei direkt mit diesem Server spricht. Das fällt erst auf, wenn genau dieser Server in Wartung geht.

Die Exchange-Templates von Kemp: was drin ist und was du nachziehst

Progress Kemp liefert für Exchange vorgefertigte Virtual-Service-Templates. Ein Template ist nichts Magisches, sondern eine Sammlung empfohlener Einstellungen, die beim Anlegen eines Virtual Service eingespielt werden: SubVS, Content Rules, Health Checks, Scheduling, Timeouts. Nach dem Anlegen ist alles ein ganz normaler Virtual Service, den du beliebig ändern kannst. Das Template merkt sich nichts und überwacht nichts.

Die Template-Pakete im Überblick

Für Exchange 2019 verteilt Progress die Templates in mehreren Paketen, die du aus dem Template-Bereich der Progress-Community herunterlädst und am LoadMaster importierst. Eigene Templates mit „SE“ im Namen sind dabei nicht nötig: Weil Exchange SE technisch auf Exchange

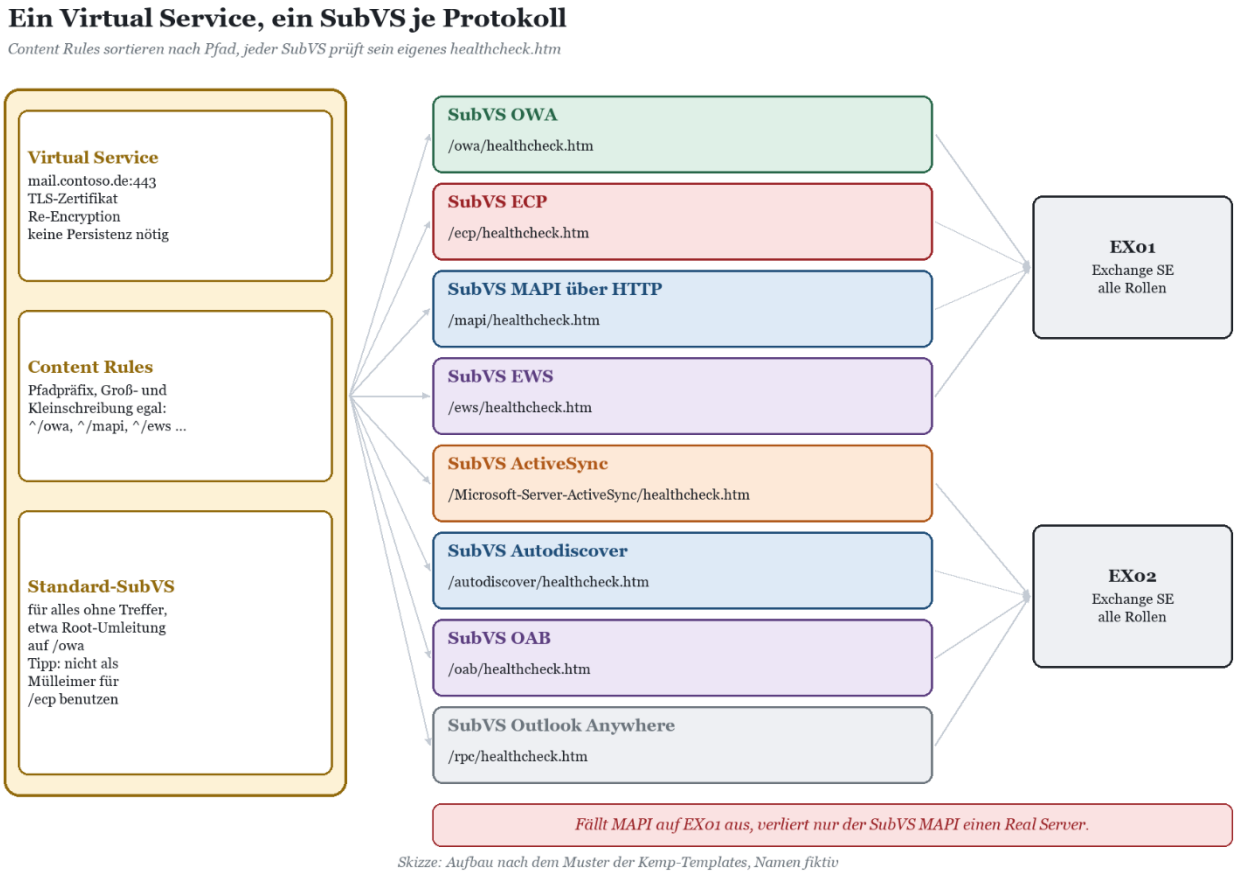
2019 CU15 aufsetzt, passen die 2019er-Templates. Prüfe trotzdem vor dem Import, ob im Download-Bereich inzwischen eine neuere Fassung liegt.

Paket	Inhalt	Brauchst du es?
Exchange2019Core	HTTPS-Dienste mit und ohne Offloading, SMTP	ja, Grundausstattung
Exchange2019ESP	HTTPS mit Edge Security Pack, SMTP mit ESP	nur für Vorauthentifizierung
Exchange2019Additional	IMAP, POP, SMTP mit STARTTLS oder TLS	wenn diese Protokolle laufen
Exchange2019WAF	HTTPS-Varianten mit Web Application Firewall	nur mit passender Lizenz

Wähle für HTTPS die Variante mit Re-Encryption. Das reine Offloading stammt aus einer Zeit, in der Extended Protection kein Thema war, und führt heute zu Anmeldeschleifen bei Outlook und EWS. Wenn du MFA vor OWA und ECP planst, kommt das ESP-Paket ins Spiel. Wie man dabei Browserpfade und Protokollpfade sauber trennt, zeigt der Beitrag MFA vor OWA, ECP und Co.: Zwei-Faktor am LoadMaster.

Ein SubVS je Protokoll

Das Herzstück der Templates ist die Aufteilung nach Pfad. Der Virtual Service beendet TLS, wertet den Pfad über Content Rules aus und reicht die Anfrage an den passenden SubVS weiter. Jeder SubVS enthält dieselben Exchange-Server als Real Server, prüft aber nur seinen eigenen Pfad. Wie Content Rules im Detail funktionieren und wie du sie für eigene Zwecke erweiterst, steht im Beitrag Content Rules: Header umschreiben, Pfade umleiten, Dinge verstecken.



Skizze: Aufbau nach dem Muster der Kemp-Templates, Namen fiktiv

SubVS	Pfadpräfix	Health-Check-URL	Besonderheit
OWA	/owa	/owa/healthcheck.htm	Browser, Formular

			oder ESP
ECP	/ecp	/ecp/healthcheck.htm	extern besser sperren
MAPI über HTTP	/mapi	/mapi/healthcheck.htm	lange Benachrichtigungs-Anfragen
EWS	/ews	/ews/healthcheck.htm	auch Teams, Hybrid, Drittsoftware
ActiveSync	/Microsoft-Server-ActiveSync	/Microsoft-Server-ActiveSync/healthcheck.htm	Heartbeat bis 59 Minuten
Autodiscover	/autodiscover	/autodiscover/healthcheck.htm	eigener Hostname
OAB	/oab	/oab/healthcheck.htm	große Downloads
Outlook Anywhere	/rpc	/rpc/healthcheck.htm	nur noch für Altclients

Was du nach dem Import prüfst

- **Zertifikat:** Dasselbe Zertifikat wie auf den Exchange-Servern, sonst stolpert Extended Protection. Nach jeder Zertifikatserneuerung an beiden Stellen tauschen.
- **Health-Check-Protokoll:** HTTPS mit HTTP/1.1 und dem richtigen Host-Header. Ohne Host-Header fragt der LoadMaster die IP-Adresse ab, und je nach IIS-Bindung antwortet dann gar nicht Exchange.
- **Persistenz:** Aus. Die Templates setzen keine Affinität, und das ist richtig. Wer aus Gewohnheit Source-IP-Persistenz nachrüstet, erzeugt hinter NAT-Gateways ungleich belastete Server und gewinnt nichts.
- **Timeouts:** Idle-Timeout so lang, dass ActiveSync-Pings und MAPI-Benachrichtigungen nicht abgeschnitten werden, siehe Praxisteil.
- **Standard-SubVS:** Was keine Content Rule trifft, landet dort. Eine Umleitung von / auf /owa ist nett, ein ungefilterter Durchgriff auf beliebige Pfade nicht.
- **Client-IP:** Entscheide, ob die Server die echte Client-Adresse sehen sollen, und richte das bewusst ein, statt es dem Zufall zu überlassen.

WICHTIG · Templates sind ein Startpunkt, kein Wartungsvertrag

Ein importiertes Template ändert sich nicht, wenn Progress eine neue Fassung veröffentlicht, und ein Virtual Service, der aus einem Template entstanden ist, bekommt keine Updates. Dokumentiere, welche Einstellungen du nach dem Import geändert hast. Beim nächsten Neuaufbau, beim Umzug auf ein neues HA-Paar oder bei der Fehlersuche um drei Uhr nachts wirst du dir dankbar sein.

Health Checks mit healthcheck.htm: was sie wissen und was nicht

Die Datei healthcheck.htm gibt es auf keinem Exchange-Server als Datei. Exchange beantwortet Anfragen an /<verzeichnis>/healthcheck.htm dynamisch, sobald Managed Availability das betreffende Protokoll auf diesem Server für gesund hält. Die Antwort ist ein schlichter HTTP-Status 200 mit dem Servernamen im Text. Hält Managed Availability das Protokoll für krank, etwa weil seine eigenen Tests mehrfach gescheitert sind, kommt statt 200 ein Fehler. Der Load Balancer muss also nichts über Exchange wissen. Er muss nur fragen und auf 200 achten.

Warum das besser ist als jeder selbst gebaute Check

Ein selbst gebauter Check auf /owa/auth/logon.aspx prüft, ob der IIS eine Seite ausliefert. Ein TCP-Check prüft, ob überhaupt jemand am Port lauscht. healthcheck.htm prüft, ob Exchange selbst das Protokoll für funktionsfähig hält, und das inklusive der Abhängigkeiten, die Managed

Availability im Blick hat. Damit verlagerst du die Frage „Ist dieser Server gesund?“ dorthin, wo die meiste Information liegt: auf den Server selbst. Warum TCP- und Port-Checks im Allgemeinen nicht reichen und wie du Health Checks für andere Anwendungen baust, beschreibt der Beitrag Health Checks, die wirklich prüfen: warum „Port 443 offen“ nicht reicht.

Wartungsmodus: der eingebaute Drain

Der schönste Nebeneffekt: Wenn du einen Exchange-Server vor dem Patchen per Set-ServerComponentState mit der Komponente ServerWideOffline auf Inactive setzt, liefern die healthcheck.htm-Seiten keinen Status 200 mehr. Der LoadMaster nimmt den Server daraufhin aus allen SubVS heraus, ohne dass du an der Weboberfläche des LoadMasters etwas anfassen musst. Neue Verbindungen gehen an die anderen Server, bestehende laufen aus. Nach dem Patchen setzt du den Status zurück, healthcheck.htm meldet wieder 200, und der Server ist zurück im Spiel.

Das funktioniert nur, wenn alle Health Checks wirklich auf healthcheck.htm zeigen. Ein einzelner SubVS mit TCP-Check, etwa für Autodiscover, weil das „ja nur XML ist“, schickt Clients weiterhin an einen Server, der sich gerade abmeldet. Willkommen bei den sporadischen Profilfehlern in Outlook, die niemand reproduzieren kann.

Was healthcheck.htm nicht weiß

healthcheck.htm prüft den Client-Zugriff auf diesem Server, nicht das Postfach dahinter. Ist eine Datenbankkopie nicht eingehängt, sagt healthcheck.htm auf allen Servern trotzdem 200, denn der Proxy funktioniert ja. Ein Load Balancer kann das auch gar nicht lösen, das ist Aufgabe der DAG. Ebenso wenig sieht healthcheck.htm Probleme mit dem Zertifikat, mit der Namensauflösung der Clients oder mit Authentifizierung. Für all das brauchst du ein Monitoring, das von außen echte Anmeldungen testet.

Check-Methode	Erkennt	Erkennt nicht
ICMP oder TCP 443	Server aus, Netzwerk weg	IIS hängt, Exchange-Dienste aus, Pool tot
HTTPS auf /owa/	IIS antwortet	MAPI, EWS, ActiveSync kaputt
healthcheck.htm je Pfad	Protokoll laut Managed Availability gesund, Wartungsmodus	Datenbank, Zertifikat, Anmeldung
Synthetische Anmeldung im Monitoring	Ende-zu-Ende-Funktion	nichts Wesentliches, aber kein Load-Balancer-Check

AUS DER PRAXIS · Der Server, der zu früh wieder da war

In einer Verwaltung mit zwei Exchange-Servern gab es nach jedem Patchday rund zehn Minuten lang Beschwerden über Outlook-Kennwortabfragen. Ursache: Der Virtual Service prüfte per TCP auf Port 443. Nach dem Neustart war der IIS nach wenigen Sekunden erreichbar, die Exchange-Anwendungspools und der Front-End-Transport aber noch lange nicht. Der LoadMaster schickte die Hälfte der Clients an einen Server, der zwar antwortete, aber noch nicht arbeiten konnte. Nach der Umstellung auf healthcheck.htm je SubVS und einem sauberen Wartungsablauf per Komponentenstatus war Ruhe. Die Helpdesk-Kollegen haben sich seitdem nicht mehr über den Patchday beschwert, nur noch über alles andere.

Wo es in der Praxis knallt: Autodiscover, MAPI über HTTP und ActiveSync

Die meisten Exchange-Tickets, die beim LoadMaster landen, sind keine LoadMaster-Fehler. Sie werden dort nur sichtbar, weil der LoadMaster an der Stelle steht, an der Clients, DNS, Zertifikate und Exchange aufeinandertreffen. Drei Kandidaten führen die Statistik an.

Autodiscover: der Dienst, den alle vergessen

Outlook findet seine Konfiguration über Autodiscover, und dabei probiert es mehrere Wege nacheinander. Domänenmitglieder fragen zuerst den Service Connection Point im Active Directory. Steht dort noch der FQDN eines einzelnen Servers, den das Setup eingetragen hat, gehen alle internen Outlook-Clients direkt an diesen Server, am LoadMaster vorbei. Korrigiere die AutoDiscoverServiceInternalUri auf jedem Server auf den gemeinsamen Namen, auch auf Servern, die du später hinzufügst.

Außerhalb der Domäne versucht Outlook unter anderem https://contoso.de/autodiscover/autodiscover.xml, bevor es autodiscover.contoso.de fragt. Antwortet auf contoso.de der Webserver der Unternehmensseite mit einem Zertifikatsfehler oder einer unerwarteten Weiterleitung, sehen Benutzer Warnungen, die mit Exchange scheinbar nichts zu tun haben. Am LoadMaster hilft das nicht, aber du solltest es kennen, bevor du stundenlang SubVS-Statistiken anstarrst.

Am LoadMaster selbst gibt es zwei typische Fehler. Erstens fehlt autodiscover.contoso.de im Zertifikat des Virtual Service oder die SNI-Auswahl liefert das falsche Zertifikat. Zweitens landet /autodiscover in einem SubVS mit falschem oder ohne Health Check, und genau dieser SubVS schickt Clients an den Server in Wartung. In hybriden Umgebungen kommt hinzu, dass Microsoft-Dienste wie der Free/Busy-Abgleich Autodiscover und EWS von außen erreichen müssen. Ein Geoblocking, das nur deutsche Adressen durchlässt, trifft diese Anfragen zuverlässig.

MAPI über HTTP: lange Anfragen, kurze Geduld

Seit Exchange 2016 ist MAPI über HTTP der Standard für Outlook, Outlook Anywhere ist nur noch Rückfallebene. MAPI über HTTP nutzt zwei Endpunkte unter /mapi: emsmdb für das Postfach und nspi für das Adressbuch. Für Benachrichtigungen über neue Elemente hält Outlook Anfragen bewusst offen, bis der Server etwas zu melden hat oder eine Wartezeit abläuft. Ein Load Balancer oder eine Firewall mit knappem Idle-Timeout schneidet diese Anfragen ab. Outlook baut dann neu auf, was meist niemand merkt, bis es sich häuft: „Verbindung getrennt“ in der Statusleiste, verzögerte neue Mails, gelegentlich Kennwortabfragen.

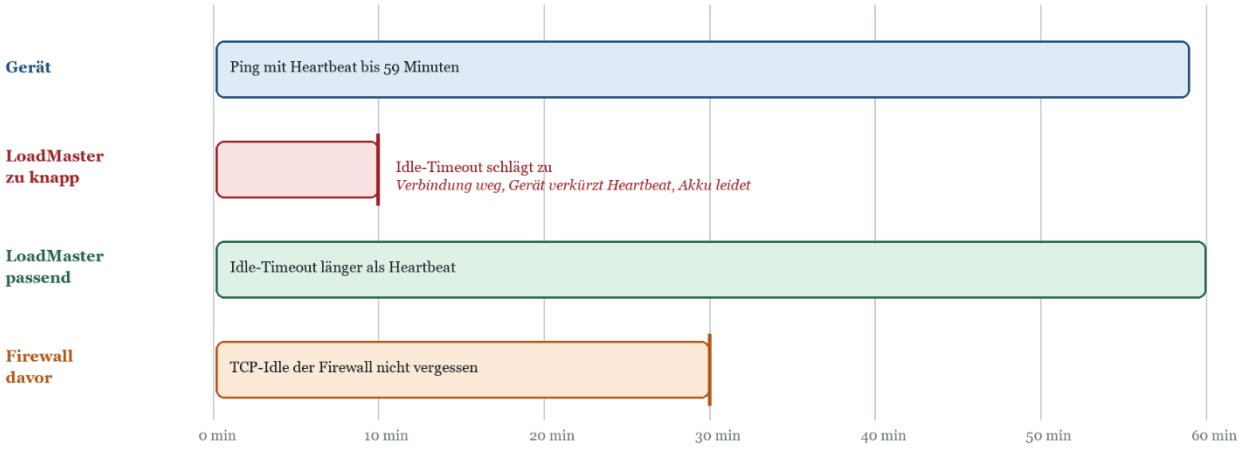
Drei Dinge prüfst du bei MAPI-Problemen zuerst: ob der MAPI-SubVS wirklich auf /mapi/healthcheck.htm prüft, ob das Idle-Timeout am LoadMaster und an allen Firewalls auf dem Weg mehrere Minuten beträgt und ob Extended Protection mit Re-Encryption und gleichem Zertifikat sauber zusammenspielt. Eine Vorauthentifizierung per ESP-Formular hat vor /mapi nichts verloren, Outlook kann kein HTML-Formular ausfüllen.

ActiveSync-Timeouts: Direct Push gegen ungeduldige Geräte

ActiveSync arbeitet mit Direct Push. Das Smartphone schickt einen Ping-Befehl mit einem Heartbeat-Intervall, und der Server hält die Anfrage offen, bis neue Daten da sind oder das Intervall abläuft. Exchange erlaubt standardmäßig Heartbeats bis knapp 59 Minuten. Das Gerät tastet sich an das längste Intervall heran, das die Strecke aushält. Kappt der LoadMaster oder eine Firewall die Verbindung früher, merkt das Gerät den Abbruch, verkürzt den Heartbeat und probiert es erneut. Ergebnis: mehr Verbindungen, mehr Last, leerere Akkus und gelegentlich Mails, die erst beim Öffnen der App kommen.

Direct Push gegen Idle-Timeout: wer zuerst auflegt

Ein ActiveSync-Ping hängt bewusst lange, der Load Balancer darf nicht ungeduldiger sein



Skizze: Zeitachse schematisch, Werte hängen von Gerät, Exchange und Firewall ab

Die Lösung ist unspektakulär: Das Idle-Timeout für den ActiveSync-Verkehr muss länger sein als der längste Heartbeat, den Exchange erlaubt, und zwar auf der ganzen Strecke vom Internet bis zum Exchange-Server. Am LoadMaster gibt es dafür eine Zeitbegrenzung für inaktive Verbindungen, global und je Virtual Service. Die Exchange-Templates setzen hier bereits einen großzügigen Wert, aber die Firewall davor kennt kein Template. Alternativ senkst du das maximale Heartbeat-Intervall in Exchange, was aber nur sinnvoll ist, wenn du ein Gerät auf der Strecke nicht ändern darfst.

Symptom	Wahrscheinliche Ursache	Erste Maßnahme
Outlook-Profil lässt sich intern nicht anlegen	SCP zeigt auf Server-FQDN oder alten Server	AutoDiscoverServiceInternalUri korrigieren
Zertifikatswarnung nur bei Autodiscover	Name fehlt im Zertifikat oder Root-Domäne antwortet	Zertifikat und SNI prüfen, Root-Domäne klären
Outlook trennt häufig die Verbindung	Idle-Timeout zu kurz für MAPI-Benachrichtigungen	Timeouts an LoadMaster und Firewall anheben
Ständige Kennwortabfragen nach Umstellung	Offloading trifft Extended Protection	Re-Encryption mit identischem Zertifikat
Smartphones ohne Push, hoher Akkuverbrauch	ActiveSync-Ping wird vorzeitig gekappt	Idle-Timeout länger als Heartbeat
Fehler nur während Wartung eines Servers	Ein SubVS prüft per TCP statt healthcheck.htm	alle SubVS auf healthcheck.htm umstellen
Free/Busy mit Exchange Online scheitert	Geoblocking oder WAF blockiert Microsoft-Dienste	Ausnahmen für Autodiscover und EWS prüfen

Client-IP, SMTP und der Rest der Familie

Zwei Dinge gehören eng zum Thema, sprengen aber diesen Beitrag. Erstens die Client-IP: Bei Layer 7 mit SNAT sehen die Exchange-Server in IIS-Logs und Protokolldateien nur noch die Adresse des LoadMasters. Für Fehlersuche, Sicherheitsanalysen und manche Konformitätsanforderungen ist das ärgerlich. Wie du das per X-Forwarded-For oder transparenter

Weiterleitung löst, steht im Beitrag Client-IP sichtbar machen: Transparenz, SNAT und X-Forwarded-For. Zweitens SMTP: Der Mailfluss läuft nicht über HTTPS, braucht eigene Virtual Services, oft auf Layer 4, und hat mit Empfangsconnectors und Relay-Berechtigungen ganz eigene Fallstricke. Die behandelt der Beitrag SMTP über den LoadMaster: Relay, Empfangsconnectors und die echte Absender-IP.

TIPP · Fehlersuche mit Blick auf beide Seiten

Wenn ein Exchange-Problem nur hinter dem LoadMaster auftritt, teste zuerst direkt gegen einen Server, etwa über einen Hosts-Eintrag auf einem Testclient. Funktioniert es dort, liegt der Fehler zwischen Client und Exchange, also am LoadMaster, an DNS oder an der Firewall. Wie du dann mit L7-Debug-Log und Mitschnitt am LoadMaster weitermachst, beschreibt der Beitrag Troubleshooting am LoadMaster: Logs, L7-Debug und TCP-Dump.

FAQ: Häufige Fragen zu Kemp und Exchange

Brauche ich für Exchange SE andere Kemp-Templates als für Exchange 2019?

Nein. Exchange SE basiert technisch auf Exchange 2019 CU15, Pfade, virtuelle Verzeichnisse und healthcheck.htm sind identisch. Die Exchange-2019-Templates passen, solange du die Variante mit Re-Encryption wählst.

Muss ich am LoadMaster Persistenz für Exchange einschalten?

Nein. Seit Exchange 2013 ist der Client-Zugriff zustandslos, Microsoft verlangt für Exchange 2016, 2019 und SE keine Sitzungsaffinität. Persistenz schadet in der Regel nicht dramatisch, sorgt aber für ungleich verteilte Last, vor allem wenn viele Clients hinter einer gemeinsamen NAT-Adresse sitzen. Hintergründe dazu stehen im Beitrag Persistence und Scheduling: wer hängt an welchem Server und warum.

Kann ich TLS am LoadMaster beenden und per HTTP zum Exchange-Server weiterleiten?

Nicht mit aktivierter Extended Protection, und die ist seit Exchange 2019 CU14 Standard. Microsoft unterstützt dann nur SSL-Bridging mit demselben Zertifikat auf LoadMaster und Exchange-Server. Extended Protection abzuschalten, um Offloading zu retten, ist ein Sicherheitsrückschritt, den du dir gut überlegen solltest.

Reicht ein einziger Health Check auf /owa für alle Protokolle?

Er reicht, um einen komplett ausgefallenen Server zu erkennen. Er reicht nicht, um einen Server zu erkennen, auf dem nur MAPI oder ActiveSync gestört ist. Mit Layer 7 und einem SubVS je Protokoll bekommst du die genauere Prüfung praktisch kostenlos.

Wie schicke ich einen Exchange-Server in Wartung, ohne am LoadMaster zu klicken?

Setze den Komponentenstatus ServerWideOffline auf Inactive. Die healthcheck.htm-Seiten melden dann keinen Status 200 mehr, und der LoadMaster nimmt den Server aus allen SubVS heraus. Voraussetzung ist, dass wirklich jeder SubVS auf healthcheck.htm prüft.

Gehört ECP ins Internet?

Im Idealfall nicht. Der ECP-SubVS lässt sich am LoadMaster für Anfragen von außen sperren, während intern weiter administriert wird. Wenn es unbedingt nach außen muss, dann nur mit Vorauthentifizierung und zweitem Faktor.

Warum bekommen Smartphones keine Push-Benachrichtigungen mehr, seit der LoadMaster davor steht?

Meist kappt ein Idle-Timeout auf der Strecke die langen ActiveSync-Ping-Anfragen. Prüfe die Zeitbegrenzung am Virtual Service und an jeder Firewall davor. Sie muss länger sein als das maximale Heartbeat-Intervall von knapp einer Stunde.

Fazit: Exchange verteilen ist leicht, Exchange verstehen lohnt sich

Exchange SE und Exchange 2019 sind für einen Load Balancer erfreulich pflegeleicht: keine Persistenz, ein Namespace, ein Zertifikat mit zwei Namen. Die Kemp-Templates liefern einen Virtual Service mit SubVS je Protokoll und Health Checks auf healthcheck.htm, und damit hast du die Architektur, die Microsoft empfiehlt, in wenigen Minuten auf dem LoadMaster. Die eigentliche Arbeit beginnt danach: Re-Encryption statt Offloading wegen Extended Protection, dasselbe Zertifikat an beiden Enden, Host-Header im Health Check, Timeouts, die zu ActiveSync und MAPI passen, und eine Autodiscover-Konfiguration, die nicht am LoadMaster vorbeiführt.

Wer das einmal sauber aufsetzt, bekommt etwas, das in vielen Exchange-Umgebungen fehlt: Patchdays, die niemand bemerkt. Server gehen per Komponentenstatus in Wartung, der LoadMaster nimmt sie heraus, die Benutzer arbeiten weiter. Das ist nicht spektakulär. Aber im Betrieb ist langweilig das schönste Kompliment, das eine Infrastruktur bekommen kann.

TIPP · Unterstützung bei Planung und Umsetzung

Wenn du eine Exchange-Umgebung hinter dem LoadMaster neu aufbaust, von Exchange 2019 auf SE umziehst oder ein gewachsenes Setup mit Layer-4-Altlasten aufräumen willst, hilft dir die Beratung zum Kemp LoadMaster. Wer Templates, SubVS und Wartungsabläufe mit dem eigenen Team im Labor durchspielen will, findet das in der Kemp-LoadMaster-Schulung.

WEITERLESEN · Weiter im Thema

› Health Checks, die wirklich prüfen: warum „Port 443 offen“ nicht reicht
› SMTP über den LoadMaster: Relay, Empfangsconnectors und die echte Absender-IP
› MFA vor OWA, ECP und Co.: Zwei-Faktor am LoadMaster
› Client-IP sichtbar machen: Transparenz, SNAT und X-Forwarded-For
› TLS-Offload, Re-Encryption und Zertifikate: PKI trifft LoadMaster