LoadMaster in Azure und hybriden Umgebungen



Skizze: die vier Baustellen eines LoadMasters in Azure

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

BERATUNG
LoadMaster nach Azure verlegen, HA-Paar hinter dem Azure Load Balancer, Real Server im eigenen Rechenzentrum? Wir planen das mit dir, bevor die Probe rot wird.
› Beratung zum Kemp LoadMaster

SCHULUNG
HA in Azure, NSG-Regeln und hybride Real Server im Labor durchspielen, wo ein abgerissener Tunnel niemandem den Montag ruiniert.
› Kemp-LoadMaster-Schulung

Irgendwann steht es in der IT-Strategie, meist auf Seite drei, zwischen „Cloud first“ und „Digitalisierung der Verwaltungsprozesse“: Das Rechenzentrum soll schrumpfen. Die ersten Workloads wandern nach Azure, der Exchange-Server bleibt vorerst im Keller, SharePoint vielleicht auch, und irgendwer fragt: Was machen wir eigentlich mit dem LoadMaster? Die naheliegende Antwort lautet: Den gibt es doch im Azure Marketplace. Stimmt. Und genau da beginnt der Spaß.

Denn ein LoadMaster in Azure ist softwareseitig derselbe LoadMaster, den du kennst: gleiche Weboberfläche, gleiche Virtual Services, gleiche Content Rules, gleiches Edge Security Pack. Das Netz darunter ist aber ein völlig anderes. Azure kennt kein Gratuitous ARP, keine geteilten MAC-Adressen, kein Layer 2 im klassischen Sinn. Netzwerksicherheitsgruppen sind keine Firewall, die irgendwo im Pfad steht, sondern Regeln direkt an der Netzwerkkarte. Und wenn die Real Server im eigenen Rechenzentrum stehen, läuft jeder Request zweimal über VPN oder ExpressRoute. Wer das ignoriert, baut sich ein HA-Paar, das nie umschaltet, oder eines, das beide Knoten gleichzeitig für tot hält.

Dieser Beitrag aus der Serie zum Kemp LoadMaster schließt die Lücke zwischen der Progress-Dokumentation und Microsoft Learn. Du erfährst, wie du einen kemp loadmaster azure aus dem Marketplace sauber aufsetzt, warum Hochverfügbarkeit in Azure über den Azure Load Balancer läuft, welche NSG-Regeln du wirklich brauchst, wie das Hybridszenario mit Real Servern on-premises funktioniert und wann du statt des LoadMasters besser zu Azure Application Gateway oder Azure Front Door greifst. Mit Microsoft-Brille, ohne Herstellerprosa.

FAKTEN · Das Wichtigste in 30 Sekunden

Progress bietet den LoadMaster im Azure Marketplace als VM-Image an, je nach Angebot mit eigener Lizenz (BYOL) oder nutzungsbasiert über die Azure-Rechnung.

Azure-Netze unterstützen kein Gratuitous ARP. Das klassische HA-Verfahren mit geteilter virtueller IP funktioniert deshalb nicht. Progress setzt stattdessen einen Azure Load Balancer vor das Paar, der per Health Probe erkennt, welcher Knoten aktiv ist.

Die Health-Check-Port-Einstellung muss auf beiden LoadMastern identisch sein und als Probe-Port im Azure Load Balancer hinterlegt werden. Der Herstellerleitfaden nutzt im Beispiel eine HTTP-Probe auf TCP 8444.

Der Basic Load Balancer ist seit dem 30. September 2025 eingestellt. Nimm den Standard Load Balancer, und denk daran: Der ist standardmäßig geschlossen, bis eine NSG den Verkehr erlaubt.

Real Server außerhalb der eigenen Subnetze sind möglich, erfordern aber die globale Option für nicht lokale Real Server und einen Virtual Service ohne Transparenz.

Application Gateway und Front Door sind HTTP(S)-Dienste. Kerberos Constrained Delegation, SMTP oder RDP-Lastverteilung bleiben LoadMaster-Terrain.

Aus dem Marketplace in die Produktion: was beim Aufsetzen zählt

Der Marketplace verkauft dir die Illusion, dass ein LoadMaster in Azure drei Klicks entfernt ist. Technisch stimmt das: Angebot auswählen, Größe, VNet, Subnetz, Kennwort, fertig. Nach fünf Minuten läuft eine VM mit LoadMaster-Firmware, und du kannst dich an der Weboberfläche anmelden. Die eigentliche Arbeit sind die Entscheidungen, die der Assistent dir nicht abnimmt, und die du später nur mit Neuaufbau korrigierst.

Lizenzmodell, Größe und Region

Im Marketplace findest du in der Regel zwei Varianten: Images mit eigener Lizenz, die du bei Progress beziehst, und Images, bei denen die LoadMaster-Lizenz nutzungsbasiert mit der VM-Laufzeit über Azure abgerechnet wird. Welche wirtschaftlich besser passt, hängt vom Durchsatz, von der Laufzeit und davon ab, ob du bereits Abonnements bei Progress hast. Details zu Editionen und Kapazitätsstufen stehen in Editionen, Lizenzierung und Sizing: welcher LoadMaster für welchen Laden. Für die Technik wichtig: Die Lizenz begrenzt den Durchsatz, die VM-Größe begrenzt CPU und Netzwerkbandbreite. Beides muss zusammenpassen. Ein hoch lizenzierter LoadMaster auf einer winzigen VM ist wie ein Sportwagen mit Fahrradreifen: sieht gut aus im Datenblatt, fährt aber nicht schneller.

Die Region wählst du nicht nach dem schönsten Namen, sondern nach Nähe zu Nutzern und Real Servern sowie nach den Anforderungen deines Datenschutzbeauftragten. Für ein HA-Paar verlangt der Herstellerleitfaden eine Verfügbarkeitsgruppe, also eine Availability Set, damit beide VMs auf getrennter Hardware landen. Wer stattdessen Verfügbarkeitszonen nutzen will, prüft vorher, ob Region, VM-Größe und Herstellerunterstützung mitspielen.

Netzwerkkarten, Subnetze und ausgehender Verkehr

Der einfachste und vom Hersteller für HA beschriebene Aufbau ist einarmig: eine Netzwerkkarte, ein Subnetz, Virtual Services und Real Server über dieselbe Schnittstelle. Mehrarmige Aufbauten mit getrennten Subnetzen für Frontend und Backend sind möglich, verlangen aber Sorgfalt. Die Azure-HA-Einstellungen kennen dafür eine Option, mit der der Health Check auf allen Schnittstellen statt nur auf eth0 lauscht. Und Bonding von Schnittstellen gibt es in Azure laut Herstellerdokumentation gar nicht, weil die Plattform es nicht hergibt.

Gern übersehen wird der ausgehende Verkehr. Der LoadMaster will Lizenzserver, Firmware-Downloads, OCSP- und CRL-Adressen und gegebenenfalls Entra ID erreichen. Microsoft hat das implizite Standard-Ausgangsrouting für VMs abgekündigt. In virtuellen Netzen, die nach dem 31. März 2026 mit aktuellen API-Versionen angelegt werden, sind Subnetze standardmäßig privat. Ohne NAT Gateway, Ausgangsregel am Load Balancer, öffentliche IP oder zentrale Firewall kommt der LoadMaster dann schlicht nicht ins Internet. Das merkst du nicht bei der Inbetriebnahme, sondern bei der Lizenzaktivierung oder beim ersten Firmware-Update.

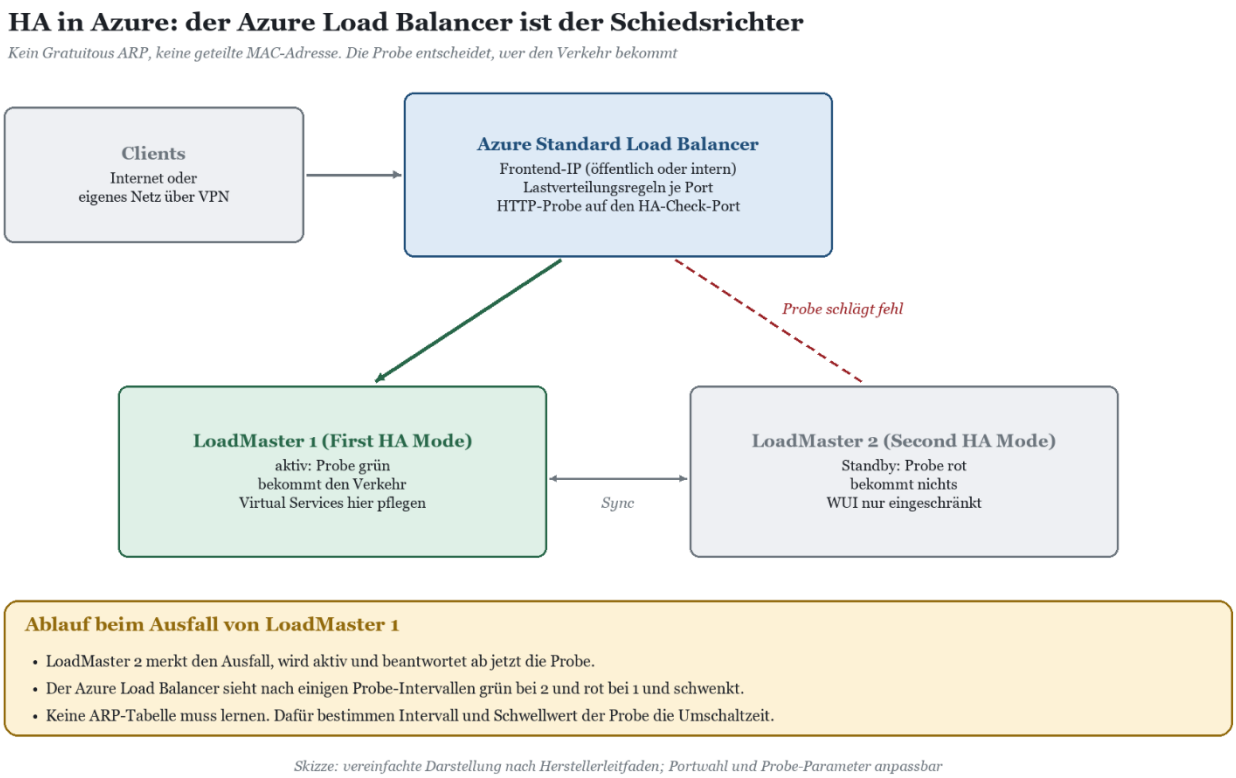
WARNUNG · Weboberfläche nicht ins Internet hängen

Der Marketplace-Assistent bietet gern eine öffentliche IP direkt an der VM an, und eine großzügige NSG-Regel gleich mit. Lass das. Die Verwaltung auf TCP 8443 und SSH auf TCP 22 gehören hinter VPN, Azure Bastion oder ein dediziertes Verwaltungsnetz. Ein LoadMaster ist ein Gerät, das TLS-Schlüssel deiner wichtigsten Dienste kennt. Das ist kein Kandidat für „mal eben aus dem Homeoffice per öffentlicher IP“.

Entscheidung	Optionen	Worauf du achtest
Lizenz	BYOL oder nutzungsbasiert	Laufzeit, Durchsatz, vorhandene Progress-Abonnements
VM-Größe	je nach Angebot	Netzwerkbandbreite der VM-Serie, TLS-Last, WAF-Nutzung
Verfügbarkeit	Availability Set, ggf. Zonen	Herstellerleitfaden nennt Availability Set für HA
Netzdesign	einarmig oder mehrarmig	Health Check auf allen Schnittstellen bei mehrarmig
Ausgang	NAT Gateway, Firewall, Outbound Rule	private Subnetze in neuen VNets seit 31.03.2026
Verwaltung	Bastion, VPN, Verwaltungs-Subnetz	keine öffentliche IP für WUI und SSH

Hochverfügbarkeit ohne Gratuitous ARP: der Azure Load Balancer als Schiedsrichter

On-premises funktioniert ein LoadMaster-HA-Paar so, wie du es aus HA-Paar, Failover und Konfig-Sync: zwei LoadMaster, ein Gedanke kennst: Beide Knoten teilen sich eine virtuelle IP. Der aktive Knoten beantwortet ARP-Anfragen für diese Adresse, und beim Failover verkündet der neue aktive Knoten per Gratuitous ARP: Ich bin es jetzt. Switches und Router aktualisieren ihre Tabellen, fertig. In Azure verhallt dieser Ruf ungehört. Das virtuelle Netz ist ein softwaredefiniertes Overlay, das genau weiß, welche IP zu welcher Netzwerkkarte gehört, und sich von keiner VM etwas anderes erzählen lässt. Eine IP, die einer Netzwerkkarte nicht zugewiesen ist, erreicht diese VM nicht. Punkt.



Skizze: vereinfachte Darstellung nach Herstellerleitfaden; Portwahl und Probe-Parameter anpassbar

Wie das Azure-HA-Paar funktioniert

Progress löst das Problem, indem es die Entscheidung, wer aktiv ist, an den Azure Load Balancer auslagert. Beide LoadMaster stehen im Backend-Pool. Der Azure Load Balancer prüft beide per Health Probe auf einem festgelegten Port. Nur der aktive LoadMaster antwortet dort positiv, also schickt der Azure Load Balancer den Verkehr nur zu ihm. Fällt der aktive Knoten aus, übernimmt der Partner, antwortet ab sofort auf der Probe, und der Azure Load Balancer schwenkt den Verkehr um. Änderungen an den Virtual Services pflegst du am aktiven Knoten, sie werden auf den Standby-Knoten repliziert. Am Standby ist die Weboberfläche auf lokale Verwaltung beschränkt.

Eingerichtet wird das in der Weboberfläche des LoadMasters unter System Configuration > HA and Clustering > HA Mode, im Bereich Azure HA Parameters, der nur in LoadMaster für Azure erscheint. Dort wählst du für den einen Knoten First HA Mode und für den anderen Second HA Mode, trägst unter Partner Name/IP den jeweils anderen Knoten ein und legst den Health Check Port fest. Haben beide Knoten denselben Modus, funktioniert HA nicht. Mit Switch to Preferred Server bestimmst du, ob nach einem Ausfall der erste Knoten die Rolle zurückholt oder ob der jeweils aktive Knoten aktiv bleibt.

TIPP · Probe und Check-Port gehören zusammen

Der Health Check Port muss auf beiden LoadMastern identisch sein und exakt der Port der Probe im Azure Load Balancer. Der Herstellerleitfaden zeigt eine HTTP-Probe auf TCP 8444 mit Pfad / und einem Intervall von fünf Sekunden. Wenn du einen anderen Port nimmst, ändere ihn an allen drei Stellen gleichzeitig. Und dokumentiere ihn: In zwei Jahren weiß niemand mehr, warum auf 8444 etwas lauscht, und irgendwer schließt den Port „aus Sicherheitsgründen“.

Was sich gegenüber on-premises ändert

Die Mechanik klingt gleichwertig, hat aber Konsequenzen, die du kennen solltest. Die Umschaltzeit wird nicht mehr von ARP bestimmt, sondern von Probe-Intervall und der Zahl fehlgeschlagener Proben, bis der Azure Load Balancer reagiert. Bestehende TCP-Verbindungen überleben den

Wechsel nicht, denn der neue Knoten kennt sie nicht. Für Outlook, ActiveSync oder RD Gateway bedeutet das einen Verbindungsabbruch mit automatischer Neuverbindung, für einen laufenden Upload nach SharePoint ein „Bitte erneut versuchen“.

Dazu kommt das Leerlauf-Zeitlimit des Azure Load Balancers. Es liegt standardmäßig bei vier Minuten und lässt sich pro Regel erhöhen. Lange ruhende Verbindungen, typisch für RDP über RD Gateway oder Exchange-Benachrichtigungen, werden sonst stillschweigend abgeräumt. Gleiche das Zeitlimit mit den Timeouts deiner Virtual Services ab, und aktiviere bei Bedarf den TCP-Reset bei Leerlauf, damit Clients einen sauberen Abbruch sehen statt einer hängenden Sitzung.

Aspekt	HA on-premises	HA in Azure
Wer bestimmt den aktiven Knoten?	die LoadMaster selbst, per HA-Protokoll	die LoadMaster, sichtbar gemacht über die Probe
Wie findet der Verkehr ihn?	Gratuitous ARP für die geteilte virtuelle IP	Azure Load Balancer leitet nur an den Knoten mit grüner Probe
Umschaltzeit	Sekunden, abhängig vom HA-Timeout	HA-Erkennung plus Probe-Intervall mal Schwellwert
Virtuelle IP	geteilte Adresse im Subnetz	Frontend-IP des Azure Load Balancers
Verwaltung einzelner Knoten	eigene Adressen im Verwaltungsnetz	eigene Adressen, ggf. NAT-Regeln mit eigenem Port je Knoten
Typischer Fehler	Switch filtert Gratuitous ARP	NSG oder Firewall blockiert die Probe

AUS DER PRAXIS · Das Paar, das nie umschaltete

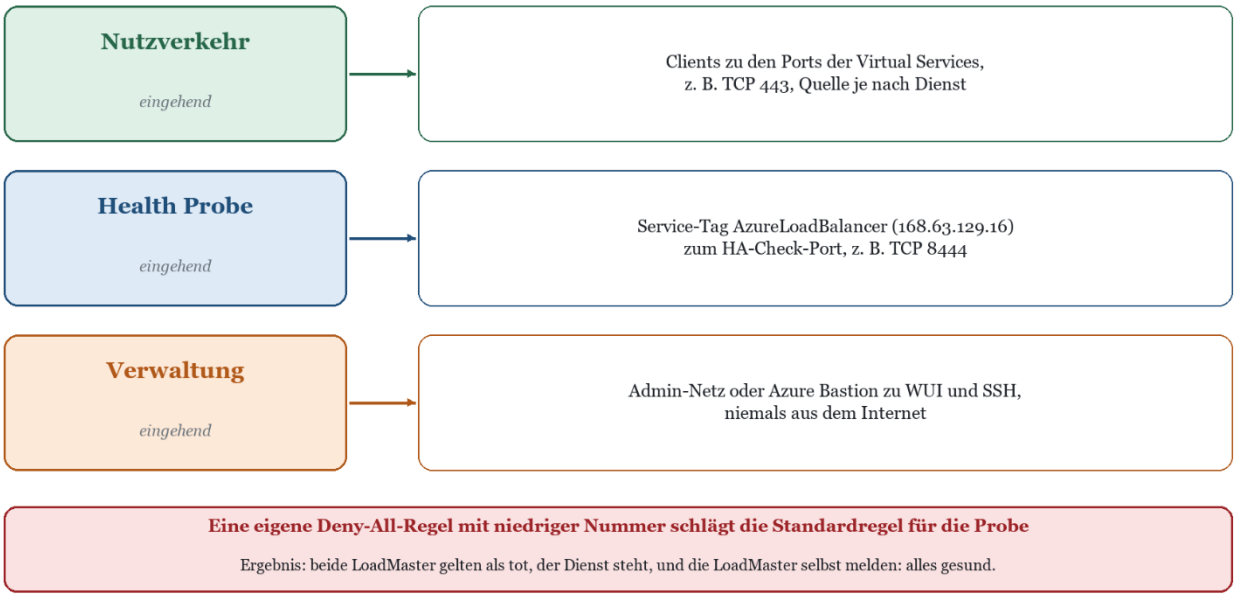
Eine Verwaltung hatte ihren LoadMaster in Azure klassisch eingerichtet: zwei VMs, HA-Modus aktiviert, Konfiguration synchron. Beim ersten Wartungsfenster wurde der aktive Knoten neu gestartet, und OWA war zehn Minuten weg. Der Grund: Vor dem Paar stand kein Azure Load Balancer, sondern eine statische DNS-Zuordnung auf die IP des ersten Knotens. Der zweite Knoten war brav aktiv geworden. Er hatte nur niemanden, der ihm Verkehr schickte. HA ist in Azure keine Eigenschaft des LoadMasters, sondern eine des gesamten Aufbaus.

Netzwerksicherheitsgruppen: die Firewall, die an jeder Netzwerkkarte klebt

Netzwerksicherheitsgruppen sind zustandsbehaftete Paketfilter, die Azure am Subnetz oder an der Netzwerkkarte auswertet. Sie kennen Quell- und Zieladressen, Ports, Protokolle und Service-Tags, aber keine Anwendungen. Regeln werden nach Priorität abgearbeitet, die niedrigste Nummer gewinnt. Am Ende jeder NSG stehen drei Standardregeln für eingehenden Verkehr: Verkehr aus dem virtuellen Netz erlauben, Verkehr vom Azure Load Balancer erlauben, alles andere verweigern. Das reicht für eine Demo. Für die Produktion reicht es nie.

Netzwerksicherheitsgruppen: wer muss wohin?

Drei Verkehrsarten, drei Regelwerke. Die Probe ist die, die alle vergessen



Skizze: Beispielports; tatsächliche Ports ergeben sich aus deinen Virtual Services und der HA-Konfiguration

Die drei Verkehrsarten, die du freigeben musst

Für einen LoadMaster in Azure brauchst du eingehend drei Regelgruppen. Erstens den Nutzverkehr zu den Ports deiner Virtual Services, also zum Beispiel TCP 443 für OWA, SharePoint oder ADFS. Wichtig: Der Azure Load Balancer ist ein Pass-Through-Dienst auf Layer 4. Er tauscht die Quelladresse nicht aus. In der NSG erscheint der Verkehr deshalb mit der echten Client-Adresse, nicht mit der des Load Balancers. Wer die Regel auf „AzureLoadBalancer“ beschränkt, sperrt also alle Nutzer aus. Zweitens die Health Probe. Sie kommt von der virtuellen Plattformadresse 168.63.129.16, in NSG-Regeln abgebildet durch das Service-Tag AzureLoadBalancer. Drittens die Verwaltung aus deinem Admin-Netz oder von Azure Bastion.

Regel	Quelle	Ziel-Port	Kommentar
Nutzverkehr HTTPS	Internet bzw. Client-Netze	TCP 443	echte Client-Adressen, kein SNAT durch den Azure Load Balancer
Nutzverkehr SMTP	Internet oder Relay-Quellen	TCP 25	nur wenn der LoadMaster SMTP annimmt; ausgehend Port 25 ist in Azure eingeschränkt
Health Probe	Service-Tag AzureLoadBalancer	HA-Check-Port, z. B. TCP 8444	ohne diese Regel gelten beide Knoten als tot
Verwaltung WUI	Admin-Netz, Bastion-Subnetz	TCP 8443 bzw. dein WUI-Port	nie aus dem Internet
Verwaltung SSH	Admin-Netz, Bastion-Subnetz	TCP 22	auch für GEO-Partner nötig, falls genutzt
HA-Synchronisation	Partner-Knoten	laut Herstellerdoku	innerhalb des Subnetzes meist durch die VNet-Standardregel abgedeckt

WARNUNG · Die Deny-All-Regel mit zu hohem Ehrgeiz

Viele Sicherheitsrichtlinien verlangen eine explizite Regel „alles verweigern“ mit einer niedrigen Prioritätsnummer, damit niemand sich auf die Standardregeln verlässt. Sitzt diese Regel vor der Standardregel AllowAzureLoadBalancerInBound und hast du keine eigene Freigabe für die Probe,

dann sieht der Azure Load Balancer beide LoadMaster als tot. Die LoadMaster selbst melden alles grün, die Real Server sind gesund, nur der Dienst ist weg. Wer dann am LoadMaster sucht, sucht am falschen Ende.

NSG, Azure Firewall und der Weg dazwischen

In vielen Azure-Landschaften steht in einem zentralen Hub-VNet eine Azure Firewall oder eine Firewall eines Drittherstellers, und benutzerdefinierte Routen zwingen allen Verkehr durch sie. Das ist sauber, bis eingehender Verkehr über den Azure Load Balancer kommt, die Antwort des LoadMasters aber über die Firewall zurückgeroutet wird. Dann läuft der Verkehr asymmetrisch, und die zustandsbehaftete Firewall verwirft die Antworten, weil sie den Verbindungsaufbau nie gesehen hat. Die Lösung ist eine Designentscheidung: Entweder liegt der öffentliche Eingang an der Firewall und der LoadMaster dahinter mit internem Azure Load Balancer, oder das LoadMaster-Subnetz bekommt Routen, die Antworten an Clients nicht über die Firewall schicken. Mischformen ohne Plan enden im TCP-Dump, und wie du den am LoadMaster ziehst, steht in Troubleshooting am LoadMaster: Logs, L7-Debug und TCP-Dump.

FAKTEN · NSG-Grundlagen mit Microsoft-Brille

Standard Load Balancer und öffentliche IP-Adressen der Standard-SKU sind „secure by default“: Eingehender Verkehr wird erst durchgelassen, wenn eine NSG ihn erlaubt.

Die Standardregeln für eingehenden Verkehr sind AllowVnetInBound (65000), AllowAzureLoadBalancerInBound (65001) und DenyAllInBound (65500).

Die Adresse 168.63.129.16 ist die virtuelle IP der Azure-Plattform. Von ihr kommen die Health Probes des Load Balancers.

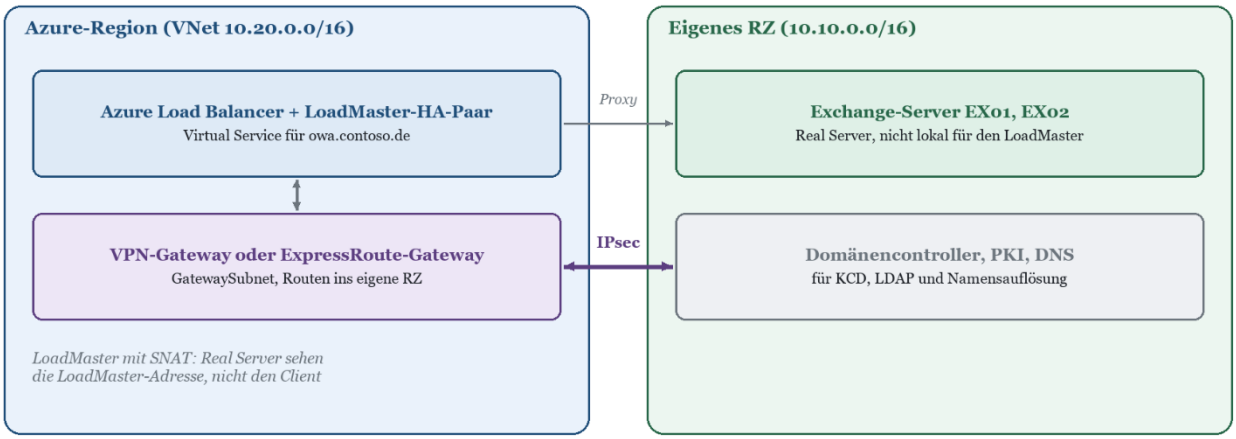
Hängt eine NSG am Subnetz und eine an der Netzwerkkarte, müssen beide den Verkehr erlauben.

Hybrid: LoadMaster in Azure, Real Server im eigenen Rechenzentrum

Das Szenario ist häufiger, als die Architekturfolien vermuten lassen. Die Firma möchte keine öffentlichen Adressen mehr im eigenen Rechenzentrum betreiben, der Internetanschluss im Keller ist zu dünn, oder das Rechenzentrum soll mittelfristig verschwinden und der LoadMaster zieht schon einmal vor. Also steht der LoadMaster in Azure, die Exchange-Server, das ADFS oder die Fachanwendung bleiben im eigenen Haus, und dazwischen liegt ein Site-to-Site-VPN oder ExpressRoute.

Hybrid: LoadMaster in Azure, Real Server im eigenen Rechenzentrum

Der Datenpfad läuft zweimal über die Leitung. Jede Millisekunde Latenz zahlst du doppelt



Wo es knallt

- Tunnel weg: alle Real Server rot, der LoadMaster lebt, der Dienst ist trotzdem tot.
- MTU im Tunnel kleiner als gedacht: TLS-Handshake hängt, kleine Pakete gehen durch. Klassiker.
- Transparenz geht über Routinggrenzen nicht. Client-IP nur per X-Forwarded-For.
- Kerberos und KCD brauchen DCs, die vom LoadMaster aus zuverlässig erreichbar sind.

Skizze: Beispieladressen und -namen frei gewählt (contoso.de)

Nicht lokale Real Server und das Ende der Transparenz

Der LoadMaster erwartet standardmäßig, dass Real Server in einem direkt angeschlossenen Subnetz liegen. Für Server hinter einem Router, also auch hinter dem Azure-VPN-Gateway, aktivierst du global die Option Enable Non-Local Real Servers, zu finden unter System Configuration > Miscellaneous Options > Network Options. Danach erlaubt der Real Server die Option Allow Remote Addresses. Der LoadMaster erreicht die nicht lokalen Server über sein Standard-Gateway, und das gilt auch für die Health Checks. Das Standard-Gateway im Subnetz ist in Azure die Plattform selbst, die Routen ins eigene Rechenzentrum lernt sie vom VPN- oder ExpressRoute-Gateway.

Die Kehrseite: Transparenz geht mit nicht lokalen Real Servern nicht, der Virtual Service muss sie abgeschaltet haben. Die Real Server sehen als Quelle also die Adresse des LoadMasters, nicht die des Clients. Für IIS-Logs, ADFS-Extranet-Sperren oder Exchange-Protokolle brauchst du deshalb X-Forwarded-For, wie in Client-IP sichtbar machen: Transparenz, SNAT und X-Forwarded-For beschrieben. Für SMTP gibt es keinen solchen Header. Wenn Exchange-Empfangsconnectors anhand der Absender-IP entscheiden, ob ein System relayen darf, sehen sie plötzlich nur noch den LoadMaster. Wie du das löst, ohne ein offenes Relay zu bauen, steht in SMTP über den LoadMaster: Relay, Empfangsconnectors und die echte Absender-IP.

WICHTIG · Transparenz in Azure ist sowieso ein Sonderfall

Selbst wenn die Real Server in Azure im selben VNet liegen: Transparenz setzt voraus, dass die Antwort des Real Servers wieder beim LoadMaster landet. Dafür müsste der LoadMaster das Gateway der Real Server sein, und dafür bräuchtest du benutzerdefinierte Routen und IP-Weiterleitung an der Netzwerkkarte. Das geht, ist aber selten die Mühe wert. In Azure ist SNAT mit X-Forwarded-For der Normalfall, nicht die Notlösung.

Latenz, MTU und der abgerissene Tunnel

Jeder Request läuft vom Client nach Azure, von dort durch den Tunnel ins eigene Rechenzentrum, und die Antwort denselben Weg zurück. Bei HTTP mit vielen kleinen Anfragen, wie sie SharePoint-Seiten oder Outlook im Web erzeugen, summiert sich die Latenz spürbar. Miss sie, bevor du dich festlegst, und zwar nicht mit Ping, sondern mit einem echten Seitenaufruf.

Das zweite Thema ist die MTU. IPsec kostet Platz im Paket, und Microsoft empfiehlt für das Azure-VPN-Gateway ein TCP-MSS-Clamping auf 1350 Byte am lokalen VPN-Gerät. Fehlt das und ist Path MTU Discovery irgendwo blockiert, passiert das Gemeinste, was ein Netz tun kann: Kleine Pakete gehen durch, große nicht. Health Checks bleiben grün, der TLS-Handshake mit einer langen Zertifikatskette hängt, und SharePoint lädt die Startseite halb. Wer so etwas einmal nachts um zwei gesucht hat, prüft MSS-Werte danach freiwillig.

Das dritte Thema ist die Abhängigkeit selbst. Fällt der Tunnel aus, werden alle Real Server rot, der Virtual Service ist tot, und der LoadMaster kann daran nichts ändern. Das HA-Paar in Azure schützt dich vor dem Ausfall einer VM, nicht vor dem Ausfall der Leitung. Wer die Leitung absichern will, braucht einen zweiten Tunnel im Aktiv-aktiv-Modus, ExpressRoute mit VPN als Rückfallebene oder einen zweiten Weg über Kemp 360 Central und Global Server Load Balancing für mehrere Standorte.

> **TIPP · Health Checks über die Leitung**
>
> Health Checks über den Tunnel sind gleichzeitig ein Leitungsmonitor. Prüf Exchange nicht nur auf TCP 443, sondern auf die healthcheck.htm des jeweiligen virtuellen Verzeichnisses. Und setz Prüfintervall und Timeout so, dass ein kurzer Tunnel-Neuaufbau nicht sofort alle Server aus dem Pool wirft. Mehr dazu in Health Checks, die wirklich prüfen: warum „Port 443 offen“ nicht reicht.

Kerberos, KCD und Entra ID aus der Cloud

Nutzt du das Edge Security Pack mit Vorauthentifizierung und Kerberos Constrained Delegation, muss der LoadMaster in Azure die Domänencontroller erreichen, und zwar zuverlässig und schnell. Stehen die DCs nur im eigenen Rechenzentrum, hängt jede Anmeldung am Tunnel. Ein DC als VM in Azure, im selben VNet oder einem gepeerten, entschärft das erheblich. Für die Einrichtung selbst gilt alles aus Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten, mit einem Zusatz: Name, Zeit und DNS müssen auch aus Azure heraus stimmen. Zeigt der LoadMaster auf den Azure-eigenen DNS-Resolver statt auf deine DCs, findet er keine SRV-Einträge, und KCD scheitert mit Fehlermeldungen, die nichts mit DNS zu tun zu haben scheinen.

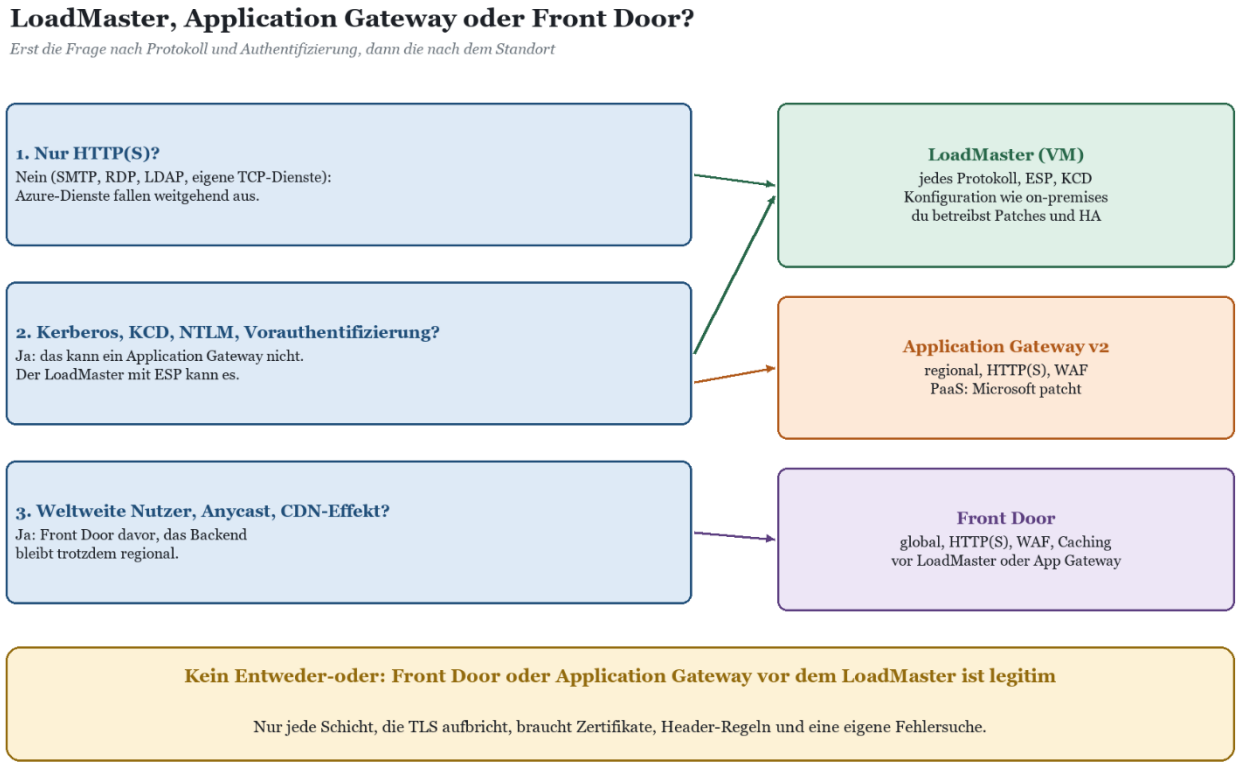
Geht die Reise Richtung Entra ID, wird es eleganter. Der LoadMaster kann als SAML-Dienstanbieter gegenüber Entra ID auftreten und danach per KCD an klassische Anwendungen weiterreichen. Damit bekommst du Bedingten Zugriff und MFA vor einer Anwendung, die nie etwas von Entra ID gehört hat. Wie das zusammenspielt, beschreibt SAML, OIDC und Entra ID: der LoadMaster als moderner Identitätsvermittler.

Symptom	wahrscheinliche Ursache	wo du nachschaust
alle Real Server rot, LoadMaster gesund	Tunnel unten oder Route fehlt	Verbindungsstatus des VPN-Gateways, effektive Routen der LoadMaster-NIC
Health Check grün, Seite lädt halb	MTU oder MSS im Tunnel	MSS-Clamping am lokalen VPN-Gerät
Real Server sehen nur LoadMaster-IP	kein Transparenzbetrieb möglich	X-Forwarded-For im Virtual Service und im IIS-Logging
KCD schlägt sporadisch	DC nur über Tunnel, DNS	DNS-Server am LoadMaster, DC-

fehl	falsch	Erreichbarkeit aus Azure
SMTP-Relay plötzlich verweigert	Empfangsconnector sieht LoadMaster-IP	Remote-IP-Bereiche der Empfangsconnectors
Sitzungen brechen nach Minuten ab	Leerlauf-Zeitlimit des Azure Load Balancers	Idle Timeout der Lastverteilungsregel, Timeouts im Virtual Service

Abgrenzung: Azure Application Gateway und Azure Front Door

Spätestens wenn jemand aus dem Cloud-Team fragt, warum du eine VM mit Firmware betreibst, wenn Azure doch eigene Load Balancer hat, brauchst du eine gute Antwort. Die ehrliche lautet: Es kommt auf die Anwendung an. Microsoft selbst empfiehlt in seinem Architekturleitfaden, jeden Dienst einzeln zu bewerten, und betont, dass gute Lösungen oft mehrere Lastverteilungsdienste kombinieren. Die ausführliche Gegenüberstellung mit Entra Application Proxy und klassischen Reverse Proxys steht in Entscheidungshilfe: LoadMaster, Entra Application Proxy, Azure Application Gateway oder Reverse Proxy?. Hier geht es um die Azure-Sicht.



Skizze: Orientierung, keine vollständige Produktmatrix; Funktionsumfang der Azure-Dienste ändert sich laufend

Application Gateway: regional, HTTP, PaaS

Azure Application Gateway ist ein regionaler Layer-7-Load-Balancer für HTTP und HTTPS mit optionaler Web Application Firewall. Er terminiert TLS, routet nach Pfad und Hostname, schreibt Header um und kann Backends auch im eigenen Rechenzentrum über VPN erreichen. Microsoft patcht und skaliert ihn, du musst dich um keine Firmware kümmern. Das ist ein echter Vorteil. Die Grenze liegt bei der Authentifizierung: Kerberos Constrained Delegation, NTLM-Weiterreichung oder eine formularbasierte Vorauthentifizierung gegen das Active Directory kann ein Application Gateway nicht. Für eine reine Eigenentwicklung mit moderner Anmeldung ist er oft die bessere Wahl. Für ein Exchange mit Vorauthentifizierung oder ein SharePoint mit KCD nicht.

WICHTIG · Application Gateway v1 ist Geschichte

Microsoft hat die erste Generation von Application Gateway und dessen WAF zum 28. April 2026

eingestellt. Wer noch einen v1-Gateway-Vergleich im Kopf hat, sollte ihn vergessen. Die Vergleiche in diesem Beitrag beziehen sich auf v2.

Front Door: global, Anycast, Edge

Azure Front Door ist ein globaler Dienst am Rand des Microsoft-Netzes: Anycast, TLS-Terminierung nahe am Nutzer, Caching, WAF und Verteilung über mehrere Regionen. Für ein mittelständisches Unternehmen mit Nutzern in Deutschland und einem Rechenzentrum in Hessen ist der globale Teil selten der Grund. Interessant wird Front Door als vorgelagerte Schutzschicht mit WAF und DDoS-Abwehr vor einem öffentlich erreichbaren Endpunkt, und das kann durchaus ein LoadMaster sein. Auch hier gilt: nur HTTP(S), keine AD-Authentifizierung. Die klassische Variante von Front Door endet am 31. März 2027. Neue Projekte setzen auf Standard oder Premium.

Kriterium	LoadMaster in Azure	Application Gateway v2	Front Door
Reichweite	regional, wo die VM steht	regional	global
Protokolle	TCP, UDP, HTTP(S), SMTP u. a.	Schwerpunkt HTTP(S)	HTTP(S)
Vorauthentifizierung AD	ja, mit Edge Security Pack	nein	nein
Kerberos Constrained Delegation	ja	nein	nein
SAML gegenüber Entra ID	ja	nein, dafür Entra-Integration der App	nein
WAF	ja, je nach Lizenz	ja, WAF-SKU	ja, WAF-Richtlinie
Betrieb und Patches	du	Microsoft	Microsoft
HA	Paar hinter Azure Load Balancer	integriert, zonenredundant möglich	integriert
Know-how-Transfer	Konfiguration wie on-premises	Azure-spezifisch	Azure-spezifisch

AUS DER PRAXIS · Drei Schichten, ein Zertifikat zu viel

Ein Unternehmen setzte Front Door vor ein Application Gateway vor einen LoadMaster vor SharePoint. Jede Schicht brach TLS auf, jede hatte eigene Timeouts, Header-Regeln und Zertifikate, und jede erzeugte eigene Protokolle. Als Uploads über 100 MB scheiterten, brauchte das Team zwei Tage, um herauszufinden, welche Schicht schuld war. Die Antwort war: alle drei, mit unterschiedlichen Grenzwerten. Weniger Schichten sind nicht weniger Sicherheit, sondern weniger Stellen für Missverständnisse.

Wenn du die Entscheidung nicht allein treffen willst oder ein bestehender Aufbau nach Azure umziehen soll, unterstützen wir dich mit der Beratung zum Kemp LoadMaster. Wer die Mechanik lieber selbst im Labor begreift, findet in der Kemp-LoadMaster-Schulung einen Azure-Teil mit HA-Paar und NSG-Fehlerbildern zum Nachbauen.

FAQ: LoadMaster in Azure

Kann ich das HA-Paar in Azure ohne Azure Load Balancer betreiben?

Nicht sinnvoll. Ohne Gratuitous ARP gibt es keinen Mechanismus, der eine gemeinsame Adresse zum aktiven Knoten bringt. Der Azure Load Balancer ist im Herstellerleitfaden fester Bestandteil der Lösung.

Brauche ich einen öffentlichen oder einen internen Azure Load Balancer?

Das hängt davon ab, woher die Clients kommen. Für Dienste aus dem Internet nimmst du eine öffentliche Frontend-IP, für Clients im eigenen Netz über VPN eine interne. Beides gleichzeitig ist mit zwei Load Balancern oder mehreren Frontends möglich.

Warum sind beide LoadMaster im Azure-Portal als fehlerhaft markiert?

Fast immer blockiert eine NSG, eine Firewall oder eine eigene Deny-Regel die Probe von 168.63.129.16, oder Probe-Port und Health Check Port stimmen nicht überein. Dass der Standby-Knoten rot ist, ist dagegen gewollt.

Funktioniert Transparenz in Azure?

Für Real Server über VPN oder ExpressRoute nicht, weil Transparenz mit nicht lokalen Real Servern nicht kombinierbar ist. Im selben Subnetz wäre es nur mit Routing-Umbau möglich. In der Praxis nutzt du SNAT und X-Forwarded-For.

Darf der LoadMaster in Azure Exchange im eigenen Rechenzentrum veröffentlichen?

Ja, technisch ohne Weiteres. Prüf aber Latenz, MTU im Tunnel und die Abhängigkeit von der Leitung. Und denk an SMTP: Empfangsconnectors sehen nur noch die Adresse des LoadMasters.

Ersetzt ein Application Gateway den LoadMaster?

Für reine HTTP(S)-Anwendungen mit moderner Authentifizierung oft ja. Für alles mit Kerberos, KCD, NTLM, SMTP oder RDP-Lastverteilung nein.

Wie lange dauert ein Failover in Azure?

Die Erkennung durch den LoadMaster plus die Zeit, die der Azure Load Balancer braucht, bis Proben am alten Knoten fehlschlagen und am neuen grün werden. Mit einem Intervall von fünf Sekunden liegt das typischerweise im Bereich weniger zehn Sekunden. Miss es im Test, statt es zu schätzen.

Fazit: derselbe LoadMaster, ein anderes Netz

Ein LoadMaster in Azure ist kein exotisches Projekt. Die Firmware ist dieselbe, die Virtual Services sind dieselben, das Wissen aus dem eigenen Rechenzentrum lässt sich fast vollständig mitnehmen. Was du neu lernen musst, ist das Netz: dass HA über den Azure Load Balancer und seine Probe läuft, dass NSGs an jeder Netzwerkkarte kleben und die Probe freilassen müssen, dass ausgehender Verkehr in neuen VNets nicht mehr selbstverständlich ist und dass im Hybridbetrieb die Leitung zum eigenen Rechenzentrum der eigentliche Single Point of Failure ist.

Application Gateway und Front Door sind keine Konkurrenz, sondern Werkzeuge für andere Aufgaben. Sie glänzen bei reinem HTTP(S) und wenn du keine Appliance betreiben willst. Der LoadMaster glänzt überall dort, wo Microsoft-Anwendungen noch Active Directory sprechen, Kerberos erwarten oder Protokolle nutzen, die nicht mit „http“ beginnen. Und das ist im Mittelstand und in Verwaltungen noch eine ganze Weile ziemlich viel. Die Cloud verändert eben nicht die Anwendungen, nur den Ort, an dem sie scheitern.

WEITERLESEN · Weiter im Thema

› Entscheidungshilfe: LoadMaster, Entra Application Proxy, Azure Application Gateway oder Reverse Proxy?
› SAML, OIDC und Entra ID: der LoadMaster als moderner Identitätsvermittler
› HA-Paar, Failover und Konfig-Sync: zwei LoadMaster, ein Gedanke
› Client-IP sichtbar machen: Transparenz, SNAT und X-Forwarded-For
› Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten
› Kemp 360 Central und Global Server Load Balancing für mehrere Standorte