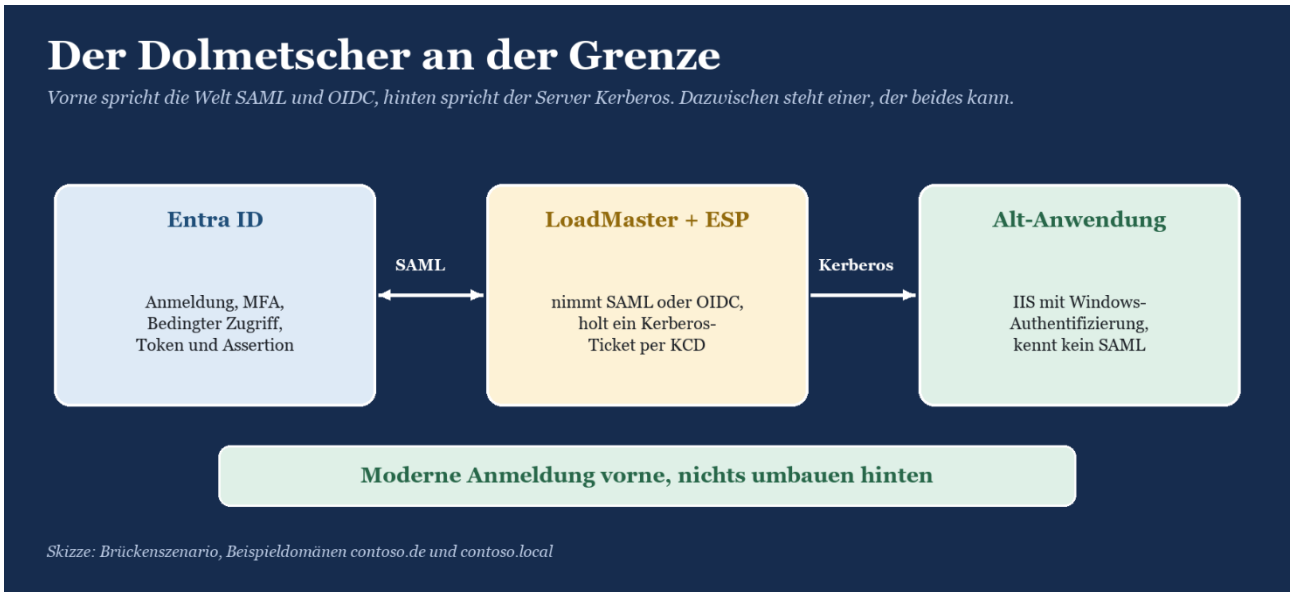
SAML, OIDC und Entra ID: der LoadMaster als moderner Identitätsvermittler



WISSEN

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

› **Kemp LoadMaster**

BERATUNG

Deine Alt-Anwendung soll hinter Entra ID und Bedingten Zugriff, ohne dass jemand ihren Code anfasst? Wir planen die Brücke mit dir.

› **Beratung zum Kemp LoadMaster**

SCHULUNG

SAML-Metadaten, KCD-Konto und Claim-Zuordnung im Labor durchspielen, bevor die Fehlerseite in Produktion auftaucht.

› **Kemp-LoadMaster-Schulung**

Jedes Unternehmen hat sie: die eine Anwendung, die 2009 jemand im Haus geschrieben hat, die auf einem IIS mit integrierter Windows-Authentifizierung läuft und die seitdem niemand mehr anfassen will. Sie funktioniert. Sie kennt Kerberos und zur Not NTLM. Von SAML, OpenID Connect oder Entra ID hat sie nie gehört, und der Entwickler ist inzwischen in Rente, im Ausland oder beides. Gleichzeitig will die Sicherheitsabteilung, dass jeder Zugriff von außen über Entra ID läuft, mit MFA, mit Bedingtem Zugriff und mit einem Anmeldeprotokoll, das man im Ernstfall auswerten kann. Zwei Welten, die sich nichts zu sagen haben.

Genau hier wird der LoadMaster zum Dolmetscher. Mit dem Edge Security Pack nimmt er auf der Client-Seite eine moderne Anmeldung per SAML oder OIDC gegen Entra ID oder ADFS entgegen und spricht auf der Server-Seite per Kerberos Constrained Delegation mit der alten Anwendung. Die Anwendung bekommt ein ganz normales Kerberos-Ticket und merkt nicht einmal, dass vorne die Cloud mitgeredet hat. Das Stichwort für Suchmaschinen lautet kemp saml entra id, das Stichwort für dein Projekt lautet Brückenszenario.

In diesem Beitrag geht es nicht darum, die Herstellerdokumentation Klick für Klick nachzuerzählen. Es geht darum, warum das Szenario so gebaut ist, wo die Nahtstellen zwischen Entra-Welt und Kerberos-Welt liegen und wo es in der Praxis knallt: bei der Identitätszuordnung, bei Zertifikaten und Geheimnissen mit Ablaufdatum, bei Clients, die keinen Browser haben, und bei Sitzungen, die länger leben als der Bedingte Zugriff denkt. Dazu kommt die Abgrenzung zu den

Microsoft-eigenen Wegen, also Entra Application Proxy und Entra Private Access. Die Einordnung aller LoadMaster-Themen mit Microsoft-Bezug findest du auf der Seite Kemp LoadMaster.

FAKTEN · Das Szenario in einem Satz

Client-Seite: Der Browser meldet sich per SAML 2.0 oder OpenID Connect an Entra ID oder ADFS an, Entra ID erledigt MFA und Bedingten Zugriff.

Mitte: Der LoadMaster prüft Signatur und Gültigkeit der Assertion oder des Tokens und hält eine eigene ESP-Sitzung per Cookie.

Server-Seite: Der LoadMaster holt sich per Protokollübergang (S4U2Self) und eingeschränkter Delegation (S4U2Proxy) ein Kerberos-Ticket im Namen des Benutzers und reicht es an die Anwendung weiter.

Voraussetzung: Jeder Benutzer hat ein lokales AD-Konto, das sich eindeutig aus der Cloud-Identität ableiten lässt.

Warum überhaupt eine Brücke? Zwei Anmeldewelten, die sich nicht verstehen

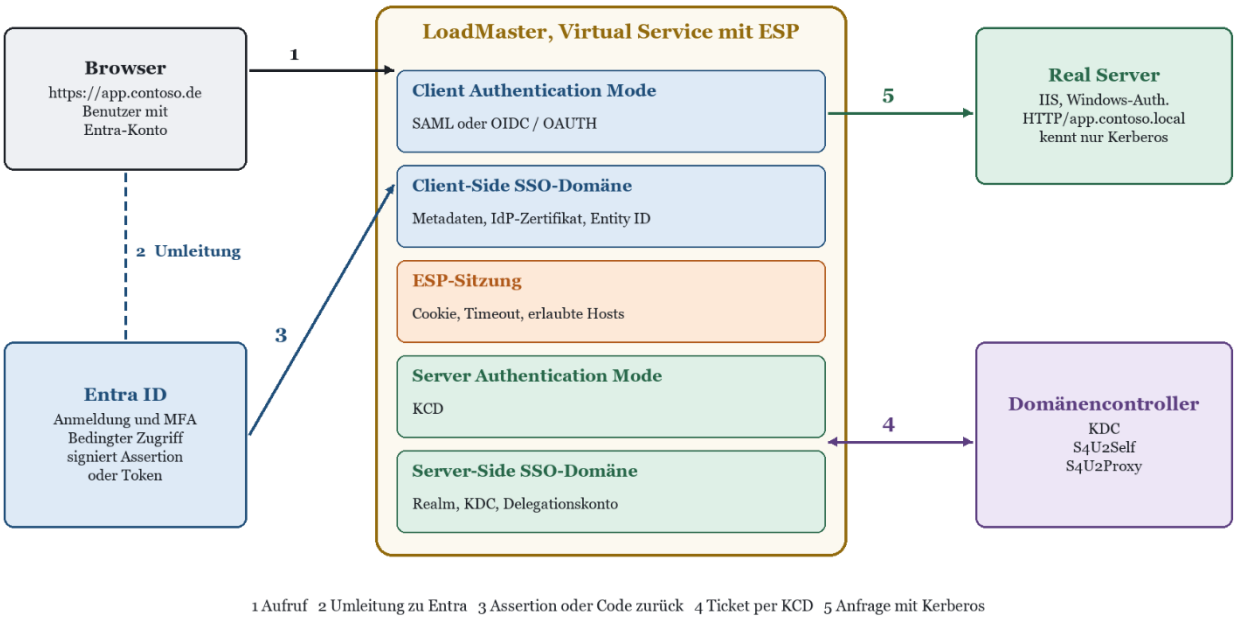
Kerberos ist ein wunderbares Protokoll, solange alle Beteiligten einen Domänencontroller sehen. Der Client holt sich ein Ticket beim KDC, legt es dem Server vor, fertig. Aus dem Internet funktioniert das nicht: Der KDC ist von außen nicht erreichbar, und das ist auch gut so. Wer einen Domänencontroller ins Internet stellt, um Kerberos von außen zu ermöglichen, braucht keinen Load Balancer mehr, sondern einen guten Anwalt.

SAML und OIDC lösen das Problem anders. Hier gibt es einen Identitätsanbieter, der über HTTPS erreichbar ist, und eine Anwendung, die dem Identitätsanbieter vertraut. Der Browser pendelt per Umleitung zwischen beiden hin und her und transportiert eine signierte Aussage über den Benutzer. Kein Kennwort landet bei der Anwendung, und der Identitätsanbieter kann vor der Ausstellung alles prüfen, was ihm wichtig ist: zweiten Faktor, Gerätezustand, Standort, Risiko. Das ist der Grund, warum Microsoft MFA und Bedingten Zugriff an Entra ID hängt und nicht an einzelne Anwendungen.

Die Alt-Anwendung kann mit einer SAML-Assertion aber nichts anfangen. Sie erwartet im Header Authorization: Negotiate ein Kerberos-Ticket, ausgestellt für ihren Dienstprinzipalnamen. Irgendjemand muss also übersetzen. Diese Rolle hat früher das TMG oder UAG gespielt, später der Web Application Proxy von ADFS für nicht anspruchsbasierte Anwendungen, und heute kommen dafür Entra Application Proxy, Entra Private Access oder eben der LoadMaster mit dem Edge Security Pack: Vorauthentifizierung, SSO-Domänen und der TMG-Ersatz infrage.

Das Brückenszenario im Überblick

Client-Seite mit SAML oder OIDC gegen Entra ID, Server-Seite mit KCD gegen das lokale AD



1 Aufruf 2 Umleitung zu Entra 3 Assertion oder Code zurück 4 Ticket per KCD 5 Anfrage mit Kerberos

Skizze: vereinfachter Ablauf, Optionsnamen sinngemäß nach LoadMaster-WUI

Was der LoadMaster dabei eigentlich ist

Aus Sicht von Entra ID ist der LoadMaster eine ganz gewöhnliche Unternehmensanwendung. Bei SAML ist er der Service Provider mit einer Entity ID und einer Antwortadresse, bei OIDC ein registrierter Client mit Umleitungs-URI und geheimem Schlüssel. Progress beschreibt die Rolle bei OIDC als Resource Server, der Zugriff anhand der vom Identitätsanbieter ausgestellten Token gewährt oder verweigert. Der LoadMaster sieht also nie ein Kennwort des Benutzers. Er sieht nur, was Entra ID ihm über den Benutzer erzählt, und glaubt es, weil die Signatur stimmt.

Aus Sicht des Active Directory ist der LoadMaster dagegen ein Dienstkonto mit Delegationsrecht. Er darf sich für beliebige Benutzer Tickets für ausgewählte Dienste besorgen, ohne deren Kennwort zu kennen. Das ist mächtig, und genau deshalb gehört das Delegationskonto behandelt wie ein Schlüssel zum Generalschlüsselkasten. Wie du KCD und die ressourcenbasierte Variante RBCD sauber aufsetzt, steht ausführlich im Beitrag Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten.

WICHTIG · Das Vertrauen wandert

Im Brückenszenario vertraut die Anwendung nicht mehr dem Benutzer, sondern dem LoadMaster. Wer den LoadMaster oder das Delegationskonto kompromittiert, kann sich als jeder beliebige Benutzer bei den freigegebenen Diensten ausgeben. Beschränke die Delegation deshalb strikt auf die SPNs der veröffentlichten Anwendungen, nie auf ganze Server mit allen Diensten, und nimm privilegierte Konten per „Konto ist vertraulich und kann nicht delegiert werden“ oder Mitgliedschaft in Protected Users aus dem Spiel.

SAML oder OIDC: was du vorne wählst

Beide Protokolle erledigen am LoadMaster dieselbe Aufgabe. Die Unterschiede liegen im Detail, und die Details entscheiden darüber, wie viel Pflegeaufwand du dir einhandelst. SAML ist das ältere, XML-basierte Protokoll und in Verwaltungen und ADFS-Landschaften seit Jahren etabliert.

OIDC baut auf OAuth 2.0 auf, arbeitet mit JSON-Token und ist der Standard, den Microsoft bei neuen Entwicklungen bevorzugt. Für das Brückenszenario gilt: Nimm, was dein Identitätsanbieter sauber kann und was dein Team im Fehlerfall lesen kann.

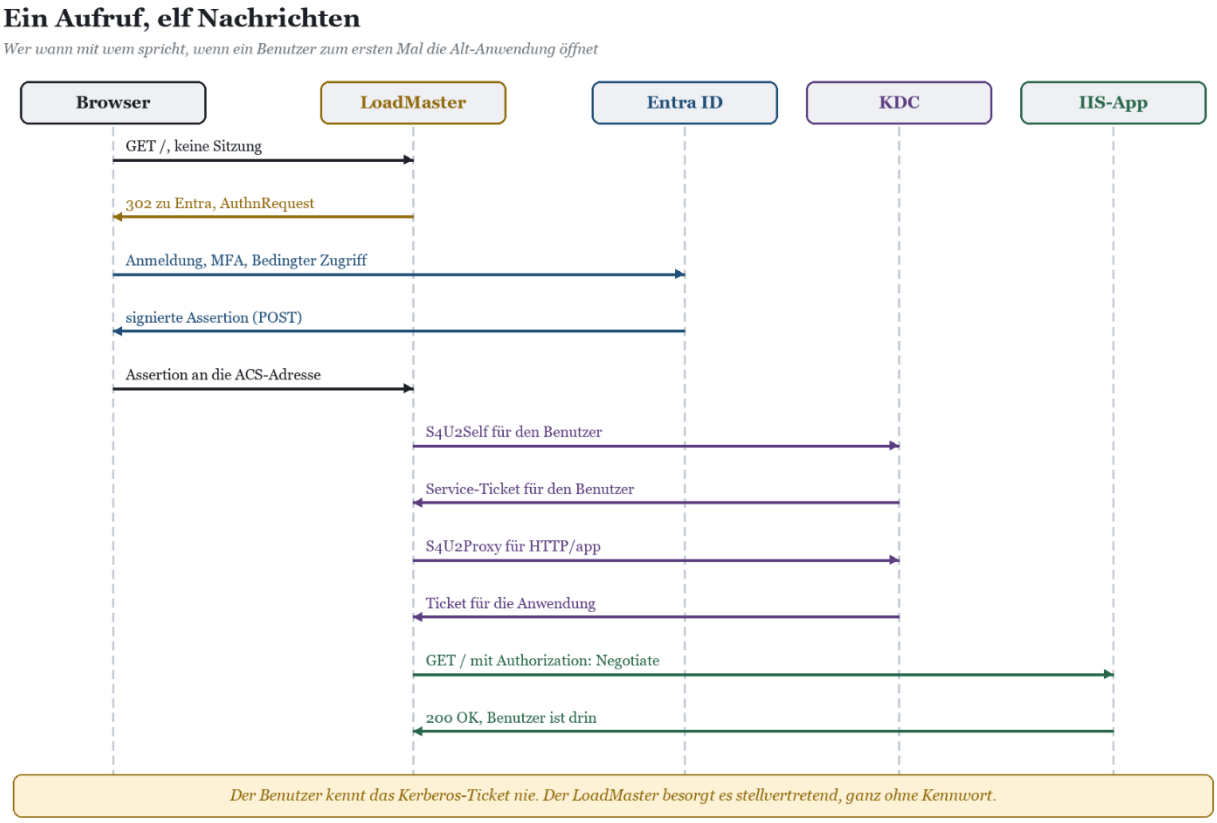
Aspekt	SAML 2.0	OpenID Connect
Format	signierte XML-Assertion, per Browser-POST	JSON Web Token, Austausch per Code
Rolle des LoadMasters	Service Provider mit Entity ID und Antwortadresse	registrierter Client mit Umleitungs-URI
Vertrauensanker	Signaturzertifikat des IdP, auf dem LoadMaster importiert	Client-ID und geheimer Schlüssel, Signaturschlüssel des IdP
Was abläuft	Signaturzertifikat in Entra ID, Standard drei Jahre	Geheimer Schlüssel der App-Registrierung, maximal 24 Monate
Konfiguration in Entra ID	Unternehmensanwendung mit SAML-SSO	App-Registrierung mit Web-Plattform
Gegen ADFS	klassische Vertrauensstellung der vertrauenden Seite	Anwendungsgruppe mit Server-Anwendung
Fehlersuche	Assertion im Browser-Trace lesbar, aber geschwätzig	Token kompakt, Code-Austausch läuft serverseitig

TIPP · Die Galerie-App ist nicht Pflicht

In der Entra-Anwendungsgalerie gibt es einen Eintrag für die Kemp-LoadMaster-Integration, und Microsoft Learn beschreibt die Einrichtung per SAML inklusive KCD. Das Tutorial nennt dabei ausdrücklich nur die vom Identitätsanbieter initiierte Anmeldung. Wenn du die vom Service Provider initiierte Anmeldung brauchst, also Benutzer die Adresse direkt aufrufen, teste das früh oder lege eine eigene Unternehmensanwendung außerhalb der Galerie an. Entscheidend sind Entity ID und Antwortadresse, nicht das Logo.

Der Ablauf im Detail: von der Umleitung bis zum Kerberos-Ticket

Der erste Aufruf eines Benutzers ist der lehrreichste, weil dabei alle Beteiligten einmal reden müssen. Später übernimmt das ESP-Sitzungscookie, und der LoadMaster erledigt die Kerberos-Seite pro Verbindung im Hintergrund.



Skizze: SAML-Variante, bei OIDC ersetzen Code und Token die Assertion

- **Aufruf ohne Sitzung:** Der Browser ruft https://app.contoso.de auf. Der Virtual Service mit aktiviertem ESP findet kein gültiges Sitzungscookie und leitet zum Identitätsanbieter um.
- **Anmeldung an Entra ID:** Hier passiert alles, was du in Entra ID konfiguriert hast: Kennwort oder kennwortlose Anmeldung, MFA, Richtlinien für Bedingten Zugriff, Prüfung der Benutzerzuweisung zur Unternehmensanwendung.
- **Rückkehr zum LoadMaster:** Bei SAML postet der Browser die signierte Assertion an die Antwortadresse, bei OIDC kommt ein Autorisierungscode, den der LoadMaster gegen Token eintauscht. Der LoadMaster prüft Signatur, Zielgruppe und Gültigkeitszeitraum.
- **Protokollübergang:** Mit dem Delegationskonto fordert der LoadMaster per S4U2Self ein Ticket für den Benutzer an sich selbst an. Dafür braucht er nur den Benutzernamen, kein Kennwort.
- **Eingeschränkte Delegation:** Per S4U2Proxy tauscht er dieses Ticket gegen eines für den SPN der Anwendung, etwa HTTP/app.contoso.local.
- **Weitergabe:** Die Anfrage geht mit Kerberos-Ticket an den Real Server. Für IIS sieht das aus wie eine ganz normale Windows-Anmeldung aus dem Intranet.

Protokollübergang: der Teil, den alle vergessen

Klassische KCD setzt voraus, dass der Benutzer sich beim Frontend bereits per Kerberos angemeldet hat. Im Brückenszenario ist das nie der Fall: Der Benutzer hat sich per SAML oder OIDC angemeldet, ein Kerberos-Ticket existiert nicht. Deshalb braucht die klassische Variante die Einstellung „Beliebiges Authentifizierungsprotokoll verwenden“ am Delegationskonto. Ohne sie bekommt der LoadMaster beim S4U2Self zwar ein Ticket, aber eines, das sich nicht weiterreichen lässt, und S4U2Proxy scheitert. Das Fehlerbild ist zuverlässig verwirrend: Entra-Anmeldung klappt, dann Fehlerseite vom LoadMaster.

Bei ressourcenbasierter Delegation, also RBCD, entscheidet das Zielkonto, wem es vertraut. Dort akzeptiert der KDC auch das nicht weiterreichbare Ticket aus S4U2Self als Nachweis, solange die

Berechtigung am Zielkonto gesetzt ist. Das macht RBCD für dieses Szenario oft eleganter, verlangt aber, dass du die Berechtigung am Dienstkonto oder Computerkonto der Anwendung pflegst. Welche Variante wann passt und wie der SPN hinter einem Namen mit mehreren Servern aussehen muss, erklären die Beiträge Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten und SPN-Probleme hinter dem Load Balancer: ein Name, mehrere Server. Die Grundlagen zu Tickets, SPNs und Verschlüsselungstypen findest du auf der Seite Microsoft Kerberos.

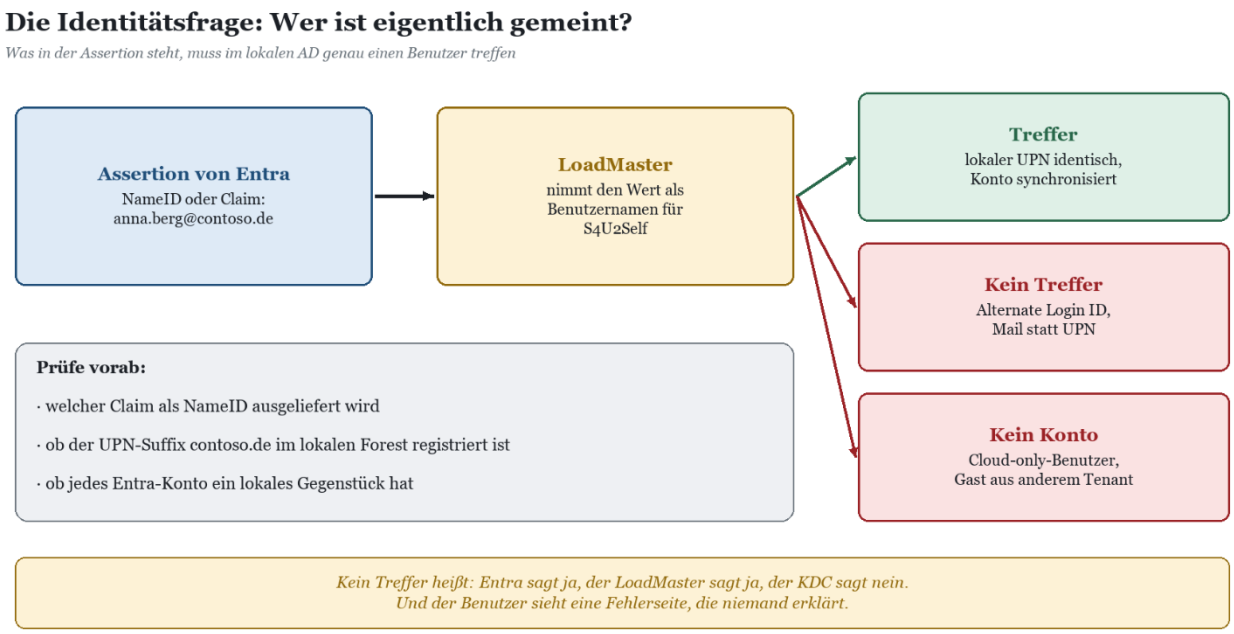
WARNUNG · AES oder gar nicht

Wer die Domäne auf AES gehärtet hat, muss auch das Delegationskonto und die Keytab des LoadMasters mitnehmen. Ein Delegationskonto ohne AES-Schlüssel oder mit veralteter Keytab führt nach der Härtung zu Ausfällen, die exakt so aussehen wie ein Konfigurationsfehler im ESP. Die Details stehen im Beitrag Die RC4-Falle: KCD-Keytab trifft AES-only-Domäne.

Die Identitätsfrage: Wer ist anna.berg@contoso.de im lokalen AD?

Der LoadMaster muss aus dem, was Entra ID ihm liefert, einen Benutzernamen für S4U2Self machen. Das ist der Punkt, an dem die meisten Projekte zum ersten Mal ins Schwitzen kommen. Entra ID schickt standardmäßig den Benutzerprinzipalnamen als NameID. Wenn der lokale UPN identisch ist und der Suffix contoso.de als UPN-Suffix im Forest registriert ist, findet der KDC den Benutzer, und alles ist gut.

Weniger gut wird es, wenn in der Synchronisation mit Entra Connect oder Cloud Sync eine alternative Anmelde-ID verwendet wird, also zum Beispiel die Mailadresse als Entra-UPN, während lokal noch anna.berg@contoso.local steht. Dann sucht der KDC einen Benutzer, den es nicht gibt. Gleiches gilt für reine Cloud-Konten und Gastbenutzer: Ohne lokales Konto gibt es kein Kerberos-Ticket, ganz egal, wie stark die MFA vorne war.



Skizze: Abbildung der Cloud-Identität auf das lokale Konto, Namen fiktiv

Die Lösung liegt meistens in Entra ID und nicht am LoadMaster. In der SAML-Konfiguration der Unternehmensanwendung legst du fest, welcher Wert als Benutzer-ID ausgeliefert wird. Wird dort ein synchronisiertes Attribut wie der lokale UPN oder eine Kombination aus Domänenname und

sAMAccountName ausgeliefert, passt der Wert zum lokalen Konto. Welches Format der LoadMaster für die Delegation erwartet, hängt von der Konfiguration der SSO-Domäne ab. Teste das mit einem Benutzer, dessen Cloud- und Lokal-UPN absichtlich voneinander abweichen, nicht nur mit deinem eigenen Konto, bei dem zufällig alles passt.

AUS DER PRAXIS · Die Fehlerseite um 7:45 Uhr

Ein typisches Projekt: Pilotgruppe aus der IT, alles funktioniert. Am ersten Produktivtag kommen die Kolleginnen und Kollegen aus einer übernommenen Tochterfirma dazu, deren Konten eine andere Mail-Domäne als UPN tragen. Entra-Anmeldung klappt, MFA klappt, dann eine nichtssagende Fehlerseite. Im ESP-Log steht, dass die Delegation für den Benutzer fehlgeschlagen ist. Ursache: Den UPN-Suffix der Tochter gab es lokal nicht. Abhilfe: Claim-Zuordnung in Entra ID angepasst, Pilotgruppe künftig quer durch alle Domänen gemischt.

MFA und Bedingter Zugriff: in Entra ID, nicht am LoadMaster

Der LoadMaster kann über das ESP selbst MFA-Szenarien abbilden, etwa per RADIUS gegen einen NPS mit MFA-Erweiterung oder eine andere OTP-Lösung. Das ist im Beitrag MFA vor OWA, ECP und Co.: Zwei-Faktor am LoadMaster beschrieben und hat seine Berechtigung, wenn kein Entra ID im Spiel ist. Im Brückenszenario wäre es aber Verschwendung: Wenn der Benutzer ohnehin bei Entra ID landet, gehört die gesamte Anmelderichtlinie dorthin. Ein Ort für Richtlinien, ein Anmeldeprotokoll, eine Stelle für Ausnahmen.

Prüfung	Wo sie im Brückenszenario hingehört	Warum
Zweiter Faktor	Entra ID, Richtlinie für Bedingten Zugriff	einheitliche Methoden, kennwortlose Anmeldung, Phishing-resistente Faktoren
Gerätezustand	Entra ID mit Intune-Konformität oder Hybrid-Join	der LoadMaster kennt kein Gerät, nur eine Verbindung
Standort und Risiko	Entra ID, benannte Orte und Risikorichtlinien	Signale aus dem gesamten Tenant, nicht aus einem Virtual Service
Wer darf die App überhaupt	Entra ID, Benutzerzuweisung zur Anwendung	Gruppenpflege an einem Ort, sichtbar in Zugriffsüberprüfungen
Hosts und Pfade	LoadMaster, erlaubte virtuelle Hosts und Verzeichnisse	Entra ID sieht keine URL-Pfade hinter der Anmeldung
Sitzungsdauer am Rand	LoadMaster, ESP-Sitzungs-Timeout	bestimmt, wie oft Entra ID überhaupt gefragt wird
Lastverteilung und Gesundheit	LoadMaster	dafür ist er gekauft worden

FAKTEN · Lizenzfragen kurz eingeordnet

Bedingter Zugriff setzt mindestens Microsoft Entra ID P1 voraus, risikobasierte Richtlinien P2. SSO zu Unternehmensanwendungen per SAML oder OIDC ist dagegen auch ohne Premium-Lizenz möglich. Entra Application Proxy setzt P1 oder P2 voraus, Entra Private Access ist eigenständig lizenziert und Teil der Global-Secure-Access-Familie. Prüfe den aktuellen Stand vor der Planung, Microsoft passt die Pakete regelmäßig an.

Die Sitzungsfalle: Bedingter Zugriff wirkt nur beim Umleiten

Hier wird es schwarzhumorig. Entra ID entscheidet nur dann, wenn der LoadMaster den Benutzer zur Anmeldung schickt. Danach lebt der Benutzer von seinem ESP-Sitzungscookie. Sperrst du das Konto in Entra ID, deaktivierst du es lokal nicht gleich mit oder änderst du eine Richtlinie, merkt der LoadMaster davon nichts, bis die ESP-Sitzung abläuft. Continuous Access Evaluation, mit der Microsoft eigene Dienste nahezu in Echtzeit über Sperrungen informiert, gilt für solche Drittanwendungen nicht.

Immerhin: Wird das lokale Konto deaktiviert, scheitert die Kerberos-Delegation beim nächsten Ticket, und der Benutzer kommt nicht mehr an die Anwendung. Bis dahin können aber bereits ausgestellte Tickets noch gelten. Wähle die Timeouts der ESP-Sitzung deshalb bewusst, typischerweise im Bereich weniger Stunden statt Tage, und beziehe das Sperren lokaler Konten in deinen Offboarding- und Notfallprozess ein.

WARNUNG · Abmelden heißt nicht abgemeldet

Ein Klick auf „Abmelden“ in der Alt-Anwendung beendet bestenfalls deren eigene Sitzung. Die ESP-Sitzung am LoadMaster und die Anmeldesitzung bei Entra ID bleiben davon unberührt, und der nächste Aufruf meldet den Benutzer stillschweigend wieder an. Auf gemeinsam genutzten Rechnern ist das ein echtes Thema. Kläre, ob und wie eine Abmeldung am LoadMaster ausgelöst wird, und dokumentiere für die Benutzer, dass nur das Schließen des Browsers wirklich zuverlässig ist.

ADFS als Identitätsanbieter: geht, aber denk an morgen

Alles in diesem Beitrag funktioniert auch mit ADFS statt Entra ID. Der LoadMaster wird dann als vertrauende Seite eingetragen, MFA erledigt ADFS selbst oder über einen Adapter, und die Benutzer-ID kommt aus einer Ausstellungsregel. Das ist für Umgebungen ohne Cloud-Anbindung oder mit strengen Vorgaben an den Datenstandort eine legitime Wahl. Wie ADFS und der Web Application Proxy selbst hinter dem LoadMaster stehen, beschreibt der Beitrag ADFS und Web Application Proxy mit dem LoadMaster: Farm, Probe, SNI.

Microsoft empfiehlt allerdings seit Jahren, Anwendungen von ADFS nach Entra ID zu migrieren. Wenn du heute ein Brückenszenario neu baust und Entra ID ohnehin im Haus ist, spar dir die Zwischenstation. Der LoadMaster ist gegenüber dem Identitätsanbieter austauschbar: Neue Metadaten, neues Zertifikat, neue SSO-Domäne, und die Server-Seite mit KCD bleibt exakt gleich. Genau das ist der Charme der Brücke.

Wo es in der Praxis knallt

Die Grundeinrichtung ist an einem Nachmittag erledigt. Die Überraschungen kommen danach, verlässlich und meistens zu ungünstigen Zeiten.

Dinge mit Ablaufdatum

Das SAML-Signaturzertifikat einer Unternehmensanwendung in Entra ID ist standardmäßig drei Jahre gültig. Drei Jahre sind genau lang genug, damit niemand mehr weiß, dass das Zertifikat auch auf dem LoadMaster importiert wurde. Entra ID verschickt vor dem Ablauf Benachrichtigungen an die hinterlegten Adressen, sofern dort jemand eingetragen ist, der noch im Haus arbeitet. Bei OIDC ist es der geheime Schlüssel der App-Registrierung, den das Portal mit höchstens 24 Monaten Laufzeit anlegt.

Der saubere Wechsel läuft in zwei Schritten: neues Zertifikat in Entra ID anlegen, aber noch nicht aktivieren, das neue Zertifikat beziehungsweise die neuen Metadaten auf dem LoadMaster hinterlegen, dann in Entra ID umschalten und testen. Bei einem HA-Paar synchronisiert der LoadMaster die Konfiguration, prüfe aber nach dem Wechsel beide Knoten.

TIPP · Ablaufdaten ins Monitoring

Trag das Ablaufdatum des Signaturzertifikats und des geheimen Schlüssels in dasselbe System ein, mit dem du TLS-Zertifikate überwachst. Als Benachrichtigungsadresse in Entra ID gehört ein Funktionspostfach des Teams hinein, nicht die Adresse der Person, die das Projekt damals umgesetzt hat.

Uhrzeit, Zielgruppe und Antwortadresse

SAML-Assertions haben einen engen Gültigkeitszeitraum, Kerberos toleriert standardmäßig fünf Minuten Zeitabweichung. Ein LoadMaster ohne funktionierende NTP-Konfiguration ist deshalb gleich doppelt im Nachteil. Die zweite Klassikerin ist die Entity ID: Sie muss auf beiden Seiten zeichengenau übereinstimmen, inklusive abschließendem Schrägstrich. Und die Antwortadresse muss der Adresse entsprechen, unter der der Browser den Virtual Service erreicht, nicht der internen.

Symptom	Wahrscheinliche Ursache	Wo du suchst
Entra meldet, die Antwortadresse passe nicht	Antwortadresse in Entra ID weicht von der öffentlichen URL ab	Entra-Anmeldeprotokoll, Fehlercode in der Fehlerseite
Endlosschleife zwischen LoadMaster und Entra	Sitzungscookie wird nicht gesetzt oder nicht zurückgeschickt, oft Host-Mismatch	Browser-Entwicklertools, ESP-Log
Anmeldung klappt, danach Fehlerseite vom LoadMaster	S4U2Self oder S4U2Proxy scheitert: Benutzer unbekannt, Protokollübergang fehlt	ESP-Log, Ereignisprotokoll der Domänencontroller
Anwendung fragt plötzlich nach Kennwort	Ticket für falschen SPN, Anwendung fällt auf NTLM zurück	IIS-Log, Kerberos-Ereignisse auf dem Real Server
Alles war gut, seit heute nichts mehr	Signaturzertifikat oder geheimer Schlüssel abgelaufen	Entra ID, Zertifikatsablauf der Unternehmensanwendung
Einzelne Benutzer scheitern	UPN-Suffix lokal unbekannt, Cloud-only-Konto, Gast	Claim-Wert in der Assertion mit lokalem Konto vergleichen

Für die Analyse auf dem LoadMaster selbst, also ESP-Logs, L7-Debug-Traces und TCP-Mitschnitte, lohnt der Blick in den Beitrag Troubleshooting am LoadMaster: Logs, L7-Debug und TCP-Dump. Wenn die Anwendung trotz Ticket nach dem Kennwort fragt, steckt fast immer ein SPN-Problem oder ein stiller Rückfall auf NTLM dahinter.

Clients ohne Browser

SAML und OIDC in dieser Form leben von Browser-Umleitungen. Ein Client, der keine Umleitung zu einer Anmeldeseite verarbeiten kann, bleibt draußen. Das betrifft Exchange ActiveSync, Outlook mit MAPI über HTTP oder EWS, Autodiscover, Skripte, die per Invoke-WebRequest mit Windows-Authentifizierung arbeiten, und das RD Gateway, das RDP über HTTPS transportiert. Für diese Pfade brauchst du eigene Virtual Services oder SubVS mit anderem Authentifizierungsmodus oder eine ganz andere Lösung.

Anwendung	Brücke mit SAML oder OIDC und KCD	Bemerkung
IIS-Eigenentwicklung mit Windows-Auth.	ideal	das Kernszenario dieses Beitrags
Exchange OWA und ECP	möglich	Exchange kann OWA und ECP auch selbst über

		ADFS-Claims absichern
Exchange ActiveSync, Outlook, EWS	nein	keine Browser-Umleitung, Hybrid Modern Authentication prüfen
SharePoint Server SE	möglich, aber selten nötig	SharePoint SE kann selbst OIDC mit Entra ID
RD Web	möglich	Anmeldung an der Weboberfläche, nicht an der Sitzung
RD Gateway	nein	RDP über HTTPS, kein Browser im Spiel
Anwendungen mit eigener Formularanmeldung	eingeschränkt	KCD hilft nur, wenn die App Windows-Auth. akzeptiert

Für SharePoint lohnt sich ein genauer Blick: SharePoint Server Subscription Edition unterstützt OpenID Connect mit Entra ID direkt. Wenn die Anwendung selbst modern authentifizieren kann, ist das fast immer besser als jede Brücke, weil die Anwendung dann die echte Identität samt Gruppen-Claims sieht. Mehr dazu in SharePoint Server Subscription Edition hinter dem LoadMaster und auf der Seite SharePoint. Für Remote Desktop gilt Ähnliches, die Details stehen im Beitrag Remote Desktop Services: RD Gateway, RD Web und Connection Broker balancieren.

Abgrenzung: Entra Application Proxy und Entra Private Access

Microsoft hat für genau dieses Problem eigene Antworten. Wer einen LoadMaster ins Brückenszenario bringt, sollte erklären können, warum nicht eine davon. Und manchmal lautet die ehrliche Antwort: Nimm eine davon.

Entra Application Proxy

Der Application Proxy veröffentlicht interne Webanwendungen über einen Connector, der ausgehend zu Microsoft verbindet. Eingehend musst du keinen Port öffnen, die Vorauthentifizierung macht Entra ID, und für Windows-Authentifizierung beherrscht der Connector KCD, ganz analog zum LoadMaster. Daneben gibt es headerbasierte Anmeldung und SAML-SSO für lokale Anwendungen. Für Umgebungen ohne DMZ und ohne Lust auf Firewall-Regeln ist das sehr attraktiv.

Die Grenzen liegen woanders: Der Verkehr läuft über die Microsoft-Cloud, du hast weniger Kontrolle über TLS-Details, Timeouts, Header-Manipulation und Lastverteilung, und wer ohnehin einen LoadMaster mit Health Checks, WAF und Content Rules vor der Anwendung betreibt, baut mit dem Application Proxy eine zweite Veröffentlichungskette parallel auf. Ein Vergleich aller Varianten inklusive Azure Application Gateway steht in der Entscheidungshilfe: LoadMaster, Entra Application Proxy, Azure Application Gateway oder Reverse Proxy?.

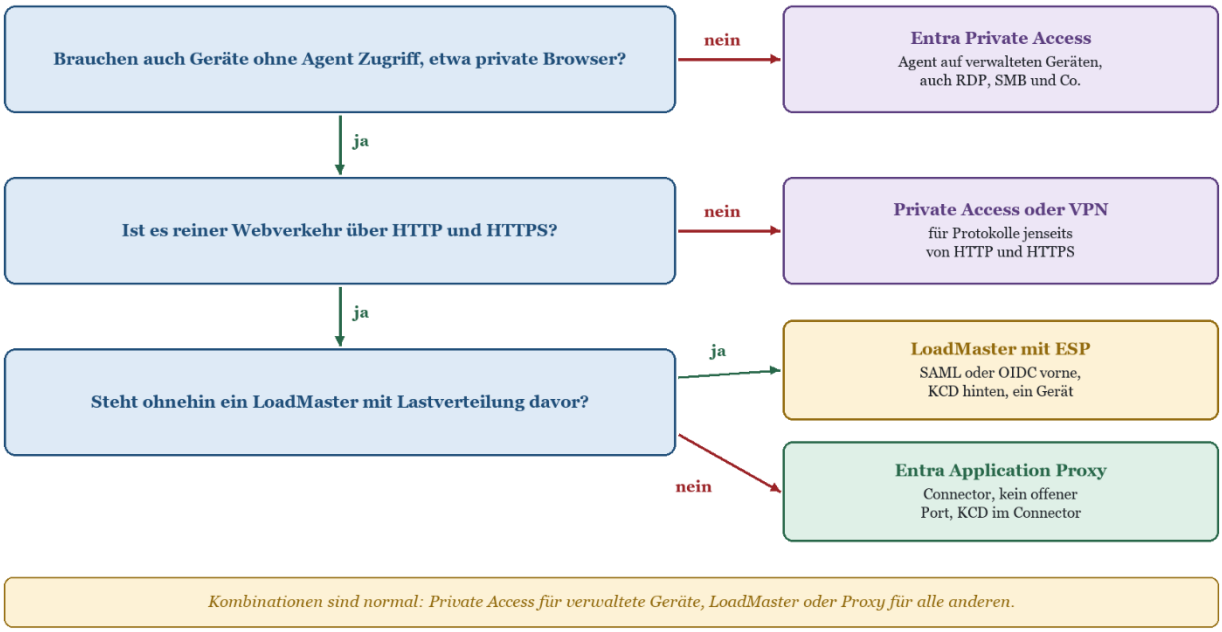
Entra Private Access

Private Access ist ein anderes Denkmodell. Es ist Teil von Global Secure Access, dem Security-Service-Edge-Angebot von Microsoft, und ersetzt eher das VPN als den Reverse Proxy. Auf dem Gerät läuft der Global-Secure-Access-Client, der Verkehr zu definierten internen Zielen über Microsoft zu einem Connector im Netz tunnelt. Weil das auf Netzwerkebene passiert, funktionieren auch RDP, SMB und andere Protokolle jenseits von HTTPS. Kerberos-SSO erreicht Private Access, indem auch die Domänencontroller über den Tunnel erreichbar gemacht werden: Der Client holt sich dann sein Ticket ganz klassisch selbst.

Damit ist auch klar, wo Private Access nicht hilft: bei Geräten ohne Agent, also privaten Rechnern, Kiosk-Systemen, Partnern und Dienstleistern. Für die bleibt der Browser-Zugang über einen Reverse Proxy der richtige Weg.

LoadMaster, Application Proxy oder Private Access?

Drei Wege zur Alt-Anwendung, drei verschiedene Denkmodelle



Skizze: grobe Orientierung, keine vollständige Entscheidungslogik

Kriterium	LoadMaster mit ESP	Entra Application Proxy	Entra Private Access
Grundprinzip	Reverse Proxy mit Vorauthentifizierung	Reverse Proxy aus der Cloud über Connector	Netzwerktunnel per Agent
Eingehende Ports	443 auf den Virtual Service	keine	keine
Client-Voraussetzung	Browser	Browser	Global-Secure-Access-Client
Protokolle	HTTP und HTTPS	HTTP und HTTPS	TCP und UDP, auch RDP und SMB
Kerberos zum Server	KCD durch den LoadMaster	KCD durch den Connector	Client holt Ticket selbst
MFA und Bedingter Zugriff	Entra ID über SAML oder OIDC	Entra ID nativ	Entra ID nativ, pro App-Segment
Lastverteilung, Health Checks, WAF	ja, im selben Gerät	nein, separat lösen	nein, separat lösen
Verkehr über Microsoft-Cloud	nein	ja	ja
Typischer Einsatz	vorhandener LoadMaster, Behörden, Partnerzugang	Web-Apps ohne DMZ	verwaltete Geräte, VPN-Ablösung

WICHTIG · Kein Entweder-oder

In vielen Häusern läuft am Ende beides: Private Access für verwaltete Geräte der eigenen Belegschaft, der LoadMaster mit SAML und KCD für den Browser-Zugang von außen und für alles, was ohnehin Lastverteilung braucht. Wichtig ist nur, dass die Richtlinien für Bedingten Zugriff für beide Wege zusammenpassen, damit niemand über den bequemeren Weg die strengere Prüfung umgeht.

FAQ

Braucht die Alt-Anwendung irgendeine Änderung?

In der Regel nein. Sie muss Windows-Authentifizierung mit Kerberos sprechen und einen sauberen SPN haben. Manchmal ist genau das die eigentliche Arbeit, weil die Anwendung bisher heimlich mit NTLM lief.

Kann ich SAML vorne ohne KCD hinten nutzen?

Ja, wenn die Anwendung selbst keine Anmeldung verlangt oder anonym erreichbar ist. Dann ist der LoadMaster reiner Türsteher. Sobald die Anwendung wissen muss, wer der Benutzer ist, brauchst du eine Server-Seite, und bei Windows-Authentifizierung ist das KCD.

Funktioniert das mit Gastbenutzern aus anderen Tenants?

Vorne ja, hinten nur, wenn es für den Gast ein lokales AD-Konto gibt, auf das die Identität abgebildet werden kann. Ohne lokales Konto gibt es kein Kerberos-Ticket.

Wo konfiguriere ich MFA?

In Entra ID per Richtlinie für Bedingten Zugriff, zugewiesen auf die Unternehmensanwendung des LoadMasters. Am LoadMaster selbst konfigurierst du dafür nichts.

SAML oder OIDC, was nehme ich?

Wenn ADFS im Spiel ist oder dein Team SAML gewohnt ist, SAML. Für neue Umgebungen rein mit Entra ID ist OIDC eine gute Wahl. Funktional ist das Brückenszenario mit beiden gleich.

Ersetzt das Szenario den Web Application Proxy von ADFS?

Für Anwendungen mit Windows-Authentifizierung kann es das. Den Proxy für ADFS selbst, also die Veröffentlichung der Anmeldeendpunkte, ersetzt es nicht.

Was passiert bei einem Failover im HA-Paar?

Die Konfiguration inklusive SSO-Domänen wird synchronisiert. Laufende ESP-Sitzungen können verloren gehen, die Benutzer werden dann erneut zu Entra ID umgeleitet und merken dank bestehender Entra-Sitzung meist nur ein kurzes Flackern.

Fazit: Moderne Anmeldung vorne, Kerberos hinten, Verstand dazwischen

Das Brückenszenario ist einer der elegantesten Einsätze des LoadMasters. Die Alt-Anwendung bleibt unangetastet, die Anmeldung wandert dorthin, wo MFA, Bedingter Zugriff und Anmeldeprotokolle ohnehin zu Hause sind, und der LoadMaster übersetzt per SAML oder OIDC auf der einen und KCD auf der anderen Seite. Wer ADFS heute nutzt und morgen ablöst, tauscht nur die Client-Seite.

Die Stolpersteine sind bekannt und gut beherrschbar: Identitäten, die in der Cloud anders heißen als lokal, Zertifikate und geheime Schlüssel mit Ablaufdatum, Clients ohne Browser und Sitzungen, die länger leben als die letzte Richtlinienänderung. Und wenn du ehrlich bist, ist für manche Anwendung Entra Application Proxy oder Private Access der einfachere Weg. Ein guter Dolmetscher weiß auch, wann er nicht gebraucht wird. Ein schlechter merkt es erst, wenn das Signaturzertifikat abgelaufen ist.

TIPP · Unterstützung bei Planung und Umsetzung

Wenn du Alt-Anwendungen hinter Entra ID bringen und dabei LoadMaster, Application Proxy und Private Access sauber gegeneinander abwägen willst, hilft dir die Beratung zum Kemp LoadMaster. Wer SAML, OIDC und KCD mit dem eigenen Team im Labor aufbauen und gezielt kaputtmachen

will, findet das in der Kemp-LoadMaster-Schulung.

WEITERLESEN · Weiter im Thema

› Edge Security Pack: Vorauthentifizierung, SSO-Domänen und der TMG-Ersatz
› Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten
› ADFS und Web Application Proxy mit dem LoadMaster: Farm, Probe, SNI
› MFA vor OWA, ECP und Co.: Zwei-Faktor am LoadMaster
› Entscheidungshilfe: LoadMaster, Entra Application Proxy, Azure Application Gateway oder Reverse Proxy?