

Active Directory Federation Services (ADFS): Architektur, Einsatzszenarien und Hochverfügbarkeit

Active Directory Federation Services

Architektur · Einsatzszenarien · Hochverfügbarkeit

AD FS-FarmWAP / DMZZertifikateGeo-DR

Farm in zwei Regionen

Region A

WAP

WAP

AD FS

AD FS

Region B

WAP

WAP

AD FS

AD FS

Wissen

Erst die Grundlagen? Token-Fluss, Claims und Protokolle in Ruhe erklärt:

› [Active Directory Federation Services \(ADFS\) – Grundlagen, Szenarien und Best Practices](#)

Beratung

Architektur-Review, Health-Check deiner Farm, Zertifikatskonzept, Notfallplan oder der geordnete Umzug nach Entra ID – mit jemandem, der die Fehlerbilder schon gesehen hat.

Schulung

Workshops für dein Admin-Team: Claim-Regeln schreiben, Fehlersuche in den Ereignisprotokollen, Rollover und Failover an der eigenen Umgebung üben.

Eine AD FS-Farm ist wie die Heizungsanlage im Keller: Niemand denkt an sie, solange es warm ist. Und dann kommt dieser eine Montag, an dem das Token-Signing-Zertifikat still und leise die Rolle gewechselt hat, die Hälfte der SaaS-Anwendungen nur noch Fehlerseiten zeigt und die Geschäftsführung wissen möchte, warum „das Internet kaputt“ ist. Ich habe solche Montage in Konzernen, Stadtverwaltungen und mittelständischen Maschinenbauern erlebt. Die Ursache war fast nie ein exotischer Bug, sondern fast immer eine Architektur, die beim Aufbau niemand zu Ende gedacht hat.

Genau darum geht es hier. Active Directory Federation Services ADFS – Microsoft schreibt den Dienst offiziell „AD FS“, im Alltag sagt jeder „ADFS“ – ist der lokale Identity Provider von Windows Server. Er stellt Identitäten aus deinem Active Directory über Sicherheitsgrenzen hinweg bereit, als signierte Token für Anwendungen, die mit Kerberos nichts anfangen können. Dieser Beitrag nimmt die Architektur auseinander: das claims-basierte Modell, die Protokolle, die Trusts zu Microsoft 365 und Partnern, die Bausteine einer hochverfügbaren Farm mit Web Application Proxy, das Zertifikatsmanagement, Monitoring und Diagnose, Geo-Redundanz und die ehrliche Frage, wann sich der Weiterbetrieb nicht mehr lohnt. Den Gesamtüberblick über alle Facetten des Themas findest du auf der Themenseite [Active Directory Federation Services](#).

Fakten: AD FS im Jahr 2026

- Serverrolle in Windows Server 2016, 2019, 2022 und 2025, ohne zusätzliche Lizenz.

- Protokolle: SAML 2.0, WS-Federation, WS-Trust, OAuth 2.0 und OpenID Connect.
- Bausteine: Farm aus AD FS-Servern, Konfigurationsdatenbank (WID oder SQL Server), Web Application Proxy in der DMZ.
- Funktional ist das Produkt fertig: Neue Features entstehen in Microsoft Entra ID, AD FS erhält Sicherheits- und Qualitätsupdates im Lebenszyklus der jeweiligen Serverversion.
- Microsoft empfiehlt ausdrücklich, Anwendungen nach Entra ID zu migrieren, statt AD FS auf eine neuere Version zu heben.
- Der erweiterte Support für Windows Server 2016 endet am 12. Januar 2027 – Farmen auf dieser Basis haben akuten Handlungsbedarf.

Architektur: Claims, Protokolle und Trusts

Das claims-basierte Modell: Aussagen statt Kennwörter

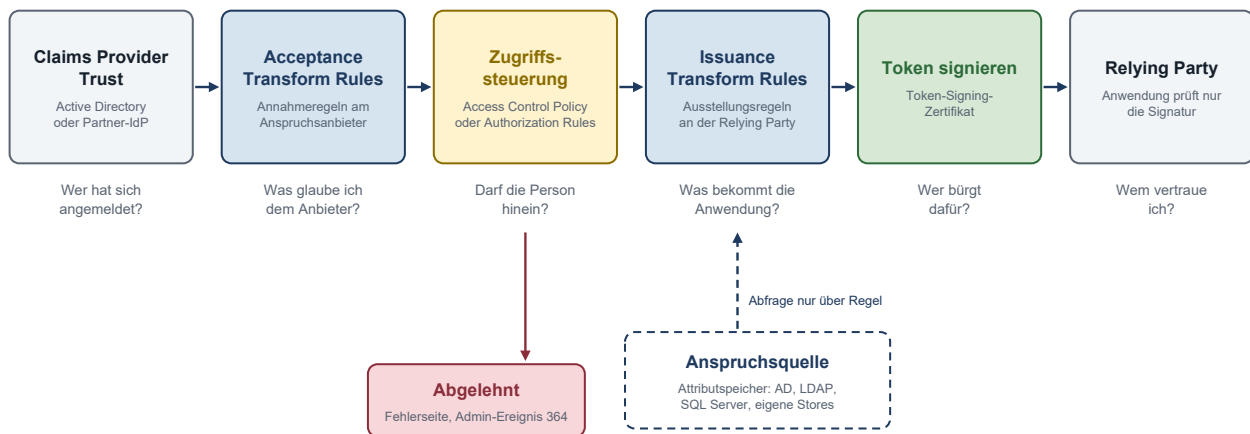
Eine Anwendung, die an AD FS hängt, sieht nie ein Kennwort und redet nie mit einem Domänencontroller. Sie bekommt ein Token: ein Paket von Aussagen über eine Person, sogenannte Claims, digital signiert vom AD FS. Ein Claim ist ein Paar aus Typ und Wert – etwa „UPN = anna.berger@contoso.com“, „Gruppe = Einkauf-Freigabe“ oder „Authentifizierungsmethode = Mehrfaktor“. Die Anwendung prüft die Signatur gegen das öffentliche Zertifikat, das sie aus den Föderationsmetadaten kennt, liest die Claims und trifft darauf ihre Entscheidung.

Daraus folgen zwei Wahrheiten, die du bei jedem Architekturgespräch im Kopf haben solltest. Erstens: Die Anwendung glaubt alles, was korrekt signiert ist. Wer den privaten Schlüssel des Token-Signing-Zertifikats besitzt, kann sich als jeder beliebige Mensch ausgeben, auch als globaler Administrator in Microsoft 365. Genau das ist der Kern des sogenannten Golden-SAML-Angriffs, und genau deshalb gehört eine AD FS-Farm in dieselbe Schutzklasse wie deine Domänencontroller. Zweitens: Die Anwendung bekommt nur die Claims, die du ihr gibst. Was nicht im Token steht, existiert für sie nicht. Das ist Datenschutz per Design – oder eine endlose Fehlersuche, wenn die Regel den falschen Claim-Typ ausstellt.

Claim-Regeln: Anspruchsquelle und Ausstellungsregel sauber trennen

Jedes Token durchläuft eine Pipeline aus Regelsätzen. Am Claims Provider Trust – meist dem eingebauten Trust „Active Directory“ – entscheiden die Acceptance Transform Rules, welche Claims des Anspruchsanbieters überhaupt angenommen werden. An der Relying Party folgt die Zugriffssteuerung: seit AD FS in Windows Server 2016 als Access Control Policy, alternativ als klassische Issuance Authorization Rules. Hier fällt die Entscheidung, ob jemand die Anwendung überhaupt betreten darf. Erst danach formen die Issuance Transform Rules das, was die Anwendung tatsächlich erhält. Zum Schluss signiert der Dienst das Ergebnis.

Claim-Pipeline in AD FS: vom Anspruchsanbieter bis zum signierten Token



Merksatz: Die Quelle liefert Daten, die Regel entscheidet. Wer beides vermischt, debuggt später nachts.

Abbildung 1: Die Claim-Pipeline in AD FS. Annahme, Zugriffsentscheidung und Ausstellung sind getrennte Stufen; Attributspeicher werden nur über Regeln abgefragt.

Die Trennung von Anspruchsquelle und Ausstellungsregel klingt akademisch, ist aber der Unterschied zwischen einer wartbaren und einer verwunschenen Farm. Die Anspruchsquelle – der Attributspeicher, also AD, ein LDAP-Verzeichnis oder eine SQL-Datenbank – liefert Rohdaten. Die Regel entscheidet, welche dieser Daten unter welchem Claim-Typ in welches Token wandern. Wer in einer einzigen Regel gleichzeitig abfragt, umrechnet, filtert und ausstellt, hat nach zwei Jahren ein Geflecht, das niemand mehr anzufassen wagt. In einem Projekt fand ich eine Relying Party mit 47 Regeln, von denen elf denselben Gruppen-Claim auf unterschiedlichen Wegen erzeugten. Die Anwendung funktionierte – aus Gründen, die keiner kannte.

Bewährt hat sich ein schlichtes Muster: Eine Regel holt Attribute aus dem Speicher und legt sie mit add statt issue als Zwischenergebnis ab. Folgeregeln transformieren und filtern. Nur die letzte Stufe stellt mit issue aus. So siehst du in jeder Regel genau eine Verantwortung, und ein geänderter Attributname im AD betrifft genau eine Stelle.

```
@RuleName = "10-Quelle: UPN und Gruppen aus AD laden"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
=> add(store = "Active Directory",
      types = ("http://contoso.com/claims/upn", "http://contoso.com/claims/gruppe"),
      query = ";userPrincipalName,tokenGroups;{0}", param = c.Value);

@RuleName = "20-Ausstellung: nur Gruppen mit Präfix APP-Einkauf"
c:[Type == "http://contoso.com/claims/gruppe", Value =~ "^APP-Einkauf"]
=> issue(Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/role", Value = c.Value);

@RuleName = "30-Ausstellung: UPN unverändert weiterreichen"
c:[Type == "http://contoso.com/claims/upn"]
=> issue(Type = "http://contoso.com/claims/anmeldename", Value = c.Value);
```

Tipp

Nummeriere Regeln im Namen (10-, 20-, 30-) und trenne „Quelle“ und „Ausstellung“ sichtbar. Exportiere alle Regelsätze regelmäßig per Get-AdfsRelyingPartyTrust in eine Versionsverwaltung. Änderungen testest du zuerst in einer Staging-Farm mit eigener Testanwendung – eine

Regeländerung in Produktion ist sofort für alle wirksam, ein Rückgängig-Knopf existiert nicht.

Protokolle im AD FS-Kontext: welcher Flow wofür passt

AD FS spricht fünf Sprachen, und die Wahl ist selten Geschmackssache. Die Anwendung entscheidet meist, was sie kann; du entscheidest, was du zulässt. Für neue Anbindungen gilt eine einfache Faustregel: Browser-Anwendung von der Stange – SAML 2.0; selbst entwickelte Web-, Mobil- oder API-Anwendung – OpenID Connect mit OAuth 2.0; alles andere nur, wenn es nicht anders geht.

Protokoll	Typischer Einsatz	Flow in AD FS	Einschätzung
SAML 2.0	SaaS- und Fachanwendungen mit Browser-Anmeldung	SP- oder IdP-initiiert, HTTP-Redirect und HTTP-POST; Artefakt-Bindung nur mit SQL-Datenbank	Standard für gekaufte Anwendungen, gut dokumentiert, robust
WS-Federation	Microsoft 365 im Browser, ältere .NET- und SharePoint-Anwendungen	Passiver Endpunkt /adfs/ls	Funktioniert, aber für neue Projekte kein Ziel mehr
WS-Trust	Aktive Clients ohne Browser, Legacy-Rich-Clients	Endpunkte unter /adfs/services/trust	Häufiges Ziel für Passwort-Spraying; ungenutzte Endpunkte am Proxy schließen
OAuth 2.0	APIs, Dienst-zu-Dienst, native Anwendungen	Authorization Code mit PKCE, Client Credentials, On-Behalf-Of; Konfiguration über Application Groups	Für eigene Anwendungen erste Wahl, Implicit Flow vermeiden
OpenID Connect	Moderne Web- und Mobilanwendungen mit Anmeldung	Authorization Code Flow mit ID-Token, Discovery unter /adfs/.well-known/openid-configuration	Erste Wahl für Neuentwicklungen – sofern sie nicht gleich an Entra ID gehen

Bei OAuth und OpenID Connect registrierst du Anwendungen über Application Groups mit Client-ID, Redirect-URIs und gegebenenfalls einem Geheimnis oder Zertifikat. Die Redirect-URI muss exakt mit dem übereinstimmen, was die Anwendung sendet – Schema, Groß- und Kleinschreibung, abschließender Schrägstrich. Eine abweichende URI quittiert AD FS mit einem Fehler im Admin-Protokoll, der den Wert und die Client-ID nennt. Lies ihn, bevor du am Server herumschraubst: Der Fehler sitzt in neun von zehn Fällen in der Registrierung.

Relying Party Trust, Claims Provider Trust und Metadaten

Ein Relying Party Trust ist die Vertrauensstellung zu einer Anwendung, die Token von deinem AD FS konsumiert. Er enthält die Kennung der Anwendung, ihre Endpunkte, ihr Verschlüsselungszertifikat und die Regelsätze. Ein Claims Provider Trust ist die Gegenrichtung: ein fremder Identity Provider – etwa der AD FS eines Partners –, dessen Token dein AD FS annimmt und in eigene Token übersetzt. In diesem Szenario agiert deine Farm als Federation Provider.

Beide Trusts lassen sich manuell pflegen oder über Föderationsmetadaten. Das ist ein XML-Dokument, das jede Seite unter einer festen Adresse veröffentlicht – bei AD FS unter /FederationMetadata/2007-06/FederationMetadata.xml – und das Endpunkte, Kennung und öffentliche Zertifikate enthält. Wird ein Trust mit der Metadaten-Adresse angelegt und die automatische Aktualisierung aktiviert, holt AD FS Änderungen der Gegenseite selbst ab.

Umgekehrt holt eine gut gebaute Anwendung deine neuen Signaturzertifikate aus deinen Metadaten. Jede Anwendung, die das nicht kann, ist ein Termin in deinem Kalender – und zwar jedes Jahr.

Merkmal	Relying Party Trust	Claims Provider Trust
Richtung	AD FS stellt Token für die Anwendung aus	AD FS nimmt Token eines fremden IdP an
Typische Gegenseite	Microsoft 365, SaaS, eigene Webanwendung	Partner-AD FS, anderer SAML-IdP, zweite Gesamtstruktur
Relevante Regeln	Zugriffssteuerung, Issuance Transform Rules	Acceptance Transform Rules
Kritisches Zertifikat	Dein Token-Signing; optional Verschlüsselungszertifikat der Anwendung	Signaturzertifikat des Partners; dein Token-Decrypting
Metadaten	Anwendung bezieht deine, du optional ihre	Du beziehst die des Partners, er deine

Die typischen Einsatzszenarien

Wofür betreibt man das alles? Die Liste ist über die Jahre kürzer geworden, weil Entra ID viele Aufgaben übernommen hat. Leer ist sie nicht.

Szenario	Was AD FS leistet	Einordnung heute
Microsoft 365 föderiert	Anmeldung an Exchange Online, SharePoint Online und Teams mit lokaler Prüfung gegen das AD	Technisch möglich, für die meisten Organisationen inzwischen durch Passwort-Hash-Sync oder Pass-Through-Authentication ersetzbar
Partnerzugriff (B2B)	Partner melden sich mit eigenen Konten an, ohne Konten im eigenen AD	Für Cloud-Anwendungen übernimmt Entra External ID die Rolle; für lokale Anwendungen bleibt AD FS üblich
Lokale und hybride Anwendungen	SSO für SAML-, WS-Fed- und OIDC-Anwendungen im eigenen Rechenzentrum und in IaaS-Workloads	Klassisches Restfeld; Migration nach Entra ID je Anwendung prüfen
Externer Zugriff über WAP	Veröffentlichung interner Webanwendungen mit Pre-Authentication	Für neue Veröffentlichungen ist der Microsoft Entra-Anwendungsproxy meist die bessere Wahl
Legacy-Anwendungen	Kerberos-Anwendungen per WAP mit Kerberos Constrained Delegation hinter eine Föderationsanmeldung stellen	Funktioniert, ist aber Wartungslast; Ablöse planen
Abgeschottete Umgebungen	Föderation ohne Abhängigkeit von einem Cloud-Dienst	Echter Grund für AD FS, etwa bei Souveränitätsauflagen oder Netzen ohne Internetanbindung

Föderation mit Microsoft 365 und Microsoft Entra ID

Domänenföderation einrichten

Die Anbindung an Microsoft 365 ist für viele Organisationen der Grund, warum es überhaupt eine Farm gibt. Technisch wird eine verifizierte Domäne im Entra-Mandanten von „verwaltet“ auf „föderiert“ umgestellt. Ab diesem Moment leitet Entra ID jede Anmeldung mit einem UPN dieser Domäne an deinen AD FS weiter, der die Anmeldung prüft und ein Token zurückschickt. Auf

deiner Seite entsteht dafür ein Relying Party Trust namens „Microsoft Office 365 Identity Platform“ mit einem vordefinierten Regelsatz für UPN und ImmutableID.

Der bequemste Weg zur Einrichtung ist Microsoft Entra Connect Sync mit der Anmeldeoption „Verbund mit AD FS“; der Assistent konfiguriert beide Seiten und kann den Trust später reparieren. Wer per Skript arbeitet, nutzt heute das Microsoft Graph PowerShell SDK oder das Modul Microsoft.Entra. Die alten Module MSONline und AzureAD sind abgeschaltet, Skripte mit Convert-MsolDomainToFederated oder Update-MsolFederatedDomain laufen ins Leere. Ihre Nachfolger heißen New-MgDomainFederationConfiguration, Update-MgDomainFederationConfiguration und Get-EntraFederationProperty. Der frühere Schalter für mehrere Top-Level-Domänen existiert nicht mehr: Du konfigurierst jede föderierte Domäne einzeln.

```
# Föderationskonfiguration einer Domäne prüfen
Connect-Entra -Scopes 'Domain.Read.All'
Get-EntraFederationProperty -DomainName contoso.com | Format-List Source, SigningCertificate

# Gegenprobe auf der AD FS-Seite
Get-AdfsCertificate -CertificateType Token-Signing | Format-List Thumbprint, IsPrimary, NotAfter
```

Ein Punkt wird bei der Einrichtung gern übersehen: das Zusammenspiel der Mehrfaktor-Authentifizierung. Über die Eigenschaft federatedIdpMfaBehavior der Domänenföderation legst du fest, ob Entra ID eine MFA akzeptiert, die AD FS bereits erledigt hat, ob es sie vom AD FS erzwingt oder ob es sie grundsätzlich selbst durchführt. Der Wert bestimmt, ob deine Conditional-Access-Richtlinien so wirken, wie du denkst. Prüfe ihn, bevor du dich auf eine Richtlinie verlässt.

Passwort-Hash-Sync, Pass-Through-Authentication oder echte Föderation

Die ehrlichste Frage, die du einer bestehenden M365-Föderation stellen kannst: Warum gibt es sie noch? Microsoft empfiehlt für die Anmeldung an Microsoft 365 heute verwaltete Authentifizierung, also Passwort-Hash-Synchronisation, optional ergänzt um Pass-Through-Authentication. Beide verlagern die Anmeldung zu Entra ID, beide machen eine Farm samt Proxys, Zertifikaten und Notfallplan für diesen Zweck überflüssig.

Kriterium	Passwort-Hash-Sync (PHS)	Pass-Through-Authentication (PTA)	Föderation mit AD FS
Wo wird das Kennwort geprüft?	In Entra ID, gegen einen abgeleiteten Hash des Hashs	Lokal am DC über einen Agenten mit ausgehender Verbindung	Lokal am AD FS
Lokale Infrastruktur	Entra Connect Sync	Entra Connect plus mindestens drei Agenten empfohlen	Farm, WAPs, Load Balancer, Zertifikate
Abhängigkeit beim Ausfall lokaler Systeme	Keine, Anmeldung funktioniert weiter	Anmeldung fällt aus, wenn alle Agenten oder DCs fehlen	Anmeldung fällt aus, wenn Farm oder Proxy fehlen
Erkennung kompromittierter Kennwörter	Ja (Leaked Credentials in Entra ID Protection)	Nur wenn PHS zusätzlich aktiv ist	Nur wenn PHS zusätzlich aktiv ist
Lokale Anmelderichtlinien (Kontoablauf, Anmeldezeiten)	Nur eingeschränkt	Ja	Ja

Kriterium	Passwort-Hash-Sync (PHS)	Pass-Through-Authentication (PTA)	Föderation mit AD FS
Smartcard- und Zertifikatsanmeldung	Über zertifikatbasierte Authentifizierung in Entra ID	Über zertifikatbasierte Authentifizierung in Entra ID	Ja, direkt
Betriebsaufwand	Gering	Mittel	Hoch

Wichtig

Aktiviere Passwort-Hash-Sync auch dann, wenn du föderiert bleibst. Es kostet nichts, liefert die Erkennung kompromittierter Kennwörter und ist dein Rettungsboot: Fällt die Farm aus, stellst du die Domäne auf verwaltete Authentifizierung um, und die Belegschaft kann sich nach kurzer Zeit wieder anmelden. Ohne vorhandene Hashes beginnt in diesem Moment erst die Synchronisation – mitten im Notfall.

Typische Fehlerbilder bei der Trust-Erneuerung

Die M365-Föderation ist meistens unauffällig, weil Entra ID sich die neuen Signaturzertifikate selbst holt. Es prüft 35 Tage vor Ablauf des aktuellen Zertifikats deine öffentlichen Föderationsmetadaten und danach täglich, bis es das neue Zertifikat findet. Das klappt, solange drei Bedingungen erfüllt sind: AutoCertificateRollover ist aktiv, die Metadaten sind aus dem Internet über den WAP erreichbar, und niemand hat den Trust manuell verbogen. Die Fehlerbilder, die ich in Projekten am häufigsten sehe:

- Metadaten nicht öffentlich erreichbar: Der WAP veröffentlicht den Metadaten-Endpunkt nicht, oder eine Web Application Firewall blockt ihn. Entra ID verschickt Warn-E-Mails, die im Sammelpostfach versauern, und am Tag der Promotion ist Schluss mit Anmelden.
- Zertifikate aus der eigenen PKI ohne Prozess: AutoCertificateRollover ist abgeschaltet, das Signaturzertifikat stammt aus der internen CA, und der Mensch mit dem Kalendereintrag hat das Unternehmen verlassen.
- Mehrere föderierte Domänen, nur eine aktualisiert: Nach einem manuellen Tausch wird Update-MgDomainFederationConfiguration für contoso.com ausgeführt, aber nicht für contoso.de. Ein Teil der Konten kann sich nicht mehr anmelden, und die Fehlersuche beginnt bei den falschen Leuten.
- Falsche Farm im Trust: Nach einer Migration auf eine neue Farm zeigt die Domäne noch auf alte Endpunkte oder alte Zertifikate. Hier hilft nur der saubere Weg über die dokumentierte Notfall-Rotation und ein Abgleich der Fingerabdrücke auf beiden Seiten.
- Warn-E-Mail trotz korrekter Konfiguration: Microsoft verschickt gelegentlich Erneuerungshinweise, obwohl keine Aktion nötig ist. Prüfe die Fingerabdrücke, statt in Panik ein neues Zertifikat zu erzeugen – das erzeugt erst das Problem, vor dem die E-Mail warnen wollte.

Hochverfügbarkeit: Farm, Datenbank und Web Application Proxy

Die Farm und der Load Balancer

Eine einzelne AD FS-Instanz ist keine Architektur, sondern eine Wette. Produktiv laufen mindestens zwei Server in einer Farm hinter einem Load Balancer, alle mit demselben Föderationsdienstnamen und demselben TLS-Zertifikat. Für Anmeldungen ist AD FS zustandslos – jeder Knoten kann jede Anfrage bedienen, weil der Kontext im Cookie und in den

Protokollnachrichten steckt. Deshalb brauchst du keine Sitzungsaffinität; Microsoft rät sogar ausdrücklich von IP-basierter Affinität ab, weil sonst einzelne Knoten unter Legacy-Mailclients zusammenbrechen.

Die Anforderungen an den Load Balancer sind knapp, aber hart: Er darf TLS nicht terminieren, er muss Server Name Indication unterstützen, und er prüft die Knoten über den HTTP-Endpunkt /adfs/probe auf Port 80, der lokal mit 200 OK antwortet. DNS-Round-Robin ist kein Load Balancing, weil es tote Knoten nicht aus der Rotation nimmt. Und das Azure Application Gateway, das in manchen Konzepten vor den Proxys auftaucht, ist für AD FS ungeeignet, weil es TLS terminiert. In Azure gehört ein Layer-4-Load-Balancer davor. Damit Extranet Smart Lockout und IP-basierte Regeln funktionieren, muss außerdem die echte Client-IP beim WAP ankommen – ein NAT, das alle Clients hinter einer Adresse versteckt, sperrt im Zweifel alle gleichzeitig aus.

Warnung

TLS-Terminierung am Load Balancer wird für keinen AD FS-Anwendungsfall unterstützt. Zertifikatsanmeldung, Gerätezertifikate und Extended Protection brechen damit. Wenn das Netzwerkteam „aus Sicherheitsgründen“ aufbrechen und neu verschlüsseln möchte: Das ist ein Architekturkonflikt, kein Konfigurationsdetail. Kläre ihn, bevor die Server bestellt sind.

WID, SQL Server Always On oder Failover-Cluster

Die Konfiguration der Farm – Trusts, Regeln, Zertifikate, Eigenschaften – liegt in einer Konfigurationsdatenbank. Du hast zwei Grundoptionen: die Windows Internal Database (WID) auf jedem AD FS-Server oder einen externen SQL Server. Mit WID gibt es genau einen primären Server, der Änderungen annimmt. Die sekundären Server halten eine schreibgeschützte Kopie und fragen den Primärserver standardmäßig alle fünf Minuten über HTTP auf Port 80 nach Änderungen. Anmeldungen bedienen alle Knoten gleichberechtigt.

Die Grenzen der WID haben nichts mit der Zahl der Benutzerkonten zu tun, auch wenn sich diese Legende hartnäckig hält. Entscheidend sind Knoten und Trusts: Bis 30 AD FS-Server und höchstens 100 Relying Party Trusts wird WID unterstützt, darüber ist SQL Server Pflicht. Zusätzlich setzen die SAML-Artefakt-Auflösung und die Token-Replay-Erkennung SQL Server voraus. Letztere brauchst du, wenn deine Farm als Federation Provider Token externer Anspruchsanbieter entgegennimmt.

Kriterium	Windows Internal Database	SQL Server Always On (Verfügbarkeitsgruppe)	SQL Server Failover-Cluster-Instanz
Unterstützte Größe	Bis 30 Knoten und 100 Relying Party Trusts	Ohne praktische Grenze	Ohne praktische Grenze
Schreibzugriff	Nur der primäre AD FS-Server	Alle AD FS-Server	Alle AD FS-Server
Artefakt-Auflösung, Token-Replay-Erkennung	Nein	Ja	Ja
Ausfall des Datenbank-Primärs	Anmeldungen laufen weiter, Konfigurationsänderungen erst nach manuellem Umstufen	Automatisches Failover über den Listener	Automatisches Failover der Instanz
Ausfall des	Jeder Knoten hat eigene	Jedes Replikat hat eigenen	Gemeinsamer Speicher ist

Kriterium	Windows Internal Database	SQL Server Always On (Verfügbarkeitsgruppe)	SQL Server Failover-Cluster-Instanz
Speichers	Kopie	Speicher	Single Point of Failure
Abhängigkeiten	Keine	SQL-Team, Lizenz, Windows-Cluster, Patchfenster	SQL-Team, Lizenz, Shared Storage
Geeignet für	Die meisten Farmen	Große Farmen, Geo-Szenarien, Federation Provider	Organisationen mit vorhandener FCI-Plattform

Klingt nach klarer Sache für SQL? Nicht so schnell. Mit SQL Server verlagerst du die Verfügbarkeit deiner Anmeldung in eine Plattform, die ein anderes Team mit anderen Patchfenstern betreibt. AD FS greift bei jeder Anmeldung mehrfach auf die Datenbank zu – fällt der Listener aus, steht die Farm. Ich habe eine Umgebung erlebt, in der ein geplanter SQL-Neustart am Samstagvormittag die komplette M365-Anmeldung lahmlegte, weil niemand die Abhängigkeit kannte. Mit WID wäre das nicht passiert. Azure SQL Database wird als Konfigurationsdatenbank übrigens nicht unterstützt.

Tipp

Bei WID fällt der Ausfall des primären Servers im Alltag kaum auf, weil Anmeldungen weiterlaufen. Lege trotzdem fest, wer im Ernstfall einen sekundären Server mit Set-AdfsSyncProperties -Role PrimaryComputer zum Primär macht und die übrigen Knoten mit Set-AdfsSyncProperties -Role SecondaryComputer -PrimaryComputerName auf ihn zeigen lässt. Wartung planst du knotenweise: Knoten am Load Balancer entleeren, patchen, Probe prüfen, zurücknehmen.

Web Application Proxy in der DMZ

AD FS-Server gehören ins interne Netz, nie direkt ins Internet. Für den Zugriff von außen stellst du Web Application Proxy (WAP) in die DMZ, eine Rollenkomponente des Remotezugriffs. Der WAP ist nicht Mitglied der Domäne, nimmt Anfragen aus dem Internet an und reicht sie an die Farm weiter. Anmelde- und Metadaten-Endpunkte werden so erreichbar, ohne dass ein Domänenmitglied exponiert ist. Ein WAP und ein AD FS-Server dürfen nicht auf derselben Maschine laufen. Statt des WAP sind Drittanbieter-Proxys zulässig, sofern sie das Protokoll MS-ADFSPIP implementieren – ein generischer Reverse Proxy reicht nicht.

Zusätzlich kann der WAP interne Webanwendungen veröffentlichen. Mit Pre-Authentication meldet sich die Person zuerst an AD FS an, und erst ein gültiges Token öffnet den Weg zur Anwendung; nicht angemeldeter Datenverkehr erreicht das Backend gar nicht. Der Gegenentwurf ist Pass-Through, bei dem der WAP nur weiterreicht und die Anwendung selbst prüft. Für neue Veröffentlichungen ist der Microsoft Entra-Anwendungsproxy meist die bessere Wahl, weil er ohne eingehende Firewallregeln auskommt und Conditional Access direkt nutzt.

Zwei Sicherheitsmechanismen verdienen eigene Aufmerksamkeit. Extended Protection for Authentication bindet die Windows-Anmeldung an den TLS-Kanal und verhindert, dass ein Angreifer abgefangene Anmeldedaten über eine andere Verbindung weiterverwendet. Die Eigenschaft ExtendedProtectionTokenCheck ist standardmäßig aktiv; die praktische Folge: Das TLS-Zertifikat auf den WAPs muss denselben Schlüssel haben wie das auf den AD FS-Servern. Zweitens das Proxy-Trust-Zertifikat. Bei der Einrichtung mit Install-WebApplicationProxy erhält jeder WAP ein Vertrauenszertifikat, mit dem er sich bei der Farm ausweist, und erneuert es danach selbstständig. War ein WAP längere Zeit ausgeschaltet oder driftet seine Uhr, scheitert die

Erneuerung – der WAP kann dann keine Konfiguration mehr abrufen, und du musst den Trust mit Install-WebApplicationProxy neu herstellen.

Referenzarchitektur: AD FS-Farm mit Web Application Proxy und Netzwerkflüssen

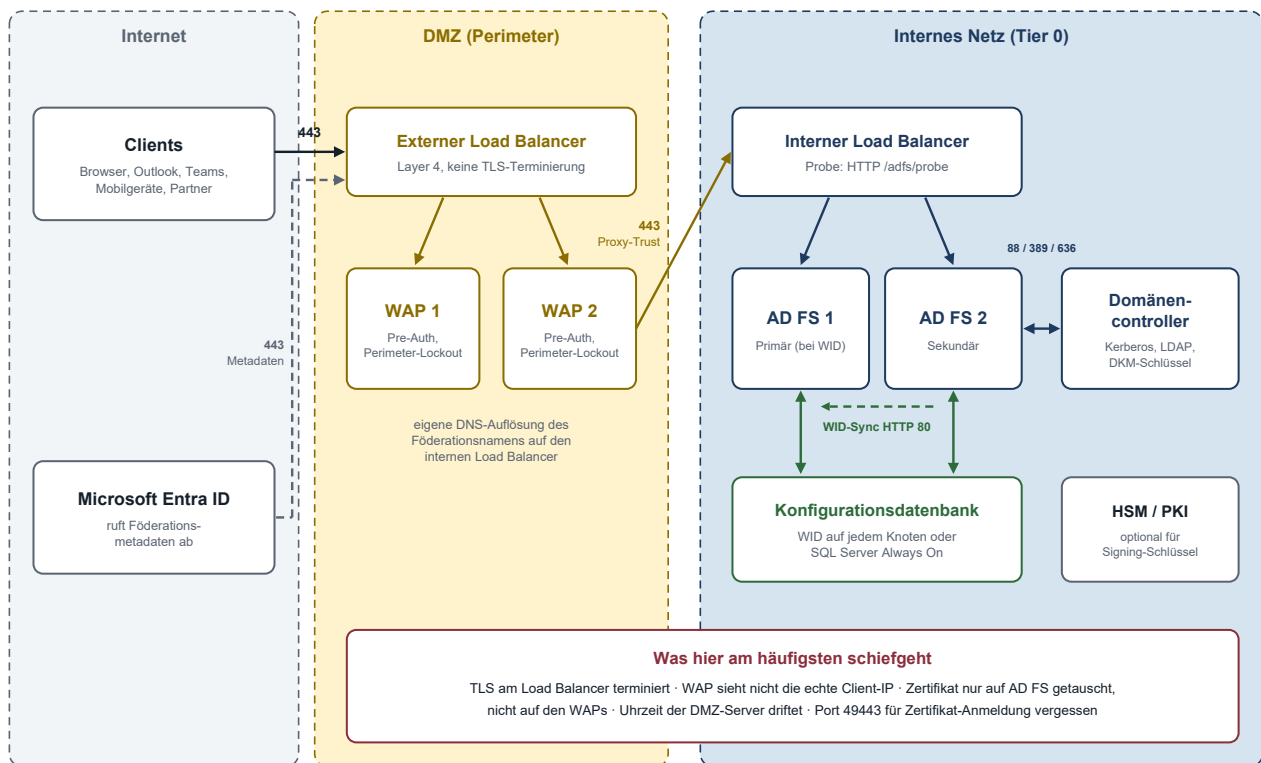


Abbildung 2: Referenzarchitektur mit zwei WAPs in der DMZ, zwei AD FS-Servern im internen Netz und den Netzwerkflüssen, die du dokumentieren musst.

Netzwerkflüsse und Portfreigaben exakt dokumentieren

Warum so pedantisch? Weil die Firewall zwischen DMZ und internem Netz in den meisten Unternehmen von einem anderen Team betreut wird, das bei der nächsten Regelbereinigung „unbenutzte“ Freigaben entfernt. Port 49443 wird nur bei Zertifikatsanmeldung genutzt, der WID-Sync-Port nur alle fünf Minuten, die Probe nur vom Load Balancer. Nichts davon fällt im Alltag auf – bis es fehlt. Eine Tabelle wie die folgende gehört ins Betriebshandbuch und in den Firewall-Antrag, mit Quelle, Ziel und Zweck.

Quelle	Ziel	Port	Zweck
Internet	Externer Load Balancer / WAP	TCP 443	Anmeldung, Metadaten, veröffentlichte Anwendungen
Internet	Externer Load Balancer / WAP	TCP 49443	Benutzerzertifikat-Anmeldung, falls nicht über certauth auf 443
Load Balancer	WAP und AD FS	TCP 80	Health Probe /ads/probe
WAP	Interner Load Balancer / AD FS	TCP 443	Weiterleitung und Proxy-Trust (MS-ADFSPIP)
AD FS sekundär	AD FS primär	TCP 80	WID-Synchronisation
AD FS	Domänencontroller	TCP/UDP 88, 389, 636, 3268, 445, 135 plus RPC-dynamisch	Kerberos, LDAP, globaler Katalog, DKM-Zugriff
AD FS	SQL Server / Listener	TCP 1433 oder eigener Port	Konfigurationsdatenbank (nur SQL-Variante)

Quelle	Ziel	Port	Zweck
AD FS	Microsoft-Endpunkte	TCP 443 ausgehend	Entra-MFA-Adapter, Connect-Health-Agent
WAP und AD FS	Zeitquelle	UDP 123	Zeitsynchronisation – Token und Proxy-Trust sind zeitkritisch

Für DNS gilt eine Besonderheit, die regelmäßig für Kopfschmerzen sorgt: Intern muss der Föderationsname auf den internen Load Balancer zeigen, extern auf den externen, und die WAPs selbst müssen ihn auf den internen Load Balancer auflösen – per eigenem DNS in der DMZ oder per Hosts-Datei. Für die integrierte Windows-Authentifizierung braucht der Name intern einen A-Eintrag, keinen CNAME, sonst fragt der Browser plötzlich nach Kennwörtern.

Zertifikate, Monitoring und Diagnose

Die Zertifikate einer Farm

Wenn eine AD FS-Umgebung ausfällt, ist in meiner Statistik ein Zertifikat der Täter, mit großem Abstand vor allem anderen. Das liegt nicht daran, dass Zertifikate kompliziert wären, sondern daran, dass eine Farm gleich mehrere davon mit unterschiedlichen Laufzeiten, Erneuerungswegen und Abhängigkeiten hat.

Zertifikat	Zweck	Herkunft und Laufzeit	Erneuerung	Wer ist betroffen?
TLS / Service Communication	HTTPS für Föderationsdienst und WAPs	Öffentliche CA, seit März 2026 höchstens 200 Tage	Manuell oder automatisiert: Set-AdfsSslCertificate, Set-WebApplicationProxySslCertificate	Alle Clients, sofort bei Ablauf
Token-Signing	Signatur aller ausgestellten Token	Standard: selbstsigniert, 1 Jahr	Automatisch per AutoCertificateRollover	Alle Relying Parties, die nicht über Metadaten aktualisieren
Token-Decrypting	Entschlüsselung eingehender Token von Claims Providern	Standard: selbstsigniert, 1 Jahr	Automatisch per AutoCertificateRollover	Claims Provider, die für dich verschlüsseln
Proxy-Trust	Authentifizierung des WAP an der Farm	Von der Farm ausgestellt, kurze Laufzeit	Automatisch durch den WAP	Einzelner WAP nach langer Abwesenheit
Entra-MFA-Mandantenzertifikat	Kommunikation des MFA-Adapters mit Entra ID	Selbstsigniert, 2 Jahre	Manuell mit New-AdfsAzureMfaTenantCertificate - Renew	Alle Anmeldungen mit Entra-MFA über AD FS

Bei den TLS-Zertifikaten hat sich die Lage verschärft. Öffentliche CAs stellen seit dem 15. März 2026 Serverzertifikate mit höchstens 200 Tagen Laufzeit aus, ab März 2027 sind es 100 Tage, ab März 2029 nur noch 47. Wer bisher einmal im Jahr am Freitagnachmittag ein Zertifikat auf vier

Server kopiert hat, macht das bald alle paar Wochen. Spätestens jetzt brauchst du ein Skript, das das neue Zertifikat auf allen AD FS-Servern und allen WAPs einspielt, die Bindungen setzt und den Fingerabdruck prüft. Denke daran: Wegen Extended Protection müssen Farm und Proxys denselben Schlüssel verwenden.

Automatischer Rollover und seine Nebenwirkungen

Mit den Standardwerten erzeugt AD FS 20 Tage vor Ablauf ein neues Token-Signing- und ein neues Token-Decrypting-Zertifikat. Beide sind zunächst sekundär, das alte signiert weiter, das neue steht aber schon in den Metadaten. Fünf Tage später wird das neue primär und signiert ab sofort alle Token. Relying Parties, die Metadaten automatisch abrufen, merken davon nichts. Alle anderen lehnen ab diesem Moment jedes Token ab.

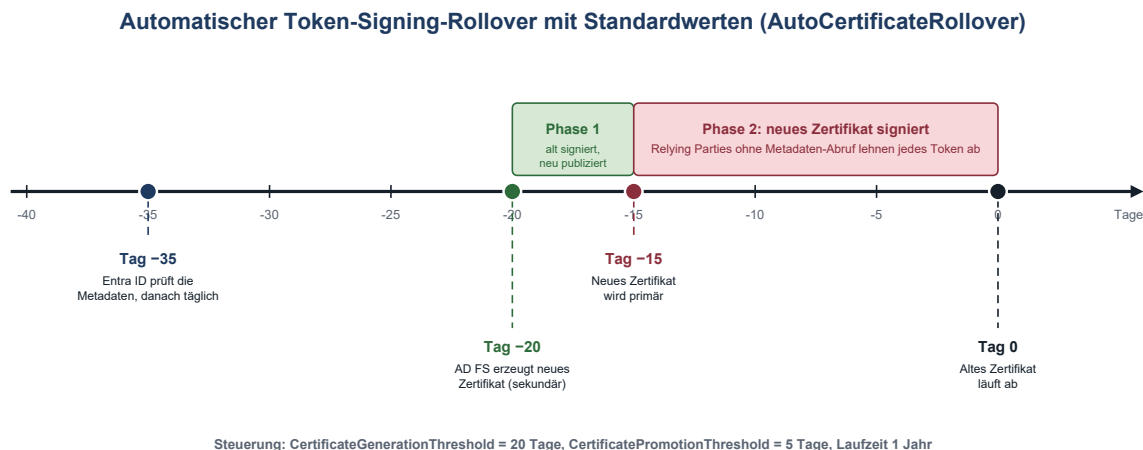


Abbildung 3: Zeitachse des automatischen Zertifikats-Rollovers. Kritisch ist nicht der Ablauf, sondern der Tag, an dem das neue Zertifikat primär wird.

Daraus ergibt sich der eigentliche Arbeitsauftrag: Du brauchst eine Liste aller Relying Parties mit der Angabe, wie sie das neue Zertifikat bekommen. Bei einem SaaS-Dienst, der deine Metadaten-Adresse kennt, steht dort „automatisch“. Bei der Fachanwendung, in die jemand vor drei Jahren eine .cer-Datei hochgeladen hat, steht „manuell, Ansprechperson, Pfad im Admin-Menü“. Für die manuellen Fälle legst du die Promotion bewusst in ein Wartungsfenster: AutoCertificateRollover bleibt aktiv, du erzeugst das neue Zertifikat früh mit Update-AdfsCertificate, verteilst es in Ruhe an die Anwendungsverantwortlichen und machst es erst am vereinbarten Tag mit Set-AdfsCertificate - IsPrimary primär.

Warnung

Führe Update-AdfsCertificate -Urgent nur aus, wenn ein Signaturschlüssel kompromittiert ist. Der Schalter ersetzt die Zertifikate sofort, ohne Übergangsphase – jede Relying Party ohne Metadaten-Abruf ist in derselben Sekunde abgeschnitten. Für Microsoft 365 gibt es dafür eine eigene Notfall-Rotation, die du einmal in Ruhe gelesen haben solltest, bevor du sie brauchst.

Und die Ablaufwarnungen? AD FS schreibt rechtzeitig Ereignisse ins Admin-Protokoll, Entra ID verschickt E-Mails an die technischen Kontakte des Mandanten, und Entra Connect Health zeigt Warnungen an. Das Problem ist selten die fehlende Warnung, sondern der Empfänger. Leite die Hinweise an ein Ticket-System oder ein überwacht Team-Postfach, nicht an die Adresse einer Person, und prüfe die Laufzeiten zusätzlich aktiv: Ein geplanter Task, der Get-AdfsCertificate auswertet und bei weniger als 45 Tagen Restlaufzeit alarmiert, kostet zehn Zeilen PowerShell.

Fakten: Zertifikats-Standardwerte

- AutoCertificateRollover: aktiv (Get-AdfsProperties).
- CertificateGenerationThreshold: 20 Tage vor Ablauf wird ein neues Zertifikat erzeugt.
- CertificatePromotionThreshold: 5 Tage nach Erzeugung wird es primär.
- CertificateDuration: 365 Tage für selbstsignierte Token-Signing- und Token-Decrypting-Zertifikate.
- Entra ID prüft die Metadaten 35 Tage vor Ablauf und danach täglich.
- Die privaten Schlüssel liegen verschlüsselt in der Konfigurationsdatenbank; der Schlüssel dafür (DKM) liegt im Active Directory.

Ereignisprotokolle und Auditing

AD FS protokolliert in zwei Welten. Das Admin-Protokoll unter „Anwendungs- und Dienstprotokolle > AD FS > Admin“ zeigt Fehler und Zustände des Dienstes. Die Audit-Ereignisse zur Token-Ausstellung landen dagegen im Sicherheitsprotokoll – aber nur, wenn du das Auditing vollständig einschaltest. Dazu gehören drei Dinge: Das Dienstkonto braucht das Recht „Generieren von Sicherheitsüberwachungen“, die Unterkategorie „Anwendungsgeneriert“ muss per auditpol für Erfolg und Fehler aktiv sein, und in AD FS selbst legst du die Audit-Stufe mit Set-AdfsProperties - AuditLevel fest. Ohne den zweiten Schritt herrscht im Sicherheitsprotokoll Stille, und du wunderst dich, warum dein SIEM nichts sieht.

Ereignis-ID	Protokoll	Bedeutung	Wofür du es nutzt
1200	Sicherheit	Token erfolgreich ausgestellt	Nutzungsstatistik je Relying Party, Inventar für die Migration
1201	Sicherheit	Token-Ausstellung fehlgeschlagen	Fehlkonfigurierte Regeln, verweigerter Zugriff
1202	Sicherheit	Neue Anmeldedaten erfolgreich geprüft	Anmeldevolumen, Herkunft
1203	Sicherheit	Prüfung neuer Anmeldedaten fehlgeschlagen	Falsche Kennwörter, Passwort-Spraying, Lockout-Ursachen
364	Admin	Fehler bei einer passiven Anfrage	Erster Blick bei jeder Fehlerseite; enthält die Aktivitäts-ID
342 / 411	Admin	Token-Validierung fehlgeschlagen	Typisch bei falschen Kennwörtern über WS-Trust und Legacy-Clients
516	Admin	Extranet-Sperre greift für ein Konto	Gesperrte Konten am Perimeter erkennen
385	Admin	Zertifikate müssen aktualisiert werden oder laufen bald ab	Frühwarnung für den Rollover

Tipp

Jede AD FS-Fehlerseite zeigt eine Aktivitäts-ID. Lass dir von der betroffenen Person einen Screenshot schicken und suche diese ID im Admin- und im Sicherheitsprotokoll aller Knoten. Damit landest du in Sekunden beim richtigen Server und beim richtigen Ereignis, statt dich durch Tausende Einträge zu scrollen.

Account-Lockout durch fehlerhafte Clients und Legacy-Authentifizierung

Der Klassiker unter den Supporttickets: „Mein Konto wird ständig gesperrt.“ Dahinter steckt fast nie ein Hacker mit persönlichem Interesse, sondern ein altes Smartphone in der Schublade, ein Drucker mit hinterlegtem Kennwort oder ein Skript mit Anmeldedaten von 2019. Das Gerät versucht unermüdlich, sich mit dem alten Kennwort über einen WS-Trust-Endpunkt anzumelden, AD FS prüft jedes Mal gegen den DC, und die Sperrschwelle im AD ist schneller erreicht, als die Person ihr neues Kennwort tippen kann. Wird die Farm zusätzlich per Passwort-Spraying angegriffen, sperrt ein Angreifer auf diesem Weg gezielt Konten aus.

Die Antwort heißt Extranet Smart Lockout. AD FS führt dann eine eigene Sperrzählung für Anmeldungen über den Proxy und unterscheidet zwischen vertrauten Orten, von denen sich jemand schon erfolgreich angemeldet hat, und unbekannten. Angriffe aus unbekannten Netzen sperren nur den unbekannten Zugang, die Person im Büro oder im gewohnten Homeoffice kommt weiter hinein. Die Schwelle in AD FS muss unter der Sperrschwelle des AD liegen, sonst kommt der Schutz zu spät.

```
# Erst beobachten, dann erzwingen
Set-AdfsProperties -EnableExtranetLockout $true -ExtranetLockoutThreshold 10 `
    -ExtranetObservationWindow (New-TimeSpan -Minutes 30) -ExtranetLockoutMode
AdfsSmartLockoutLogOnly
# nach einigen Tagen Auswertung
Set-AdfsProperties -ExtranetLockoutMode AdfsSmartLockoutEnforce

# Einzelnes Konto analysieren und zurücksetzen
Get-AdfsAccountActivity -Identity anna.berger@contoso.com
Reset-AdfsAccountLockout -Identity anna.berger@contoso.com -Location Unknown
```

Parallel räumst du die Ursachen ab. Exchange Online hat die Basic Authentication für die klassischen Protokolle längst abgeschaltet, trotzdem tauchen über die WS-Trust-Endpunkte noch Altlasten auf. Schließe am WAP alle Endpunkte, die niemand nutzt – insbesondere die usernamemixed-Varianten, wenn keine Anwendung sie braucht –, und werte Ereignis 1203 nach Quell-IP und Benutzeragent aus. Gesperrte IP-Bereiche pflegst du über die Eigenschaft BannedIpList. Der nachhaltigste Schritt ist allerdings, Kennwörter zu ersetzen: Mit MFA oder kennwortlosen Verfahren als primärer Methode laufen Spraying-Angriffe ins Leere.

Analyse-Werkzeuge

Werkzeug	Was es leistet	Hinweis
Microsoft Entra Connect Health für AD FS	Agent auf AD FS und WAP: Nutzungsanalysen je Anwendung, Fehlanmeldungen, Bericht über riskante IP-Adressen, Warnungen	Erfordert Entra ID P1; liefert auch die Datenbasis für den Migrationsbericht
ADFSToolbox (PowerShell-Galerie)	Diagnostics Analyzer mit Konfigurations- und Gesundheitsprüfungen, Ereignisauswertung über alle Knoten	Ideal für den Health-Check vor Wartung und Migration
Test-Relying-Party „Claims X-Ray“	Zeigt, welche Claims ein Token tatsächlich enthält	Spart Stunden beim Debuggen von Regeln; nur mit Testkonten verwenden
IdP-initiierte Anmeldeseite	Schneller Funktionstest unter /adfs/ls/idpinitiatedsignon.aspx	Standardmäßig deaktiviert; nur temporär für Tests einschalten
Sicherheitsprotokoll im SIEM	Korrelation von 1200 bis 1203 mit Anmeldungen in Entra ID	Grundlage für Angriffserkennung und Kapazitätsplanung

Geo-Redundanz, Disaster Recovery und Lifecycle

Azure Traffic Manager: eine eigene Architekturentscheidung

Eine Farm mit zwei Knoten im selben Rechenzentrum schützt gegen den Ausfall eines Servers, nicht gegen den Ausfall des Standorts. Für standortübergreifende Verfügbarkeit beschreibt Microsoft eine Variante mit Azure Traffic Manager: Die Farm wird mit WAPs, Load Balancern und eigenen Domänencontrollern in zwei Azure-Regionen aufgebaut, der öffentliche Föderationsname wird per CNAME auf ein Traffic-Manager-Profil gelegt, und Traffic Manager verteilt die Clients per DNS auf die Regionen. Als Routing stehen Priorität, Performance und Gewichtung zur Verfügung; Microsoft empfiehlt Performance, für eine Aktiv-Passiv-Auslegung ist Priorität ehrlicher. Die Regionen brauchen untereinander keine direkte Verbindung für die Anmeldung, wohl aber für die AD- und Datenbankreplikation.

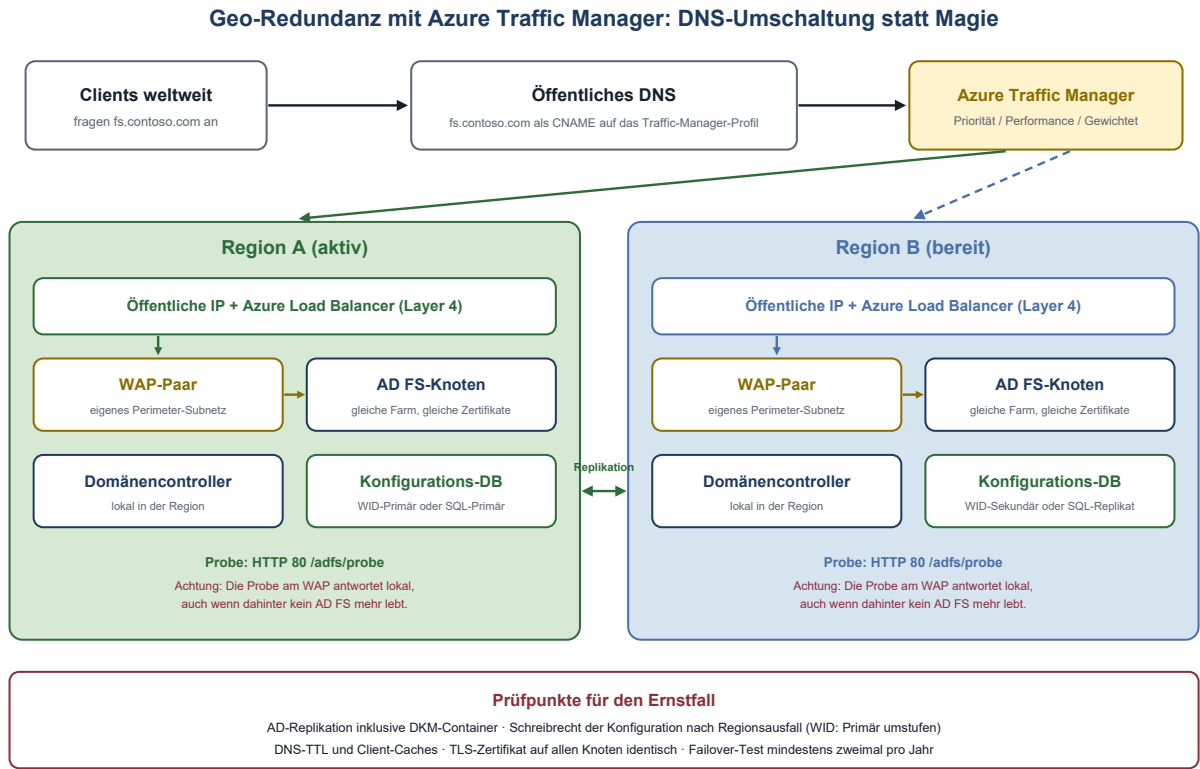


Abbildung 4: Geo-redundante AD FS-Farm mit Azure Traffic Manager. Die Umschaltung erfolgt per DNS; Replikation von AD und Konfiguration bleibt deine Aufgabe.

Klingt elegant, ist aber keine Option, die man nebenbei aktiviert. Traffic Manager arbeitet ausschließlich auf DNS-Ebene. Clients verbinden sich direkt mit dem Endpunkt, den sie aufgelöst haben, und behalten ihn, bis TTL und lokale Caches abgelaufen sind. Ein Failover dauert also Minuten, nicht Sekunden. Gravierender ist ein Detail, das ich in fast jedem Konzept vermisste: Traffic Manager prüft die Endpunkte über HTTP Port 80 und den Pfad /adfs/probe – und genau diese Probe beantwortet der WAP lokal, ohne das Backend zu fragen. Liegt in Region A die Farm am Boden, die WAPs aber laufen, meldet Region A sich weiter als gesund und bekommt weiter Datenverkehr. Du brauchst also entweder eine Probe, die einen echten Anmeldepfad prüft, oder ein Verfahren, mit dem der Betrieb die Region bewusst deaktiviert.

Variante	Schützt gegen	Aufwand	Wann sinnvoll
Farm in einem Standort	Ausfall einzelner Server	Gering	Wenn PHS als Rückfallebene für M365 aktiv ist und lokale Apps einen Standortausfall verkraften

Variante	Schützt gegen	Aufwand	Wann sinnvoll
Farm über zwei eigene Rechenzentren	Server- und Standortausfall	Mittel bis hoch	Wenn ohnehin zwei Standorte mit AD-Präsenz und Layer-4-Load-Balancing existieren
Geo-Farm in Azure mit Traffic Manager	Regionsausfall, Latenz für weltweite Nutzer	Hoch	Weltweit verteilte Organisationen mit vielen Anwendungen, die nicht kurzfristig nach Entra ID können
Umstellung auf verwaltete Authentifizierung	Ausfall der gesamten Farm für M365	Gering	Als Notfallplan immer; als Zielbild für die M365-Anmeldung in den meisten Fällen

Anforderungen an Zertifikats- und Konfigurationsreplikation

Damit beide Regionen gleichwertig sind, müssen sie dieselben Token mit demselben Schlüssel ausstellen. Innerhalb einer Farm ist das automatisch so: Die Zertifikate liegen in der gemeinsamen Konfigurationsdatenbank, verschlüsselt mit dem DKM-Schlüssel aus dem Active Directory. Daraus folgen drei Bedingungen. Die AD-Replikation zwischen den Regionen muss funktionieren, inklusive des DKM-Containers. Die Konfigurationsdatenbank muss in beiden Regionen verfügbar sein: Bei WID steht der Primärserver nur in einer Region, nach deren Ausfall laufen Anmeldungen weiter, aber Änderungen und Zertifikats-Rollover erst nach dem Umstufen. Bei SQL Server brauchst du eine Verfügbarkeitsgruppe mit Replikat in der zweiten Region und einen Plan für das Failover über Regionsgrenzen. Und das TLS-Zertifikat muss auf allen Knoten und allen WAPs beider Regionen identisch sein – bei 200 Tagen Laufzeit ein starkes Argument für Automatisierung.

Zwei unabhängige Farmen mit demselben Dienstnamen sind übrigens keine Abkürzung. Sie müssten dieselben Token-Signing- und Token-Decrypting-Zertifikate tragen, also mit abgeschaltetem automatischen Rollover und exportierten Schlüsseln betrieben werden, und jede Regeländerung doppelt gepflegt. Das ist fehleranfällig und vergrößert die Angriffsfläche für die wertvollsten Schlüssel deiner Organisation. Wenn Schlüsselschutz ein Thema ist – und das sollte er sein –, gehört ein Hardware-Sicherheitsmodul in die Diskussion, und das muss dann ebenfalls in beiden Regionen erreichbar sein.

Regelmäßige Failover-Tests als Prüfpunkt

Ein Notfallplan, der nie geprobt wurde, ist eine Vermutung mit Inhaltsverzeichnis. Ich habe Umgebungen gesehen, in denen das Failover-Konzept perfekt dokumentiert war und beim ersten echten Test scheiterte, weil der DMZ-Server in Region B seit acht Monaten ausgeschaltet war und sein Proxy-Trust abgelaufen. Plane Tests mindestens zweimal im Jahr, bei Geo-Architekturen besser vierteljährlich, und behandle jedes Ergebnis wie einen Befund.

Prüfpunkt	Wie testen	Erfolgskriterium
Knotenausfall	AD FS- und WAP-Knoten nacheinander am Load Balancer entleeren und stoppen	Anmeldungen laufen ohne Unterbrechung weiter
Regionswechsel	Region A im Traffic Manager deaktivieren oder Farm dort stoppen	Anmeldung nach DNS-TTL über Region B; Probe-Verhalten dokumentiert
Datenbank-Failover	WID: Sekundär zum Primär umstufen; SQL: geplantes AG-Failover	Konfigurationsänderung danach möglich, kein Anmeldeabbruch
Proxy-Trust	Selten genutzte WAPs einschalten und Konfigurationsabruf prüfen	Kein Fehler im WAP-Protokoll, keine Neuinstallation nötig

Prüfpunkt	Wie testen	Erfolgskriterium
Zertifikate	Restlaufzeiten aller Zertifikate auf allen Knoten auslesen	Identische Fingerabdrücke, keine Laufzeit unter 45 Tagen
Rückfallebene M365	Testdomäne oder Staged Rollout mit Testgruppe auf PHS umstellen	Anmeldung über Entra ID funktioniert, Ablauf und Dauer bekannt
Wiederherstellung	Konfiguration mit dem AD FS Rapid Restore Tool sichern und in Testumgebung zurückspielen	Farm aus Sicherung lauffähig, Schlüssel verfügbar

Versionen, Updates und die Abhängigkeit zwischen AD FS und WAP

Die Version einer Farm wird durch das Farmverhaltensniveau (Farm Behavior Level, FBL) bestimmt, nicht durch das Betriebssystem einzelner Knoten. Das höchste Niveau ist seit Windows Server 2019 unverändert; Knoten auf Windows Server 2022 und 2025 bringen Sicherheitsverbesserungen und eine aktuelle Plattform mit, aber kein neues FBL. Der übliche Upgrade-Weg: neue Knoten auf aktuellem Betriebssystem zur Farm hinzufügen, den Primärserver bei WID auf einen neuen Knoten verlegen, alte Knoten entfernen, mit Test-AdfsFarmBehaviorLevelRaise prüfen und mit Invoke-AdfsFarmBehaviorLevelRaise anheben.

Die WAPs müssen dabei mitziehen. Ein WAP älterer Generation lässt sich nicht an eine Farm mit höherem FBL anbinden – ein Proxy auf Windows Server 2012 R2 funktioniert nicht mit einer Farm ab FBL 2016. Hebe daher erst alle WAPs auf die neue Version, setze anschließend mit Set-WebApplicationProxyConfiguration die Konfigurationsversion und erhöhe danach das FBL. Bei den Updates gilt: AD FS und WAP erhalten ihre Korrekturen über die monatlichen kumulativen Updates von Windows Server. Ein vierteljährlicher Patchzyklus ist für eine Tier-0-Komponente mit Internetanschluss zu langsam. Patche knotenweise, mit Entleeren am Load Balancer, und prüfe nach jedem Knoten die Probe und eine Testanmeldung.

Warnung

Windows Server 2016 verlässt am 12. Januar 2027 den erweiterten Support, Windows Server 2012 R2 ist bereits seit Oktober 2023 ohne reguläre Sicherheitsupdates. Eine Farm oder ein WAP auf diesen Versionen ist ein Internet-exponierter Identitätsdienst ohne Patches. Das ist kein Lifecycle-Thema mehr, sondern ein Sicherheitsvorfall mit Ansage.

Ablöse statt Weiterbetrieb: realistische Kriterien

Microsofts Position ist eindeutig: Neue Funktionen entstehen in Entra ID, und statt eine Farm auf die nächste Version zu heben, solltest du Anwendungen dorthin migrieren. Das heißt nicht, dass jede Farm morgen abgeschaltet werden muss. Es heißt, dass jede Investition in AD FS eine Begründung braucht. Der Umstieg erfolgt in der Regel in zwei Strängen. Für Microsoft 365 stellst du die Anmeldung auf PHS oder PTA um, zuerst mit Staged Rollout für Pilotgruppen, dann für die gesamte Domäne. Für die übrigen Relying Parties hilft der Bericht zur AD FS-Anwendungsmigration im Entra Admin Center, der mit Daten aus Connect Health für jede Anwendung zeigt, ob ihre Regeln in Entra ID abbildbar sind. Moderne SAML- und OIDC-Anwendungen ziehen zuerst um, Legacy-Anwendungen über den Entra-Anwendungsproxy oder Partnerlösungen für sicheren Hybridzugriff zuletzt. Während der Koexistenz laufen beide Welten parallel; die Farm schrumpft mit jeder umgezogenen Anwendung.

Kriterium	Spricht für Ablöse	Spricht für Weiterbetrieb (vorerst)
Hauptzweck	Farm existiert überwiegend für die M365-Anmeldung	Viele lokale Anwendungen mit komplexen Regeln ohne Entra-Äquivalent
Betriebsbasis	Knoten auf Windows Server 2016 oder älter, Hardware am Ende	Aktuelle Plattform, geübter Betrieb, gepflegte Dokumentation
Sicherheitsanforderung	Conditional Access, Risikoerkennung, kennwortlose Anmeldung gewünscht	Auflage, ohne Cloud-Abhängigkeit zu authentifizieren
Know-how	Wissen hängt an einer Person, Regeln sind undokumentiert	Team beherrscht Regeln, Zertifikate und Fehlersuche
Partnerföderation	Partner nutzen Cloud-Anwendungen, Entra External ID passt	Partner-IdPs für lokale Anwendungen, die nicht migrieren können
Kosten	Server, Lizenzen, Load Balancer, Zertifikate, Bereitschaft	Migrationsaufwand je Anwendung übersteigt den Betriebsaufwand deutlich

Meine Erfahrung aus Migrationsprojekten: Die Technik ist selten das Problem. Schwierig wird es bei den Anwendungen, deren Verantwortliche niemand mehr kennt, und bei Claim-Regeln, die eine Geschäftslogik enthalten, die nirgends sonst dokumentiert ist. Ein Inventar auf Basis der Ereignisse 1200 – welche Relying Party wurde in den letzten 90 Tagen überhaupt genutzt? – räumt regelmäßig ein Drittel der Trusts als tot ab. Genau an dieser Stelle lohnt sich ein Architektur-Review mit externer Unterstützung, weil ein unbeteiligter Blick die Altlasten schneller sieht als das Team, das sie seit Jahren mit sich trägt.

Fazit

Active Directory Federation Services ADFS ist ausgereift, gut verstanden und für viele Organisationen weiterhin ein tragendes Stück Infrastruktur. Wer die Farm betreibt, betreibt allerdings ein Tier-0-System mit Internetanschluss und den wertvollsten Signaturschlüsseln des Unternehmens. Hochverfügbarkeit entsteht dabei nicht durch einen zweiten Server, sondern durch ein Gesamtbild: Layer-4-Load-Balancing ohne TLS-Terminierung, die passende Konfigurationsdatenbank, WAPs mit gepflegtem Proxy-Trust, dokumentierte Netzwerkflüsse, ein Zertifikatsprozess, der kürzere TLS-Laufzeiten und den jährlichen Signatur-Rollover aushält, Auditing, das tatsächlich im SIEM ankommt, und Failover-Tests, die regelmäßig stattfinden.

Geo-Redundanz mit Azure Traffic Manager ist dabei eine eigene, aufwendige Architekturentscheidung und kein Häkchen in einer Checkliste. Für Microsoft 365 ist die bessere Rückfallebene fast immer Passwort-Hash-Sync – und oft auch das bessere Zielbild. Die ehrliche Bilanz für die meisten Umgebungen lautet daher: Betreibe die Farm so gut, dass sie dich nicht nachts weckt, und nutze die gewonnene Ruhe, um ihren Aufgabenbereich Anwendung für Anwendung nach Entra ID zu verlagern. Die Farm, die am zuverlässigsten läuft, ist am Ende die, die du nicht mehr brauchst.

FAQ: Häufige Fragen zu Architektur und Hochverfügbarkeit von ADFS

Was sind Active Directory Federation Services?

AD FS ist eine Serverrolle von Windows Server, die als Identity Provider und Security Token Service arbeitet. Sie authentifiziert Personen gegen das lokale Active Directory und stellt signierte

Token mit Claims aus, mit denen sich Anwendungen außerhalb der Domäne per Single Sign-On anmelden lassen – über SAML 2.0, WS-Federation, OAuth 2.0 oder OpenID Connect.

Wie viele AD FS-Server brauche ich für Hochverfügbarkeit?

Mindestens zwei AD FS-Server im internen Netz und zwei WAPs in der DMZ, jeweils hinter einem Layer-4-Load-Balancer. Die Kapazität richtet sich nach der CPU-Last zu Spitzenzeiten; Microsoft stellt dafür ein Planungsblatt bereit. Speicher und Plattenplatz sind unkritisch: 4 GB RAM und 100 GB Platte sind die empfohlene Größe pro Knoten.

Bis zu welcher Größe reicht die Windows Internal Database?

Bis 30 AD FS-Server in der Farm und höchstens 100 Relying Party Trusts. Die Zahl der Benutzerkonten spielt keine Rolle. SQL Server brauchst du darüber hinaus, für SAML-Artefakt-Auflösung, für Token-Replay-Erkennung oder wenn alle Knoten Konfigurationsänderungen schreiben sollen.

Kann ich das Azure Application Gateway vor den Web Application Proxy stellen?

Nein. Das Application Gateway terminiert TLS, und das wird für AD FS in keinem Anwendungsfall unterstützt. Zertifikatsanmeldung und Extended Protection brechen damit. In Azure gehört ein Layer-4-Load-Balancer vor die WAPs, für die Verteilung über Regionen kommt Azure Traffic Manager auf DNS-Ebene hinzu.

Muss der WAP dieselbe Windows-Server-Version haben wie die Farm?

Der WAP muss zum Farmverhaltensniveau passen. Ein älterer Proxy lässt sich nicht an eine Farm mit höherem FBL anbinden. Hebe deshalb vor dem Anheben des FBL alle WAPs auf die neue Version, setze die Konfigurationsversion und erhöhe erst dann das FBL der Farm.

Was passiert beim automatischen Rollover des Token-Signing-Zertifikats?

AD FS erzeugt mit den Standardwerten 20 Tage vor Ablauf ein neues Zertifikat und macht es fünf Tage später primär. Microsoft 365 und Anwendungen mit Metadaten-Abruf übernehmen es automatisch. Anwendungen mit manuell hinterlegtem Zertifikat lehnen ab der Promotion alle Token ab, bis jemand das neue Zertifikat einträgt.

Warum wird ein Konto immer wieder gesperrt, obwohl die Person ihr Kennwort richtig eingibt?

Meist versucht ein Gerät oder Programm mit einem alten, gespeicherten Kennwort die Anmeldung über AD FS, etwa ein Smartphone, ein Drucker oder ein Skript. Ereignis 1203 im Sicherheitsprotokoll und Get-AdfsAccountActivity zeigen Quell-IP und Häufigkeit. Extranet Smart Lockout verhindert, dass Fehlversuche aus unbekannten Netzen das AD-Konto sperren.

Lohnt sich eine geo-redundante Farm mit Azure Traffic Manager?

Nur, wenn viele geschäftskritische Anwendungen weltweit von AD FS abhängen und nicht kurzfristig nach Entra ID umziehen können. Für Microsoft 365 ist Passwort-Hash-Sync als Rückfallebene deutlich günstiger und robuster. Wer Traffic Manager einsetzt, muss beachten, dass die Standard-Probe am WAP das Backend nicht prüft, und das Failover regelmäßig testen.

Sollte ich AD FS noch auf Windows Server 2025 aktualisieren oder gleich migrieren?

Microsoft empfiehlt die Migration nach Entra ID statt eines Upgrades. Läuft die Farm auf Windows Server 2016 oder älter und dient sie hauptsächlich der M365-Anmeldung, ist die Ablöse fast immer der bessere Weg. Gibt es viele lokale Anwendungen ohne kurzfristige

Migrationsperspektive, ist ein Plattformwechsel auf Windows Server 2022 oder 2025 als Übergangslösung vertretbar – mit festem Migrationsplan.