

ADFS abschalten – die Farm sauber außer Betrieb nehmen

ADFS · Außerbetriebnahme · Rückbau

Der letzte Dienst, den du deiner Farm erweist

Nachweis, Beobachtung, Rückbau, Aufräumen: Wie du ADFS so abschaltest, dass hinterher niemand nach einem Server fragt, den es nicht mehr gibt.

boddenberg.de



WISSEN

Grundlagen, Architektur und alle Praxisbeiträge rund um ADFS an einem Ort.

› [Active Directory Federation Services](#)

BERATUNG

Du willst die Farm abschalten, aber niemand kann garantieren, dass nichts mehr dranhängt? Wir machen den Nachweis mit dir.

› [Consulting zu ADFS](#)

SCHULUNG

Inventar, Migration, Rückbau: der ganze Ausstieg aus ADFS einmal im Labor, bevor du es in Produktion machst.

› [ADFS-Schulungen](#)

Es gibt diesen Moment am Ende jeder Migration. Microsoft 365 läuft seit Wochen über Password Hash Sync, die SAML-Anwendungen hängen an Entra ID, das Projekt ist offiziell abgeschlossen, und im Rechenzentrum surren immer noch zwei ADFS-Server und zwei Web Application Proxies vor sich hin. Niemand traut sich, sie auszuschalten. Nicht, weil jemand an ihnen hängt, sondern weil niemand sicher sagen kann, dass nicht doch irgendetwas an ihnen hängt. Also laufen sie weiter, bekommen Patches, erneuern brav ihre Zertifikate und werden zu dem, was man in der Medizin einen Wachkomapatienten nennen würde: Vitalfunktionen stabil, Aufgabe unklar.

Dieser Beitrag ist für genau diesen Moment. Er zeigt dir, wie du ADFS abschaltest und dekommissionierst, ohne dass in drei Monaten die Buchhaltung anruft, weil der Monatsabschluss in einer Anwendung hängt, von der nie jemand wusste, dass sie gefördert ist. Es geht um den Nachweis, dass keine Anmeldungen mehr kommen, um einen ehrlichen Beobachtungszeitraum, um den Umzug der WAP-Veröffentlichungen, um DNS, Zertifikate, Dienstkonto und DKM-Container im Active Directory, um Firewall-Regeln und um die Dokumentation, die hinterher niemand lesen will, bis sie jemand braucht.

Eine Sache vorweg, damit kein falscher Eindruck entsteht: ADFS ist nicht tot. Viele Unternehmen betreiben ihre Farm seit über zehn Jahren, stabil und gut gehärtet, und haben gute Gründe, das weiter zu tun. Wer dazugehört, findet die Grundlagen und den sauberen Betrieb auf der Übersichtsseite [Active Directory Federation Services](#). Dieser Beitrag richtet sich an alle, die den Ausstieg bereits hinter sich haben und jetzt nur noch den letzten Schritt gehen müssen – den, den viele am längsten vor sich herschieben.

FAKTEN – ADFS-Außerbetriebnahme in Kürze

Microsoft beschreibt die Außerbetriebnahme in einem eigenen Leitfaden. Voraussetzung: Benutzer-authentifizierung und alle Anwendungen sind nach Entra ID migriert, und auf der Farm gibt es keine Relying Party mehr mit Verkehr.

Für den Nachweis nennt Microsoft die ADFS-Ereignisprotokolle und Microsoft Entra Connect Health. Connect Health soll mindestens eine Woche laufen, nach der Umstellung der Authentifizierung soll die Umgebung ebenfalls mindestens eine Woche getestet werden. Das ist die Untergrenze, keine Empfehlung für dich.

Die Reihenfolge laut Microsoft: optionales letztes Backup, Load-Balancer-Einträge entfernen, DNS-Einträge löschen, CertificateSharingContainer notieren, SQL-Datenbank löschen, WAP deinstallieren, ADFS beginnend mit den Sekundärknoten deinstallieren, SSL-Zertifikate löschen, Server neu aufsetzen, ADFS-Konto löschen, DKM-Container leeren.

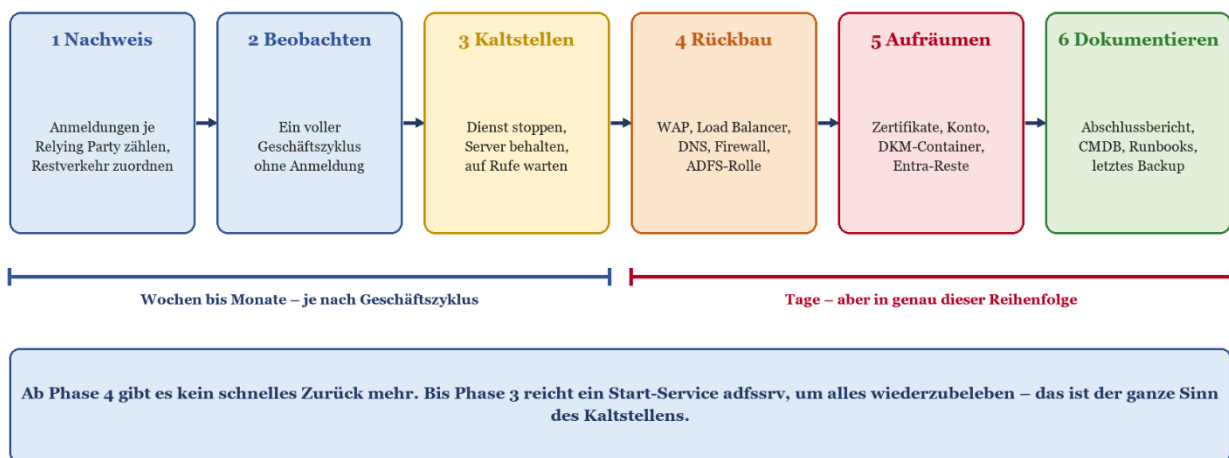
Der Web Application Proxy speichert seine Konfiguration in der ADFS-Konfiguration. Ohne ADFS gibt es keinen WAP – also müssen auch Veröffentlichungen umziehen, die mit ADFS-Authentifizierung gar nichts zu tun haben.

Der Nachweis: Kommt wirklich keine Anmeldung mehr?

Bevor du irgendetwas abbaust, brauchst du eine belastbare Antwort auf eine einzige Frage: Stellt diese Farm noch Tokens aus, und wenn ja, für wen? Belastbar heißt: nicht „glaube ich nicht“, nicht „steht nicht im Inventar“, sondern gemessen, je Relying Party, über einen Zeitraum, der auch die seltenen Prozesse einschließt. Das Inventar aus der Migrationsphase ist dafür der Ausgangspunkt, nicht der Beweis. Wie du es aufbaust, beschreibt [Relying Parties inventarisieren – die Bestandsaufnahme vor der Entra-Migration](#).

Skizze 1: Sechs Phasen bis zum letzten Handgriff

Die ersten drei Phasen kosten Zeit, die letzten drei kosten nur Sorgfalt



Skizze 1: Die sechs Phasen der Außerbetriebnahme. Bis zum Kaltstellen ist alles mit einem Dienststart umkehrbar, danach nicht mehr.

Was die Farm selbst über ihre Nutzung verrät

ADFS schreibt ab Windows Server 2016 mit der Standard-Auditstufe Basic Ereignisse der Quelle „AD FS Auditing“ ins Sicherheitsprotokoll – vorausgesetzt, die Überwachungsrichtlinie für „Anwendung generiert“ ist für Erfolg und Fehler aktiv und das Dienstkonto darf Sicherheitsüberwachungen erzeugen. Für deinen Nachweis zählen vor allem vier Ereignisse: 1200 (Token erfolgreich ausgestellt), 1201 (Tokenausstellung fehlgeschlagen), 1202 (frische Anmeldedaten erfolgreich geprüft) und 1203 (Prüfung frischer Anmeldedaten fehlgeschlagen). Die Ereignisse enthalten im XML-Teil unter anderem die Relying Party, für die angefragt wurde. Wie

du diese Ereignisse liest und was die anderen Protokolle hergeben, steht ausführlich in [ADFS-Ereignisprotokolle lesen – Admin-Log, Debug-Tracing und Auditing](#).

Der Haken: Das Sicherheitsprotokoll ist auf ausgelasteten Servern schnell überschrieben. Wenn du über Wochen zählen willst, brauchst du entweder eine Weiterleitung in dein SIEM oder ein kleines Skript, das täglich zusammenfasst. Das folgende Beispiel läuft auf jedem ADFS-Knoten und zählt Tokenausstellungen je Relying Party für die letzten 24 Stunden.

```
# Auf jedem ADFS-Knoten ausführen – Tokenausstellungen je Relying Party, letzte 24 Stunden
$seit = (Get-Date).AddDays(-1)
Get-WinEvent -FilterHashtable @{
    LogName       = 'Security'
    ProviderName = 'AD FS Auditing'
    Id            = 1200, 1201
    StartTime     = $seit
} -ErrorAction SilentlyContinue |
    ForEach-Object {
        if ($_.ToXml() -match '<RelyingParty>(.*?)</RelyingParty>') { $Matches[1] } else {
            '(unbekannt)'
        }
        Group-Object | Sort-Object Count -Descending |
        Select-Object Count, Name |
        Export-Csv "C:\Temp\adfs-rp-nutzung-$(Get-Date).ToString('yyyyMMdd')-
$env:COMPUTERNAME.csv" -
        -NoTypeInformation -Encoding UTF8
```

Täglich per geplanter Aufgabe ausführen und die CSV-Dateien zentral sammeln. Leere Ergebnisse sind erst dann eine gute Nachricht, wenn die Auditierung nachweislich funktioniert.

WARNUNG – Null Ereignisse heißt nicht null Anmeldungen

Bevor du dich über ein leeres Protokoll freust, prüfe, ob überhaupt protokolliert wird. Get-AdfsProperties zeigt die AuditLevel-Einstellung; auditpol /get /subcategory:"Anwendung generiert" (auf englischen Systemen „Application Generated“) zeigt die Richtlinie. Melde dich zum Test einmal selbst an einer noch vorhandenen Relying Party an und schau, ob dein Ereignis auftaucht. Ein Monat Stille, weil seit der letzten GPO-Änderung niemand mehr auditiert, ist kein Nachweis, sondern ein Missverständnis.

Was Entra Connect Health und die Gegenseite verraten

Wenn der Connect-Health-Agent für ADFS installiert ist, zeigt dir die Nutzungsanalyse im Entra Admin Center Anfragen nach Relying Party, Erfolg und Fehler, ohne dass du Protokolle einsammeln musst. Microsoft nennt genau diese Ansicht als Kriterium: Kommen keine neuen Authentifizierungsanfragen mehr und melden sich alle Benutzer und Clients erfolgreich bei Entra ID an, kann der Microsoft-365-Trust weg. Details zum Agenten findest du in [ADFS überwachen – Health Checks, Diagnose-Toolbox und Entra Connect Health](#).

Mindestens genauso wichtig ist der Blick von der anderen Seite. Prüfe in Entra ID, ob alle Domänen tatsächlich auf Managed stehen und keine Föderationskonfiguration mehr existiert. Das geht mit Microsoft Graph PowerShell in drei Zeilen:

```
Connect-MgGraph -Scopes "Domain.Read.All"
Get-MgDomain | Select-Object Id, AuthenticationType, IsVerified
# Für jede Domäne, die noch "Federated" zeigt:
Get-MgDomainFederationConfiguration -DomainId "contoso.de"
```

Steht irgendwo noch Federated, bist du nicht beim Abschalten, sondern noch mitten in der Migration.

Früher stand an dieser Stelle in jeder Anleitung Get-MsolDomain aus dem MSOnline-Modul. Das Modul ist ausgemustert; wenn dein altes Runbook noch so aussieht, ist das ein guter Zeitpunkt, es

mit zu beerdigen. Wie die Umstellung selbst mit Update-MgDomain und Staged Rollout funktioniert, steht in [Microsoft 365 von Federated auf Managed umstellen – mit Staged Rollout](#).

Die üblichen Verdächtigen für Restverkehr

Wenn nach der Migration noch Anmeldungen kommen, stecken fast immer dieselben Kandidaten dahinter. Die Tabelle hilft dir, Restverkehr schneller zuzuordnen.

Quelle	Woran du sie erkennst	Was zu tun ist
Microsoft-365-Trust	Relying Party „Microsoft Office 365 Identity Platform“ zeigt noch Verkehr	Domäne noch föderiert oder alte Clients mit Legacy-Authentifizierung; Domänenstatus prüfen, Clients aktualisieren
Vergessene SAML-App	Selten genutzte Relying Party mit sporadischen 1200-Ereignissen	Fachbereich suchen, nach Entra ID umziehen: SAML-Anwendungen von ADFS nach Entra ID migrieren
Partner per Claims Provider Trust	Anmeldungen über einen fremden Anspruchsanbieter	Partner informieren, Zugang neu regeln: Claims Provider Trust – Partnerorganisationen anbinden
Gerätebezogene Abläufe	Anfragen an Endpunkte für Geräteregistrierung oder Hybrid Join	Gerätestatus in Entra ID prüfen, alte Join-Pfade und DNS-Einträge ablösen
Monitoring-Sonden	Regelmäßige Anfragen im Minutentakt, immer vom selben System	Kein echter Verkehr; Überwachung umstellen, sonst misst du dich selbst
Skripte und Dienste	Anmeldungen mit Dienstkonten über WS-Trust oder OAuth	Eigentümer finden, auf Entra-App-Registrierung oder verwaltete Identität umstellen

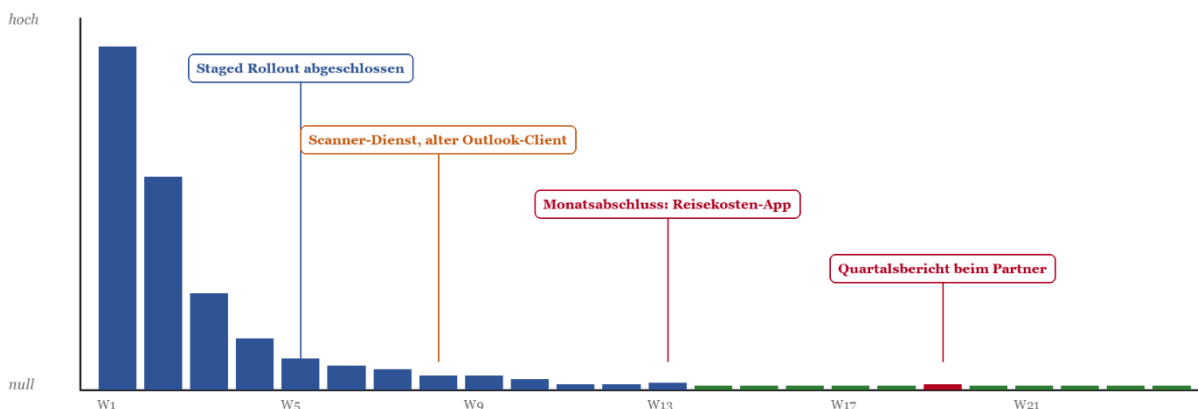
Tabelle 1: Typische Quellen für Restverkehr auf einer eigentlich migrierten Farm

Beobachtungszeitraum und Kaltstellen: Wie lange ist lange genug?

Microsoft nennt eine Woche als Untergrenze. Für eine Testumgebung ist das in Ordnung. Für eine Farm, die zehn Jahre lang Anwendungen gesammelt hat, ist eine Woche ungefähr so aussagekräftig wie ein einzelner Blick aus dem Fenster für die Wettervorhersage des Jahres. Der richtige Zeitraum hängt nicht von ADFS ab, sondern von deinem Geschäft: Er muss den seltensten Prozess einschließen, der über die Farm laufen könnte.

Skizze 3: Wie der Restverkehr typischerweise ausläuft

Schematisches Beispiel: Anmeldungen pro Woche nach der Umstellung von Microsoft 365 auf Managed



Die Nullen in der Mitte sind trügerisch. Der Beobachtungszeitraum muss den seltensten Prozess einschließen, nicht den häufigsten.

Skizze 3: Schematisches Beispiel für auslaufenden Restverkehr. Die gefährlichen Anmeldungen sind die einzelnen Ausreißer lange nach der Umstellung.

Den Zeitraum an den Geschäftszyklus koppeln

Frag die Fachbereiche nicht „Nutzt ihr ADFS?“ – die Antwort ist immer Nein, weil niemand weiß, was ADFS ist. Frag stattdessen nach Prozessen mit festen Rhythmen: Monatsabschluss, Quartalsberichte, Reisekostenabrechnung, Inventur, Jahresabschluss, Gehaltsabrechnung, Zertifizierungsaudits beim Partner. Jeder dieser Prozesse ist ein Kandidat für eine Anwendung, die einmal im Quartal gefördert anmeldet und sonst schweigt.

Ausgangslage	Empfohlener Beobachtungszeitraum	Begründung
Nur Microsoft 365 fördert, keine weiteren Relying Parties	Vier Wochen	Ein Monatswechsel inklusive, Restclients fallen schnell auf
Wenige gut dokumentierte SAML-Anwendungen	Ein bis zwei Monatsabschlüsse	Monatliche Prozesse sicher erfasst
Viele Relying Parties, Partneranbindungen	Ein Quartal	Quartalsprozesse, Partnerberichte, Urlaubszeiten der Eigentümer
Unklare Historie, keine verlässliche Dokumentation	Ein Quartal plus Kaltstellen	Wo die Dokumentation schweigt, muss die Messung länger reden

Tabelle 2: Erfahrungswerte für den Beobachtungszeitraum – keine Microsoft-Vorgabe, sondern Praxis

TIPP — Jährliche Prozesse gezielt abfragen statt abwarten

Niemand wartet ein Jahr auf den Jahresabschluss, nur um ADFS abzuschalten. Für jährliche Prozesse gilt deshalb: Eigentümer gezielt anschreiben, Anwendung nennen, Testanmeldung über Entra ID vereinbaren. Ein erfolgreicher Test im Oktober ist mehr wert als ein ungeprüftes Schweigen bis Januar.

Kaltstellen: der ehrlichste Test, den es gibt

Wenn die Zählung über den Beobachtungszeitraum bei null liegt, schaltest du die Farm nicht ab – du stellst sie kalt. Das heißt: Relying Parties deaktivieren, den ADFS-Dienst auf allen Knoten stoppen und den Starttyp auf Deaktiviert setzen, die Server aber unverändert stehen lassen. In der Branche heißt das gern „Scream Test“: Du schaltest ab und wartest, wer schreit. Klingt brutal, ist aber deutlich freundlicher als ein Rückbau, nach dem niemand mehr zurück kann.

```
# 1. Alle verbliebenen Relying Parties deaktivieren (außer du willst einzelne gezielt testen)
Get-AdfsRelyingPartyTrust | Select-Object Name, Enabled | Format-Table -AutoSize
Get-AdfsRelyingPartyTrust | ForEach-Object { Disable-AdfsRelyingPartyTrust -TargetName $_.Name
}

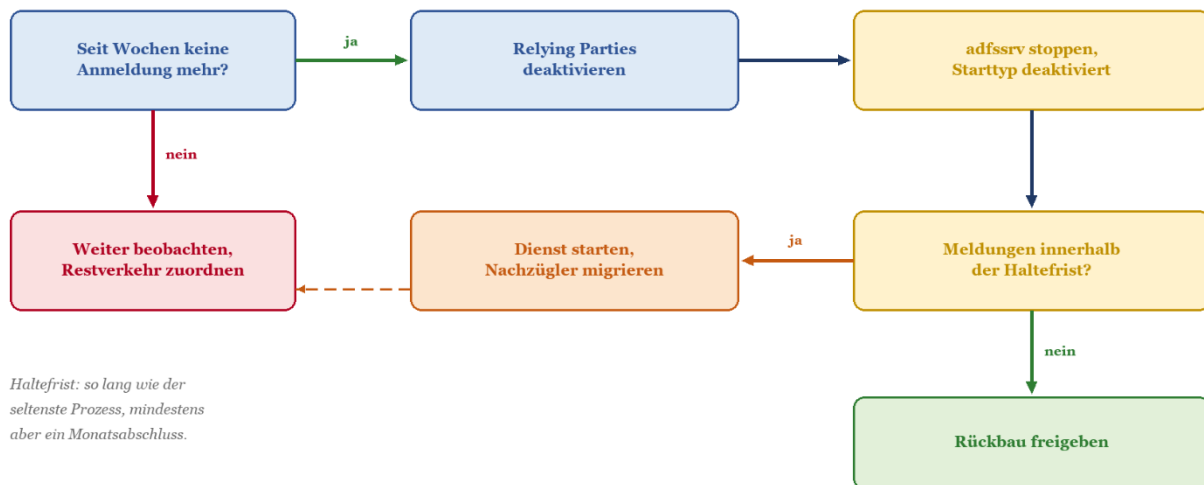
# 2. Auf jedem ADFS-Knoten: Dienst stoppen und am Neustart hindern
Stop-Service -Name adfssrv
Set-Service -Name adfssrv -StartupType Disabled

# Rückweg, falls sich doch jemand meldet:
# Set-Service -Name adfssrv -StartupType Automatic; Start-Service -Name adfssrv
# Enable-AdfsRelyingPartyTrust -TargetName "<Name>"
```

Kaltstellen ist reversibel. Genau deshalb kommt es vor dem Rückbau – und nicht stattdessen.

Skizze 5: Der Kaltstell-Test als Entscheidungsweg

Ein gestoppter Dienst ist ehrlicher als jede Inventarliste



Skizze 5: Der Kaltstell-Test. Wer sich in der Haltefrist meldet, wird migriert; wer schweigt, gibt den Rückbau frei.

Die Haltefrist für das Kaltstellen orientiert sich am Beobachtungszeitraum, ist aber meist kürzer: zwei bis vier Wochen, mindestens ein Monatsabschluss. Kündige sie an, mit Datum und Ansprechpartner. Wer dann anruft, weil „das Portal nicht mehr geht“, hat dir einen Gefallen getan: Du findest die letzte Anwendung, solange du sie noch mit einem Dienststart retten kannst. Die Server laufen in dieser Zeit weiter und bekommen weiter Updates – ein kaltgestellter, aber ungepatchter Server ist kein Abschied, sondern eine Einladung.

WICHTIG — Ansprechpartner statt Schweigen

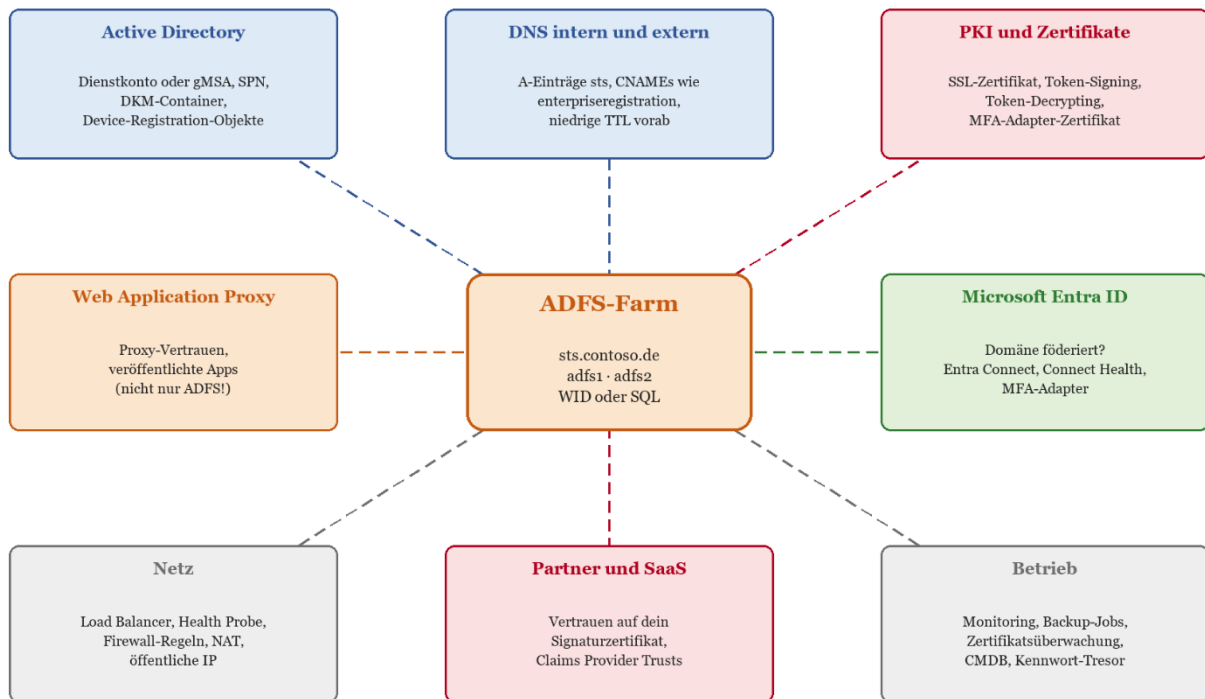
Lege für die Haltefrist eine feste Anlaufstelle fest, etwa ein Ticket-Template „Anmeldung über alte Firmenanmeldeseite“. Der Servicedesk muss wissen, dass Meldungen in diesem Zeitraum kein Fehler sind, sondern das Ergebnis, auf das du wartest. Sonst landet der Hinweis auf die vergessene Anwendung in einem Ticket, das als „Benutzer hat Kennwort vergessen“ geschlossen wird.

Der Rückbau: von außen nach innen

Wenn die Haltefrist ohne Meldung verstrichen ist, beginnt der Teil, der sich endgültig anfühlt, weil er es ist. Die wichtigste Regel: von außen nach innen. Erst schließt du die Türen zum Internet, dann baust du die Proxies ab, dann die Farm selbst, und ganz am Ende entfernst du, was im Active Directory und in der PKI zurückbleibt. Wer andersherum anfängt, hat für ein paar Tage eine öffentliche Adresse, hinter der ein halb abgerissener Dienst antwortet – oder gar nichts mehr und irgendwann jemand ganz anderes.

Skizze 2: Die Spinne im Netz – was alles an der Farm hängt

Jeder Faden ist ein Aufräumposten. Die meisten sieht man in keiner ADFS-Konsole.



Skizze 2: Was an einer ADFS-Farm alles hängt. Die ADFS-Konsole zeigt dir davon vielleicht ein Drittel.

Zuerst sichern – und das Backup gleich mit befristen

Microsoft empfiehlt ein optionales letztes Backup mit dem Rapid Restore Tool. Mach es. Es ist deine Versicherung, falls doch noch eine Anwendung auftaucht, deren Konfiguration du nachbauen musst, und es ist die vollständigste Dokumentation deiner Farm, die du je haben wirst. Wie das Werkzeug arbeitet, beschreibt [ADFS sichern und wiederherstellen – Rapid Restore Tool in der Praxis](#).

WARNUNG – Das letzte Backup ist ein Schlüsselbund

Ein Rapid-Restore-Backup enthält auf Wunsch die privaten Schlüssel der Token-Signing- und Token-Decrypting-Zertifikate. Wer diese Datei hat, kann theoretisch Tokens fälschen, solange irgendein System dem Signaturzertifikat noch vertraut. Lege das Backup verschlüsselt ab, beschränke den Zugriff auf wenige Personen, lege ein Löschdatum fest und halte es ein. Ein Backup ohne Ablaufdatum ist keine Vorsorge, sondern ein Erbstück, das niemand haben will.

Hintergrund zu gefälschten Tokens: [ADFS-Sicherheit: Angriffe, Härtung, Golden SAML und MFA](#).

WAP-Veröffentlichungen umziehen

Der Web Application Proxy wird oft unterschätzt, weil man ihn gedanklich als „den Reverse Proxy für ADFS“ abspeichert. In vielen Umgebungen veröffentlicht er aber deutlich mehr: Exchange-Dienste, SharePoint, interne Webportale, manchmal mit Vorauthentifizierung über ADFS, manchmal im Pass-Through. Weil der WAP seine Konfiguration in der ADFS-Konfigurationsdatenbank ablegt und ohne Proxy-Vertrauen zur Farm nicht arbeitet, verschwinden mit ADFS auch alle diese Veröffentlichungen. Also schaust du vor dem Abbau nach, was dort wirklich liegt:

Auf einem WAP-Server: alle veröffentlichten Anwendungen auflisten

```
Get-WebApplicationProxyApplication |
    Select-Object Name, ExternalUrl, BackendServerUrl, ExternalPreauthentication |
    Format-Table -AutoSize
```

```
# Nach dem Umzug: Veröffentlichung entfernen
Remove-WebApplicationProxyApplication -Name "Intranet-Portal"
```

Veröffentlichung	Möglicher Nachfolger	Achte auf
Anwendung mit ADFS-Vorauthentifizierung (Claims-basiert)	Microsoft Entra Application Proxy oder direkte SAML/OIDC-Anbindung an Entra ID	Anwendung muss vorher nach Entra ID umgezogen sein
Anwendung mit Kerberos-Delegierung über WAP	Entra Application Proxy mit eingeschränkter Kerberos-Delegierung	SPN und Delegierung neu für den Connector einrichten; Grundlagen: Microsoft Kerberos
Pass-Through-Veröffentlichung ohne Vorauthentifizierung	Reverse Proxy oder Load Balancer in der DMZ	Zertifikat, Header und Timeouts übernehmen
Exchange- oder SharePoint-Dienste	Je nach Szenario Entra Application Proxy oder Reverse Proxy	Mobile Clients und Protokolle einzeln testen
Die ADFS-Endpunkte selbst	Kein Nachfolger nötig	Erst entfernen, wenn alles andere umgezogen ist

Tabelle 3: Wohin die WAP-Veröffentlichungen umziehen können

Mehr zur Architektur und zu den Ablöseoptionen steht in [Web Application Proxy: Architektur und Ablöse](#). Erst wenn auf dem WAP nichts mehr veröffentlicht ist, deinstallierst du die Rolle. Microsoft nennt dafür den Befehl `Uninstall-WindowsFeature Web-Application-Proxy,CMAK,RSAT-RemoteAccess`. Danach gehört der Server, wie die ADFS-Knoten auch, neu aufgesetzt – Microsoft empfiehlt ausdrücklich ein Re-Image mit vollständiger Formatierung.

Load Balancer, DNS und Firewall

Als Nächstes verschwinden die Wege zur Farm. Auf den Load Balancern entfernst du die virtuellen Dienste für ADFS und WAP samt Health Probes und Persistenzprofilen; was dort typischerweise konfiguriert ist, beschreibt [ADFS hinter dem Load Balancer – Health Probe, SNI und Persistenz](#). Bei DNS lohnt sich Vorbereitung: Setze die TTL der betroffenen Einträge einige Tage vorher herunter, damit eine eventuelle Korrektur schnell greift.

Eintrag	Wo	Was tun
sts.contoso.de (A oder CNAME)	Externes DNS	Löschen, sobald der WAP nichts mehr veröffentlicht
sts.contoso.de (A)	Internes DNS, oft Split-Brain	Löschen nach dem Abbau der ADFS-Knoten
enterpriseregistration.contoso.de	Intern und extern	Prüfen, wohin er zeigt; zeigte er auf ADFS, für Entra-Geräteregistrierung umstellen oder löschen
Weitere WAP-Hostnamen	Extern	Auf den Nachfolger umziehen oder löschen
Zertifikatsanmeldung (falls genutzt)	Extern	Eigene Hostnamen oder Ports für Benutzerzertifikate mit entfernen

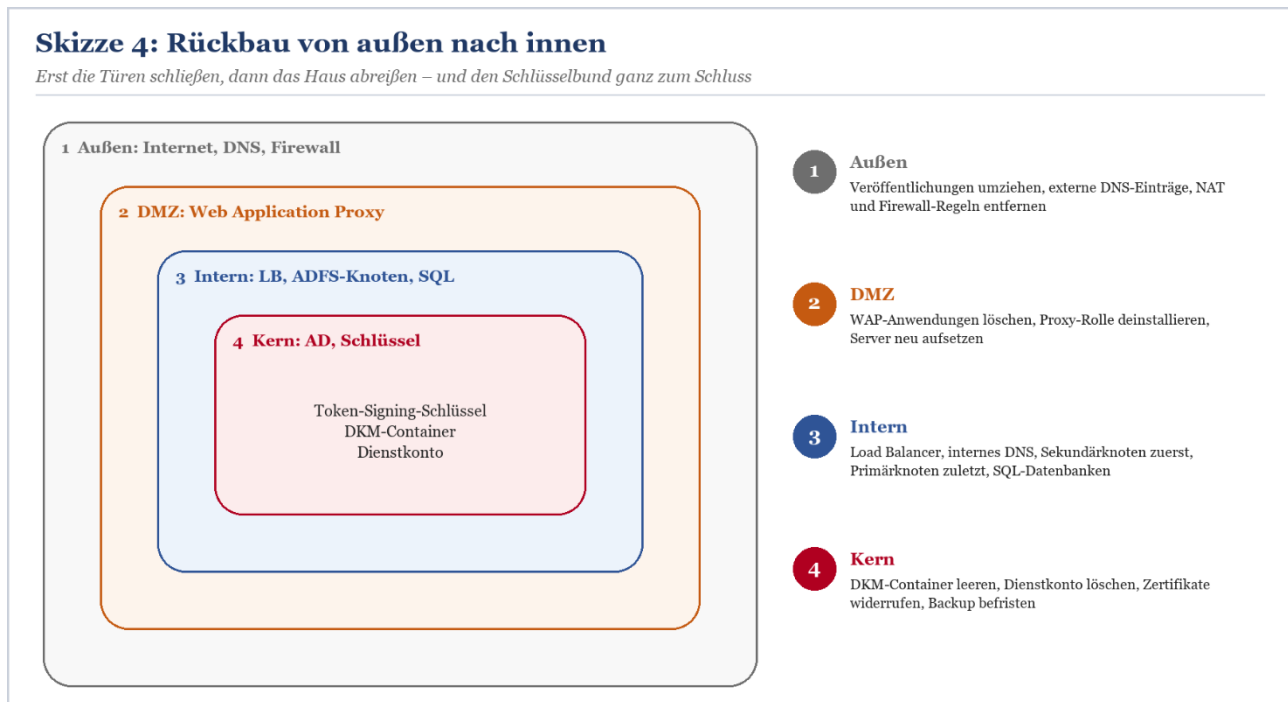
Tabelle 4: DNS-Einträge, die mit der Farm gehen

WARNUNG – Verwaiste DNS-Einträge sind Einladungen

Wenn ein externer DNS-Eintrag noch auf eine öffentliche IP-Adresse zeigt, die du bei deinem Provider oder in der Cloud längst freigegeben hast, kann diese Adresse irgendwann jemand anders bekommen. Dann antwortet unter `sts.contoso.de` ein fremder Server – mit deinem Namen und dem Vertrauen deiner Benutzer. Lösche DNS-Einträge deshalb immer vor oder gleichzeitig mit der Freigabe der Adresse, nie danach.

In der Firewall gehen die Regeln mit: eingehend TCP 443 aus dem Internet auf den WAP oder den externen Load Balancer, TCP 443 vom WAP auf die ADFS-Farm, gegebenenfalls der Port für die Benutzerzertifikat-Anmeldung, die NAT-Regeln und die Ausnahmen für Connect Health und die Zertifikatssperrlisten. Lösche die Regeln nicht einfach, sondern dokumentiere sie vorher mit Regelnamen, Quelle, Ziel und Port im Abschlussbericht. Firewall-Regeln sind die Fossilien, an denen spätere Generationen ablesen, was einmal war.

Die ADFS-Knoten deinstallieren



Skizze 4: Die Rückbau-Reihenfolge von außen nach innen. Der Kern – Schlüssel und AD-Objekte – kommt zuletzt.

Vor der Deinstallation notierst du auf dem primären Knoten den CertificateSharingContainer – du brauchst den Distinguished Name später im Active Directory. Bei einer WID-Farm deinstallierst du zuerst die Sekundärknoten und zuletzt den Primärknoten. Bei einer SQL-Farm löschst du laut Microsoft die Datenbanken vor der Deinstallation; das sind die Konfigurationsdatenbank (AdfsConfiguration mit Versionssuffix) und der AdfsArtifactStore. Welches Modell du hast, falls das aus der Doku nicht mehr hervorgeht, zeigt Get-AdfsSyncProperties; Hintergrund dazu in [WID oder SQL Server als ADFS-Konfigurationsdatenbank](#).

```
# Auf dem primären Knoten: Daten für den Abschlussbericht und das AD-Aufräumen sichern
Get-AdfsProperties | Select-Object HostName, CertificateSharingContainer, AuditLevel |
Format-List
Get-AdfsSyncProperties | Format-List
Get-AdfsCertificate | Select-Object CertificateType, IsPrimary, Thumbprint,
    @{n='Ablauf';e={$_.Certificate.NotAfter}} | Format-Table -AutoSize

# Auf jedem Knoten, Sekundärknoten zuerst:
Uninstall-WindowsFeature ADFS-Federation, Windows-Internal-Database
# Danach die WID-Datenbankdateien entfernen (laut Microsoft-Leitfaden):
Remove-Item -Path 'C:\Windows\WID\data\adfs\*' -Force
```

Die Befehle entsprechen dem Microsoft-Leitfaden zur Außerbetriebnahme. Bei SQL-Farmen entfällt Windows-Internal-Database, dafür werden die Datenbanken auf dem SQL Server gelöscht.

Anschließend löschst du die SSL-Zertifikate aus dem Computerspeicher jedes Servers und setzt die Maschinen neu auf. Das klingt übertrieben für Server, die ohnehin verschwinden sollen, hat aber

einen nüchternen Grund: Auf den Platten liegen Schlüsselmaterial, Protokolle und Konfiguration. Eine VM, die „nur ausgeschaltet“ in einem Cluster steht, wird in zwei Jahren von jemandem eingeschaltet, der wissen will, was sie macht.

Aufräumen: Zertifikate, Dienstkonto, DKM-Container und Entra-Reste

Die Server sind weg. Jetzt kommt der Teil, der am häufigsten vergessen wird, weil man ihn in keinem Rechenzentrum sieht: die Spuren im Active Directory, in der PKI, in Entra ID und bei den Partnern. Genau hier sitzt aber das Restrisiko, denn die gefährlichste Hinterlassenschaft einer ADFS-Farm ist nicht der Server, sondern das Vertrauen, das andere Systeme ihrem Signaturzertifikat entgegenbringen.

Zertifikate: widerrufen, was widerrufbar ist

Zertifikat	Typische Herkunft	Was tun
SSL-Zertifikat (sts.contoso.de)	Öffentliche oder interne Zertifizierungsstelle	Bei der ausstellenden Stelle widerrufen, Grund „Einstellung des Betriebs“; Zertifikatsüberwachung austragen
Token-Signing	Meist selbstsigniert mit AutoCertificateRollover	Nicht widerrufbar; entscheidend ist, dass kein System ihm mehr vertraut (siehe unten)
Token-Decrypting	Meist selbstsigniert	Schlüssel mit der Farm vernichten; Partner, die damit verschlüsseln, informieren
Service-Communications	Meist identisch mit dem SSL-Zertifikat	Siehe SSL-Zertifikat
MFA-Adapter-Zertifikat	Selbstsigniert, an einem Entra-Dienstprinzipal hinterlegt	In Entra ID die Anmeldeinformation entfernen; Hintergrund: ADFS mit Entra-MFA koppeln – Adapter, Zertifikat und Fallstricke
Proxy-Vertrauenszertifikate des WAP	Von ADFS ausgestellt	Verfallen mit der Farm; Server neu aufsetzen

Tabelle 5: Zertifikate einer ADFS-Farm und ihr Ende

Bei Zertifikaten aus der internen PKI nicht vergessen: Wenn es für ADFS eine eigene Zertifikatvorlage gab, entferne sie aus der Ausstellung der Zertifizierungsstelle, damit niemand mehr ein Zertifikat für sts.contoso.de beantragen kann. Wie die Zertifikate einer Farm zusammenhängen, erklärt [ADFS Token-Signing-Zertifikat erneuern – mit und ohne AutoCertificateRollover](#).

WARNUNG – Das Signaturzertifikat lebt weiter – bei den anderen

Jede SaaS-Anwendung, jeder Partner und jede Anwendung, die einmal ADFS als Identitätsanbieter eingetragen hatte, kennt den öffentlichen Teil deines Token-Signing-Zertifikats. Solange dort die alte ADFS-Konfiguration hinterlegt ist, würde die Anwendung ein Token annehmen, das mit diesem Schlüssel signiert ist – von wem auch immer. Deshalb gehört zum Abschalten: in jeder ehemals angebundenen Anwendung die ADFS-Konfiguration entfernen und beim Partner die Löschung des Vertrauens schriftlich bestätigen lassen. Das ist kein Paranoia-Zuschlag, sondern der Kern der Golden-SAML-Problematik.

Dienstkonto, SPN und KDS-Schlüssel

Läuft ADFS unter einem gruppenverwalteten Dienstkonto, entfernst du es mit Remove-ADServiceAccount. Ein klassisches Dienstkonto deaktivierst du zuerst und löschst es nach ein paar Wochen, falls doch noch ein vergessener Dienst darunter laufen sollte. Mit dem Konto

verschwindet auch der SPN host/sts.contoso.de. Prüfe trotzdem mit setspn, ob er nicht zusätzlich an einem anderen Konto hängt – doppelte SPNs überleben gern ihre Erschaffer. Wie das gMSA einmal eingerichtet wurde, steht in [gMSA als ADFS-Dienstkonto einrichten und umstellen](#).

```
# SPN-Reste suchen
setspn -Q host/sts.contoso.de

# gMSA prüfen und entfernen
Get-ADServiceAccount -Identity gmsa-adfs -Properties
PrincipalsAllowedToRetrieveManagedPassword,
ServicePrincipalNames
Remove-ADServiceAccount -Identity gmsa-adfs

# Klassisches Konto: erst deaktivieren, später löschen
Disable-ADAccount -Identity svc-adfs
```

TIPP – Den KDS-Root-Key bitte stehen lassen

Für gMSAs wurde irgendwann ein KDS-Root-Key angelegt. Der gehört nicht zu ADFS, sondern zur Domäne, und vermutlich nutzen ihn inzwischen andere gMSAs. Er bleibt, wo er ist. Abschiede sind schön, aber man muss nicht gleich die ganze Familie mitnehmen.

Den DKM-Container im Active Directory leeren

ADFS verschlüsselt den privaten Schlüssel seiner automatisch verwalteten Zertifikate mit einem Schlüssel aus dem Distributed Key Manager, kurz DKM. Dieses Schlüsselmaterial liegt im Active Directory, typischerweise unter CN=<GUID>,CN=ADFS,CN=Microsoft,CN=Program Data,DC=contoso,DC=local – der genaue Pfad ist der CertificateSharingContainer, den du vor der Deinstallation notiert hast. Wer Lesezugriff auf diesen Container und eine Kopie der Konfigurationsdatenbank hat, kann die Signaturschlüssel entschlüsseln. Deshalb ist das Leeren des Containers kein kosmetischer Schritt, sondern der eigentliche Schlusstein.

Microsoft beschreibt das Entfernen mit ADSI-Bearbeitung nach der Deinstallation. Mit dem ActiveDirectory-Modul geht es ebenso, wenn du vorher genau hinschaust, was du löschst:

```
# Den notierten DN aus Get-AdfsProperties verwenden
$dkm = "CN=<GUID>,CN=ADFS,CN=Microsoft,CN=Program Data,DC=contoso,DC=local"

# Erst anschauen, dann löschen
Get-ADObject -SearchBase $dkm -Filter * -Properties whenCreated |
    Select-Object DistinguishedName, ObjectClass, whenCreated

Remove-ADObject -Identity $dkm -Recursive -Confirm
```

Den übergeordneten Container CN=ADFS nur entfernen, wenn darunter keine weiteren Farmen liegen – etwa eine Testfarm, die niemand erwähnt hat.

Hatte die Farm den Geräteregistrierungsdienst aktiviert, liegen außerdem Objekte für die Geräteregistrierung in der Konfigurationspartition und gegebenenfalls ein Container mit registrierten Geräten in der Domäne. Bevor du sie entfernst, prüfe, ob der Dienstverbindungspunkt für den Hybrid Join inzwischen auf Entra ID zeigt – denn den brauchst du weiterhin, nur eben nicht mehr für ADFS.

Entra ID, Entra Connect und Connect Health

- Domänen: Get-MgDomain zeigt für alle Domänen AuthenticationType Managed, Get-MgDomainFederationConfiguration liefert nichts mehr zurück.

- Entra Connect: Im Assistenten unter „Benutzeranmeldung ändern“ steht die Anmeldemethode auf Password Hash Sync oder Pass-Through-Authentifizierung. Die Föderationsaufgaben im Assistenten werden nicht mehr gebraucht.
- Connect Health: Agenten auf den ADFS- und WAP-Servern sind mit den Servern verschwunden; im Entra Admin Center entfernst du die Dienstinstanz und die Servereinträge, sonst meldet das Portal ewig unerreichbare Server.
- MFA-Adapter: Die Zertifikat-Anmeldeinformation für den Entra-MFA-Adapter am zugehörigen Dienstprinzipal entfernen.
- Conditional Access: Richtlinien, die sich auf ADFS-Claims wie insidecorporatenetwork verlassen haben, sind spätestens jetzt auf Named Locations umgestellt; mehr dazu in [Claim Rules nach Conditional Access übersetzen](#).
- Notfallkonten: Prüfen, dass sie Cloud-only sind und nie über ADFS liefern.

Checkliste, Risiken und Dokumentation

Am Ende steht eine Liste. Sie ist nicht spektakulär, aber sie ist das, woran du in zwei Jahren erkennst, ob die Farm sauber gegangen ist oder nur leise. Druck sie aus, hak sie ab, leg sie in den Abschlussbericht.

FAKTEN – Checkliste: ADFS abschalten und dekommissionieren

1. Alle Domänen in Entra ID auf Managed, keine Föderationskonfiguration mehr
2. Auditierung auf allen Knoten nachweislich aktiv, Testanmeldung sichtbar
3. Anmeldungen je Relying Party über den vollen Beobachtungszeitraum bei null
4. Jährliche und quartalsweise Prozesse mit Eigentümern gezielt getestet
5. Relying Parties deaktiviert, Dienst gestoppt, Haltefrist ohne Meldung verstrichen
6. Letztes Rapid-Restore-Backup erstellt, verschlüsselt, Löschedatum festgelegt
7. WAP-Veröffentlichungen umgezogen und entfernt, WAP deinstalliert
8. Load-Balancer-Dienste, Health Probes und Persistenzprofile entfernt
9. Externe und interne DNS-Einträge gelöscht, vor Freigabe der öffentlichen IP
10. Firewall- und NAT-Regeln dokumentiert und entfernt
11. SQL-Datenbanken gelöscht bzw. WID-Dateien entfernt, Sekundärknoten vor Primärknoten deinstalliert
12. SSL-Zertifikat widerrufen, Vorlage aus der Ausstellung genommen
13. ADFS-Konfiguration bei allen ehemaligen SaaS-Anwendungen und Partnern entfernt, schriftlich bestätigt
14. Server neu aufgesetzt oder vernichtet, VMs und Snapshots gelöscht
15. Dienstkonto bzw. gMSA entfernt, SPN-Reste geprüft
16. DKM-Container (CertificateSharingContainer) geleert
17. Connect Health, MFA-Adapter-Zertifikat und Geräteregistrierung bereinigt
18. Monitoring, Backup-Jobs, Zertifikatsüberwachung, CMDB, Kennwort-Tresor aktualisiert
19. Abschlussbericht erstellt und abgelegt

Die Risikotabelle

Risiko	Auslöser	Folge	Gegenmittel
Vergessene Anwendung	Seltener Prozess, nicht im Inventar	Ausfall beim nächsten Monats- oder Jahresabschluss	Langer Beobachtungszeitraum, Kaltstellen vor Rückbau

Messfehler	Auditierung inaktiv oder Protokoll überschrieben	Scheinbare Ruhe, echter Verkehr	Testanmeldung, zentrale Sammlung der Ereignisse
Fremdes Vertrauen bleibt	SaaS oder Partner behält ADFS als Identitätsanbieter	Gefälschte Tokens wären weiter gültig	Konfiguration bei jeder Gegenstelle entfernen lassen
Schlüsselmaterial überlebt	Backup, Snapshot, alte VM, DKM-Container	Signaturschlüssel rekonstruierbar	Backup befristen, Re-Image, DKM leeren, Snapshots löschen
Verwaister DNS-Eintrag	Öffentliche IP vor DNS-Eintrag freigegeben	Fremder Server unter deinem Namen	DNS zuerst, IP danach
Mitgerissene Veröffentlichung	WAP veröffentlicht mehr als ADFS	Exchange, SharePoint oder Portale extern nicht erreichbar	WAP-Inventar mit Get-WebApplicationProxyApplication
Zu viel gelöscht	CN=ADFS mit Testfarm, KDS-Root-Key, geteilter SPN	Andere Dienste fallen aus	Erst anzeigen, dann löschen; Löschungen dokumentieren
Ewiger Wachkomapatient	Niemand traut sich, den Rückbau freizugeben	Kosten, Patchaufwand, Angriffsfläche ohne Nutzen	Klare Kriterien und ein Freigabetermin im Projektplan

Tabelle 6: Risiken der Außerbetriebnahme und wie du sie beherrschst

Der Abschlussbericht

Die Dokumentation einer abgeschalteten Farm ist ein Nachruf mit praktischem Nutzen. Sie beantwortet die Fragen, die in zwei Jahren garantiert gestellt werden: Wann wurde ADFS abgeschaltet? Welche Anwendungen liefen darüber, und wo laufen sie heute? Welche Zertifikate wurden widerrufen, mit welchem Fingerabdruck? Welche Partner haben die Löschung des Vertrauens bestätigt? Wo liegt das letzte Backup, und wann wurde es gelöscht? Dazu gehört auch der Export aller Relying Parties und Claims Provider Trusts mit Get-AdfsRelyingPartyTrust und Get-AdfsClaimsProviderTrust samt Regeln als XML, damit spätere Fragen zur alten Autorisierungslogik beantwortbar bleiben, auch wenn es keine Farm mehr gibt.

Vergiss dabei nicht die Systeme, die die Farm noch erwähnen: CMDB-Einträge, Überwachungsregeln, Zertifikatsüberwachung, Backup-Jobs, Runbooks, Notfallhandbücher, Kennwort-Tresor-Einträge für das Dienstkonto, Wartungsverträge, Lizenzzuordnungen. Ein Notfallhandbuch, das im Ernstfall auf eine ADFS-Farm verweist, die es nicht mehr gibt, ist die unangenehmste Art, an einen Verstorbenen erinnert zu werden.

WEITER – Passende Beiträge für die letzten Schritte

- › [Relying Parties inventarisieren – die Bestandsaufnahme vor der Entra-Migration](#)
- › [Microsoft 365 von Federated auf Managed umstellen – mit Staged Rollout](#)
- › [SAML-Anwendungen von ADFS nach Entra ID migrieren](#)
- › [ADFS sichern und wiederherstellen – Rapid Restore Tool in der Praxis](#)
- › [Web Application Proxy: Architektur und Ablöse](#)
- › [ADFS-Sicherheit: Angriffe, Härtung, Golden SAML und MFA](#)
- › [Microsoft Entra ID](#)

Fazit: Ein würdiger Abschied braucht Geduld und eine Liste

ADFS abzuschalten ist technisch kein Kunststück. Die Befehle passen auf eine Seite, Microsoft hat die Reihenfolge dokumentiert, und die eigentliche Arbeit – Benutzer und Anwendungen umziehen – ist zu diesem Zeitpunkt längst erledigt. Schwierig ist etwas anderes: die Gewissheit, dass wirklich

nichts mehr dranhängt. Die bekommst du nicht durch Hoffen, sondern durch Messen über einen ehrlichen Zeitraum, durch Kaltstellen vor dem Rückbau und durch einen Rückbau von außen nach innen, der mit dem Schlüsselmaterial endet und nicht mit den Servern.

Wer seine Farm weiter betreibt, macht damit übrigens nichts falsch. Eine gut gepflegte ADFS-Umgebung ist kein Zombie, sondern Infrastruktur. Und wenn der Tag des Abschieds kommt, verdient sie denselben Respekt wie im Betrieb: sorgfältig, dokumentiert und ohne Hinterlassenschaften, die anderen später auf die Füße fallen. Wenn du dabei Unterstützung beim Nachweis oder beim Rückbau willst, findest du sie im [Consulting zu ADFS \(Active Directory Federation Services\)](#). Den gesamten Lebenszyklus einer Farm vom Aufbau bis zum Abschied vertieft [ADFS in der Praxis – das Buch im Detail](#), und wer den Ausstieg einmal in Ruhe im Labor durchspielen will, findet das passende Format in den [ADFS-Schulungen](#).

FAQ: ADFS abschalten und dekommissionieren

Woran erkenne ich, dass ADFS nicht mehr genutzt wird?

An null Ereignissen 1200 bis 1203 der Quelle AD FS Auditing über den ganzen Beobachtungszeitraum, an einer leeren Nutzungsanalyse in Entra Connect Health und daran, dass alle Domänen in Entra ID auf Managed stehen. Voraussetzung ist, dass die Auditierung nachweislich funktioniert.

Wie lange sollte ich vor dem Abschalten beobachten?

Microsoft nennt mindestens eine Woche. In der Praxis sollte der Zeitraum den seltensten Geschäftsprozess abdecken, mindestens einen Monatsabschluss, bei vielen Relying Parties eher ein Quartal.

Was ist der Unterschied zwischen Kaltstellen und Abschalten?

Beim Kaltstellen stoppst du den Dienst und deaktivierst die Relying Parties, die Server bleiben aber unverändert. Ein Dienststart macht alles rückgängig. Beim Abschalten baust du Rollen, DNS, Zertifikate und AD-Objekte endgültig ab.

Kann ich den Web Application Proxy ohne ADFS weiterbetreiben?

Nein. Der WAP speichert seine Konfiguration in ADFS und braucht das Proxy-Vertrauen zur Farm. Alle Veröffentlichungen müssen vorher auf einen Nachfolger wie Entra Application Proxy oder einen Reverse Proxy umziehen.

In welcher Reihenfolge deinstalliere ich die ADFS-Server?

Erst die WAP-Server, dann die ADFS-Sekundärknoten, zuletzt den Primärknoten. Bei einer SQL-Farm löschst du die Datenbanken laut Microsoft vor der Deinstallation.

Was ist der DKM-Container und muss er wirklich weg?

Er enthält das Schlüsselmaterial, mit dem ADFS die privaten Schlüssel seiner Zertifikate schützt. Den genauen Pfad zeigt CertificateSharingContainer in Get-AdfsProperties. Ja, er muss weg, sobald die Farm deinstalliert ist.

Muss ich das Token-Signing-Zertifikat widerrufen?

Selbstsignierte Zertifikate lassen sich nicht widerrufen. Entscheidend ist, dass keine Anwendung und kein Partner der alten ADFS-Konfiguration mehr vertraut. Das SSL-Zertifikat einer Zertifizierungsstelle widerrufst du dagegen regulär.

Darf ich den KDS-Root-Key löschen, wenn das ADFS-gMSA weg ist?

Nein. Der KDS-Root-Key gehört zur Domäne und wird von allen gMSAs genutzt. Entfernt wird nur das ADFS-Dienstkonto.

Brauche ich das letzte Backup überhaupt?

Microsoft nennt es optional, empfehlenswert ist es trotzdem. Weil es Schlüsselmaterial enthalten kann, gehört es verschlüsselt abgelegt und mit einem festen Löschdatum versehen.

Was passiert mit Entra Connect, wenn ADFS weg ist?

Entra Connect synchronisiert weiter. Die Anmeldemethode steht dann auf Password Hash Sync oder Pass-Through-Authentifizierung, die Föderationsfunktionen des Assistenten werden nicht mehr gebraucht.

Wie gehe ich mit Partnern um, die per Claims Provider Trust angebunden waren?

Rechtzeitig informieren, den Zugang neu regeln, zum Beispiel über B2B-Zusammenarbeit in Entra ID, und die Löschung des Vertrauens auf beiden Seiten dokumentieren.