

gMSA als ADFS-Dienstkonto einrichten und umstellen

WISSEN

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

› [Active Directory Federation Services](#)

BERATUNG

Dienstkonto umstellen, ohne dass montags die Anmeldung klemmt – mit jemandem, der das schon oft gemacht hat.

› [Consulting zu ADFS](#)

SCHULUNG

gMSA anlegen, Farm umstellen, SPN-Chaos auflösen – im Workshop an echten Farmen.

› [ADFS-Schulungen](#)

Es gibt in fast jeder gewachsenen ADFS-Umgebung ein Konto, über das niemand gern spricht. Es heißt svc-adfs, adfs-service oder, für die Mutigen, einfach adfs. Sein Kennwort wurde bei der Installation vor elf Jahren vergeben, steht in einem Passwort-Tresor, auf den noch zwei Leute Zugriff haben, und „läuft nie ab“ ist angehakt. Mit etwas Pech ist es außerdem Mitglied der Domänen-Admins, „weil es damals anders nicht ging“. Niemand weiß mehr, was damals nicht ging. Aber niemand traut sich, es auszuprobieren.

Dieser Beitrag räumt mit dem Konto auf. Du erfährst, warum ein gruppenverwaltetes Dienstkonto (Group Managed Service Account, kurz gMSA) für ADFS die bessere Wahl ist, wie du den KDS-Root-Key anlegst, das gMSA erstellst und berechtigt – und vor allem, wie du eine laufende Farm vom klassischen Benutzerkonto auf das gMSA umstellst, ohne dass am nächsten Morgen die Anmeldung an Microsoft 365 klemmt. Die Grundlagen zu Farm, Federation Service und Vertrauensstellungen setzen wir voraus; die findest du auf der Pillar-Seite [Active Directory Federation Services](#).

FAKTEN — Die Kurzfassung für Eilige

ADFS unterstützt gMSAs als Dienstkonto seit AD FS 3.0 unter Windows Server 2012 R2. Microsoft empfiehlt das gMSA ausdrücklich; das klassische Benutzerkonto ist die Ausweichlösung für sehr alte Domänen.

Ein gMSA braucht einen KDS-Root-Key in der Gesamtstruktur. Nach dem Anlegen warten die Domänencontroller bis zu 10 Stunden, bevor sie Kennwörter daraus ableiten.

Das Kennwort des gMSA berechnet der Domänencontroller; abrufen dürfen es nur die Computerkonten, die du in PrincipalsAllowedToRetrieveManagedPassword einträgst.

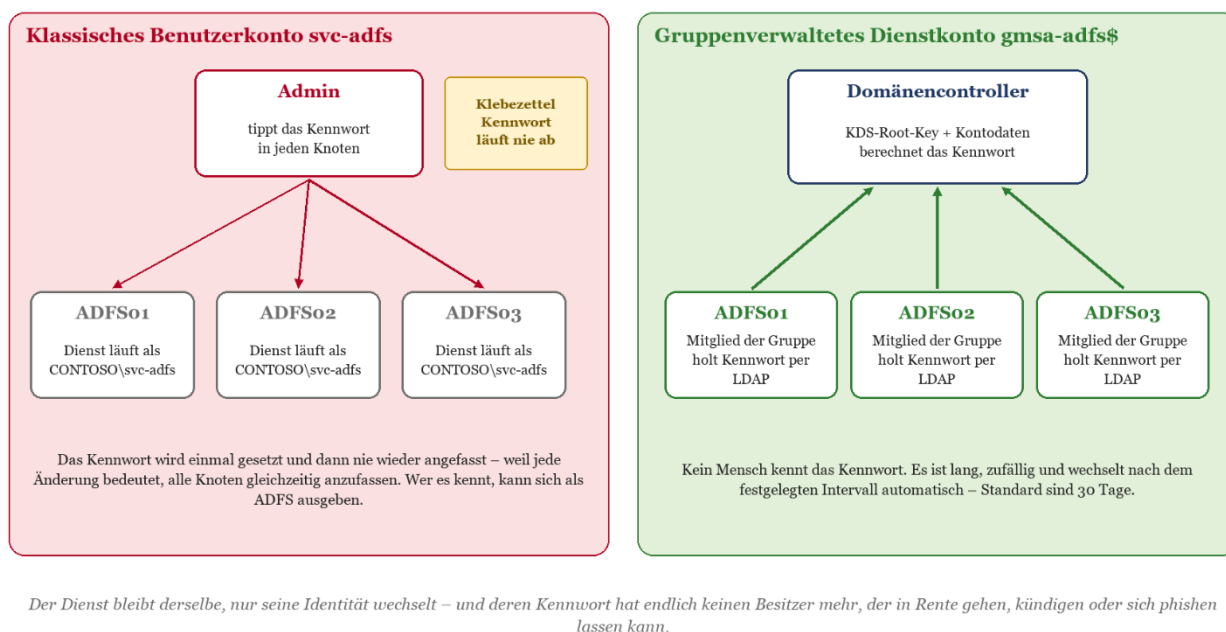
Standardintervall für den Kennwortwechsel: 30 Tage, änderbar nur beim Anlegen.

Für die Umstellung einer Bestandsfarm stellt Microsoft in der ADFS-Toolbox das Service-Account-Modul bereit. Es funktioniert mit WID- und SQL-Farmen.

Das ADFS-Dienstkonto braucht keine Domänen-Admin-Rechte. Nie.

Skizze 1: Wer kennt das Passwort? Klassisches Dienstkonto und gMSA

Links wohnt das Kennwort im Kopf eines Admins, rechts rechnet es der Domänencontroller aus



Skizze 1: Beim klassischen Dienstkonto kennt ein Mensch das Kennwort, beim gMSA niemand – der Domänencontroller berechnet es, und nur die ADFS-Server dürfen es abholen.

Warum gMSA statt klassischem Dienstkonto

Der ADFS-Dienst adfssrv braucht eine Domänenidentität. Nicht aus Bürokratie, sondern wegen Kerberos: Wenn ein Client im internen Netz per integrierter Windows-Authentifizierung ein Ticket für sts.contoso.de anfordert, verschlüsselt der Domänencontroller dieses Ticket mit dem Schlüssel des Kontos, an dem der SPN HOST/sts.contoso.de hängt. Damit jeder Knoten der Farm dieses Ticket öffnen kann, müssen alle Knoten unter demselben Konto laufen. Ein lokales Konto oder Network Service scheidet damit aus – Microsoft warnt selbst, dass das zu zufälligen Kerberos-Fehlern führt.

Was ein gMSA eigentlich ist

Ein gMSA ist ein Domänenkonto der Objektklasse msDS-GroupManagedServiceAccount, das sich mehrere Server teilen dürfen, ohne dass ein Mensch das Kennwort je sieht. Der Key Distribution Service auf den Domänencontrollern leitet das Kennwort aus dem KDS-Root-Key und Kontoattributen ab. Berechtigte Computer holen es per LDAP ab und wechseln es nach dem festgelegten Intervall automatisch. Interaktive Anmeldungen sind mit einem gMSA nicht vorgesehen, und ein Kennwort, das niemand kennt, kann auch niemand in eine Phishing-Seite tippen.

Was bei ADFS konkret besser wird

Aspekt	Klassisches Benutzerkonto	gMSA
Kennwort	von einem Menschen gesetzt, meist „läuft nie ab“	vom DC berechnet, niemand kennt es
Kennwortwechsel	manuell, alle Knoten gleichzeitig, in der Praxis: nie	automatisch, standardmäßig alle 30 Tage
Wer kann das Konto nutzen?	jeder, der das Kennwort kennt – von überall	nur Computer in PrincipalsAllowedToRetrieveManagedPassword

Interaktive Anmeldung	möglich und damit Angriffsfläche	nicht vorgesehen
Kerberos-Verschlüsselung	hängt an Kontoeinstellungen und Kennwortalter	moderne Verschlüsselungstypen, Schlüssel rotieren mit
Neuer Knoten	Kennwort muss bekannt sein und eingegeben werden	Computerkonto in die Gruppe, fertig
Voraussetzung	keine	KDS-Root-Key, Funktionsebene ab Windows Server 2012
Microsoft-Empfehlung	Ausweichlösung	empfohlene Option seit Windows Server 2012 R2

Tabelle 1: Klassisches Dienstkonto und gMSA im direkten Vergleich

Der wichtigste Punkt steht nicht in der Tabelle, sondern zwischen den Zeilen: Das Dienstkonto ist bei ADFS kein Nebendarsteller. Es darf auf die privaten Schlüssel der Token-Signatur zugreifen – direkt oder über den DKM-Container im Active Directory, wenn AutoCertificateRollover aktiv ist. Wer das Konto übernimmt, kann sich im schlimmsten Fall Token für Microsoft 365 und jede andere Relying Party selbst ausstellen. Genau das ist der Kern von Golden SAML, den wir in [ADFS-Sicherheit: Angriffe, Härtung, Golden SAML und MFA](#) ausführlich behandeln.

WARNUNG – Dienstkonto mit Domänen-Admin-Rechten

Wenn dein ADFS-Dienstkonto Mitglied der Domänen-Admins, Organisations-Admins oder einer vergleichbar mächtigen Gruppe ist, hast du nicht ein Problem, sondern zwei: Jeder, der einen ADFS-Server kompromittiert, bekommt die Domäne gleich mit – und jeder, der die Domäne kompromittiert, hat ohnehin ADFS.

ADFS braucht diese Rechte nicht. Weder für den Betrieb noch für Zertifikatswechsel noch für Microsoft 365. Die Legende, es gehe „ohne nicht“, stammt meist aus einer Installation, bei der ein fehlender SPN oder ein fehlendes SQL-Recht mit dem größtmöglichen Hammer erschlagen wurde. Prüfe die Mitgliedschaften deines heutigen Kontos, bevor du umstellst, und nimm sie nach der Umstellung nicht mit. Das gMSA bekommt genau die Rechte aus Skizze 3 – nichts weiter.

```
# Wer ist das heutige Dienstkonto, und in welchen Gruppen steckt es?
(Get-CimInstance Win32_Service -Filter "Name='adfssrv']").StartName

Get-ADPrincipalGroupMembership -Identity svc-adfs | Select-Object Name

# Ist es irgendwo über Verschachtelung privilegiert?
Get-ADUser svc-adfs -Properties MemberOf, AdminCount, PasswordLastSet, PasswordNeverExpires
```

Listing 1: Bestandsaufnahme des klassischen Dienstkontos. AdminCount = 1 ist ein Hinweis, dass das Konto irgendwann Mitglied einer geschützten Gruppe war.

Voraussetzungen und KDS-Root-Key

Bevor es ein gMSA geben kann, muss die Gesamtstruktur wissen, woraus sie dessen Kennwörter ableiten soll. Das ist der KDS-Root-Key. Er wird einmal pro Gesamtstruktur angelegt, liegt in der Konfigurationspartition und bedient alle Domänen. Gibt es in deiner Umgebung schon gMSAs – etwa für Entra Connect, Defender for Identity oder SQL Server –, existiert er bereits, und du kannst diesen Abschnitt mit einem zufriedenen Nicken überspringen.

Voraussetzungen prüfen

Voraussetzung	Wie prüfen	Anmerkung
Domänen- und Gesamtstruktur-Funktionsebene ab Windows Server 2012	Get-ADDomain, Get-ADForest	in allen heute unterstützten Umgebungen der Normalfall

KDS-Root-Key vorhanden	Get-KdsRootKey	leere Ausgabe: noch keiner da
Rechte zum Anlegen des Root-Keys	Mitgliedschaft Domänen-Admins oder Organisations-Admins	nur für diesen einen Schritt – nicht für das Dienstkonto
AD-PowerShell auf den ADFS-Servern	Get-WindowsFeature RSAT-AD-PowerShell	für Test-ADServiceAccount und die Umstellung
Funktionierende AD-Replikation	repadmin /replsummary	sonst wird aus 10 Stunden Wartezeit eine offene Frage
Uhrzeit synchron	w32tm /query /status	Kerberos verzeiht keine Zeitreisen

Tabelle 2: Was vor dem ersten gMSA erfüllt sein muss

Den KDS-Root-Key anlegen

Der Befehl ist ein Einzeiler, der Name des Parameters aber irreführend. Add-KdsRootKey -EffectiveImmediately legt den Schlüssel sofort an – benutzen kann ihn der Rest der Gesamtstruktur trotzdem erst, wenn er repliziert ist. Die Domänencontroller warten deshalb bis zu 10 Stunden ab Erstellung, bevor sie daraus Kennwörter erzeugen. Das ist eine Sicherheitsleine, kein Fehler. Plane den Root-Key also mindestens einen Tag vor dem eigentlichen Termin ein.

```
# Produktion: anlegen, dann bis zu 10 Stunden Replikation abwarten
Add-KdsRootKey -EffectiveImmediately

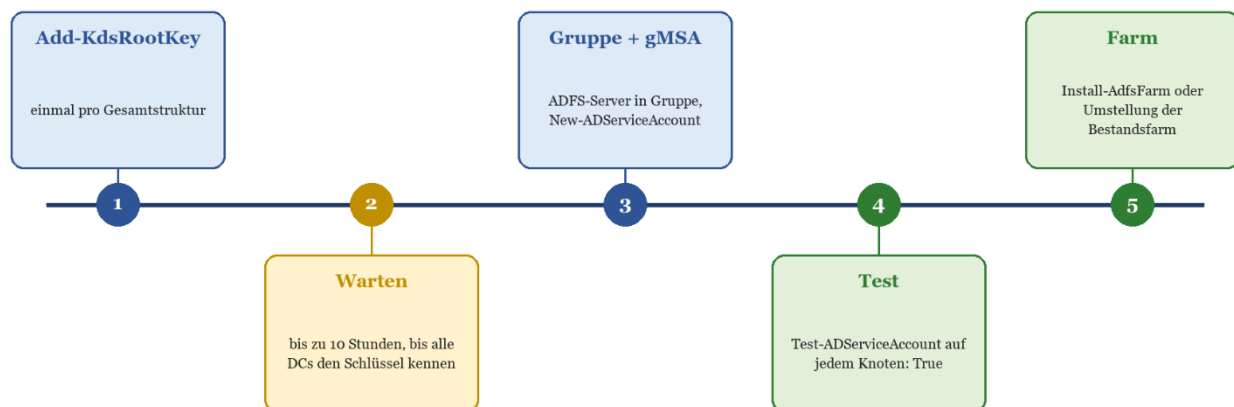
# Kontrolle
Get-KdsRootKey | Select-Object KeyId, EffectiveTime, CreationTime

# NUR Testumgebung mit einem einzigen DC: Wirksamkeit in die Vergangenheit legen
Add-KdsRootKey -EffectiveTime ((Get-Date).AddHours(-10))
```

Listing 2: KDS-Root-Key anlegen. Die Variante mit der zurückdatierten EffectiveTime ist laut Microsoft ausschließlich für Testumgebungen mit einem Domänencontroller gedacht.

Skizze 2: Vom KDS-Root-Key zur laufenden Farm

Der Schlüssel ist schnell angelegt – der Wartezeit ist das egal



Wer Schritt 2 überspringt, erlebt Schritt 4 als „False“ und sucht den Fehler stundenlang an der falschen Stelle.

Skizze 2: Die fünf Schritte vom Root-Key zur Farm. Die Wartezeit in Schritt 2 lässt sich in der Produktion nicht sinnvoll abkürzen.

TIPP – Erfolgreiche Erstellung nachweisen

Microsoft empfiehlt, im Protokoll KdsSvc/Operational auf den Domänencontrollern nach dem Ereignis 4004 zu sehen. Das ist der schriftliche Beleg, dass der Schlüssel angekommen ist – hilfreich, wenn später jemand fragt, ob „das mit dem Key“ wirklich erledigt war.

Die Einzelheiten beschreibt Microsoft unter [Microsoft Learn: KDS-Stammschlüssel erstellen](#).

WARNUNG — Root-Key nicht löschen und neu anlegen

Wenn ein gMSA nicht funktioniert, liegt es fast nie am Root-Key. Ihn zu löschen und neu zu erzeugen, löst das Problem nicht, sondern schafft ein neues: Durch Caching kann der alte Schlüssel weiterverwendet werden, Microsoft empfiehlt nach einem Neuanlegen den Neustart des KDC auf allen Domänencontrollern. Such den Fehler lieber bei Gruppenmitgliedschaft, Replikation oder Tippfehler im Kontonamen.

gMSA anlegen und berechtigen

Das gMSA selbst ist in zwei Minuten angelegt. Die eigentliche Arbeit liegt darin, festzulegen, wer das Kennwort abholen darf, und dem Konto genau die Rechte zu geben, die ADFS braucht – und keins mehr.

Eine Gruppe für die ADFS-Server

Du kannst die Computerkonten der ADFS-Server direkt in PrincipalsAllowedToRetrieveManagedPassword eintragen. Besser ist eine eigene Sicherheitsgruppe, etwa grp-adfs-server. Dann bedeutet ein neuer Knoten nur: Computerkonto in die Gruppe. Einen Haken hat das: Ein Computer erfährt von seiner neuen Gruppenmitgliedschaft erst mit einem neuen Kerberos-Ticket. Starte den Server neu oder verwirft die Tickets des Computerkontos, sonst meldet Test-ADServiceAccount ein ratloses False.

```
# Gruppe anlegen und ADFS-Server aufnehmen
New-ADGroup -Name grp-adfs-server -GroupScope Global -GroupCategory Security `
  -Path "OU=Gruppen,OU=Tier0,DC=contoso,DC=local"
Add-ADGroupMember -Identity grp-adfs-server -Members "ADFS01$", "ADFS02$", "ADFS03$"

# Auf jedem ADFS-Server: Tickets des Computerkontos erneuern (oder neu starten)
klist -li 0x3e7 purge
```

Listing 3: Gruppe für die ADFS-Server. Die ADFS-Server gehören in dieselbe Schutzstufe wie die Domänencontroller – entsprechend sollte auch die Gruppe verortet sein.

Das gMSA anlegen

Für eine neue Farm legst du den SPN gleich beim Anlegen mit an. Für die Umstellung einer Bestandsfarm lässt du ihn bewusst weg, denn HOST/sts.contoso.de hängt noch am alten Konto – und ein SPN an zwei Konten ist genau der Fehler, den du vermeiden willst. Beim Namen gilt: kurz und sprechend. Der sAMAccountName eines gMSA hat dieselbe 15-Zeichen-Grenze wie ein Computerkonto, und der Name muss in der gesamten Gesamtstruktur eindeutig sein.

```
# Variante A - neue Farm: SPN direkt mitgeben
New-ADServiceAccount -Name gmsa-adfs `
  -DNSHostName gmsa-adfs.contoso.local `
  -PrincipalsAllowedToRetrieveManagedPassword grp-adfs-server `
  -ServicePrincipalNames "HOST/sts.contoso.de" `
  -Path "OU=Dienstkonten,OU=Tier0,DC=contoso,DC=local"

# Variante B - Umstellung einer Bestandsfarm: OHNE SPN anlegen
New-ADServiceAccount -Name gmsa-adfs `
  -DNSHostName gmsa-adfs.contoso.local `
  -PrincipalsAllowedToRetrieveManagedPassword grp-adfs-server

# Auf jedem ADFS-Server prüfen - muss True liefern
Test-ADServiceAccount -Identity gmsa-adfs
```

Listing 4: gMSA anlegen. Der DNSHostName ist ein Pflichtattribut und meint den Namen des Kontos, nicht den Namen des Federation Service.

WICHTIG — Das Intervall wird beim Anlegen festgelegt

Ohne Angabe wechselt das Kennwort alle 30 Tage. Wer ein anderes Intervall will, gibt - ManagedPasswordIntervalInDays beim New-ADServiceAccount mit. Nachträglich ändern lässt es sich nicht – dann bleibt nur ein neues gMSA und eine zweite Umstellung. Für ADFS gibt es keinen Grund, vom Standard abzuweichen.

Was das Konto braucht – und was nicht

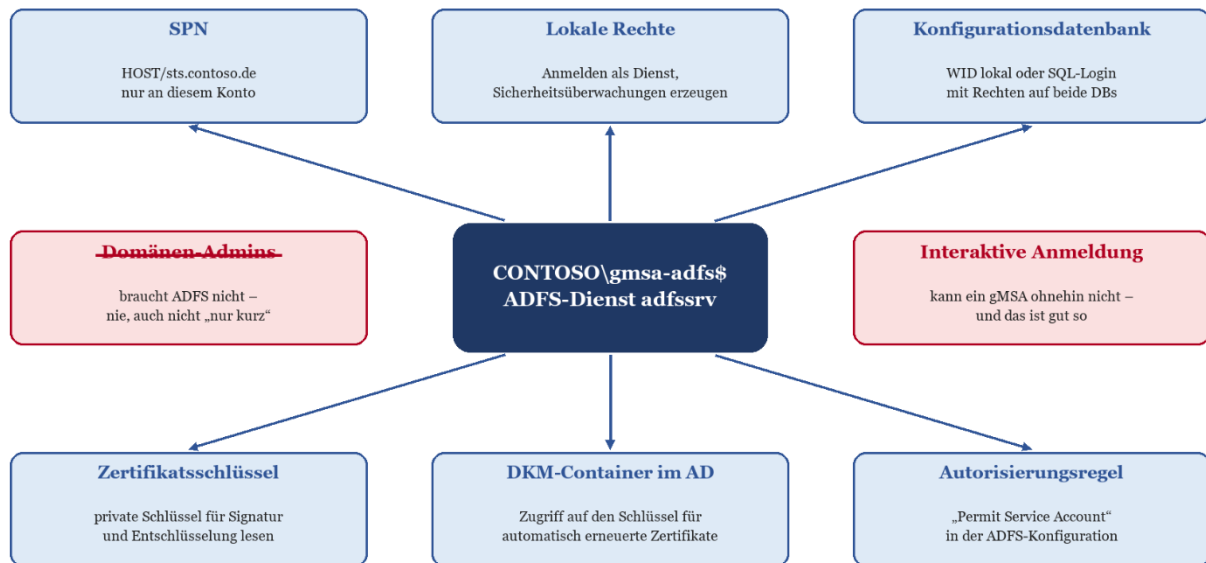
Die gute Nachricht: Die meisten Rechte musst du nicht von Hand setzen. Bei einer Neuinstallation erledigt das der Konfigurationsassistent beziehungsweise Install-AdfsFarm, bei einer Umstellung das Service-Account-Modul. Du solltest trotzdem wissen, was passiert, damit du beim Prüfen weißt, wonach du suchst.

Recht	Wofür	Wer setzt es
SPN HOST/sts.contoso.de	Kerberos-Tickets für den Federation Service	New-ADServiceAccount oder Umstellungsmodul
Anmelden als Dienst	adfssrv darf unter dem Konto starten	Assistent beziehungsweise Modul
Generieren von Sicherheitsüberwachungen	ADFS-Auditing ins Sicherheitsprotokoll	Assistent beziehungsweise Modul
Zugriff auf die Konfigurationsdatenbank	WID lokal, bei SQL ein Login mit Rechten auf Konfigurations- und Artefaktdatenbank	Assistent beziehungsweise Modul
Private Schlüssel der ADFS-Zertifikate	Token signieren und entschlüsseln	Assistent beziehungsweise Modul
DKM-Container im AD	Schlüssel für automatisch erneuerte Zertifikate	Assistent beziehungsweise Modul
Autorisierungsregel „Permit Service Account“	ab AD FS unter Windows Server 2016: Zugriff auf die eigene Konfiguration	Add-AdfsServiceAccountRule
Domänen-Admins	nichts	niemand

Tabelle 3: Die Rechte des ADFS-Dienstkontos im Überblick

Skizze 3: Was das ADFS-Dienstkonto wirklich braucht – und was nicht

Sechs gezielte Rechte statt einer Mitgliedschaft in Domänen-Admins



Alles, was hier blau ist, richtet der Konfigurationsassistent oder das Umstellungsmodul ein. Alles Rote richtest du bitte gar nicht ein.

Skizze 3: Sechs gezielte Berechtigungen machen das ADFS-Dienstkonto arbeitsfähig. Die roten Felder sind die, die du bewusst nicht vergibst.

Zusätzlich gibt es die Rechte, die nur in deiner Umgebung existieren: ein SQL-Attributspeicher, der unter dem Dienstkonto abgefragt wird, ein LDAP-Attributspeicher mit Leserechten auf einen bestimmten Bereich, ein MFA-Adapter, der auf eine Datei oder einen Registrierungsschlüssel zugreift. Die kennt kein Modul. Die musst du vorher finden – dazu gleich mehr in der Bestandsaufnahme.

Neue Farm direkt mit gMSA

Wenn du eine Farm neu aufbaust, ist das gMSA schlicht ein Parameter. Auf dem ersten Knoten gibst du es bei `Install-AdfsFarm` an, auf allen weiteren bei `Add-AdfsFarmNode`. Wichtig ist das Dollarzeichen am Ende des Kontonamens. Den vollständigen Ablauf mit Zertifikat, DNS und Load Balancer findest du in [ADFS-Farm installieren – Schritt für Schritt auf Windows Server 2022](#).

```
# Erster Knoten (WID-Farm)
$cert = (Get-ChildItem Cert:\LocalMachine\My | Where-Object Subject -like
"*sts.contoso.de*").Thumbprint
Install-AdfsFarm -CertificateThumbprint $cert `
  -FederationServiceName sts.contoso.de `
  -FederationServiceDisplayName "Contoso Anmeldung" `
  -GroupServiceAccountIdentifier "CONTOSO\gmsa-adfs$"

# Jeder weitere Knoten
Add-AdfsFarmNode -CertificateThumbprint $cert `
  -PrimaryComputerName adfs01.contoso.local `
  -GroupServiceAccountIdentifier "CONTOSO\gmsa-adfs$"
```

Listing 5: Neue Farm mit gMSA. Bei einer SQL-Farm kommt statt `-PrimaryComputerName` der Parameter `-SQLConnectionString` hinzu.

Bestehende Farm von Benutzerkonto auf gMSA umstellen

Jetzt der Teil, für den du wahrscheinlich hier bist. Eine Farm, die seit Jahren unter svc-adfs läuft, soll auf gmsa-adfs\$ umziehen. Das ist kein Hexenwerk, aber auch nichts, was man zwischen zwei Besprechungen nebenbei erledigt. Das Dienstkonto steckt an mehr Stellen, als die Dienste-Konsole zeigt: in der Konfigurationsdatenbank, in den ACLs der Zertifikatsschlüssel, im DKM-Container, am SPN, in lokalen Benutzerrechten und bei SQL-Farmen im SQL Server.

So stand es früher in jeder Anleitung

In älteren Blogartikeln findest du eine Anleitung, die im Kern so lautet: Dienst in der Dienste-Konsole auf das neue Konto umstellen, SPN mit setspn umhängen, Schlüsselrechte im Zertifikats-Snap-in anpassen, SQL-Rechte vergeben, Daumen drücken. Unter Windows Server 2012 R2 ging das mit etwas Glück gut. Ab AD FS unter Windows Server 2016 fehlt dabei aber ein entscheidender Baustein: Die Konfiguration enthält eine Autorisierungsregel, die das Dienstkonto über seine SID zulässt. Stellst du nur den Dienst um, startet adfssrv unter dem neuen Konto – und darf seine eigene Konfiguration nicht lesen. Ein Dienst, der sich selbst nicht kennt, ist ein philosophisch reizvoller, betrieblich aber unerfreulicher Zustand.

Das Werkzeug: das Service-Account-Modul

Microsoft stellt in der ADFS-Toolbox auf GitHub das Modul serviceAccountModule bereit. Es ist für genau diesen Zweck gebaut, funktioniert mit WID- und SQL-Farmen und exportiert vier Funktionen. Lade es herunter, prüfe es in Ruhe – es ist PowerShell, du kannst jede Zeile lesen – und importiere es auf allen ADFS-Servern.

Funktion	Wo ausführen	Was sie tut
Add-AdfsServiceAccountRule	primärer Knoten (bei SQL: ein beliebiger Knoten)	fügt der ADFS-Autorisierung eine Regel für die SID des neuen Kontos hinzu, legt vorher eine XML-Sicherung an; mit -SecondaryServers stößt sie in WID-Farmen den sofortigen Abgleich an
Update-AdfsServiceAccount	jeder Knoten, sekundäre zuerst, primärer zuletzt	stoppt adfssrv, stellt die Dienstidentität um, setzt Datenbank- und Schlüsselrechte, lokale Benutzerrechte und DKM-Zugriff, verschiebt beim letzten Server den SPN, startet den Dienst
Remove-AdfsServiceAccountRule	primärer Knoten, erst nach erfolgreicher Umstellung	entfernt die Regel für das alte Konto, ebenfalls mit XML-Sicherung
Restore-AdfsSettingsFromBackup	primärer Knoten, nur im Fehlerfall	spielt die Einstellungen aus der XML-Sicherung einer der beiden Regel-Funktionen zurück

Tabelle 4: Die vier Funktionen des Service-Account-Moduls

Update-AdfsServiceAccount fragt interaktiv, ob du gerade einen weiteren Federation-Server oder den letzten Server der Umstellung bearbeitest. Diese Unterscheidung ist wichtig: Erst beim letzten Server werden die farmweiten Einstellungen angepasst und der SPN umgehängt. Bei einem gMSA gibst du den Kontonamen mit Dollarzeichen an; ein Kennwort wird dann nicht abgefragt.

Die Bestandsaufnahme vorher

Die meisten missglückten Umstellungen scheitern nicht am Modul, sondern an einer Abhängigkeit, von der niemand wusste. Nimm dir vorher eine Stunde und geh diese Liste durch:

Prüfpunkt	Warum	Wie
Aktuelles Dienstkonto und dessen Kennwort	für den Rückweg brauchst du beides	Win32_Service StartName, Passwort-Tresor

WID oder SQL, primärer Knoten	bestimmt Reihenfolge und Ausführungsort	Get-AdfsSyncProperties, siehe WID oder SQL Server als ADFS-Konfigurationsdatenbank
Zertifikate: automatisch oder manuell	manuell importierte Schlüssel brauchen ACLs	Get-AdfsProperties, siehe ADFS Token-Signing-Zertifikat erneuern – mit und ohne AutoCertificateRollover
Device Registration Service aktiv?	braucht einen eigenen Schritt	Get-AdfsDeviceRegistration
SQL- oder LDAP-Attributspeicher	laufen unter dem Dienstkonto	Get-AdfsAttributeStore
Zusätzliche MFA- oder Authentifizierungsadapter	eigene Datei-, Registrierungs- oder Netzwerkrechte	Get-AdfsAuthenticationProvider
Geplante Aufgaben und Skripte unter svc-adsf	brechen beim Deaktivieren des Altkontos	Aufgabenplanung auf allen Knoten
Überwachung, die das Konto prüft	meldet sonst Fehlalarm	Monitoring-Konfiguration

Tabelle 5: Checkliste vor der Umstellung

TIPP – Web Application Proxy bleibt unberührt

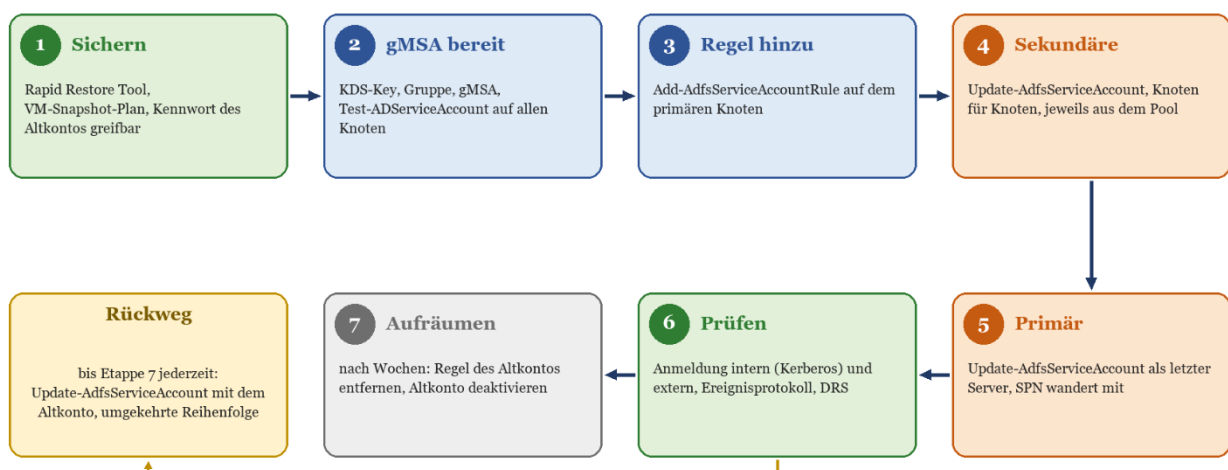
Die WAP-Server laufen nicht unter dem ADFS-Dienstkonto und vertrauen der Farm über ein Zertifikat. Die Umstellung betrifft sie nicht. Nur wenn der Proxy während der Umstellung alle ADFS-Knoten gleichzeitig nicht erreicht, merkt er etwas – und das vermeidest du mit der richtigen Reihenfolge.

Die Reihenfolge

Die Umstellung läuft in sieben Etappen. Die Reihenfolge ist nicht Geschmackssache, sondern folgt der Logik der Farm: Erst muss das neue Konto in der Konfiguration berechtigt sein, dann ziehen die sekundären Knoten um, zuletzt der primäre Knoten, der die farmweiten Einstellungen und den SPN mitnimmt.

Skizze 4: Umstellung einer Bestandsfarm in sieben Etappen

Sekundäre Knoten zuerst, der primäre Knoten zuletzt – das alte Konto bleibt bis zum Schluss am Leben



Das Wartungsfenster betrifft die Etappen 4 und 5. Mit Load Balancer und mindestens zwei Knoten merkt davon im Idealfall niemand etwas – außer dir, weil du um 6 Uhr morgens im Ereignisprotokoll sitzt.

Skizze 4: Die sieben Etappen der Umstellung. Solange das Altkonto aktiv ist und sein Kennwort bekannt ist, bleibt der Rückweg offen.

- **Sichern.** Eine aktuelle Sicherung mit dem Rapid Restore Tool, dazu ein abgestimmter Plan für Snapshots oder Systemsicherungen aller Knoten. Wie das geht, steht in [ADFS sichern und wiederherstellen – Rapid Restore Tool in der Praxis](#).
- **gMSA vorbereiten.** KDS-Root-Key vorhanden, Gruppe gefüllt, gMSA ohne SPN angelegt, Test-ADServiceAccount liefert auf jedem Knoten True.
- **Regel hinzufügen.** Auf dem primären Knoten Add-AdfsServiceAccountRule mit dem neuen Konto ausführen, in WID-Farmen die sekundären Server mitgeben. Die XML-Sicherung, die dabei entsteht, legst du beiseite.
- **Sekundäre Knoten.** Jeden Knoten einzeln am Load Balancer aus dem Pool nehmen, Update-AdfsServiceAccount ausführen, Dienst prüfen, zurück in den Pool. Wie du Knoten sauber aus dem Pool nimmst, beschreibt [ADFS hinter dem Load Balancer – Health Probe, SNI und Persistenz](#).
- **Primärer Knoten.** Zuletzt Update-AdfsServiceAccount auf dem primären Knoten als letzten Server ausführen. Hier wandert der SPN vom Alt- auf das neue Konto.
- **Prüfen.** Interne Anmeldung per Kerberos, externe Anmeldung über den Proxy, Microsoft 365, eine SAML-Anwendung, das ADFS-Admin-Protokoll. Ist der Device Registration Service aktiv, stellst du ihn mit Set-AdfsDeviceRegistration -ServiceAccountIdentifier auf das gMSA um.
- **Aufräumen.** Erst nach einer Beobachtungsphase von einigen Wochen entfernst du mit Remove-AdfsServiceAccountRule die Regel für das Altkonto und deaktivierst es. Löschen kommt noch später.

```
# Auf ALLEN Knoten: Modul importieren
Import-Module .\AdfsServiceAccountModule.psm1

# Etappe 3 – primärer Knoten einer WID-Farm
Add-AdfsServiceAccountRule -ServiceAccount "CONTOSO\gmsa-adfs$" `
    -SecondaryServers adfs02.contoso.local, adfs03.contoso.local

# Etappe 4 – auf adfs02, dann adfs03 (Abfrage: weiterer Federation-Server)
Update-AdfsServiceAccount

# Etappe 5 – auf adfs01 (Abfrage: letzter Federation-Server)
Update-AdfsServiceAccount

# Etappe 6 – nur bei aktivem Device Registration Service
Set-AdfsDeviceRegistration -ServiceAccountIdentifier "CONTOSO\gmsa-adfs$"

# Kontrolle auf jedem Knoten
(Get-CimInstance Win32_Service -Filter "Name='adfssrv']").StartName
setspn -Q HOST/sts.contoso.de

# Etappe 7 – Wochen später, primärer Knoten
Remove-AdfsServiceAccountRule -ServiceAccount "CONTOSO\svc-adfs" `
    -SecondaryServers adfs02.contoso.local, adfs03.contoso.local
```

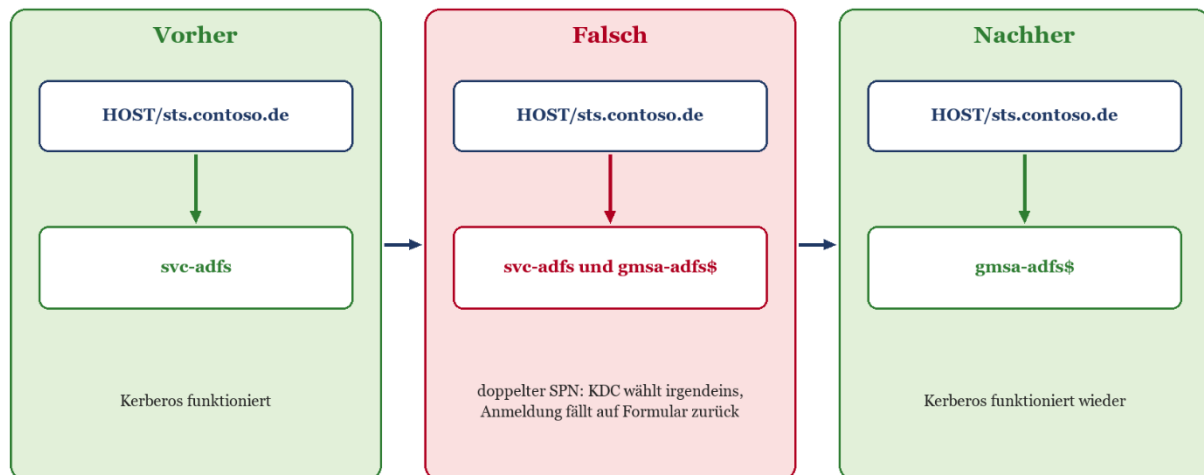
Listing 6: Umstellung einer WID-Farm mit drei Knoten. In einer SQL-Farm entfällt -SecondaryServers.

Der SPN – die Stelle, an der Kerberos zurückschlägt

Der unscheinbarste Teil der Umstellung ist zugleich der, der am häufigsten schiefeht. Der SPN HOST/sts.contoso.de sagt dem Domänencontroller, mit wessen Schlüssel er Tickets für den Federation Service verschlüsseln soll. Solange er am Altkonto hängt, bekommen Clients Tickets, die nur das Altkonto öffnen kann. Laufen die Knoten schon als gMSA, scheitert Kerberos, und der Browser fällt brav auf die Formularanmeldung zurück. Hängt der SPN an beiden Konten, ist es noch schlimmer: Der Domänencontroller kann den Dienst nicht mehr eindeutig zuordnen, und die Fehler werden zufällig.

Skizze 5: Der SPN zieht um – und darf nie an zwei Konten gleichzeitig hängen

HOST/sts.contoso.de entscheidet, mit welchem Schlüssel der DC das Kerberos-Ticket verschlüsselt



Prüfen mit `setspn -Q HOST/sts.contoso.de` und `setspn -X`. Ein Treffer ist richtig. Zwei Treffer sind ein Ticket – nur leider keins von Kerberos.

Skizze 5: Der SPN darf nur an genau einem Konto hängen. Das Umstellungsmodul verschiebt ihn beim letzten Server – prüfen solltest du trotzdem.

Deshalb legst du das gMSA für eine Umstellung ohne SPN an und lässt das Modul den Umzug erledigen. Danach prüfst du mit `setspn -Q`, dass genau ein Konto antwortet, und mit `setspn -X`, dass es keine Duplikate gibt. Clients mit alten Tickets im Cache melden sich bis zum Ablauf des Tickets oder bis zu einem `klist purge` eventuell noch mit Formular an. Wie SPN, DNS-Einträge und Browserzonen für ADFS zusammenspielen, beschreibt [SPN, DNS und Kerberos für ADFS – warum die interne Anmeldung auf Formular zurückfällt](#); die Kerberos-Grundlagen dahinter – Tickets, Schlüssel, Verschlüsselungstypen – stehen auf der Pillar-Seite [Microsoft Kerberos](#).

WICHTIG – Nie einen SPN mit `setspn -A` doppelt eintragen

Wer den SPN von Hand umzieht, nimmt `setspn -S`, nicht `setspn -A`. Die Variante `-S` prüft vor dem Eintragen auf Duplikate und verweigert den Dienst, wenn der SPN schon an einem anderen Konto hängt. Reihenfolge von Hand: erst mit `setspn -D` vom Altkonto entfernen, dann mit `setspn -S` am gMSA eintragen.

Risiken und Gegenmittel

Risiko	Symptom	Gegenmittel
Autorisierungsregel fehlt	adfsrv startet nicht oder protokolliert Zugriffsfehler auf die Konfiguration	Add-AdfsServiceAccountRule vor dem ersten Update-AdfsServiceAccount
Computer kennt Gruppenmitgliedschaft noch nicht	Test-ADServiceAccount liefert False, Dienst startet nicht	Neustart oder <code>klist -li ox3e7 purge</code>
KDS-Root-Key zu jung	Kennwortabruf schlägt fehl, obwohl alles richtig aussieht	Wartezeit abwarten, Replikation prüfen
SPN falsch oder doppelt	interne Anmeldung fällt auf Formular zurück	<code>setspn -Q</code> und <code>setspn -X</code> , SPN genau einmal
Attributspeicher oder Adapter ohne Rechte	Claims fehlen, einzelne Anwendungen melden Fehler	Bestandsaufnahme, Rechte vorab für das gMSA vergeben
SQL-Login fehlt (SQL-	Dienst startet, findet aber seine	Moduldurchlauf prüfen, Login und

Farm)	Datenbank nicht	Rechte im SQL Server kontrollieren
Altkonto zu früh deaktiviert	vergessene Aufgaben scheitern, Rückweg ist verbaut	Beobachtungsphase, erst deaktivieren, spät löschen

Tabelle 6: Was bei der Umstellung schiefgehen kann – und wie du es verhinderst

Die Ereignisse, die du in dieser Phase im Blick behalten solltest, stehen im ADFS-Admin-Protokoll und im Systemprotokoll der Dienststeuerung. Wie du sie liest und wann sich Debug-Tracing lohnt, zeigt [ADFS-Ereignisprotokolle lesen – Admin-Log, Debug-Tracing und Auditing](#). Klemmt die Anmeldung trotz allem, hilft die Systematik aus [ADFS-Anmeldung schlägt fehl – die häufigsten Ursachen und ihre Lösung](#).

Der Rückweg

Ein Rollback ist bei dieser Umstellung erfreulich unspektakulär – vorausgesetzt, du hast drei Dinge nicht getan: das Altkonto deaktiviert, sein Kennwort vergessen oder die Regel für das Altkonto entfernt. Dann führst du Update-AdfsServiceAccount einfach erneut aus, diesmal mit dem Altkonto und seinem Kennwort, wieder sekundäre Knoten zuerst und den primären zuletzt. Der SPN wandert dabei zurück.

- Ist bei Add-AdfsServiceAccountRule oder Remove-AdfsServiceAccountRule etwas schiefgegangen, stellst du die Autorisierungseinstellungen mit Restore-AdfsSettingsFromBackup -BackupPath und der XML-Datei wieder her.
- Ist die Farm insgesamt in einem Zustand, den du nicht mehr verstehst, ist die Sicherung aus Etappe 1 dein Freund. Das Rapid Restore Tool stellt die ADFS-Konfiguration wieder her, nicht das Active Directory – den SPN prüfst du danach von Hand.
- Snapshots von ADFS-Servern sind ein Notfallwerkzeug für einzelne Knoten, kein Rollback-Konzept für die ganze Farm. Bei WID-Farmen gehört mindestens der primäre Knoten in die Sicherung, bei SQL-Farmen die Datenbank.

FAKTEN — Aus der Praxis, anonymisiert

Eine Farm mit vier Knoten, betrieben seit 2014, Dienstkonto Mitglied der Domänen-Admins. Die Umstellung selbst dauerte am Ende 50 Minuten. Die Vorbereitung zwei Wochen – denn in der Bestandsaufnahme tauchten ein SQL-Attributspeicher auf, der sich mit dem Dienstkonto an einer Personaldatenbank anmeldete, und drei geplante Aufgaben, die unter svc-adfs Berichte verschickten. Die Domänen-Admin-Mitgliedschaft wurde übrigens nie gebraucht. Sie war 2014 eingetragen worden, weil der SPN fehlte und die interne Anmeldung nicht funktionierte. Der SPN wurde zwei Tage später gesetzt. Die Mitgliedschaft blieb zehn Jahre.

Fazit

Ein gMSA als ADFS-Dienstkonto ist keine Kür, sondern schlichte Betriebshygiene. Es nimmt dem wichtigsten Konto deiner Anmeldeinfrastruktur den menschlichen Kennwortbesitzer, wechselt seine Schlüssel von selbst und lässt sich nur von den Servern benutzen, die du dafür vorgesehen hast. Bei einer neuen Farm kostet es genau einen Parameter. Bei einer Bestandsfarm kostet es eine gründliche Bestandsaufnahme, einen Tag Vorlauf für den KDS-Root-Key und ein ruhiges Wartungsfenster. Das ist wenig im Vergleich zu dem, was ein kompromittiertes Dienstkonto mit Domänen-Admin-Rechten kostet.

Und ganz gleich, ob deine Farm noch zehn Jahre läuft oder der Ausstieg nach Entra ID schon geplant ist: Solange ADFS Token für dein Unternehmen ausstellt, gehört es sauber betrieben. Wenn du die Umstellung nicht allein planen willst, ist das ein typischer Fall für [Consulting zu ADFS \(Active Directory Federation Services\)](#). Das Anlegen von gMSA, KDS-Root-Key und die

Umstellung einer Übungsfarm kannst du in den [ADFS-Schulungen](#) selbst durchspielen. Und wer Dienstkonto, Zertifikate und Farmbetrieb im Zusammenhang nachlesen möchte, findet das ausführlich in [ADFS in der Praxis – das Buch im Detail](#).

WEITER — Passend zu diesem Beitrag

- › [SPN, DNS und Kerberos für ADFS – warum die interne Anmeldung auf Formular zurückfällt](#)
- › [ADFS-Farm installieren – Schritt für Schritt auf Windows Server 2022](#)
- › [ADFS-Sicherheit: Angriffe, Härtung, Golden SAML und MFA](#)
- › [ADFS sichern und wiederherstellen – Rapid Restore Tool in der Praxis](#)
- › [Microsoft Kerberos](#)

FAQ

Unterstützt ADFS überhaupt ein gMSA als Dienstkonto?

Ja, seit AD FS 3.0 unter Windows Server 2012 R2. Microsoft bezeichnet das gMSA als empfohlene Option; das klassische Benutzerkonto ist nur noch für Domänen mit sehr alter Funktionsebene gedacht.

Wie lange muss ich nach Add-KdsRootKey warten?

Die Domänencontroller warten bis zu 10 Stunden ab Erstellung, damit der Schlüssel überall repliziert ist. In der Produktion solltest du diese Zeit abwarten; das Zurückdatieren der EffectiveTime ist nur für Testumgebungen mit einem einzigen Domänencontroller vorgesehen.

Warum liefert Test-ADServiceAccount False?

Meist kennt der Server seine neue Gruppenmitgliedschaft noch nicht. Ein Neustart oder klist -li ox3e7 purge hilft. Weitere Ursachen sind ein zu junger oder nicht replizierter KDS-Root-Key, ein Tippfehler im Namen oder ein Server, der gar nicht in PrincipalsAllowedToRetrieveManagedPassword steht.

Kann ich das Dienstkonto einfach in der Dienste-Konsole umstellen?

Nicht zuverlässig. Ab AD FS unter Windows Server 2016 fehlt dem neuen Konto dann die Autorisierungsregel in der Konfiguration, außerdem Schlüssel-, Datenbank- und DKM-Rechte sowie der SPN. Nimm das Service-Account-Modul aus der ADFS-Toolbox.

In welcher Reihenfolge stelle ich die Knoten um?

Zuerst Add-AdfsServiceAccountRule auf dem primären Knoten, dann Update-AdfsServiceAccount auf allen sekundären Knoten und zuletzt auf dem primären Knoten als letztem Server. Erst dabei zieht der SPN um.

Braucht das ADFS-Dienstkonto Domänen-Admin-Rechte?

Nein. ADFS braucht einen SPN, lokale Dienstrechte, Zugriff auf seine Datenbank, die Zertifikatsschlüssel und den DKM-Container. Domänen-Admin-Rechte machen aus jedem kompromittierten ADFS-Server eine kompromittierte Domäne.

Muss ich den Web Application Proxy anpassen?

Nein. Der Proxy läuft nicht unter dem ADFS-Dienstkonto und vertraut der Farm über ein Zertifikat. Wichtig ist nur, dass während der Umstellung immer mindestens ein ADFS-Knoten erreichbar bleibt.

Wann darf ich das alte Dienstkonto löschen?

Erst nach einer Beobachtungsphase. Entferne zuerst mit `Remove-AdfsServiceAccountRule` die Regel des Altkontos, deaktiviere es dann und lösche es erst, wenn über Wochen keine vergessene Aufgabe und kein Attributspeicher mehr danach gerufen hat.

Kann ich das Kennwortintervall des gMSA später ändern?

Nein. `ManagedPasswordIntervalInDays` lässt sich nur beim Anlegen setzen. Für ein anderes Intervall brauchst du ein neues gMSA – und damit eine weitere Umstellung.