

ADFS-Farm upgraden – Farm Behavior Level anheben ohne Ausfall

WISSEN

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

› [Active Directory Federation Services](#)

BERATUNG

Upgrade-Plan, Rollback-Punkte und Change-Fenster gemeinsam festzurren – bevor die Farm es für dich tut.

› [Consulting zu ADFS](#)

SCHULUNG

Knotentausch, Primärrolle und FBL-Hochstufung im Workshop an einer echten Farm üben.

› [ADFS-Schulungen](#)

Es gibt ADFS-Farmen, die sind älter als manches Azubi-Team. Sie laufen auf Windows Server 2016, manchmal noch auf 2012 R2, haben drei Admin-Generationen überlebt und funktionieren so zuverlässig, dass niemand sie anfassen will. Genau das ist das Problem. Irgendwann klopft der Lebenszyklus des Betriebssystems an, das Audit fragt nach dem Patchstand, und plötzlich steht auf deinem Zettel: „ADFS upgraden, bitte ohne Ausfall.“ Das klingt nach einem Wochenende mit viel Kaffee und wenig Schlaf. Muss es aber nicht sein.

Denn ADFS bringt seit Windows Server 2016 einen eingebauten Upgrade-Mechanismus mit, den Farm Behavior Level. Du baust keine neue Farm, exportierst keine Relying Party Trusts und betest nicht, dass die Claim Rules den Umzug überleben. Stattdessen holst du neue Server in die bestehende Farm, verschiebst die Primärrolle, verabschiedest die alten Knoten und hebst am Ende das Level an. Der Web Application Proxy zieht hinterher. Dieser Beitrag geht den Weg Schritt für Schritt – mit echten Cmdlets, einem Ablaufplan samt Rollback-Punkten und den Stellen, an denen es in der Praxis knirscht. Die Grundlagen zu Farm, Datenbank und Proxy setzen wir voraus; die findest du auf der Pillar-Seite [Active Directory Federation Services](#) und im Beitrag [ADFS: Architektur, Einsatzszenarien und Hochverfügbarkeit](#).

Ein Wort zur Grundhaltung, bevor es losgeht: Microsoft schreibt über jede Upgrade-Anleitung inzwischen den Hinweis, dass statt eines ADFS-Upgrades die Migration nach Microsoft Entra ID empfohlen wird. Das ist richtig und trotzdem kein Grund, eine Farm auf einem alten Betriebssystem verrotten zu lassen. Die Migration braucht Zeit, Bestandsaufnahme und Nerven. Bis dahin muss ADFS sauber laufen. Ein Upgrade auf ein aktuelles Windows Server ist die Hausaufgabe, die dir die Zeit für einen geordneten Ausstieg verschafft.

FAKTEN – Die Kurzfassung für Eilige

Der Weg führt über neue Knoten: Server mit der neuen Windows-Version treten der bestehenden Farm bei. Die Farm läuft dann im Mischbetrieb auf dem bisherigen Farm Behavior Level (FBL).

Belegte Zuordnung laut Microsoft: Windows Server 2012 R2 = FBL 1, Windows Server 2016 = FBL 3, Windows Server 2019 und 2022 = FBL 4.

Schema-Voraussetzung: Ziel Windows Server 2016 oder neuer verlangt ein AD-Schema von mindestens 85, Ziel 2019 oder neuer mindestens 88.

Bei WID wandert die Primärrolle per Set-AdfsSyncProperties auf einen neuen Knoten. Bei SQL Server entfällt dieser Schritt, dort gelten alle Knoten als primär.

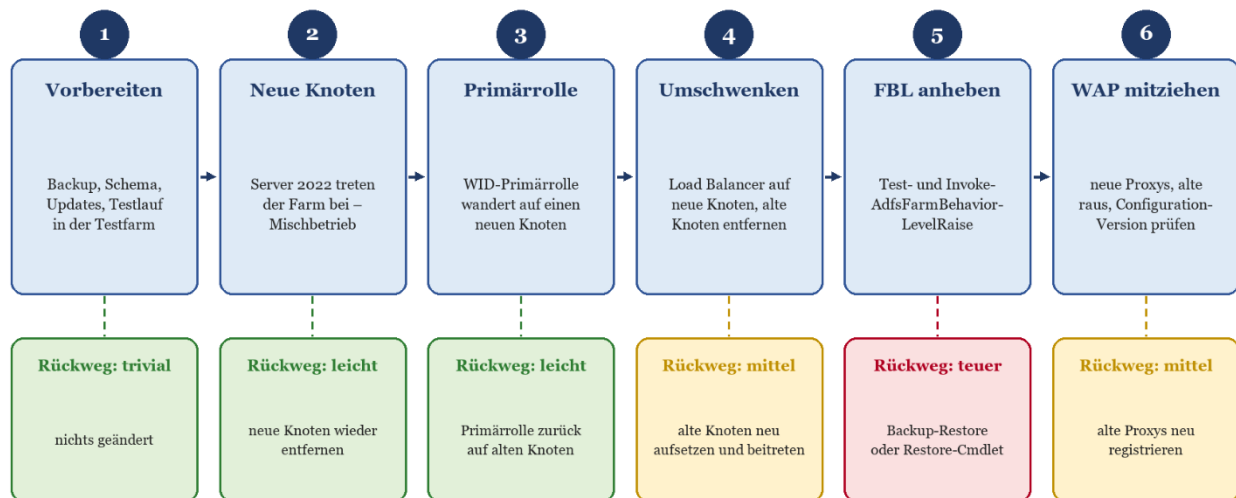
Die Hochstufung erledigen Test-AdfsFarmBehaviorLevelRaise und Invoke-AdfsFarmBehaviorLevelRaise. Dabei entsteht eine neue Konfigurationsdatenbank.

Danach folgt der Web Application Proxy: neue Proxys per Install-WebApplicationProxy, alte abmelden, ConfigurationVersion prüfen.

„Ohne Ausfall“ heißt ehrlich gesagt: ohne ungeplanten Ausfall. Die FBL-Hochstufung selbst beschreibt Microsoft als relativ kurze Unterbrechung – plane dafür ein Wartungsfenster.

Skizze 1: Der Upgrade-Pfad in sechs Etappen

Oben die Arbeit, unten die Frage, wie teuer der Rückweg an dieser Stelle wird



Bis einschließlich Etappe 3 ist alles ein Spaziergang mit Notausgang. Ab Etappe 4 sind die alten Knoten weg, ab Etappe 5 ist die Farm auf einer neuen Konfigurationsdatenbank. Wer hier ohne Backup steht, betreibt Identitätsmanagement als Mutprobe.

Skizze 1: Die sechs Etappen des Upgrades und darunter, wie aufwendig der Rückweg an jeder Stelle ist. Bis zur Primärrolle ist alles umkehrbar, ab der FBL-Hochstufung wird es teuer.

Bestandsaufnahme: Wo steht deine Farm?

Bevor du einen neuen Server auch nur auspackst, willst du drei Dinge wissen: auf welchem Farm Behavior Level die Farm läuft, welche Knoten sie zu kennen glaubt und welche Datenbank dahinter steckt. Die letzte Frage klingt banal, entscheidet aber über die Hälfte der folgenden Schritte.

Farm Behavior Level und Knoten abfragen

Auf jedem ADFS-Server ab Windows Server 2016 liefert ein einziges Cmdlet die Antwort. Achte auf CurrentFarmBehavior und FarmNodes. In der Knotenliste tauchen gern Server auf, die seit Jahren nicht mehr existieren – Leichen aus früheren Umbauten, die niemand ausgetragen hat.

```
# Auf einem ADFS-Knoten, PowerShell als Administrator
Get-AdfsFarmInformation

# Nur das Wichtigste
Get-AdfsFarmInformation | Select-Object CurrentFarmBehavior, FarmNodes

# WID oder SQL? Die Antwort steckt in der Verbindungszeichenfolge
(Get-WmiObject -Namespace root/ADFS -Class
SecurityTokenService).ConfigurationDatabaseConnectionString

# WID: Wer ist primär, wer sekundär?
Get-AdfsSyncProperties
```

Bestandsaufnahme auf einem ADFS-Knoten. Get-AdfsFarmInformation gibt es ab Windows Server 2016; auf einer reinen 2012-R2-Farm fehlt das Cmdlet, dort liegt das Level implizit bei 1.

Die folgende Tabelle zeigt die Zuordnung, die Microsoft für Farm Behavior Level und Konfigurationsdatenbank dokumentiert. Mehr gibt es nicht, auch wenn Foren gern anderes erzählen. Ein FBL 2 existiert nicht, und Windows Server 2019 und 2022 teilen sich dasselbe Level.

Windows Server	FBL-Wert	Konfigurationsdatenbank	Schema für Hochstufung
2012 R2	1	AdfsConfiguration	–

2016	3	AdfsConfigurationV3	mindestens 85
2019	4	AdfsConfigurationV4	mindestens 88
2022	4	AdfsConfigurationV4	mindestens 88

Tabelle 1: Belegte Zuordnung von Windows-Server-Version, Farm Behavior Level und Datenbankname laut Microsoft.

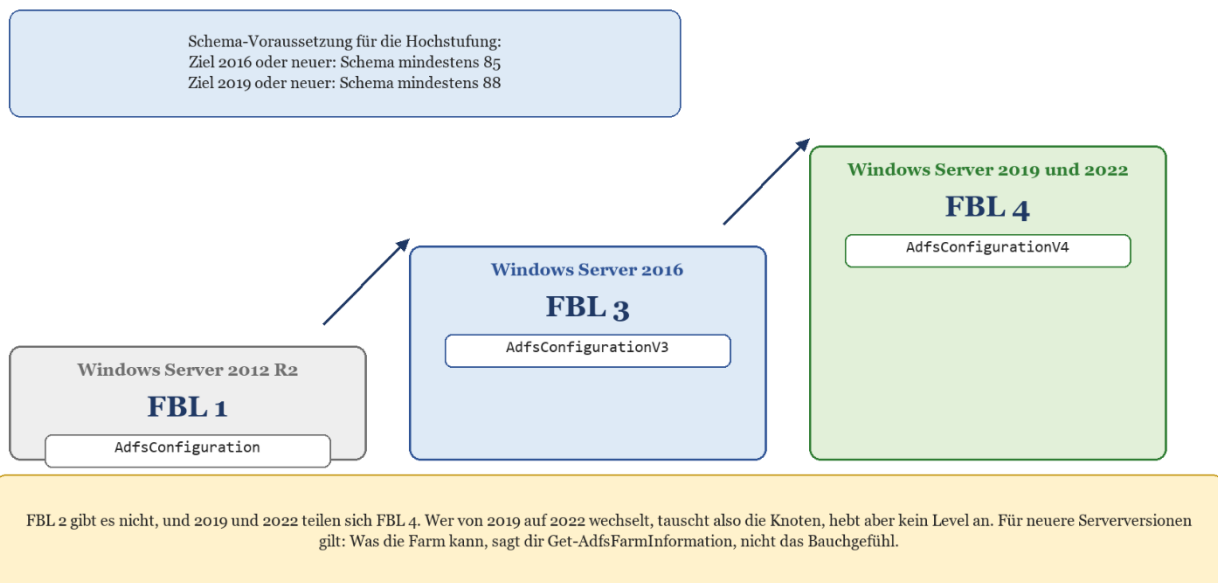
WICHTIG – 2019 auf 2022 ist ein Knotentausch, kein Levelsprung

Läuft deine Farm auf Windows Server 2019 und du willst auf 2022, bleibt das Farm Behavior Level bei 4. Du tauschst Knoten, verschiebst die Primärrolle und ziehst den WAP mit – aber Invoke-AdfsFarmBehaviorLevelRaise hat nichts zu tun. Test-AdfsFarmBehaviorLevelRaise wird dir das auch so sagen.

Für Windows Server 2025 führt Microsofts FBL-Tabelle zum Zeitpunkt dieses Beitrags keinen eigenen Wert auf. Die FBL-Cmdlets sind im ADFS-Modul für 2025 dokumentiert. Verlass dich deshalb nicht auf eine Zahl aus einem Blog, sondern auf das, was Test-AdfsFarmBehaviorLevelRaise und Get-AdfsFarmInformation in deiner Testfarm melden.

Skizze 3: Farm Behavior Level und Konfigurationsdatenbank

Die belegte Zuordnung laut Microsoft – jede Hochstufung legt eine neue Datenbank an



Skizze 3: Die Treppe der Farm Behavior Levels. Jede Stufe bringt eine eigene Konfigurationsdatenbank mit, und die Hochstufung verlangt ein ausreichend aktuelles AD-Schema.

Schema, Updates und Backup

Die Schema-Anforderung ist der Klassiker, an dem ein Upgrade am Samstagvormittag hängen bleibt. Die Domänencontroller dürfen durchaus noch auf älteren Versionen laufen, entscheidend ist die Schemaversion des Forests. Die fragst du in zehn Sekunden ab:

```
# Schemaversion des Forests (Modul ActiveDirectory)
Get-ADObject (Get-ADRootDSE).schemaNamingContext -Properties objectVersion |
Select-Object objectVersion
```

Liefert die objectVersion des Schemas. Für ein Ziel ab Windows Server 2019 muss hier mindestens 88 stehen.

Reicht die Version nicht, steht vor dem ADFS-Upgrade eine Schemaerweiterung mit adprep /forestprep aus dem Installationsmedium der Zielversion an. Das ist ein Change mit eigenem Genehmigungsweg in den meisten Häusern, also plane ihn nicht für Freitag, 16 Uhr. Ebenfalls Pflicht: Die neuen Server sind vollständig gepatcht, bevor sie der Farm beitreten, und du hast ein

aktuelles Backup der Farmkonfiguration. Wie das mit dem Rapid Restore Tool geht, steht im Beitrag [ADFS sichern und wiederherstellen – Rapid Restore Tool in der Praxis](#).

WARNUNG – Kein In-Place-Upgrade des Betriebssystems

Microsoft beschreibt den Weg ausschließlich über neue Server. Für den Schritt von 2012 R2 auf 2016 heißt es ausdrücklich: Ein alter Knoten wird durch ein Betriebssystem-Upgrade nicht zu einem neuen Knoten, er muss entfernt und durch einen frisch installierten ersetzt werden. Übertrag das auf jede Version. Ein In-Place-Upgrade eines ADFS-Servers ist der schnellste Weg zu einer Farm, die sich selbst nicht mehr versteht.

WID oder SQL Server – was sich am Ablauf ändert

Die meisten Farmen laufen mit der Windows Internal Database. Dort gibt es genau einen primären Knoten, der schreiben darf; alle anderen ziehen sich die Änderungen regelmäßig ab. Bei SQL Server schreiben alle Knoten in dieselbe Datenbank. Das hat Folgen für die Primärrolle, für die Hochstufung und für etwaige Replikation. Die Details zur Wahl der Datenbank erklärt [WID oder SQL Server als ADFS-Konfigurationsdatenbank](#).

Aspekt	Windows Internal Database	SQL Server
Primärrolle	ein primärer Knoten, muss per Set-AdfsSyncProperties verschoben werden	entfällt, alle Knoten gelten als primär
Hochstufung	Invoke-AdfsFarmBehaviorLevelRaise ohne weitere Anmeldedaten	Invoke-AdfsFarmBehaviorLevelRaise - Credential mit Administratorrechten auf SQL Server und allen ADFS-Knoten
Neue Datenbank	entsteht lokal in der WID jedes Knotens	entsteht auf dem SQL Server, Rechte des Dienstkontos vorher prüfen
Replikation	eigene WID-Synchronisation, keine Vorarbeit	AlwaysOn-Verfügbarkeitsgruppen oder Merge-Replikation vorher entfernen und danach für die neuen Datenbanken neu einrichten
Typischer Stolperstein	vergessene Sekundäre, die noch auf den alten Primären zeigen	fehlende Rechte des Kontos, das die Hochstufung ausführt

Tabelle 2: Was sich beim Upgrade je nach Konfigurationsdatenbank unterscheidet.

Neue Knoten beitreten lassen und die Primärrolle verschieben

Jetzt wird es konkret. Unser Beispiel: eine WID-Farm mit ADFS01 und ADFS02 auf Windows Server 2016, Dienstname sts.contoso.de, gMSA als Dienstkonto, davor zwei Web Application Proxys WAP01 und WAP02. Ziel ist Windows Server 2022. Dazu kommen ADFS03 und ADFS04 als neue Knoten, später WAP03 und WAP04. Alles läuft in der Domäne contoso.local.

Die neuen Server vorbereiten

Die neuen Knoten bekommen ein frisches, vollständig gepatchtes Windows Server, die Rolle ADFS und das SSL-Zertifikat des Dienstnamens samt privatem Schlüssel. Wenn die Farm ein gMSA nutzt, müssen die neuen Computerkonten berechtigt sein, dessen Kennwort abzurufen – sonst scheitert der Beitritt mit einer Fehlermeldung, die eher nach Kerberos als nach Rechten klingt. Wie du die Berechtigung ergänzt, zeigt [gMSA als ADFS-Dienstkonto einrichten und umstellen](#). Den Zertifikatsimport auf ADFS und WAP beschreibt [SSL-Zertifikat auf ADFS und Web Application Proxy tauschen](#); die Grundinstallation einer Farm auf Windows Server 2022 steht in [ADFS-Farm installieren – Schritt für Schritt auf Windows Server 2022](#).

```
# Auf ADFS03 und ADFS04
Install-WindowsFeature ADFS-Federation -IncludeManagementTools

# gMSA-Berechtigung für die neuen Computerkonten ergänzen (auf einem DC, Modul ActiveDirectory)
Set-ADServiceAccount -Identity gmsa-adfs `
    -PrincipalsAllowedToRetrieveManagedPassword "ADFS01$","ADFS02$","ADFS03$","ADFS04$"

# Auf ADFS03: Beitritt zur WID-Farm, Primärer ist noch ADFS01
$thumb = "<Fingerabdruck des SSL-Zertifikats für sts.contoso.de>"
Add-AdfsFarmNode -GroupServiceAccountIdentifier "CONTOSO\gmsa-adfs$" `
    -PrimaryComputerName "adfs01.contoso.local" `
    -CertificateThumbprint $thumb

# Variante für eine SQL-Farm
# Add-AdfsFarmNode -GroupServiceAccountIdentifier "CONTOSO\gmsa-adfs$" `
#     -SQLConnectionString "Data Source=sql01.contoso.local;Integrated Security=True" `
#     -CertificateThumbprint $thumb
```

Beitritt eines neuen Knotens per PowerShell. Der Assistent im Server-Manager erledigt dasselbe mit „Einem Verbundserverfarm einen Verbundserver hinzufügen“.

WARNUNG – PrincipalsAllowedToRetrieveManagedPassword ersetzt, statt zu ergänzen

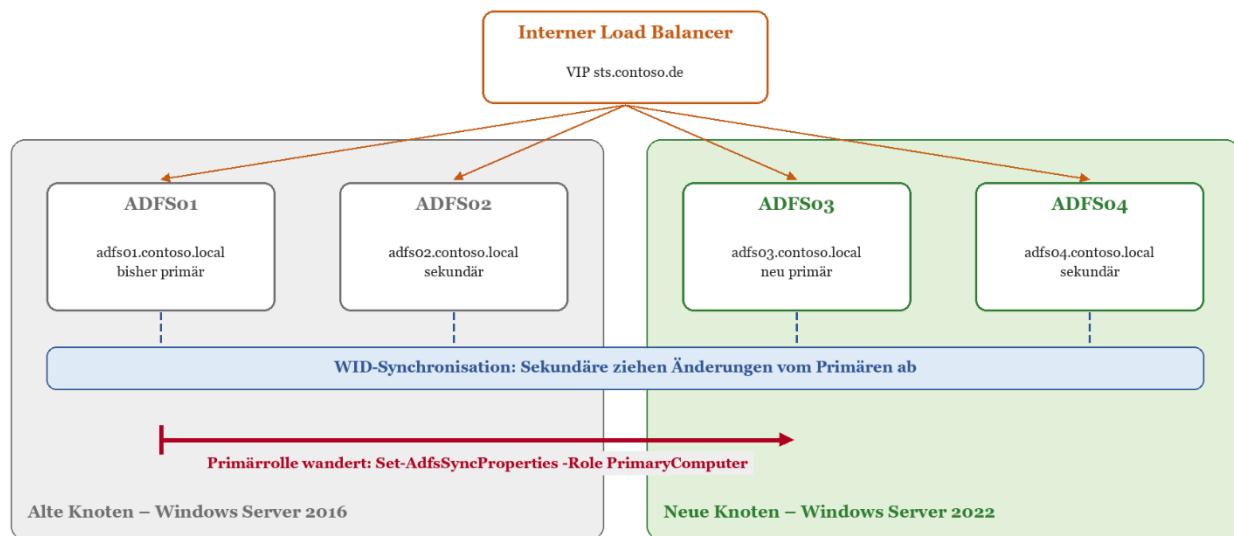
Set-ADServiceAccount mit diesem Parameter schreibt die Liste neu. Wer nur die neuen Server einträgt, sperrt die alten Knoten aus, sobald deren zwischengespeichertes Kennwort abläuft. Deshalb stehen im Beispiel alle vier Computerkonten. Wenn du mit einer Gruppe arbeitest, nimmst du stattdessen einfach die neuen Server in die Gruppe auf und startest sie neu.

Mischbetrieb: was jetzt geht und was nicht

Sobald ADFS03 und ADFS04 beigetreten sind, läuft die Farm im Mischbetrieb. Die neuen Knoten arbeiten auf dem Farm Behavior Level der alten, also FBL 3. Sie bedienen Anmeldungen genauso wie ihre älteren Kollegen, können aber keine Funktionen nutzen, die erst mit dem höheren Level kommen. Das ist gewollt: Die Farm verhält sich konsistent, egal welcher Knoten die Anfrage bekommt.

Skizze 2: Die WID-Farm im Mischbetrieb

Alte und neue Knoten laufen gemeinsam auf dem alten Farm Behavior Level – die Primärrolle wandert



Skizze 2: Mischbetrieb in der WID-Farm. Alte und neue Knoten laufen gemeinsam, die Primärrolle wandert von ADFS01 auf ADFS03, die übrigen Knoten synchronisieren vom neuen Primären.

Microsoft rät ausdrücklich davon ab, den Mischbetrieb lange stehen zu lassen. Plane das Upgrade also mit einem festen Zeitrahmen: Tage, nicht Monate. Die Versuchung ist groß, nach dem Beitritt der neuen Knoten erst einmal durchzuatmen und das Projekt ins nächste Quartal zu schieben. Genau so entstehen Farmen, in denen drei Jahre später niemand mehr weiß, warum ein 2016er-Knoten noch mitläuft.

TIPP – Neue Knoten testen, bevor der Load Balancer sie kennt

Trag auf einem Testclient per HOSTS-Datei sts.contoso.de direkt auf die IP von ADFS03 ein. Dann prüfst du die Metadaten unter /FederationMetadata/2007-06/FederationMetadata.xml, die Health Probe unter /adfs/probe auf Port 80 und eine echte Anmeldung an einer unkritischen Relying Party. Erst wenn das klappt, kommt der Knoten in den Pool.

Die IdP-initiierte Anmeldeseite ist ab Windows Server 2016 standardmäßig abgeschaltet. Wenn du sie für den Test brauchst, schalte sie mit Set-AdfsProperties -EnableIdpInitiatedSignonPage \$true bewusst ein – und danach bewusst wieder aus.

Die Primärrolle bei WID verschieben

Solange ADFS01 primär ist, hängt die gesamte Schreibfähigkeit der Farm an einem Server, den du demnächst abschalten willst. Also wandert die Rolle vorher auf einen neuen Knoten. Die Reihenfolge ist wichtig: erst den neuen Primären ernennen, dann allen anderen Knoten – alten wie neuen – den neuen Primären mitteilen. Zwischen beiden Schritten gibt es kurz zwei Knoten, die sich für primär halten. Das ist unschön, aber harmlos, solange du in dieser Zeit nicht an der Konfiguration schraubst.

```
# Auf ADFS03: wird neuer Primärer
Set-AdfsSyncProperties -Role PrimaryComputer
```

```
# Auf ADFS01, ADFS02 und ADFS04: auf den neuen Primären zeigen
```

```
Set-AdfsSyncProperties -Role SecondaryComputer -PrimaryComputerName "adfs03.contoso.local"
```

```
# Kontrolle auf jedem Knoten
```

```
Get-AdfsSyncProperties | Select-Object Role, PrimaryComputerName, LastSyncStatus
```

Primärrolle einer WID-Farm verschieben. Bei SQL Server entfällt dieser Schritt komplett.

Warte nach der Umstellung mindestens einen Synchronisationszyklus ab und prüfe auf jedem sekundären Knoten, ob die letzte Synchronisation erfolgreich war. Ein Sekundärer, der noch auf ADFS01 zeigt, fällt erst auf, wenn ADFS01 weg ist und er keine Änderungen mehr bekommt. Dann ist er ein Knoten mit eingefrorener Konfiguration, und der nächste neue Relying Party Trust funktioniert nur jedes zweite Mal. Das ist die Sorte Fehler, die man in Ereignisprotokollen findet, wenn man weiß, wo man suchen muss – siehe [ADFS-Ereignisprotokolle lesen – Admin-Log, Debug-Tracing und Auditing](#).

Load Balancer umschwenken und alte Knoten entfernen

Jetzt nimmt der Load Balancer die neuen Knoten in den Pool auf und lässt die alten leerlaufen. Die meisten Geräte können einen Real Server in einen Drain-Zustand versetzen: keine neuen Verbindungen, bestehende laufen aus. Da ADFS für die Anmeldung zustandslos ist, geht das schnell. Wie Health Probe und Pool richtig eingestellt sind, steht in [ADFS hinter dem Load Balancer – Health Probe, SNI und Persistenz](#); für ein konkretes Gerät hilft die Pillar-Seite [Kemp LoadMaster](#).

Skizze 5: Der Load-Balancer-Pool im Zeitverlauf

Wer ist wann aktiv? Grün nimmt Anmeldungen an, Gelb läuft leer, Grau ist raus

	To Start	T1 Beitritt	T2 Primärrolle	T3 Umschwenken	T4 Entfernt
ADFS01 (2016)	aktiv	aktiv	aktiv	Drain	entfernt
ADFS02 (2016)	aktiv	aktiv	aktiv	Drain	entfernt
ADFS03 (2022)	–	Test per HOSTS	aktiv	aktiv	aktiv
ADFS04 (2022)	–	Test per HOSTS	aktiv	aktiv	aktiv

Der Trick heißt: nie mehr als einen Schritt gleichzeitig. Die neuen Knoten beweisen sich erst per HOSTS-Eintrag auf einem Testclient, dann im Pool. Die alten laufen leer, bevor jemand die Rolle deinstalliert.

Skizze 5: Der Load-Balancer-Pool im Zeitverlauf. Neue Knoten beweisen sich erst per HOSTS-Eintrag, alte laufen leer, bevor sie aus der Farm verschwinden.

Haben ADFS01 und ADFS02 eine Weile keine Anfragen mehr bekommen und alles läuft sauber, deinstallierst du auf ihnen die Rolle und trägst sie aus der Farm aus. Der zweite Schritt wird gern vergessen – und dann steht der Server in Get-AdfsFarmInformation noch Jahre später als Knoten herum.

```
# Auf ADFS01 und ADFS02
```

```
Uninstall-WindowsFeature ADFS-Federation
```

```
Restart-Computer
```

```
# Auf dem neuen Primären ADFS03: Einträge bereinigen
```

```
Set-AdfsFarmInformation -RemoveNode "adfs01.contoso.local"
```

```
Set-AdfsFarmInformation -RemoveNode "adfs02.contoso.local"
```

```
# Kontrolle: nur noch neue Knoten
Get-AdfsFarmInformation | Select-Object -ExpandProperty FarmNodes
```

Alte Knoten sauber verabschieden. Erst danach lässt sich das Farm Behavior Level anheben.

Farm Behavior Level anheben

Jetzt kommt der Moment, auf den der ganze Aufwand hinausläuft. Die Farm besteht nur noch aus Knoten der neuen Version, die Primärrolle sitzt auf ADFS03, der Load Balancer ist zufrieden. Solange noch ein Knoten mit älterer Version in der Farm steht, verweigert die Hochstufung ihren Dienst. Das ist keine Schikane, sondern Selbstschutz.

Erst testen, dann anheben

Test-AdfsFarmBehaviorLevelRaise prüft die Voraussetzungen, ohne etwas zu verändern – etwa, ob alle Knoten die neue Version haben und erreichbar sind. Lies die Ausgabe vollständig. Die Meldungen sind nicht immer elegant formuliert, aber sie sind ehrlich. Erst wenn der Test sauber durchläuft, folgt die eigentliche Hochstufung auf dem primären Knoten.

```
# Auf dem primären Knoten ADFS03 (WID)
Test-AdfsFarmBehaviorLevelRaise

# Hochstufung, mit Rückfrage
Invoke-AdfsFarmBehaviorLevelRaise

# Mit gMSA ausdrücklich angeben
Invoke-AdfsFarmBehaviorLevelRaise -GroupServiceAccountIdentifier "CONTOSO\gmsa-adfs$"

# SQL-Farm: Anmeldedaten mit Administratorrechten auf SQL Server und allen ADFS-Knoten
$cred = Get-Credential
Invoke-AdfsFarmBehaviorLevelRaise -Credential $cred

# Ergebnis prüfen
Get-AdfsFarmInformation | Select-Object CurrentFarmBehavior, FarmNodes
```

Die Hochstufung. Das Cmdlet hebt auf das höchste Level an, das alle Knoten unterstützen; eine Zielzahl gibst du nicht an.

FAKTEN – Was bei der Hochstufung passiert

Die Hochstufung legt eine neue Konfigurationsdatenbank an, bei einer Farm auf Windows Server 2022 also AdfsConfigurationV4. Die Farm arbeitet danach mit dieser Datenbank.

Microsoft beschreibt den gesamten Upgrade-Weg als online durchführbar – mit Ausnahme einer relativ kurzen Unterbrechung während der FBL-Hochstufung selbst.

Bei SQL Server muss das Konto hinter -Credential Administrator auf jedem ADFS-Server sein und auf dem SQL Server die nötigen Rechte haben. Das ADFS-Dienstkonto braucht Zugriff auf die neue Datenbank.

Ein Zielniveau gibt es nicht als Parameter: Das Cmdlet hebt auf die höchste Stufe an, die die Knoten der Farm unterstützen.

Das Wartungsfenster: ehrlich planen

Der Titel dieses Beitrags verspricht „ohne Ausfall“, und das stimmt für fast alle Schritte. Knoten hinzufügen, Primärrolle verschieben, Load Balancer umschwenken, alte Knoten entfernen – all das bemerkt niemand, wenn du sauber arbeitest. Die Hochstufung selbst ist die Ausnahme. Sie dauert nicht lange, aber sie greift in die Datenbank ein, und in diesem Moment willst du keine Montagmorgen-Anmeldewelle haben. Also: kurzes Wartungsfenster am frühen Morgen oder Abend, vorher angekündigt, mit jemandem am Telefon, der Microsoft 365 und zwei, drei kritische Anwendungen testet.

Der schwarzhumorige Teil der Wahrheit: Die meisten Ausfälle bei ADFS-Upgrades entstehen nicht durch die Hochstufung, sondern durch das, was nebenbei passiert. Jemand nutzt das Fenster, um „schnell noch“ das SSL-Zertifikat zu tauschen. Ein anderer patcht die Domänencontroller. Ein Dritter räumt die Firewall-Regeln der DMZ auf. Wenn dann etwas klemmt, weiß niemand mehr, was es war. Ein Change, eine Änderung.

Nach der Hochstufung: prüfen, was du prüfen kannst

Nach der Hochstufung ist vor der Kontrolle. Die Zertifikate, die Relying Party Trusts, die Claims Provider Trusts und die Zugriffsrichtlinien sollten unverändert da sein. Vergleich die Zahl der Trusts mit deiner Bestandsaufnahme von vorher – wer vor dem Upgrade eine Liste exportiert hat, ist jetzt klar im Vorteil. Wie so eine Bestandsaufnahme aussieht, beschreibt [Relying Parties inventarisieren – die Bestandsaufnahme vor der Entra-Migration](#).

```
# Auf ADFS03
Get-AdfsFarmInformation | Select-Object CurrentFarmBehavior
Get-AdfsCertificate | Select-Object CertificateType, IsPrimary, Thumbprint,
@{n="Ablauf";e={$_.Certificate.NotAfter}}
(Get-AdfsRelyingPartyTrust).Count
(Get-AdfsClaimsProviderTrust).Count
Get-AdfsProperties | Select-Object HostName, Identifier

# Microsoft 365: Stimmt die Federation noch? (Microsoft Graph PowerShell)
Connect-MgGraph -Scopes "Domain.Read.All"
Get-MgDomainFederationConfiguration -DomainId "contoso.de" |
    Select-Object IssuerUri, PassiveSignInUri, SigningCertificate
```

Kontrolle nach der Hochstufung. Früher stand an dieser Stelle in jeder Anleitung Get-MsolFederationProperty aus dem MSOnline-Modul – das Modul ist ausgemustert, Microsoft Graph PowerShell ist der aktuelle Weg.

Da die Hochstufung keine neuen Signaturzertifikate erzeugt, muss der Federation Trust zu Microsoft 365 normalerweise nicht angefasst werden. Vergleiche trotzdem den Fingerabdruck des primären Token-Signing-Zertifikats mit dem, was Entra ID für die Domäne kennt. Weicht beides ab, hast du ein Problem, das mit dem Upgrade nichts zu tun hat, aber jetzt auffällt – der Beitrag [Microsoft-365-Federation-Trust nach Zertifikatswechsel aktualisieren](#) hilft weiter.

WICHTIG – Windows Hello for Business mit Zertifikatsvertrauen

Wer ADFS ab Windows Server 2019 zusammen mit Windows Hello for Business im Zertifikatsvertrauensmodell nutzt, kann nach dem Upgrade im Protokoll die Meldung sehen, dass der Client für den Scope „ugs“ keinen Zugriff hat. Microsoft dokumentiert die Abhilfe: Scope-Beschreibung „ugs“ anlegen und dem Client die Berechtigung geben.

Die Befehle: \$id = (Get-AdfsApplicationPermission -ServerRoleIdentifiers 'http://schemas.microsoft.com/ws/2009/12/identityserver/selfscope' | ?{ \$_.ClientRoleIdentifier -eq '38aa3b87-a06d-4817-b275-7a316988d93b' }).ObjectIdentifier und danach Set-AdfsApplicationPermission -TargetIdentifier \$id -AddScope 'ugs'. Anschließend den ADFS-Dienst neu starten.

Und wenn es schiefgeht?

Das ADFS-Modul kennt mit Test-AdfsFarmBehaviorLevelRestore und Restore-AdfsFarmBehaviorLevel zwei Cmdlets, die eine Farm auf das Level vor einer kürzlichen Hochstufung zurücksetzen sollen. Die Dokumentation dazu ist allerdings ausgesprochen wortkarg. Verlass dich deshalb nicht darauf als geplanten Rückweg. Dein eigentlicher Rollback-Punkt ist das Backup von vor der Hochstufung, und zwar eines, dessen Wiederherstellung du in der Testfarm schon einmal geübt hast. Ein Backup, das nie zurückgespielt wurde, ist eine Hoffnung mit Dateiendung.

Den Web Application Proxy mitziehen

Die Farm ist hochgestuft, jetzt folgt die DMZ. Auch hier gilt: kein In-Place-Upgrade, sondern neue Proxys. WAP03 und WAP04 bekommen Windows Server 2022, die Rolle Remote Access mit dem Rollendienst Web Application Proxy und das SSL-Zertifikat von sts.contoso.de. Die HOSTS-Datei oder das DMZ-DNS muss den Dienstnamen auf die interne VIP der Farm auflösen. Architektur und Rolle des Proxys erklärt [Web Application Proxy: Architektur und Ablöse](#).

Skizze 4: Den Web Application Proxy mitziehen

Neue Proxys registrieren, alte abmelden, dann erst an der ConfigurationVersion drehen



- 1 Install-WebApplicationProxy auf jedem neuen Proxy
- 2 Externen Load Balancer umschwenken
externe VIP zeigt auf WAP03/04, alte Proxys laufen leer
- 3 Set-WebApplicationProxyConfiguration -ConnectedServersName WAP03, WAP04
nur noch die neuen Proxys eintragen
- 4 Get-WebApplicationProxyConfiguration
ConfigurationVersion ablesen
- 5 Set-WebApplicationProxyConfiguration -UpgradeConfigurationVersion
nur wenn dort noch nicht „Windows Server 2016“ steht

Die Reihenfolge ist keine Geschmacksfrage: Solange ein alter Proxy noch in ConnectedServersName steht, wird er sich über die neue Konfigurationsversion nicht freuen. Und ein Proxy, der sich nicht freut, liefert Fehlerseiten statt Anmeldungen.

Skizze 4: Den Web Application Proxy mitziehen. Neue Proxys registrieren sich an der hochgestuften Farm, danach werden die alten abgemeldet und erst dann wird die ConfigurationVersion geprüft.

```
# Auf WAP03 und WAP04
Install-WindowsFeature Web-Application-Proxy -IncludeManagementTools

$trustcred = Get-Credential -Message "Administrator auf den ADFS-Servern"
Install-WebApplicationProxy -CertificateThumbprint "<Fingerabdruck>" `
    -FederationServiceName "sts.contoso.de" `
    -FederationServiceTrustCredential $trustcred

# Nach dem Umschwenken des externen Load Balancers, auf einem neuen WAP:
Get-WebApplicationProxyConfiguration | Select-Object ConnectedServersName, ConfigurationVersion

# Nur noch die neuen Proxys eintragen
Set-WebApplicationProxyConfiguration -ConnectedServersName "WAP03", "WAP04"

# Nur nötig, wenn ConfigurationVersion noch nicht "Windows Server 2016" lautet
Set-WebApplicationProxyConfiguration -UpgradeConfigurationVersion
```

WAP-Umzug in der Reihenfolge, die Microsoft dokumentiert.

TIPP – Die ConfigurationVersion ist kein Tippfehler

Get-WebApplicationProxyConfiguration zeigt auch auf einem Proxy unter Windows Server 2022 als ConfigurationVersion „Windows Server 2016“ an. Laut Microsoft ist das der richtige Wert für den Web Application Proxy ab Windows Server 2016. Steht dort schon dieser Wert – etwa weil deine alten Proxys bereits auf 2016 liefen –, lässt du -UpgradeConfigurationVersion einfach weg.

Richtig zu tun hat das Cmdlet nur, wenn die Proxys vorher noch auf Windows Server 2012 R2

standen.

Die alten Proxys nimmst du aus dem externen Pool, lässt sie leerlaufen und deinstallierst dann die Rolle. Veröffentlichte Anwendungen liegen in der Konfiguration der Farm, nicht auf dem einzelnen Proxy – die neuen WAPs bringen sie also automatisch mit. Prüfe trotzdem mit `Get-WebApplicationProxyApplication`, ob alles da ist, und teste jede veröffentlichte Anwendung einmal von außen. Und wenn ein neuer Proxy nach einiger Zeit meldet, dass er der Farm nicht mehr vertraut, liegt das meist am Proxy-Vertrauenszertifikat – dazu mehr in [WAP-Proxy-Vertrauen erneuern – wenn der Web Application Proxy plötzlich nicht mehr will](#).

WARNUNG – Nicht vergessen: Firewall und Client-IP

Neue Proxys bekommen neue IP-Adressen. Regeln der DMZ-Firewall zwischen WAP und interner VIP, Ausnahmen am Load Balancer und Einträge im Monitoring müssen die neuen Adressen kennen, bevor die alten verschwinden. Sonst läuft der Health Check grün und die Anmeldung trotzdem ins Leere.

Der Ablaufplan mit Rollback-Punkten

Alles Bisherige in einer Tabelle, die du so oder ähnlich in deinen Change-Antrag kopieren kannst. Die Spalte Rollback-Punkt ist die wichtigste: Sie sagt dir, bis wann du ohne Drama zurück kannst und ab wann nur noch das Backup hilft.

Nr.	Schritt	Prüfung danach	Rollback-Punkt	Rückweg
0	Backup der Farm, Export der Trusts, Schema prüfen, Testlauf in Testfarm	Backup zurückgespielt in Testumgebung	Ausgangszustand	nichts zu tun
1	ADFS03/04 installieren, gMSA-Rechte ergänzen, Add-AdfsFarmNode	Get-AdfsFarmInformation, Test per HOSTS-Datei	RP 1: Farm unverändert, nur mehr Knoten	neue Knoten deinstallieren, Set-AdfsFarmInformation -RemoveNode
2	Primärrolle auf ADFS03 (nur WID)	Get-AdfsSyncProperties auf allen Knoten	RP 2: alte Knoten noch vollwertig	ADFS01 wieder primär, alle anderen zeigen auf ADFS01
3	Neue Knoten in den LB-Pool, alte auf Drain	Anmeldungen M365 und kritische Apps	RP 3: alte Knoten noch installiert	alte Knoten wieder aktiv, neue auf Drain
4	Rolle auf ADFS01/02 deinstallieren, -RemoveNode	nur neue Knoten in FarmNodes	RP 4: letzter Punkt vor Datenbankwechsel	alte Knoten neu aufsetzen, solange FBL noch unverändert
5	Test- und Invoke-AdfsFarmBehaviorLevelRaise im Wartungsfenster	CurrentFarmBehavior, Zertifikate, Anzahl Trusts	RP 5: nur noch Backup	Wiederherstellung aus Backup von Schritt 0
6	WAP03/04 installieren, LB extern umschwenken	externe Anmeldung, veröffentlichte Apps	RP 6: alte Proxys noch registriert	externe VIP zurück auf WAP01/02
7	ConnectedServersName bereinigen, ggf. -UpgradeConfigurationVersion	Get-WebApplicationProxyConfiguration	Ende	alte Proxys per Install-WebApplicationProxy neu registrieren

Tabelle 3: Ablaufplan für das ADFS-Farm-Upgrade mit Rollback-Punkten (RP). Zwischen den Schritten darfruhig ein Tag liegen – aber keine Monate.

WICHTIG – Aus der Praxis: der Knoten, den es nicht gab

In einer Farm mit vier Knoten lief der Test vor der Hochstufung plötzlich auf einen Fehler: Ein Server war nicht erreichbar. Der Server existierte nicht mehr, und zwar seit einer Hardwareerneuerung vor fünf Jahren. Die VM war gelöscht, der Farmeintrag nicht. Zwei Minuten mit Set-AdfsFarmInformation -RemoveNode, und der Test war grün. Die Moral: Get-AdfsFarmInformation gehört an den Anfang des Projekts, nicht an das Ende des Wartungsfensters.

Wenn du ein solches Upgrade zum ersten Mal machst, lohnt es sich, den ganzen Ablauf einmal in einer Testfarm durchzuspielen – inklusive Rückweg aus dem Backup. Genau dafür sind unsere [ADFS-Schulungen](#) gedacht. Wer den Plan mit jemandem durchgehen will, der das schon öfter gemacht hat, findet Unterstützung unter [Consulting zu ADFS \(Active Directory Federation Services\)](#). Hintergründe zu Farmdesign, Datenbank und Upgrade-Strategien vertieft auch das Buch [ADFS in der Praxis – das Buch im Detail](#).

Fazit: Ein Upgrade ist Handwerk, kein Heldenepos

Das Upgrade einer ADFS-Farm ist erstaunlich unspektakulär, wenn du es in kleinen Schritten machst. Neue Knoten beitreten lassen, Primärrolle verschieben, alte Knoten sauber austragen, Level anheben, Proxys mitziehen. Jeder Schritt lässt sich prüfen, fast jeder lässt sich zurückdrehen. Die einzige echte Einbahnstraße ist die Hochstufung selbst, und für die hast du ein geprüft Backup und ein kurzes Wartungsfenster. Wer so arbeitet, erlebt kein Heldenepos, sondern einen ruhigen Dienstag.

Und wenn die Farm danach frisch und gepatcht läuft, ist das der richtige Moment, den nächsten Schritt mit Verstand zu planen: welche Anwendungen wirklich an ADFS hängen, welche nach [Microsoft Entra ID](#) umziehen können und wann Microsoft 365 von Federated auf Managed wechselt – dazu passt [Microsoft 365 von Federated auf Managed umstellen – mit Staged Rollout](#). Ein sauber betriebenes ADFS ist die beste Ausgangslage für einen geordneten Ausstieg, und ganz am Ende hilft [ADFS abschalten – die Farm sauber außer Betrieb nehmen](#).

WEITER – Passend zu diesem Beitrag

- › [ADFS-Farm installieren – Schritt für Schritt auf Windows Server 2022](#)
- › [WID oder SQL Server als ADFS-Konfigurationsdatenbank](#)
- › [gMSA als ADFS-Dienstkonto einrichten und umstellen](#)
- › [ADFS hinter dem Load Balancer – Health Probe, SNI und Persistenz](#)
- › [ADFS sichern und wiederherstellen – Rapid Restore Tool in der Praxis](#)
- › [WAP-Proxy-Vertrauen erneuern – wenn der Web Application Proxy plötzlich nicht mehr will](#)
- › [Relying Parties inventarisieren – die Bestandsaufnahme vor der Entra-Migration](#)

FAQ

Welches Farm Behavior Level gehört zu welcher Windows-Server-Version?

Laut Microsoft: Windows Server 2012 R2 hat FBL 1, Windows Server 2016 FBL 3, Windows Server 2019 und 2022 teilen sich FBL 4. Ein FBL 2 gibt es nicht. Welches Level deine Farm hat, zeigt Get-AdfsFarmInformation im Feld CurrentFarmBehavior.

Kann ich einen ADFS-Server einfach per In-Place-Upgrade aktualisieren?

Nein. Microsoft beschreibt den Weg über neue Server, die der bestehenden Farm beitreten. Alte Knoten werden danach entfernt. Ein per Betriebssystem-Upgrade aktualisierter Server wird nicht automatisch zu einem Knoten der neuen Version.

Wie lange darf die Farm im Mischbetrieb laufen?

So kurz wie möglich. Microsoft rät ausdrücklich davon ab, den Mischbetrieb über längere Zeit stehen zu lassen, weil das Probleme in der Farm verursachen kann. Plane einen festen Zeitrahmen von wenigen Tagen ein.

Muss ich bei SQL Server auch die Primärrolle verschieben?

Nein. Bei einer Farm mit SQL Server gelten alle Knoten als primär, Set-AdfsSyncProperties ist nicht nötig. Dafür braucht Invoke-AdfsFarmBehaviorLevelRaise den Parameter -Credential mit einem Konto, das Administrator auf allen ADFS-Servern ist und die nötigen Rechte auf dem SQL Server hat.

Welche Schemaversion brauche ich für das Upgrade?

Für ein Ziel ab Windows Server 2016 mindestens Schemaversion 85, für ein Ziel ab Windows Server 2019 mindestens 88. Die Domänencontroller selbst müssen dafür nicht auf die neue Version, nur das Schema des Forests muss erweitert sein.

Führt das Anheben des Farm Behavior Levels zu einem Ausfall?

Zu einem kurzen. Microsoft beschreibt die FBL-Hochstufung als relativ kurze Unterbrechung, alle anderen Schritte laufen online. Plane für die Hochstufung ein kleines Wartungsfenster und teste danach die wichtigsten Anwendungen.

Muss ich nach dem Upgrade den Federation Trust zu Microsoft 365 aktualisieren?

In der Regel nicht, weil die Hochstufung keine neuen Signaturzertifikate erzeugt. Prüfe trotzdem mit Get-AdfsCertificate und Get-MgDomainFederationConfiguration aus Microsoft Graph PowerShell, ob die Fingerabdrücke übereinstimmen.

Kann ich das Farm Behavior Level wieder absenken?

Das ADFS-Modul enthält Test-AdfsFarmBehaviorLevelRestore und Restore-AdfsFarmBehaviorLevel. Die Dokumentation dazu ist knapp. Plane als verlässlichen Rückweg deshalb die Wiederherstellung aus einem Backup, das du vor der Hochstufung erstellt und in einer Testumgebung geprüft hast.

Warum zeigt mein neuer WAP auf Windows Server 2022 „Windows Server 2016“ als ConfigurationVersion?

Weil das laut Microsoft der korrekte Wert für den Web Application Proxy ab Windows Server 2016 ist. Set-WebApplicationProxyConfiguration -UpgradeConfigurationVersion brauchst du nur, wenn der Wert noch auf einer älteren Version steht.

Muss ich auf Windows Server 2022 upgraden, wenn meine Farm schon auf 2019 läuft?

Das hängt am Lebenszyklus deines Betriebssystems, nicht am Farm Behavior Level. 2019 und 2022 teilen sich FBL 4, der Wechsel ist ein reiner Knotentausch ohne Hochstufung. Neue ADFS-Funktionen bringt er dir nicht, einen aktuelleren Unterbau schon.