

ADFS-Farm installieren – Schritt für Schritt auf Windows Server 2022

WISSEN

Alle Grundlagen, Szenarien und Spokes rund um ADFS an einem Ort.

› [Active Directory Federation Services](#)

BERATUNG

Neue Farm, Migration oder Aufräumen – mit jemandem, der das schon oft gemacht hat.

› [Consulting zu ADFS](#)

SCHULUNG

Installieren, betreiben, Fehler finden – im Workshop an echten Farmen.

› [ADFS-Schulungen](#)

Eine ADFS-Farm zu installieren ist ein bisschen wie Zelte aufbauen: Die eigentliche Arbeit dauert zwanzig Minuten, das Suchen nach dem fehlenden Hering den Rest des Nachmittags. Der Assistent in der Serververwaltung ist schnell durchgeklickt, Install-AdfsFarm läuft in wenigen Minuten durch – und dann steht da eine Farm, die intern nach dem Kennwort fragt, obwohl sie es nicht sollte, extern eine Zertifikatswarnung zeigt und deren zweiter Knoten sich weigert, dem ersten beizutreten. Nichts davon ist ein ADFS-Problem. Alles davon ist ein Problem der Vorbereitung.

Dieser Beitrag ist deshalb keine Einführung in Claims, Tokens und Vertrauensstellungen. Die stehen auf der Pillar-Seite [Active Directory Federation Services](#) und in den bestehenden Fachartikeln. Hier geht es um genau eine Aufgabe: Du hast zwei leere Windows Server 2022 im internen Netz, zwei weitere in der DMZ, und am Ende des Tages soll sich ein Benutzer an sts.contoso.de anmelden können – intern ohne Kennwortabfrage, extern über den Web Application Proxy mit sauberem Zertifikat. Dazwischen liegen sieben Etappen, und wir gehen sie der Reihe nach durch.

Und bevor jemand fragt, warum man 2026 überhaupt noch eine ADFS-Farm aufsetzt: weil viele Unternehmen ADFS seit über zehn Jahren produktiv betreiben, weil daran Anwendungen hängen, die nicht über Nacht nach Entra ID umziehen, und weil ein sauber neu aufgesetzter Knoten auf aktuellem Betriebssystem die beste Grundlage ist – für den Weiterbetrieb ebenso wie für einen geordneten Ausstieg irgendwann. Eine verwahrloste Farm lässt sich schlechter migrieren als eine gepflegte. Das ist keine Panikmache, das ist Handwerk.

FAKTEN – Was am Ende dieses Beitrags steht

Zwei ADFS-Knoten auf Windows Server 2022 in der Domäne contoso.local, Konfiguration in der Windows Internal Database (WID).

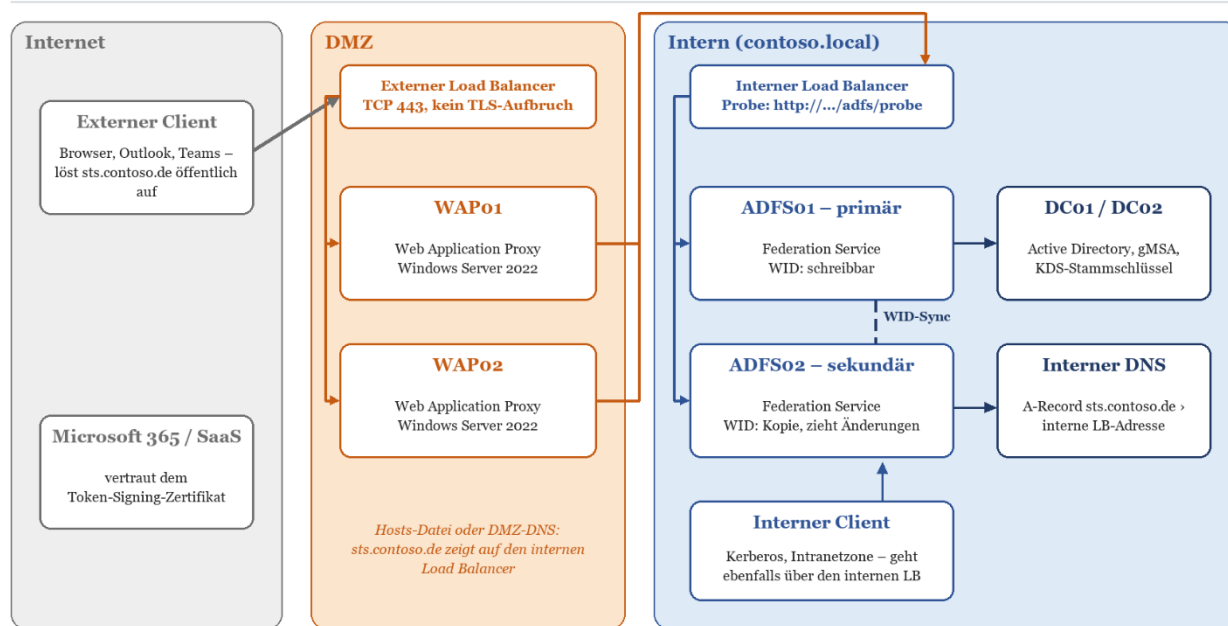
Federation-Dienstname sts.contoso.de, intern per A-Record auf den internen Load Balancer, extern auf den Load Balancer vor zwei Web-Application-Proxy-Servern.

Dienstkonto als gruppenverwaltetes Dienstkonto (gMSA), ein gemeinsames SSL-Zertifikat auf allen vier Servern.

Ein erfolgreicher Funktionstest über die IdpInitiatedSignOn-Seite – intern mit Kerberos, extern mit Formular.

Skizze 1: Die fertige Farm – zwei ADFS-Knoten, zwei WAP, ein Name

Beispielumgebung contoso.local, Federation-Dienstname sts.contoso.de



Ein Zertifikat, ein Schlüssel, ein Name: WAP und ADFS tragen dasselbe SSL-Zertifikat für sts.contoso.de. Wer hier spart, findet es beim ersten Test wieder.

Skizze 1: Die Zielarchitektur. Der Federation-Dienstname gehört den Load Balancern, nicht einzelnen Servern. Die WAP-Knoten in der DMZ sind nicht Mitglied der Domäne.

Vorbereitung: Zertifikat, DNS und Dienstkonto

Die meisten fehlgeschlagenen ADFS-Installationen scheitern nicht am Setup, sondern an den drei Dingen, die vorher hätten erledigt sein sollen. Wenn du nur einen Abschnitt dieses Beitrags gründlich liest, dann diesen. Die Installation selbst ist danach fast enttäuschend unspektakulär.

Namen festlegen, bevor irgendjemand ein Zertifikat bestellt

Der wichtigste Name ist der Federation-Dienstname, in unserem Beispiel sts.contoso.de. Er taucht später in Metadaten, in jedem Relying Party Trust, im Federation-Trust mit Microsoft 365 und in den Köpfen der Anwender auf. Er lässt sich nachträglich ändern – so wie man ein tragendes Mauerwerk nachträglich versetzen kann. Also wähle ihn einmal richtig: kurz, neutral, ohne Servernamen, ohne Versionsnummer, ohne „test“. Namen wie adfs2022.contoso.de altern schlecht, spätestens mit dem nächsten Betriebssystem.

Objekt	Beispiel	Anmerkung
Federation-Dienstname	sts.contoso.de	Öffentlicher Name, gehört dem Load Balancer, nie einem einzelnen Knoten
ADFS-Knoten	ADFS01, ADFS02	Domänenmitglieder in contoso.local, gleiche Domäne für alle Knoten
WAP-Knoten	WAP01, WAP02	In der DMZ, keine Domänenmitglieder, eigene Arbeitsgruppe
Dienstkonto	CONTOSO\gmsa-adfs\$	Gruppenverwaltetes Dienstkonto, das Dollarzeichen gehört dazu
Anzeigename	Contoso Anmeldung	Steht auf der Anmeldeseite, jederzeit änderbar

Tabelle 1: Die Namen der Beispielumgebung. Echte Hostnamen deiner Umgebung gehören in dein Betriebshandbuch, nicht in Blogartikel.

Das SSL-Zertifikat

ADFS braucht für den Start genau ein Zertifikat von dir: das SSL-Zertifikat für den Federation-Dienstnamen. Token-Signing- und Token-Decrypting-Zertifikat erzeugt ADFS selbst, selbstsigniert, und Microsoft empfiehlt ausdrücklich, bei diesen internen Zertifikaten zu bleiben. Wer aus Prinzip auch dafür die eigene PKI verwenden möchte, kann das über Parameter von Install-AdfsFarm tun – und hat sich damit einen zusätzlichen Kalendereintrag für die Erneuerung eingehandelt. Wie das Token-Signing-Zertifikat im Betrieb gewechselt wird, steht in [ADFS Token-Signing-Zertifikat erneuern – mit und ohne AutoCertificateRollover](#).

Für das SSL-Zertifikat gelten wenige, aber harte Regeln:

- Für den produktiven Betrieb öffentlich vertrauenswürdig – schließlich zeigt es auch jeder externe Browser und jede Partnerorganisation an.
- Der Federation-Dienstname steht im Subject oder, besser, im Subject Alternative Name.
- Die erweiterte Schlüsselverwendung Serverauthentifizierung ist enthalten.
- Wer Benutzerzertifikate über Port 443 nutzen will, braucht zusätzlich certauth.sts.contoso.de im SAN. Wer Geräteregistrierung für ältere Clients plant, enterpriseregistration.<UPN-Suffix> pro UPN-Suffix.
- Der private Schlüssel ist exportierbar – sonst bekommst du ihn nicht auf den zweiten Knoten und die WAP-Server.

WARNUNG – Unterschiedliche Zertifikate auf ADFS und WAP

Die Eigenschaft ExtendedProtectionTokenCheck ist in ADFS standardmäßig aktiv. In diesem Fall muss der Web Application Proxy dasselbe Zertifikat mit demselben Schlüssel tragen wie die ADFS-Knoten. Ein „gleichwertiges“ Zertifikat mit gleichem Namen, aber anderem Schlüssel reicht nicht. Der Klassiker: Das Netzwerkteam bestellt für die DMZ ein eigenes Zertifikat, weil es „ja nur der Proxy“ ist. Ergebnis sind Anmeldefehler, die aussehen wie alles Mögliche, nur nicht wie ein Zertifikatsproblem. Bestelle ein Zertifikat und verteile es auf alle vier Server.

Auf ADFS01 importierst du das Zertifikat samt privatem Schlüssel in den Computerspeicher und merkst dir den Fingerabdruck. Der wird gleich zum wichtigsten Parameter des Tages:

```
$pfxPass = Read-Host -AsSecureString -Prompt "PFX-Kennwort"
Import-PfxCertificate -FilePath C:\Install\sts.contoso.de.pfx `
  -CertStoreLocation Cert:\LocalMachine\My -Password $pfxPass

Get-ChildItem Cert:\LocalMachine\My |
  Where-Object { $_.Subject -like "*sts.contoso.de*" } |
  Format-List Subject, DnsNameList, NotAfter, Thumbprint, HasPrivateKey
```

Zertifikat importieren und prüfen – HasPrivateKey muss True sein, sonst brauchst du gar nicht weiterzumachen.

DNS: A-Record, Split-DNS und kein CNAME

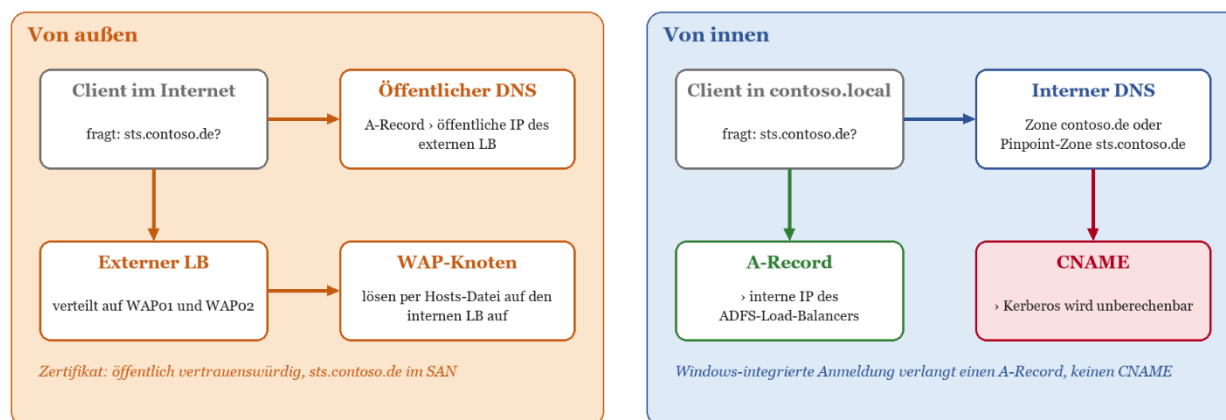
Der Federation-Dienstname muss intern und extern unterschiedlich aufgelöst werden. Interne Clients sollen direkt beim internen Load Balancer vor den ADFS-Knoten landen, externe Clients beim Load Balancer vor den WAP-Servern. Die WAP-Server selbst wiederum müssen den Namen auf den internen Load Balancer auflösen – meist über die Hosts-Datei oder einen eigenen DNS-Server in der DMZ. Das nennt sich Split-DNS und ist ungefähr so aufregend, wie es klingt, bis es fehlt.

Eine Regel ist nicht verhandelbar: Für die Windows-integrierte Anmeldung verlangt Microsoft einen A-Record für den Federation-Dienstnamen, keinen CNAME. Mit einem CNAME fragt der Client je nach Situation ein Kerberos-Ticket für den Zielnamen des Alias an, der SPN passt nicht mehr, und die interne Anmeldung fällt auf das Kennwortformular zurück. Wenn dir das bereits

passiert ist, findest du die Diagnose in [SPN, DNS und Kerberos für ADFS – warum die interne Anmeldung auf Formular zurückfällt](#).

Skizze 2: Split-DNS – ein Name, zwei Antworten

Derselbe Federation-Dienstname muss intern und extern zu unterschiedlichen Zielen führen



Faustregel: Der Dienstname ist kein Servername. sts.contoso.de gehört dem Load Balancer, nie einem einzelnen Knoten – sonst ist die Farm nur ein Server mit Begleitpersonal.

Skizze 2: Split-DNS für sts.contoso.de. Intern zeigt ein A-Record auf den ADFS-Load-Balancer, extern der öffentliche DNS auf den Load Balancer vor den WAP-Servern.

TIPP – Pinpoint-Zone statt ganzer Zone

Wenn intern keine Zone contoso.de existiert und du nicht die komplette öffentliche Zone intern nachpflegen willst, lege auf den internen DNS-Servern eine eigene Zone mit dem Namen sts.contoso.de an und darin einen A-Record ohne Hostnamen. So beantwortet der interne DNS genau diesen einen Namen selbst und reicht alles andere weiter.

Für die Installation reicht es übrigens zunächst, wenn der A-Record auf ADFS01 zeigt. Sobald der zweite Knoten steht, ziehst du ihn auf den internen Load Balancer um.

Das Dienstkonto: gMSA

ADFS läuft unter einem Domänenkonto. Früher war das ein normales Benutzerkonto mit einem Kennwort, das auf einem Post-it im Serverschrank klebte und seit 2014 nicht mehr geändert wurde, weil niemand wusste, was dann passiert. Heute nimmt man ein gruppenverwaltetes Dienstkonto: Das Kennwort verwaltet Active Directory selbst, es wechselt automatisch, und kein Mensch kennt es. Voraussetzung ist ein KDS-Stammschlüssel in der Gesamtstruktur und mindestens ein Domänencontroller ab Windows Server 2012.

Wie du den KDS-Stammschlüssel anlegst, warum du in einer Produktivumgebung die Wartezeit für die Replikation nicht mit einem rückdatierten Zeitstempel austrickst und wie man eine bestehende Farm von einem klassischen Konto auf ein gMSA umzieht, steht ausführlich in [gMSA als ADFS-Dienstkonto einrichten und umstellen](#). Für die Installation reicht dir eine Kurzfassung: Das gMSA existiert, und die Computerkonten der ADFS-Knoten dürfen sein Kennwort abrufen. Das prüfst du auf jedem ADFS-Knoten mit einem einzigen Befehl:

```
Install-WindowsFeature RSAT-AD-PowerShell
Test-ADServiceAccount -Identity gmsa-adfs
# Erwartung: True
```

Liefert Test-ADServiceAccount False, fehlt meistens die Berechtigung für das Computerkonto – oder der Server wurde seit der Gruppenänderung nicht neu gestartet.

WICHTIG – Die Anmeldeinformationen des Installierenden

Für den ersten Knoten muss der PDC-Emulator erreichbar sein, und das Konto, mit dem du installierst, braucht lokale Administratorrechte auf dem Server sowie das Recht, im Active Directory den Container für die Zertifikatsschlüsselverteilung anzulegen. In der Praxis ist das ein Domänen-Admin.

Darf das nicht sein, lässt du die AD-Objekte vorab von jemandem mit den nötigen Rechten anlegen und installierst dann mit dem Parameter AdminConfiguration. Das ist sauber, erfordert aber Absprache – plane sie ein, statt sie am Installationstag zu entdecken.

WID oder SQL Server

Die Konfiguration einer ADFS-Farm liegt in einer Datenbank, entweder in der mitgelieferten Windows Internal Database auf jedem Knoten oder zentral in SQL Server. Für die allermeisten Umgebungen ist WID die richtige Wahl, und diese Anleitung verwendet sie. Die Grenzen sind überschaubar: Microsoft unterstützt WID-Farmen mit bis zu 30 Knoten und bis zu 100 Relying Party Trusts. Darüber hinaus sowie für SAML-Artefaktauflösung und Token-Replay-Erkennung brauchst du SQL Server. Die ganze Abwägung, inklusive Hochverfügbarkeit auf SQL-Seite, gehört nicht hierher, sondern in [WID oder SQL Server als ADFS-Konfigurationsdatenbank](#).

Kriterium	WID	SQL Server
Knoten pro Farm	bis 30	über 30 möglich
Relying Party Trusts	bis 100	über 100 möglich
SAML-Artefaktauflösung	nicht unterstützt	unterstützt
Token-Replay-Erkennung	nicht unterstützt	unterstützt
Schreibender Knoten	nur der primäre Knoten	alle Knoten
Zusätzliche Abhängigkeit	keine	SQL-Instanz inklusive Hochverfügbarkeit

Tabelle 2: WID und SQL Server im Vergleich – Grenzwerte gemäß den ADFS-Anforderungen von Microsoft.

FAKTEN – Checkliste vor dem ersten Install-AdfsFarm

Zwei Windows Server 2022 als ADFS-Knoten, Mitglied derselben Domäne, aktuell gepatcht, Zeit synchron mit der Domäne.

Zwei Windows Server 2022 als WAP-Knoten in der DMZ, nicht in der Domäne, TCP 443 von der DMZ zum internen Load Balancer freigeschaltet.

SSL-Zertifikat für sts.contoso.de mit exportierbarem privatem Schlüssel als PFX, öffentlich vertrauenswürdig, Serverauthentifizierung, Fingerabdruck notiert.

Interner A-Record sts.contoso.de (zunächst auf ADFS01, später auf den internen Load Balancer), öffentlicher A-Record auf den externen Load Balancer.

Kein CNAME für den Federation-Dienstnamen – nirgends.

gMSA angelegt, Test-ADServiceAccount liefert auf beiden ADFS-Knoten True.

PDC-Emulator erreichbar, Installationskonto mit ausreichenden Rechten oder AD-Objekte vorab angelegt.

Entscheidung WID oder SQL getroffen und dokumentiert.

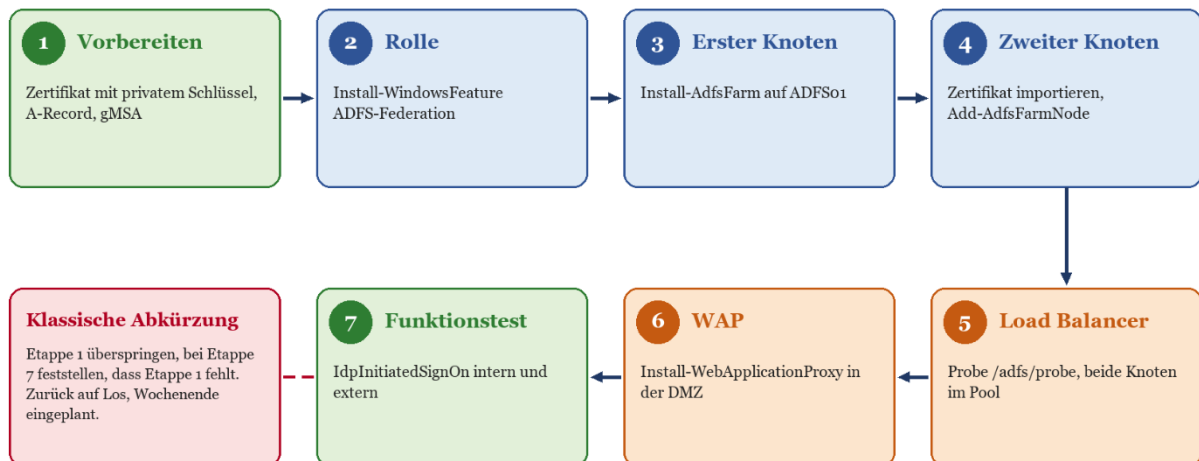
Wartungsfenster und Ansprechpartner aus Netzwerk-, PKI- und AD-Team bekannt – nicht nur deren Namen, sondern auch deren Telefonnummern.

Der erste Knoten: Rolle installieren und Install-AdfsFarm

Jetzt wird es kurz. Das ist kein Tippfehler, sondern die Belohnung für die Vorbereitung.

Skizze 3: Der Weg vom leeren Server zur ersten Anmeldung

Sieben Etappen – die ersten drei entscheiden, ob die übrigen vier langweilig werden



Etappe 1 dauert einen Vormittag. Etappe 1 nachzuholen dauert gern eine Woche, weil dann plötzlich PKI, Netzwerk und AD-Team gleichzeitig gefragt sind.

Skizze 3: Die sieben Etappen. Etappe 1 ist die langwierigste – und die einzige, deren Fehlen man erst bei Etappe 7 bemerkt.

Die Rolle installieren

Die ADFS-Rolle installierst du auf ADFS01 wahlweise über die Serververwaltung oder mit einer Zeile PowerShell. Ein Neustart ist in der Regel nicht nötig, schadet aber auch niemandem, der sowieso gerade Kaffee holt.

```
Install-WindowsFeature ADFS-Federation -IncludeManagementTools
Import-Module ADFS
```

Damit liegen die Binärdateien auf dem Server, aber es gibt noch keine Farm. Der Dienst adfssrv existiert, startet aber sinnvollerweise erst nach der Konfiguration. Wer an dieser Stelle schon die Verwaltungskonsole öffnet, sieht eine freundliche Aufforderung, den Server zu konfigurieren – sonst nichts.

Die Farm anlegen mit Install-AdfsFarm

Der Assistent in der Serververwaltung erzeugt am Ende ein PowerShell-Skript mit genau diesem Aufruf, du kannst also auch gleich den Aufruf nehmen. Vorher lohnt sich ein Probelauf mit Test-AdfsFarmInstallation, der dieselben Parameter prüft, ohne etwas zu verändern:

```
$thumb = "<Fingerabdruck des SSL-Zertifikats>"

Test-AdfsFarmInstallation `
  -FederationServiceName "sts.contoso.de" `
  -CertificateThumbprint $thumb `
  -GroupServiceAccountIdentifier "CONTOSO\gmsa-adfs$"

Install-AdfsFarm `
  -FederationServiceName "sts.contoso.de" `
  -FederationServiceDisplayName "Contoso Anmeldung" `
  -CertificateThumbprint $thumb `
  -GroupServiceAccountIdentifier "CONTOSO\gmsa-adfs$"
```

Erster Knoten mit WID und gMSA. Das Dollarzeichen am Kontonamen ist Absicht; in doppelten Anführungszeichen stört es hier nicht, weil kein gültiger Variablenname folgt.

Ohne Angabe einer SQL-Verbindungszeichenfolge legt Install-AdfsFarm eine WID-Farm an und macht ADFS01 zum primären Knoten. Die wichtigsten Parameter im Überblick:

Parameter	Wozu	Anmerkung
FederationServiceName	Dienstname der Farm	Muss zum Zertifikat passen, sonst bricht der Aufruf ab
FederationServiceDisplayName	Anzeigename auf der Anmeldeseite	Später mit Set-AdfsProperties änderbar
CertificateThumbprint	SSL-Zertifikat aus dem Computerspeicher	Wird zugleich Dienstkommunikationszertifikat
GroupServiceAccountIdentifier	gMSA als Dienstkonto	Alternative: ServiceAccountCredential für ein klassisches Konto
SQLConnectionString	Konfiguration in SQL Server	Weglassen bedeutet WID
AdminConfiguration	Vorab angelegte AD-Objekte verwenden	Wenn das Installationskonto keine Domänen-Admin-Rechte hat
SigningCertificateThumbprint, DecryptingCertificateThumbprint	Eigene Token-Zertifikate	Nur mit gutem Grund; Standard sind selbstsignierte Zertifikate
OverwriteConfiguration	Vorhandene Konfiguration überschreiben	Nur bei bewusster Neuinstallation – der Name ist Programm

Tabelle 3: Die relevanten Parameter von Install-AdfsFarm.

WARNUNG – So stand es früher in jeder Anleitung

Viele ältere Installationsanleitungen enden mit Convert-MsolDomainToFederated oder New-MsolFederatedDomain aus dem MSONline-Modul. Dieses Modul und das AzureAD-Modul sind ausgemustert und kein aktueller Weg mehr. Die Federation-Konfiguration einer Microsoft-365-Domäne pflegst du heute mit Microsoft Graph PowerShell, etwa mit New-MgDomainFederationConfiguration und Update-MgDomainFederationConfiguration, oder über Entra Connect.

Für die Installation der Farm selbst spielt das keine Rolle – wichtig ist nur, dass du alte Skripte nicht blind weiterverwendest.

Die erste Kontrolle

Läuft der Aufruf ohne Fehler durch, meldet er eine Erfolgsmeldung und gegebenenfalls Warnungen. Lies die Warnungen. Eine davon betrifft typischerweise den SPN: ADFS registriert den benötigten Dienstprinzipalnamen beim Anlegen der Farm selbst am Dienstkonto. Scheitert das, etwa weil der SPN schon an einem anderen Konto hängt, bekommst du eine Warnung und musst von Hand nachbessern. Wer das ignoriert, wundert sich später über Kennwortformulare im Intranet.

```
Get-Service adfssrv
Get-AdfsProperties | Format-List HostName, Identifier, DisplayName,
EnableIdPInitiatedSignonPage
Get-AdfsCertificate | Format-Table CertificateType, IsPrimary, Thumbprint
Get-AdfsSyncProperties
Invoke-WebRequest -Uri "http://localhost/adfs/probe" -UseBasicParsing | Select-Object
StatusCode
```

Dienst läuft, Eigenschaften stimmen, drei Zertifikatstypen vorhanden, Rolle PrimaryComputer, Probe antwortet mit 200.

TIPP – Die Metadaten als Lebenszeichen

Ein schneller Test aus einem Browser auf einem Domänen-Client: Ruf auf dem Federation-Dienstnamen den Pfad /FederationMetadata/2007-06/FederationMetadata.xml auf. Kommt ein XML-Dokument ohne Zertifikatswarnung zurück, sind DNS, Zertifikat und Dienst grundsätzlich in Ordnung. Kommt eine Warnung, stimmt etwas am Zertifikat oder am Namen nicht – und zwar jetzt schon, nicht erst am WAP.

Der zweite Knoten mit Add-AdfsFarmNode

Ein ADFS-Server ist keine Farm, sondern ein Einzelfall mit Ambitionen. Hochverfügbar wird es erst mit dem zweiten Knoten – und der ist schneller installiert als der erste, weil fast alles schon da ist.

Vorbereitung auf ADFS02

Auf ADFS02 wiederholst du drei Schritte aus der Vorbereitung: das SSL-Zertifikat mit privatem Schlüssel importieren, Test-ADServiceAccount ausführen und die Rolle installieren. Achte darauf, wirklich dasselbe Zertifikat zu importieren, nicht ein neu ausgestelltes mit gleichem Namen. Der Fingerabdruck muss identisch sein.

```
Import-PfxCertificate -FilePath C:\Install\sts.contoso.de.pfx `
  -CertStoreLocation Cert:\LocalMachine\My -Password $pfxPass
Test-ADServiceAccount -Identity gmsa-adfs
Install-WindowsFeature ADFS-Federation -IncludeManagementTools
```

Der Beitritt zur Farm

Bei einer WID-Farm teilst du dem neuen Knoten mit, wer der primäre Knoten ist. Auch hier gibt es einen Probelauf, Test-AdfsFarmJoin, bevor es ernst wird:

```
$thumb = "<Fingerabdruck des SSL-Zertifikats>"

Test-AdfsFarmJoin `
  -GroupServiceAccountIdentifier "CONTOSO\gmsa-adfs$" `
  -PrimaryComputerName "ADFS01.contoso.local"

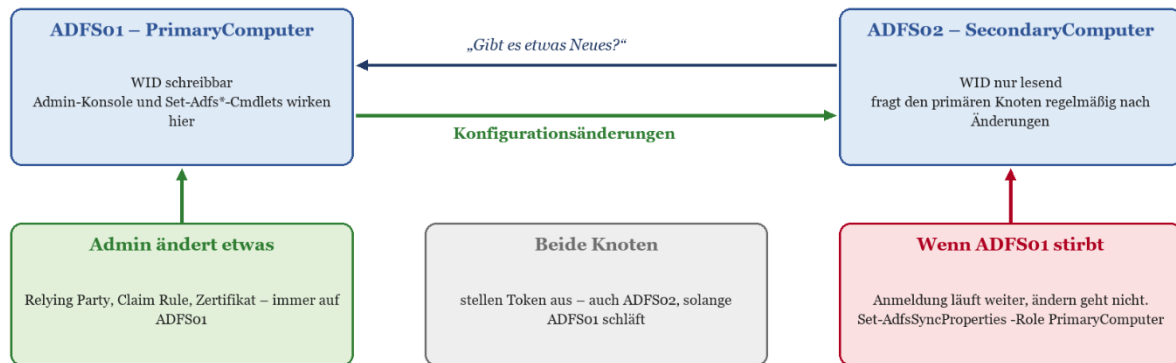
Add-AdfsFarmNode `
  -GroupServiceAccountIdentifier "CONTOSO\gmsa-adfs$" `
  -PrimaryComputerName "ADFS01.contoso.local" `
  -CertificateThumbprint $thumb
```

Zweiter Knoten einer WID-Farm. Bei einer SQL-Farm ersetzt SqlConnectionString den Parameter PrimaryComputerName.

Add-AdfsFarmNode holt die Konfiguration vom primären Knoten, legt eine lokale WID an und richtet ADFS02 als sekundären Knoten ein. Ab jetzt stellen beide Knoten Token aus. Ändern kannst du die Konfiguration aber nur auf ADFS01 – der sekundäre Knoten fragt regelmäßig nach, ob es etwas Neues gibt, standardmäßig alle fünf Minuten.

Skizze 4: Wer schreibt, wer liest – die WID-Farm im Betrieb

Änderungen landen nur auf dem primären Knoten, der sekundäre zieht sie in festen Abständen nach



Die WID-Farm ist hochverfügbar im Ausstellen, nicht im Verwalten. Das ist kein Mangel, sondern ein Designentscheid – man sollte ihn nur vor dem Ausfall kennen.

Skizze 4: Die WID-Farm im Betrieb. Beide Knoten stellen Token aus, geschrieben wird nur auf dem primären Knoten.

Die Synchronisation prüfen

```
# Auf ADFS02
Get-AdfsSyncProperties
# Role                : SecondaryComputer
# PrimaryComputerName : ADFS01.contoso.local
# LastSyncStatus      : 0 (0 = erfolgreich)
```

Ein kurzer Praxistest: Ändere auf ADFS01 etwas Harmloses, etwa den Anzeigenamen, warte die Synchronisation ab und prüfe mit Get-AdfsProperties auf ADFS02, ob die Änderung angekommen ist. Wenn ja, ist die Farm im eigentlichen Sinne fertig. Wenn nein, liegt es fast immer an der Namensauflösung zwischen den Knoten oder an einer Firewall, die den primären Knoten für den sekundären un erreichbar macht.

WARNUNG – Wenn der primäre Knoten ausfällt

Fällt ADFS01 aus, laufen Anmeldungen über ADFS02 weiter. Konfigurationsänderungen sind dann aber nicht möglich, weil ADFS02 nur eine Lesekopie hat. Ist absehbar, dass ADFS01 nicht wiederkommt, machst du ADFS02 mit Set-AdfsSyncProperties -Role PrimaryComputer zum neuen primären Knoten und stellst alle weiteren Knoten mit Set-AdfsSyncProperties -Role SecondaryComputer -PrimaryComputerName auf den neuen Primärknoten um.

Tu das nie, solange der alte Primärknoten noch lebt und Änderungen annimmt. Zwei Primärknoten in einer Farm sind wie zwei Kapitäne auf einem Schiff: Irgendwann fahren sie in unterschiedliche Richtungen, und das Schiff hat eine Meinung dazu.

Load Balancer davor und Knoten in den Pool

Sobald beide Knoten laufen, ziehst du den internen A-Record von ADFS01 auf die virtuelle Adresse des internen Load Balancers um. Microsoft empfiehlt dafür drei Dinge: TLS am Load Balancer nicht aufbrechen, einen Load Balancer mit SNI-Unterstützung verwenden und als Health Probe den HTTP-Endpunkt /adfs/probe abfragen, der lokal mit 200 antwortet. DNS-Round-Robin ist kein Lastverteiler, sondern ein Würfelspiel ohne Gesundheitsprüfung. Die Details, von Persistenz bis zur Fallback-Bindung für Clients ohne SNI, stehen in [ADFS hinter dem Load Balancer – Health](#)

Probe, SNI und Persistenz. Wer einen Kemp LoadMaster einsetzt, findet die passende Konfiguration auf der Pillar-Seite [Kemp LoadMaster](#).

Web Application Proxy in der DMZ anbinden

Die Farm steht, intern funktioniert alles – jetzt fehlt der Weg von außen. Der Web Application Proxy nimmt Anmeldungen aus dem Internet entgegen und reicht sie an die Farm durch, ohne dass ein ADFS-Knoten selbst im Internet steht. ADFS und WAP dürfen übrigens nicht auf demselben Server installiert werden; wer das versucht, spart einen Server und verliert die Trennung, die der Proxy überhaupt erst herstellt.

Vorbereitung auf WAPo1 und WAPo2

- Das SSL-Zertifikat für sts.contoso.de mit privatem Schlüssel importieren – dasselbe wie auf den ADFS-Knoten.
- sts.contoso.de per Hosts-Datei oder DMZ-DNS auf die Adresse des internen ADFS-Load-Balancers auflösen.
- Die ausstellende Zertifizierungsstelle des Zertifikats muss auf dem WAP-Server vertrauenswürdig sein – bei öffentlichen Zertifikaten in der Regel gegeben.
- TCP 443 vom WAP zum internen Load Balancer freischalten.

```
Install-WindowsFeature Web-Application-Proxy -IncludeManagementTools

$cred = Get-Credential -Message "Konto mit lokalen Adminrechten auf den ADFS-Knoten"
Install-WebApplicationProxy `
    -FederationServiceName "sts.contoso.de" `
    -FederationServiceTrustCredential $cred `
    -CertificateThumbprint "<Fingerabdruck des SSL-Zertifikats>"
```

Anbindung eines WAP-Knotens an die Farm. Die Anmeldeinformationen werden nur für den Aufbau des Proxy-Vertrauens benötigt.

Install-WebApplicationProxy baut ein Vertrauensverhältnis zwischen Proxy und Farm auf, das auf einem Zertifikat beruht, das sich im Betrieb selbst erneuert – solange der Proxy regelmäßig Kontakt zur Farm hat. Steht ein WAP-Server wochenlang ausgeschaltet im Schrank, kann dieses Vertrauen ablaufen. Wie du es wiederbelebst, steht in [WAP-Proxy-Vertrauen erneuern – wenn der Web Application Proxy plötzlich nicht mehr will](#). Zur Architektur des Proxys und zu der Frage, was ihn eines Tages ablösen kann, lies [Web Application Proxy: Architektur und Ablöse](#).

TIPP – Den WAP nicht zum Domänenmitglied machen

Für die reine ADFS-Veröffentlichung muss der Web Application Proxy nicht Mitglied der Domäne sein, und er sollte es auch nicht. Nur wenn du über den WAP Anwendungen mit Kerberos Constrained Delegation veröffentlichen willst, brauchst du den Domänenbeitritt – und dann eine sehr gute Begründung für die Firewallregeln, die das nach sich zieht.

Funktionstest über die IdpInitiatedSignOn-Seite

Bevor die erste echte Anwendung angebunden wird, willst du wissen, ob die Farm überhaupt Benutzer anmelden kann. Dafür gibt es in ADFS eine eingebaute Testseite unter dem Pfad /adfs/ls/idpinitiatedsignon.aspx auf dem Federation-Dienstnamen. Sie meldet einen Benutzer direkt am Identitätsanbieter an, ohne dass eine Relying Party beteiligt ist, und listet auf Wunsch die SAML-Relying-Parties zur Auswahl auf.

Die Seite ist ab Werk ausgeschaltet

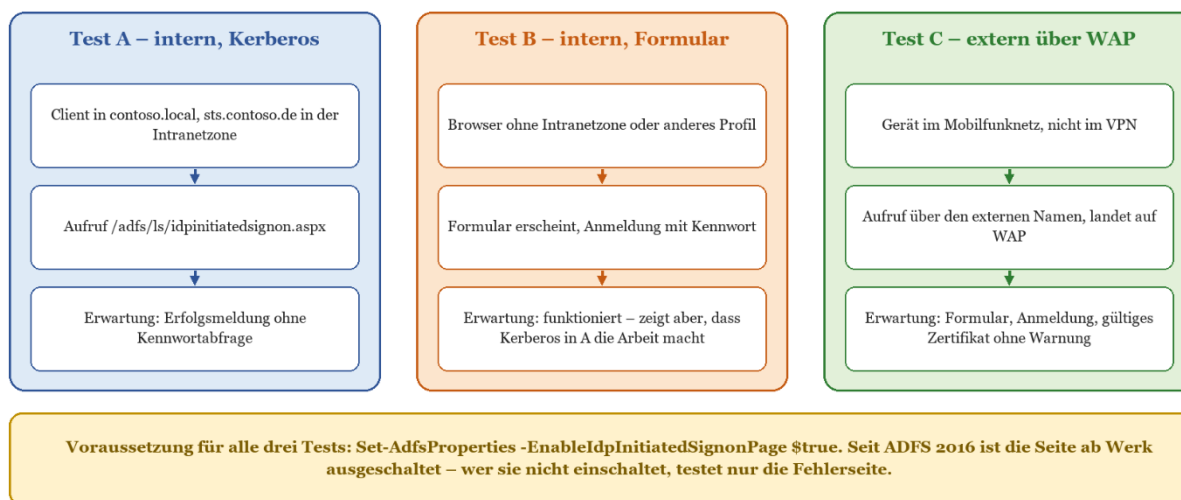
Und hier stolpern viele Anleitungen, die noch aus der Zeit von ADFS 2012 R2 stammen: Seit ADFS unter Windows Server 2016 ist die IdpInitiatedSignOn-Seite standardmäßig deaktiviert. Wer sie aufruft, bekommt eine Fehlerseite und zweifelt an der gesamten Installation. Dabei fehlt nur ein Schalter, den du auf dem primären Knoten umlegst:

```
Get-AdfsProperties | Select-Object EnableIdpInitiatedSignonPage
Set-AdfsProperties -EnableIdpInitiatedSignonPage $true
Get-AdfsProperties | Select-Object EnableIdpInitiatedSignonPage
```

Set-AdfsProperties quittiert kommentarlos. Deshalb danach noch einmal nachsehen – und auf ADFS02 die Synchronisation abwarten.

Skizze 5: Der Funktionstest über die IdpInitiatedSignOn-Seite

Drei Tests, drei Aussagen – und die Seite danach wieder bewusst behandeln



Skizze 5: Drei Tests mit drei unterschiedlichen Aussagen. Erst wenn alle drei grün sind, ist die Farm bereit für Relying Party Trusts.

Test intern: Kerberos statt Kennwort

Auf einem Domänen-Client muss sts.contoso.de in der Zone Lokales Intranet stehen, am besten per Gruppenrichtlinie. Dann rufst du die Seite auf, klickst auf Anmelden und solltest ohne jede Kennwortabfrage die Meldung erhalten, dass du angemeldet bist. Genau das ist der Moment, in dem sich die A-Record-Sorgfalt aus der Vorbereitung auszahlt. Erscheint stattdessen das Formular, stimmt meist etwas an Zone, DNS oder SPN nicht – die Zusammenhänge zwischen Kerberos, Dienstprinzipalnamen und Namensauflösung erklärt die Pillar-Seite [Microsoft Kerberos](#).

Test extern: über den WAP

Der externe Test gehört auf ein Gerät, das wirklich draußen ist: ein Smartphone im Mobilfunknetz, ein Notebook ohne VPN. Aus dem Büro heraus mit „einfach mal den externen Namen“ testen, beweist nur, dass dein interner DNS funktioniert. Extern erwartest du das Anmeldeformular, keine Zertifikatswarnung und nach der Anmeldung dieselbe Erfolgsmeldung wie intern.

Symptom	Wahrscheinliche Ursache	Erster Blick
Fehlerseite statt Anmeldeseite	IdpInitiatedSignOn-Seite nicht aktiviert	Get-AdfsProperties, Eigenschaft EnableIdpInitiatedSignonPage
Intern Formular statt Kerberos	Zone, CNAME statt A-Record oder SPN-Problem	Intranetzone, nslookup, setspn -Q für den Dienstnamen
Zertifikatswarnung	Anderes Zertifikat auf dem WAP oder	Fingerabdruck auf WAP und ADFS

extern	fehlende Zwischenzertifikate	vergleichen
Extern nicht erreichbar, intern gut	Hosts-Datei auf WAP, Firewall DMZ nach intern	Test-NetConnection sts.contoso.de -Port 443 vom WAP
Mal geht es, mal nicht	Ein Knoten im Pool ist krank	Probe /adfs/probe je Knoten, Admin-Log beider Knoten
Anmeldung schlägt mit gültigem Kennwort fehl	Dienstkonto, Zeitabweichung, Kontosperr	ADFS-Admin-Ereignisprotokoll

Tabelle 4: Die häufigsten Befunde beim ersten Funktionstest.

Wenn eines dieser Symptome bleibt, helfen dir zwei Beiträge weiter: [ADFS-Anmeldung schlägt fehl – die häufigsten Ursachen und ihre Lösung](#) für die typischen Ursachen und [ADFS-Ereignisprotokolle lesen – Admin-Log, Debug-Tracing und Auditing](#) für den Blick in Admin-Log und Debug-Tracing, der die meisten Rätsel in Minuten auflöst.

Und danach: Seite anlassen oder ausschalten?

Microsoft hat die Seite nicht ohne Grund standardmäßig deaktiviert: Sie ist eine zusätzliche, öffentlich erreichbare Anmelde-möglichkeit, die im Alltag die wenigsten Anwender brauchen. Wenn du sie nur für den Funktionstest und die Fehlersuche verwendest, schalte sie nach dem Test mit Set-AdfsProperties -EnableIdpInitiatedSignonPage \$false wieder ab und bei Bedarf kurz wieder ein. Wenn Anwendungen sie für IdP-initiierte Anmeldungen tatsächlich benötigen, lass sie an – dann aber bewusst, dokumentiert und mit einem Blick auf die übrigen Schutzmaßnahmen der Farm, wie sie in [ADFS-Sicherheit: Angriffe, Härtung, Golden SAML und MFA](#) beschrieben sind.

WICHTIG – Eine neue Farm ist noch keine fertige Farm

Nach dem erfolgreichen Funktionstest fehlen noch Dinge, die nichts mit der Installation zu tun haben, aber alles mit dem Betrieb: Extranet Smart Lockout gegen Passwort-Spray, eine Sicherung der Konfiguration, eine Überwachung beider Knoten und eine dokumentierte Zertifikatsstrategie.

Die wichtigsten Einstiege: [Extranet Smart Lockout – ADFS gegen Passwort-Spray schützen](#), [ADFS sichern und wiederherstellen – Rapid Restore Tool in der Praxis](#) und [ADFS überwachen – Health Checks, Diagnose-Toolbox und Entra Connect Health](#).

Was nach der Installation kommt

Die Farm meldet Benutzer an. Das ist der Moment, in dem die eigentliche Arbeit beginnt: Anwendungen anbinden, Anmeldeseite gestalten, Betrieb absichern. Die folgende Tabelle ordnet die nächsten Schritte, mit Verweis auf den jeweils passenden Beitrag.

Nächster Schritt	Warum jetzt	Weiterlesen
Erste Relying Party anbinden	Ohne Anwendung ist eine Farm nur eine sehr gut abgesicherte Anmeldeseite	Relying Party Trust anlegen – per Metadaten und von Hand
Anmeldeseite anpassen	Anwender vertrauen einer Seite mit bekanntem Logo mehr als einer mit Standardgrau	ADFS-Anmeldeseite anpassen – Logo, Texte, Hilfelinks
Extranet Smart Lockout	Die Farm ist extern erreichbar – Passwort-Spray ist keine Frage des Ob	Extranet Smart Lockout – ADFS gegen Passwort-Spray schützen
Sicherung einrichten	Eine Farm ohne Sicherung ist eine Wette	ADFS sichern und wiederherstellen – Rapid Restore Tool in der Praxis
Überwachung	Ausfälle fallen sonst zuerst den Anwendern auf	ADFS überwachen – Health Checks, Diagnose-Toolbox und Entra Connect Health
Zertifikatstausch	Das SSL-Zertifikat läuft ab, bevor du es	SSL-Zertifikat auf ADFS und Web

üben	vergessen hast	Application Proxy tauschen
-------------	-----------------------	---

Tabelle 5: Die nächsten Schritte nach der Installation.

Wenn du eine bestehende Farm auf älterem Betriebssystem durch neue Knoten auf Windows Server 2022 ersetzen willst, statt eine Farm neu anzulegen, ist der Weg ein anderer: neue Knoten mit Add-AdfsFarmNode in die bestehende Farm aufnehmen, Primärrolle verschieben, alte Knoten entfernen und anschließend das Farm Behavior Level anheben. Das beschreibt [ADFS-Farm upgraden – Farm Behavior Level anheben ohne Ausfall](#). Und wenn am anderen Ende des Lebenszyklus der Ausstieg ansteht, hilft [ADFS abschalten – die Farm sauber außer Betrieb nehmen](#).

Fazit

Eine ADFS-Farm auf Windows Server 2022 zu installieren ist technisch keine Hexerei. Zwei Cmdlets, Install-AdfsFarm und Add-AdfsFarmNode, erledigen den Kern der Arbeit in wenigen Minuten. Was über Erfolg oder Frust entscheidet, passiert davor: ein Federation-Dienstname, der zehn Jahre hält, ein Zertifikat mit exportierbarem Schlüssel auf allen vier Servern, ein A-Record statt eines CNAME und ein gMSA, das niemand kennt und niemand vergisst.

Danach kommt der Test, und der Test braucht eine Seite, die seit ADFS 2016 ab Werk aus ist. Wer das weiß, spart sich eine Stunde Zweifel an der eigenen Installation. Wer intern ohne Kennwort und extern ohne Zertifikatswarnung angemeldet wird, hat eine Farm, auf der man die nächsten Jahre sauber arbeiten kann – ob sie nun noch lange läuft oder eines Tages geordnet in Rente geht.

Wenn du die Installation lieber gemeinsam planst oder eine bestehende Farm vor der Erweiterung einmal gründlich durchleuchten lassen willst, ist das ein typischer Fall für [Consulting zu ADFS \(Active Directory Federation Services\)](#). Wer das Ganze selbst am lebenden Objekt üben möchte, findet passende Termine unter [ADFS-Schulungen](#). Und wer lieber nachliest, statt nachzufragen: Aufbau, Betrieb und Fehlersuche einer ADFS-Farm vertieft [ADFS in der Praxis – das Buch im Detail](#).

WEITER – Passend zu diesem Beitrag

- › [gMSA als ADFS-Dienstkonto einrichten und umstellen](#)
- › [WID oder SQL Server als ADFS-Konfigurationsdatenbank](#)
- › [ADFS hinter dem Load Balancer – Health Probe, SNI und Persistenz](#)
- › [SPN, DNS und Kerberos für ADFS – warum die interne Anmeldung auf Formular zurückfällt](#)
- › [ADFS: Architektur, Einsatzszenarien und Hochverfügbarkeit](#)

FAQ

Brauche ich für eine ADFS-Farm mindestens zwei Server?

Nein, auch ein einzelner Server ist technisch eine Farm mit einem Knoten. Hochverfügbar ist das aber nicht, und jede Wartung wird zum Ausfall. Für produktive Umgebungen sind zwei ADFS-Knoten und zwei WAP-Knoten das sinnvolle Minimum.

Kann ich ADFS und Web Application Proxy auf demselben Server installieren?

Nein. Microsoft schließt die Installation von Federation Server und Web Application Proxy auf demselben Computer aus. Der Proxy gehört in die DMZ, die ADFS-Knoten ins interne Netz.

Warum fragt ADFS intern nach dem Kennwort, obwohl Kerberos funktionieren sollte?

Meist steht der Dienstname nicht in der Intranetzone, er ist als CNAME statt als A-Record angelegt, oder der SPN fehlt beziehungsweise ist doppelt vergeben. Die Diagnose Schritt für Schritt steht in [SPN, DNS und Kerberos für ADFS – warum die interne Anmeldung auf Formular zurückfällt](#).

Warum zeigt die IdpInitiatedSignOn-Seite nur einen Fehler?

Weil sie seit ADFS unter Windows Server 2016 standardmäßig deaktiviert ist. Mit Set-AdfsProperties -EnableIdpInitiatedSignonPage \$true schaltest du sie auf dem primären Knoten ein.

Muss ich für das Token-Signing-Zertifikat ein eigenes Zertifikat kaufen?

Nein. ADFS erzeugt Token-Signing- und Token-Decrypting-Zertifikat selbst, und Microsoft empfiehlt, bei diesen selbstsignierten Zertifikaten zu bleiben. Kaufen oder aus der eigenen PKI beziehen musst du nur das SSL-Zertifikat für den Federation-Dienstnamen.

WID oder SQL Server – was nehme ich?

Für die meisten Umgebungen WID: bis 30 Knoten und bis 100 Relying Party Trusts ohne zusätzliche Abhängigkeit. SQL Server brauchst du für größere Farmen, SAML-Artefaktauflösung oder Token-Replay-Erkennung. Die ausführliche Abwägung steht in [WID oder SQL Server als ADFS-Konfigurationsdatenbank](#).

Muss der Web Application Proxy Mitglied der Domäne sein?

Für die Veröffentlichung von ADFS nicht. Nur wenn du über den Proxy Anwendungen mit Kerberos Constrained Delegation veröffentlichst, ist der Domänenbeitritt nötig.

Kann ich die Farm mit einem normalen Benutzerkonto statt einem gMSA betreiben?

Ja, Install-AdfsFarm akzeptiert mit ServiceAccountCredential auch ein klassisches Domänenkonto. Du übernimmst dann aber die Kennwortpflege selbst. Wie du später auf ein gMSA umstellst, beschreibt [gMSA als ADFS-Dienstkonto einrichten und umstellen](#).