

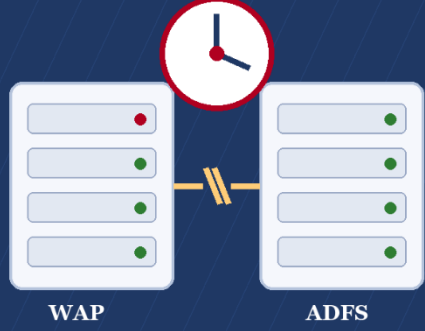
WAP-Proxy-Vertrauen erneuern – wenn der Web Application Proxy plötzlich nicht mehr will

ADFS · Web Application Proxy

Der Proxy hat Schluss gemacht – und keiner hat es gemerkt

Abgelaufenes Proxy-Trust-Zertifikat, falsche Uhrzeit in der DMZ, blockierte Verbindung: Diagnose und Reparatur in einer Viertelstunde.

boddenberg.de



WISSEN

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

› [Active Directory Federation Services](#)

BERATUNG

Dein Proxy zickt, und das Wartungsfenster ist schon vorbei? Wir schauen mit dir drauf.

› [Consulting zu ADFS](#)

SCHULUNG

WAP aufsetzen, Vertrauen kaputt machen, Vertrauen reparieren – im Labor statt am Montagmorgen.

› [ADFS-Schulungen](#)

Montagmorgen, kurz nach acht. Intern meldet sich jeder problemlos an, aber alle, die von zu Hause oder unterwegs arbeiten, sehen statt der Anmeldeseite eine Fehlermeldung. Der Web Application Proxy stand über das lange Wochenende ausgeschaltet im Wartungsfenster, oder jemand hat die VM aus einem älteren Snapshot zurückgeholt, oder die Uhr in der DMZ geht seit Wochen still und leise nach. Das Ergebnis ist immer dasselbe: Der Proxy und die ADFS-Farm vertrauen sich nicht mehr. Beziehungsprobleme unter Servern, nur ohne Paartherapeut.

Die gute Nachricht: Das Fehlerbild ist bekannt, die Reparatur dauert in der Regel eine Viertelstunde, und du musst dafür weder den Proxy neu installieren noch die veröffentlichten Anwendungen neu anlegen. Dieser Beitrag zeigt dir, wie du das Problem sauber eingrenzt, warum du zuerst auf die Uhr schauen solltest und wie du das Vertrauen mit Install-WebApplicationProxy neu herstellst. Wie der Proxy grundsätzlich aufgebaut ist und welche Alternativen es gibt, steht im Fachartikel [Web Application Proxy: Architektur und Ablöse](#); den Gesamtzusammenhang findest du auf der Übersichtsseite [Active Directory Federation Services](#).

FAKTEN – Proxy-Trust auf einen Blick

Der Web Application Proxy weist sich gegenüber ADFS mit einem eigenen Client-Zertifikat aus. Es heißt „ADFS ProxyTrust – <Name des WAP>“ und liegt im Zertifikatspeicher des Computers auf dem Proxy.

Das Zertifikat wird beim Ausführen von Install-WebApplicationProxy ausgestellt. ADFS merkt sich, welchen Zertifikaten es als Proxy vertraut.

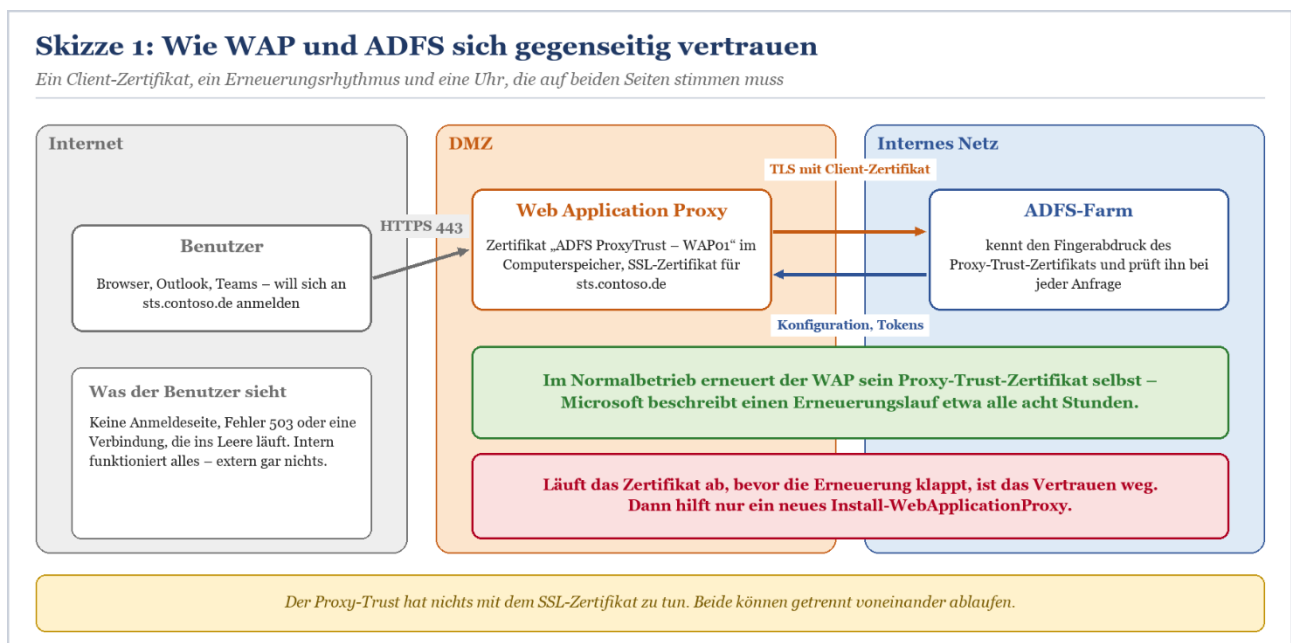
Im laufenden Betrieb erneuert der Proxy das Zertifikat selbstständig. Microsoft nennt für diesen Erneuerungsprozess einen Rhythmus von etwa acht Stunden.

Microsoft listet als Ursachen für ein ungültiges Proxy-Trust-Zertifikat: zu lange ausgeschalteter Proxy, Verbindungsabbrüche zwischen Proxy und ADFS, Probleme der Zertifikatsinfrastruktur,

Änderungen auf ADFS-Seite und nicht synchronisierte Uhren.
Die offizielle Lösung lautet in allen Fällen gleich: Uhren synchronisieren, Install-WebApplicationProxy erneut ausführen.

Das Fehlerbild: Was „der Proxy will nicht mehr“ konkret bedeutet

Bevor du irgendetwas reparierst, solltest du sicher sein, dass du das richtige Problem vor dir hast. Ein abgelaufenes Proxy-Vertrauen sieht von außen aus wie ein Dutzend anderer Störungen: abgelaufenes SSL-Zertifikat, falsch konfigurierter Load Balancer, Firewallregel nach einem Change verschwunden. Der Unterschied liegt im Detail – und im Ereignisprotokoll des Proxys.



Skizze 1: Der Proxy authentifiziert sich bei ADFS per Client-Zertifikat. Das Proxy-Trust-Zertifikat ist nicht das SSL-Zertifikat für sts.contoso.de.

Typische Symptome

- Interne Anmeldungen direkt an der ADFS-Farm funktionieren, externe Anmeldungen über den Proxy nicht.
- Die Verwaltungskonsole für den Remotezugriff meldet auf dem Proxy Fehler, oder Get-WebApplicationProxyApplication liefert statt der veröffentlichten Anwendungen eine Fehlermeldung.
- Im Admin-Protokoll des Web Application Proxy taucht das Ereignis 12000 auf: Der Proxy konnte seit mindestens 60 Minuten nicht nach Konfigurationsänderungen suchen. Microsoft nennt als Ursache fehlende Verbindung zu ADFS oder die Notwendigkeit, das Vertrauen zu erneuern.
- PowerShell-Befehle auf dem Proxy melden, dass das Vertrauenszertifikat „ADFS ProxyTrust – <Name>“ ungültig ist.
- Bei reinen Zeitproblemen findest du zusätzlich Hinweise auf abgelaufene oder noch nicht gültige Tokens, etwa das Ereignis 13013 für ein abgelaufenes Edge-Token, das Microsoft ausdrücklich auf nicht synchronisierte Uhren zurückführt.

Die Protokolle findest du in der Ereignisanzeige unter Anwendungs- und Dienstprotokolle › Microsoft › Windows › Web Application Proxy › Admin. Auf der ADFS-Seite lohnt ein Blick ins Admin-Protokoll von AD FS – dort siehst du, ob Anfragen des Proxys überhaupt ankommen und abgelehnt werden. Wie du die ADFS-Protokolle lesen und das Debug-Tracing gezielt einschalten kannst, beschreibt [ADFS-Ereignisprotokolle lesen – Admin-Log, Debug-Tracing und Auditing](#).

Symptom	Wahrscheinliche Ursache	Wo du nachsiehst
Ereignis 12000 im WAP-Admin-Log	keine Verbindung zu ADFS oder Vertrauen abgelaufen	Test-NetConnection, Zertifikatspeicher, Ereignisse der letzten Tage
„ADFS ProxyTrust“ ungültig	Proxy zu lange offline, Uhr falsch, Erneuerung gescheitert	Ablaufdatum des Zertifikats, w32tm /query /status
Ereignis 13013 oder 13028	Uhren von WAP und ADFS laufen auseinander	w32tm /stripchart gegen einen Domänencontroller
Browser meldet Zertifikatsfehler	SSL-Zertifikat abgelaufen oder falsch gebunden	Get-WebApplicationProxySslCertificate, netsh http show sslcert
Timeout ohne Fehlermeldung	Firewall, DNS oder Load Balancer	Test-NetConnection sts.contoso.de -Port 443 vom Proxy aus

Tabelle 1: Symptome und ihre häufigsten Ursachen.

WARNUNG — Proxy-Trust und SSL-Zertifikat nicht verwechseln

Das SSL-Zertifikat für sts.contoso.de hast du selbst gekauft oder bei deiner Zertifizierungsstelle bestellt. Das Proxy-Trust-Zertifikat stellt ADFS selbst aus. Wer nach einem abgelaufenen SSL-Zertifikat nur Install-WebApplicationProxy ausführt, repariert das falsche Problem – und umgekehrt. Für den Tausch des SSL-Zertifikats gibt es einen eigenen Ablauf: [SSL-Zertifikat auf ADFS und Web Application Proxy tauschen](#).

Wie das Vertrauen überhaupt verloren geht

Das Proxy-Trust-Zertifikat ist absichtlich kurzlebig. Solange der Proxy läuft, ADFS erreicht und beide Seiten dieselbe Uhrzeit haben, merkst du davon nichts: Der Proxy holt sich rechtzeitig ein neues Zertifikat, und ADFS nimmt es an. Probleme entstehen genau dann, wenn eine dieser drei Voraussetzungen wegfällt. Die Gültigkeitsdauer des Vertrauens steuert die ADFS-Eigenschaft ProxyTrustTokenLifetime, die du mit Get-AdfsProperties auslesen kannst. Ändern solltest du sie nur mit gutem Grund – ein Proxy, der wochenlang ausgeschaltet sein darf, ohne sein Vertrauen zu verlieren, ist auch ein Proxy, dessen gestohlene Identität wochenlang gültig bleibt.

Skizze 2: Wie ein Proxy sein Vertrauen verliert

Drei typische Wege – am Ende steht immer dasselbe Fehlerbild



Die gemeinen Varianten

Ein WAP, der aus einem alten Snapshot zurückgeholt wird, bringt ein altes Zertifikat und oft eine falsche Uhrzeit mit. Ein Zweitknoten, der monatelang als „kalte Reserve“ ausgeschaltet war, ebenso.

Skizze 2: Offline-Zeit, Zeitabweichung oder alter Snapshot – das Ergebnis ist dasselbe.

Besonders tückisch sind zwei Fälle aus der Praxis. Erstens der zweite Proxy, der als „kalte Reserve“ ausgeschaltet im Rechenzentrum steht und genau dann einspringen soll, wenn der erste ausfällt. Er hat sein Vertrauen längst verloren, und das merkst du ausgerechnet im Notfall. Zweitens der Snapshot: Wer einen Proxy auf einen Stand von vor drei Wochen zurücksetzt, holt ein altes Zertifikat und eine veraltete Systemzeit zurück. Bis der Zeitdienst die Uhr korrigiert hat, ist das Vertrauen bereits gescheitert.

TIPP — Kalte Reserve regelmäßig aufwecken

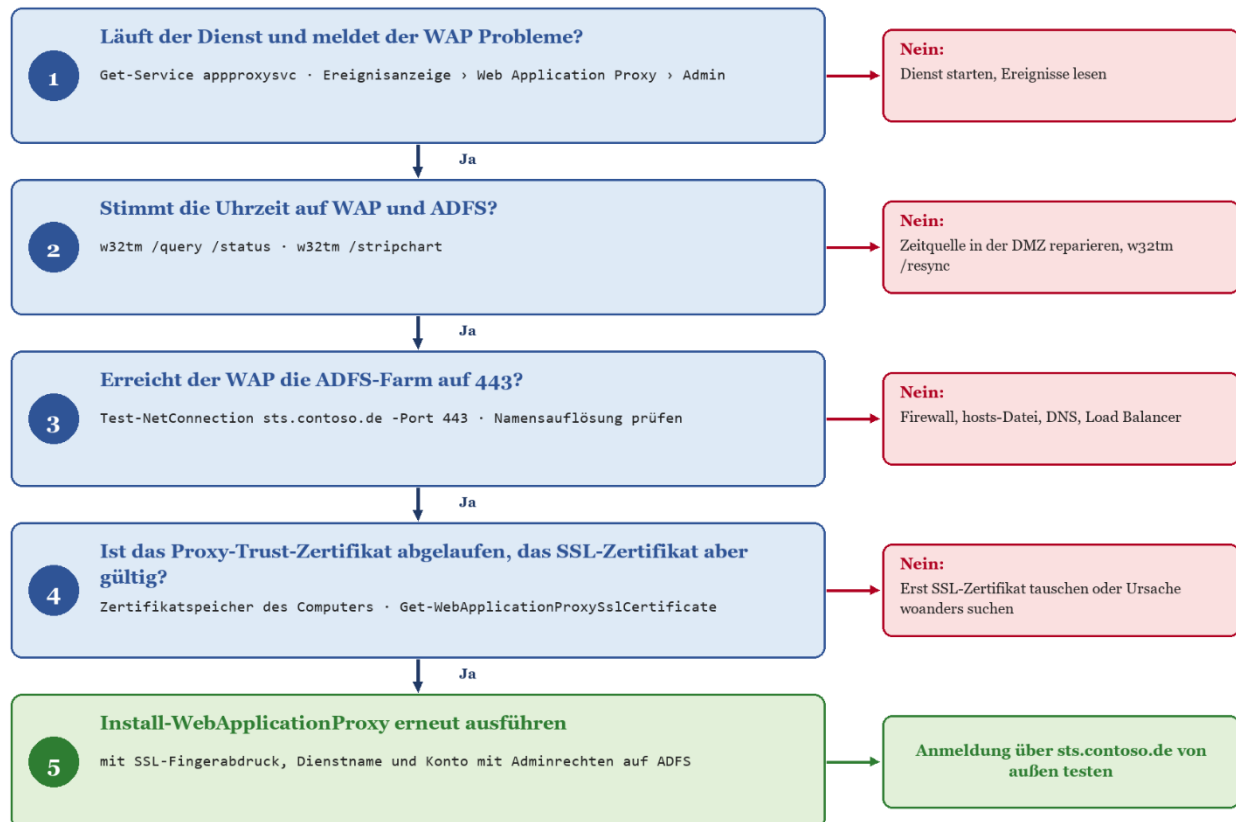
Wenn du einen Ersatz-Proxy bewusst ausgeschaltet vorhältst, plane einen festen Termin, an dem er hochfährt, die Uhr synchronisiert und sein Vertrauen erneuert. Noch besser: Lass beide Proxys hinter dem Load Balancer aktiv laufen. Ein laufender Knoten pflegt sein Vertrauen selbst, ein ausgeschalteter verrottet.

Diagnose in fünf Fragen – bevor du irgendetwas neu installierst

Der Reflex, sofort Install-WebApplicationProxy zu starten, ist verständlich. Er ist trotzdem falsch, solange du nicht weißt, warum das Vertrauen verloren gegangen ist. Läuft die Uhr falsch, scheitert auch die Neueinrichtung. Ist die Firewall zu, ebenso. Arbeite die folgenden fünf Fragen der Reihe nach ab – das kostet fünf Minuten und spart dir die Stunde, in der du dich fragst, warum die Reparatur nicht repariert.

Skizze 3: Diagnoseablauf in fünf Fragen

Von oben nach unten abarbeiten – jede Ja-Antwort bringt dich eine Stufe weiter



Schritt 5 vor Schritt 2 auszuführen, ist der Klassiker: Mit falscher Uhr scheitert auch die Neuinstallation.

Skizze 3: Der Diagnoseablauf – erst Dienst, Uhr und Netzwerk, dann das Vertrauen.

Frage 1: Läuft der Dienst, und was sagt das Protokoll?

Auf dem Proxy prüfst du zuerst, ob der Dienst läuft und welche Ereignisse er zuletzt geschrieben hat. Die folgenden Befehle laufen in einer PowerShell mit Administratorrechten direkt auf dem WAP:

```
# Dienst des Web Application Proxy
Get-Service -Name approxysvc

# Letzte Fehler und Warnungen im Admin-Protokoll
Get-WinEvent -LogName "Microsoft-Windows-WebApplicationProxy/Admin" -MaxEvents 30 |
    Where-Object Level -le 3 |
    Format-Table TimeCreated, Id, Message -Wrap

# Gesamtzustand (ab Windows Server 2016)
Get-WebApplicationProxyHealth
```

Listing 1: Dienst und Protokoll auf dem Proxy prüfen.

Frage 2: Stimmt die Uhrzeit?

Zeitabweichung ist der unterschätzte Hauptverdächtige. Zertifikate und Tokens haben Gültigkeitsfenster, und wenn die Uhr des Proxys gegenüber ADFS deutlich daneben liegt, hält die Gegenseite gültige Zertifikate für abgelaufen oder noch nicht gültig. Prüfe deshalb auf dem Proxy, woher er seine Zeit bezieht und wie weit er von einem Domänencontroller oder dem ADFS-Server abweicht:

```
# Zeitquelle und letzter erfolgreicher Abgleich
w32tm /query /status
w32tm /query /source

# Abweichung gegenüber einem internen Server messen
w32tm /stripchart /computer:dc01.contoso.local /samples:5 /dataonly
```

Listing 2: Zeitquelle und Zeitabweichung auf dem Proxy ermitteln.

Steht als Quelle „Local CMOS Clock“ oder „Free-running System Clock“, hat dein Proxy schlicht keine Zeitquelle – er läuft frei und driftet, wie es ihm gefällt. Wie du das dauerhaft reparierst, steht weiter unten im Abschnitt zur Zeitsynchronisation in der DMZ.

Frage 3: Erreicht der Proxy die ADFS-Farm?

Der Proxy muss den Federation-Service-Namen auf die internen ADFS-Server oder den internen Load Balancer auflösen und dort Port 443 erreichen. In der DMZ geschieht das häufig über einen Eintrag in der hosts-Datei – der nach einem Neuaufbau des Load Balancers gern auf eine IP-Adresse zeigt, die es nicht mehr gibt.

```
# Namensauflösung und Port prüfen
Resolve-DnsName sts.contoso.de
Get-Content C:\Windows\System32\drivers\etc\hosts | Select-String "sts"
Test-NetConnection -ComputerName sts.contoso.de -Port 443

# Metadaten der Farm abrufen - klappt das, steht die Leitung
Invoke-WebRequest -Uri "https://sts.contoso.de/FederationMetadata/2007-
06/FederationMetadata.xml" -
    -UseBasicParsing | Select-Object StatusCode
```

Listing 3: Verbindung vom Proxy zur ADFS-Farm prüfen.

Die Metadaten-Adresse empfiehlt Microsoft selbst als Verbindungstest zwischen Proxy und ADFS. Kommt hier ein Statuscode 200 zurück, sind Namensauflösung, Firewall und SSL-Kette zur Farm in Ordnung. Ein Timeout deutet auf Firewall oder Load Balancer, ein Zertifikatsfehler auf eine

fehlende Stamm- oder Zwischenzertifizierungsstelle auf dem Proxy. Läuft dein Proxy hinter einem Load Balancer, prüfe dort zusätzlich die Health Probes – Details dazu in [ADFS hinter dem Load Balancer – Health Probe, SNI und Persistenz](#).

Frage 4: Welches Zertifikat ist abgelaufen?

```
# Proxy-Trust-Zertifikat im Computerspeicher des WAP
Get-ChildItem Cert:\LocalMachine\My |
  Where-Object Subject -like "*ADFS ProxyTrust*" |
  Format-List Subject, NotBefore, NotAfter, Thumbprint

# SSL-Zertifikat, das der Proxy für den Federation Service verwendet
Get-WebApplicationProxySslCertificate
netsh http show sslcert
```

Listing 4: Proxy-Trust- und SSL-Zertifikat auf dem Proxy prüfen.

Ist das Proxy-Trust-Zertifikat abgelaufen oder fehlt es ganz, und haben Uhr und Netzwerk die Prüfungen aus Frage 2 und 3 bestanden, bist du bei Frage 5 angekommen. Ist dagegen das SSL-Zertifikat abgelaufen, tauschst du zuerst dieses – sonst scheitert auch die Neueinrichtung des Vertrauens.

Merkmal	Proxy-Trust-Zertifikat	SSL-Zertifikat
Wer stellt aus?	ADFS selbst	deine Zertifizierungsstelle oder ein öffentlicher Anbieter
Wofür?	Proxy weist sich gegenüber ADFS aus	Clients vertrauen sts.contoso.de
Erneuerung	automatisch im laufenden Betrieb	manuell oder per Automatisierung, typisch jährlich
Bei Ablauf	Install-WebApplicationProxy erneut ausführen	neues Zertifikat einspielen und binden
Wo zu finden?	Computerspeicher des WAP, Name „ADFS ProxyTrust – ...“	Computerspeicher auf WAP und ADFS

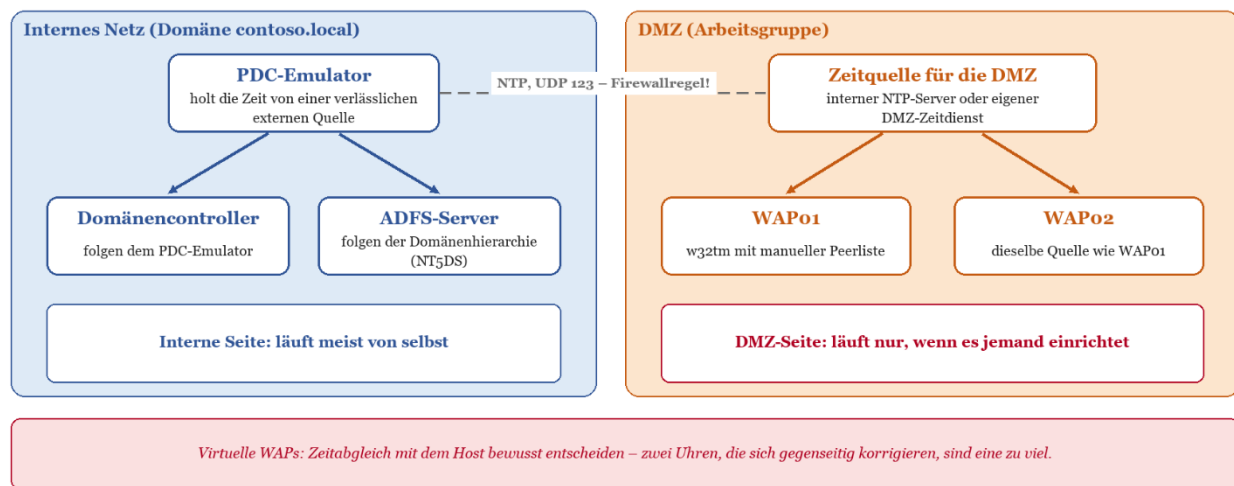
Tabelle 2: Zwei Zertifikate, zwei Lebensläufe.

Zeitsynchronisation in der DMZ – die Ursache hinter der Ursache

Interne ADFS-Server sind Mitglieder der Domäne und holen sich ihre Zeit über die Domänenhierarchie, an deren Spitze der PDC-Emulator steht. Das funktioniert in den meisten Umgebungen ohne weiteres Zutun. Der Web Application Proxy steht dagegen meist als Arbeitsgruppenrechner in der DMZ. Er hat keine Domänenhierarchie, der er folgen könnte, und eine Firewall, die ausgehendes NTP gern blockiert. Ergebnis: eine Uhr, die frei läuft und irgendwann so weit daneben liegt, dass die Kryptografie aufgibt.

Skizze 4: Woher die Uhr in der DMZ ihre Zeit bekommt

Interne Server folgen der Domänenhierarchie – der WAP in der Arbeitsgruppe braucht eine eigene Quelle



Skizze 4: Die Domäne versorgt sich selbst mit Zeit, die DMZ braucht eine bewusst eingerichtete Quelle.

Die Lösung ist unspektakulär: Gib dem Proxy eine feste Zeitquelle, die dieselbe Zeit liefert wie dein internes Netz. Das kann ein interner NTP-Server sein, den du per Firewallregel für UDP 123 aus der DMZ erreichbar machst, oder ein eigener Zeitdienst in der DMZ, der selbst an derselben Quelle hängt wie dein PDC-Emulator.

```
# Feste Zeitquelle auf dem WAP einrichten (Beispiel)
w32tm /config /manualpeerlist:"ntp.contoso.local,0x8" /syncfromflags:manual /reliable:no
/update
Restart-Service w32time
w32tm /resync /force

# Kontrolle
w32tm /query /status
w32tm /query /peers
```

Listing 5: Zeitquelle für einen Proxy in der Arbeitsgruppe festlegen.

WICHTIG – Virtuelle Proxys und die Zeit des Hosts

Läuft dein Proxy als VM, bekommt er die Zeit möglicherweise zusätzlich vom Virtualisierungshost. Entscheide bewusst, wer die Uhr führt. Zwei Zeitquellen, die sich gegenseitig korrigieren, erzeugen genau das Springen, das Zertifikate nicht mögen. Und wenn der Host selbst falsch geht, nützt dir die schönste NTP-Konfiguration im Gast nichts.

TIPP – Zeitabweichung überwachen statt entdecken

Nimm die Zeitabweichung der Proxys in dein Monitoring auf – ein einfacher geplanter w32tm-Abgleich gegen einen Domänencontroller mit Schwellwert reicht. Wie du ADFS und Proxy insgesamt sinnvoll überwachst, steht in [ADFS überwachen – Health Checks, Diagnose-Toolbox und Entra Connect Health](#).

Am Rande: Eine falsche Uhr auf dem Proxy schadet nicht nur dem Proxy-Trust. Wer über den Web Application Proxy Anwendungen mit Kerberos Constrained Delegation veröffentlicht, bekommt bei Zeitabweichungen zusätzlich Kerberos-Fehler. Hintergründe dazu findest du auf der Seite [Microsoft Kerberos](#).

Das Vertrauen neu herstellen mit Install-WebApplicationProxy

Uhr stimmt, Netzwerk steht, SSL-Zertifikat ist gültig – jetzt stellst du das Vertrauen neu her. Install-WebApplicationProxy erledigt genau das: Der Proxy meldet sich mit einem Konto, das auf den ADFS-Servern Administratorrechte besitzt, bei der Farm an und erhält ein neues Proxy-Trust-Zertifikat. Die veröffentlichten Anwendungen liegen in der ADFS-Konfiguration und bleiben erhalten.

Vorbereitung

- Den Fingerabdruck des SSL-Zertifikats für sts.contoso.de auf dem Proxy ermitteln, etwa mit `Get-ChildItem Cert:\LocalMachine\My`.
- Den exakten Federation-Service-Namen kennen. Auf der ADFS-Seite liefert `Get-AdfsProperties` ihn in der Eigenschaft `HostName`.
- Ein Konto bereithalten, das lokaler Administrator auf den ADFS-Servern ist. Das Kennwort brauchst du nur für diesen einen Vorgang.
- Die Liste der veröffentlichten Anwendungen vorher sichern, etwa mit `Get-WebApplicationProxyApplication` und `Export-Clixml` – falls doch etwas schiefgeht, hast du die Parameter griffbereit.

Die Ausführung

```
# Auf dem Web Application Proxy, PowerShell als Administrator
$cred = Get-Credential -Message "Konto mit Adminrechten auf den ADFS-Servern"
$thumb = "<Fingerabdruck des SSL-Zertifikats für sts.contoso.de>"

Install-WebApplicationProxy `
  -FederationServiceName "sts.contoso.de" `
  -CertificateThumbprint $thumb `
  -FederationServiceTrustCredential $cred

# Dienst neu starten und Zustand prüfen
Restart-Service approxysvc
Get-WebApplicationProxyApplication | Format-Table Name, ExternalUrl, BackendServerUrl
```

Listing 6: Proxy-Vertrauen neu herstellen.

Bei mehreren Proxys führst du den Befehl auf jedem Knoten aus, dessen Vertrauen abgelaufen ist. Jeder Proxy hat sein eigenes Proxy-Trust-Zertifikat – dass WAP01 wieder läuft, sagt nichts über WAP02. Wenn dein Load Balancer beide Knoten bedient, nimm den noch nicht reparierten Knoten so lange aus dem Pool, bis auch er wieder vertraut wird.

WARNUNG — Vorsicht mit dem Registrierungsschlüssel aus alten Foren

In vielen Anleitungen findest du den Hinweis, den Wert `ProxyConfigurationStatus` unter `HKLM\Software\Microsoft\ADFS` auf 1 zu setzen, damit der Konfigurationsassistent in der Verwaltungskonsole wieder erscheint. Das funktioniert, ist aber nur der Umweg über die Oberfläche zum selben Ziel. Der direkte und dokumentierte Weg ist `Install-WebApplicationProxy` in PowerShell – nachvollziehbar, skriptbar und ohne Eingriff in die Registrierung.

Funktionstest danach

Prüfung	Werkzeug	Erwartung
Dienst	<code>Get-Service approxysvc</code>	Status Running
Proxy-Trust	Zertifikatspeicher des WAP	neues „ADFS ProxyTrust“-Zertifikat mit

		frischem Ablaufdatum
Konfiguration	Get-WebApplicationProxyApplication	alle Anwendungen ohne Fehler aufgelistet
Protokoll	WAP-Admin-Log	kein neues Ereignis 12000
Anmeldung extern	Browser außerhalb des Netzes, sts.contoso.de/adfs/ls/idpinitiatedsignon	Anmeldeseite erscheint, Anmeldung klappt (sofern die Seite aktiviert ist)
Microsoft 365	Anmeldung mit föderiertem Konto von außen	Weiterleitung über den Proxy, Token wird ausgestellt

Tabelle 3: Prüfliste nach dem Neuaufbau des Vertrauens.

Klappt die externe Anmeldung trotz neu hergestelltem Vertrauen nicht, liegt das Problem woanders – bei Claims, Benutzerkonten oder Relying Party Trusts. Die häufigsten Ursachen dafür sammelt [ADFS-Anmeldung schlägt fehl – die häufigsten Ursachen und ihre Lösung](#).

WEITER — Passende Beiträge rund um den Proxy

- › [Web Application Proxy: Architektur und Ablöse](#) – Aufbau, Grenzen und mögliche Nachfolger des Proxys
- › [SSL-Zertifikat auf ADFS und Web Application Proxy tauschen](#) – wenn nicht das Vertrauen, sondern das SSL-Zertifikat abgelaufen ist
- › [ADFS sichern und wiederherstellen – Rapid Restore Tool in der Praxis](#) – warum der Proxy-Trust nach jeder Wiederherstellung neu aufgebaut wird

Fazit: Uhr vor Zertifikat, Diagnose vor Reparatur

Ein Web Application Proxy, der plötzlich nicht mehr will, ist selten ein Rätsel. In der überwältigenden Mehrheit der Fälle stand er zu lange still, seine Uhr lief weg, oder die Verbindung zur Farm war unterbrochen – und das Proxy-Trust-Zertifikat ist abgelaufen. Die Reparatur mit Install-WebApplicationProxy dauert Minuten. Die eigentliche Arbeit steckt davor: in der Reihenfolge Dienst, Uhr, Netzwerk, Zertifikat. Wer diese Reihenfolge einhält, repariert einmal. Wer sie überspringt, repariert öfter.

Damit der nächste Montagmorgen ruhiger wird, gehören drei Dinge in deinen Betrieb: eine feste Zeitquelle für die DMZ, ein Monitoring, das Zeitabweichung und Ereignis 12000 meldet, und keine Proxys, die monatelang ausgeschaltet als Reserve verstauben. ADFS und der Web Application Proxy laufen in vielen Unternehmen seit über zehn Jahren zuverlässig – mit dieser Pflege bleibt das auch so, bis du den Ausstieg in Ruhe geplant hast. Wenn du dabei Unterstützung möchtest, findest du uns im [Consulting zu ADFS \(Active Directory Federation Services\)](#). Betrieb und Fehlersuche rund um Farm und Proxy vertieft außerdem das Buch – mehr dazu unter [ADFS in der Praxis – das Buch im Detail](#).

FAQ: Web Application Proxy Vertrauen erneuern

Wie erneuere ich das Vertrauen zwischen Web Application Proxy und ADFS?

Indem du auf dem Proxy Install-WebApplicationProxy mit dem Federation-Service-Namen, dem Fingerabdruck des SSL-Zertifikats und einem Konto mit Administratorrechten auf den ADFS-Servern erneut ausführst. Vorher prüfst du Uhrzeit und Netzwerkverbindung.

Gehen beim erneuten Ausführen von Install-WebApplicationProxy meine veröffentlichten Anwendungen verloren?

Nein. Die Veröffentlichungen liegen in der ADFS-Konfiguration und stehen nach dem Neuaufbau des Vertrauens wieder zur Verfügung. Eine Sicherung der Liste mit Get-WebApplicationProxyApplication schadet trotzdem nicht.

Warum läuft das Proxy-Trust-Zertifikat ab?

Weil es bewusst kurzlebig ist und im laufenden Betrieb regelmäßig erneuert wird. War der Proxy zu lange offline, gab es Verbindungsprobleme zu ADFS oder laufen die Uhren auseinander, kommt die Erneuerung zu spät.

Wie oft erneuert der Web Application Proxy sein Vertrauenszertifikat?

Microsoft beschreibt einen Erneuerungslauf etwa alle acht Stunden. Solange der Proxy läuft und ADFS erreicht, musst du dich darum nicht kümmern.

Was bedeutet Ereignis 12000 auf dem Web Application Proxy?

Der Proxy konnte mindestens 60 Minuten lang nicht nach Konfigurationsänderungen bei ADFS suchen. Ursache ist fehlende Verbindung zu ADFS oder ein Vertrauen, das erneuert werden muss.

Welche Rolle spielt die Uhrzeit beim Proxy-Trust?

Eine zentrale. Zertifikate und Tokens haben Gültigkeitsfenster. Weicht die Uhr des Proxys deutlich von ADFS ab, werden gültige Zertifikate als abgelaufen oder noch nicht gültig abgelehnt – und auch die Neueinrichtung des Vertrauens scheitert.

Wie synchronisiere ich die Zeit auf einem WAP in der Arbeitsgruppe?

Mit w32tm und einer manuellen Peerliste, die auf einen internen NTP-Server oder einen Zeitdienst in der DMZ zeigt. Die Firewall muss dafür UDP 123 zulassen.

Ist das Proxy-Trust-Zertifikat dasselbe wie das SSL-Zertifikat?

Nein. Das SSL-Zertifikat für den Federation Service stellt deine Zertifizierungsstelle aus, das Proxy-Trust-Zertifikat stellt ADFS selbst aus. Sie laufen unabhängig voneinander ab und werden auf unterschiedliche Weise erneuert.

Muss ich das Vertrauen auf jedem Proxy einzeln erneuern?

Ja. Jeder Proxy hat sein eigenes Proxy-Trust-Zertifikat. Führe Install-WebApplicationProxy auf jedem Knoten aus, dessen Vertrauen abgelaufen ist.

Kann ich die Gültigkeit des Proxy-Vertrauens verlängern?

Die Gültigkeitsdauer steuert die ADFS-Eigenschaft ProxyTrustTokenLifetime. Eine Verlängerung ist technisch möglich, verlängert aber auch die Zeit, in der ein gestohlenes Proxy-Zertifikat missbraucht werden kann. Besser ist ein Betrieb, in dem Proxys nicht wochenlang ausgeschaltet sind.