RD Gateway Zertifikat abgelaufen: schnell erneuern, künftig vorbeugen



WISSEN
Aufbau, Rollen und Betrieb von Remotedesktopdiensten im Überblick.
› Remote Desktop Services

BERATUNG
Gateway, Zertifikate und Load Balancing sauber planen und erneuern.
› Beratung zu Remote Desktop Services

SCHULUNG
RD Gateway, Zertifikate und PowerShell für Terminalserver im Team lernen.
› Schulung Remote Desktop Services

Mittwoch, 7:58 Uhr. Im Büro Frankfurt läuft alles, im Homeoffice läuft gar nichts. Der Remotedesktopclient meldet sinngemäß, das Zertifikat des Remotedesktopgateways sei abgelaufen oder gesperrt, und der Außendienst in Hamburg schickt Screenshots in Schriftgröße 72. Wenn du gerade nach „rd gateway zertifikat erneuern“ suchst, ist die gute Nachricht: Das ist in einer halben Stunde behoben, wenn du ein gültiges Zertifikat mit privatem Schlüssel in der Hand hast. Die schlechte: Ohne dieses Zertifikat hilft dir keine PowerShell der Welt.

Dieser Beitrag zeigt dir, wie du das Symptom von extern einordnest, mit lesenden Befehlen prüfst, welches Zertifikat das Gateway gerade ausliefert, und wie du das neue Zertifikat mit Set-RDCertificate für die Rolle RDGateway setzt. Dazu kommen die üblichen Fallen: fehlende Zwischenzertifikate, eine PFX ohne privaten Schlüssel, zwei Gateways hinter einem Load Balancer und die Frage, ob eine interne PKI für ein Gateway im Internet reicht. Am Ende steht eine Checkliste, damit das Zertifikat nächstes Jahr nicht wieder heimlich stirbt. Wie Gateway, Connection Broker und Session Hosts grundsätzlich zusammenspielen, steht auf der Übersichtsseite Remote Desktop Services.

FAKTEN · Das Wichtigste in Kürze

Ein abgelaufenes Gateway-Zertifikat trifft nur Verbindungen über das Gateway, also fast immer die externen. Interne Clients, die direkt zum Session Host verbinden, merken nichts.

Gehört das Gateway zur RDS-Bereitstellung, setzt du das Zertifikat zentral am Connection Broker: Set-RDCertificate -Role RDGateway mit -ImportPath (PFX) oder seit Windows Server 2019 mit -

Thumbprint.

Get-RDCertificate -Role RDGateway zeigt Subject, SAN, Aussteller, Ablaufdatum, Fingerabdruck und die Stufe Trusted, Untrusted oder Not Configured.

Das Zertifikat braucht einen privaten Schlüssel, den Zweck Serverauthentifizierung, den externen Gateway-Namen im SAN und eine Kette, der die Clients vertrauen.

Mit Load Balancer muss jedes Gateway dasselbe Zertifikat tragen. Beendet der Load Balancer TLS selbst, erneuerst du es dort zusätzlich.

Symptom: das Gateway-Zertifikat ist abgelaufen, und nur extern brennt es

Ein abgelaufenes Zertifikat am RD Gateway ist ein Fehler mit perfektem Timing: Er tritt exakt zum Ablaufdatum ein, meist über Nacht, und trifft alle externen Benutzer gleichzeitig. Weil interne Verbindungen ohne Gateway weiter funktionieren, hören Admins im Büro zuerst: „Bei mir geht es doch." Das stimmt. Es hilft nur niemandem im Homeoffice.

Was Anwender sehen	Was dahintersteckt	Erste Prüfung
Meldung: Zertifikat des Remotedesktopgateways abgelaufen oder gesperrt	NotAfter überschritten oder Sperrstatus nicht prüfbar	Get-RDCertificate -Role RDGateway, ExpiresOn
Nur externe Verbindungen scheitern, intern alles gut	Interne Clients nutzen das Gateway nicht (Bypass für lokale Adressen)	RDP-Datei: gatewayhostname, gatewayusagemethod
Warnung zum Namen trotz neuem Zertifikat	Gateway-Name fehlt im SAN, etwa nur rdgw01.contoso.local	SubjectAlternateName prüfen
Nach dem Tausch geht es auf RDGW01, auf RDGW02 nicht	Load Balancer verteilt auf ein Gateway mit altem Zertifikat	Zertifikat je Gateway per Fingerabdruck vergleichen
Private Geräte scheitern, Firmengeräte nicht	Kette einer internen PKI ist auf Privatgeräten unbekannt	Aussteller prüfen: interne CA oder öffentliche CA
Web-Client im Browser zeigt Zertifikatsfehler	Auch RD Web Access und Web Client hängen am Zertifikat	Get-RDCertificate ohne -Role, alle Rollen

Die Warnung beim Verbinden zum Session Host selbst, also die Frage „Der Identität des Remotecomputers kann nicht vertraut werden", ist ein verwandtes, aber eigenes Thema. Dort geht es um die Rollen RDRedirector und RDPublishing und um die Zertifikate der Session Hosts. Das behandelt der Beitrag RDS-Zertifikatswarnung beim Verbinden beheben.

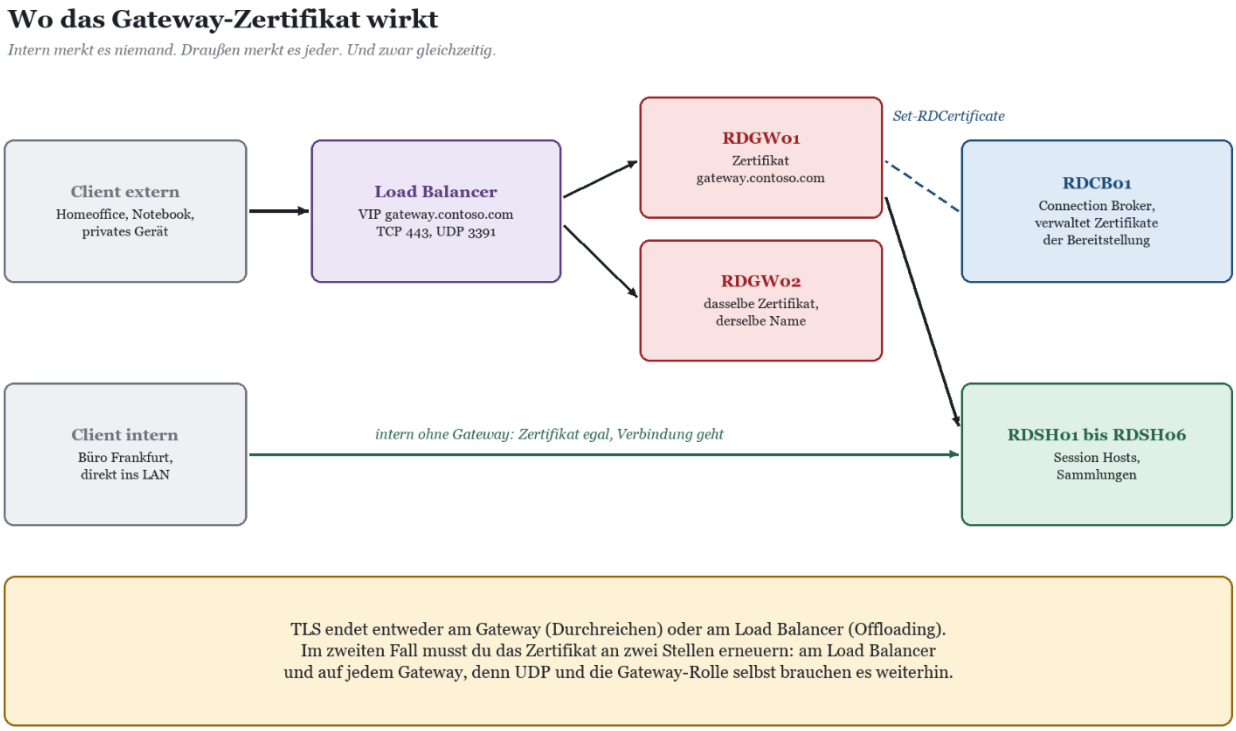
AUS DER PRAXIS · Ein Maschinenbauer mit 300 Benutzern

Ein Maschinenbauer mit 300 Benutzern und Standorten in Köln und Hamburg hatte das Zertifikat pünktlich erneuert, dem Load Balancer importiert und Feierabend gemacht. Am nächsten Morgen scheiterte jede zweite externe Verbindung. Der Load Balancer reichte TLS an zwei Gateways durch, und nur eines davon hatte das neue Zertifikat bekommen, weil das zweite Gateway nie in die Bereitstellung aufgenommen worden war und Set-RDCertificate es deshalb nicht kannte. Statistisch war die Lösung zu 50 Prozent richtig. Die Anwender fanden das weniger lustig.

Warum ein abgelaufenes Zertifikat das RD Gateway sofort lahmlegt

Das RD Gateway kapselt RDP in HTTPS. Der Client baut zuerst eine TLS-Verbindung zum Gateway auf, authentifiziert sich dort und lässt sich erst danach zum Session Host weiterreichen. Das Gateway-Zertifikat ist damit kein Schmuck, sondern die Eintrittskarte: Lehnt der Client das

Zertifikat ab, kommt er nie bis zur Anmeldung. Der optionale UDP-Transport auf Port 3391 nutzt ebenfalls das Zertifikat des Gateways.



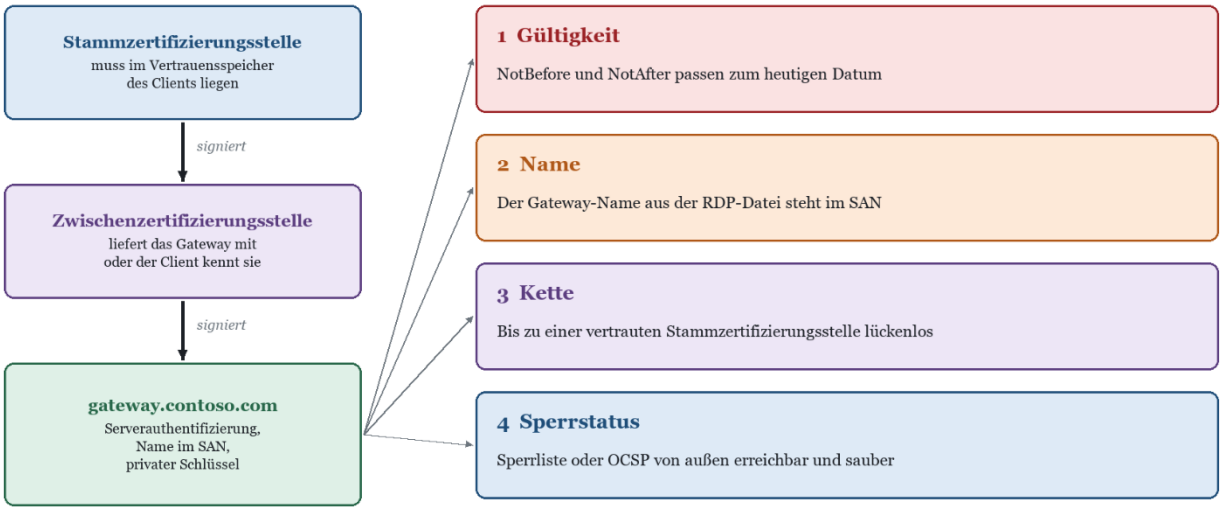
Skizze: Zwei Gateways hinter einem Load Balancer, Contoso-Beispiel

Was der Client am Zertifikat prüft

Der Remotedesktopclient prüft das Gateway-Zertifikat strenger als viele Browser es dir durchgehen lassen. Ein Klick auf „Trotzdem verbinden“ ist beim Gateway nicht vorgesehen. Er kontrolliert die Gültigkeit, ob der in der RDP-Datei hinterlegte Gateway-Name im Zertifikat steht, ob die Kette zu einer vertrauten Stammzertifizierungsstelle führt und ob das Zertifikat gesperrt ist. Ist die Sperrliste der ausstellenden CA von außen nicht erreichbar, kann auch ein gültiges Zertifikat abgelehnt werden. Das ist die klassische Falle bei interner PKI.

Was der Client prüft, bevor er dir vertraut

Vier Fragen, vier Chancen zu scheitern. Die Gültigkeit ist nur die bekannteste.



Skizze: Zertifikatskette und Prüfungen des Remotedesktopclients, vereinfacht

Wo das Zertifikat technisch hinterlegt ist

Gehört das Gateway zur RDS-Bereitstellung, verwaltet der Connection Broker die Zertifikate aller Rollen. Im Server-Manager findest du sie unter Remotedesktopdienste › Übersicht › Bereitstellungsübersicht › Aufgaben › Bereitstellungseigenschaften bearbeiten › Zertifikate. Dort stehen vier Rollendienste: RD-Verbindungsbroker mit einmaligem Anmelden und mit Veröffentlichung, RD-Web Access und RD-Gateway. Der Connection Broker verteilt das Zertifikat beim Setzen an alle Gateway-Server, die er als Teil der Bereitstellung kennt. Genau hier liegt die Falle aus dem Praxisbeispiel: Ein Gateway, das nur im Load Balancer steht, aber nicht in der Bereitstellung, bekommt nichts.

Ein Gateway ohne Bereitstellung, etwa ein eigenständiges Gateway vor einer alten Farm, verwaltest du direkt im RD-Gateway-Manager unter Eigenschaften › SSL-Zertifikat. Auf dem Gateway selbst landet das Zertifikat in beiden Fällen im Computerspeicher unter Zertifikate (Lokaler Computer) › Eigene Zertifikate.

Rolle in Get-RDCertificate	Wofür	Typischer Name im SAN
RDGateway	TLS zwischen Client und Gateway, auch UDP	gateway.contoso.com
RDWebAccess	RD-Webzugriff und Web Client im Browser	gateway.contoso.com oder rdweb.contoso.com
RDPublishing	Signatur der RDP-Dateien und RemoteApps	rdcb.contoso.com
RDRedirector	Einmaliges Anmelden am Connection Broker	rdcb.contoso.com

FAKTEN · Stufen in Get-RDCertificate

Trusted: Zertifikat einer Unternehmens-CA oder einer öffentlichen CA.

Untrusted: selbstsigniertes Zertifikat, wie es die Bereitstellung beim Einrichten erzeugen kann.

Not Configured: kein Zertifikat hinterlegt oder das Zertifikat ist nicht gültig. Ein abgelaufenes

Gateway-Zertifikat landet deshalb hier und nicht etwa bei „Trusted, aber alt“.

Diagnose Schritt für Schritt: lesen, bevor du etwas tauschst

Alle Befehle in diesem Abschnitt ändern nichts. Führe sie auf dem Connection Broker RDCB01 oder einer Verwaltungsstation mit den RSAT-Werkzeugen für Remotedesktopdienste aus. Bei einem hochverfügbaren Connection Broker gibst du mit -ConnectionBroker den aktiven Broker an, Details dazu im Beitrag RDS Connection Broker hochverfügbar machen.

Schritt 1: Zertifikate der Bereitstellung auslesen

```
Import-Module RemoteDesktop
Get-RDCertificate -ConnectionBroker RDCB01.contoso.local |
    Select-Object Role, Level, Subject, SubjectAlternateName, IssuedBy, ExpiresOn, Thumbprint |
    Format-List
```

Steht bei RDGateway die Stufe Not Configured und ein ExpiresOn in der Vergangenheit, ist die Diagnose eigentlich schon fertig. Schau trotzdem weiter, denn oft laufen RDGateway und RDWebAccess mit demselben Zertifikat und damit am selben Tag ab.

Schritt 2: Zertifikatsspeicher auf jedem Gateway prüfen

Jetzt die Gegenprobe auf den Gateways selbst. Interessant sind Ablaufdatum, privater Schlüssel und der Zweck Serverauthentifizierung. Liegt dort schon ein neues Zertifikat, das nur noch nicht gebunden ist, sparst du dir die Beschaffung.

```
$gw = 'RDGW01.contoso.local','RDGW02.contoso.local'
Invoke-Command -ComputerName $gw -ScriptBlock {
    Get-ChildItem Cert:\LocalMachine\My |
      Where-Object { $_.EnhancedKeyUsageList.FriendlyName -contains 'Server Authentication' -or
                     $_.EnhancedKeyUsageList.ObjectId -contains '1.3.6.1.5.5.7.3.1' } |
      Select-Object Subject, NotAfter, HasPrivateKey, Thumbprint,
        @{n='SAN';e={ ($_.Extensions | Where-Object { $_.Oid.Value -eq '2.5.29.17' }).Format($false)
}}
} | Sort-Object PSComputerName, NotAfter | Format-Table PSComputerName, Subject, NotAfter,
HasPrivateKey, Thumbprint
```

Schritt 3: gebundenes Zertifikat per CIM abfragen

Welches Zertifikat die Gateway-Rolle tatsächlich verwendet, verrät die WMI-Klasse Win32_TSGatewayServerSettings. Der dort hinterlegte SHA1-Hash muss zum Fingerabdruck aus Schritt 1 passen, auf jedem Gateway.

```
Get-CimInstance -ComputerName RDGW01.contoso.local,RDGW02.contoso.local `
    -Namespace root/CIMV2/TerminalServices -ClassName Win32_TSGatewayServerSettings |
    Select-Object PSComputerName, @{n='Hash';e={ -join ($_.SSLCertificateSHA1Hash |
        ForEach-Object { $_.ToString('X2') }) }}
```

Schritt 4: Ereignisprotokoll des Gateways lesen

Das Gateway protokolliert Verbindungsversuche im Kanal Microsoft-Windows-TerminalServices-Gateway/Operational. Scheitert der TLS-Aufbau am Zertifikat, kommen viele Clients gar nicht bis zur Protokollierung, das Protokoll wird dann auffällig still. Auch Stille ist ein Befund. Zusätzlich lohnt der Blick in das System-Protokoll auf Schannel-Fehler. Welche Ereignis-IDs im RDS-Umfeld wichtig sind, steht im Beitrag Wichtige RDS-Ereignis-IDs und was sie bedeuten.

```
Get-WinEvent -ComputerName RDGW01.contoso.local -MaxEvents 50 `
    -LogName 'Microsoft-Windows-TerminalServices-Gateway/Operational' |
```

```
    Select-Object TimeCreated, Id, LevelDisplayName, Message | Format-Table -Wrap

Get-WinEvent -ComputerName RDGW01.contoso.local -FilterHashtable @{
    LogName='System'; ProviderName='Schannel'; StartTime=(Get-Date).AddDays(-2) } -ErrorAction
SilentlyContinue |
    Select-Object TimeCreated, Id, Message | Format-Table -Wrap
```

Schritt 5: von außen prüfen, was ausgeliefert wird

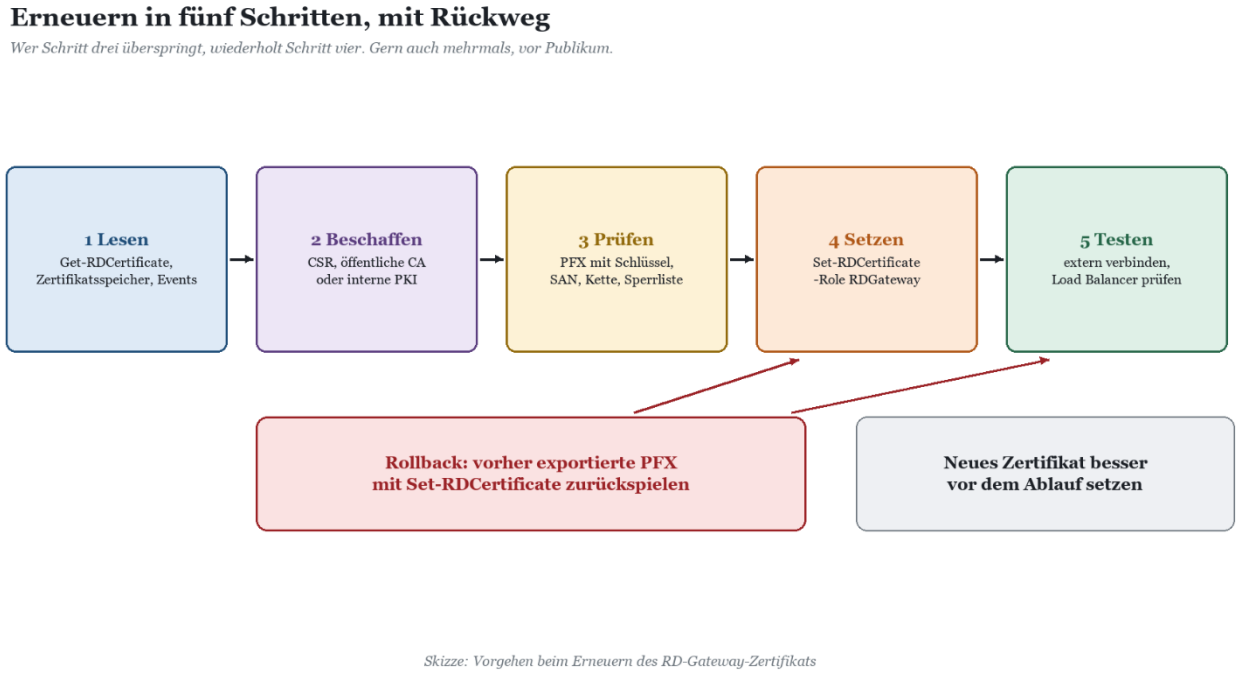
Der ehrlichste Test kommt von außen, also von einem Gerät im Internet und nicht aus dem LAN. So siehst du, welches Zertifikat der Load Balancer oder das Gateway wirklich ausliefert. Bei mehreren Gateways wiederholst du den Test, bis du beide erwischt hast, oder du prüfst die Gateways intern einzeln über ihre eigenen Namen.

```
$name = 'gateway.contoso.com'
$tcp  = [System.Net.Sockets.TcpClient]::new($name, 443)
$ssl  = [System.Net.Security.SslStream]::new($tcp.GetStream(), $false, { $true })
$ssl.AuthenticateAsClient($name)
$c = [System.Security.Cryptography.X509Certificates.X509Certificate2]$ssl.RemoteCertificate
$c | Select-Object Subject, Issuer, NotAfter, Thumbprint
$ssl.Dispose(); $tcp.Dispose()
```

TIPP · Kette und Sperrliste gleich mitprüfen

Exportiere das ausgelieferte Zertifikat als CER und prüfe es auf einem externen Gerät mit certutil -urlfetch -verify gateway.cer. Der Befehl lädt Zwischenzertifikate und Sperrlisten über die im Zertifikat hinterlegten Adressen. Was dort scheitert, scheitert auch beim Remotedesktopclient.

RD Gateway Zertifikat erneuern: Lösung mit Set-RDCertificate



Skizze: Vorgehen beim Erneuern des RD-Gateway-Zertifikats

Neues Zertifikat beschaffen

Ob öffentlich oder intern: Das Zertifikat braucht den Zweck Serverauthentifizierung, einen exportierbaren privaten Schlüssel und den externen Gateway-Namen im SAN. Wenn RD-Webzugriff unter einem anderen Namen erreichbar ist, kommt dieser Name ebenfalls hinein. Den Zertifikatsantrag erzeugst du am einfachsten auf dem Gateway oder dem Connection Broker im

Computerspeicher, damit der private Schlüssel dort entsteht. Nach der Ausstellung schließt du den Antrag auf derselben Maschine ab und exportierst das Zertifikat mit Schlüssel und vollständiger Kette als PFX.

Kriterium	Öffentliche CA	Interne PKI (ADCS)
Vertrauen auf privaten Geräten	von Haus aus vorhanden	nur mit verteiltem Stammzertifikat
Sperrliste von außen	von der CA bereitgestellt	musst du selbst extern veröffentlichen
Laufzeit	kurz und wird kürzer, häufiger Tausch	frei wählbar über die Vorlage
Automatisierung	abhängig vom Anbieter	Registrierung über Vorlagen und Berechtigungen
Typischer Einsatz	Gateway im Internet, gemischte Clients	nur verwaltete Firmengeräte

Für ein Gateway, das aus dem Internet von beliebigen Geräten erreicht wird, ist ein öffentliches Zertifikat die pragmatische Wahl. Die interne PKI passt, wenn ausschließlich verwaltete Geräte zugreifen und du die Sperrlisten von außen erreichbar machst. Wie du eine Unternehmens-PKI sauber aufbaust, mit Vorlagen und Sperrlistenverteilung, steht auf der Seite PKI mit ADCS. Beachte bei öffentlichen Zertifikaten: Die Branchenvorgaben verkürzen die maximale Laufzeit schrittweise, seit März 2026 auf höchstens 200 Tage. Der Tausch wird also vom Jahresereignis zur Routine.

WARNUNG · PFX ohne privaten Schlüssel

Der häufigste Grund, warum Set-RDCertificate scheitert oder das Gateway nach dem Tausch stumm bleibt: Die Datei enthält nur das Zertifikat, nicht den Schlüssel. Eine CER- oder CRT-Datei der CA reicht nicht. Der Schlüssel liegt dort, wo der Antrag erzeugt wurde. Wurde der Antrag auf einer anderen Maschine oder im Webportal des Anbieters erstellt, musst du Zertifikat und Schlüssel dort zusammenführen und als PFX exportieren.

PFX vor dem Setzen prüfen

```
$pw  = Read-Host -AsSecureString -Prompt 'PFX-Kennwort'
$pfx = Get-PfxData -FilePath 'C:\Install\gateway-2027.pfx' -Password $pw
$pfx.EndEntityCertificates | Select-Object Subject, NotAfter, HasPrivateKey, Thumbprint, DnsNameList
$pfx.OtherCertificates     | Select-Object Subject, NotAfter   # Zwischen- und Stammzertifikate
```

HasPrivateKey muss True sein, DnsNameList muss gateway.contoso.com enthalten, und unter OtherCertificates sollte mindestens das Zwischenzertifikat der ausstellenden CA auftauchen. Fehlt es, liefert das Gateway eine unvollständige Kette aus, und Clients ohne passendes Zwischenzertifikat scheitern.

Altes Zertifikat sichern, dann setzen

Bevor du etwas änderst, notierst du den alten Fingerabdruck und exportierst das bisherige Zertifikat, sofern der Schlüssel exportierbar ist. Bei einem bereits abgelaufenen Zertifikat ist das kein Rückweg für den Betrieb, aber eine Absicherung, falls das neue Zertifikat Fehler hat und du die Ursache vergleichen willst. Erneuerst du vorbeugend vor dem Ablauf, ist es dein echter Rückweg.

```
# Sicherung: aktueller Stand
```

```
Get-RDCertificate -Role RDGateway -ConnectionBroker RDCB01.contoso.local |
    Export-Clixml C:\Install\rdcert-vorher.xml

# Variante A: PFX importieren und an alle Gateways der Bereitstellung verteilen
Set-RDCertificate -Role RDGateway -ImportPath 'C:\Install\gateway-2027.pfx' `
    -Password $pw -ConnectionBroker RDCB01.contoso.local -Force

# Variante B (ab Windows Server 2019): bereits installiertes Zertifikat per Fingerabdruck
Set-RDCertificate -Role RDGateway -Thumbprint '<Fingerabdruck>' `
    -ConnectionBroker RDCB01.contoso.local -Force

# Gleicher Name auch für RD-Webzugriff? Dann diese Rolle direkt mitziehen
Set-RDCertificate -Role RDWebAccess -ImportPath 'C:\Install\gateway-2027.pfx' `
    -Password $pw -ConnectionBroker RDCB01.contoso.local -Force
```

Im Server-Manager geht dasselbe über Bereitstellungseigenschaften bearbeiten › Zertifikate › RD-Gateway markieren › Vorhandenes Zertifikat auswählen › Zertifikatpfad und Kennwort angeben › Übernehmen. Bei einer internen PKI bietet der Dialog an, das Zertifikat auf den Zielservern als vertrauenswürdig einzutragen. Die Parameter im Detail beschreibt Set-RDCertificate in der Microsoft-Dokumentation.

WICHTIG · Die Sitzungen fliegen raus

Beim Setzen des Gateway-Zertifikats wird der Gateway-Dienst neu gebunden. Bestehende Verbindungen über das Gateway können dabei getrennt werden. Bei einem abgelaufenen Zertifikat ist das egal, es kommt ohnehin niemand rein. Bei einem vorbeugenden Tausch planst du ein kurzes Wartungsfenster und sagst es vorher an.

Mehrere Gateways hinter dem Load Balancer

Mit zwei oder mehr Gateways gilt: Alle tragen dasselbe Zertifikat mit dem gemeinsamen Namen des Load Balancers, also gateway.contoso.com. Set-RDCertificate verteilt es an alle Gateway-Server der Bereitstellung. Prüfe deshalb vorher mit Get-RDServer -Role RDS-GATEWAY, ob wirklich alle Gateways dort auftauchen, die der Load Balancer bedient. Fehlt eines, nimmst du es mit Add-RDServer -Role RDS-GATEWAY in die Bereitstellung auf oder bindest das Zertifikat dort manuell im RD-Gateway-Manager.

```
Get-RDServer -ConnectionBroker RDCB01.contoso.local -Role RDS-GATEWAY
```

Entscheidend ist, wo TLS endet. Reicht der Load Balancer die Verbindung nur durch, genügt das Zertifikat auf den Gateways. Beendet er TLS selbst und verschlüsselt erneut zum Gateway, liegt das Zertifikat zusätzlich auf dem Load Balancer, und genau dort wird es beim Tausch gern vergessen. Den UDP-Verkehr auf Port 3391 reichen Load Balancer in der Regel nur durch, die Gateways brauchen das Zertifikat also in jedem Fall. Wie das mit einem Kemp LoadMaster sauber aufgesetzt wird, einschließlich Persistenz für die Gateway-Kanäle, steht auf der Seite Kemp LoadMaster.

Aufbau	Wo das Zertifikat liegt	Was beim Erneuern zu tun ist
Ein Gateway, kein Load Balancer	RDGW01	Set-RDCertificate, fertig
Mehrere Gateways, Durchreichen	RDGW01 und RDGW02	Set-RDCertificate, alle Gateways in der Bereitstellung prüfen
Mehrere Gateways, TLS-Offloading	Load Balancer und alle Gateways	Load Balancer und Set-RDCertificate, beide Stellen testen
Gateway ohne	jedes Gateway einzeln	RD-Gateway-Manager › Eigenschaften ›

Bereitstellung		SSL-Zertifikat

Testen und Rollback

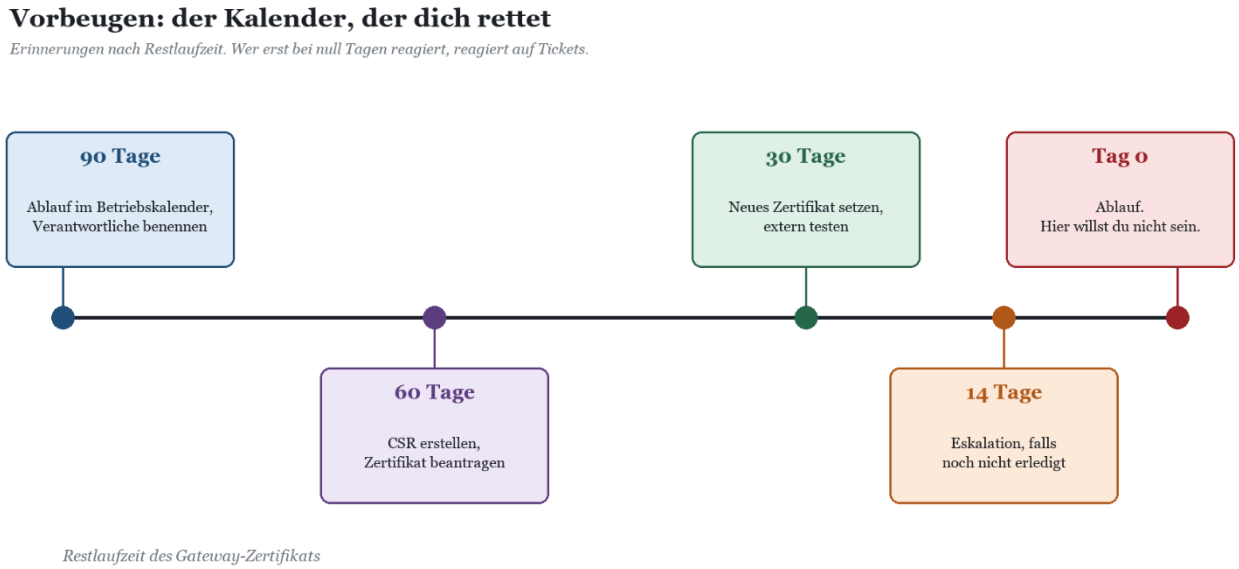
Nach dem Setzen wiederholst du die lesenden Schritte 1, 3 und 5. Get-RDCertificate muss Trusted und das neue Ablaufdatum zeigen, die CIM-Abfrage auf jedem Gateway denselben Hash, und der Test von außen das neue Zertifikat. Danach verbindest du dich mit einem externen Gerät, idealerweise einem privaten ohne Firmen-Stammzertifikate, und ebenso über den Web Client, falls du ihn nutzt. Dazu passt der Beitrag RD Web Client (HTML5) installieren und veröffentlichen.

WARNUNG · Rollback-Hinweis

Läuft mit dem neuen Zertifikat etwas schief, etwa weil der Name im SAN fehlt, spielst du das vorher exportierte, noch gültige Zertifikat mit demselben Befehl zurück: Set-RDCertificate -Role RDGateway -ImportPath mit der alten PFX. Ist das alte schon abgelaufen, gibt es keinen sinnvollen Rückweg, sondern nur ein korrigiertes neues Zertifikat. Lösche das alte Zertifikat erst aus dem Speicher, wenn das neue mindestens einen Arbeitstag ohne Beschwerden gelaufen ist.

Vorbeugung: damit das Gateway-Zertifikat nie wieder überrascht

Ein abgelaufenes Zertifikat ist kein technischer Fehler, sondern ein organisatorischer. Die Technik hat sich exakt an das Datum gehalten, das jemand vor einem Jahr selbst eingetragen hat. Vorbeugung heißt deshalb: Termin sichtbar machen, Verantwortung klären, Ablauf prüfen lassen, bevor er eintritt.



Skizze: Erinnerungsstufen bis zum Zertifikatsablauf, Vorschlag

Prüfpunkt	Wie	Wann
Ablaufdatum aller RDS-Rollen bekannt	Get-RDCertificate, Ergebnis in die Farmdokumentation	nach jedem Tausch
Erinnerung mit Vorlauf	Termin bei 90, 60, 30 und 14 Tagen, mit Vertretung	beim Tausch anlegen
Automatische Prüfung	geplante Aufgabe mit Get-RDCertificate und Mail bei weniger als 30 Tagen	täglich
Alle Gateways in der	Get-RDServer -Role RDS-GATEWAY gegen Load-	vierteljährlich

Bereitstellung	Balancer-Pool	
Zertifikat auf dem Load Balancer	Ablaufdatum der TLS-Konfiguration am Load Balancer	beim Tausch mitprüfen
Kette und Sperrliste von außen	certutil -urlfetch -verify auf externem Gerät	nach jedem Tausch
PFX und Kennwort auffindbar	Ablage im Kennworttresor, nicht im Postfach des Kollegen	beim Tausch
Runbook für den Tausch	die Befehle aus diesem Beitrag mit euren Namen	einmalig, dann pflegen

Für die automatische Prüfung genügt ein kleines Skript als geplante Aufgabe auf dem Connection Broker. Es liest alle Rollen und schreibt bei geringer Restlaufzeit ein Ereignis, das deine Überwachung ohnehin einsammelt.

```
$grenze = (Get-Date).AddDays(30)
Get-RDCertificate -ConnectionBroker RDCB01.contoso.local |
  Where-Object { $_.ExpiresOn -and $_.ExpiresOn -lt $grenze } |
  ForEach-Object {
    Write-EventLog -LogName Application -Source 'RDS-Zertifikatskontrolle' -EventId 4101 -EntryType
Warning `
      -Message ("Rolle {0}: Zertifikat {1} läuft am {2:dd.MM.yyyy} ab." -f $_.Role, $_.Subject,
$_.ExpiresOn)
  }
# Einmalig vorher: New-EventLog -LogName Application -Source 'RDS-Zertifikatskontrolle'
```

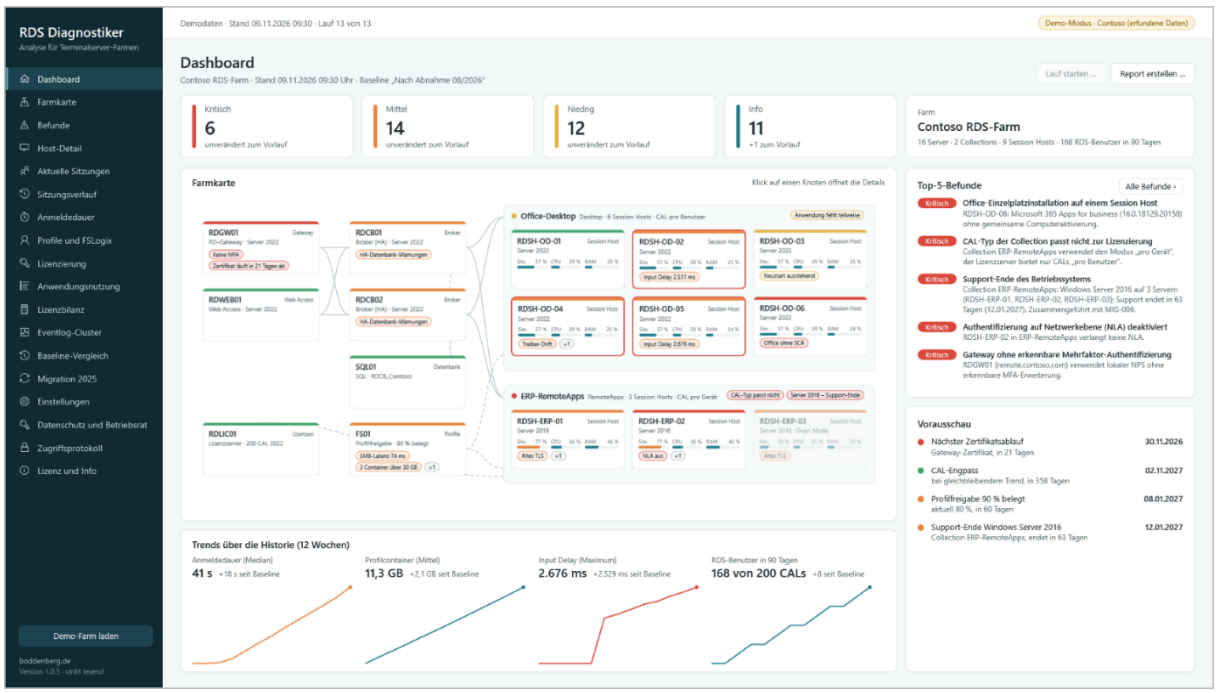
Der Zertifikatstausch gehört außerdem in die regelmäßige Prüfung der ganzen Farm, zusammen mit Lizenzierung, Updates und Konfiguration. Wie so ein Rhythmus aussieht, zeigt RDS Health Check: Farm regelmäßig prüfen statt nur reagieren. Und weil das Gateway die Tür nach draußen ist, lohnt es sich, Zertifikat, Mehrfaktor-Authentifizierung und Ressourcenrichtlinien gemeinsam zu betrachten, siehe RDS-Farm härten: Sicherheits-Checkliste für Terminalserver. Wo der Fingerabdruck, die Ablage der PFX und die Ansprechpartner dokumentiert gehören, beschreibt RDS-Farm dokumentieren: was in eine gute Farmdokumentation gehört.

SO FINDET ES DER RDS DIAGNOSTIKER · Zertifikatsvorausschau

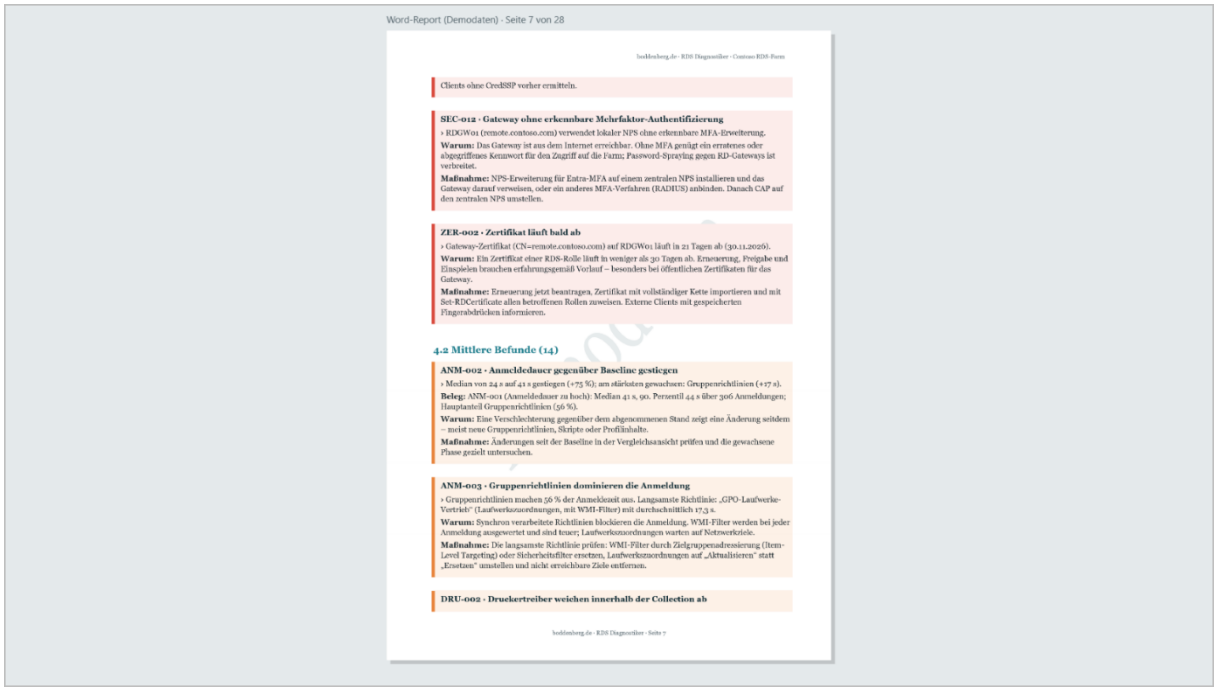
Der RDS Diagnostiker liest die Farm agentlos und strikt lesend über WinRM, CIM und das Remote-Eventlog. Die Zertifikatsvorausschau zeigt die Restlaufzeit der Zertifikate in der Bereitstellung, auch der Gateway-Rolle, bevor sie zum Problem werden. Auf dem Dashboard steht der nächste Ablauf neben CAL-Typ, Support-Ende und Profilfreigabe.

Ein bald ablaufendes Gateway-Zertifikat erscheint als Befund mit Schweregrad, Begründung und Maßnahme, auf Wunsch im Word-Report mit Aktionsplan. Über die Aufgabenplanung laufen die Prüfungen regelmäßig, sodass der Ablauf nicht vom Gedächtnis einzelner Admins abhängt.

Mehr dazu auf der Seite RDS Diagnostiker. Du kannst ihn 15 Tage kostenlos testen.



Im Dashboard siehst du rechts die Vorausschau mit dem nächsten Zertifikatsablauf, Demo-Daten.



Im Bericht steht der Befund zum Gateway-Zertifikat, das in 21 Tagen abläuft, mit Begründung und Maßnahme, Demo-Daten.

Wenn du Gateways neu aufbaust oder ergänzt, prüft der UB Mechaniker für RDS in seiner Vorabprüfung mit Ampel unter anderem DNS, Netz und Zertifikate, bevor ein Skript etwas verändert.

Und wenn du die Zertifikatsstrategie für Gateway, Load Balancer und interne PKI einmal gemeinsam mit jemandem aufräumen willst, der das schon öfter gemacht hat, hilft dir die Beratung zu Remote Desktop Services. Für Teams, die den Tausch künftig selbst routiniert erledigen sollen, gibt es die Schulung Remote Desktop Services.

FAQ: RD Gateway Zertifikat erneuern

Wie erneuere ich das Zertifikat am RD Gateway per PowerShell?

Auf dem Connection Broker mit Set-RDCertificate -Role RDGateway -ImportPath <PFX> -Password <SecureString> -ConnectionBroker RDCB01.contoso.local -Force. Ab Windows Server 2019 geht auch -Thumbprint für ein bereits installiertes Zertifikat. Danach mit Get-RDCertificate kontrollieren.

Warum geht Remotedesktop intern, aber extern nicht mehr?

Interne Clients verbinden meist direkt zum Session Host und umgehen das Gateway. Externe Verbindungen laufen über das Gateway und scheitern, sobald dessen Zertifikat abgelaufen, gesperrt oder nicht vertrauenswürdig ist.

Wo finde ich das Gateway-Zertifikat im Server-Manager?

Unter Remotedesktopdienste › Übersicht › Bereitstellungsübersicht › Aufgaben › Bereitstellungseigenschaften bearbeiten › Zertifikate, Rollendienst RD-Gateway. Ein eigenständiges Gateway ohne Bereitstellung verwaltest du im RD-Gateway-Manager unter Eigenschaften › SSL-Zertifikat.

Set-RDCertificate meldet einen Fehler beim Import, was tun?

Meist fehlt der private Schlüssel in der Datei, das Kennwort stimmt nicht oder der Pfad ist vom Connection Broker aus nicht erreichbar. Prüfe die Datei mit Get-PfxData auf HasPrivateKey und lege sie lokal auf den Connection Broker.

Brauche ich bei zwei RD Gateways zwei Zertifikate?

Nein. Beide Gateways tragen dasselbe Zertifikat mit dem gemeinsamen Namen des Load Balancers. Achte darauf, dass beide Gateways Teil der Bereitstellung sind, sonst verteilt Set-RDCertificate das Zertifikat nicht an beide. Bei TLS-Offloading braucht auch der Load Balancer das Zertifikat.

Reicht ein Zertifikat aus der internen PKI für das RD Gateway?

Für verwaltete Firmengeräte ja, wenn das Stammzertifikat dort verteilt ist und die Sperrliste von außen erreichbar ist. Für private Geräte, Partner oder den Web Client im fremden Browser ist ein öffentliches Zertifikat praktikabler.

Muss ich nach dem Zertifikatstausch die Session Hosts neu starten?

Nein. Das Gateway-Zertifikat betrifft den Terminalserver selbst nicht. Die Session Hosts bleiben unberührt, lediglich Verbindungen über das Gateway können beim Tausch kurz getrennt werden.

Wie bekomme ich rechtzeitig Bescheid, bevor das RDS-Zertifikat abläuft?

Mit einer geplanten Aufgabe, die Get-RDCertificate auswertet und bei weniger als 30 Tagen Restlaufzeit ein Ereignis oder eine Mail erzeugt, plus Kalendererinnerungen mit Vertretung. Das Ablaufdatum gehört außerdem in die Farmdokumentation.

Fazit: dreißig Minuten Arbeit, ein Jahr Ruhe

Ein abgelaufenes RD-Gateway-Zertifikat sieht dramatisch aus, ist aber einer der dankbarsten Fehler in Remotedesktopdiensten: Die Ursache ist eindeutig, die Lösung ein einziger Befehl. Schwierig wird es nur an den Rändern, beim fehlenden privaten Schlüssel, der unvollständigen Kette, dem vergessenen zweiten Gateway und dem Load Balancer, der TLS selbst beendet. Wer diese vier Punkte prüft, Set-RDCertificate sauber einsetzt und das nächste Ablaufdatum mit Vorlauf in den Kalender und in eine automatische Prüfung schreibt, erlebt den nächsten Mittwochmorgen entspannt. Das Zertifikat stirbt trotzdem. Aber diesmal erst, nachdem sein Nachfolger längst im Dienst ist.

WEITERLESEN · Weiter in dieser Serie

› RDS-Zertifikatswarnung beim Verbinden beheben
› Wichtige RDS-Ereignis-IDs und was sie bedeuten
› RDS-Farm härten: Sicherheits-Checkliste für Terminalserver
› RDS Health Check: Farm regelmäßig prüfen statt nur reagieren
› RD Web Client (HTML5) installieren und veröffentlichen
› RDS-Farm dokumentieren: was in eine gute Farmdokumentation gehört