RDS-Zertifikatswarnung beim Verbinden beheben



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

BERATUNG
Zertifikate, PKI und Namen der Farm einmal sauber ordnen lassen.
› Beratung zu Remote Desktop Services

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

Jeden Morgen dasselbe Ritual: Remotedesktop starten, gelben Warndialog wegklicken, arbeiten. Die Belegschaft hat längst gelernt, dass „Trotzdem verbinden“ der eigentliche Anmeldeknopf ist. Genau das macht die RDS-Zertifikatswarnung so unangenehm: Sie ist nicht nur lästig, sie trainiert allen das Wegklicken an, und an dem Tag, an dem wirklich ein falscher Server antwortet, klickt auch jeder brav auf „Ja“. Wenn du nach „RDS Zertifikat Warnung“ suchst, weil auf deinem Terminalserver der Dialog „Die Identität des Remotecomputers kann nicht überprüft werden“ erscheint, bist du hier richtig.

Dieser Beitrag ordnet die Warnungen den Stellen zu, an denen sie entstehen: den vier Rollen-Zertifikaten der Bereitstellung (Broker Publishing, Broker SSO, Web Access, Gateway) und dem Zertifikat, das jeder Session Host selbst für RDP vorzeigt. Du bekommst lesende PowerShell-Befehle für die Diagnose, eine Zuordnung Warnungstext › Ursache › Lösung, die Schritte für den Tausch mit Rückweg und die Verteilung des Stammzertifikats auf die Clients. Wie Connection Broker, Session Hosts, Web Access und Gateway in den Remotedesktopdiensten grundsätzlich zusammenspielen, steht auf der Übersichtsseite Remote Desktop Services.

FAKTEN · Das Wichtigste in Kürze

Eine RDS-Bereitstellung kennt vier Rollen-Zertifikate, die du zentral am Connection Broker mit Set-RDCertificate setzt: RDRedirector (Broker SSO), RDPublishing (Broker Veröffentlichung), RDWebAccess und RDGateway.

Das Zertifikat, das ein Session Host beim Verbinden zeigt, gehört nicht dazu. Es ist ohne weiteres Zutun selbstsigniert und wird per Gruppenrichtlinie, Zertifikatsvorlage oder CIM gesetzt.

Die Warnung entsteht, wenn der Client den Server nicht über Kerberos authentifizieren kann und das Zertifikat dann eine von vier Prüfungen nicht besteht: Kette, Name, Gültigkeit, Sperrstatus.

Der Name im Zertifikat muss zu dem Namen passen, den der Client tatsächlich aufruft. Eine IP-Adresse oder ein Kurzname im Verbindungsdialog reicht für eine Warnung.

Seit dem Sicherheitsupdate vom April 2026 zeigt der Remotedesktopclient beim Öffnen von RDP-Dateien zusätzlich einen Herausgeber-Dialog. Unsignierte Dateien gelten als unbekannte Remoteverbindung.

RDS Zertifikat Warnung: wie sie sich zeigt und was dahintersteckt

Die Warnung hat viele Gesichter, und jedes zeigt auf eine andere Rolle. Anwender sehen nur „irgendwas mit Zertifikat“, Admins sehen meist gar nichts, weil ihre eigenen Verbindungen über Kerberos laufen und still bleiben. Deshalb lohnt sich zuerst ein genauer Blick darauf, wann, wo und bei wem der Dialog kommt. Die folgenden Texte sind sinngemäß wiedergegeben, der genaue Wortlaut hängt von Clientversion und Sprache ab.

Warnungstext (sinngemäß)	Ursache	Lösung
Die Identität des Remotecomputers kann nicht überprüft werden. Das Zertifikat stammt nicht von einer vertrauenswürdigen Zertifizierungsstelle.	Session Host zeigt sein selbstsigniertes Zertifikat, oder das Stammzertifikat der internen PKI fehlt auf dem Client.	Zertifikat aus der PKI per GPO-Vorlage auf die Session Hosts, Stammzertifikat auf die Clients verteilen.
Der Name im Zertifikat des Remotecomputers ist ungültig bzw. stimmt nicht überein.	Aufgerufen wird ein Name, der nicht im SAN steht: IP-Adresse, Kurzname, DNS-Alias.	Mit dem FQDN verbinden oder den genutzten Namen in den SAN aufnehmen.
Das Zertifikat ist abgelaufen oder noch nicht gültig.	NotAfter überschritten, oft bei manuell gesetzten Zertifikaten ohne automatische Erneuerung.	Neues Zertifikat setzen, künftig Autoregistrierung nutzen.
Fehler bei der Sperrüberprüfung des Zertifikats.	Sperrliste oder OCSP der ausstellenden CA ist vom Client nicht erreichbar.	CDP und AIA erreichbar veröffentlichen, besonders für externe Clients.
Vorsicht: Unbekannte Remoteverbindung, Herausgeber unbekannt.	RDP-Datei ist nicht signiert, etwa selbst gebaut oder aus alter Quelle.	Dateien über RD Web beziehen oder mit rdpsign signieren.
Herausgeber dieser Remoteverbindung überprüfen, mit Name des Herausgebers.	Datei ist signiert, aber das Zertifikat der Rolle RDPublishing ist nicht als vertrauenswürdiger Herausgeber hinterlegt.	Fingerabdruck per GPO als vertrauenswürdigen RDP-Herausgeber eintragen.
Browserwarnung beim Aufruf von /RDWeb oder des Web Clients.	Rolle RDWebAccess hat ein selbstsigniertes Zertifikat oder einen anderen Namen.	Set-RDCertificate -Role RDWebAccess mit passendem Namen.
Zertifikat des Remotedesktopgateways abgelaufen, gesperrt oder Name falsch.	Rolle RDGateway, betrifft fast nur externe Verbindungen.	Set-RDCertificate -Role RDGateway, siehe eigener Beitrag zum Gateway.
Keine Warnung, aber doppelte Kennwortabfrage beim Verbinden.	SSO am Broker greift nicht, Rolle RDRedirector oder Name passt nicht.	Gleiches Zertifikat für RDRedirector und RDPublishing mit Broker-Namen.

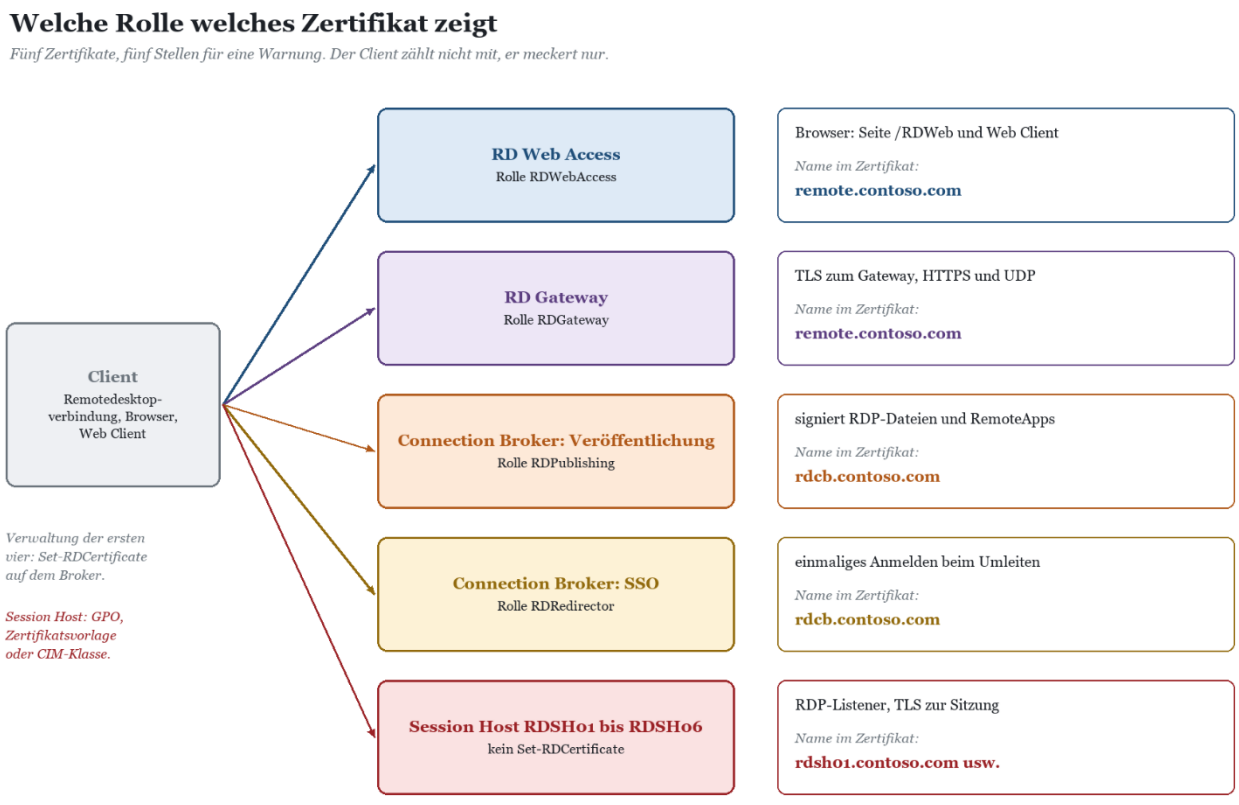
Gateway-Probleme haben ihre eigene Dramaturgie, weil sie meist alle externen Benutzer gleichzeitig treffen. Die Schritte dafür stehen im Beitrag RD Gateway Zertifikat abgelaufen: schnell erneuern, künftig vorbeugen. Hier geht es vor allem um die Warnungen beim Verbinden zum Connection Broker und zum Session Host.

AUS DER PRAXIS · Ein Klinikverbund mit drei Standorten

In einem Klinikverbund mit Standorten in Frankfurt, Köln und Hamburg kam die Warnung nur in Köln. Gleiche Clients, gleiche Farm, gleiche Benutzer. Des Rätsels Lösung: In Köln hatte jemand vor Jahren eine Desktopverknüpfung mit der IP-Adresse des Brokers verteilt, weil „DNS damals gesponnen hat“. Mit IP-Adresse gibt es kein Kerberos, also prüft der Client das Zertifikat, und das kannte nur rdcb.contoso.com. Das Zertifikat war unschuldig. Die Verknüpfung hatte acht Jahre überlebt, länger als drei IT-Leiter.

Technischer Hintergrund: welche Rolle welches Zertifikat zeigt

Eine RDS-Bereitstellung besteht aus mehreren Rollen, und jede, die per TLS spricht oder etwas signiert, braucht ein Zertifikat. Vier davon verwaltet der Connection Broker gemeinsam. Das fünfte, das des Session Hosts, lebt sein eigenes Leben auf jedem einzelnen Terminalserver.



Skizze: Zertifikate der Rollen in einer RDS-Bereitstellung, Contoso-Beispiel mit Split-DNS

Die vier Rollen-Zertifikate der Bereitstellung

Rolle in Get-RDCertificate	Server-Manager-Bezeichnung	Wofür	Name im Zertifikat
RDRedirector	RD-Verbindungsbroker – einmaliges Anmelden aktivieren	Weitergabe der Anmeldung beim Umleiten zum Session Host	FQDN des Brokers, bei HA der DNS-Name des Clusters
RDPublishing	RD-Verbindungsbroker –	Signatur der RDP-Dateien	FQDN des Brokers, bei

	Veröffentlichung aktivieren	und RemoteApps	HA der DNS-Name des Clusters
RDWebAccess	RD-Webzugriff	HTTPS für /RDWeb, Feed und Web Client	Name, den Benutzer im Browser aufrufen
RDGateway	RD-Gateway	TLS zum Gateway, HTTPS und UDP	externer Gateway-Name

Microsoft beschreibt für diese Zertifikate klare Anforderungen: Zweck Serverauthentifizierung (OID 1.3.6.1.5.5.7.3.1), ein exportierbarer privater Schlüssel, ausgestellt von einer Zertifizierungsstelle, der Server und Clients vertrauen. Mit einer Unternehmens-PKI eignet sich eine Kopie der Vorlage Webserver. Details stehen in Zertifikate in Remotedesktopdiensten in der Microsoft-Dokumentation. In der Praxis funktioniert ein gemeinsames Zertifikat mit allen Namen im SAN gut: rdcb.contoso.com für die beiden Broker-Rollen, remote.contoso.com für Web Access und Gateway. Ob du lieber getrennte Zertifikate pflegst, ist Geschmackssache, solange jeder Name dort steht, wo er gebraucht wird.

FAKTEN · Stufen in Get-RDCertificate

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

Untrusted: selbstsigniertes Zertifikat, wie es der Assistent beim Einrichten der Bereitstellung erzeugen kann. Für Clients bedeutet das fast immer eine Warnung.

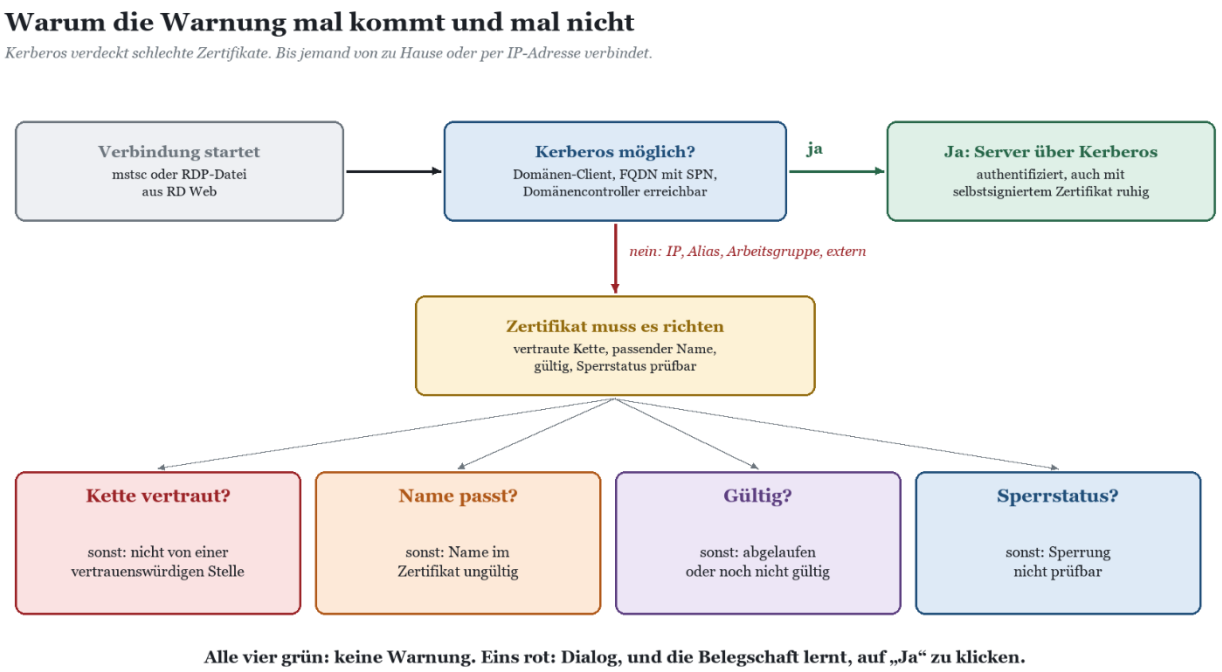
Not Configured: kein Zertifikat hinterlegt oder nicht gültig, zum Beispiel abgelaufen.

Das Session-Host-Zertifikat für RDP

Jeder Session Host erzeugt beim ersten Start des Remotedesktopdienstes ein selbstsigniertes Zertifikat und legt es im Computerspeicher unter Remotedesktop ab. Dieses Zertifikat zeigt er jedem Client beim TLS-Aufbau. Set-RDCertificate fasst es nicht an. Welches Zertifikat der RDP-Listener verwendet, steht als SHA1-Fingerabdruck in der CIM-Klasse Win32_TSGeneralSetting im Namespace root/cimv2/TerminalServices. Setzen lässt es sich auf zwei Wegen: dauerhaft über die Gruppenrichtlinie „Vorlage für Serverauthentifizierungszertifikat“, die per Autoregistrierung ein Zertifikat aus deiner PKI holt und erneuert, oder einmalig über das Setzen des Fingerabdrucks per CIM.

Warum Kerberos die Warnung verdeckt

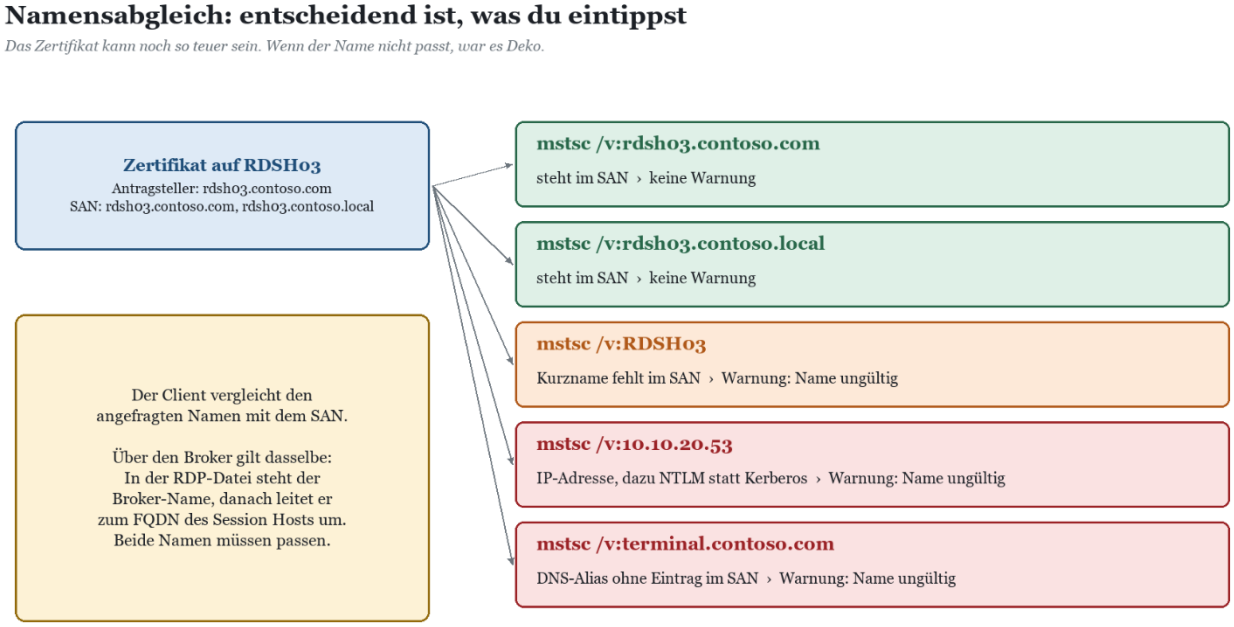
Der Remotedesktopclient will wissen, ob er mit dem richtigen Server spricht. Gelingt die Anmeldung über Kerberos, ist der Server bereits über seinen Dienstprinzipalnamen authentifiziert, und ein selbstsigniertes Zertifikat fällt nicht auf. Deshalb sieht ein domänengebundener Client im Büro, der per FQDN verbindet, oft nie eine Warnung. Sobald Kerberos ausfällt, etwa bei Aufruf per IP-Adresse oder Alias ohne passenden SPN, bei Geräten außerhalb der Domäne oder ohne Sicht auf einen Domänencontroller, muss das Zertifikat allein die Identität beweisen. Dann kommt die Warnung. Mehr zum Zusammenspiel von Dienstprinzipalnamen und Tickets steht auf der Seite Microsoft Kerberos.



Skizze: Serverauthentifizierung beim RDP-Verbindungsaufbau, vereinfacht

Namensabgleich mit dem tatsächlich aufgerufenen FQDN

Der Client prüft nicht, ob das Zertifikat zum Server passt, sondern ob es zu dem Namen passt, den er selbst aufgerufen hat. Verbindet ein Benutzer über RD Web, enthält die RDP-Datei den Namen des Connection Brokers. Der Broker leitet dann auf den Session Host um, und der Client prüft dessen Zertifikat gegen den FQDN des Session Hosts. Bei einem hochverfügbaren Broker ist es der gemeinsame DNS-Name, den du beim Einrichten der Hochverfügbarkeit festlegst, Details im Beitrag RDS Connection Broker hochverfügbar machen.



Skizze: Abgleich zwischen aufgerufenem Namen und Zertifikat, Contoso-Beispiel

WICHTIG · .local und öffentliche Zertifikate

Öffentliche Zertifizierungsstellen stellen keine Zertifikate für interne Namen wie rdcb.contoso.local

aus. Wenn deine Farm intern unter .local läuft und du ein öffentliches Zertifikat willst, brauchst du Split-DNS, also interne Einträge unter contoso.com, oder du nimmst für die internen Namen deine eigene PKI. Beides funktioniert. Ein öffentliches Zertifikat für remote.contoso.com auf einem Broker, den alle als rdcb.contoso.local aufrufen, funktioniert nicht.

Neu seit April 2026: der Herausgeber-Dialog

Seit dem Sicherheitsupdate vom April 2026 zeigt die Remotedesktopverbindung beim Öffnen jeder RDP-Datei einen Sicherheitsdialog, bevor sie verbindet. Bei unsignierten Dateien steht dort ein Warnbanner zur unbekannten Remoteverbindung und „Unbekannter Herausgeber“, bei signierten Dateien der Hinweis, den Herausgeber zu überprüfen, samt Namen. Umleitungen wie Laufwerke, Zwischenablage oder Drucker sind in diesem Dialog zunächst abgewählt. Für Dateien, deren Signaturzertifikat per Gruppenrichtlinie als vertrauenswürdiger Herausgeber hinterlegt ist, entfällt die Warnung, und die angeforderten Umleitungen werden übernommen. Mit dem Update vom Juli 2026 akzeptiert diese Richtlinie auch SHA-256-Fingerabdrücke, SHA-1 gilt als Auslaufmodell. Verbindungen, die du direkt im Client eintippst, betrifft der Dialog nicht. Hintergründe beschreibt Microsoft in der Erläuterung der neuen Sicherheitswarnungen bei Microsoft.

WARNUNG · Kein Grund zum Abschalten

Microsoft nennt einen Registrierungswert, mit dem sich der alte Dialog vorübergehend zurückholen lässt, und kündigt zugleich an, dass er in einem künftigen Update entfallen kann. Das ist eine Krücke, keine Lösung. Der Dialog schützt gegen präparierte RDP-Dateien aus Phishing-Mails. Wer ihn abschaltet, statt zu signieren, entfernt den Rauchmelder, weil er beim Kochen piept.

Diagnose Schritt für Schritt: erst lesen, dann tauschen

Alle Befehle in diesem Abschnitt ändern nichts. Du führst sie auf dem Connection Broker RDCB01 oder einer Verwaltungsstation mit den RSAT-Werkzeugen für Remotedesktopdienste und Gruppenrichtlinienverwaltung aus.

Schritt 1: Rollen-Zertifikate der Bereitstellung auslesen

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

Achte auf drei Dinge: Steht irgendwo Untrusted, ist das Zertifikat selbstsigniert. Enthält SubjectAlternateName bei RDRedirector und RDPublishing den Namen, den deine RDP-Dateien als Broker verwenden? Und hängt ExpiresOn bedenklich nah am heutigen Datum? Im Server-Manager findest du dieselben Angaben unter Remotedesktopdienste › Übersicht › Bereitstellungsübersicht › Aufgaben › Bereitstellungseigenschaften bearbeiten › Zertifikate.

Schritt 2: welchen Broker-Namen die Clients aufrufen

Lade eine RDP-Datei aus RD Web herunter oder nimm die aus dem Feed und öffne sie im Editor. Die Zeilen full address und gatewayhostname zeigen, welche Namen der Client aufruft. Genau diese Namen müssen in den Zertifikaten stehen. Prüfe außerdem, welche Server zur Bereitstellung gehören:

```
Get-RDServer -ConnectionBroker RDCB01.contoso.local | Format-Table Server, Roles
Get-RDConnectionBrokerHighAvailability -ConnectionBroker RDCB01.contoso.local   # nur bei HA
```

Schritt 3: Session-Host-Zertifikate per CIM vergleichen

Jetzt zu den Terminalservern selbst. Die folgende Abfrage zeigt je Session Host den Fingerabdruck des Listener-Zertifikats und das passende Zertifikat aus dem Speicher mit Aussteller, Namen und Ablaufdatum. Ein Host, der aus der Reihe tanzt, fällt sofort auf.

```
$rdsh = 1..6 | ForEach-Object { 'RDSH{0:D2}.contoso.local' -f $_ }
Invoke-Command -ComputerName $rdsh -ScriptBlock {
    $ts = Get-CimInstance -Namespace root/cimv2/TerminalServices -ClassName Win32_TSGeneralSetting `
          -Filter "TerminalName='RDP-Tcp'"
    $c  = Get-ChildItem Cert:\LocalMachine\My, 'Cert:\LocalMachine\Remote Desktop' |
          Where-Object Thumbprint -eq $ts.SSLCertificateSHA1Hash | Select-Object -First 1
    [pscustomobject]@{
        Hash       = $ts.SSLCertificateSHA1Hash
        Speicher   = $c.PSParentPath -replace '.*::',''
        Aussteller = $c.Issuer
        Namen      = ($c.DnsNameList.Unicode -join ', ')
        Ablauf     = $c.NotAfter
        Selbst     = ($c.Subject -eq $c.Issuer)
    }
} | Format-Table PSComputerName, Selbst, Namen, Aussteller, Ablauf -AutoSize
```

Selbst = True bedeutet selbstsigniert. Liegt das Zertifikat im Speicher Remote Desktop, hat der Host es sich selbst gebaut. Unterscheiden sich die Hosts einer Sammlung, ist das ein klassischer Fall von Konfigurationsdrift: Ein nachträglich hinzugefügter Host hat die Gruppenrichtlinie nie bekommen, weil er in der falschen Organisationseinheit liegt. Wie du solche Unterschiede systematisch findest, beschreibt Session Hosts verhalten sich unterschiedlich: Konfigurationsdrift erkennen.

Schritt 4: Gruppenrichtlinie für die Zertifikatsvorlage prüfen

In der Gruppenrichtlinienverwaltung liegt die Einstellung unter Computerkonfiguration › Richtlinien › Administrative Vorlagen › Windows-Komponenten › Remotedesktopdienste › Remotedesktop-Sitzungshost › Sicherheit › Vorlage für Serverauthentifizierungszertifikat. Ob sie auf einem Host ankommt, zeigen der Richtlinienergebnissatz und der Registrierungswert, den die Richtlinie schreibt:

```
Import-Module GroupPolicy
Get-GPResultantSetOfPolicy -Computer RDSH03.contoso.local -ReportType Html -Path C:\Temp\rsop-
rdsh03.html

Invoke-Command -ComputerName $rdsh -ScriptBlock {
    Get-ItemProperty 'HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services' `
        -Name CertTemplateName -ErrorAction SilentlyContinue | Select-Object CertTemplateName
} | Format-Table PSComputerName, CertTemplateName
```

Für Get-GPResultantSetOfPolicy muss sich der Computer bereits mit dem aktuellen Stand der Richtlinien gemeldet haben. Zur Suche, in welchem GPO die Einstellung steckt, hilft Get-GPOReport -All -ReportType Xml mit einer Textsuche nach dem Vorlagennamen. Wie du Richtlinien für Terminalserver insgesamt sauber organisierst, steht in Gruppenrichtlinien für Terminalserver: Best Practice mit Loopback.

Schritt 5: Ereignisprotokolle lesen

Wenn die Autoregistrierung scheitert oder der Remotedesktopdienst das Zertifikat nicht laden kann, steht das im Protokoll. Interessant sind der Admin-Kanal des RemoteConnectionManager und die Meldungen der Autoregistrierung im Anwendungsprotokoll.

```
Get-WinEvent -ComputerName RDSH03.contoso.local -FilterHashtable @{
    LogName = 'Microsoft-Windows-TerminalServices-RemoteConnectionManager/Admin'
    Level   = 2,3; StartTime = (Get-Date).AddDays(-7) } -ErrorAction SilentlyContinue |
```

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

Get-WinEvent -ComputerName RDSH03.contoso.local -FilterHashtable @{
    LogName = 'Application'; ProviderName = 'Microsoft-Windows-CertificateServicesClient-
AutoEnrollment'
    StartTime = (Get-Date).AddDays(-7) } -ErrorAction SilentlyContinue |
    Select-Object TimeCreated, Id, LevelDisplayName, Message | Format-Table -Wrap
```

Welche Ereignis-IDs im RDS-Umfeld sonst noch wichtig sind, sammelt Wichtige RDS-Ereignis-IDs und was sie bedeuten.

Schritt 6: auf dem Client nachsehen

Klick im Warndialog auf „Zertifikat anzeigen“ und lies drei Felder ab: Ausgestellt für, Ausgestellt von und den Zertifizierungspfad. Vergleiche den Namen mit dem, was in der Adresszeile des Clients steht. Auf dem Client prüfst du außerdem, ob das Stammzertifikat da ist:

```
Get-ChildItem Cert:\LocalMachine\Root | Where-Object Subject -like '*CONTOSO-ROOT-CA*' |
    Select-Object Subject, NotAfter, Thumbprint

# Kette und Sperrliste eines exportierten Zertifikats prüfen
certutil -urlfetch -verify C:\Temp\rdsh03.cer
```

TIPP · Gegenprobe mit Absicht

Verbinde einmal bewusst per IP-Adresse und einmal per FQDN vom selben Client. Kommt die Warnung nur bei der IP-Adresse, ist das Zertifikat wahrscheinlich in Ordnung und das Problem ist der Name. Kommt sie auch beim FQDN von einem Gerät außerhalb der Domäne, ist das Zertifikat selbst nicht vertrauenswürdig.

Lösung: Zertifikate richtig setzen, mit Rückweg

Die Reihenfolge ist einfach: zuerst sichern, dann die Rollen-Zertifikate der Bereitstellung, dann die Session Hosts, dann die Clients. So beseitigst du die Warnung an der Wurzel, statt sie nur auf einen anderen Server zu verschieben.

Vorher sichern

```
Get-RDCertificate -ConnectionBroker RDCB01.contoso.local | Export-Clixml C:\Install\rdcert-
vorher.xml
Invoke-Command -ComputerName $rdsh -ScriptBlock {
    (Get-CimInstance -Namespace root/cimv2/TerminalServices -ClassName Win32_TSGeneralSetting `
        -Filter "TerminalName='RDP-Tcp'").SSLCertificateSHA1Hash
} | Export-Clixml C:\Install\rdsh-hash-vorher.xml
```

Rollen-Zertifikate mit Set-RDCertificate setzen

Besorge ein Zertifikat mit Zweck Serverauthentifizierung, privatem Schlüssel und allen benötigten Namen im SAN und exportiere es samt Kette als PFX. Dann setzt du es nacheinander für die Rollen. Das Kennwort liest du sicher ein:

```
$pw  = Read-Host -AsSecureString -Prompt 'PFX-Kennwort'
$pfx = 'C:\Install\rds-contoso-2027.pfx'
Get-PfxData -FilePath $pfx -Password $pw | Select-Object -ExpandProperty EndEntityCertificates |
    Select-Object Subject, DnsNameList, HasPrivateKey, NotAfter     # erst prüfen

foreach ($r in 'RDRedirector','RDPublishing','RDWebAccess','RDGateway') {
    Set-RDCertificate -Role $r -ImportPath $pfx -Password $pw `
        -ConnectionBroker RDCB01.contoso.local -Force
```

```
}

# ab Windows Server 2019 alternativ: bereits installiertes Zertifikat per Fingerabdruck
# Set-RDCertificate -Role RDPublishing -Thumbprint '<Fingerabdruck>' -ConnectionBroker
RDCB01.contoso.local -Force
```

Im Server-Manager geht dasselbe unter Bereitstellungseigenschaften bearbeiten › Zertifikate › Rolle markieren › Vorhandenes Zertifikat auswählen › Übernehmen. Dort fällt dir auch auf, dass RDRedirector und RDPublishing in der Oberfläche als „RD-Verbindungsbroker – einmaliges Anmelden aktivieren“ und „RD-Verbindungsbroker – Veröffentlichung aktivieren“ erscheinen. Gib beiden dasselbe Zertifikat mit dem Broker-Namen. Wenn du gerade den Web Client einführst, gehört das Web-Access-Zertifikat dort ohnehin dazu, siehe RD Web Client (HTML5) installieren und veröffentlichen.

WICHTIG · Gateway-Sitzungen beim Tausch

Beim Setzen des Gateway-Zertifikats wird der Gateway-Dienst neu gebunden, bestehende Verbindungen über das Gateway können dabei abbrechen. Plane für die Rolle RDGateway ein kurzes Wartungsfenster ein und kündige es an. Die anderen Rollen sind in der Regel weniger empfindlich, ein ruhiger Zeitpunkt schadet trotzdem nicht.

Session Hosts: Zertifikat per Gruppenrichtlinie und Vorlage

Der dauerhafte Weg führt über deine Unternehmens-PKI. Lege dort eine Zertifikatsvorlage an, zum Beispiel als Kopie von Computer oder Arbeitsstationsauthentifizierung, mit dem Zweck Serverauthentifizierung, dem DNS-Namen des Computers im SAN und Registrieren- sowie Autoregistrieren-Berechtigung für eine Gruppe mit allen Session Hosts. Veröffentliche die Vorlage auf der CA. Wie du Vorlagen und Sperrlistenverteilung sauber aufsetzt, steht auf der Seite PKI mit ADCS.

- **Gruppenrichtlinienverwaltung:** neues GPO, zum Beispiel „RDSH Zertifikat“, an die Organisationseinheit der Session Hosts verknüpfen.
- **Einstellung:** Computerkonfiguration › Richtlinien › Administrative Vorlagen › Windows-Komponenten › Remotedesktopdienste › Remotedesktop-Sitzungshost › Sicherheit › Vorlage für Serverauthentifizierungszertifikat, aktivieren und den Vorlagennamen eintragen.
- **Optional, gleiche Stelle:** „Bestimmte Sicherheitsebene für Remoteverbindungen (RDP) erfordern“ auf SSL setzen, damit niemand auf die alte RDP-Sicherheitsebene ausweicht.
- **Anwenden:** gpupdate /force auf einem Testhost, danach Schritt 3 der Diagnose wiederholen.

```
Invoke-Command -ComputerName RDSH03.contoso.local -ScriptBlock { gpupdate /target:computer /force }
# danach die CIM-Abfrage aus Schritt 3: Selbst muss False sein, Aussteller die Contoso-CA
```

Session Hosts: Fingerabdruck einmalig per CIM setzen

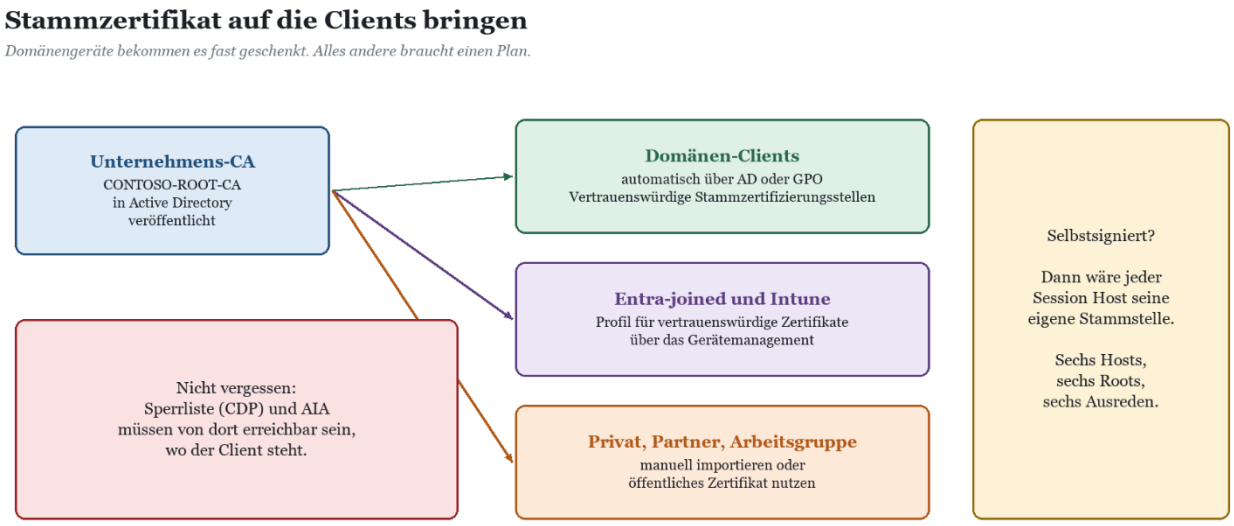
Ohne Autoregistrierung, etwa mit einem gekauften Zertifikat, importierst du das PFX in den Computerspeicher Eigene Zertifikate des Session Hosts und bindest den Fingerabdruck direkt. Das Konto NETZWERKDIENST braucht Leserecht auf den privaten Schlüssel, sonst kann der Remotedesktopdienst ihn nicht verwenden. Diesen Weg musst du bei jeder Erneuerung wiederholen, deshalb ist er die Ausnahme.

```
$thumb = '<Fingerabdruck des neuen Zertifikats>'
Invoke-Command -ComputerName RDSH03.contoso.local -ArgumentList $thumb -ScriptBlock {
    param($t)
    $ts = Get-CimInstance -Namespace root/cimv2/TerminalServices -ClassName Win32_TSGeneralSetting `
```

```
          -Filter "TerminalName='RDP-Tcp'"
    Set-CimInstance -InputObject $ts -Property @{ SSLCertificateSHA1Hash = $t }
}
```

Root auf die Clients verteilen

Ein Zertifikat aus der eigenen PKI hilft nur, wenn die Clients der Stammzertifizierungsstelle vertrauen. Eine Unternehmens-CA, die in Active Directory veröffentlicht ist, landet auf Domänenmitgliedern automatisch im Vertrauensspeicher. Für eine eigenständige Stamm-CA oder zur Sicherheit verteilst du sie per GPO unter Computerkonfiguration › Richtlinien › Windows-Einstellungen › Sicherheitseinstellungen › Richtlinien für öffentliche Schlüssel › Vertrauenswürdige Stammzertifizierungsstellen › Importieren. Entra-joined Geräte bekommen das Stammzertifikat über ein Zertifikatsprofil aus dem Gerätemanagement. Für private Geräte und Partner ist ein öffentliches Zertifikat für Web Access und Gateway meist die entspanntere Wahl.



Skizze: Verteilwege für das Stammzertifikat einer internen PKI, Contoso-Beispiel

RDP-Dateien als vertrauenswürdig kennzeichnen

Für den Herausgeber-Dialog trägst du den Fingerabdruck des RDPublishing-Zertifikats ein, unter Computerkonfiguration › Richtlinien › Administrative Vorlagen › Windows-Komponenten › Remotedesktopdienste › Remotedesktopverbindungs-Client › Fingerabdrücke von Zertifikaten angeben, die vertrauenswürdige RDP-Herausgeber darstellen. Ältere Vorlagen nennen sie noch SHA1-Fingerabdrücke. Nutze nach Möglichkeit den SHA-256-Fingerabdruck. Den bekommst du so:

```
$c = Get-RDCertificate -Role RDPublishing -ConnectionBroker RDCB01.contoso.local
$x = Get-ChildItem Cert:\LocalMachine\My\$($c.Thumbprint)    # auf RDCB01 ausführen
[System.BitConverter]::ToString(
    [System.Security.Cryptography.SHA256]::Create().ComputeHash($x.RawData)).Replace('-','')
```

Selbst gebaute RDP-Dateien, etwa für eine Verknüpfung auf dem Desktop, signierst du mit rdpsign und demselben Zertifikat. Mit Entra-joined Clients und SSO kommt noch die Anmeldung dazu, das ist ein eigenes Thema: Single Sign-on auf RDS für Entra-joined Clients einrichten.

Testen und Rollback

Nach jedem Schritt wiederholst du die lesenden Befehle: Get-RDCertificate muss überall Trusted zeigen, die CIM-Abfrage auf jedem Session Host ein Zertifikat der Contoso-CA. Dann verbindest du von einem Domänen-Client per FQDN, von einem Client außerhalb der Domäne und einmal über RD Web und Web Client.

WARNUNG · Rollback-Hinweis

Rollen-Zertifikate: Die alte PFX mit Set-RDCertificate für dieselbe Rolle zurückspielen. War die Rolle vorher selbstsigniert, kannst du mit New-RDCertificate wieder ein selbstsigniertes erzeugen, nur ist das kein Fortschritt, sondern der alte Zustand.

Session Host per CIM: Den gesicherten Fingerabdruck aus rdsh-hash-vorher.xml mit Set-CimInstance zurückschreiben. Lösche das alte Zertifikat nicht vorschnell aus dem Speicher.

Session Host per GPO: Verknüpfung des GPO aufheben, gpupdate ausführen und den Fingerabdruck wie oben zurücksetzen. Teste den Rückweg einmal auf einem Host, bevor du ihn im Ernstfall brauchst.

Root-Verteilung und Herausgeber-GPO: Einstellung entfernen, beim nächsten Richtlinienabgleich ist der alte Zustand wieder da.

Vorbeugung: damit die Warnung nicht zurückkommt

Zertifikatswarnungen kommen selten aus dem Nichts. Sie kehren zurück, wenn ein neuer Session Host ohne GPO in die Farm kommt, ein Zertifikat abläuft oder jemand eine Verknüpfung mit IP-Adresse verteilt. Gegen alle drei gibt es Routinen.

Prüfpunkt	Wie	Wann
Rollen-Zertifikate	Get-RDCertificate: Stufe, Namen, Ablaufdatum	monatlich und nach jedem Tausch
Session-Host-Zertifikate	CIM-Abfrage aus Schritt 3 über alle Hosts	monatlich
Neue Session Hosts	OU und GPO vor der Aufnahme in die Sammlung prüfen	bei jedem neuen Host
Verknüpfungen und RDP-Dateien	nur FQDN, nur signierte Dateien aus RD Web	bei Änderungen am Client
Stammzertifikat auf Clients	Vertrauensspeicher stichprobenartig, auch Entra-joined	vierteljährlich
Sperrliste und AIA	certutil -urlfetch -verify intern und extern	nach PKI-Änderungen
Ablauftermine	Kalender mit Vorlauf und Vertretung, Werte in der Farmdokumentation	beim Tausch

Wer einen neuen Terminalserver aufnimmt, sollte die Zertifikatsprüfung in die Checkliste schreiben, siehe Session Host zur bestehenden RDS-Farm hinzufügen, ohne Überraschungen. Den regelmäßigen Blick auf Zertifikate, Lizenzen und Konfiguration bündelt RDS Health Check: Farm regelmäßig prüfen statt nur reagieren. Und weil ein wegtrainierter Warndialog ein Sicherheitsproblem ist, gehören signierte RDP-Dateien und eine erzwungene TLS-Sicherheitsebene auch in RDS-Farm härten: Sicherheits-Checkliste für Terminalserver.

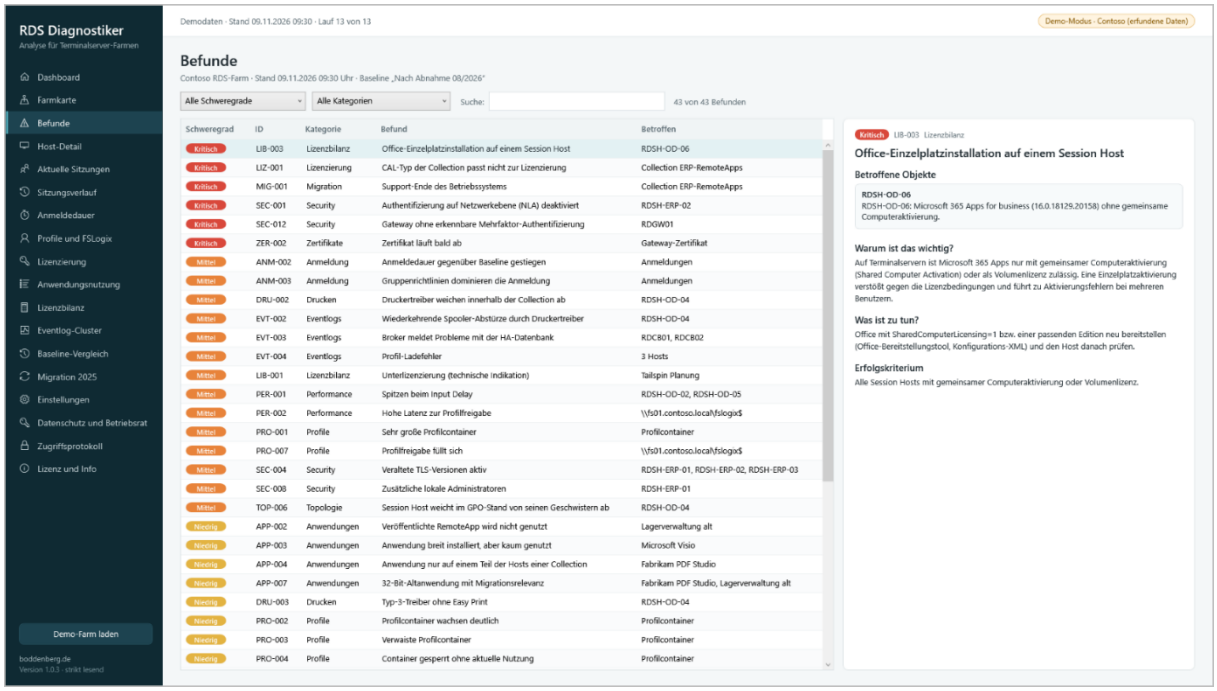
SO FINDET ES DER RDS DIAGNOSTIKER · Prüfbereich Zertifikate

Der RDS Diagnostiker erfasst die Farm agentlos und strikt lesend über WinRM, CIM und das

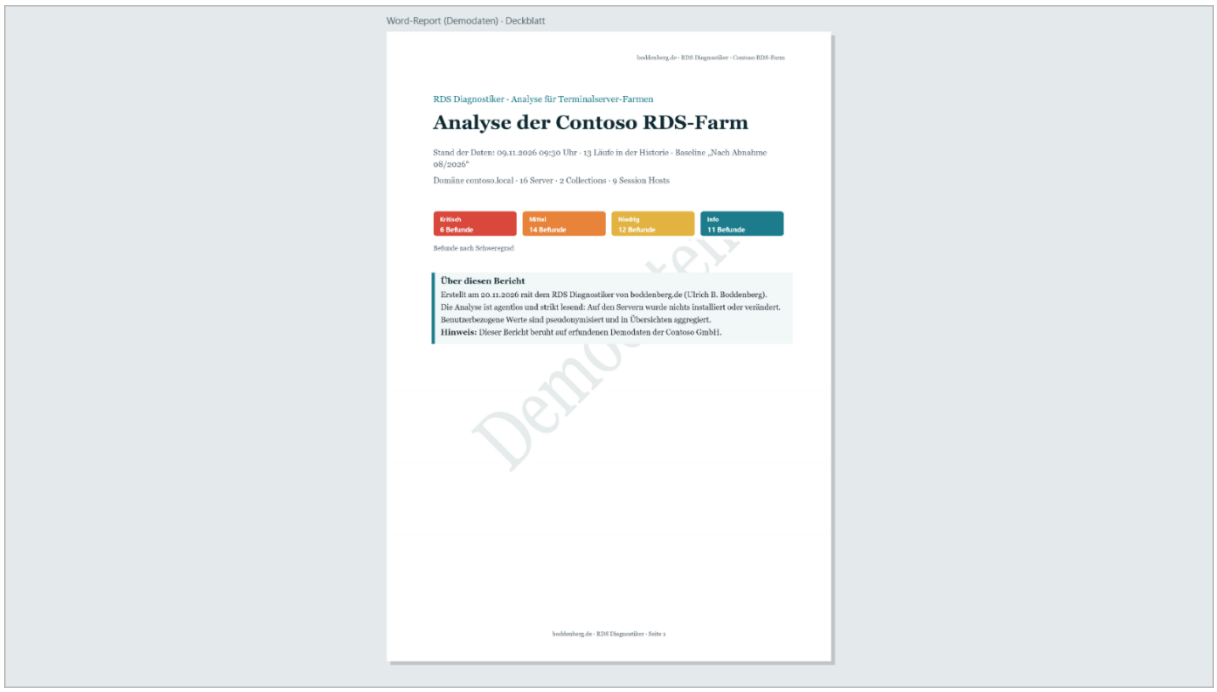
Remote-Eventlog. Zu seinen über 80 Prüfregeln in zwölf Prüfbereichen gehört der Prüfbereich Zertifikate. Auffälligkeiten erscheinen dort als Befund mit Schweregrad, Begründung und Maßnahme.

Die Zertifikatsvorausschau zeigt, welche Zertifikate in der Farm demnächst ablaufen. Unter den Host-Abweichungen innerhalb einer Sammlung fällt ein Session Host auf, der anders konfiguriert ist als seine Nachbarn. Die Befunde lassen sich als Word-Report mit Aktionsplan ausgeben, und über die Aufgabenplanung läuft die Prüfung regelmäßig.

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



So siehst du in der Befunde-Ansicht, welche Punkte kritisch sind und welche Maßnahme vorgeschlagen wird, Demo-Daten.



So sieht das Deckblatt des Word-Reports aus, mit Umfang der Farm und Befunden nach Schweregrad, Demo-Daten.

Wenn du Session Hosts neu aufbaust, prüft der UB Mechaniker für RDS in seiner Vorabprüfung mit Ampel unter anderem DNS, Domäne und Zertifikate, bevor ein Skript etwas verändert.

Wenn du PKI, Split-DNS und die Zertifikate der Farm einmal gemeinsam mit jemandem ordnen willst, der das schon öfter gemacht hat, hilft dir die Beratung zu Remote Desktop Services. Für Teams, die das künftig selbst routiniert erledigen sollen, gibt es die Schulung Remote Desktop Services.

FAQ zur RDS-Zertifikatswarnung

Warum kommt beim Terminalserver die Meldung „Die Identität des Remotecomputers kann nicht überprüft werden“?

Weil der Client den Server nicht über Kerberos authentifizieren konnte und das Zertifikat des Session Hosts die Prüfung nicht besteht. Meist ist es selbstsigniert, oder der aufgerufene Name steht nicht im Zertifikat.

Wie werde ich die RDP-Zertifikatswarnung dauerhaft los, ohne sie abzuschalten?

Indem jeder Session Host ein Zertifikat aus deiner PKI per Gruppenrichtlinie „Vorlage für Serverauthentifizierungszertifikat“ bekommt, die Clients der Stamm-CA vertrauen und alle per FQDN verbinden. Das Häkchen „Nicht erneut nachfragen“ ist keine Lösung, sondern eine Ausnahme pro Benutzer und Server.

Welche Zertifikate braucht eine RDS-Bereitstellung?

Vier Rollen-Zertifikate am Connection Broker, nämlich RDRedirector für SSO, RDPublishing für signierte RDP-Dateien, RDWebAccess und RDGateway, plus ein Zertifikat je Session Host für den RDP-Listener. Ein gemeinsames Zertifikat mit allen Namen im SAN ist für die vier Rollen üblich.

Warum sehen nur manche Benutzer die Zertifikatswarnung auf dem RDSH?

Domänen-Clients, die per FQDN verbinden, authentifizieren den Server über Kerberos und sehen oft nichts. Wer per IP-Adresse, Alias oder von einem Gerät außerhalb der Domäne verbindet, ist auf das Zertifikat angewiesen und bekommt die Warnung.

Was bedeutet „Unbekannter Herausgeber“ beim Öffnen einer RDP-Datei?

Die Datei ist nicht signiert. Seit dem Update vom April 2026 zeigt der Client dafür einen deutlichen Warndialog. Beziehe Dateien über RD Web, signiere selbst gebaute mit rdpsign und trage das Zertifikat der Rolle RDPublishing per Gruppenrichtlinie als vertrauenswürdigen Herausgeber ein.

Kann ich ein Wildcard-Zertifikat für die Remotedesktopdienste nutzen?

Für die Rollen-Zertifikate ist das verbreitet, sofern alle aufgerufenen Namen darunter fallen. Achte darauf, dass ein Wildcard für *.contoso.com keine Namen unter contoso.local abdeckt und dass der private Schlüssel dann auf vielen Servern liegt.

Muss ich nach dem Zertifikatstausch die Session Hosts neu starten?

In der Regel nicht. Neue Verbindungen verwenden das neu gebundene Zertifikat. Bestehende Sitzungen laufen weiter, nur beim Gateway können Verbindungen während des Tauschs kurz abbrechen.

Wo stelle ich das Zertifikat für den Session Host in der Gruppenrichtlinie ein?

Unter Computerkonfiguration › Richtlinien › Administrative Vorlagen › Windows-Komponenten › Remotedesktopdienste › Remotedesktop-Sitzungshost › Sicherheit › Vorlage für Serverauthentifizierungszertifikat. Dort trägst du den Namen der Zertifikatsvorlage ein.

Fazit: fünf Zertifikate, ein Name, null Klicks auf „Ja“

Die RDS-Zertifikatswarnung ist selten ein einzelner Fehler, sondern meist eine Kette aus Kleinigkeiten: selbstsignierte Session Hosts, die Kerberos jahrelang gnädig verdeckt hat, ein Broker-Zertifikat ohne den Namen, den die RDP-Dateien tatsächlich enthalten, eine Verknüpfung mit IP-Adresse und Clients ohne Stammzertifikat. Wer die vier Rollen-Zertifikate sauber setzt, die Session Hosts per Gruppenrichtlinie aus der PKI versorgt, die Root verteilt und nur noch per FQDN verbindet, hat Ruhe. Das Beste daran: Die Belegschaft verlernt das reflexhafte Wegklicken. Und der nächste Warndialog, der dann doch auftaucht, bekommt wieder die Aufmerksamkeit, die er verdient.

WEITERLESEN · Weiter in dieser Serie

› RD Gateway Zertifikat abgelaufen: schnell erneuern, künftig vorbeugen
› RDS-Farm härten: Sicherheits-Checkliste für Terminalserver
› RDS Connection Broker hochverfügbar machen
› RD Web Client (HTML5) installieren und veröffentlichen
› Session Hosts verhalten sich unterschiedlich: Konfigurationsdrift erkennen
› RDS Health Check: Farm regelmäßig prüfen statt nur reagieren