Remote Desktop Services: RDS-Farmen planen, bauen und im Griff behalten

Praxiswissen zu Terminalserver-Farmen zwischen Connection Broker, FSLogix und CAL-Zählerei

Totgesagte leben länger. Seit Jahren wird der Terminalserver von irgendwem beerdigt, erst von den Thin-Client-Visionären, dann von VDI, jetzt von Azure Virtual Desktop und Windows 365. Und trotzdem steht in fast jedem Unternehmen, das ich betreue, eine RDS-Farm im Keller oder im Rechenzentrum. Mal mit zwei Session Hosts für die Warenwirtschaft, mal mit zwanzig Hosts für die komplette Belegschaft. Sie läuft, sie ist günstig, und sie macht genau das, was sie soll. Meistens jedenfalls.

Denn eine RDS-Farm ist wie ein altes Mehrfamilienhaus: Von außen sieht alles ordentlich aus, aber hinter jeder Tür hat irgendwann mal jemand etwas umgebaut. Ein Drucker hier, eine Gruppenrichtlinie da, ein Zertifikat, das „erst mal“ selbstsigniert bleiben sollte. Nach zwei Jahren weiß niemand mehr, warum Host 4 sich anders verhält als Host 3. Und montags um acht, wenn sich alle gleichzeitig anmelden, zeigt die Farm, was sie davon hält.

Auf dieser Seite bekommst du den Überblick: wie eine Farm aufgebaut ist, wo sie typischerweise klemmt, was du bei Lizenzen, Hochverfügbarkeit, Sicherheit und der Migration auf Windows Server 2025 beachten musst und wann AVD die bessere Wahl ist. Dazu gibt es zwei Werkzeuge aus meiner Werkstatt, die genau für diesen Alltag gebaut sind: den RDS Diagnostiker und den UB Mechaniker für RDS.

Remote Desktop Services auf einen Blick	
Was es ist	Serverrolle von Windows Server, mit der viele Benutzer gleichzeitig auf einem Server arbeiten, als kompletter Desktop oder als einzelne RemoteApp
Früherer Name	Terminaldienste beziehungsweise Terminalserver, umbenannt mit Windows Server 2008 R2
Bausteine	Session Host, Connection Broker, Web Access, Gateway, Lizenzserver, dazu Profilablage und Active Directory
Protokoll	RDP, intern über TCP 3389, von außen über das Gateway per HTTPS 443, optional UDP 3391
Lizenzierung	Windows-Server-Lizenz plus RDS-CALs je Benutzer oder je Gerät; Anwendungen wie Office brauchen eine für Terminalserver zugelassene Lizenz
Aktuelle Version	Windows Server 2025; für Windows Server 2016 endet der erweiterte Support am 12.01.2027
Alternativen	Azure Virtual Desktop, Windows 365, Citrix auf RDS-Basis

Wie eine RDS-Farm aufgebaut ist

Eine Farm besteht aus mehreren Rollen, die zusammenspielen. Bei kleinen Umgebungen liegen alle auf einem Server, ab ein paar Dutzend Benutzern verteilt man sie. Das Grundprinzip ist immer

gleich: Der Benutzer meldet sich beim Zugang, der Connection Broker sucht ihm einen passenden Session Host, und dort läuft seine Sitzung mit seinem Profil.

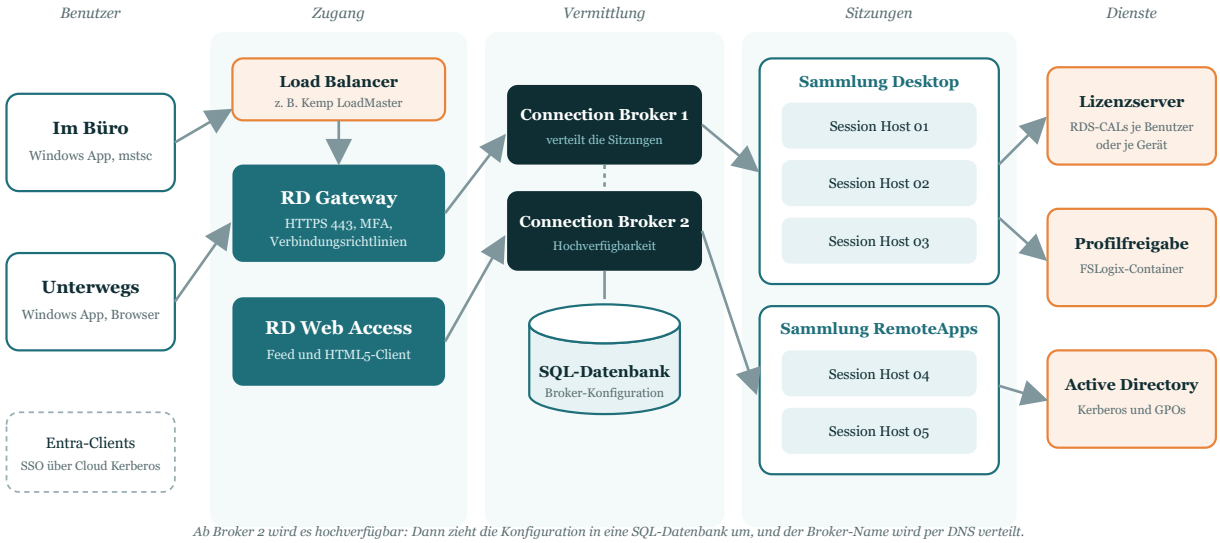


Abbildung 1: Aufbau einer hochverfügbaren RDS-Farm mit zwei Sammlungen

Rolle	Aufgabe	Typischer Stolperstein
Session Host	Hier laufen die Sitzungen und Anwendungen der Benutzer	Hosts einer Sammlung driften auseinander: andere Treiber, andere Patches, andere Software
Connection Broker	Verteilt Sitzungen, verbindet getrennte Sitzungen wieder, hält die Farmkonfiguration	Ohne Hochverfügbarkeit ein Single Point of Failure, mit HA ein SQL-Thema
Web Access	Liefert den Feed für die Windows App und den HTML5-Webclient	Zertifikat passt nicht zum Namen, den die Clients aufrufen
Gateway	Bringt RDP sicher über HTTPS ins Haus, mit Verbindungsrichtlinien und MFA	Abgelaufenes Zertifikat, fehlende MFA, offenes RDP am Gateway vorbei
Lizenzserver	Verwaltet RDS-CALs und stellt Gerätelizenzen aus	Falscher Lizenzmodus oder CALs einer älteren Generation
Profilablage	FSLogix-Container für die Benutzerprofile	Langsame Freigabe, volle Container, fehlende Virenscanner-Ausnahmen

Sammlung, Collection, Farm: Wer meint was?

Microsoft spricht von einem **Deployment** (Bereitstellung), das aus einer oder mehreren **Sammlungen** (Collections) besteht. Eine Sammlung ist eine Gruppe von Session Hosts mit gleichen Einstellungen, zum Beispiel „Desktop für alle“ oder „RemoteApps Buchhaltung“. Im Alltag sagen fast alle einfach **Farm**. Wichtig ist nur: Innerhalb einer Sammlung müssen die Hosts gleich gebaut sein, sonst würfelt der Broker, wer welches Problem bekommt.

Die typischen Baustellen

Die Beschwerden über RDS-Farmen klingen überall gleich. Die Ursachen auch, wenn man genau hinschaut. Hier die Klassiker aus meiner Praxis:

Beschwerde	Häufige Ursache	Wo du hinschaust
„Die Anmeldung dauert ewig“	Gruppenrichtlinie mit WMI-Filter, Logon-Skript, großes Profil, langsame Profilfreigabe	Anmeldephasen zerlegen: Profil, GPOs, Skripte, Shell
„Montags ruckelt alles“	Anmeldesturm, Datenträgerlatenz auf der Profilfreigabe, zu viele Sitzungen je Host	Leistungsindikatoren zur Anmeldespitze, User Input Delay
„Auf Host 4 geht SAP nicht“	Host weicht vom Rest der Sammlung ab	Software- und Patchstand gegen einen Referenzhost vergleichen
„Drucken geht nur manchmal“	Treiber-Wildwuchs, Typ-3-Treiber, Spooler-Abstürze	Treiberbestand je Host, Ereignisprotokolle
„Von extern geht nichts mehr“	Gateway-Zertifikat abgelaufen oder Kette unvollständig	Zertifikatslaufzeiten aller Rollen im Blick behalten
„Temporäre Lizenzen ohne Ende“	Lizenzserver, Lizenzmodus oder CAL-Typ passen nicht zusammen	Lizenzkonfiguration der Sammlung, Ereignisprotokoll des Lizenzservers

> **Aus der Praxis: Tausende temporäre Lizenzen**
>
> In einer großen Kundenumgebung verteilte der Lizenzserver nur noch temporäre Gerätelizenzen, obwohl 500 gültige CALs installiert waren. Ausgestellt waren am Ende mehr als 7.000 temporäre Lizenzen und ganze drei dauerhafte. Die Ursache lag nicht bei den CALs, sondern tiefer: Der Lizenzserver konnte sein eigenes Zertifikat nicht mehr erzeugen, ausgelöst durch eine wacklige Zeitsynchronisation. Solche Fälle findet man nicht mit Bauchgefühl, sondern nur mit Ereignisprotokollen, Registry und Geduld.

Lizenzierung: CALs zählen, aber richtig

Neben der Windows-Server-Lizenz brauchst du für jede Nutzung der Remotedesktopdienste eine RDS-CAL. Die gibt es in zwei Geschmacksrichtungen:

	Je Benutzer	Je Gerät
Passt für	Benutzer mit mehreren Geräten, Homeoffice, mobiles Arbeiten	Schichtbetrieb, viele Benutzer an wenigen festen Geräten
Technische Durchsetzung	Keine. Der Lizenzserver protokolliert, erzwingt aber nichts	Ja, der Lizenzserver stellt Gerätelizenzen aus
Risiko	Unterlizenzierung fällt erst beim Audit auf	Temporäre Lizenzen bei Problemen mit dem Lizenzserver

- **Die CAL-Generation muss passen:** Die CALs müssen mindestens die Version der Session Hosts haben. Wer auf Server 2025 umsteigt, braucht CALs der Generation 2025.
- **Die Übergangsfrist ist endlich:** Ohne konfigurierten Lizenzserver läuft eine Farm 120 Tage. Danach ist Schluss mit Anmelden, und zwar meist an einem Montag.
- **Office ist ein eigenes Thema:** Auf Session Hosts brauchst du eine Office-Lizenz, die dafür zugelassen ist, etwa eine Volumenlizenz oder Microsoft 365 Apps mit gemeinsamer Computeraktivierung. Eine normale Einzelplatzinstallation ist dort fehl am Platz.

> **Tipp: Bedarf messen statt schätzen**
>
> Wie viele Benutzer haben sich in den letzten 90 Tagen tatsächlich angemeldet? Wie hoch war die gleichzeitige Spitze? Der RDS Diagnostiker stellt diese Zahlen deinem Lizenzbestand gegenüber, in beide Richtungen: Überlizenzierung ist verschenktes Geld, Unterlizenzierung wird beim Audit teuer.

Hochverfügbarkeit: wenn der Broker nicht ausfallen darf

Mit einem einzelnen Connection Broker steht die ganze Farm, sobald dieser eine Server zickt. Für ernsthafte Umgebungen gehören deshalb mindestens zwei Broker dazu. Das klingt einfach, ist aber der Umbau, vor dem die meisten Administratoren den größten Respekt haben, und zwar zu Recht:

1. Die Farmkonfiguration zieht in eine **SQL-Datenbank** um, entweder auf einen SQL Server, gern in einer Verfügbarkeitsgruppe, oder in Azure SQL.
2. Alle Broker brauchen den passenden **SQL-Treiber**, ihre Computerkonten brauchen **Rechte** auf dem SQL Server.
3. Der Broker-Name wird per **DNS-Round-Robin** auf alle Broker verteilt, die Zertifikate müssen diesen Namen kennen.
4. Gateway und Web Access werden mehrfach ausgelegt und hinter einen **Load Balancer** gestellt.

Gerade der letzte Punkt hat es in sich: Persistenz, Health Checks und Kerberos hinter dem Load Balancer sind eigene Themen. Wie das mit einem Kemp sauber funktioniert, steht im Kompetenzbereich Kemp LoadMaster, die Kerberos-Seite der Medaille unter Microsoft Kerberos.

Sicherheit: RDP gehört nicht ins Internet

RDP direkt aus dem Internet erreichbar zu machen, ist ungefähr so klug, wie den Haustürschlüssel unter die Fußmatte zu legen und ein Schild dranzuhängen. Der Weg nach draußen führt über das Gateway. Und auch innen gibt es ein paar Hausaufgaben:

Zugang

Nur über das RD Gateway mit HTTPS

Mehrstufige Authentifizierung am Gateway, etwa über die NPS-Erweiterung für Entra MFA

Verbindungsrichtlinien auf echte Gruppen beschränken

Anmeldung

Netzwerkebenenauthentifizierung (NLA) erzwingen

Kerberos statt NTLM, also SPNs und Namen sauber halten

Lokale Administratoren auf den Hosts klein halten

Sitzung

Geräteumleitungen bewusst freigeben: Laufwerke, Zwischenablage, USB

Sitzungslimits für getrennte Sitzungen

AppLocker oder WDAC gegen „mal eben installiert“

Wer NTLM in der Farm loswerden will, findet Hilfe beim NTLM Diagnostiker. Und wenn Clients nur noch in Entra ID eingebunden sind, die Session Hosts aber im lokalen AD stehen, wird Single Sign-on zur Kür: Ohne Cloud Kerberos Trust und Windows Hello for Business tippen die Leute ihr Kennwort zweimal. Mehr dazu im Kompetenzbereich Microsoft Entra ID.

Migration auf Windows Server 2025

Am 12.01.2027 endet der erweiterte Support für Windows Server 2016. Viele Farmen laufen noch darauf, und die Zeit wird knapp. Bei RDS kommt es auf die Reihenfolge an. Wer die Session Hosts zuerst aktualisiert, erlebt mit einem älteren Broker und alten CALs eine Überraschung.

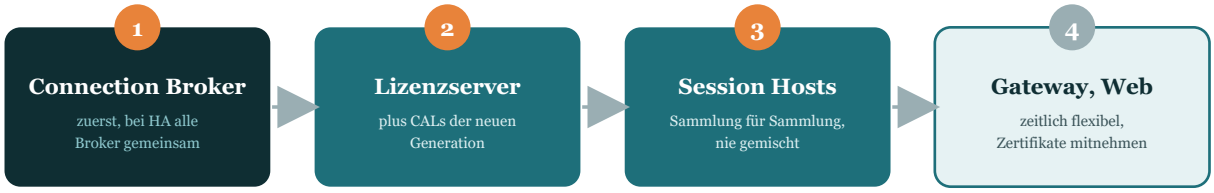


Abbildung 2: Bewährte Reihenfolge beim Upgrade einer RDS-Farm

> **Achtung: Gemischte Sammlungen**
>
> Innerhalb einer Sammlung sollten alle Session Hosts dieselbe Windows-Server-Version haben. Für eine Übergangszeit baust du lieber eine zweite Sammlung mit den neuen Hosts auf und ziehst die Benutzer gruppenweise um, statt alte und neue Hosts zu mischen.

Oft ist der Umstieg die Gelegenheit, die Farm gleich neu und sauber zu bauen statt in place zu aktualisieren. Genau dafür ist der UB Mechaniker für RDS gedacht: Neubau nach Standard, Gruppenrichtlinien nach Baseline, Lasttest vor der Übergabe.

RDS, Azure Virtual Desktop oder Windows 365?

Die Frage kommt in jedem zweiten Gespräch. Eine pauschale Antwort gibt es nicht, aber eine ehrliche Gegenüberstellung:

	RDS	Azure Virtual Desktop	Windows 365
Betrieb	Alles in deiner Hand: Server, Broker, Gateway, Lizenzen	Broker und Gateway betreibt Microsoft, Session Hosts sind deine Azure-VMs	Cloud-PC je Benutzer, fast alles betreibt Microsoft
Kosten	Kauflizenzen, eigene Hardware, planbar	Verbrauchsabhängig, Sparen über Skalierungspläne	Fester Monatspreis je Benutzer
Stärken	Bestehende Infrastruktur, Fachanwendungen, die lokal bleiben müssen	Windows 11 mit mehreren Sitzungen, elastisch	Einfach, persönlicher Desktop
Schwächen	Pflegeaufwand, Hochverfügbarkeit ist Handarbeit	Azure-Kenntnisse, Kostenkontrolle	Teuer bei vielen Benutzern, wenig Spielraum

Meine Erfahrung: Wo die Anwendungen ohnehin im eigenen Rechenzentrum laufen, ist RDS meist die wirtschaftlichere und schnellere Lösung. Wo ohnehin alles nach Azure geht, spricht viel für AVD. Und manchmal ist die Antwort ein Mischbetrieb für eine Übergangszeit.

Werkzeuge für deine Farm

Aus vielen Jahren mit RDS-Farmen bei Kunden sind zwei Werkzeuge entstanden. Sie decken zusammen den ganzen Lebenszyklus einer Farm ab: Der Mechaniker baut und erweitert, der Diagnostiker prüft im Betrieb. Beide arbeiten mit derselben Farmerkennung.

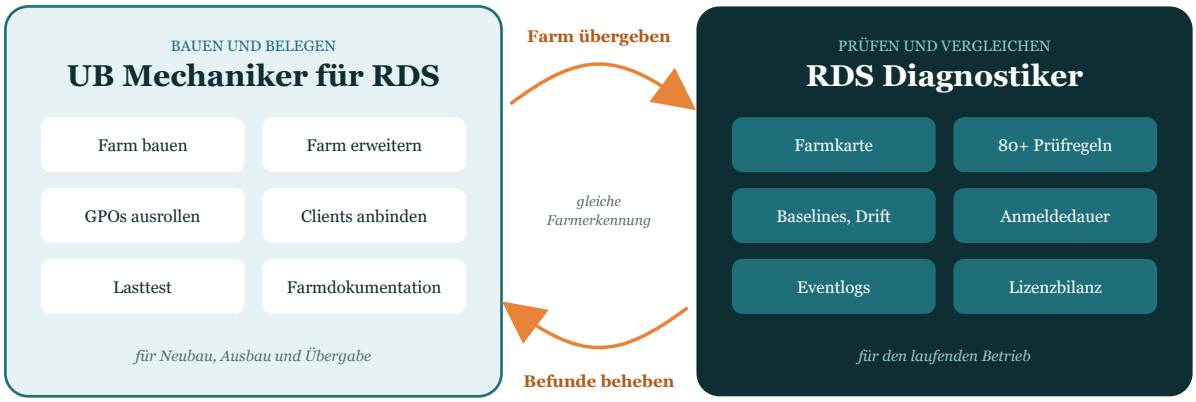
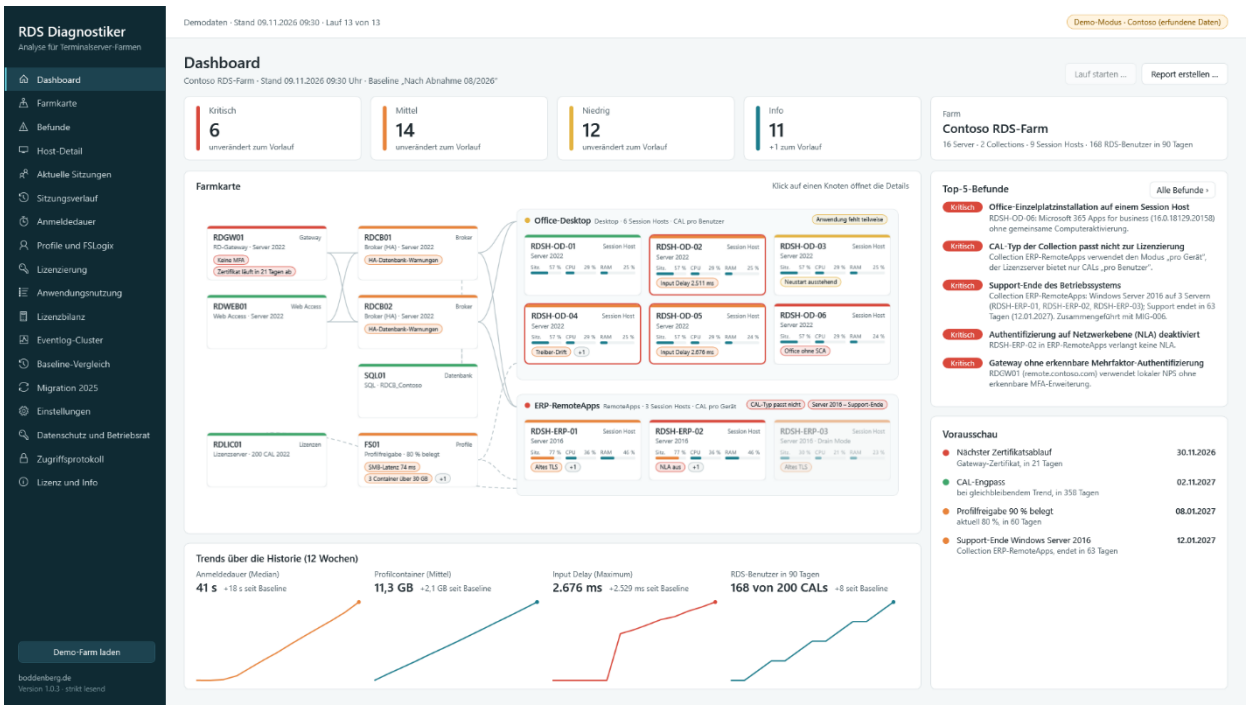


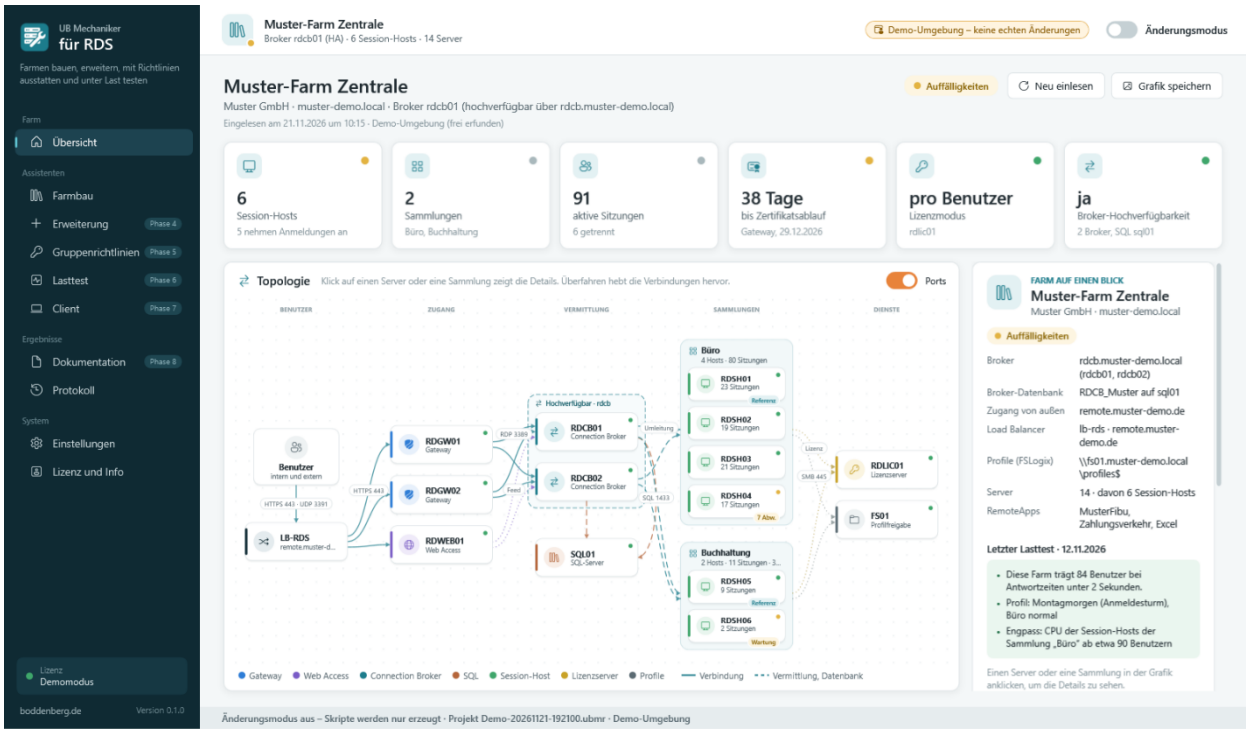
Abbildung 3: UB Mechaniker für RDS und RDS Diagnostiker im Zusammenspiel

RDS Diagnostiker: prüfen im Betrieb



RDS Diagnostiker: Dashboard mit Farmkarte, Befundzähler und Trends (Demo-Modus)

UB Mechaniker für RDS: bauen nach Standard



UB Mechaniker für RDS: Farmübersicht mit Topologie und Kennzahlen (Demo-Modus)

RDS Diagnostiker

Analysiert bestehende Farmen agentlos und strikt lesend: Farmkarte, über 80 Prüfregeln, Baselines, Anmeldedauer, Eventlogs, Lizenzbilanz und Word-Report.

Zum RDS Diagnostiker

UB Mechaniker für RDS

Baut und erweitert Farmen mit Assistenten, rollt Gruppenrichtlinien aus, testet unter Last und schreibt die Farmdokumentation gleich mit.

Zum UB Mechaniker für RDS

Einen kompakten Vergleich beider Werkzeuge findest du auf der Seite RDS-Werkzeuge im Überblick. Und falls auf deinen Session Hosts SharePoint-Bibliotheken als Laufwerke gebraucht werden: CosyTrack.Drive läuft auch auf Terminalservern.

Beratung und Schulung

Du willst deine Farm nicht allein auf Vordermann bringen? In der RDS-Beratung fange ich mit einem Farm-Check an, entwickle das Zielbild und begleite Neubau, Erweiterung oder Migration bis zur Übergabe. Wenn dein Team selbst fit werden soll, gibt es die RDS-Schulung als Firmenschulung, vom Kompakttag bis zum Workshop für Systemhaus-Teams.

Häufige Fragen zu Remote Desktop Services

Ist RDS noch zeitgemäß?

Ja. Microsoft entwickelt die Rolle weiter, Windows Server 2025 bringt sie selbstverständlich mit. Für Unternehmen mit lokalen Anwendungen ist RDS oft die wirtschaftlichste Art, zentral bereitzustellen. Zeitgemäß wird eine Farm aber erst mit Gateway, MFA, FSLogix und sauberer Pflege.

Wie viele Benutzer passen auf einen Session Host?

Das hängt an den Anwendungen und weniger an der Hardware. Ein Host mit Office und Browser trägt etwas anderes als einer mit CAD-Viewer oder Fachanwendung. Belastbar wird die Zahl erst mit einem Lasttest, alles andere ist Kaffeesatz.

Brauche ich RDS-CALs auch für Administratoren?

Für die reine Verwaltung über die zwei administrativen Remotedesktop-Verbindungen nicht. Sobald die Rolle Session Host installiert ist und Benutzer darauf arbeiten, brauchst du CALs.

Was ist besser: User Profile Disks oder FSLogix?

FSLogix. Die User Profile Disks sind ein Auslaufmodell. FSLogix-Container sind schneller, robuster und funktionieren genauso unter Azure Virtual Desktop, was dir eine spätere Migration erleichtert.

Kann ich eine RDS-Farm in Azure betreiben?

Ja, Session Hosts und Rollen laufen auch auf Azure-VMs. Bei den Lizenzen musst du aber genau hinschauen, RDS-CALs dürfen nicht einfach so in die Cloud umziehen. Und die Frage „Warum nicht gleich AVD?“ solltest du vorher beantwortet haben.

Wie bekomme ich einen schnellen Überblick über meine bestehende Farm?

Mit dem RDS Diagnostiker: Connection Broker eintragen, Lauf starten, nach wenigen Minuten stehen Farmkarte und Befunde. Er ändert dabei nichts, alle Abfragen sind lesend.

Wer hilft mir, wenn es richtig brennt?

Schreib mir über die Kontaktseite oder nutze „Frag Uli“ am Ende dieser Seite. Für akute Störungen ist ein kurzer Termin per Teams meist der schnellste Weg.

Wie geht es weiter?

Werkzeuge

Farm prüfen oder bauen mit Diagnostiker und Mechaniker.

RDS-Werkzeuge ansehen

Beratung

Farm-Check, Konzept und Umsetzung aus einer Hand.

Zur RDS-Beratung

Schulung

Firmenschulungen für Admins und Systemhaus-Teams.

Zur RDS-Schulung