



Windows Server 2019 Remote Desktop Services

Henrik Mai

Speaker

- Henrik Mai
- Senior IT-Consultant
Modern Workplace & Cloud Solutions
- On-Premises Datacenter Infrastruktur
 - › Hyper-V
 - › System Center
- Cloud Technologien
 - › Microsoft 365
 - › Modern Workplace Management
 - › Microsoft Azure



Organisatorisches

- Kurszeiten

- › 9:00 – 10:30
- › 10:45 – 12:15
- › 13:00 – 14:30
- › 14:45 – 16:15

- Speisen & Getränke

- Telefon

- Fragen

Vorstellung Kursteilnehmer

- Name
- Firma/Abteilung
- Aufgabengebiet
- Erfahrungen mit Windows/Desktop Virtualisierung
- Erwartungen an den Kurs

Gliederung

1. Konzept und Architekturen
2. Installation Session-based Deployment
3. Konfiguration von Sammlungen
4. Konfiguration des RDP-Client
5. Konfiguration des RDS-Web Access
6. Konfiguration User Environment
7. Zertifikate
8. Installation des RDS-Gateway
9. Konfiguration des RDS-Gateway

Schulungsumgebung

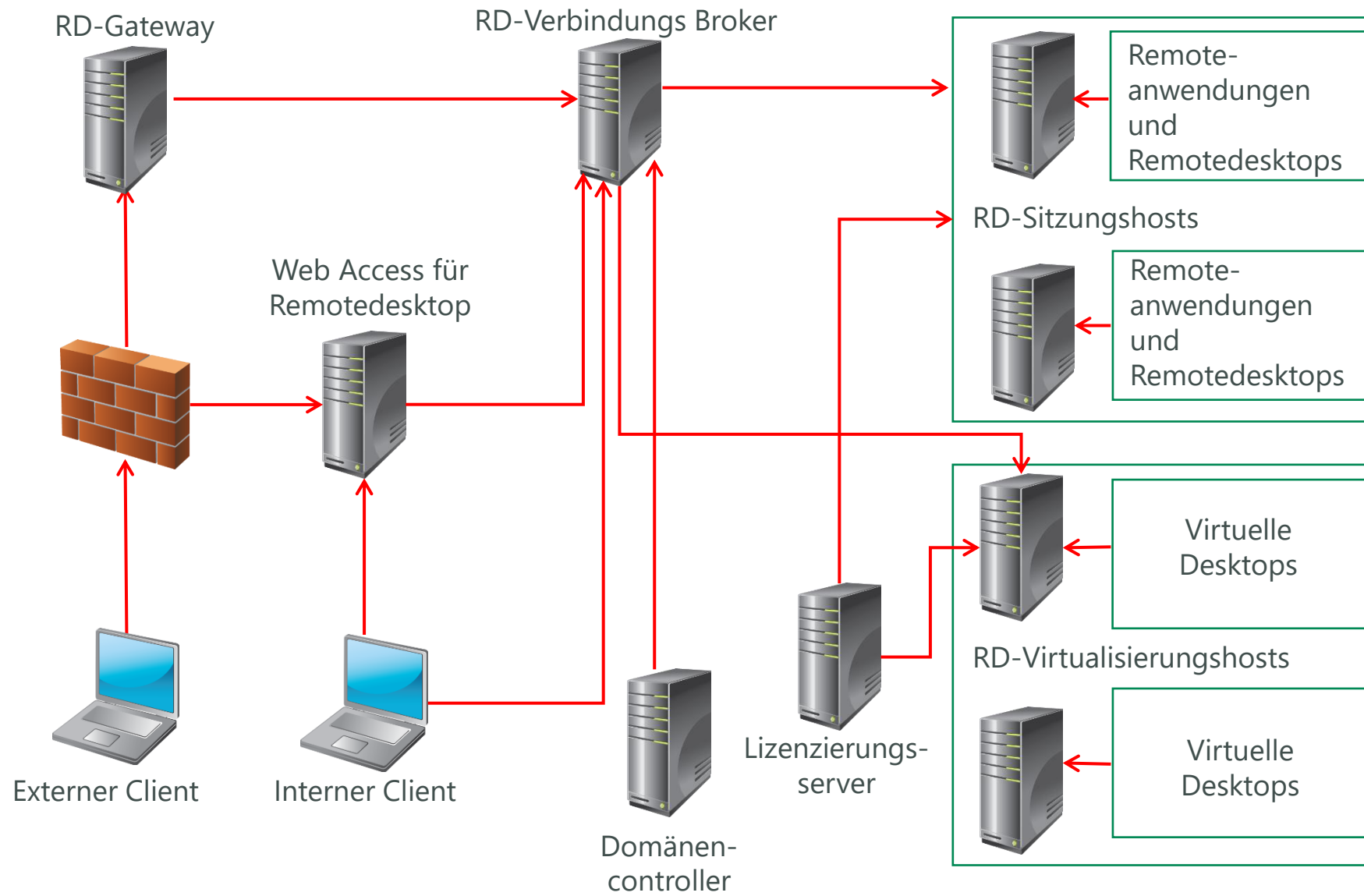
- Virtuelle Maschinen auf Basis Hyper-V
 - › Benutzername: LabAdmin
 - › Kennwort: Pa55w.rd
- Eigene Domäne vorbereitet
 - › Domain Admin: Administrator
 - › Kennwort: Pa55w.rd
- Übungen bauen aufeinander auf

Name	Rolle
RDS-DC1	Domain Controller
RDS-CB1	Connection Broker
RDS-WA1	Web Access
RDS-GW1	Gateway
RDS-SH1	Session Host 1
RDS-SH2	Session Host 2
RDS-CA	Certification Authority
RDS-Client1	Windows 10 Client

Module 1 – Konzepte und Architekturen

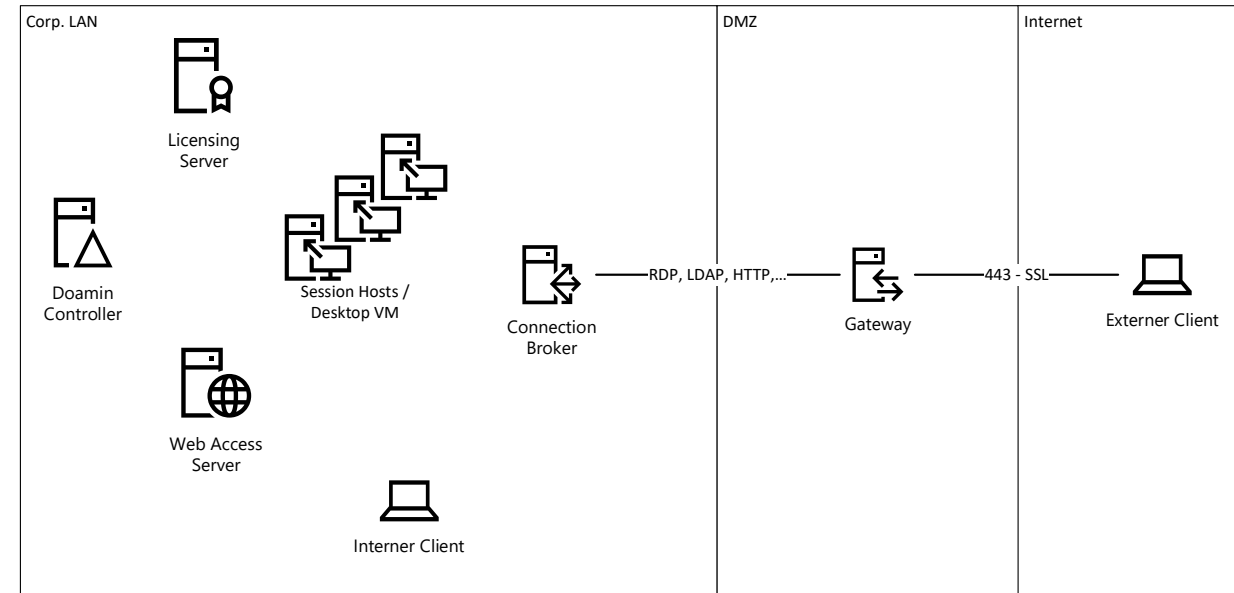
Module 1 – Konzepte und Architekturen

- Front End
- Server-based Computing
- Persistent VDI
- Pooled VDI



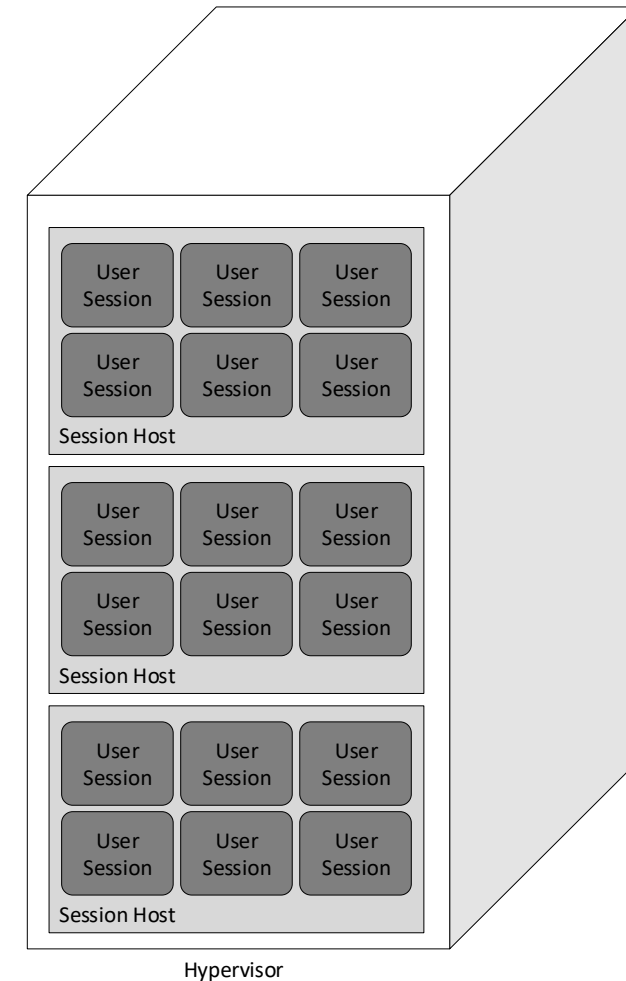
Front End

- Gemeinsam für SBC/VDI
- Broker als zentrale Komponente
- Gateway in DMZ als SSL-Tunnel-Instanz
- Alle Komponenten optional hochverfügbar



Back End – Server Based Computing

- Jeder Benutzer eine Sitzung auf Session Host
- Session Host bietet Zugriff auf Desktops und Anwendungen
- Geteilter Ressourcenzugriff
- Zugriff über Thin Clients, Notebooks, Desktops, Mobile Endgeräte

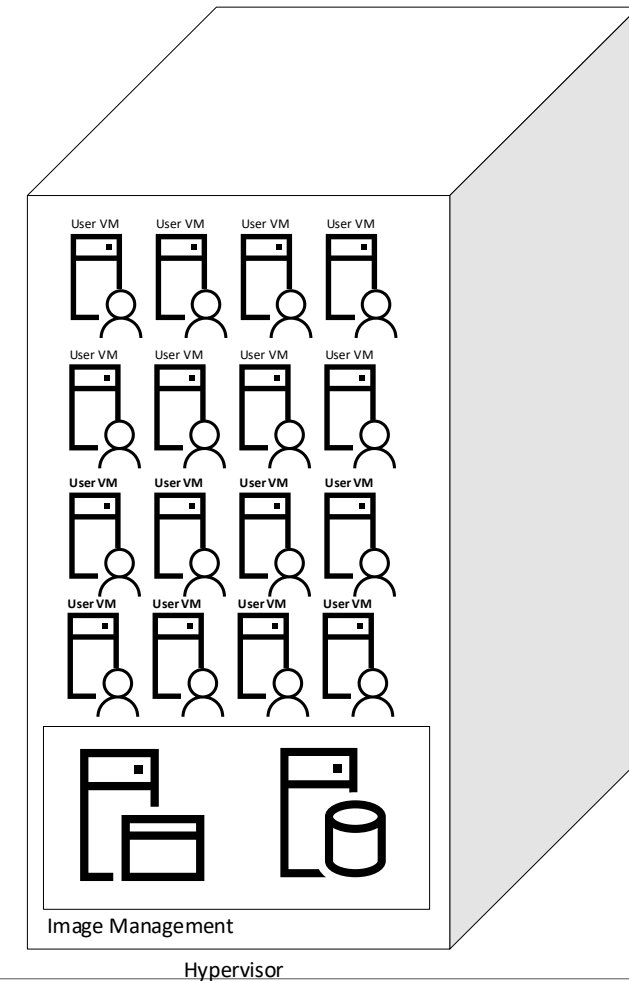


Pro und Contra – Server Based Computing



Back End – Persistent VDI

- Benutzer arbeitet immer mit selber Virtueller Maschine
- Management analog zu Fat Clients
- Zugriff über Thin Clients, Notebooks, Desktops, Mobile Endgeräte

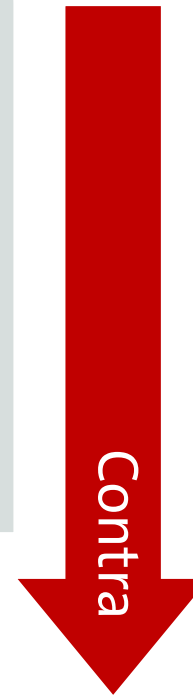


Pro und Contra – Persistent VDI



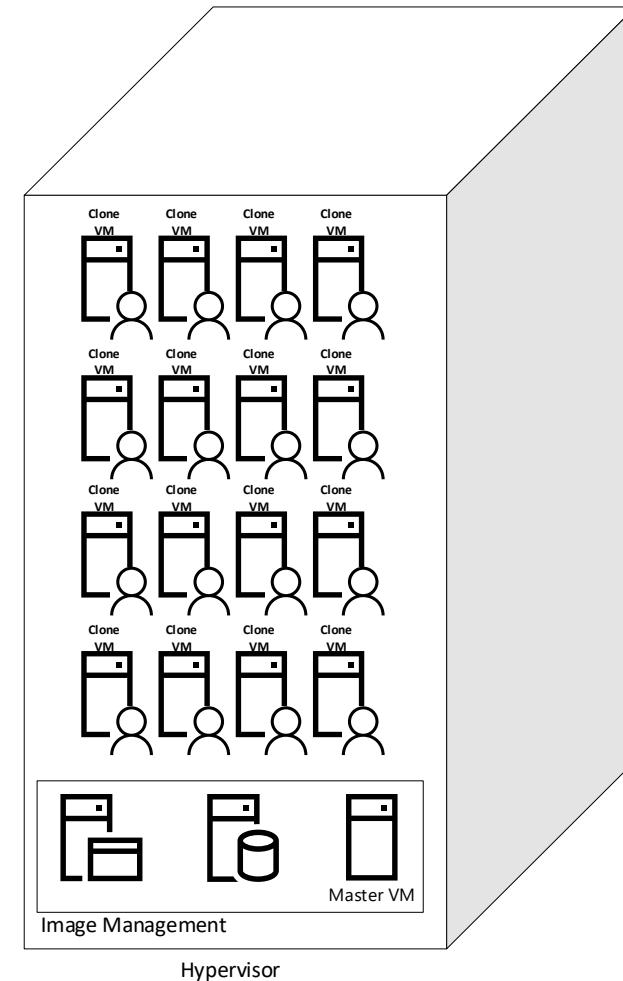
Verwaltbarkeit
Anwendungs-
Kompatibilität
Keine
Notwendigkeit von
Value Add-
Produkten

Storagebelastung
Speicherplatz
Storagebelastung
IOPS
Management-
Aufwand
„Pets vs. Cattle“



Back End – Pooled VDI

- Benutzer gelangt täglich auf „frische“ Maschine
- Master Image wird zentral verwaltet
- Mehrere Pools möglich
- Zugriff über Thin Clients, Notebooks, Desktops, Mobile Endgeräte

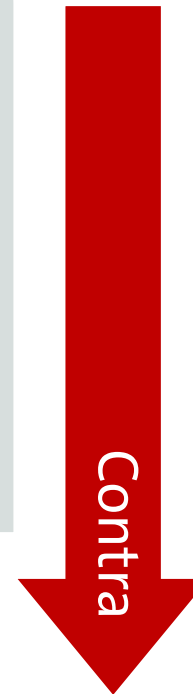


Pro und Contra – Pooled VDI



Performance
Speicherbedarf
Compliance

Persistenz
Troubleshooting
Management-
Aufwand
Anwendungs-
Kompatibilität



Module 2 – Installation Session-based Deployment

Module 2 – Installation Session-based Deployment

- Motivation
- Rollen
- Installation mit Quick Deployment-Wizard
- Installation mit Standard Deployment-Wizard

Motivation

- Application Compatibility
- Hardware Requirements
- Licensing Costs
- Remote Access

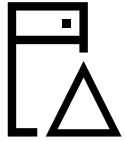
Rollen

- Remote Desktop Session Host
 - › Sitzungshost
 - › Freigabe von Anwendungen und Desktops
- Remote Desktop Connection Broker
 - › Verwaltet Zugriff auf Sitzungshosts
 - › Bietet Load Balancing, Session Reconnection
- Remote Desktop Web Access
 - › Bietet Browserzugriff auf freigegebene Ressourcen

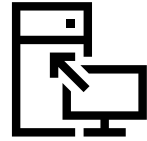
Installation Quick Deployment Wizard

- Installation über Server Manager
- Installiert alle Rollen auf einem Server
- Automatische Freigabe installierter Anwendungen
- Bietet keine Skalierung, Ausfallsicherheit

Übung 1 – Quick Deployment-Wizard



RDS-DC1
192.168.0.1



RDS-SH1
DHCP
All Roles




RDS-Client1
DHCP
RDS Client

1. Anmeldung an RDS-SH1
2. Add Roles and Features im ServerMgr
3. Auswahl Quick Start
4. Auswahl Session-based deployment
5. Deployment starten
6. Verifikation nach Neustart
7. Rücksetzen der virtuellen Maschinen

Installation Standard Deployment

- Installation über Server Manager
- Verteilt Rollen auf mehrere Server
- Bietet Skalierung und erhöhte Verfügbarkeit
- Remote Apps und Sammlung müssen manuell publiziert werden


Übung 2 – Standard Deployment



RDS-SH1
DHCP
Session Host



RDS-Client1
DHCP
RDS Client



RDS-DC1
192.168.0.1



RDS-WA1
DHCP
Web Access



RDS-CB1
DHCP
Connection
Broker

1. Anmeldung an RDS-CB1
2. Hinzufügen aller Server zum Server Manager
3. Standard Deployment starten
4. Deployment verifizieren
5. Sammlung anlegen
6. Beispielanwendungen publizieren

Module 3 – Konfiguration von Sammlungen

Module 3 – Konfiguration von Sammlungen

- Weitere Rollen
- Zertifikate
- Sammlungseigenschaften
- Sitzungseigenschaften

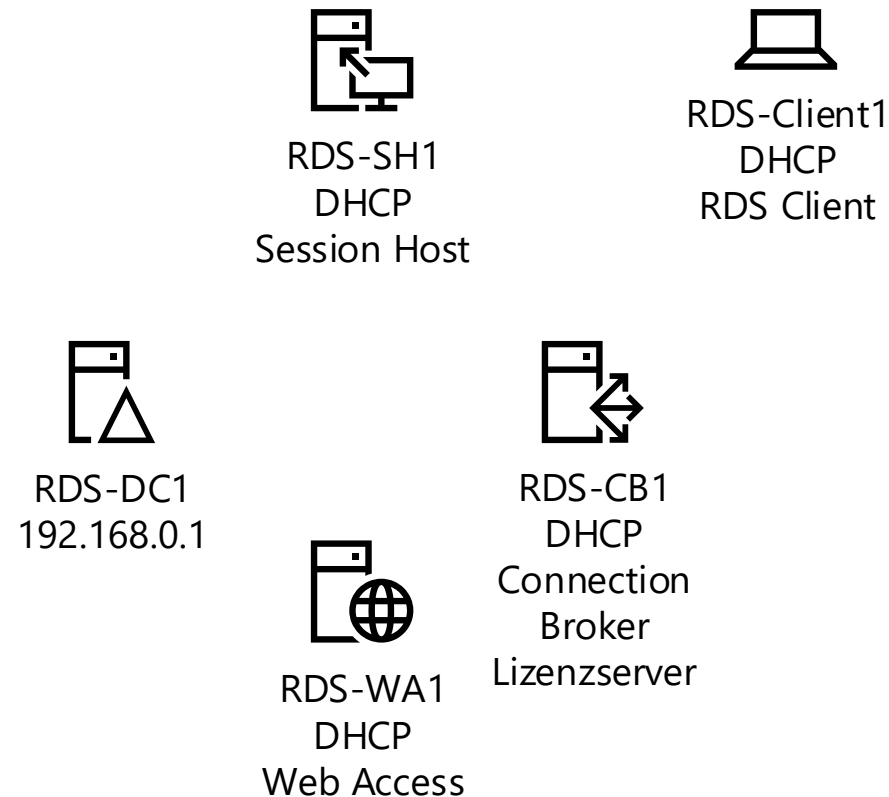
Weitere Rollen – RD Gateway

- Remote Desktop Gateway
 - › Benötigt bei Zugriff über DMZ
 - › Prüft Credentials
 - › Weiterleitung von Clients an Connection Broker
 - › Konfiguration in Deployment Einstellungen

Weitere Rollen – RD License Server

- Remote Desktop License Server
 - › Pro Server standardmäßig zwei CAL für Administration
 - › Nach Installation des Lizenzservers 119 Tage zur Aktivierung
 - › Lizenzierungsmodi (einmalige Entscheidung pro Deployment)
 - › Per User
 - › Per Device
 - › Mehrere Lizenzserver möglich (ab Windows Server 2019 HA mit SQL Server)

Übung 3 – Installation Lizenzserver

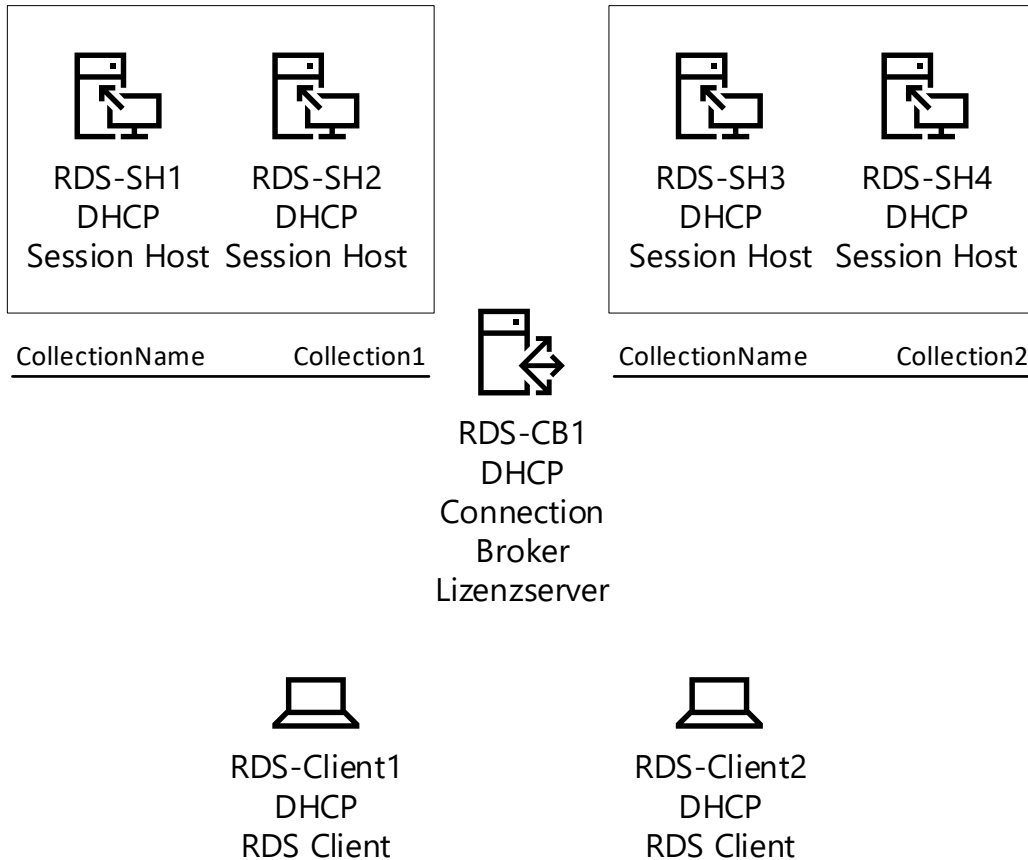


1. Anmeldung an RDS-CB1
2. Installation Lizenzserver
3. Aktivierung (nicht möglich)

Zertifikate

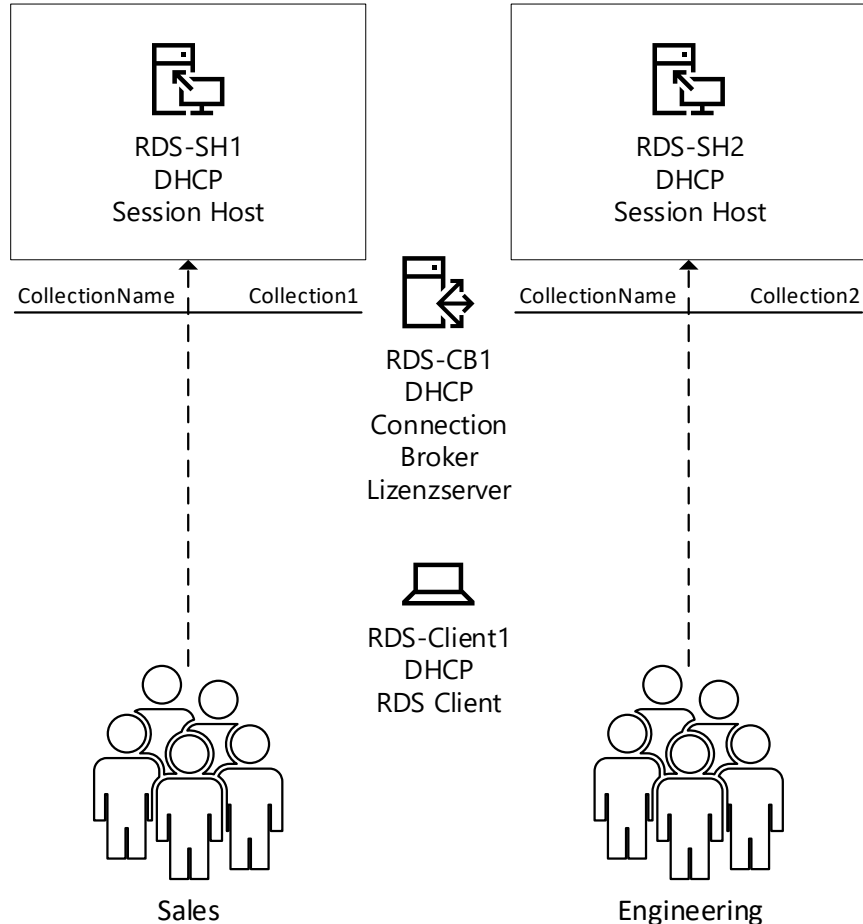
Rolle	Benötigt Zertifikat für
Remote Desktop Connection Broker	Single Sign-On
Remote Desktop Connection Broker	Publishing
Remote Desktop Web Access	HTTPS
Remote Desktop Gateway	Server Authentication

Sammlungen



- Einsatzzweck
 - › Aufteilung von Session Hosts in mehrere Farmen
 - › Organisation von Ressourcen

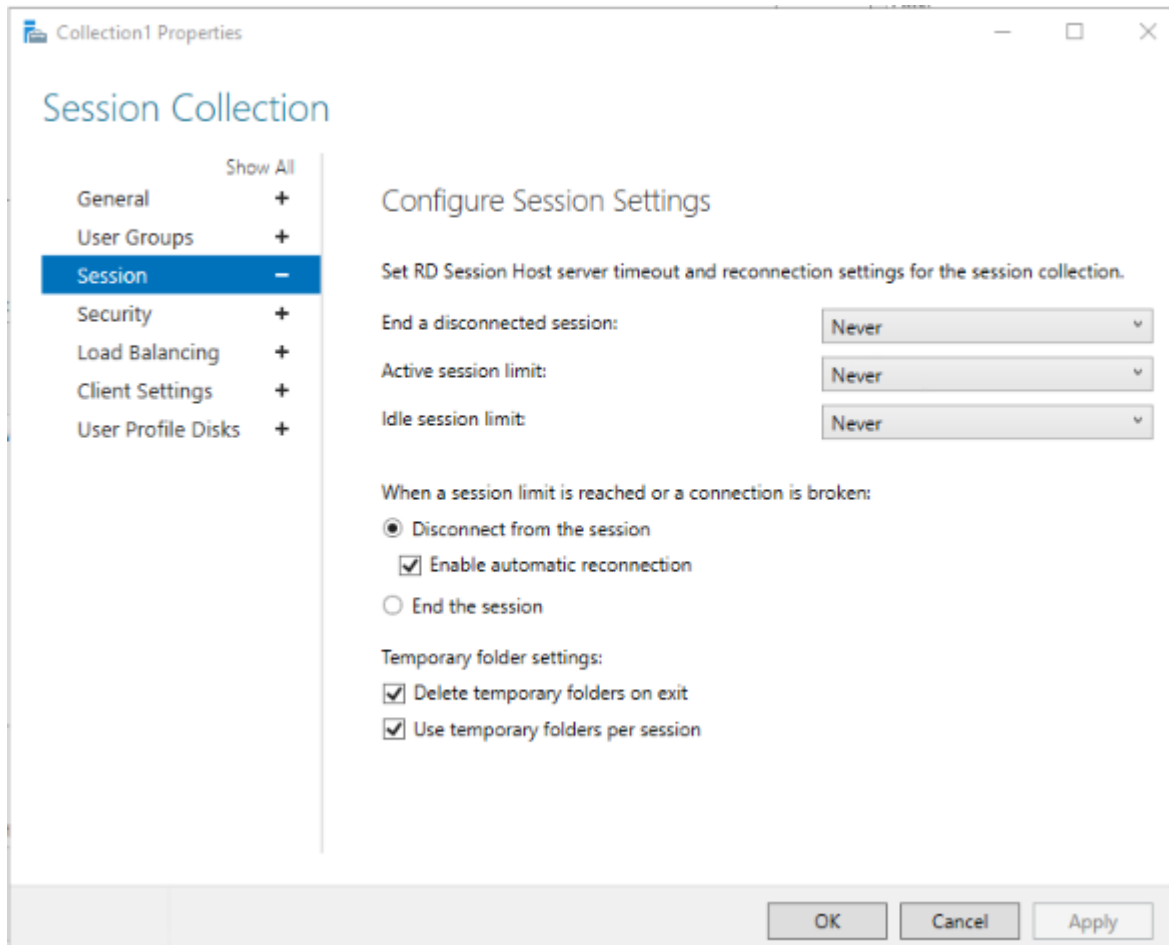
Übung 4 - Sammlungen



1. Anmeldung an RDS-CB1
2. Aufnahme RDS-SH2 in Serverpool
3. Anlegen Session Collection „Collection2“
4. Anlegen AD-Gruppen Sales, Engineering
5. Zuordnung Collection 1 → Sales
6. Zuordnung Collection 2 → Engineering
7. Verifikation der (Direkt-)Verbindungen

Session Limits

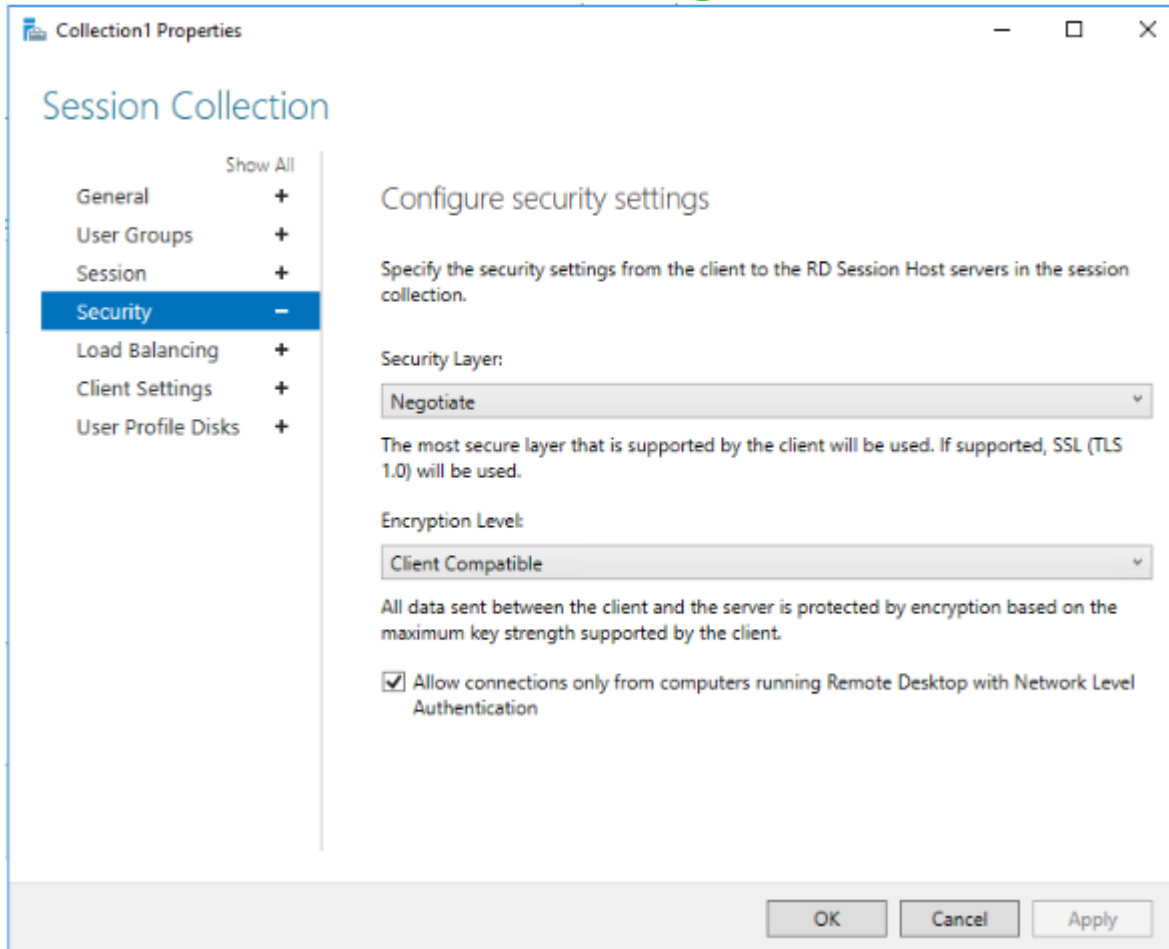
- Anpassung an Bedarf/Benutzerdichte



Übung 5 – Session Limits

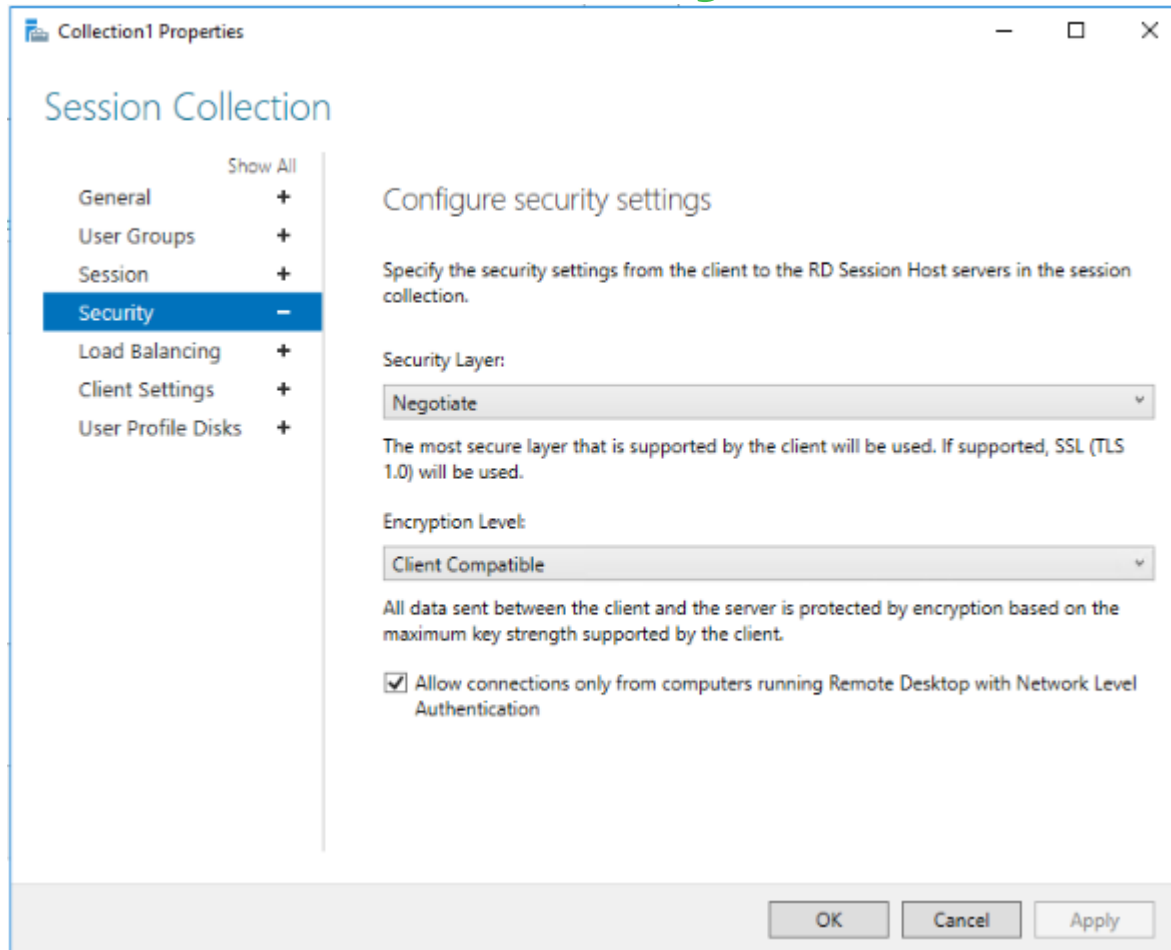
1. Anmeldung an RDS-CB1
2. Öffnen der Session Limits für Collection2
 1. Konfiguration des Disconnected Timers auf 1 Minute
3. Prüfung des Disconnect-Verhaltens für Alice, Bob

Session Security



- Security Layer:
 - › RDP Security Layer
 - › Keine beidseitige Authentifizierung
 - › Keine NLA
 - › SSL TLS
 - › Serverauthentifizierung
 - › Datenverschlüsselung
 - › Zertifikat benötigt
 - › Negotiate
 - › Unterstützte Ebene wird verhandelt

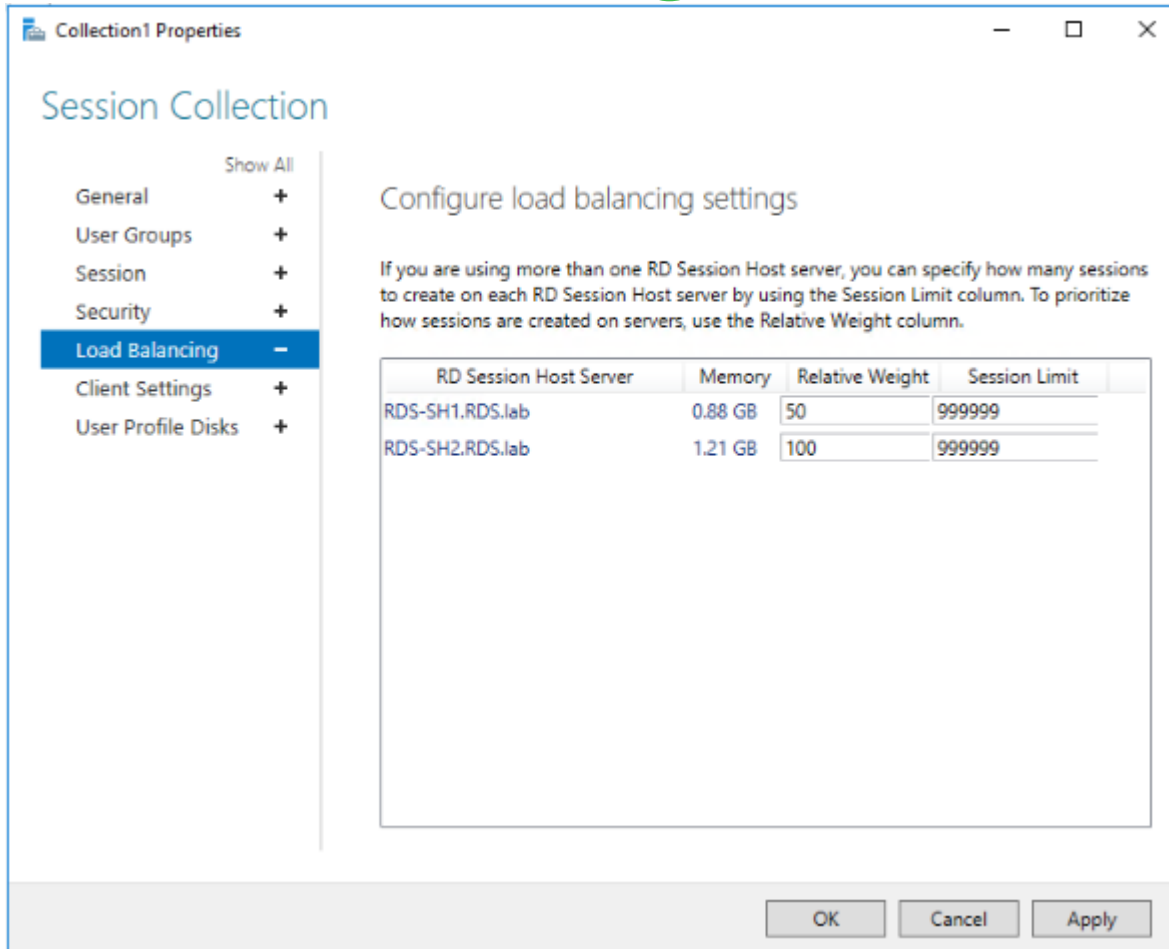
Session Security



■ Encryption Level:

- › Low
 - › Data (CL→SRV) 56bit-Encryption
 - › Data (SRV→ CLT) No Encryption
- › Client compatible
 - › Default
 - › Client bestimmt Schlüssellänge
- › High
 - › 128bit bidirektional erforderlich
 - › Keine Verbindung bei fehlendem Support
- › FIPS
 - › Federal Information Processing Standards

Load Balancing

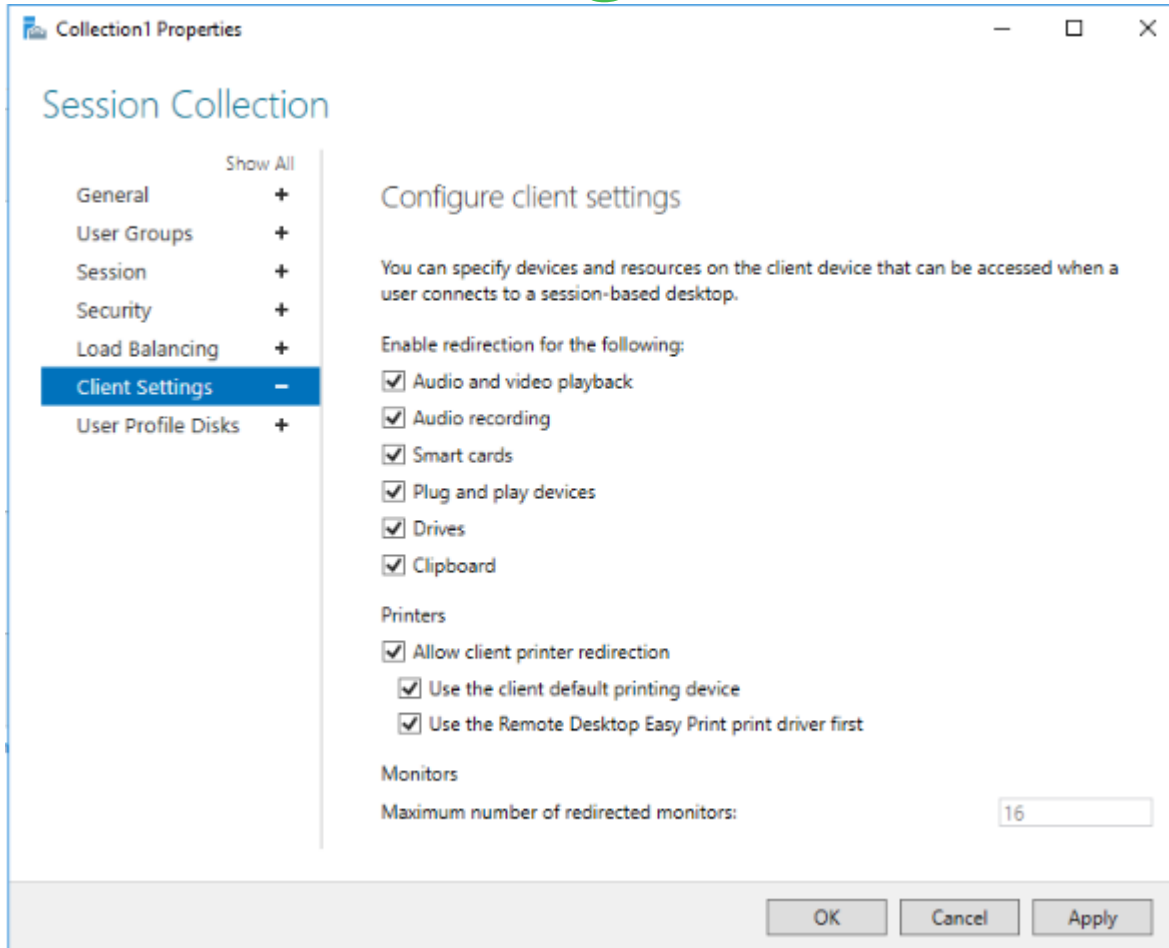


- Relatives Gewicht
 - › Anteil der Verbindungen pro Session Host im Verhältnis zur gesamten vergebenen Gewichte
- Session Limit
 - › Maximale Anzahl von Sitzungen pro Session Host

Übung 6 – Load Balancing

1. Anmeldung an RDS-CB1
2. Entfernen der Collection2
3. Hinzufügen von RDS-SH2 zu Collection1
4. Änderung des relativen Gewichts für RDS-SH1 auf 50
5. Konfiguration des RDP Client für Connection Broker

Client Settings



- Redirection muss auf Client und Server konfiguriert werden
- Drucken erfordert besonderen Augenmerk
 - › Druckerzuordnung
 - › Benötigte Features
 - › Inkompatibilitäten

User Profile Disk

- Auslagerung von Anwendungs- und Benutzerdaten in VHD
- Template UVHD-template.vhdx erlaubt Anpassung des Default-Profiles
- Neue VHDX pro Benutzer auf Freigabe
- Name der VHDX: GUID des Benutzers
 - › Zuordnung per PowerShell
 - › Sidder-Application

Übung 7 – User Profile Disks

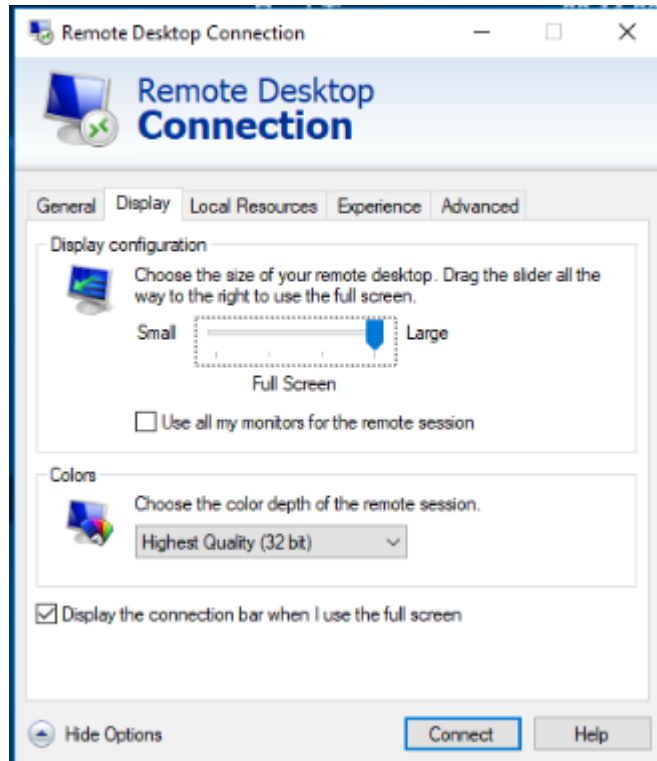
1. Anmeldung an RDS-CB1
2. Ordnererstellung C:\UPD_Collection1 und Freigabe als UPD_Collection1
3. Anpassung der Collection Settings für Collection1 zur Nutzung User Profile Disks (UPD)
4. Prüfung der Berechtigungen
5. Anmeldung an RDS-Client1 mit RDS\Alice
6. Sitzungsaufbau

Module 4 – Konfiguration des RDP-Clients

Module 4 – Konfiguration des RDP-Clients

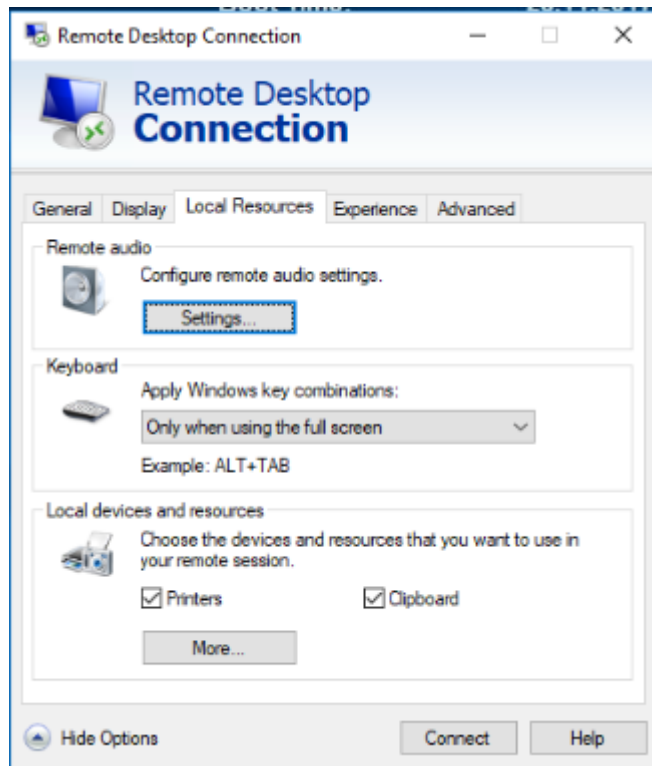
- Anzeigeeinstellungen
- Lokale Ressourcen
- Programme
- User Experience
- Erweitert
- Remote App und Desktop Verbindungen

Display



- Beeinflusst Skalierung und Benutzererfahrung

Lokale Ressourcen



- Remote Audio
 - › Qualität vs. Performance
- Keyboard
 - › Shortcuts
- Lokale Geräte
 - › Erfordert serverseitige Konfiguration

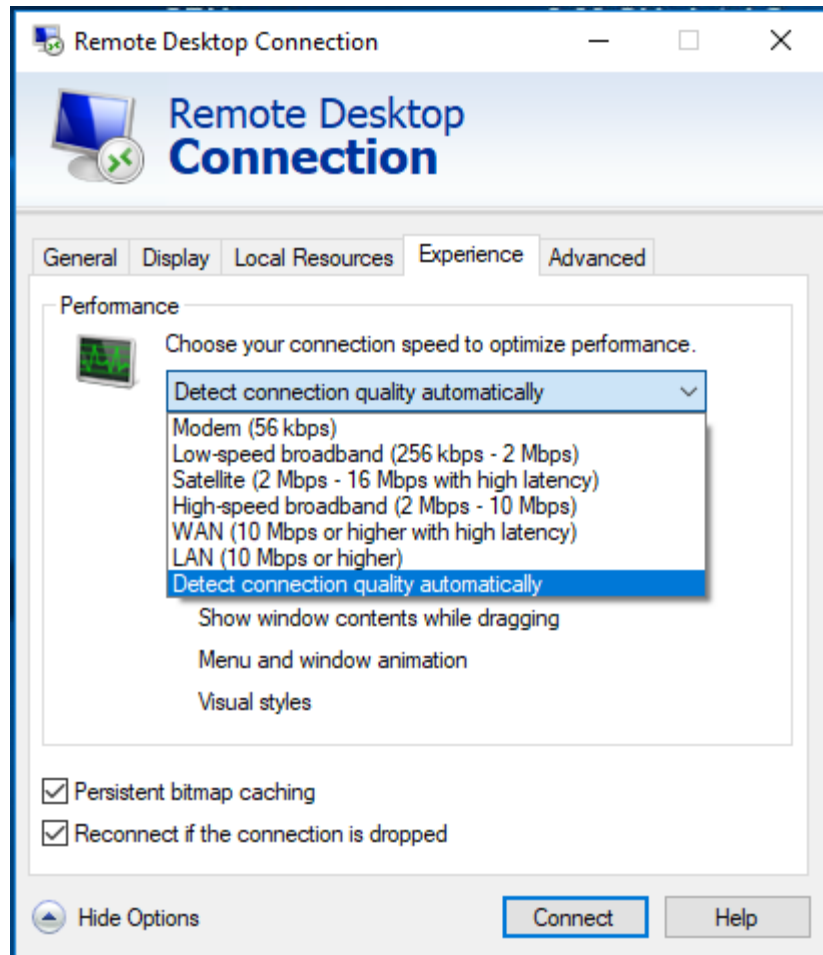
Übung 8 - Geräteumleitung

1. Anmeldung an RDS-CL1
2. Aktivierung der Geräteumleitung für lokale Laufwerke
3. Servereinstellungen prüfen
4. Anmeldung an RDS-CB1 (per MSTSC)
5. Geräteumleitung verifizieren

Programme

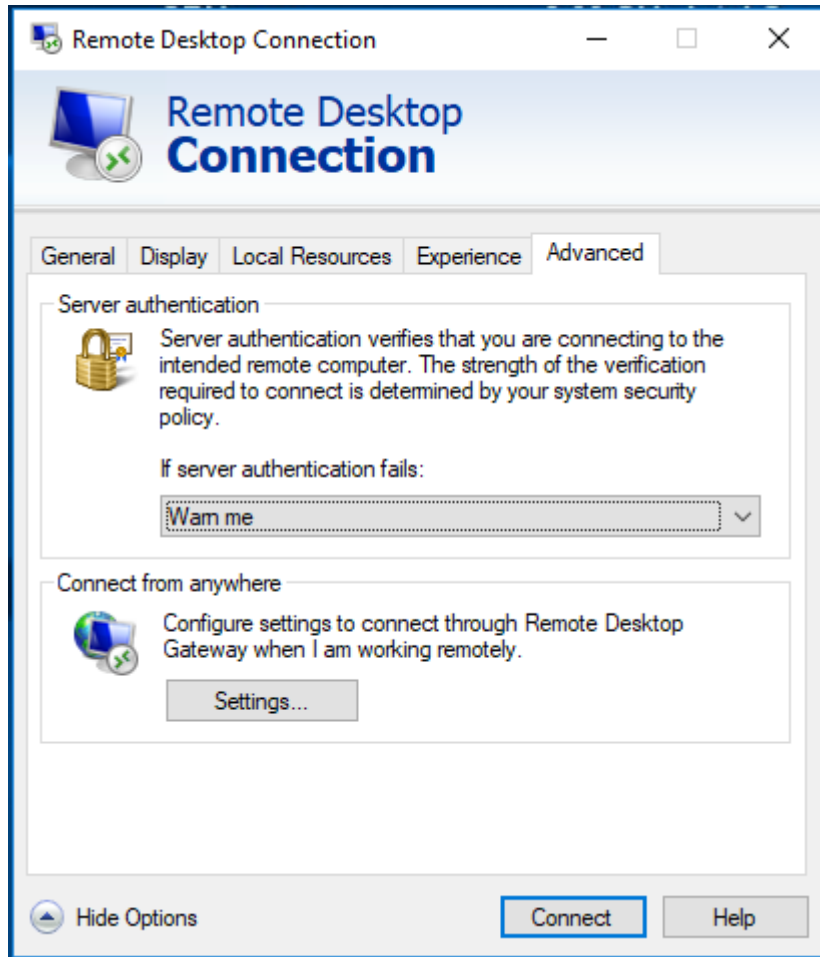
- Automatischer Start nach Verbindungsaufbau möglich
- Tab fehlt in Windows 10 MSTSC-Client
- Konfiguration über Alternative Shell-Eintrag in RDP-File
- Zu startende Anwendung muss publiziert sein

Benutzererfahrung



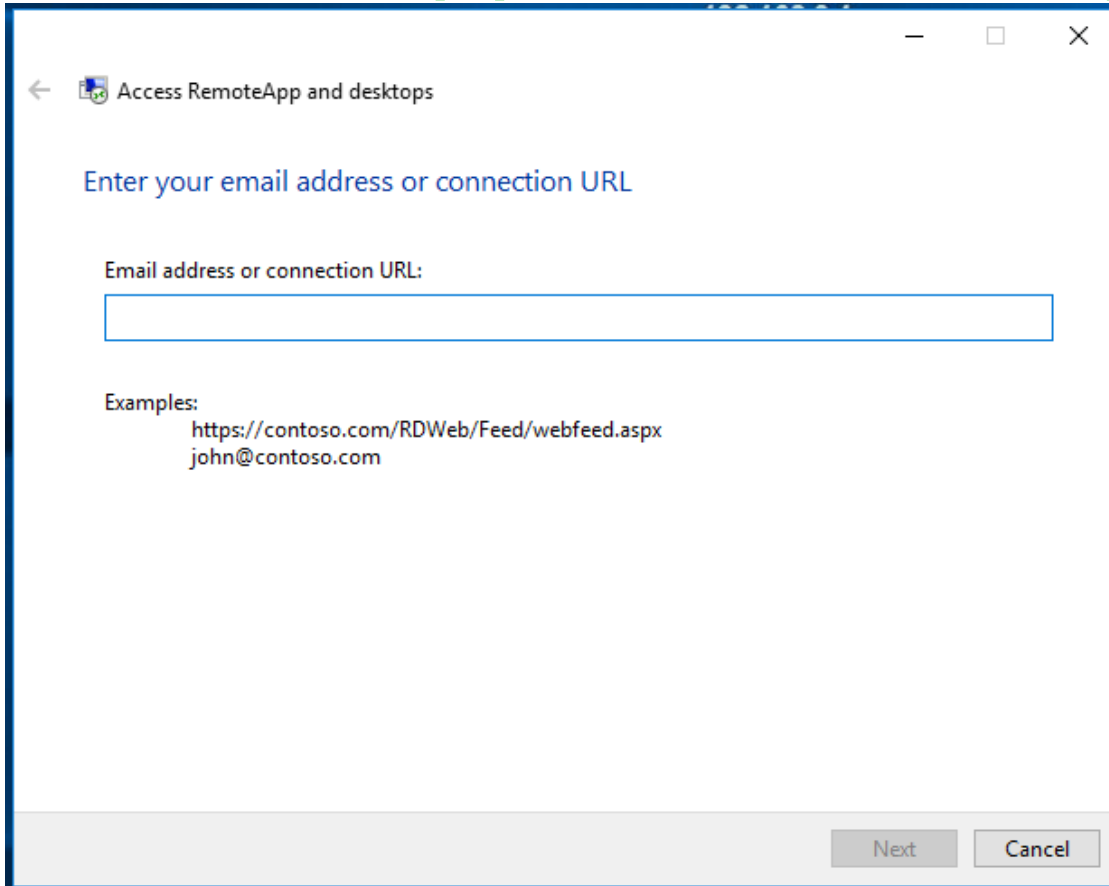
- Vorlagen für Verbindungsqualitäten
- Persistent Bitmap Caching
 - › Bilder werden auf Client zwischengespeichert
- Reconnection
 - › Automatische Verbindungswiederaufnahme

Erweitert



- Server Authentication
 - › Warnung
 - › Verbindung ohne Warnung
 - › Verbindungsabbruch
- Connect from anywhere
 - › Konfiguration Remote Desktop Gateway

RemoteApp und Desktop Verbindungen



← Access RemoteApp and desktops

Enter your email address or connection URL

Email address or connection URL:

Examples:

`https://contoso.com/RDWeb/Feed/webfeed.aspx`
`john@contoso.com`

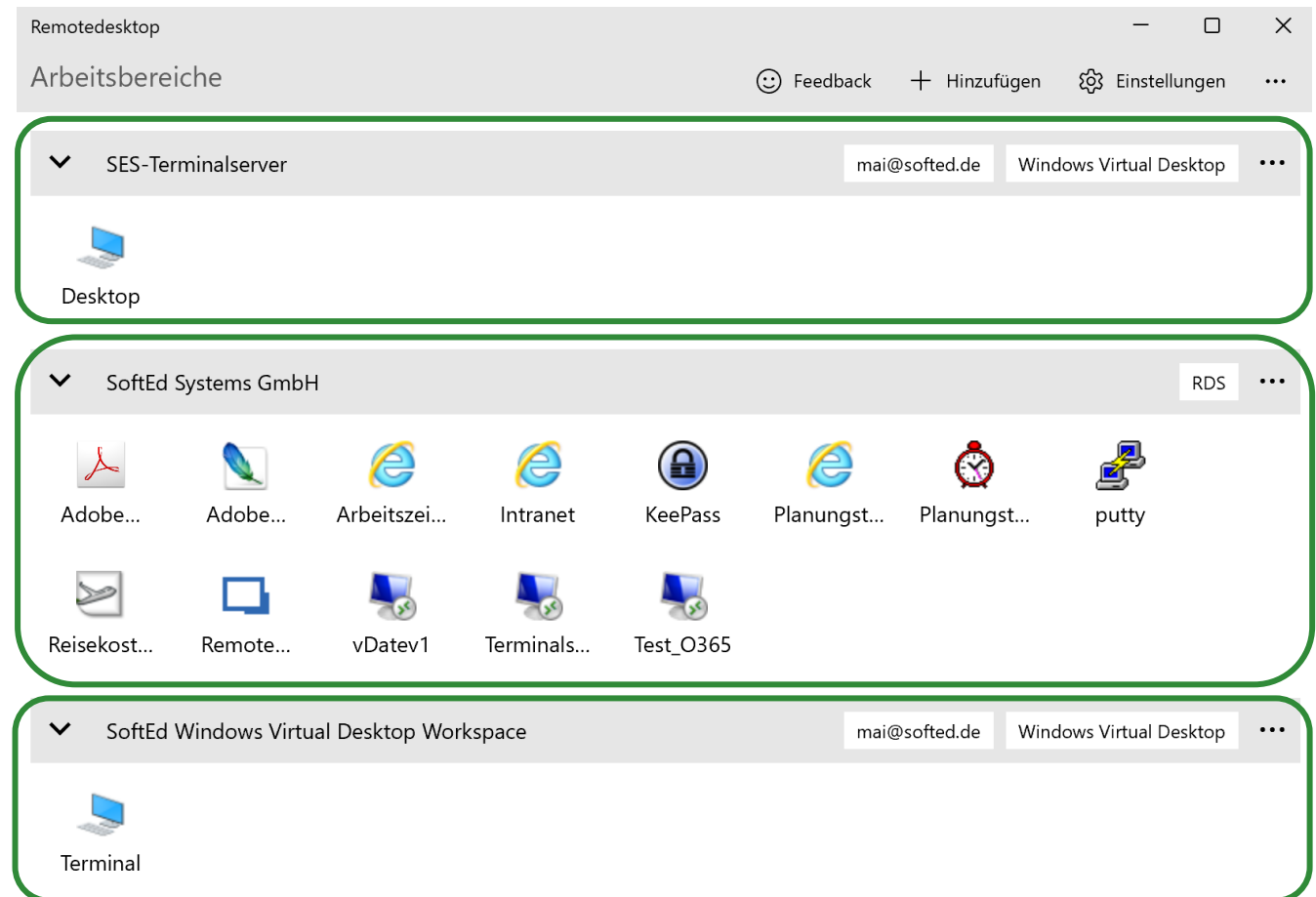
Next Cancel

- URL des Web Access Servers
 - › `https://<FDQN>/rdweb`
- Wenn E-Mail
 - › DNS TXT Record „_msradc“
- Ressourcen werden Startmenü hinzugefügt
- Zertifikat muss vertrauenswürdig sein
- Gruppenrichtlinie oder MDM

Remotedesktop App



- On-Premises Ressourcen
- Modern Desktop Infrastructure (Azure)



Übung 9 – Einrichtung RemoteApp und Desktop

1. Anmeldung an RDS-Client1 als RDS\Administrator
2. Aufruf <https://RDS-WA1.rds.lab/rdweb> im Microsoft Edge
3. Sicherung des Zertifikats in Local Machine\Trusted Root CA
4. Öffnen RemoteApp and Desktops-Anwendung
5. Hinzufügen der Verbindungen von RDS-WA1

Module 7 – Konfiguration RD Web Access

- SSL
- Veröffentlichung von Anwendungen
- Anpassung der Website
- Single Sign-On
- Hochverfügbarkeit

SSL für RD Web Access

- Zentrales Zertifikatmanagement auf Connection Broker
- Zertifikat muss für Serverauthentifizierung ausgestellt sein

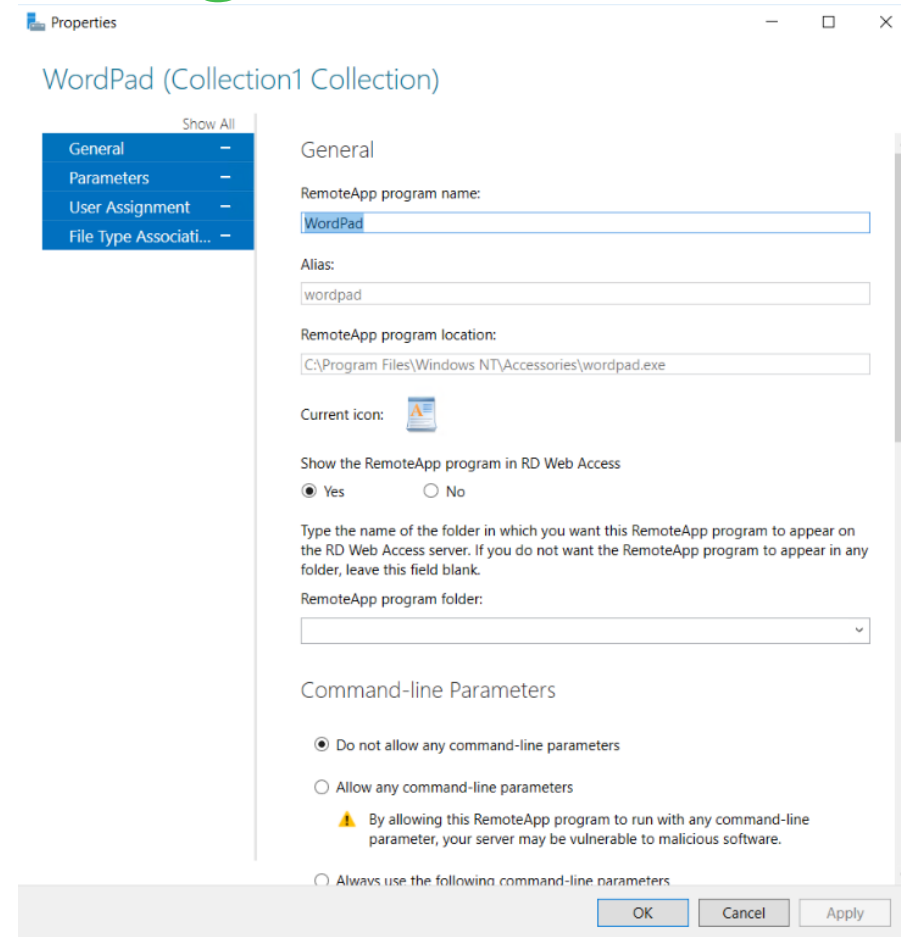
Übung 16 – Zertifikat für RD Web

1. Anmeldung an RDS-WA1
2. Erstellung / Prüfung und Export des Zertifikats für RDS-WA1.rds.lab
3. Anmeldung an RDS-CB1
4. Öffnen der Deployment Properties
5. Anpassung des WA Zertifikats
6. Wiederholung for Connection Broker Zertifikat

Anwendungsveröffentlichung

■ Einstellungen

- › Name
- › Anzeige in Web Access
- › Ordner
- › Parameter
- › Benutzerzuweisung
- › FTA



Anpassung der RD Website

- Password Reset Link
- Standardbilder
 - › Hinzufügen zu Images-Ordner
 - › Anpassung Site.xls
- Textnachrichten
 - › Set-RDWorkspace auf Connection Broker
 - › Anpassung RDWAstrings.xml
 - › Anpassung logon.aspx

Übung 17 – Password Reset

1. Anmeldung an RDS-WA1

2. IIS Manager

- › \Pages
 - › Application Settings
 - › PasswordChangeEnabled aktivieren

3. C:\Windows\Web\RDWeb\Pages\en-us\login.aspx

- › Suche nach UserPass
- › Code hinzufügen
 - › `<tr><td align="right">
Click here to reset your
password.
</td></tr>`

Single Sign-On

- Zertifikate
- Gruppenrichtlinie
 - › Credential Delegation
 - › Remote Desktop
 - › Internet Explorer
- IIS
 - › Authentication
 - › Web.config

Übung 18 – Setup Single Sign-on für RD Web

1. IIS Manager auf RDS-WA1

1. Anpassung Authentication
 1. Disable Anonymous
 2. Enable Windows Authentication
2. Web.Config
 1. Entkommentieren: Windows Authentication
 2. Kommentieren:
 1. Forms Authentication
 2. Modules
 3. Security

2. Default.aspx

1. ShowPublicCheckbox: false
2. PrivateMode: true

Übung 18 – Setup Single Sign-on für RD Web II

3. GPMC auf RDS-DC1: Default Domain Policy

Pfad	Policy	Wert
Computer Cfg.\Adm. Templates\System\Credential Delegation	Allow delegating default credentials with NTLM-only Server Authentication	TERMSRV/rds-cb1.rds.lab; TERMSRV/rds-sh1.rds.lab alternativ TERMSRV/*.rds.lab
Computer Cfg.\Adm. Templates\System\Credential Delegation	Allow delegating default credentials	TERMSRV/rds-cb1.rds.lab; TERMSRV/rds-sh1.rds.lab alternativ TERMSRV/*.rds.lab
Computer Cfg.\Adm. Templates\Windows Components\Remote Desktop Services\Remote Desktop Connection Client	Prompt for User Credentials	Disabled
Computer Cfg.\Adm. Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page*	Site to Zone Assignment List	Rds-wa1.rds.lab:2
Computer Cfg.\Adm. Templates\Windows Components\Internet Explorer\Internet Control Panel\Trusted Sites Zone*	Logon Options	Enabled (Automatic Logon with current username and password)

*auch für Benutzerrichtlinie

Hochverfügbarkeit für RD Web

- DNS Round Robin
 - › Nicht empfohlen
- NLB Clustering
 - › Erfordert DNS Konfiguration
 - › Erfordert NLB auf allen RD Web Servern

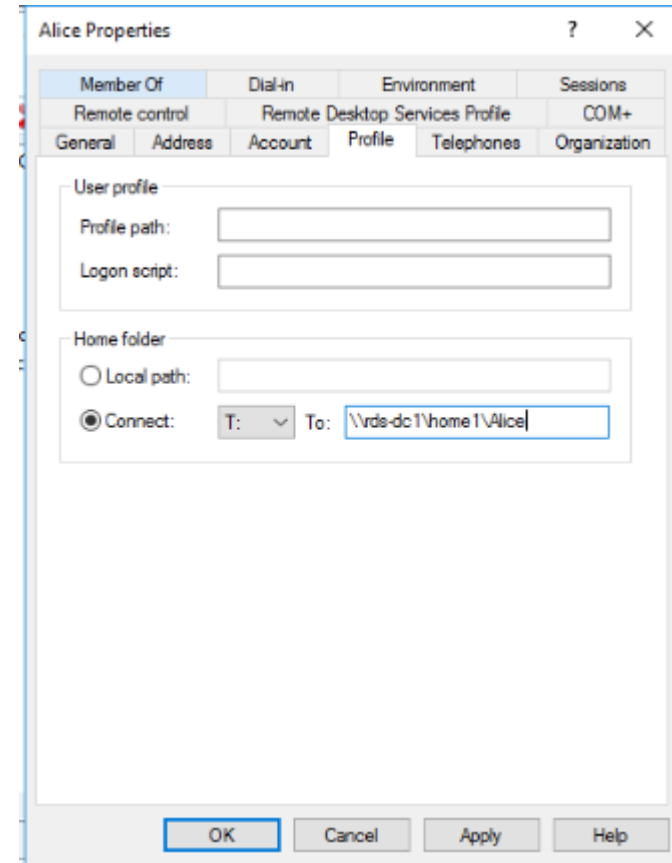
Module 8 – Anpassung der Benutzerumgebung

Module 8 – Anpassung der Benutzerumgebung

- Homedrive
- Benutzerprofile
- User State Virtualization
- User Experience Virtualization

Homedrive

- Konfiguration
 - › Gruppenrichtlinie
 - › Benutzerkonto
- Netzlaufwerk für jeden Benutzer
- Kein Ersatz für Gruppenlaufwerke



Benutzerprofile

Profilart	Beschreibung	Vor- und Nachteile
Roaming Profile	Servergespeichertes Profil	+ Persistenz + Anwendungskompatibilität - Profilladezeit - Last Write Wins
Mandatory Profile	Schreibgeschütztes Profil	+ Profilladezeit + Compliance - Keine Persistenz
Local Profile	Lokales Profile auf Session Host	+ Profilladezeit - Wechsel zwischen Servern - Profilsicherung

User State Virtualization

- Ordnerumleitung
- Umleitung bekannter Ordner in Netzwerkpfade
- Üblich für Dokumente, Downloads, Bilder, ...
- Verkleinert Benutzerprofile
- Probleme
 - › Latenzen
 - › Kompatibilität

User Experience Virtualization

- Anwendungsgesteuerte Sicherung von Benutzerdaten
- Agent lädt XML-basierte Vorlagen
- Sicherung von Anwendungsbezogenen Daten auf Netzwerkspeicherort
- Ab Windows 10 / Windows Server 2016 in Enterprise CAL
- Probleme
 - › Erstellung Anwendungsprofile
 - › Adoption

Module 5 – Zertifikate und PKI

- Zweck
- Termini
- Aufbau

Zweck

- Identifikation

- › Digitale Signatur

- Verschlüsselung

- › Symmetrisch

- › Verschlüsselung und Entschlüsselung mit identischem Key
- › Problem: Schlüsselübergabe

- › Asymmetrisch

- › Kombination privater und öffentlicher Schlüssel
- › Privater Schlüssel muss geschützt werden

Termini

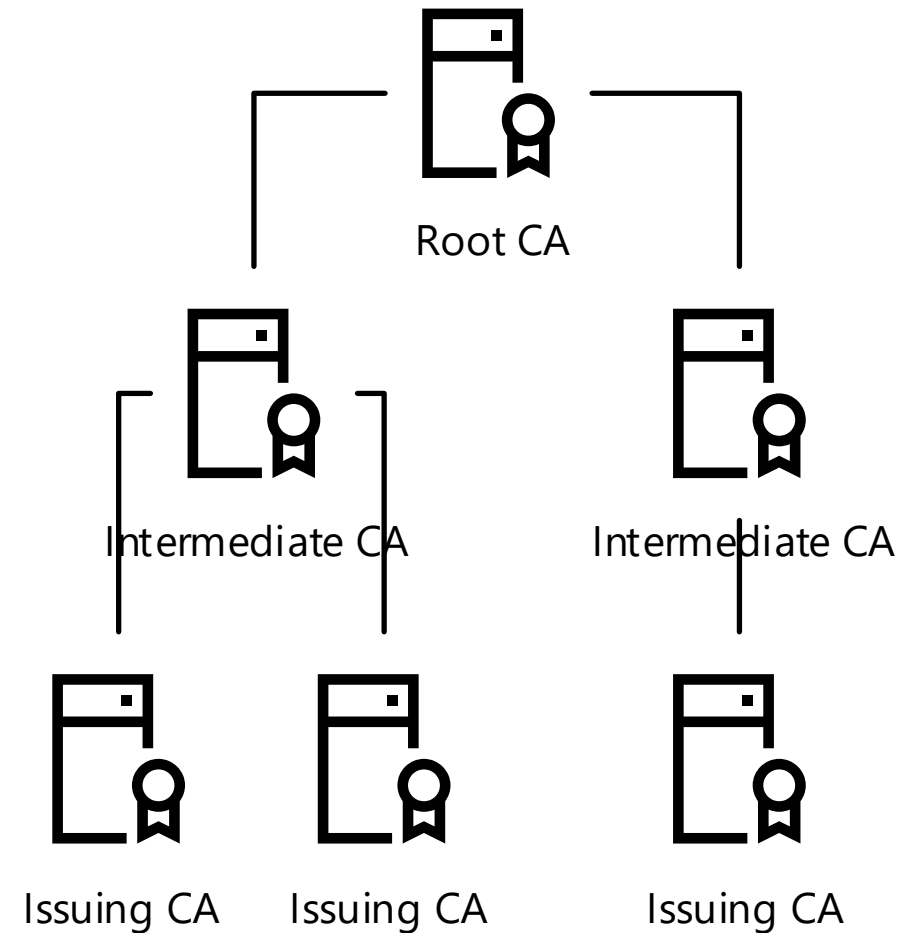
■ PKI

- › Public/Private Key Infrastructure
 - › Public
 - › Eigene Firma
 - › Erstellt Zertifikate gegen Bezahlung
 - › Globales Vertrauen
 - › Private
 - › Werden innerhalb der Unternehmen betrieben

Termini

- Hierarchie

- › Mehrere Zertifizierungsstellen stehen in Beziehung



Vertrauen

- Grundlage für Akzeptanz des Zertifikats
- In Windows:
 - › Public Key der Root CA in Trusted Root Certification Authorities
 - › Verifikation Certificate Revocation List

Arten privater CA

- Enterprise CA
 - › Active Directory-integriert
 - › Automatisches Vertrauen in Organisation
 - › Automatische Verteilung möglich
- Stand-Alone CA
 - › Manuelles Setup der CA/Zertifikate
- Empfehlung
 - › Kombination durch Stand-Alone Root und Enterprise-integrierte Intermediate CA

Übung 10 – Einrichtung einer CA

1. Anmeldung an RDS-CA1
2. Installation der CA-Rolle und Web Enrollment
3. Konfiguration:
 1. Enterprise CA
 2. Root CA
 3. Neuer privater Schlüssel
 4. Rest: Defaults

Revocation

- Zertifikate

- › Haben Ablaufdaten
- › Können zurückgezogen werden

- CRL

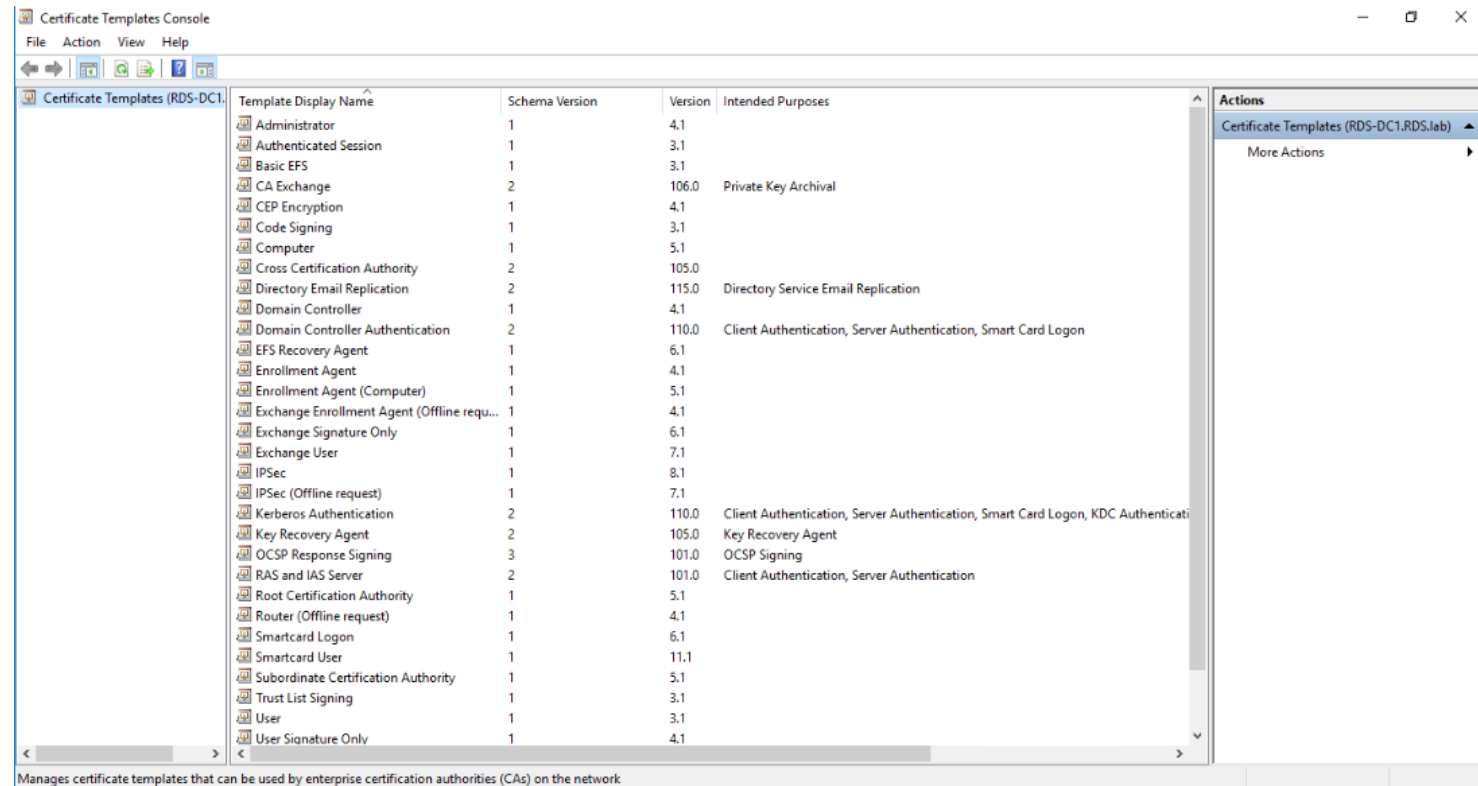
- › Vollständige Liste abgelaufener und zurückgezogener Zertifikate

- Certificate Revocation List Distribution Point

- › Punkt in Netzwerk, an welchem CRL geprüft werden kann
- › Mehrere Protokolle möglich
 - › FTP, HTTP, SMB, ...

Zertifikatsvorlagen

- Sammlung/Voreinstellung von Zertifikatseinstellungen
- Freigabe an CA
- Erfordert Berechtigungen zum Abruf



Übung 11 – Erstellung Zertifikatsvorlage

1. Anmeldung an RDS-DC1
2. Öffnung der Vorlagenkonsole
3. Duplikation Web Server Zertifikat als „RDP SSL Certificate“
4. Anpassung
 1. Sicherheit: Authenticated Users: Read/Enroll/Autoenroll
 2. Private Key: exportierbar
5. Publikation der neuen Vorlage an CA

Enrollment

- Vorgang des Ausfassens eines Zertifikats
- Methoden
 - › Certificate Snapin
 - › Browser: `http://<FQDN>/CertSrv`
 - › IIS Manager
 - › Gruppenrichtlinie
 - › Kommandozeile
 - › PowerShell
 - › ...

Übung 12 – Erstellung Zertifikate

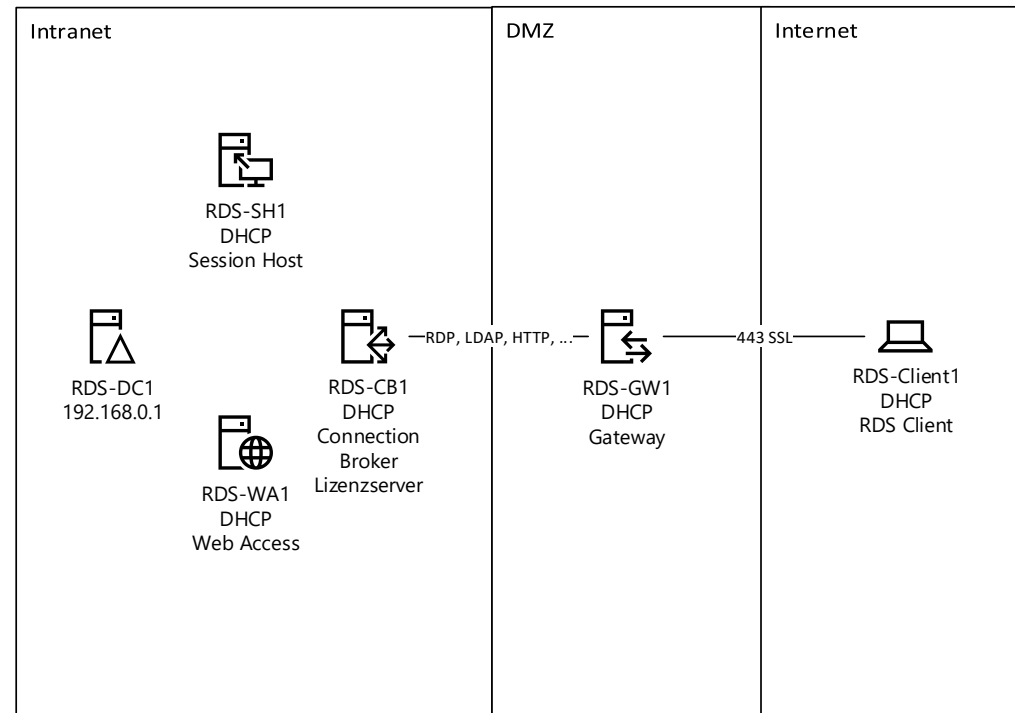
1. Anmeldung and RDS-GW1
2. Erstellung RDS SSL Zertifikat via Certificate Snapin
 1. Common Names: rds-gw1,rds-gw1.rds.lab
3. Anmeldung an RDS-WA1
 1. Erstellung Certificate Request in IIS Mgr (Achtung: Schlüssellänge)
 2. Erstellung Certificate Request in CA Website
 3. Download des Zertifikats
 4. Aktualisierung des SSL-Bindings
 5. Verifikation des SSL-Bindings

Module 6 – Remote Desktop Gateway

Module 6 – Remote Desktop Gateway

- Protokolle und Ports
- Anforderungen
- Umbau Labumgebung

Überblick



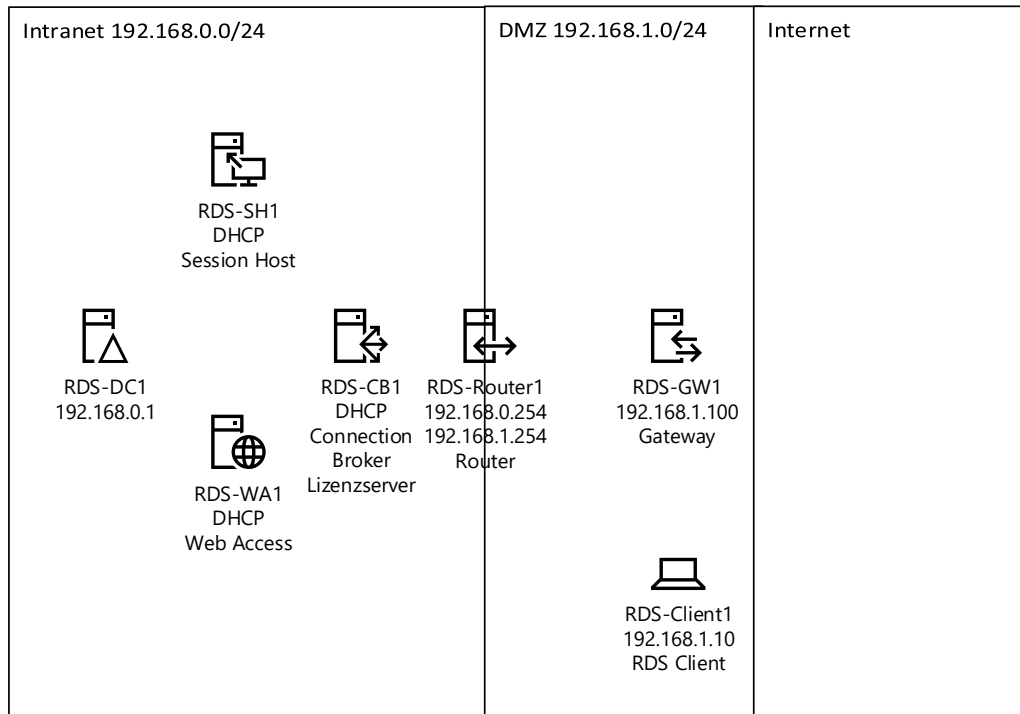
Protokolle und Ports

- Remote Desktop Gateway Transport
 - › Zwei SSL Tunnel
 - › Ingoing
 - › Outgoing
 - › Ältere Server: RPC over HTTP
- Ab 2012 HTTP Transport
 - › Für RDP 8.0
- Remote FX over UDP möglich

Firewall Remote Desktop Gateway

Interface	TCP/UDP	Port	Description
External	TCP	443	SSL
External	UDP	3391	Connection Creation
Internal	TCP	88	Kerberos
Internal	TCP	135	RPC Endpoint Mapper
Internal	UDP/TCP	389	LDAP
Internal	UDP/TCP	53	DNS
Internal	TCP/UDP	3389	RDP
Internal	TCP	80	HTTP
Internal	TCP	21	FTP
Internal	UDP	1812/1813	RADIUS

Übung 13 – Umbau Lab Umgebung



1. Import RDS-Router1
2. Rekonfiguration Netzwerkadapter
3. Aufbau und Verifikation Netzwerkverbindungen

Voraussetzungen RD Gateway

- IP-Konnektivität
 - › Routing, NAT, ...
- DNS-Auflösung für externe und interne Clients
 - › Split-Brain DNS
- Zertifikate
 - › Zertifikat muss vertraut werden
 - › CDP muss erreichbar sein

Überlegungen zur Platzierung von RDS Gateway

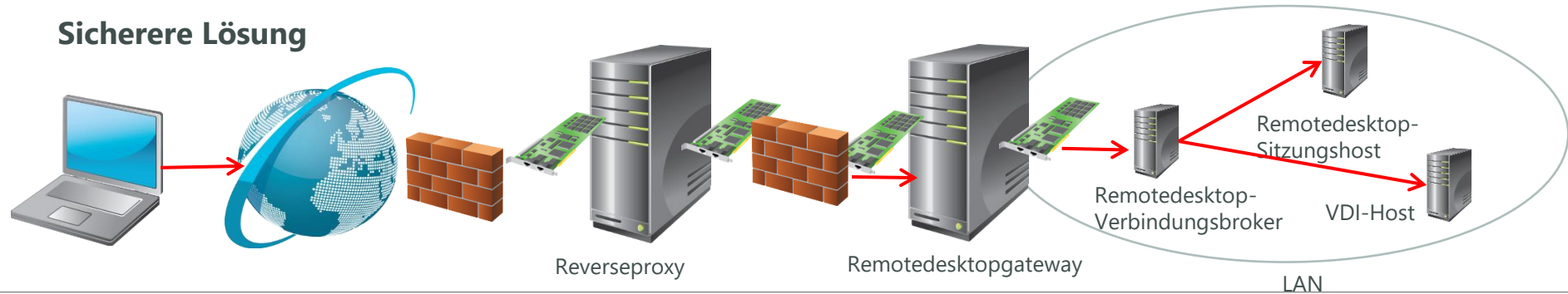
Einfach, aber nicht sicher



Sicher, aber zu komplex für SSO



Sicherere Lösung



Übung 14 – Installation RD Gateway

1. Anmeldung an RDS-CB1
2. Hinzufügen RDS-GW1 zu Server Manager
3. Installation RD Gateway-Rolle mit Selbst-signiertem Zertifikat

Übung 15 – Konfiguration RD Gateway

1. Erstellung Wildcard-Zertifikat auf RDS-GW1
2. Export des Zertifikats
3. Aktualisierung des RD Gateway-Zertifikats
4. Anpassung RDP-File auf RDS-Client1 zur Nutzung RD-Gateway
5. Aktualisierung Connection Broker SSO- und Publishing-Zertifikat mit Wildcard-Zertifikat
6. Verifikation der Verbindung über RD Gateway Manager auf RDS-GW1

Gateway Authorization Policies

- RD Connection Authorization Policies
 - › Welche Benutzer dürfen durch RD Gateway zugreifen?
- RD Resource Authorization Policies
 - › Welche Ressourcen dürfen durch RD Gateway zugreifen?
- Konfiguration über RD Gateway Manager

Module 7 – Konfiguration des RD Gateway

Module 7 – Konfiguration des RD Gateway

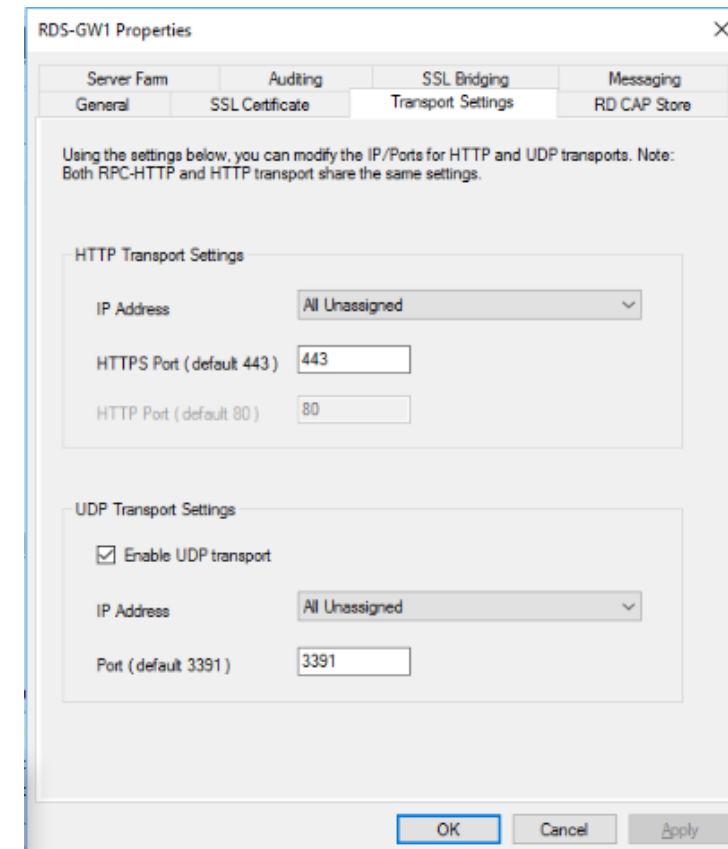
- SSL Bridging
- Port Konfiguration
- Messaging
- Gateway Farms
- Gruppenrichtlinien

SSL Bridging

- Erlaubt Firewall, eingehende Pakete zu inspizieren
- Terminiert SSL an Firewall
- Typen
 - › HTTPS-HTTPS
 - › Wiederverschlüsselung an Firewall
 - › SSL Zertifikat und privater Schlüssel auf Firewall benötigt
 - › HTTPS-HTTP
 - › Niedrigerer Overhead
 - › Konfiguration an RD Gateway Manager

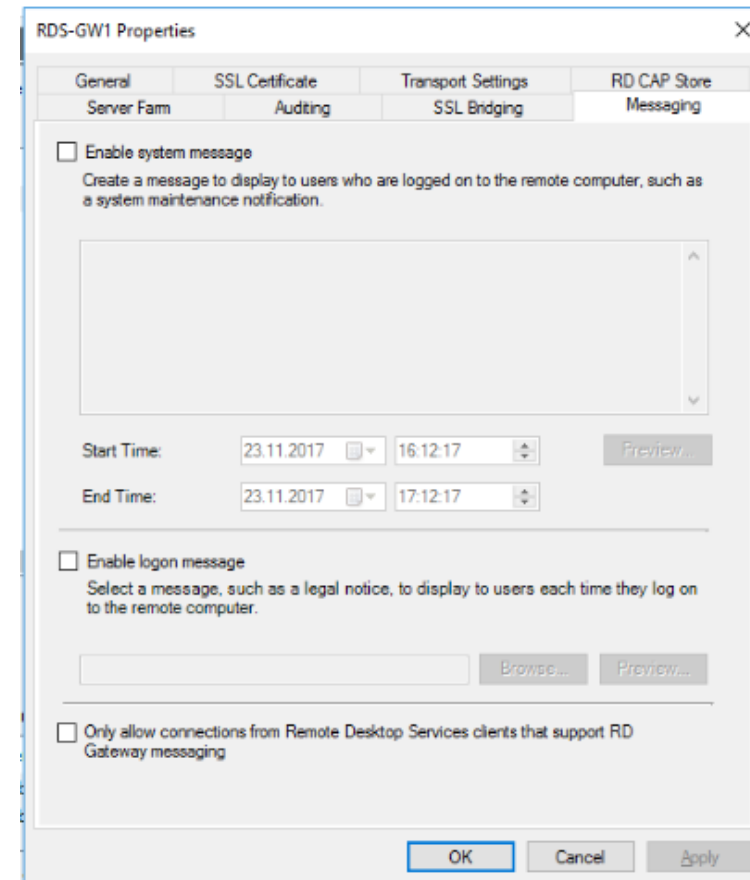
Anpassung Portkonfiguration

- Erfordert RDP Client 8.0
 - › Windows 8 oder Windows 7 mit aktualisiertem RDP-Client
- Anpassung der RDS Collection notwendig
 - › PowerShell
- Steuerung in RD Gateway Transport Settings



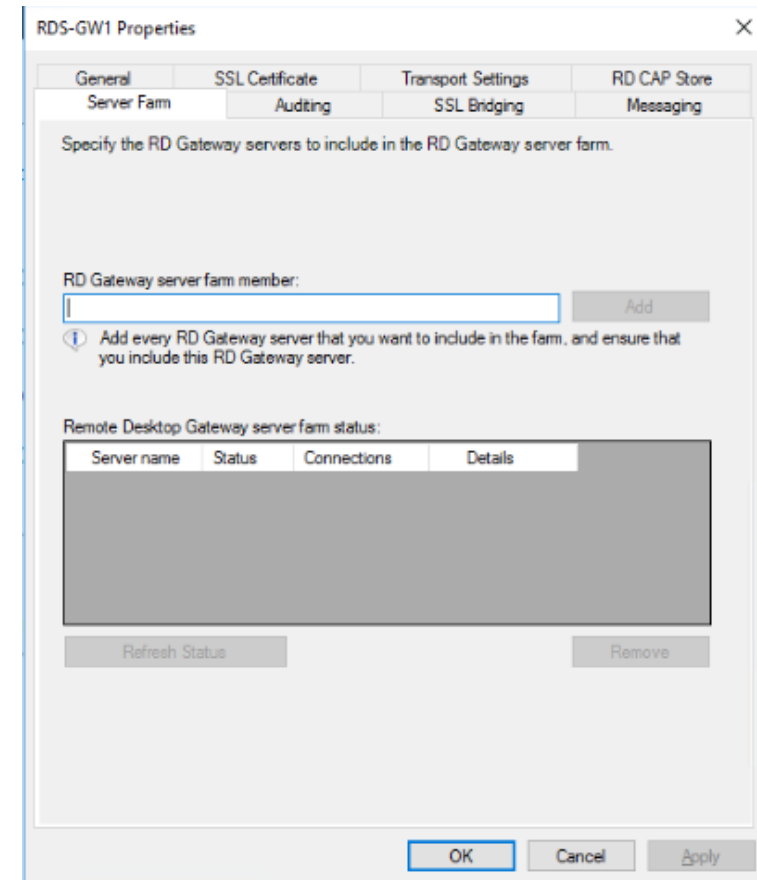
Messaging

- Logon Message
 - › Import einer Textdatei
 - › Anzeige bei jeder Anmeldung
- Maintenance Message
 - › Textfeld
 - › Anzeige in festem Zeitraum
 - › Anzeige in Session und auf Client
- Konfiguration in RD Gateway Manager



RD Gateway Farms

- Ermöglicht Hochverfügbarkeit für RD Gateway
- DNS Round Robin nicht mehr unterstützt
- Implementiert Network Load Balancing
- Server müssen in RD Gateway Manager hinzugefügt werden



Gruppenrichtlinien

- Benutzerkonfiguration

- › Administrative Vorlagen\Windows Komponenten\Remote Desktop Services\RD Gateway
- › Settings
 - › Gateway-Adresse
 - › Nutzung des Gateway
 - › Authentifizierungsmethoden

Vielen Dank für die
Aufmerksamkeit!

Bei fortführenden
Fragen zum
Terminalserver
Umgebungen,
sprechen Sie uns an!

Henrik Mai

Fon 0351 / 867700

Mail training@softed.de
projekte@softed.de

www.softed.de