Unterrichtseinheit 8:

Unterstützen des Remotezugriffs auf ein Netzwerk:

Der Routing und RAS-Dienst von Windows 2000 sowie der Internetauthentifizierungsdienst (IAS) von Windows 2000 verwenden beide RAS-Richtlinien (eine Gruppe von Bedingungen und Verbindungseinstellungen), um zu bestimmen, ob Verbindungsversuche angenommen oder verweigert werden.

Zugriffsversuch des Client

⇒ RAS-Richtlinie (Standard, Speziell) → *immer auf RAS-Server*

⇒ Einwahlberechtigung im Benutzerkonto → *z.B. Aktiv Directory*

⇒ Authentifizierungsvorgang

Untersuchen von RAS-Richtlienien

RAS-Richtlinien werden immer (auf der Serverseite) lokal und nicht im Aktiv Directory gespeichert. Eine RAS-Richtlinie besteht aus drei Komponenten, die mit dem Aktiv Directory zusammenarbeiten, um sicheren Zugriff auf RAS-Server bereit zu stellen:

- **Bedingungen**
  Die Bedingungen einer RAS-Richtlinie bilden eine Parameterliste, wie z.B. Tageszeit, Benutzergruppen, Anruferkennung oder IP-Adressen (Internetprotokoll), die mit den Parametern des Clients übereinstimmen müssen, der eine Verbindung zum Server herstellt.
- **Berechtigung**
  Kombination aus den Einwähleigenschaften eines Benutzerkontos und den RAS-Richtlinien. Die Berechtigungseinstellung einer RAS-Richtlinie arbeitet mit den Einwählrechten des Benutzers in Active Directory zusammen.
- **Profil**
  Jede Richtlinie schließt ein Profil mit Einstellungen ein, wie z.B. Authentifizierungs- und Verschlüsselungsprotokolle, die auf die Verbindung angewendet werden.

Folgen der Auswertungslogik von Richtlinien

⇒ siehe Graphik Kapitel 8 / Seite 5

RAS-Richtlinien werden folgendermaßen ausgewertet:

1. Routing und RAS vergleicht die Bedingungen der RAS-Richtlinie mit den Bedingungen des Verbindungsversuchs
2. Routing und RAS überprüft die Einwählrechte des Benutzerkontos
3. Routing und RAS wendet die Einstellungen im Richtlinienprofil auf die eingehende Verbindung an

Untersuchen von Standardrichtlinien

Die RAS-Standardrichtlinie hat keinen Einfluss auf eingehende Verbindungen, wenn sich die Domäne im gemischten Modus befindet. (Eine Domäne im gemischten Modus lässt Domänencontroller zu, die Windows 2000 oder NT 4.0 ausführen. Eine Domäne im einheitlichen Modus erfordert, dass alle Domänencontroller Windows 2000 ausführen.)

Die Standardrichtlinie lautet: ***Zugriff zulassen, wenn Einwählrechte erteilt worden sind***.

Einheitlicher Modus und eigenständige Server

Ist das Einwählrecht eines Benutzers auf **Zugriff gestatten** festgelegt, so werden alle Verbindungsversuche des jeweiligen Benutzers angenommen (im Benutzerkonto nachschauen)

Gemischter Modus

Die Standardrichtlinie wird in einer Domäne mit gemischten Modus immer außer Kraft gesetzt. Ist aber das Einwählrecht eines Benutzers auf **Zugriff gestatten** festgelegt, muss der Benutzer weiterhin die Bedingung einer Richtlinie (mindestens eine Richtlinie muss existieren) erfüllen um einen Zugriff zu erhalten.

Mehrere Richtlinien

Sind mehrere Richtlinien festgelegt, so wird immer die erste Richtlinie in der geordneten Liste der RAS-Richtlinien geprüft. Stimmen nicht alle Bedingungen der Richtlinie mit dem Verbindungsversuch überein, wird die nächste Richtlinie in der geordneten Liste überprüft, bis eine Richtlinie mit dem Verbindungsversuch übereinstimmt und anschließend mit Hinblick auf die Einstellungen des Profils und des Benutzerkontos ausgewertet. Treten hierbei Unstimmigkeiten auf, so wird der Verbindungsversuch zurückgewiesen – andere Richtlinien werden nicht überprüft.

⇒ RAS-Server
→ Benutzer
⇒ 1. Richtlinie → passt nicht; weiter
⇒ 2. Richtlinie → passt auf Benutzer ⇒ Profil widerspricht Benutzer
⇒ kein Zugriff
⇒ 3. Richtlinie → passt (wird nicht mehr angewendet)

Die 3. Richtlinie wird nicht mehr angewandt, da laut Auswertung die 2. Richtlinie passt und weitere Richtlinien nicht mehr abgefragt werden. Lösung des Problems: Richtlinienreihenfolge wechseln!

Wichtig:
Da Routing und RAS erfordert, dass mindestens die Bedingungen einer Richtlinie erfüllt sein müssen, werden alle Verbindungsversuche zurückgewiesen, wenn die Standardrichtlinie entfernt wird und keine andere Richtlinien vorhanden sind.

Konfigurieren von RAS-Richtlinienbedingungen

Eine RAS-Richtlinie besteht aus den Einwähleinstellungen des Benutzers, den RAS-Richtlinienbedingungen (Attribute, die mit den Einstellungen eines Verbindungsversuchs verglichen werden) und den RAS-Richtlinieneinstellungen.

Beispiel für Bedingungen von Verbindungsversuchen

- liegt zwischen 8.oo und 17.oo Uhr, Montag – Freitag
  und
- kommt von einer IP-Adresse, die 192.168.*.* entspricht
  und
- kommt von einem Benutzer der Gruppe „Sales“

Es können folgende RAS-Richtlinienbedingungen festgelegt werden:

- NAS-IP-Adress
- Service-Type
- Framed-Protocol
- Called-Station-ID
- Calling-Station-ID
- NAS-Identifier
- NAS-Port-Type
- Day-And-Time-Restrictions
- Client-IP-Adress
- Client-Vendor
- Client-Friendly-Name
- Windows-Groups
- Tunnel-Type

Um eine RAS-Richtlinie hinzuzufügen, muss folgendermaßen vorgegangen werden:
Programme → Verwaltung → Routing und RAS → mit rechter Maustaste auf RAS-Richtlinien → Neue RAS-Richtlinie → RAS-Richtlinie hinzufügen → Angezeigter Richtlinienname → Weiter → Hinzufügen → Attribut auswählen → Hinzufügen → Attributnamen eingeben *→ OK → Weiter → RAS-Berechtigungen erteilen* oder *RAS-Berechtigungen verweigern → Weiter → Fertig stellen*

Konfigurieren von RAS-Richtlinienbedingungen

Beispiel für Profileinstellungen

- 90 Minuten Verbindungszeit
  und
- vier Mehrfachverbindungsleitungen
  und
- erfordert IPSec-Verschlüsselung

Das RAS-Profil gibt an, welche Art Zugriff der Benutzer erhält, falls die Bedingungen erfüllt werden.

Ein Profil kann mit folgendenden Parametern konfiguriert werden:

- Einwähleinschränkungen
- IP
- Mehrfachverbindungen
- Authentifizierung
- Verschlüsselung
- Weitere Optionen

Überwachen des Remotezugriffs

Ereignisprotokolle
Das Windows 2000-Ereignisprotokoll enthält Informationen zu Systemkomponenten in Windows 2000 und sollte daher als erster überprüft werden, um Informationen zu einem Problem zu erhalten.
Arbeitsplatz → Verwalten → Computerverwaltung → Ereignisanzeige → System → RemoteAccess → Quelle

Modemprotokollierung
Windows 2000 Professional zeichnet während einer Verbindung automatisch ein Protokoll der Datenübertragung von Computer zu einem Modem auf. Bei Windows 2000 Server und Advanced Server muss die Protokolldatei manuell aktiviert werden.
Systemsteuerung → Telefon- und Modenoptionen → Modems → auf das zu konfigurierende Modem klicken → Eigenschaften → Diagnose → aktivieren von „Protokoll aufzeichnen", bzw. „An Protokoll anhängen" → OK
Um das Protokoll anzuzeigen muss man auf der Registerkarte *Diagnose* auf *Protokoll anzeigen* klicken.

Verfolgen des Ablaufs von RAS-Verbindungen

Windows 2000 verfügt über eine umfangreiche Ablaufverfolgungsmöglichkeit, mit der komplexe Netzwerkprobleme behandelt werden können. Die Ablaufverfolgungs-möglichkeiten müssen unter folgendem Registry-Schlüssel geändert werden: (siehe Kapitel 8/Seite25-26)

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing

Wert:	**Datentyp:**
EnableFileTracing	REG_DWORD (auf 1 festlegen) um Ablaufverfolgungsinformationen in einer Datei zu aktivieren (Standard 0)
FileDirectory	REG_EXPAND_SZ (Speicherortinformationen)
FileTracingMask	REG_DWORD (festlegen, wie viele Ablaufverfolgungsinformationen protokolliert werden)
MaxFileSize	REG_DWORD (Größe der Protokolldatei – Standard 64kB)

Da Ablaufverfolgungen sehr viel Systemressourcen benötigen, dürfen diese keinesfalls auf Computern mit mehreren Prozessoren aktiviert werden und sollten nur kurzzeitig zum Erkennen von Fehlern im Netzwerk verwendet werden.