

Unterrichtseinheit 4

Erstellen und Verwalten von Benutzerkonten:

Benutzerkonten enthalten eindeutige Informationen eines Benutzers und ermöglichen diesem die Anmeldung und somit den Zugriff auf lokale und Domänen-Ressourcen.
(Ist man mit einem normalen Benutzeraccount angemeldet, kann man trotzdem als Administrator fungieren: *Start → Einstellungen → Systemsteuerung → System → Verwaltung → mit rechter Maustaste und gedrückter Umschalttaste auf Active Directory-Benutzer und -Computer klicken → Ausführen als*)

Lokale Benutzerkonten:

ermöglichen einem Benutzer die Anmeldung an einem bestimmten Computer, um Zugriff auf dessen Ressourcen zu erhalten. Die Benutzerkonten befinden sich im SAM des Computers.

Domänenbenutzerkonten:

ermöglichen einem Benutzer die Anmeldung an einer Domäne, um Zugriff auf Netzwerkressourcen zu erhalten. Die Domänenbenutzerkonten befinden sich im Active Directory.

Vordefinierte Benutzerkonten:

ermöglichen einem Benutzer die Ausführung von Verwaltungsaufgaben, bzw. den temporären Zugriff auf Netzwerkressourcen. Diese Konten befinden sich sowohl im SAM (vordefinierte lokale Benutzerkonten), als auch im Active Directory (vordefinierte Domänenbenutzerkonten).

Es stehen zwei vordefinierte Benutzerkonten zur Verfügung, die nicht gelöscht werden können: **Administrator** und **Gast**. Diese werden automatisch während der Installation von W2K und Active Directory erstellt.

Namenskonventionen:

Die Namenskonvention legt fest, wie Benutzerkonten in der Domäne identifiziert werden.

- Benutzeranmeldenamen müssen im Active Directory, vollständige Namen innerhalb der Domäne und lokale auf dem Computer eindeutig sein.
- Benutzeranmeldenamen können eine Kombination aus bis zu 20 speziellen und alphanumerischen Zeichen, sowohl in Groß-, als auch in Kleinschreibung enthalten. (*Ausnahmen: „/\[]: / =, + * ? < >*)
- die Namenskonvention sollte Benutzer, welche den gleichen Namen besitzen und temporäre Benutzer identifizieren können

Kennwortrichtlinien:

Um den Zugriff auf die Domäne oder einen Computer zu schützen, sollte jedem Benutzerkonto ein komplexes Kennwort zugewiesen werden.

- dem Konto Administrator sollte stets ein Passwort zugewiesen werden, um unautorisierten Zugriff zu verhindern
- der Administrator legt fest, ob Benutzer das Kennwort selbstständig ändern können oder nicht
- es können bis zu 128 Zeichen mit einer Kombination aus Groß- und Kleinbuchstaben, sowie aus speziellen und alphanumerischen Zeichen verwendet werden. (Mindestlänge von 8 Zeichen in komplexer Form wird empfohlen)

Kontooptionen:

Benutzerkontooptionen legen fest, wie ein Benutzer auf die Domäne oder einen Computer zugreifen kann.

- die Anmeldezeiten sollten nach den Arbeitszeiten des Benutzers festgelegt werden
- um die Sicherheit zu erhöhen, können Domänenbenutzer auf bestimmte Computer eingeschränkt werden; standardmäßig können sie sich an jedem Computer der Domäne anmelden
- es kann eine Ablaufzeit für ein Benutzerkonto festgelegt werden, damit sich dieses automatisch nach dem Ablaufdatum deaktiviert

Erstellen eines lokalen Benutzerkontos:

Ein lokales Benutzerkonto wird nur in kleineren Netzwerkumgebungen, wie Arbeitsgruppen, oder alleinstehenden Computern, welche nicht an ein Netzwerk angeschlossen sind, verwendet. Es wird in der SAM-Datenbank des Computers gespeichert und ermöglicht dem Benutzer, auf seine lokalen Ressourcen zugreifen zu können.

(Start → Programme → Verwaltung → Computerverwaltung → erweitern von Lokale Benutzern und Gruppen → rechte Maustaste auf Benutzer → Neuer Benutzer → Kennwort eingeben und bestätigen → Kennwortschränkungen festlegen → Erstellen)

Verwaltungsprogramme von Windows 2000:

Verwaltungsprogramme (befinden sich auf der W2K-Server CD und sind standardgemäß auf einem Domänencontroller installiert) für die Remoteverwaltung von Domänencontrollern (nur mit Administratorrechten möglich) können von jedem W2K-Rechner aus installiert werden.

(Explorer → Ordner I386 → Adminpak.msi → nach der Installation : Start → Programme → Verwaltung)

(Aus Sicherheitsgründen sollte man sich als normaler Benutzer anmelden und sich für die Verwaltungsaufgaben mit **Ausführen als** als Administrator verbinden lassen)

Erstellen eines Domänenbenutzerkontos:

Ein Domänenbenutzerkonto befindet sich auf einem Domänencontroller und wird automatisch auf alle anderen Domänencontroller repliziert).

Um ein Domänenbenutzerkonto (im Standardordner **Users**) zu erstellen, muß folgendes beachtet werden:

- öffnen des **Active Directory-Benutzer und –Computer** vom Menü **Verwaltung** aus
- rechte Maustaste auf den Ordner, der das Benutzerkonto enthalten soll, dann auf **Neu** und **User** klicken.

Konfigurierbare Optionen:

- Vorname / Nachname / Initialen
- Vollständiger Name: dieser Name muß innerhalb des Ordners, in dem das Konto erstellt wird, eindeutig sein.
(W2K vervollständigt diesen Eintrag selbstständig, wenn der Vor- und Nachname eingegeben wurde)
- Benutzeranmeldename: dieser eindeutige Anmeldename des Benutzers ist erforderlich und muss im Active Directory eindeutig sein.
Benutzeranmeldenamen für WindowsNT 3.5x/4.0 werden verwendet, um eine Anmeldung von vorherigen Versionen von Windows durchzuführen und müssen innerhalb der Domäne eindeutig sein (max. 20 Zeichen)

Verwalten von Benutzerdaten durch das Erstellen von Basisordnern:

Bei den Basisordnern für Benutzer handelt es sich um einen zentralen Netzwerkspeicherort für jeden einzelnen User.

Beim Festlegen dieses Basisordners sollten folgende Punkte berücksichtigt werden:

- um Datenverluste zu verhindern, ist eine Datensicherung/-wiederherstellung unvermeidlich. Um viel effizienter arbeiten zu können, empfiehlt es sich, die Dateien an einem zentralen Speicherort auf einem Server abzulegen.
- auf dem Server muß genügend Speicherplatz für die Benutzerdaten zur Verfügung stehen. Durch die Datenträgerkontingente bietet W2K eine präzise Kontrolle über den zu verwendenden Festplattenspeicherplatz.
- es muß auf dem Benutzercomputer ausreichend Speicherplatz vorhanden sein.
- befindet sich der Basisordner auf dem lokalen Computer des Benutzers, so entsteht zwar weniger Netzwerkverkehr, macht aber eine zentrale Datensicherung durch den Administrator nahezu unmöglich.

Eigenschaften für Domänenbenutzerkonten:

Um im Active Directory nach Benutzern zu suchen, können definierte Eigenschaften im Domänenbenutzerkonto angegeben werden. Man kann z.B. nach einer Person suchen, indem man als Kriterium die Telefonnummer, den Arbeitsplatz, den Namen des Vorgesetzten oder den Nachnamen eingibt. Aus diesem Grund sollten für jedes Domänenbenutzerkonto, welches erstellt wird, detaillierte Eigenschaftsdefinitionen angegeben werden.

Um diese persönlichen Eigenschaften festzulegen, müssen folgende Schritte ausgeführt werden:

- öffnen des **Active Directory-Benutzer und -Computer** vom Menü **Verwaltung** aus
- Domäne auswählen und auf entsprechenden Ordner klicken, um die verfügbaren Domänenbenutzerkonten anzuzeigen
- rechte Maustaste auf das jeweilige Domänenbenutzerkonto
- **Eigenschaften** und dann die jeweilige Registerkarte auswählen

Eigenschaften für Domänenbenutzerkonten:

Das Festlegen von Anmeldeoptionen für ein Domänenbenutzerkonto ermöglicht, die Anmeldezeiten (sinnvoll vor allem in einem Regierungsnetzwerk und in Umgebungen mit mehreren Schichten) und die Computer, in, bzw. von denen sich ein Benutzer anmelden kann, zu steuern.

Verbindungen zu Netzwerkressourcen in der Domäne werden allerdings nicht getrennt, wenn die Anmeldezeiten des Benutzers ablaufen. Der Benutzer kann jedoch keine neuen Verbindungen zu anderen Computern in der Domäne herstellen.

Kopieren von Domänenbenutzerkonten:

Es kann nur ein Benutzerkonto auf einem Domänencontroller, nicht aber auf einem W2K-Computer kopiert werden.

Folgende Eigenschaften werden beim Kopieren in das neue Benutzerkonto übertragen:

- **Allgemein / Rufnummern:** es werden keine Eigenschaften kopiert
- **Adresse:** alle außer Straße
- **Konto:** alle außer Anmeldename
- **Profil:** alle außer Profilpfad und Basisordner
- **Organisation:** alle außer Anrede
- **Mitglied von:** alle
- **Einwählen / Umgebung / Sitzungen / Remoteüberwachung / Terminaldienstprofile:** es werden keine Eigenschaften kopiert, sondern nur Standardeinstellungen angewendet.

Achtung: Rechte und Berechtigungen, die einem einzelnen Benutzerkonto erteilt werden, werden nicht in das neue Benutzerkonto kopiert!

Erstellen von Benutzerkonten (User Template):

Eine Benutzerkontenvorlage (Domänenbenutzerkonto, in dem das Kontrollkästchen **Konto ist deaktiviert** aktiviert ist) ist ein Standardbenutzerkonto, welches die Eigenschaften enthält, die auf Benutzer mit gemeinsamen Anforderungen angewendet werden.

Bei der Erstellung von Vorlagen sind folgende Richtlinien zu beachten:

- es sollte eine Vorlage für jede Klassifizierung von Mitarbeitern erstellt werden
- für Mitarbeiter, die das Netzwerk nur für kurze Zeit oder temporär nutzen, sollte eine Vorlage mit beschränkten Anmeldezeiten, Arbeitsstationsspezifikationen und anderen notwendigen Beschränkungen erstellt werden

Um die Vorlage stets oben in der Liste im Detailfensterbereich des **Active Directory-Benutzer und -Computer** anzeigen zu lassen, sollte man die Vorlagenamen mit einem _ beginnen lassen.

Um eine Vorlage zur Erstellung eines neuen Benutzerkontos zu verwenden, wird das Vorlagenkonto kopiert und ein Benutzername, ein Kennwort und die entsprechenden Änderungen in den Benutzerkontoeigenschaften eingestellt. Das Kontrollkästchen **Konto ist deaktiviert** muss deaktiviert werden, um das Benutzerkonto dem Benutzer zur Verfügung zu stellen.

Anpassen von Benutzereinstellungen mit Benutzerprofilen

Unter W2K wird die Computerumgebung eines Benutzers hauptsächlich durch das Benutzerprofil bestimmt, da dieses alle Einstellungen, welche der Benutzer für seine Arbeitsumgebung benötigt, enthält.

Ein solches Benutzerprofil wird erstellt, wenn sich ein Benutzer zum ersten Mal an einem Computer anmeldet. Alle benutzerspezifischen Einstellungen werden automatisch im Ordner des Benutzers innerhalb des Ordners **C:\Dokumente und Einstellungen\Benutzername** gespeichert.

Die Aktualisierung des Profils auf dem Computer erfolgt beim Abmelden des Benutzers.

Profiltypen:

Standardbenutzerprofil: dient als Basis für alle Benutzerprofile. Den Anfang für jedes Benutzerprofil bildet eine Kopie des Standardbenutzerprofils, das auf jedem Computer unter W2K gespeichert ist.

Lokales Benutzerprofil: wird erstellt und auf dem lokalen Computer gespeichert, wenn sich ein Benutzer zum ersten Mal an einem Computer anmeldet. Alle Änderungen, die am lokalen Benutzerprofil vorgenommen werden sind spezifisch für den Computer, an dem die Änderungen vorgenommen wurden. Auf einem Computer können mehrere lokale Benutzerprofile vorhanden sein.

Servergespeichertes Benutzerprofil: wird vom Systemadministrator erstellt und auf einem Server gespeichert. Dieses Profil ist jedes Mal verfügbar, wenn sich ein Benutzer an einem Computer im Netzwerk anmeldet. Bei Änderungen des Profils werden diese beim Abmelden im Benutzerprofil auf dem Server aktualisiert.

Verbindliches Benutzerprofil: wird vom Systemadministrator erstellt, um eine bestimmte Einstellung für Benutzer anzugeben. Dieses Profil kann sowohl lokal-, als auch servergespeichert sein. Ein verbindliches Benutzerprofil ermöglicht einem Benutzer zwar, Änderungen an seinen Desktopeinstellungen vorzunehmen, diese aber nicht zu speichern.

Erstellen eines servergespeicherten Benutzerprofils:

- 1) Erstellen eines freigegebenen Ordners (mit der Berechtigung Vollzugriff) auf einem Server
- 2) Angabe des Pfades für diesen Ordner.

Start → Einstellungen → Systemsteuerung → System → Verwaltung → Active Directory-Benutzer und -Computer → mit rechter Maustaste auf entsprechendes Benutzerkonto klicken → Eigenschaften → Profil → im Benutzerprofil die Pfadinformationen eingeben

(\\Servername\Name des freigegebenen Ordners\Benutzername) → Profilpfad

Statt Benutzername kann die Variable **%username%** angegeben werden, da W2K diese automatisch mit dem Benutzerkontennamen für das servergespeicherte Profil ersetzt.

Ein servergespeichertes Benutzerprofil kann nur von einem Administrator geändert werden. Die Datei **Ntuser.dat** (im Profilordner des Benutzers) enthält den Abschnitt der Registrierung, der für das Benutzerkonto (Benutzerprofileinstellungen) gilt.

Erstellen eines verbindlichen servergespeicherten Benutzerprofils:

- 1) Erstellen eines freigegebenen Ordners mit einem Profilordner (mit der Berechtigung Vollzugriff) für das Benutzerprofil auf einem Server.
- 2) Ein konfiguriertes, servergespeichertes Benutzerprofil einrichten, indem ein neuer Benutzer im **Active Directory-Benutzer und -Computer** erstellt und darin die Pfadangabe aus 1) eingestellt wird.
Um dieses Profil zu konfigurieren ist es notwendig, sich an der Domäne mit dem eben erstellten Profil anzumelden, die Einstellungen vorzunehmen und sich anschließend wieder abzumelden.
- 3) Die Profildatei **Ntuser.dat** muss nun in **Ntuser.man** umbenannt werden, da hiermit das Profil schreibgeschützt und somit verbindlich wird.

Die Datei **Ntuser.dat** wird im Profilordner des Benutzers nicht angezeigt.

Um sie anzuzeigen, müssen folgende Schritte ausgeführt werden:

Windows Explorer starten → Extras → Ordneroptionen → Ansicht → Erweiterte Einstellungen → Alle Dateien und Ordner anzeigen → das Kontrollkästchen „Dateinamenerweiterung bei bekannten Dateitypen ausblenden“ deaktivieren → OK

Optimale Methoden für das Erstellen und Verwalten von Benutzerprofilen:

- Umbenennen des Administratorkontos
- Erstellen eines Benutzerkontos mit Administratorrechten
- Erstellen eines Benutzerkontos für nicht administrative Aufgaben
- Aktivieren des Kontos „Gast“ mit Vergabe eines Passwortes nur in Netzwerken mit niedriger Sicherheit
- Erstellen zufälliger anfänglicher Kennwörter
- Auffordern von neuen Benutzern, ihre Kennwörter zu ändern
- Festlegen von Benutzerkonto-Ablaufdaten für temporäre Mitarbeiter