Microsoft®
Training &
Certification

Microsoft® Official
Curriculum

Unterrichtseinheit 4: Implementieren von Benutzer-, Gruppen- und Computerkonten

Inhalt

Microsoft®

Hinweise für Kursleiter

Präsentation:
120 Minuten

Übungseinheit:
60 Minuten

In dieser Unterrichtseinheit werden den Kursteilnehmern die Kenntnisse und Fähigkeiten vermittelt, die erforderlich sind, um Benutzer-, Gruppen- und Computerkonten im Active Directory®-Verzeichnisdienst unter Microsoft® Windows Server™ 2003 zu planen und zu implementieren. In der Unterrichtseinheit wird erklärt, wie mehrere Benutzer- und Computerkonten mithilfe von Befehlszeilenprogrammen (z. B. Csvde und Ldifde) erstellt und mithilfe von Windows Script Host verwaltet werden. Darüber hinaus wird erläutert, wie Benutzerprinzipalnamen-Suffixe implementiert werden.

Am Ende dieser Unterrichtseinheit werden die Kursteilnehmer in der Lage sein, die folgenden Aufgaben auszuführen:

- Beschreiben der Typen von Active Directory-Konten und –gruppen.
- Erstellen mehrerer Benutzer- und Computerkonten.
- Implementieren von Benutzerprinzipalnamen-Suffixen.
- Verschieben von Objekten innerhalb einer Domäne und zwischen den Domänen in einer Gesamtstruktur.
- Planen einer Strategie für Benutzer-, Gruppen- und Computerkonten.
- Planen einer Active Directory-Überwachungsstrategie.

Erforderliche Unterlagen

Um diese Unterrichtseinheit zu unterrichten, benötigen Sie folgende Unterlagen:

- Microsoft PowerPoint®-Datei 2195A_04.ppt

Vorbereitende Aufgaben

So bereiten Sie diese Unterrichtseinheit vor:

- Lesen Sie alle Unterlagen für diese Unterrichtseinheit. Überlegen Sie sich, welche Fragen während dieser Unterrichtseinheit von den Kursteilnehmern gestellt werden können, und bereiten Sie die Antworten darauf vor.
- Arbeiten Sie die Übungseinheit durch.
- Gehen Sie die praktischen Übungen, die Bewertungsfragen sowie die vorgeschlagenen Antworten durch. Bereiten Sie sich auf andere Antworten der Kursteilnehmer vor, und überlegen Sie sich, was Sie dazu sagen.

Schulungsraum-einrichtung

Dieser Abschnitt enthält Informationen zur Einrichtung, die für die Vorbereitung des Kursleitercomputers bzw. der Schulungsraumkonfiguration für eine Übungseinheit erforderlich sind.

► **Bereiten Sie die Übungseinheit vor**

- Führen Sie die Windows Script Host-Datei UpnSuffixes.vbs auf dem Server London aus, bevor die Kursteilnehmer mit der Übungseinheit für diese Unterrichtseinheit beginnen. Die Datei befinden Sie im Ordner Setup auf der Kursleiter-CD.

Vermitteln dieser Unterrichtseinheit

Dieser Abschnitt enthält Informationen, die Ihnen beim Unterrichten dieser Unterrichtseinheit helfen.

Wichtig Diese Unterrichtseinheit enthält Bewertungspunkte für jede Lektion, die sich auf der Kursteilnehmer-CD befindet. Sie können sie bereits vorab zur Einstufung hinzuziehen, um Problemfelder zu ermitteln, oder Sie können damit bei einer abschließenden Bewertung den Lernerfolg überprüfen.

Es empfiehlt sich, am Tagesende den Lehrstoff anhand dieser Bewertungspunkte zu vertiefen. Sie können jedoch auch morgens die den Kursteilnehmern am Vortag vermittelten Kenntnisse anhand dieser Punkte überprüfen.

Lassen Sie den Kursteilnehmern 10 Minuten Zeit für die Bearbeitung der Bewertungsfragen. Sie können die Fragen und Antworten gemeinsam durchgehen oder die Kursteilnehmer bitten, den Bewertungsteil alleine zu beantworten.

Anmerkung Einige Themen verweisen auf zusätzliche Informationen in den Anhängen. Diese Kenntnisse werden zur Ausführung des Übungs- und Bewertungsteils dieser Unterrichtseinheit nicht vorausgesetzt. Sehen Sie sich jedoch vor der Unterrichtung dieses Kurses die Informationen auf der Seite Anhänge der Kursteilnehmer-CD an. Weisen Sie die Kursteilnehmer während des Unterrichts auf die zusätzlichen Informationen auf der Seite Anhänge hin.

Anleitungen, praktische Übungen und Übungseinheiten

Erklären Sie den Kursteilnehmern, wie die Anleitungen, praktischen Übungen und Übungseinheiten für diesen Kurs beschaffen sind. Eine Unterrichtseinheit besteht aus mindestens zwei Lektionen. Die meisten Lektionen beinhalten Anleitungen und eine praktische Übung. Nachdem die Kursteilnehmer die Lektionen bearbeitet haben, wird die Unterrichtseinheit mit einer Übungseinheit abgeschlossen.

Anleitungen

Die Anleitungen sollen Sie dabei unterstützen, die Ausführung einer Aufgabe zu veranschaulichen. Die Kursteilnehmer lösen die Aufgaben in der Anleitung nicht zusammen mit dem Kursleiter. Mit diesen Schritten führen sie die praktische Übung am Ende der einzelnen Lektionen aus.

Praktische Übungen

Nachdem Sie ein Thema besprochen und die Anleitungen der Lektion vorgeführt haben, erklären Sie den Kursteilnehmern, dass sie in den praktischen Übungen die Gelegenheit haben, alle in der Lektion behandelten Aufgaben in der Praxis durchzuführen.

Übungseinheiten

Am Ende jeder Unterrichtseinheit können die Kursteilnehmer die in der Unterrichtseinheit behandelten Aufgaben in einer Übungseinheit üben.

Jede Übungseinheit stellt ein Beispiel aus der Praxis dar. Zu diesem Beispiel erhalten die Kursteilnehmer eine Reihe von Anweisungen in Form einer Tabelle mit zwei Spalten. In der linken Spalte wird die Aufgabe gestellt (Beispiel: Erstellen Sie eine Gruppe.). Die rechte Spalte enthält spezifische Anweisungen zum Ausführen der Aufgabe (Beispiel: Doppelklicken Sie in Active Directory-Benutzer und -Computer auf den Domänenknoten.).

Falls die Kursteilnehmer schrittweise Anleitungen zum Bearbeiten der Übungseinheit benötigen, finden sie auf der Kursteilnehmer-CD Antworten zu jeder Übungseinheit. Sie können auch die praktischen Übungen und Anleitungen der Unterrichtseinheit durchgehen.

Lektion: Einführung in Konten

In diesem Abschnitt werden die didaktischen Methoden zum Unterrichten der einzelnen Themen in dieser Lektion beschrieben.

Die Informationen in dieser Lektion sind Voraussetzung für diesen Kurs. Verwenden Sie die Informationen im Thema „Kontotypen“ als Übersicht.

Konzentrieren Sie sich beim Thema „Gruppentypen“ auf Sicherheitsgruppen. Es genügt, wenn die Kursteilnehmer den Zweck von Verteilergruppen kennen.

Bei den Themen „Was sind lokale Domänengruppen?“, „Was sind globale Gruppen?“ und „Was sind universelle Gruppen?“ müssen Sie sicherstellen, dass die Kursteilnehmer verstehen, wann sie die verschiedenen Gruppentypen verwenden müssen.

Praktische Übung

Für diese Lektion gibt es keine praktische Übung.

Lektion: Erstellen und Verwalten mehrerer Konten

Beim Thema „Tools zum Erstellen und Verwalten mehrerer Konten“ müssen Sie sicherstellen, dass sich die Kursteilnehmer darüber im Klaren sind, dass die Konten bei der Verwendung von Csvde zum Erstellen von Konten leere Kennwörter haben.

Demonstrieren Sie die Verfahren zum Erstellen von Konten mithilfe der Befehlszeilenprogramme Csvde und Ldifde. Verweisen Sie die Kursteilnehmer auf die Anhänge, die eine Liste der häufig verwendeten Optionen für Csvde enthalten. Erstellen Sie ein Windows Script Host-Beispielskript, das ein Benutzerkonto zu Active Directory hinzufügt. Verweisen Sie die Kursteilnehmer auf die Anhänge, die ein Beispielskript zum Erstellen eines Benutzerkontos enthalten.

Praktische Übung

Am Ende dieser Lektion erstellen die Kursteilnehmer eine Skriptdatei, die Befehle zum Erstellen von drei Benutzerkonten enthält. Anschließend führen sie die Skriptdatei aus und überprüfen mithilfe von Active Directory-Benutzern und -Computern, ob die Benutzer erstellt wurden.

Lektion: Implementieren von Benutzerprinzipalnamen-Suffixen

Beim Thema „Was ist ein Benutzerprinzipalname?“ müssen Sie sicherstellen, dass die Kursteilnehmer die Vorteile der Verwendung von Benutzerprinzipalnamen und die Regeln zur Eindeutigkeit von Benutzeranmeldenamen verstehen.

Fassen Sie die Hauptpunkte am Ende der Multimediapräsentation „Funktionsweise des Namensuffixroutings“ zusammen.

Demonstrieren Sie das Erstellen und Entfernen eines Benutzerprinzipalnamen-Suffixes. Demonstrieren Sie außerdem das Aktivieren und Deaktivieren des Namensuffixroutings in Vertrauensstellungen.

Praktische Übung

Am Ende dieser Lektion erstellen die Kursteilnehmer ein Namensuffix für eine Domäne zweiter Ebene und aktivieren das Namensuffixrouting in zwei Gesamtstrukturen.

Lektion: Verschieben von Objekten in Active Directory

Das Verschieben von Active Directory-Objekten, wie z. B. Benutzerkonten, hat schwerwiegende Auswirkungen. Wenn beispielsweise ein Benutzerkonto verschoben wird, kann der Benutzer alle E-Mail-Nachrichten verlieren. Beim Thema „Auswirkungen der Objektverschiebung“ müssen Sie sicherstellen, dass die Kursteilnehmer diese Auswirkungen verstehen.

Demonstrieren Sie bei den Themen „Anleitung: Verschieben von Objekten innerhalb einer Domäne“ und „Anleitung: Verschieben von Objekten zwischen Domänen“, wie Objekte innerhalb einer Domäne und zwischen Domänen verschoben werden.

Demonstrieren Sie außerdem die Verwendung von LDP.exe zum Anzeigen der Eigenschaften verschobener Objekte.

Praktische Übung

Am Ende dieser Lektion verschieben die Kursteilnehmer ein Benutzerkonto von einer Domäne in eine andere und zeigen anschließend die Sicherheitskennung (Security Identifier, SID), den SID-Verlauf und die Eigenschaften für den Globally Unique Identifier (GUID) an, um zu überprüfen, ob diese Eigenschaften geändert wurden.

Lektion: Planen einer Strategie für Benutzer-, Gruppen- und Computerkonten

Diese Lektion behandelt Richtlinien zum Benennen von Konten, zum Erstellen einer Kennwortrichtlinie und zum Entwickeln von Strategien für Gruppen sowie zur Kontoauthentifizierung, -autorisierung und -verwaltung.

Regen Sie eine Gruppendiskussion zu diesen Themen an. Vereinfachen Sie diese Diskussionen vorsichtig, damit die Kursteilnehmer die Diskussionen verfolgen können und damit nicht zu viel Zeit für dieses Thema aufgewendet wird.

Praktische Übung

Am Ende dieser Lektion planen die Kursteilnehmer auf der Grundlage eines fiktiven Szenarios eine Strategie zum Benennen von Konten, eine Kennwortrichtlinie, eine Authentifizierungs-, Autorisierungs- und Verwaltungsstrategie sowie eine Gruppenstrategie für eine Gesamtstruktur.

Lektion: Planen einer Active Directory-Überwachungsstrategie

Diese Lektion behandelt die Richtlinien zur Überwachung von Änderungen an Active Directory.

Bringen Sie bei den Themen dieser Lektion persönliche Erfahrungen bei der Planung einer Überwachungsstrategie ein, um die Informationen in den Themen zu vertiefen.

Praktische Übung

Am Ende dieser Lektion planen die Kursteilnehmer eine Überwachungsstrategie auf der Grundlage eines Szenarios.

Übungseinheit A: Implementieren einer Konten- und Überwachungsstrategie

In dieser Übungseinheit planen und implementieren die Kursteilnehmer eine Kontenstrategie. Sie erstellen mehrere Benutzerkonten mithilfe des Befehlszeilenprogramms Csvde. Die Kursteilnehmer erstellen darüber hinaus ein Benutzerprinzipalnamen-Suffix und beheben anschließend Probleme bei Benutzerprinzipalnamen-Suffixroutingkonflikten zwischen zwei Gesamtstrukturen. Schließlich verschieben die Kursteilnehmer, die paarweise zusammenarbeiten, eine Benutzergruppe zwischen den entsprechenden Domänen und zeigen die Änderungen an den SID- und den SID-Verlaufseigenschaften der verschobenen Konten an.

Anpassungsinformationen

Dieser Abschnitt befasst sich mit den Konfigurationsanforderungen der Übungseinheiten für eine Unterrichtseinheit und den Konfigurationsänderungen, die während den Übungseinheiten an den Kursteilnehmercomputern vorgenommen werden. Diese Informationen sollen Ihnen beim Replizieren oder Anpassen der Microsoft Official Curriculum-Courseware (MOC) helfen.

Wichtig Die Übungseinheit in dieser Unterrichtseinheit ist auch von der Schulungsraumkonfiguration abhängig, die im Abschnitt „Anpassungsinformationen“ am Ende des Handbuchs für das Einrichten von Schulungscomputern für Kurs 2195A, *Planen, Implementieren und Warten einer Active Directory-Infrastruktur unter Microsoft Windows Server 2003*, angegeben ist.

Konfiguration der Übungseinheit

In der folgenden Liste sind die Konfigurationsanforderungen für die Übungseinheit dieser Unterrichtseinheit beschrieben.

Konfigurations-anforderung 1

Bei den Übungseinheiten dieser Unterrichtseinheit muss jeder Kursteilnehmercomputer als Domänencontroller in seiner eigenen Gesamtstruktur konfiguriert sein. Um die Kursteilnehmercomputer auf diese Anforderungen vorzubereiten, führen Sie zunächst die manuelle oder die automatisierte Einrichtung für diesen Kurs aus. Führen Sie anschließend die Übungseinheiten in Unterrichtseinheit 2, „Implementieren einer Active Directory-Gesamt- und Domänenstruktur“, im Kurs 2195A, *Planen, Implementieren und Warten einer Active Directory-Infrastruktur unter Microsoft Windows Server 2003*, aus.

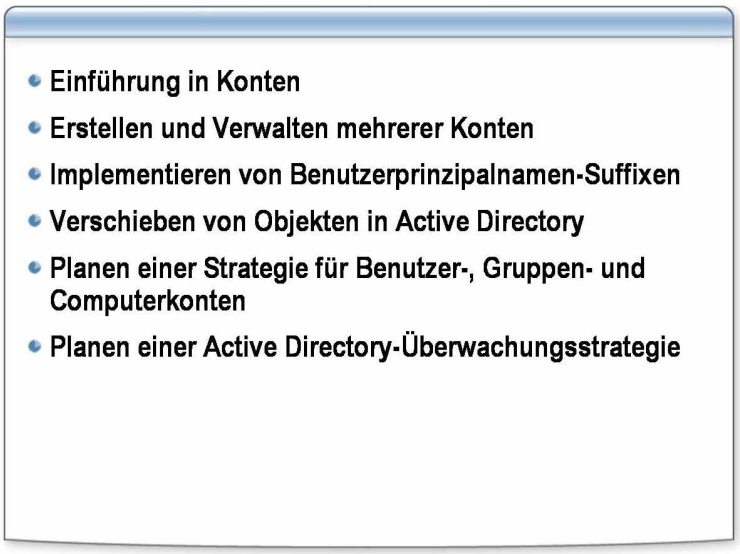
Ergebnisse der Übungseinheit

Durch Ausführen der Übungseinheit in dieser Unterrichtseinheit werden die folgenden Konfigurationsänderungen vorgenommen:

- Die folgenden Organisationseinheiten werden in jeder Kursteilnehmerdomäne erstellt:
  - IT Admin
    - IT Users
    - IT Groups
  - NWTraders Groups
    - Domain Local
    - Global
    - Universal
  - IT Test
    - IT Test Move

- In jeder Kursteilnehmerdomäne wird eine globale Gruppe G IT Admins erstellt.
- Es werden 26 lokale Domänengruppen DL *ComputerName* OU Administrators erstellt.
- Es wird eine lokale Domänengruppe DL IT OU Administrators erstellt.
- Es werden 26 Benutzer mit dem Namen ComputernameAdmin erstellt.
- Es werden zwei Benutzerprinzipalnamen-Suffixe *ComputerName* zu jeder Gesamtstruktur der Kursteilnehmer hinzugefügt (eines für jeden Kursteilnehmercomputer in der Gesamtstruktur).

Übersicht



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

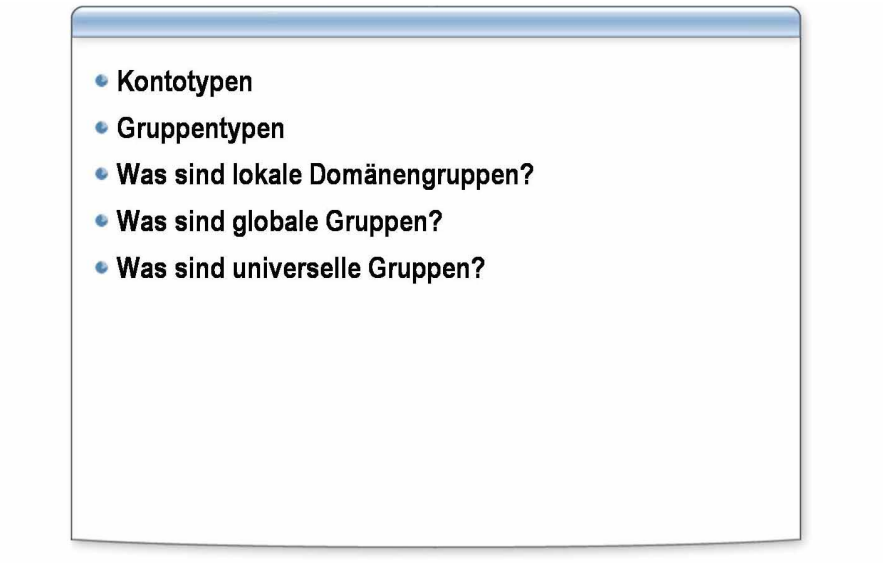
In dieser Unterrichtseinheit erfahren Sie, wie Sie Benutzer-, Gruppen- und Computerkonten im Active Directory®-Verzeichnisdienst planen und implementieren. Sie erfahren außerdem, wie Sie mehrere Benutzer- und Computerkonten erstellen und wie Sie Benutzerprinzipalnamen-Suffixe implementieren.

Lernziele der Lektion

Am Ende dieser Unterrichtseinheit werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Beschreiben der Typen von Active Directory-Konten und –gruppen.
- Erstellen mehrerer Benutzer- und Computerkonten.
- Implementieren von Benutzerprinzipalnamen-Suffixen.
- Verschieben von Objekten innerhalb einer Domäne und zwischen den Domänen in einer Gesamtstruktur.
- Planen einer Strategie für Benutzer-, Gruppen- und Computerkonten.
- Planen einer Active Directory-Überwachungsstrategie.

Lektion: Einführung in Konten



Einführung

In dieser Lektion werden die Konten- und Gruppentypen beschrieben, die Sie unter Microsoft® Windows Server™ 2003 erstellen können. Darüber hinaus wird das Verhalten von globalen, domänenlokalen und universellen Gruppen erläutert.

Lernziele

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Beschreiben der Kontotypen, die unter Windows Server 2003 erstellt werden können.
- Beschreiben der Gruppentypen, die unter Windows Server 2003 erstellt werden können.
- Beschreiben des Verhaltens von lokalen Domänengruppen.
- Beschreiben des Verhaltens von globalen Gruppen.
- Beschreiben des Verhaltens von universellen Gruppen.

Kontotypen

**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

In Active Directory können drei Kontotypen erstellt werden: Benutzer-, Gruppen- und Computerkonten. Active Directory-Benutzer- und Computerkonten stellen eine physische Einheit dar, wie z. B. ein Computer oder eine Person. Sie können Benutzerkonten bei manchen Anwendungen auch als dedizierte Dienstkonten verwenden.

Benutzerkonten

Ein *Benutzerkonto* ist ein in Active Directory gespeichertes Objekt, das ein *einmaliges Anmelden* ermöglicht. Das bedeutet, dass ein Benutzer seinen Namen und sein Kennwort nur einmal eingibt, wenn er sich für einen authentifizierten Zugriff auf Netzwerkressourcen an einer Arbeteitsstation anmeldet.

Es gibt drei Typen von Benutzerkonten, die jeweils eine bestimmte Funktion haben:

- Bei einem *lokalen Benutzerkonto* kann sich der Benutzer an einem bestimmten Computer anmelden, um auf die Ressourcen dieses Computers zuzugreifen.
- Bei einem *Domänenbenutzerkonto* kann sich ein Benutzer an der Domäne anmelden, um auf die Netzwerkressourcen zuzugreifen, oder er kann sich an einem einzelnen Computer anmelden, um auf die Ressourcen des Computers zuzugreifen.
- Bei einem *vordefinierten Benutzerkonto* kann ein Benutzer Verwaltungsaufgaben ausführen oder vorübergehend auf Netzwerkressourcen zugreifen.

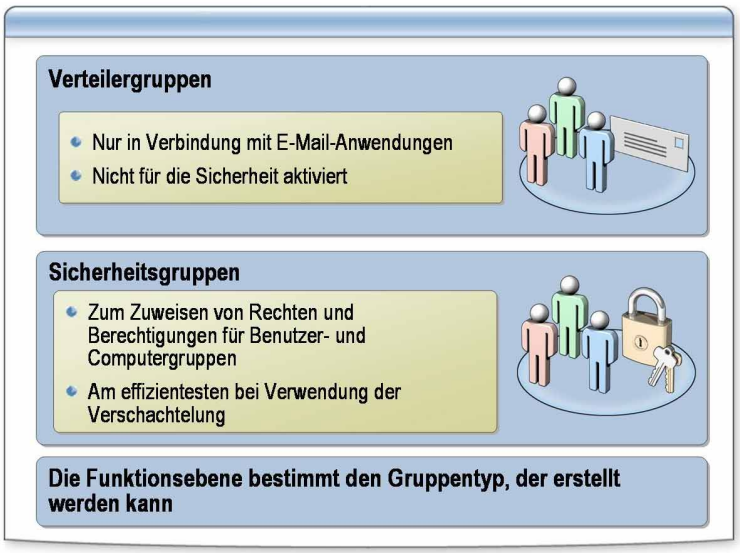
Computerkonten

Alle Computer, die unter Microsoft Windows NT®, Microsoft Windows 2000 oder Microsoft Windows XP ausgeführt werden, oder Server, die unter Microsoft Windows Server 2003 laufen und zu einer Domäne gehören, verfügen über ein *Computerkonto*. Ähnlich Benutzerkonten, bieten Computerkonten eine Möglichkeit, den Computerzugriff auf das Netzwerk und auf Domänenressourcen zu authentifizieren und zu überwachen. Jedes Computerkonto muss eindeutig sein.

Gruppenkonten

Ein *Gruppenkonto* ist eine Sammlung von Benutzern, Computern oder anderen Gruppen. Sie können den Zugriff auf Domänenressourcen mithilfe von Gruppen effizient verwalten, was die Verwaltung vereinfacht. Beim Verwenden von Gruppen weisen Sie einzelnen Benutzern Berechtigungen für freigegebene Ressourcen, wie Ordner und Drucker, nur einmal und nicht mehrmals zu.

Gruppentypen



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

In Active Directory gibt es zwei Gruppentypen, Verteilergruppen und Sicherheitsgruppen. Beide verfügen über ein Bereichsattribut, das festlegt, wer Mitglied der Gruppe sein kann und wo diese Gruppe in einem Netzwerk verwendet werden darf. Sie können eine Gruppe jederzeit von einer Sicherheitsgruppe in eine Verteilergruppe und umgekehrt konvertieren. Dies ist jedoch nur möglich, wenn die Domänenfunktionsebene auf Windows 2000 pur oder höher festgelegt wurde.

Verteilergruppen

Sie können Verteilergruppen nur in Verbindung mit E-Mail-Anwendungen, wie Microsoft Exchange, verwenden, um Nachrichten an Benutzergruppen zu senden. Verteilergruppen sind nicht *für die Sicherheit aktiviert*. Das bedeutet, dass sie nicht in Discretionary Access Control Lists (DACLs) aufgeführt werden dürfen. Erstellen Sie eine Sicherheitsgruppe, um den Zugriff auf freigegebene Ressourcen zu steuern.

Sicherheitsgruppen

Sicherheitsgruppen werden verwendet, um Benutzer- und Computergruppen Rechte und Berechtigungen zuzuweisen. Rechte legen fest, welche Funktionen die Mitglieder einer Sicherheitsgruppe in einer Domäne oder einer Gesamtstruktur ausführen können. Berechtigungen legen fest, auf welche Netzwerkressourcen ein Gruppenmitglied zugreifen darf.

Eine Möglichkeit zur effizienten Nutzung von Sicherheitsgruppen besteht in der Verwendung von *Verschachtelung*, d. h. dem Hinzufügen einer Gruppe zu einer anderen Gruppe. Die verschachtelte Gruppe erbt die Berechtigungen der Gruppe, zu der sie gehört. Dies vereinfacht die gleichzeitige Zuweisung von Berechtigungen zu mehreren Gruppen und reduziert den Datenverkehr, der durch die Replikation von Änderungen an der Gruppenmitgliedschaft entsteht. Im Modus für gemischte Domänen können keine Gruppen verschachtelt werden, die denselben Gruppenbereich aufweisen.

Sowohl Verteiler- als auch Sicherheitsgruppen unterstützen einen der drei folgenden Gruppenbereiche: lokal (in Domäne), global oder universell. Die Domänenfunktionsebene bestimmt den Gruppentyp, der erstellt werden kann. Im gemischten Modus von Windows 2000 dürfen keine universellen Sicherheitsgruppen erstellt werden.

Was sind lokale Domänengruppen?

**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Eine lokale Domänengruppe ist eine Sicherheits- oder Verteilergruppe, die universelle Gruppen, globale Gruppen, andere lokale Domänengruppen der eigenen Domäne sowie Konten aus allen anderen Domänen in der Gesamtstruktur enthalten kann. In lokalen Domänensicherheitsgruppen können Sie Rechte und Berechtigungen für Ressourcen erteilen, die nur in der Domäne vorhanden sind, in der sich die lokale Domänengruppe befindet.

So könnten Sie z. B. eine lokale Domänensicherheitsgruppe mit den Namen Setup erstellen und der Gruppe Berechtigungen für eine Freigabe namens Setup auf einem der Mitgliedsserver in der Domäne erteilen. Sie könnten globale und universelle Gruppen als Mitglieder der lokalen Domänengruppe Setup hinzufügen. Die Mitglieder wären dann berechtigt, auf den freigegebenen Ordner Setup zuzugreifen.

Mitgliedschaft, Bereich und Berechtigungen in lokalen Domänengruppen

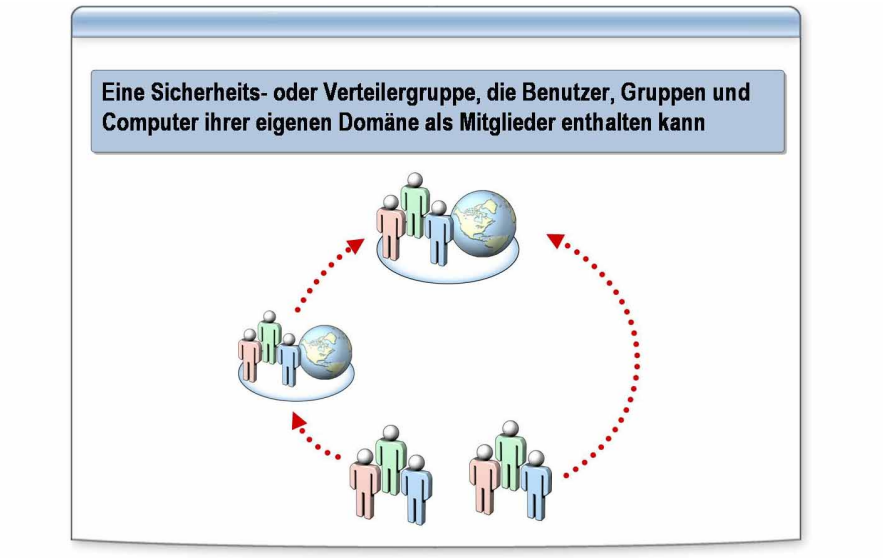
Die folgenden Regeln gelten für Mitgliedschaft, Bereich und Berechtigungen in lokalen Domänengruppen:

- *Mitgliedschaft*. Im gemischten Modus von Windows 2000 können lokale Domänengruppen Benutzerkonten und globale Gruppen aus beliebigen Domänen enthalten. Im Modus Windows 2000 pur können lokale Domänengruppen Benutzerkonten, globale Gruppen, universelle Gruppen aus allen vertrauenswürdigen Domänen sowie lokale Domänengruppen aus derselben Domäne enthalten.
- *Kann Mitglied sein von*. Im gemischten Modus von Windows 2000 kann eine lokale Domänengruppe kein Mitglied einer Gruppe sein. Im Modus Windows 2000 pur kann eine lokale Domänengruppe Mitglied lokaler Domänengruppen derselben Domäne sein.
- *Bereich*. Eine lokale Domänengruppe ist nur in ihrer eigenen Domäne sichtbar.
- *Berechtigung für*. Sie können eine Berechtigung zuweisen, die für die Domäne gilt, in der sich die lokale Domänengruppe befindet.

Verwendung von lokalen Domänengruppen

Verwenden Sie eine lokale Domänengruppe, wenn Sie Zugriffsberechtigungen für Ressourcen erteilen möchten, die sich in der Domäne befinden, in der Sie die lokale Domänengruppe erstellen. Sie können alle globale Gruppen, die dieselben Ressourcen gemeinsam nutzen müssen, zur passenden lokalen Domänengruppe hinzufügen.

Was sind globale Gruppen?



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Eine globale Gruppe ist eine Sicherheits- oder Verteilergruppe, die Benutzer, Gruppen und Computer ihrer eigenen Domäne als Mitglieder enthalten kann. Sie können globalen Sicherheitsgruppen Rechte und Berechtigungen für Ressourcen in jeder Domäne der Gesamtstruktur erteilen.

Verwenden Sie eine globale Gruppe zum Organisieren von Benutzern, die dieselben beruflichen Aufgaben ausführen und ähnliche Anforderungen an den Netzwerkzugriff haben, wie z. B. alle Buchhalter in der Buchhaltungsabteilung einer Organisation.

Mitgliedschaft, Bereich und Berechtigungen in globalen Gruppen

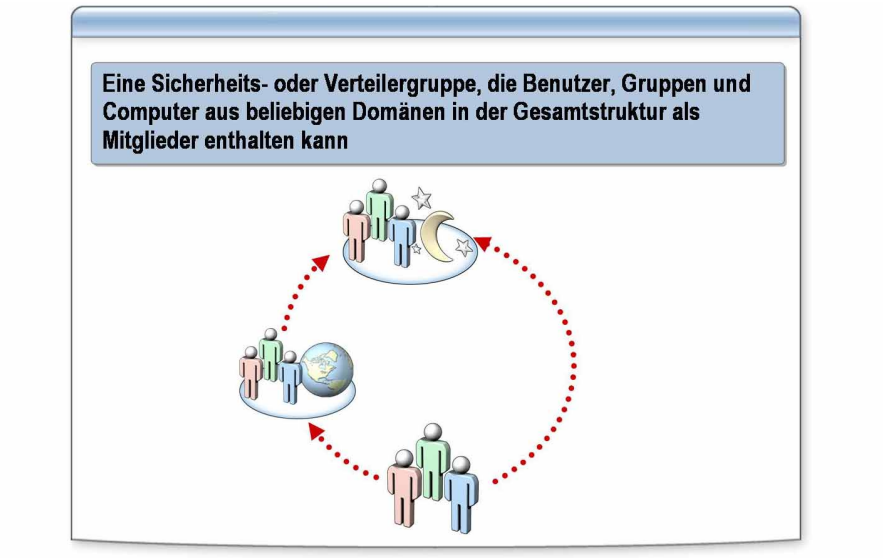
Die folgenden Regeln gelten für Mitgliedschaft, Bereich und Berechtigungen in globalen Gruppen:

- *Mitgliedschaft*. Im gemischten Modus von Windows 2000 kann eine globale Gruppe Benutzerkonten von derselben Domäne enthalten. Im Modus Windows 2000 pur und im Windows Server 2003-Modus können globale Gruppen Benutzerkonten und globale Gruppen derselben Domäne enthalten.
- *Kann Mitglied sein von*. Im gemischten Modus von Windows 2000 kann eine globale Gruppe Mitglied einer lokalen Domänengruppe jeder vertrauenswürdigen Domäne sein. Im Modus Windows 2000 pur und im Windows Server 2003-Modus kann eine globale Gruppe Mitglied universeller und lokaler Domänengruppen in jeder Domäne und von globalen Gruppen in derselben Domäne sein.
- *Bereich*. Eine globale Gruppe ist in ihrer Domäne und allen vertrauenswürdigen Domänen sichtbar, die alle Domänen in der Gesamtstruktur umfassen.
- *Berechtigungen*. Sie können einer globalen Gruppe Berechtigungen zuweisen, die für alle vertrauenswürdigen Domänen gelten.

Verwendung globaler Gruppen

Da globale Gruppen in der ganzen Gesamtstruktur sichtbar sind, sollten Sie sie nicht dazu verwenden, um Benutzern Zugriff auf domänenspezifische Ressourcen zu gewähren. Verwenden Sie globale Gruppen zum Organisieren von Benutzern oder Benutzergruppen. Eine lokale Domänengruppe ist besser geeignet, um den Benutzerzugriff auf die Ressourcen in einer einzelnen Domäne zu steuern.

Was sind universelle Gruppen?



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Eine universelle Gruppe ist eine Sicherheits- oder Verteilergruppe, die Benutzer, Gruppen und Computer aus allen Domänen in ihrer Gesamtstruktur als Mitglieder enthalten kann. Universellen Sicherheitsgruppen können Rechte und Berechtigungen für Ressourcen in allen Domänen der Gesamtstruktur gewährt werden.

Mitgliedschaft, Bereich und Berechtigungen in universellen Gruppen

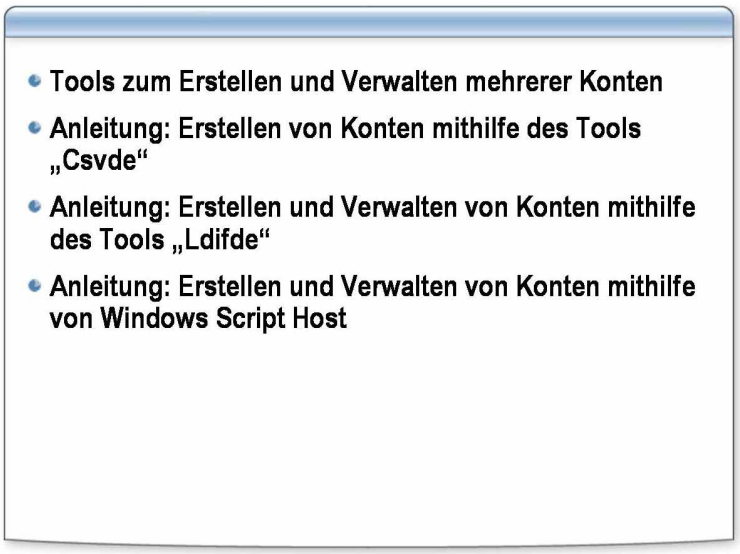
Die folgenden Regeln gelten für Mitgliedschaft, Bereich und Berechtigungen in universellen Gruppen:

- *Mitgliedschaft*. Im gemischten Modus von Windows 2000 können keine universellen Sicherheitsgruppen erstellt werden. Im Modus Windows 2000 pur und im Windows Server 2003-Modus können universelle Gruppen Benutzerkonten, globale Gruppen und andere universelle Gruppen aus allen Domänen in der Gesamtstruktur enthalten.
- *Kann Mitglied sein von*. Die universelle Gruppe kann im gemischten Modus von Windows 2000 nicht angewendet werden. Im Modus Windows 2000 pur kann eine universelle Gruppe Mitglied domänenlokaler und universeller Gruppen aus allen Domänen sein.
- *Bereich*. Universelle Gruppen sind in allen Domänen der Gesamtstruktur sichtbar.
- *Berechtigungen*. Sie können einer universellen Gruppe Berechtigungen zuweisen, die für alle Domänen in der Gesamtstruktur gelten.

Verwendung universeller Gruppen

Verwenden Sie universelle Gruppen, wenn Sie globale Gruppen verschachteln möchten. Auf diese Weise können Sie Berechtigungen für zugehörige Ressourcen in mehreren Domänen zuweisen. Eine Windows Server 2003-Domäne muss sich im Modus Windows 2000 pur oder im Windows Server 2003-Modus befinden, um universelle Sicherheitsgruppen verwenden zu können. Sie können universelle Verteilergruppen in einer Windows Server 2003-Domäne verwenden, die sich im gemischten Modus von Windows 2000 oder in einem höheren Modus befindet.

Lektion: Erstellen und Verwalten mehrerer Konten



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

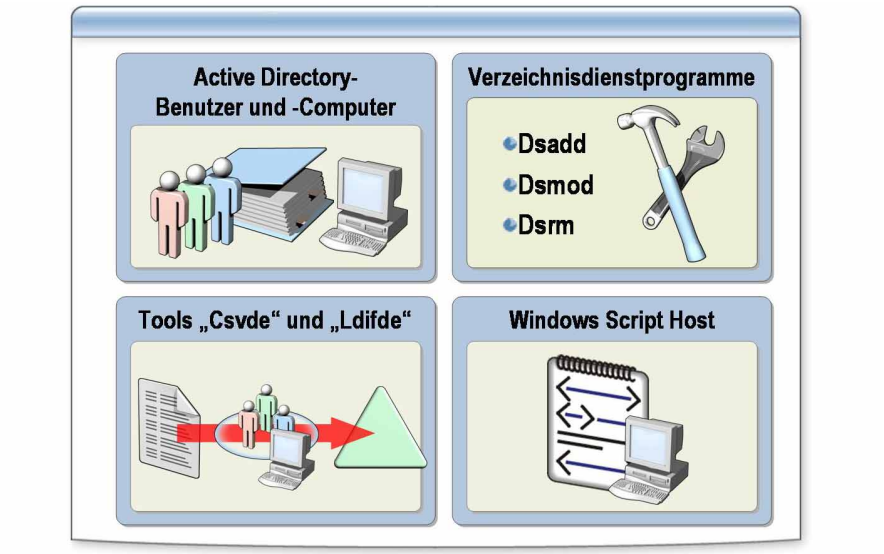
In dieser Lektion werden die verschiedenen Befehlszeilenprogramme beschrieben, mit denen Sie mehrere Benutzerkonten erstellen und verwalten können.

Lernziele der Lektion

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Beschreiben der Tools zum Erstellen und Verwalten mehrerer Konten.
- Verwenden des Befehlszeilenprogramms Csvde zum Erstellen von Konten.
- Verwenden des Befehlszeilenprogramms Ldifde zum Erstellen und Verwalten von Konten.
- Erstellen und Verwalten von Konten mithilfe von Windows Script Host.

Tools zum Erstellen und Verwalten mehrerer Konten



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Windows Server 2003 bietet eine Reihe von Microsoft Management Console- (MMC-) Snap-Ins und -Tools, mit denen automatisch mehrere Benutzerkonten in Active Directory erstellt werden können. Bei einigen dieser Tools müssen Sie eine Textdatei verwenden, die Informationen über die zu erstellenden Benutzerkonten enthält. Sie können auch Skripts zum Hinzufügen oder zum Ändern von Objekten in Active Directory verwenden.

Active Directory Benutzer und -Computer

Active Directory-Benutzer und -Computer ist ein MMC-Snap-In, mit dem Sie Benutzer-, Computer- und Gruppenkonten verwalten können. Verwenden Sie dieses Snap-In, wenn nur wenige Konten verwaltet werden müssen.

Verzeichnisdienst-programme

Sie können auch die Befehlszeilenprogramme Dsadd, Dsmod und Dsrm zum Verwalten von Benutzer-, Computer- und Gruppenkonten in Active Directory verwenden. Sie müssen den Objekttyp angeben, den Sie erstellen, ändern oder löschen möchten. Verwenden Sie z. B. den Befehl **dsadd user** zum Erstellen eines Benutzerkontos. Verwenden Sie den Befehl **dsrm group** zum Löschen eines Gruppenkontos. Obwohl sich mit den Verzeichnisdienstprogrammen immer nur jeweils ein Active Directory-Objekt erstellen lässt, können Sie die Tools in Batchdateien und Skripts verwenden.

Das Tool „Csvde“

Das Befehlszeilenprogramm Csvde verwendet als Eingabe zum Erstellen mehrerer Konten in Active Directory eine *durch Trennzeichen getrennte* Textdatei, die auch als *durch Trennzeichen getrenntes Werteformat* (Csvde-Format) bezeichnet wird.

Sie können mit dem Csvde-Format Benutzerobjekte und andere Objekttypen zu Active Directory hinzufügen. Das Csvde-Format kann nicht zum Löschen oder Ändern von Objekten in Active Directory verwendet werden. Vor dem Import einer Csvde-Datei müssen Sie sicherstellen, dass die Datei ordnungsgemäß formatiert ist. Die Eingabedatei:

- Muss den Pfad zum Benutzerkonto in Active Directory, den Objekttyp (d. h. das Benutzerkonto) und den Benutzeranmeldenamen (für Microsoft Windows NT® 4.0 und ältere Versionen) enthalten.
- Sollte den Benutzerprinzipalnamen enthalten und sollte angeben, ob das Benutzerkonto aktiviert oder deaktiviert ist. Wenn Sie keinen Wert angeben, wird das Konto deaktiviert.
- Kann persönliche Daten enthalten, z. B. Telefonnummern und Privatadressen. Fügen Sie so viele Benutzerkontoinformationen wie möglich hinzu, damit die Benutzer erfolgreich in Active Directory suchen können.
- Darf keine Kennwörter enthalten. Beim Massenimport wird das Kennwort für Benutzerkonten leer gelassen. Da eine unberechtigte Person bei einem leeren Kennwort auf das Netzwerk zugreifen kann, wenn sie nur den Benutzernamen kennt, müssen Sie die Benutzerkonten so lange deaktivieren, bis die Benutzer mir der Anmeldung beginnen.

Verwenden Sie zum Bearbeiten und Formatieren der Eingabetextdatei eine Anwendung mit guten Bearbeitungsfunktionen, wie z. B. Microsoft Excel oder Microsoft Word. Speichern Sie die Datei anschließend als durch Trennzeichen getrennte Textdatei. Sie können Daten aus Active Directory in eine Excel-Kalkulationstabelle exportieren oder Dateien aus einer Kalkulationstabelle in Active Directory importieren.

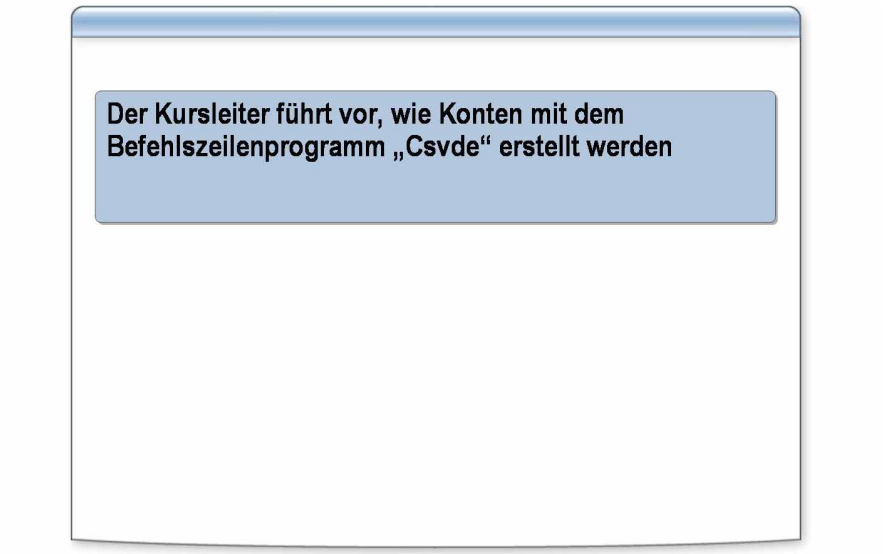
Das Tool „Ldifde“

Das Befehlszeilenprogramm Ldifde verwendet ein *durch Zeilen getrenntes Werteformat* zum Erstellen, Ändern und Löschen von Objekten in Active Directory. Eine Ldifde-Eingabedatei besteht aus einer Reihe von Datensätzen, die durch eine Leerzeile voneinander getrennt sind. Ein *Datensatz* beschreibt ein einzelnes Verzeichnisobjekt oder eine Gruppe von Änderungen an den Attributen eines vorhandenen Objekts und besteht aus mindestens einer Zeile in der Datei. Die meisten Datenbankanwendungen können Textdateien erstellen, die Sie in eines dieser Formate importieren können. Die Anforderungen für die Eingabedatei sind ähnlich den Anforderungen des Befehlszeilenprogramms Csvde.

Windows Script Host

Sie können Windows Script Host-Skripts erstellen, die Active Directory Service Interfaces (ADSI) zum Erstellen, Ändern und Löschen von Active Directory-Objekten verwenden. Verwenden Sie Skripts, wenn Sie die Attributwerte mehrerer Active Directory-Objekte ändern möchten oder wenn die Auswahlkriterien für diese Objekte komplex sind.

Anleitung: Erstellen von Konten mithilfe des Tools „Csvde“



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Sie können mit dem Befehlszeilenprogramm Csvde mehrere Konten in Active Directory erstellen. Sie können das Tool Csvde nur zum Erstellen und nicht zum Ändern von Konten verwenden.

Verfahren

Führen Sie die folgenden Schritte aus, um Konten mithilfe des Befehlszeilenprogramms Csvde zu erstellen:

1. Erstellen Sie die Csvde-Datei für den Import. Formatieren Sie die Datei, so dass sie die folgenden Informationen enthält:
   - *Die Attributzeile*. Dies ist die erste Zeile der Datei. Sie gibt den Namen der einzelnen Attribute an, die für die neuen Benutzerkonten definiert werden sollen. Sie können die Attribute in beliebiger Reihenfolge anordnen, müssen sie jedoch durch Komma voneinander trennen. Der folgende Code zeigt ein Beispiel für eine Attributzeile:

     ```
     DN,objectClass,sAMAccountName,userPrincipalName,
     displayName,userAccountControl
     ```

   - *Die Benutzerkontozeile*. Die Importdatei enthält für jedes erstellte Benutzerkonto eine Zeile, die den Wert der einzelnen Attribute in der Attributzeile angibt. Die folgenden Regeln gelten für die Werte in einer Benutzerkontozeile:
     - Die Attributwerte müssen entsprechend der Reihenfolge in der Attributzeile angegeben werden.
     - Wenn ein Wert für ein Attribut fehlt, lassen Sie ihn leer, fügen aber alle Kommas ein.
     - Wenn ein Wert Kommas enthält, müssen Sie ihn zwischen Anführungszeichen setzen.

Der folgende Code zeigt ein Beispiel für eine Benutzerkontozeile:

```
"cn=Suzan Fine,ou=Human Resources,dc=asia,dc=contoso,
dc=msft",user,suzanf,suzanf@contoso.msft,Suzan Fine,514
```

Die folgende Tabelle enthält die Attribute und Werte aus dem vorhergehenden Beispiel.

Attribut	Wert
DN (definierter Name)	cn=Suzan Fine,ou=Human Resources, dc=asia,dc=contoso,dc=msft (Dies gibt den Pfad zur Organisationseinheit an, die das Benutzerkonto enthält.)
objectClass	user
sAMAccountName	suzanf
userPrincipalName	suzanf@contoso.msft
displayName	Suzan Fine
userAccountControl	514 (Der Wert 514 deaktiviert das Benutzerkonto, und der Wert 512 aktiviert das Benutzerkonto.)

Die in dieser Tabelle aufgeführten Attribute sind die Attribute, die zum Ausführen von **csvde** mindestens erforderlich sind.

Wichtig Sie können Csvde nicht zum Erstellen aktivierter Benutzerkonten erstellen, wenn die Domänenkennwortrichtlinie eine Mindestkennwortlänge oder komplexe Kennwörter erfordert. Verwenden Sie in diesem Fall den userAccountControl-Wert 514, der das Benutzerkonto deaktiviert. Aktivieren Sie das Konto anschließend mithilfe von Windows Script Host oder Active Directory-Benutzer und -Computer.

2. Führen Sie den Befehl **csvde** aus, indem Sie den folgenden Befehl an der Eingabeaufforderung eingeben:

```
csvde –i –f filename –b UserName Domain Password
```

Dabei gilt Folgendes:

-i gibt an, dass Sie eine Datei in Active Directory importieren.

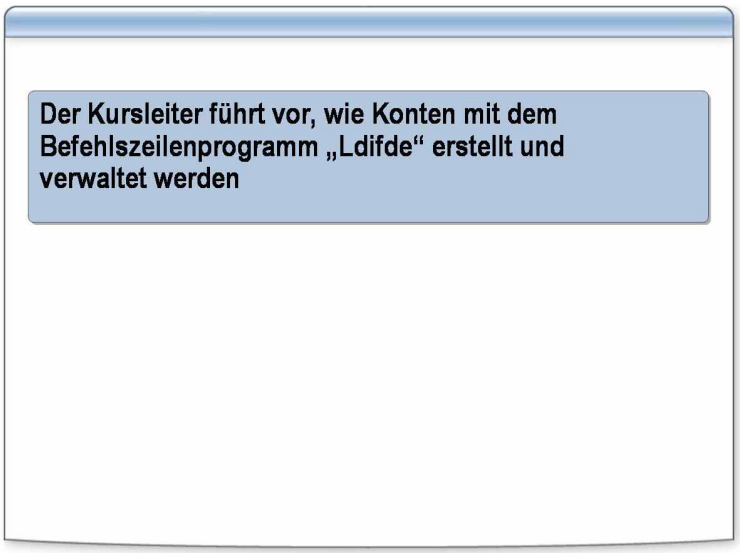
-f gibt an, dass der nächste Parameter der Name der zu importierenden Datei ist.

–b legt fest, dass der Befehl als *username*, *domain* und *password* ausgeführt wird.

Der Befehl **csvde** stellt Statusinformationen über den Erfolg oder das Fehlschlagen des Vorgangs bereit. Er listet darüber hinaus den Namen der Datei auf, die zum Anzeigen detaillierter Fehlerinformationen geöffnet werden kann. Selbst wenn die Statusinformationen angeben, dass der Vorgang erfolgreich war, sollten Sie mithilfe von Active Directory-Benutzer und -Computer einige der erstellten Benutzerkonten überprüfen, um sicherzustellen, dass sie alle bereitgestellten Informationen enthalten.

Anmerkung Informationen zu den allgemeinen Optionen, die mit dem Befehlszeilenprogramm Csvde erstellt werden, finden Sie unter „Anleitung: Erstellen von Konten mithilfe des Tools „Csvde“ in Unterrichtseinheit 4 im Ordner *Anhänge* der Kursteilnehmer-CD. Informationen finden Sie auch in Windows Server 2003 Hilfe und Support.

Anleitung: Erstellen und Verwalten von Konten mithilfe des Tools „Ldifde“



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Sie können mit dem Befehlszeilenprogramm Ldifde mehrere Konten erstellen und ändern.

Verfahren

Führen Sie die folgenden Schritte aus, um mithilfe des Befehlszeilenprogramms Ldifde Konten zu erstellen:

1. Bereiten Sie die Ldifde-Datei für den Import vor.

   Formatieren Sie die Ldifde-Datei, so dass Sie einen Datensatz mit einer Folge von Zeilen enthält, die entweder einen Eintrag für ein Benutzerkonto oder eine Gruppe von Änderungen für ein Benutzerkonto in Active Directory beschreiben. Der Eintrag für das Benutzerkonto gibt die Namen der verschiedenen Attribute an, die für das neue Benutzerkonto definiert werden sollen. Das Active Directory-Schema definiert die Attributnamen. Die Datei enthält für jedes erstellte Benutzerkonto eine Zeile, die den Wert der einzelnen Attribute in der Attributzeile angibt. Für die Werte der einzelnen Attribute gelten die folgenden Regeln:

   - Alle mit einem Nummernzeichen (#) beginnenden Zeilen sind Kommentarzeilen, die beim Ausführen der Ldifde-Datei ignoriert werden.

- Wenn ein Wert für ein Attribut fehlt, muss der Doppelpunkt als *Attributbeschreibung* ":" FILL SEP dargestellt werden.

  Der folgende Code zeigt ein Beispiel für einen Eintrag in einer Ldifde-Importdatei:

```
# Create Suzan Fine
dn: cn=Suzan Fine,ou=Human
Resources,dc=asia,dc=contoso,dc=msft
Changetype: Add
objectClass: user
sAMAccountName: suzanf
userPrincipalName: suzanf@contoso.msft
displayName: Suzan Fine
userAccountControl: 514
```

Die folgende Tabelle enthält die Attribute und Werte aus dem vorhergehenden Beispiel.

Attribut	Attributwert
#	Create Suzan Fine (Das Zeichen # gibt an, dass diese Zeile ein Kommentar ist.)
DN	cn=Suzan Fine, ou=Human Resources, dc=asia,dc=contoso,dc=msft (Dieser Wert gibt den Pfad zum Objektcontainer an.)
Changetype	Add
objectClass	user
sAMAccountName	suzanf
userPrincipalName	suzanf@contoso.msft
displayName	Suzan Fine
userAccountControl	512

2. Führen Sie den Befehl **ldifde** aus, um die Datei zu importieren und mehrere Benutzerkonten in Active Directory zu erstellen.

   Geben Sie den folgenden Befehl an der Eingabeaufforderung ein:

```
ldifde –i –f filename –b UserName Domain Password
```

   Dabei gilt Folgendes:

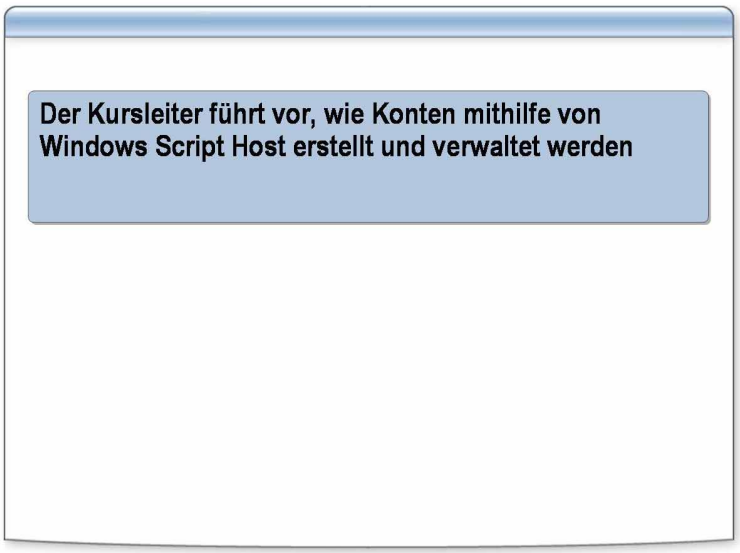
   -i gibt den Importmodus an. Wird nichts angegeben, wird der Standardmodus, d. h. der Exportmodus verwendet.

   -k ignoriert Fehler während eines Importvorgangs und setzt die Verarbeitung fort.

   -f gibt den Import- oder Exportdateinamen an.

   -b gibt den Benutzernamen, den Domänennamen und das Kennwort für das Benutzerkonto an, das zum Durchführen des Import- oder Exportvorgangs verwendet wird.

Anleitung: Erstellen und Verwalten von Konten mithilfe von Windows Script Host



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Mithilfe von ADSI können Sie Active Directory-Objekte über Windows Script Host-Skripts erstellen. Wie im folgenden Verfahren gezeigt, ist das Erstellen eines Active Directory-Objekts ein aus vier Schritten bestehender Prozess.

Verfahren für das Erstellen eines Active Directory-Objekts

Führen Sie die folgenden Schritte aus, um ein Active Directory-Objekt (z. B. ein Benutzerkonto in einer Domäne) zu erstellen:

1. Verwenden Sie Microsoft Editor, um eine Textdatei mit der Erweiterung VBS zu erstellen. Schreiben Sie die folgenden Befehle in die Datei, und speichern Sie die Datei.

   a. Stellen Sie eine Verbindung zu dem Container her, in dem Sie das Active Directory-Objekt erstellen möchten. Geben Sie dazu die Lightweight Directory Access Protocol- (LDAP-) Abfrage an.

   ```
   Set objOU =
   GetObject("LDAP://ou=management,dc=fabrikam,dc=com")
   ```

   Wichtig Im Beispiel oben muss LDAP in Großbuchstaben geschrieben werden; andernfalls schlägt der Befehl fehl.

   b. Erstellen Sie das Active Directory-Objekt, und geben Sie die Objektklasse und den Objektnamen an.

   ```
   Set objUser = objOU.Create("Benutzer", "cn=MyerKen")
   ```

   c. Legen Sie die Eigenschaften für das Active Directory-Objekt fest.

   ```
   objUser.Put "sAMAccountName", "myerken"
   ```

d. Schreiben Sie die Informationen in die Active Directory-Datenbank.

```
objUser.SetInfo
```

Die Eigenschaften bestimmter Active Directory-Objekte können bei deren Erstellung nicht festgelegt werden. Wenn Sie z. B. ein Benutzerkonto erstellen, können Sie das Konto nicht aktivieren oder sein Kennwort festlegen. Wie im folgenden Beispielcode gezeigt, können Sie diese Eigenschaften erst nach dem Erstellen des Objekts festlegen:

```
objUser.AccountDisabled = FALSE
objUser.ChangePassword "", "jl3R86df"
objUser.SetInfo
```

e. Speichern Sie Datei mit der Erweiterung VBS.

2. Führen Sie das Skript aus, indem Sie den folgenden Befehl an der Eingabeaufforderung eingeben:

```
Wscript.exe filename
```

Dabei ist *filename* der Name der Skriptdatei, die Sie im vorhergehenden Schritt erstellt haben.

Anmerkung Ein Beispielskript zum Erstellen eines Benutzerkontos finden Sie unter „Anleitung: Erstellen und Verwalten von Konten mithilfe von Windows Script Host“ in Unterrichtseinheit 4 auf der Seite *Anhänge* der Kursteilnehmer-CD.

Verfahren für das Ändern eines Eigenschaftswerts

Um den Eigenschaftswert eines Active Directory-Objekts (z. B. die Telefonnummer eines Benutzers) zu ändern, öffnen Sie Editor, um mit diesem eine neue Textdatei zu erstellen. Fügen Sie die folgenden Befehle zur Datei hinzu, und führen Sie dann die Skriptdatei aus, indem Sie sie von einer Eingabeaufforderung aus starten:

1. Stellen Sie eine Verbindung zu dem Objekt her, dessen Eigenschaft geändert werden soll.

```
Set objUser = GetObject _
      ("LDAP://cn=myerken,ou=TestOU,dc=nwtraders,dc=msft")
```

2. Legen Sie den neuen Wert der Eigenschaft fest, z. B. die Raumnummer eines Mitarbeiters, der in ein neues Büro umgezogen ist.

```
objUser.Put "physicalDeliveryOfficeName", "Room 4358"
```

3. Schreiben Sie die Änderung in Active Directory.

```
objUser.SetInfo
```

4. Speichern Sie die Datei mit der Erweiterung VBS.
5. Führen Sie das Skript aus, indem Sie den folgenden Befehl an der Eingabeaufforderung eingeben:

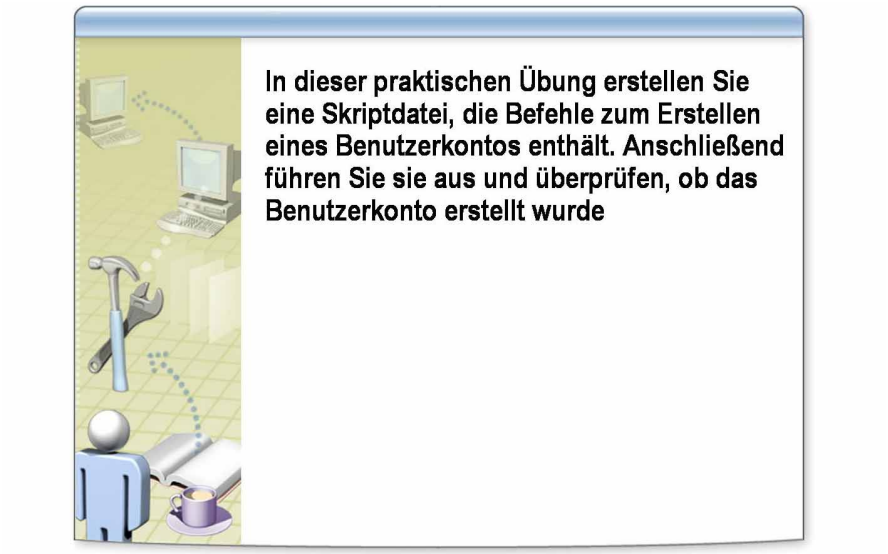
```
wscript.exe filename
```

   Dabei ist *filename* der Name der Skriptdatei, die Sie im vorhergehenden Schritt erstellt haben.

Anmerkung Weitere Informationen zum Erstellen von Verwaltungsskripts mithilfe von Windows Script Host finden Sie im Microsoft TechNet Script Center unter: www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/default.asp (auf Englisch).

Informationen finden Sie auch in Kurs 2433, *Microsoft Visual Basic Scripting Edition and Microsoft Windows Script Host Essentials* (auf Englisch).

Praktische Übung: Erstellen von Benutzerkonten



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Lernziele

In dieser praktischen Übung erstellen Sie eine Skriptdatei, die Befehle zum Erstellen eines Benutzerkontos enthält. Anschließend führen Sie sie aus und überprüfen, ob das Benutzerkonto erstellt wurde.

Szenario

Northwind Traders hat einen neuen Vertriebsmitarbeiter, Brenda Diaz, eingestellt. Sie müssen den Benutzeranmeldenamen für sie erstellen. In der Firma Northwind Traders werden standardmäßig der Vorname und die ersten drei Buchstaben vom Nachnamen des Benutzers verwendet. Sie verwenden Windows Script Host zum Erstellen dieses Benutzerkontos in der Organisationseinheit *IhrComputerName*\Sales.

Praktische Übung

Führen Sie die folgenden Schritte aus, um das Benutzerkonto zu erstellen:

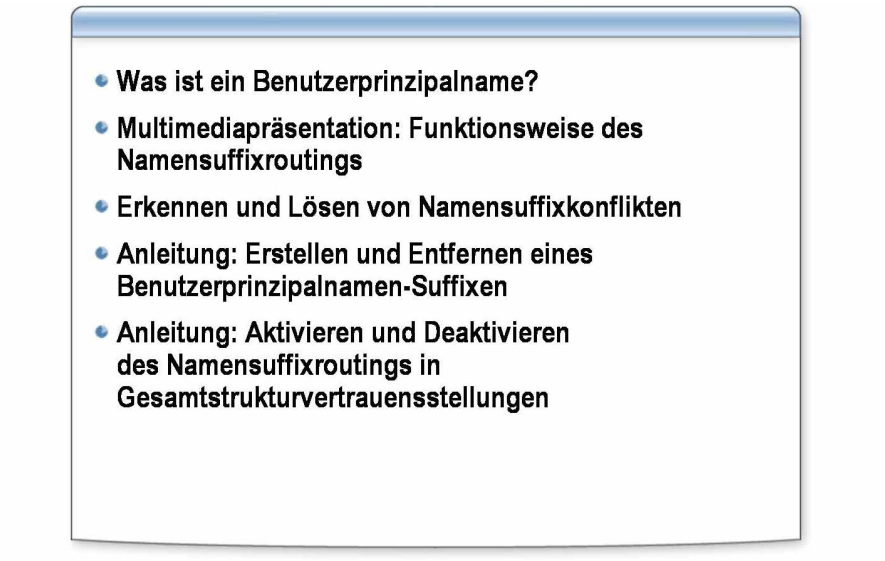
1. Melden Sie sich als **Nwtraders***x**ComputerName***User** mit dem Kennwort **P@ssw0rd** an.
2. Erstellen Sie mit Editor eine Skriptdatei, die Befehle zum Erstellen des neuen Benutzerkontos enthält.
   a. Öffnen Sie Editor.
   b. Geben Sie das Skript zum Erstellen des Benutzerkontos ein.
   c. Klicken Sie im Menü **Datei** auf **Speichern unter**.
   d. Geben Sie in das Feld **Dateiname** den Namen **createusers.vbs** ein.
   e. Wählen Sie im Feld **Dateityp** den Eintrag **Alle Dateien** aus.
   f. Klicken Sie auf **Speichern**.

3. Führen Sie die Skriptdatei aus.
   a. Klicken Sie auf **Start**, klicken Sie mit der rechten Maustaste auf **Eingabeaufforderung**, und klicken Sie dann auf **Ausführen als**.
   b. Klicken Sie im Dialogfeld **Ausführen als** auf **Folgender Benutzer**, geben Sie als Benutzername *IhreDomäne***Administrator** und das Kennwort **P@ssw0rd** ein, und klicken Sie dann auf **OK**.
   c. Wechseln Sie zu dem Ordner, in dem Sie die Datei **createusers.vbs** gespeichert haben.
   d. Geben Sie an der Eingabeaufforderung **wscript.exe createusers.vbs** ein.
4. Überprüfen Sie mithilfe von Active Directory-Benutzer und -Computer, ob der Benutzer erstellt wurde.
   a. Öffnen Sie Active Directory-Benutzer und -Computer.
   b. Klicken Sie in der Konsolenstruktur auf **Sales**.
   c. Sehen Sie sich im Detailfenster die aufgelisteten Benutzerkonten an.

Der folgende Abschnitt zeigt eine Beispielantwortdatei.

```
Set objOU =
GetObject("LDAP://OU=Sales,OU=Vancouver,dc=nwtraders1,dc=msft"
)
Set objUser = objOU.Create("Benutzer", "cn=BrendaDia")
objUser.Put "sAMAccountName", "BrendaDia"
objUser.SetInfo
objUser.AccountDisabled = FALSE
objUser.ChangePassword "", "P@ssw0rd"
objUser.Put "userPrincipalName", "BrendaDia@nwtraders1.msft"
objUser.SetInfo
```

Lektion: Implementieren von Benutzerprinzipalnamen-Suffixen



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

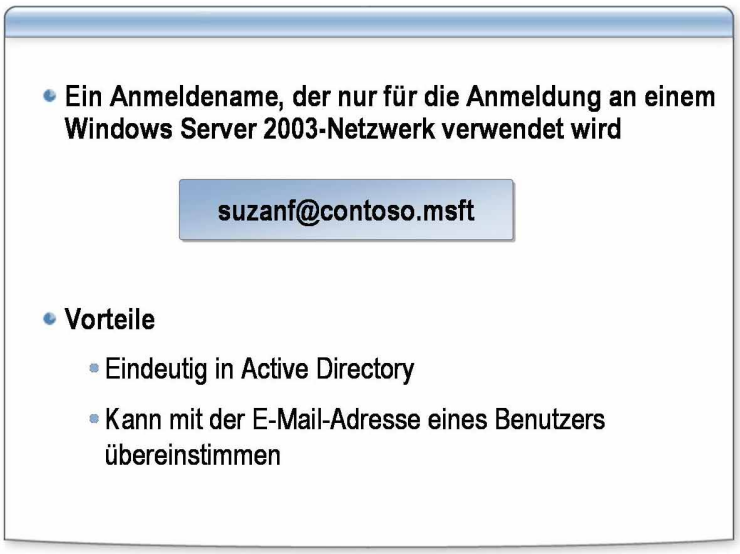
In dieser Lektion wird der Zweck von Benutzerprinzipalnamen beschrieben. Es wird erläutert, wie ein Benutzerprinzipalnamen-Suffix in einer vertrauenswürdigen Umgebung weitergeleitet und wie das Namensuffixrouting in gesamtstrukturübergreifenden Vertrauensstellungen erstellt, entfernt, aktiviert, deaktiviert und ausgeschlossen wird.

Lernziele der Lektion

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Beschreiben des Zwecks eines Benutzerprinzipalnamens.
- Erklären, wie ein Benutzerprinzipalnamen-Suffix in einer vertrauenswürdigen Umgebung weitergeleitet wird.
- Beschreiben, wie Namensuffixkonflikte erkannt und gelöst werden.
- Erstellen und Entfernen eines Benutzerprinzipalnamen-Suffixes.
- Aktivieren, Deaktivieren und Ausschließen des Namensuffixroutings in gesamtstrukturübergreifenden Vertrauensstellungen.

Was ist ein Benutzerprinzipalname?



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

In einem Windows Server 2003-Netzwerk kann sich ein Benutzer entweder mit einem Benutzerprinzipalnamen oder mit einem Benutzeranmeldenamen (Microsoft Windows NT 4.0 und ältere Versionen) anmelden. Domänencontroller können zum Authentifizieren der Anmeldeanforderung entweder den Benutzerprinzipalnamen oder den Benutzeranmeldenamen verwenden.

Was ist ein Benutzerprinzipalname?

Ein *Benutzerprinzipalname* ist ein Anmeldename, der nur für die Anmeldung an einem Microsoft Windows Server 2003-Netzwerk verwendet wird. Dieser Name wird auch als Benutzeranmeldename bezeichnet.

Ein Benutzerprinzipalname besteht aus zwei Teilen, die durch das Zeichen @ voneinander getrennt sind (z. B. suzanf@contoso.msft):

- Dem *Benutzerprinzipalnamen-Präfix*, das in diesem Beispiel suzanf lautet.
- Dem *Benutzerprinzipalnamen-Suffix*, das in diesem Beispiel contoso.msft lautet. Das Suffix ist standardmäßig der Name der Domäne, in der das Benutzerkonto erstellt wurde. Sie können die anderen Domänen im Netzwerk oder andere, von Ihnen erstellte Suffixe verwenden, um andere Suffixe für Benutzer zu konfigurieren. So könnten Sie z. B. ein Suffix zum Erstellen von Benutzeranmeldenamen erstellen, das den E-Mail-Adressen der Benutzer entspricht.

Vorteile der Verwendung von Benutzerprinzipalnamen

Die Verwendung von Benutzerprinzipalnamen hat folgende Vorteile:

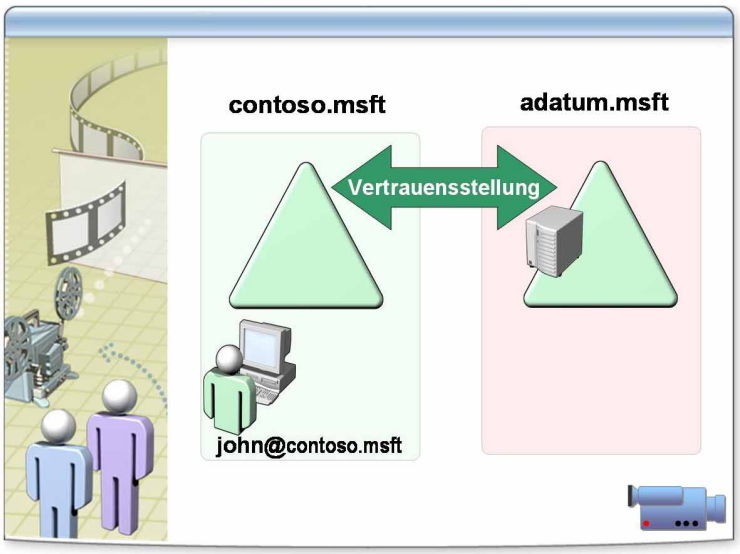
- Sie bleiben gleich, wenn Sie ein Benutzerkonto in eine andere Domäne verschieben, weil der Name in der Active Directory-Gesamtstruktur eindeutig ist.
- Sie können den Namen der E-Mail-Adresse eines Benutzers haben, weil sie das gleiche Format wie Standard-E-Mail-Adressen haben.

Eindeutigkeitsregeln für Benutzeranmeldenamen

Benutzeranmeldenamen für Domänenbenutzerkonten müssen den folgenden Eindeutigkeitsregeln in Active Directory entsprechen:

- Der vollständige Name muss in dem Container, in dem Sie das Benutzerkonto erstellen, eindeutig sein. Der vollständige Name wird als der Relative Distinguished Name verwendet.
- Der Benutzerprinzipalname muss in der Gesamtstruktur eindeutig sein.

Multimediapräsentation: Funktionsweise des Namensuffixroutings



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Speicherort der Datei

Um die Präsentation *Funktionsweise des Namensuffixroutings* anzuzeigen, öffnen Sie die Webseite auf der Kursteilnehmer-CD, klicken Sie auf **Multimedia** und anschließend auf den Titel der Präsentation. Öffnen Sie diese Präsentation erst, wenn Sie der Kursleiter dazu auffordert.

Lernziele

Am Ende dieser Präsentation können Sie erklären, wie das Namensuffixrouting in Active Directory funktioniert.

Kernpunkte

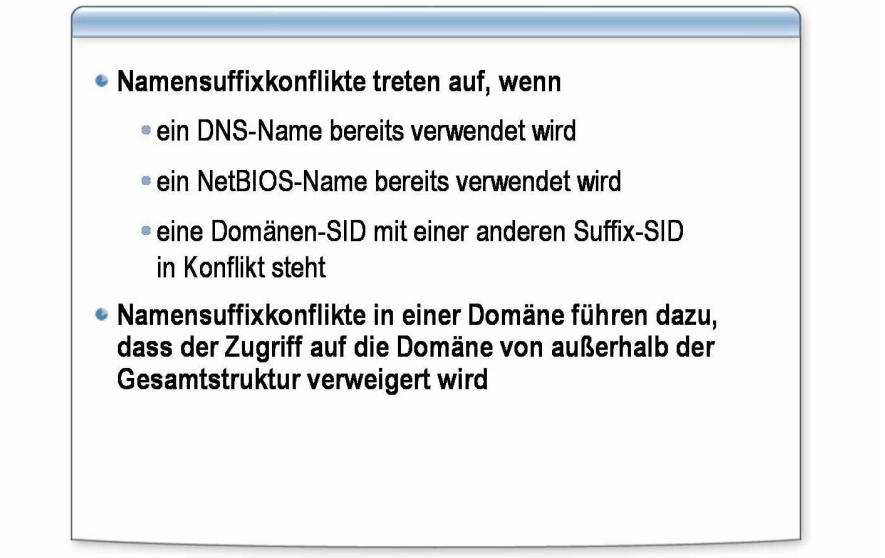
Das Namensuffixrouting ist ein Mechanismus, der über Gesamtstrukturen hinweg eine Namensauflösung bereitstellt. Gesamtstrukturen können mehrere Namensuffixe enthalten.

Wenn zwei Windows Server 2003-Gesamtstrukturen durch eine Gesamtstrukturvertrauensstellung verbunden sind, werden Authentifizierungsanforderungen von Domänennamensuffixen weitergeleitet, die in beiden Gesamtstrukturen vorhanden sind. Daher werden alle Authentifizierungsanforderungen von Gesamtstruktur A für ein Suffix in Gesamtstruktur B erfolgreich zu ihren Zielressourcen weitergeleitet.

Namensuffixe, die in einer Gesamtstruktur nicht enthalten sind, können an eine zweite Gesamtstruktur weitergeleitet werden. Wenn eine neue untergeordnete Domäne (z. B. child.contoso.com) zu einem Domänennamensuffix zweiter Ebene (z. B. contoso.com) hinzugefügt wird, erbt die untergeordnete Domäne die Routingkonfiguration der Domäne zweiter Ordnung, zu der sie gehört.

Alle neuen Namensuffixe zweiter Ordnung, die nach dem Einrichten einer Gesamtstrukturvertrauensstellung erstellt wurden, sind im Dialogfeld **Eigenschaften** für diese Gesamtstrukturvertrauensstellung sichtbar. Allerdings ist das Routing von Suffixen für die Domänenstrukturen, die Sie nach dem Einrichten der Vertrauensstellung erstellen, standardmäßig deaktiviert. Sie müssen das Routing für diese Suffixe manuell aktivieren. Wenn Active Directory einen doppelten Namensuffix erkennt, wird das Routing für den neuesten Namensuffix standardmäßig deaktiviert. Sie können das Routing für einzelne Namensuffixe mithilfe des Dialogfelds **Eigenschaften** manuell aktivieren oder deaktivieren.

Erkennen und Lösen von Namensuffixkonflikten



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Wenn zwei Windows Server 2003-Gesamtstrukturen durch eine Gesamtstrukturvertrauensstellung verknüpft sind, kann es sein, dass ein Domänennamensuffix zweiter Ebene oder ein Benutzerprinzipalnamen-Suffix der einen Gesamtstruktur mit einem ähnlichen Namensuffix der zweiten Gesamtstruktur kollidiert. Durch eine Kollisionserkennung stellt der Assistent für neue Vertrauensstellungen sicher, dass nur eine Gesamtstruktur für einen bestimmten Namensuffix autorisierend ist.

Kollisionserkennung

Der Assistent für neue Vertrauensstellungen erkennt Namensuffixkonflikte in den folgenden Situationen:

- Ein Domain Name System- (DNS-) Name wird bereits verwendet.
- Ein NetBIOS-Name wird bereits verwendet.
- Eine Domänensicherheitskennung steht mit einer anderen Sicherheitskennung eines Namensuffixes in Konflikt.

Angenommen, Sie möchten eine bidirektionale Gesamtstrukturvertrauensstellung zwischen der Gesamtstruktur contoso.com und der Gesamtstruktur fabrikam.com erstellen. Die Gesamtstrukturen contoso.com und fabrikam.com haben denselben Benutzerprinzipalnamen-Suffix, nwtraders.msft. Beim Erstellen der bidirektionalen Gesamtstrukturvertrauensstellung erkennt der Assistent für neue Vertrauensstellungen den Konflikt zwischen den beiden Benutzerprinzipalnamen-Suffixen und zeigt diesen an.

Lösen von Konflikten

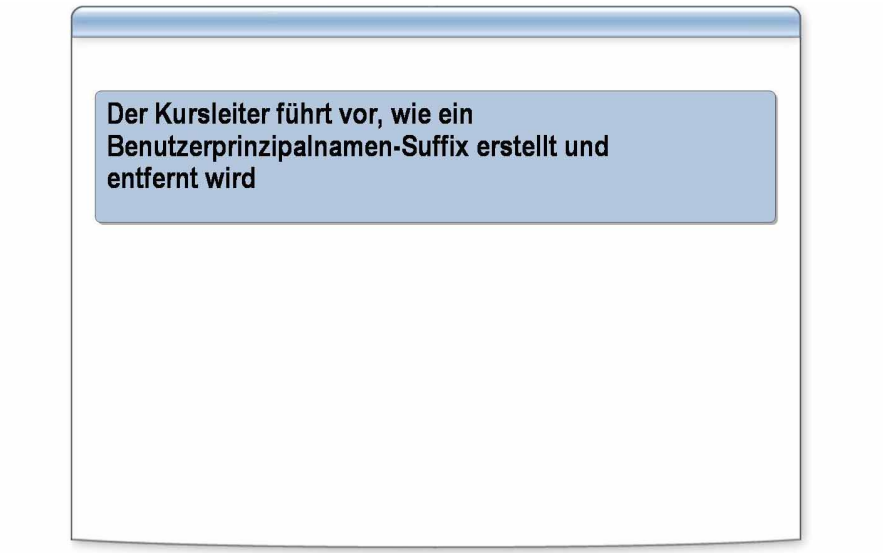
Der Assistent für neue Vertrauensstellungen deaktiviert automatisch einen Domänennamensuffix zweiter Ebene, wenn der Namensuffix bereits in einer zweiten Gesamtstruktur vorhanden ist. So tritt z. B. ein Konflikt auf, wenn eine Gesamtstruktur fabrikam.com heißt und die zweite Gesamtstruktur sales.fabrikam.com.

Wenn der Assistent für neue Vertrauensstellungen einen Namensuffixkonflikt erkennt, verweigert er den Zugriff auf diese Domäne von außerhalb der Gesamtstruktur. Der Zugriff auf die Domäne von innerhalb der Gesamtstruktur funktioniert jedoch normal.

Wenn die Domäne fabrikam.com beispielsweise in den Gesamtstrukturen contoso.com und nwtraders.msft vorhanden ist, können die Benutzer in der Gesamtstruktur contoso.com auf Ressourcen in der Domäne fabrikam.com zugreifen, die sich in der Gesamtstruktur contoso.com befindet. Benutzern in der Gesamtstruktur contoso.com wird der Zugriff auf Ressourcen in der Domäne fabrikam.com, die sich in der Gesamtstruktur befindet, jedoch verweigert.

Wenn der Assistent für neue Vertrauensstellungen einen Namensuffixkonflikt erkennt, werden Sie aufgefordert, eine Protokolldatei für die Konflikte zu speichern. Er listet die Konflikte anschließend im Dialogfeld **Eigenschaften von** *Gesamtstrukturvertrauensstellung* auf der Registerkarte **Namensuffixrouting** in der Spalte **Routing** auf.

Anleitung: Erstellen und Entfernen eines Benutzerprinzipalnamen-Suffixen



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Wenn Sie ein Benutzerprinzipalnamen-Suffix verwenden, vereinfachen Sie den Verwaltungs- und Benutzeranmeldeprozess, indem Sie einen Benutzerprinzipalnamen-Suffix für alle Benutzer bereitstellen. Beim Erstellen eines Benutzerkontos können Sie ein Benutzerprinzipalnamen-Suffix auswählen. Wenn das Suffix nicht vorhanden ist, können Sie es mithilfe von Active Directory-Domänen und -Vertrauensstellungen hinzufügen, vorausgesetzt, Sie sind Mitglied der vordefinierten Gruppe Organisations-Admins.

Verfahren für das Hinzufügen eines Benutzerprinzipalnamen-Suffixes

Führen Sie die folgenden Schritte aus, um ein Benutzerprinzipalnamen-Suffix hinzuzufügen:

1. Öffnen Sie Active Directory-Domänen und -Vertrauensstellungen.
2. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Active Directory-Domänen und -Vertrauensstellungen**, und klicken Sie dann auf **Eigenschaften**.
3. Geben Sie auf der Registerkarte **Benutzerprinzipalnamen-Suffixe** ein alternatives Benutzerprinzipalnamen-Suffix ein, und klicken Sie dann auf **Hinzufügen**.

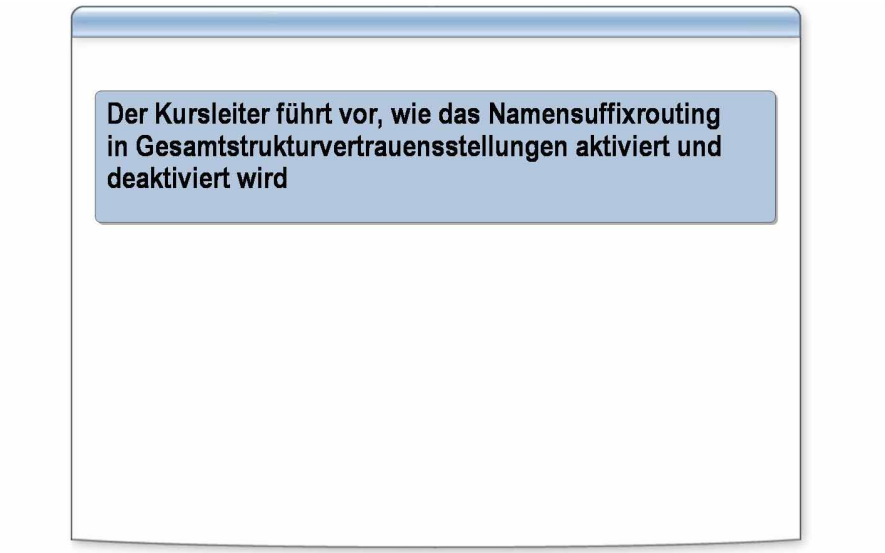
Anmerkung Wenn Sie ein Benutzerkonto mithilfe von Windows Script Host oder einem anderen Tool als Active Directory-Benutzer- und -Computer erstellen, besteht keine Einschränkung durch die Benutzerprinzipalnamen-Suffixe, die in Active Directory gespeichert sind. Sie können ein Suffix beim Erstellen des Kontos zuweisen. Allerdings werden die auf diese Weise erstellten Suffixe nicht automatisch über Gesamtstrukturvertrauensstellungen weitergeleitet.

Verfahren für das Entfernen eines Benutzerprinzipalnamen-Suffixes

Führen Sie die folgenden Schritte aus, um ein Benutzerprinzipalnamen-Suffix zu entfernen:

1. Klicken Sie in der Konsolenstruktur von Active Directory-Domänen und -Vertrauensstellungen mit der rechten Maustaste auf **Active Directory-Domänen und -Vertrauensstellungen**, und klicken Sie dann auf **Eigenschaften**.
2. Wählen Sie auf der Registerkarte **Benutzerprinzipalnamen-Suffixe** den Namen des zu entfernenden Benutzerprinzipalnamensuffixes aus, und klicken Sie dann auf **Entfernen**.

Anleitung: Aktivieren und Deaktivieren des Namensuffixroutings in Gesamtstrukturvertrauensstellungen



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Mit Active Directory-Domänen und -Vertrauensstellungen aktivieren und deaktivieren Sie das Routing für ein Namensuffix.

Verfahren

Führen Sie die folgenden Schritte aus, um das Routing für ein Namensuffix zweiter Ebene zu aktivieren oder zu deaktivieren:

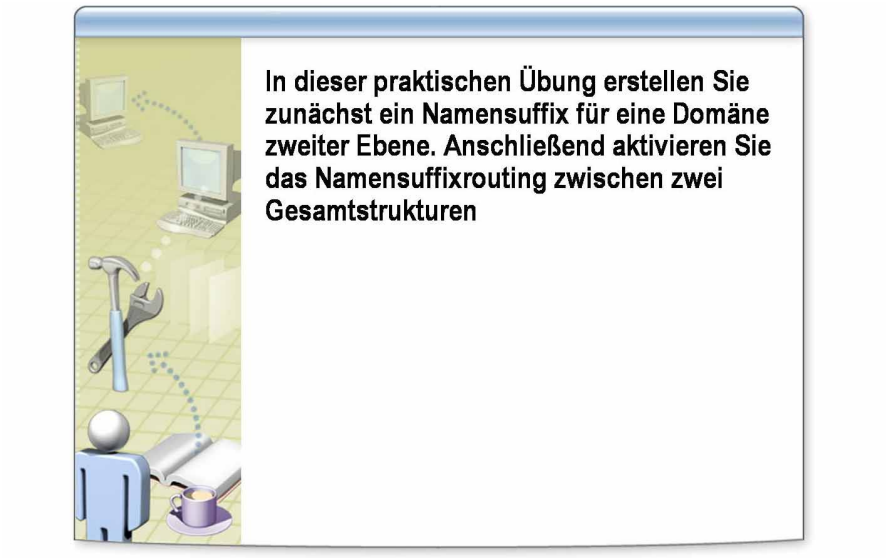
1. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Domänenknoten für die Domäne, die Sie verwalten möchten, und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf der Registerkarte **Vertrauensstellungen** unter **Domänen, denen diese Domäne vertraut (ausgehende Vertrauensstellungen)** oder unter **Domänen, die dieser Domäne vertrauen (eingehende Vertrauensstellungen)** auf die Gesamtstrukturvertrauensstellung, die Sie verwalten möchten, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Namensuffixrouting** unter **Namensuffixe in der Gesamtstruktur <***Gesamtstrukturname***>** auf das Suffix, für das Sie das Routing aktivieren oder deaktivieren möchten, und klicken Sie dann auf **Aktivieren** bzw. **Deaktivieren**.

Wichtig Wenn Sie das Routing für ein Domänensuffix zweiter Ebene deaktivieren, dann deaktivieren Sie auch das Routing von Suffixen für alle untergeordneten Domänensuffixe.

Führen Sie die folgenden Schritte aus, um den Routingstatus eines Namensuffixes der dritten oder einer höheren Ebene zu ändern:

1. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Domänenknoten für die Domäne, die Sie verwalten möchten, und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf der Registerkarte **Vertrauensstellungen** unter **Domänen, denen diese Domäne vertraut (ausgehende Vertrauensstellungen)** oder unter **Domänen, die dieser Domäne vertrauen (eingehende Vertrauensstellungen)** auf die Gesamtstrukturvertrauensstellung, die Sie verwalten möchten, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Namensuffixrouting** unter **Namensuffixe in der Gesamtstruktur <***Gesamtstrukturname***>** auf das Suffix, das das übergeordnete Suffix des Suffixes ist, für das Sie den Routingstatus ändern möchten, und klicken Sie dann auf **Bearbeiten**.
4. Klicken Sie unter **Bestehende Namensuffixe in <***Gesamtstrukturname***>** auf das zu ändernde Suffix, und klicken Sie dann auf **Aktivieren** oder **Deaktivieren**.

Praktische Übung: Erstellen von Benutzerprinzipalnamen-Suffixen



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Lernziele

In dieser praktischen Übung erstellen Sie zunächst ein Namensuffix für eine Domäne zweiter Ebene. Anschließend aktivieren Sie das Namensuffixrouting zwischen zwei Gesamtstrukturen.

Szenario

Northwind Traders verfügt über eine Gesamtstruktur mit mehreren Domänen. Die Firma hat einen neuen Domänennamen gewählt, der als Name der Firmenwebsite und als E-Mail-Adresse verwendet wird. Sie müssen das neue Suffix hinzufügen und das Routing dafür aktivieren.

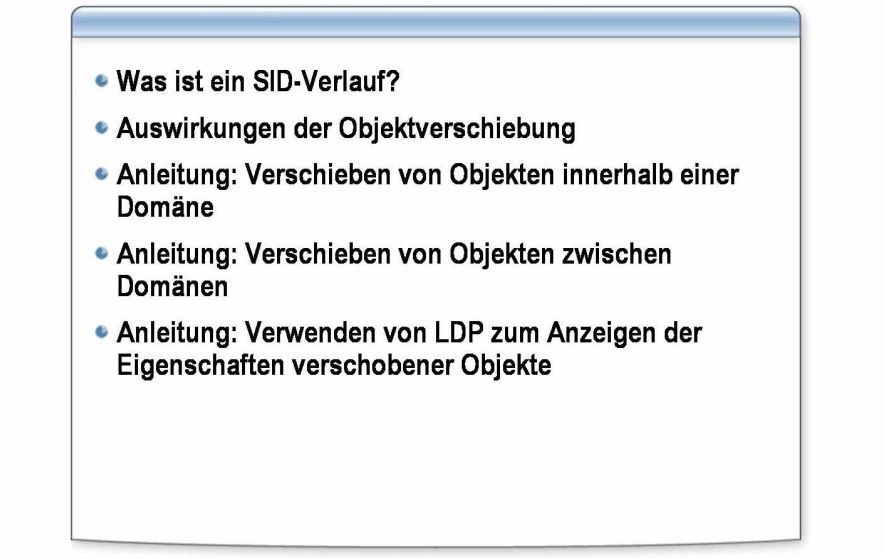
Praktische Übung

► **Erstellen Sie ein Namensuffix, und aktivieren Sie das Routing des Namensuffixes**

1. Erstellen Sie ein neues Namensuffix für eine Domäne *IhrVorname***.**msft, die eine Domäne zweiter Ebene sein muss.
   a. Melden Sie sich als **Nwtraders***x**ComputerName***User** mit dem Kennwort **P@ssw0rd** an.
   b. Verwenden Sie **Ausführen als**, um die Active Directory-Domänen und -Vertrauensstellungen als *IhreDomäne***Administrator** mit dem Kennwort **P@ssw0rd** zu starten.
   c. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Active Directory-Domänen und -Vertrauensstellungen**, und klicken Sie dann auf **Eigenschaften**.
   d. Geben Sie auf der Registerkarte **Benutzerprinzipalnamen-Suffixe** das Benutzerprinzipalnamen-Suffix *IhrVorname***.msft** ein, klicken Sie auf **Hinzufügen** und dann auf **OK**.

2. Aktivieren Sie das Routing der neuen, gerade erstellten Namensuffixe für die Gesamtstruktur **nwtraders.msft**.
   a. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Active Directory-Domänen und -Vertrauensstellungen**, und klicken Sie dann auf **Verbindung zum Domänencontroller herstellen**.
   b. Geben Sie im Dialogfeld **Verbindung zum Domänencontroller herstellen** im Feld **Domäne** den Namen **nwtraders.msft** ein.
   c. Klicken Sie auf **OK** und dann auf **Ja**.
   d. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **nwtraders.msft**, und klicken Sie dann auf **Eigenschaften**.
   e. Klicken Sie auf der Registerkarte **Vertrauensstellungen** unter **Domänen, die dieser Domäne vertrauen (eingehende Vertrauensstellungen)** auf **nwtraders*x*.msft**, klicken Sie auf **Eigenschaften** und dann auf die Registerkarte **Namensuffixrouting**.
   f. Geben Sie im Dialogfeld **Active Directory** den Benutzernamen **Administrator** und das Kennwort **P@ssw0rd** ein, und klicken Sie dann auf **OK**.
   g. Klicken Sie auf der Registerkarte **Namensuffixrouting** unter **Namensuffixe in der Gesamtstruktur nwtraders*x*** auf *IhrVorname***.msft**, klicken Sie auf **Aktivieren** und dann zweimal auf **OK**.

Lektion: Verschieben von Objekten in Active Directory



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

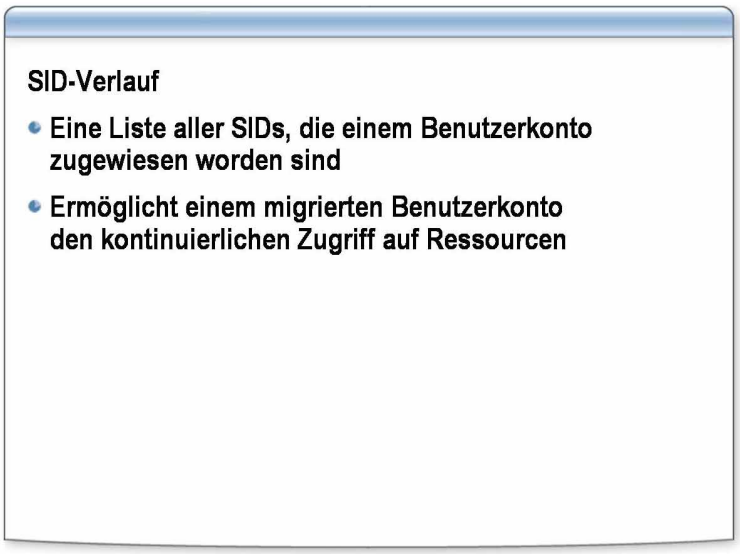
In dieser Lektion werden der SID-Verlauf (Security Identifier, Sicherheitskennung) und die Auswirkungen beim Verschieben von Active Directory-Objekten behandelt. Darüber hinaus wird erklärt, wie ein Active Directory-Objekt zwischen Containern in derselben Domäne und zwischen Domänen in derselben Gesamtstruktur verschoben werden.

Lernziele der Lektion

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Beschreiben des Zwecks eines SID-Verlaufs.
- Erläutern der Auswirkungen beim Verschieben von Objekten in Active Directory.
- Verschieben von Objekten in einer Domäne.
- Verschieben von Objekten zwischen Domänen.
- Anzeigen der Eigenschaften verschobener Objekte.

Was ist ein SID-Verlauf?



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

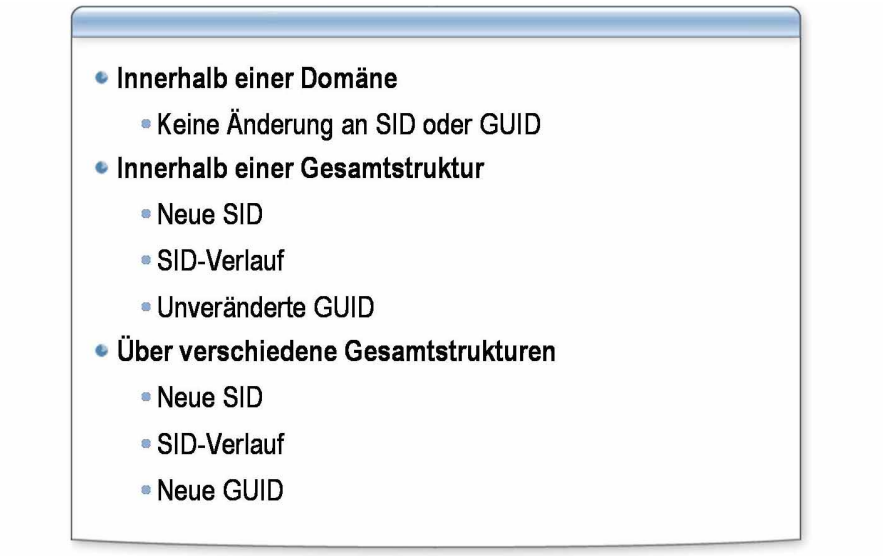
Einführung

Beim Verschieben eines Active Directory-Objekts (z. B. eines Benutzerkontos) werden die Sicherheitsprinzipale, die dem Objekt zugewiesen sind, ebenfalls verschoben. Active Directory verfolgt diese Sicherheitsprinzipale in einer Liste, die als SID-Verlauf bezeichnet wird.

Zweck eines SID-Verlaufs

Der SID-Verlauf ermöglicht einem migrierten Benutzer den kontinuierlichen Zugriff auf Ressourcen. Wenn Sie ein Benutzerkonto zu einer anderen Domäne migrieren, weist Active Directory ihm eine neue SID zu. Der SID-Verlauf enthält die vorhergehende SID des migrierten Benutzerkontos. Wenn Sie ein Benutzerkonto mehrmals migrieren, speichert der SID-Verlauf eine Liste aller SIDs, die dem Benutzer zugewiesen wurden, und aktualisiert dann die erforderlichen Gruppen und Zugriffsteuerungslisten mit der neuen Konto-SID. Guppenmitgliedschaften, die auf der alten Konto-SID basieren, bestehen nicht mehr.

Auswirkungen der Objektverschiebung



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Damit der SID-Verlauf aktiviert ist, müssen Sie die Domänenfunktionsebene auf Windows 2000 pur oder auf Windows Server 2003 festlegen. Der SID-Verlauf ist deaktiviert, wenn die Funktionsebene auf Windows 2000 gemischt festgelegt ist. Wenn ein Objekt innerhalb einer Domäne verschoben wird, dann wird dessen SID oder dessen Globally Unique Identifier (GUID) nicht geändert. Wenn Sie ein Objekt in eine andere Domäne in derselben Gesamtstruktur verschieben, weist Active Directory dem Objekt eine neue SID zu und behält die GUID bei.

Sicherheitsauswirkungen des SID-Verlaufs

Der SID-Verlauf ermöglicht migrierten Benutzern den kontinuierlichen Zugriff auf die Ressourcen in ihren alten Domänen. Allerdings ist es Benutzern dadurch auch möglich, unzulässigerweise auf andere Domänen zuzugreifen – d. h., dass eine Übertragung scheinbar von einem autorisierten Benutzer stammt–, indem SIDs anderer Domänen in den SID-Verlauf ihrer Benutzerkonten gestellt werden. Zum Schutz vor einem derartigen Spoofing können Sie SID-Filter auf Vertrauensstellungen anwenden.

Achtung SID-Filter sind für Vertrauensstellungen zwischen Gesamtstrukturen oder für externe Vertrauensstellungen gedacht. Eine falsche Anwendung von SID-Filtern wäre, sie zwischen Domänen in derselben Gesamtstruktur zu verwenden. Wenn Sie eine Domäne innerhalb derselben Gesamtstruktur unter Quarantäne stellen, werden beim SID-Filtervorgang die SIDs entfernt, die für die Active Directory-Replikation erforderlich sind. Durch Verwendung von SID-Filtern kann die Authentifizierung von Benutzern aus Domänen mit transitiver Vertrauensstellung durch die unter Quarantäne gestellte Domäne fehlschlagen.

Entfernen Sie die SID-Verlaufsinformationen aus dem Benutzerkonto, damit ein zwischen Domänen verschobenes Benutzerkonto nicht mithilfe von Berechtigungen, die dem SID-Verlaufsattribut zugeordnet sind, auf Ressourcen zugreifen kann.

Anmerkung Weitere Informationen zum Entfernen des SID-Verlaufs finden Sie im Artikel 295758, „HOWTO: Use Visual Basic Script to Clear SidHistory“ in der Microsoft Knowledge Base unter http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B295758 (nur auf Englisch verfügbar).

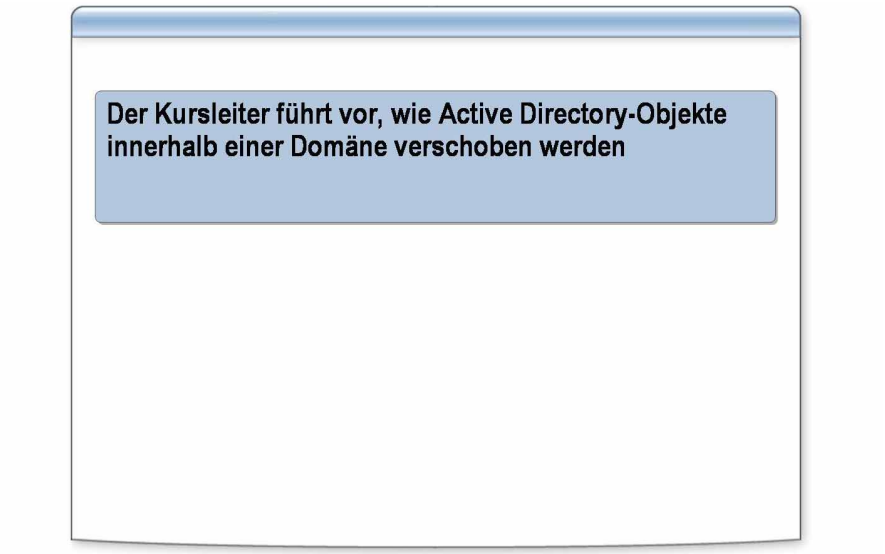
Weitere Auswirkungen der Objektverschiebung

Beachten Sie die folgenden zusätzlichen Auswirkungen beim Verschieben von Objekten in Active Directory:

- Benutzerkonten mit Administratorrechten für die Organisationseinheit, in die ein Benutzerkonto verschoben wird, können die Eigenschaften des verschobenen Benutzerkontos verwalten.
- Die Gruppenrichtlinienbeschränkungen der Organisationseinheit, Domäne oder Site, aus der das Benutzerkonto verschoben wurde, gelten nicht mehr für das Benutzerkonto.

  Für das Benutzerkonto gelten die Gruppenrichtlinieneinstellungen am neuen Standort.

Anleitung: Verschieben von Objekten innerhalb einer Domäne



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

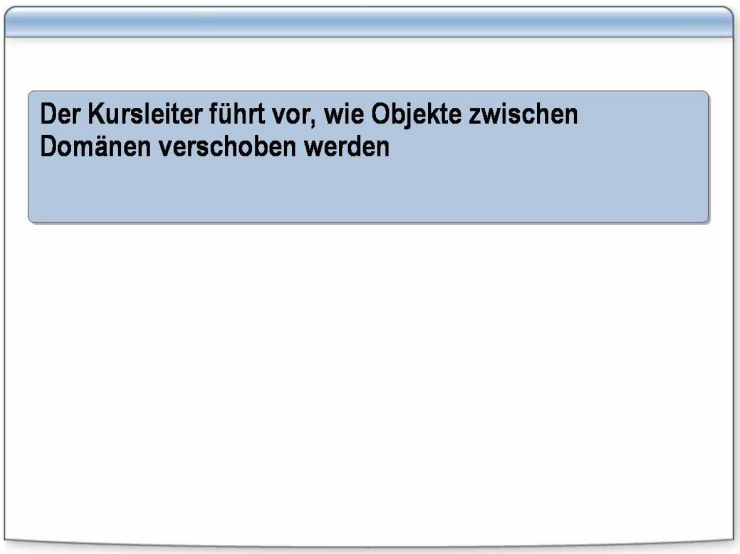
Objekte werden in einer Domäne mithilfe von Active Directory-Benutzer und -Computer verschoben.

Verfahren

Führen Sie die folgenden Schritte, aus um ein Objekt in einer Domäne zu verschieben:

- Ziehen Sie das Objekt im Detailfenster von Active Directory-Benutzer und -Computer zum neuen Container.

Anleitung: Verschieben von Objekten zwischen Domänen



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Verwenden Sie das Active Directory-Migrationsprogramm in Windows Server 2003, um Objekte von einer Domäne in einer Gesamtstruktur in eine andere Domäne in einer anderen Gesamtstruktur zu verschieben.

Verfahren

Führen Sie die folgenden Schritte aus, um Benutzer oder Gruppen von einer Domäne zu einer anderen zu migrieren:

1. Führen Sie das Active Directory-Migrationsprogramm aus.

   Anmerkung Das Active Directory-Migrationsprogramm wird nicht standardmäßig installiert. Sie können es über den Ordner \i386\ADMT der Windows Server 2003-CD installieren.

2. Klicken Sie mit der rechten Maustaste auf **Active Directory-Migrationsprogramm**, und wählen Sie dann den Assistenten für das Objekt, das migriert werden soll.

   Wenn Sie z. B. ein Benutzerkonto verschieben möchten, klicken Sie auf **Assistent zum Migrieren von Benutzerkonten**.

3. Klicken Sie auf der Seite **Willkommen** auf **Weiter**.
4. Führen Sie anhand der folgenden Schritte eine Testmigration durch:
   a. Klicken Sie auf der Seite **Testen oder Änderungen vornehmen** auf **Die Migrationseinstellungen testen und später migrieren**, und klicken Sie dann auf **Weiter**.
   b. Wählen Sie auf der Seite **Domänenauswahl** die Quelldomäne und die Zieldomäne aus, und klicken Sie dann auf **Weiter**.
   c. Klicken Sie auf der Seite **Benutzerauswahl** auf **Hinzufügen**, geben Sie den Objektnamen ein, klicken Sie auf **OK** und dann auf **Weiter**.
   d. Klicken Sie auf der Seite **Auswahl der Organisationseinheit** auf **Durchsuchen**, wählen Sie den Zielcontainer aus, klicken Sie auf **OK** und dann auf **Weiter**.

e. Legen Sie auf der Seite **Benutzeroptionen** die Benutzeroptionen fest, und klicken Sie dann auf **Weiter**.

   Diese Optionen geben an, ob die Gruppenmitgliedschaft, die Profile und die Sicherheitseinstellungen migriert werden.

f. Wenn das Dialogfeld **Achtung** angezeigt wird, klicken Sie auf **OK**.

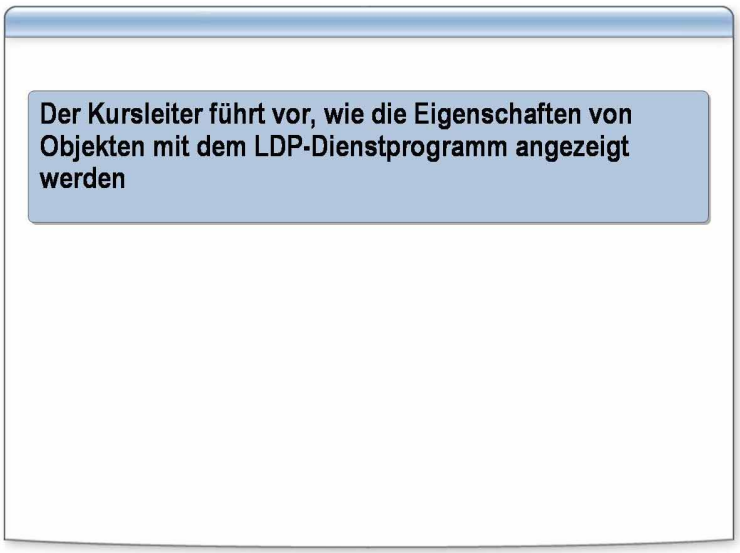
g. Wählen Sie auf der Seite **Namenskonflikte** die gewünschten Optionen aus, um anzugeben, wie bei einem Namenskonflikt vorzugehen ist, und klicken Sie dann auf **Weiter**.

h. Klicken Sie auf der Seite **Fertigstellen des Assistenten** auf **Fertig stellen**.

i. Klicken Sie im Dialogfeld **Migrationsstatus** auf **Protokoll anzeigen**, um das Fehlerprotokoll anzuzeigen.

5. Führen Sie eine tatsächliche Migration durch, indem Sie die Schritte 2 bis 4.l wiederholen. Wählen Sie in Schritt 4.a **Jetzt migrieren** anstelle von **Die Migrationseinstellungen testen und später migrieren**.

Anleitung: Verwenden von LDP zum Anzeigen der Eigenschaften verschobener Objekte



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

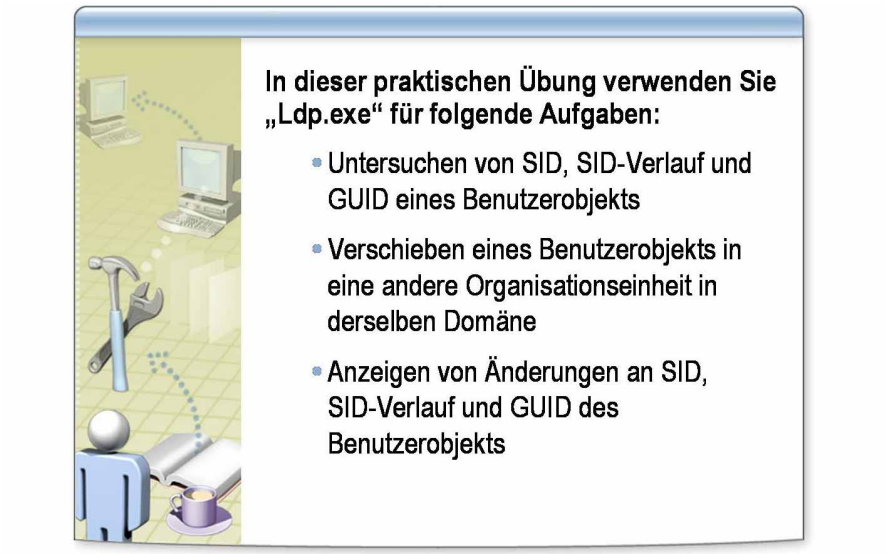
Nachdem Sie einen Benutzer, eine Gruppe oder ein anderes Objekt verschoben haben, müssen Sie überprüfen, ob die Eigenschaften des Objekts ordnungsgemäß aktualisiert wurden. Prüfen Sie z. B. die SID- und die SID-Verlaufseigenschaften des Objekts. Verwenden Sie Ldp.exe, um diese Informationen anzuzeigen. Sie müssen die Windows-Supporttools aus dem Ordner \Support\Tools auf der Windows Server 2003-CD installieren, bevor Sie Ldp.exe verwenden können.

Verfahren

Führen Sie die folgenden Schritte aus, um die Eigenschaften eines verschobenen Objekts anzuzeigen:

1. Klicken Sie auf **Start**, klicken Sie auf **Ausführen**, geben Sie **ldp** ein, und klicken Sie auf **OK**.
2. Klicken Sie im Dialogfeld **Ldp** im Menü **Connection** (Verbindung) auf **Connect** (Verbinden).
3. Geben Sie im Dialogfeld **Connection** (Verbindung) im Feld **Server** den Namen Ihres Servers ein, und klicken Sie dann auf **OK**.
4. Klicken Sie im Dialogfeld **Ldp** im Menü **Connection** (Verbindung) auf **Bind** (Gebunden).
5. Geben Sie im Dialogfeld **Bind** (Gebunden) den Benutzernamen **Administrator**, das Administratorkennwort und den Namen der zu überprüfenden Domäne ein, und klicken Sie dann auf **OK**.
6. Klicken Sie dazu im Menü **View** (Ansicht) auf **Tree** (Struktur).
7. Wählen Sie in der **Tree View** (Baumansicht) in der Liste **BaseDN** den gewünschten Domänennamen aus der Liste aus, und klicken Sie dann auf **OK**.
8. Doppelklicken Sie in der Konsolenstruktur auf das Objekt, dessen Eigenschaften Sie anzeigen möchten.
9. Sehen Sie sich die Eigenschaften des Objekts im Detailfenster an.

Praktische Übung: Verschieben von Objekten



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Lernziele

In dieser praktischen Übung führen Sie die folgenden Aufgaben aus:

- Überprüfen von SID, SID-Verlauf und Globally Unique Identifier (GUID) eines Benutzerobjekts mithilfe von Ldp.exe.
- Verschieben eines Benutzerobjekts in eine andere Organisationseinheit in derselben Domäne.
- Anzeigen von Änderungen an SID, SID-Verlauf und GUID des Benutzerobjekts mithilfe von Ldp.exe.

Szenario

Ihre Organisation verfügt über 2.000 Benutzer. Brenda Diaz, ein Benutzer in Ihrer Domäne, hat in der Firma eine neue Position übernommen. Sie müssen ihr Benutzerkonto-Objekt verschieben, damit es ihrer neuen Aufgabe entspricht.

Praktische Übung

► **Verschieben Sie ein Benutzerkonto, und zeigen Sie die Änderungen an, die durch das Verschieben am Konto vorgenommen wurden**

1. Melden Sie sich als **Nwtraders***x**ComputerName*__User__ mit dem Kennwort **P@ssw0rd** an.
2. Überprüfen Sie mithilfe von Ldp.exe SID, SID-Verlauf und GUID des Benutzerobjekts von Brenda Diaz in der Organisationseinheit *IhrComputerName*\Sales, die sich in der Domäne Ihres Kursteilnehmercomputers befindet.
   a. Klicken Sie auf **Start**, klicken Sie auf **Eingabeaufforderung**, geben Sie **ldp** ein, und drücken Sie die EINGABETASTE.
   b. Klicken Sie im Dialogfeld **Ldp** im Menü **Connection** (Verbindung) auf **Connect** (Verbinden).
   c. Geben Sie im Dialogfeld **Connect** (Verbinden) im Textfeld **Server** den Namen Ihres Servers ein, und klicken Sie dann auf **OK**.

d. Klicken Sie im Dialogfeld **Ldp** im Menü **Connection** (Verbindung) auf **Bind** (Gebunden).

e. Geben Sie im Dialogfeld **Bind** (Gebunden) den Benutzernamen **Administrator**, das Kennwort **P@ssw0rd** und den Namen der Domäne auf Ihrem Server ein, und klicken Sie dann auf **OK**.

f. Klicken Sie dazu im Menü **View** (Ansicht) auf **Tree** (Struktur).

g. Wählen Sie im Dialogfeld **Tree View** (Baumansicht) in der Liste **BaseDN** Ihren Domänennamen aus, und klicken Sie dann auf **OK**.

h. Erweitern Sie in der Konsolenstruktur Ihre Domäne, doppelklicken Sie auf *IhrComputerName*, doppelklicken Sie auf das Objekt für die Organisationseinheit **Sales**, und doppelklicken Sie dann auf das Benutzerobjekt für Brenda Diaz.

i. Sehen Sie sich die Eigenschaften des Objekts im Detailfenster an.

i. Wie lautet die Objekt-GUID dieses Kontos?

Die Antworten variieren.

_____

ii. Wie lautet die Objekt-SID dieses Kontos?

Die Antworten variieren.

_____

iii. Gibt es für dieses Benutzerkonto einen Eintrag für den SID-Verlauf? Wenn ja, welche SIDs sind aufgelistet?

Für dieses Konto gibt es keinen Eintrag für einen SID-Verlauf.

_____

3. Verschieben Sie das Benutzerobjekt für Brenda Diaz zur Organisationseinheit *IhrComputerName*\HR in Ihrer Domäne.

a. Verwenden Sie **Ausführen als**, um die Active Directory-Benutzer und -Computer als *IhreDomäne***Administrator** mit dem Kennwort **P@ssw0rd** zu starten.

b. Ziehen Sie im Detailfenster das Benutzerobjekt **BrendaDia** von der Organisationseinheit *IhrComputerName*\Sales zur Organisationseinheit *IhrComputerName*\HR.

4. Überprüfen Sie mithilfe von Ldp.exe, ob SID, SID-Verlauf oder GUID des Benutzerobjekts für Brenda Diaz geändert wurde.

a. Doppelklicken Sie in der Konsolenstruktur auf **HR**, und klicken Sie dann auf das Benutzerobjekt für Brenda Diaz.

b. Sehen Sie sich die Eigenschaften des Objekts im Detailfenster an.

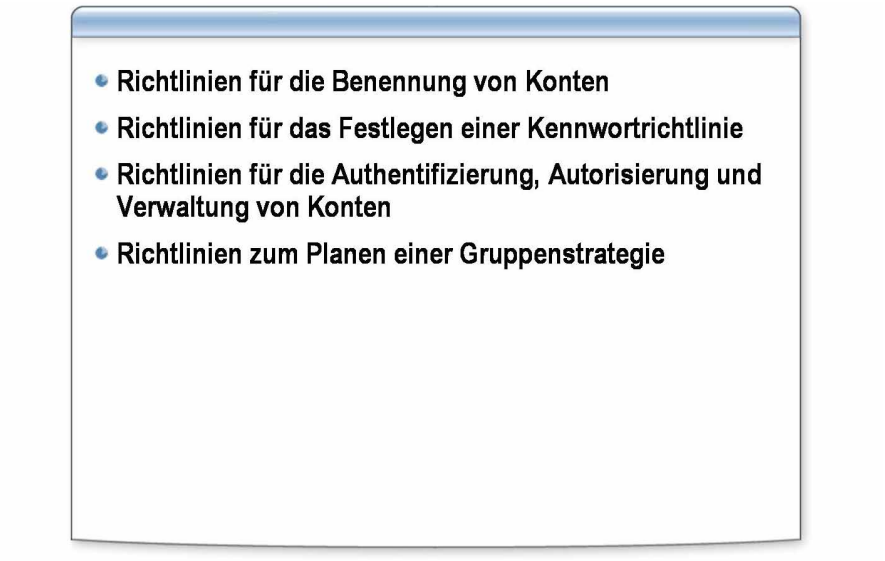
Wurde SID, SID-Verlauf oder GUID dieses Kontos geändert? Wenn dies der Fall ist, welche wurden geändert?

SID, SID-Verlauf und GUID des Benutzerkontos wurden bei diesem Verschiebevorgang nicht geändert.

_____

_____

Lektion: Planen einer Strategie für Benutzer-, Gruppen- und Computerkonten



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

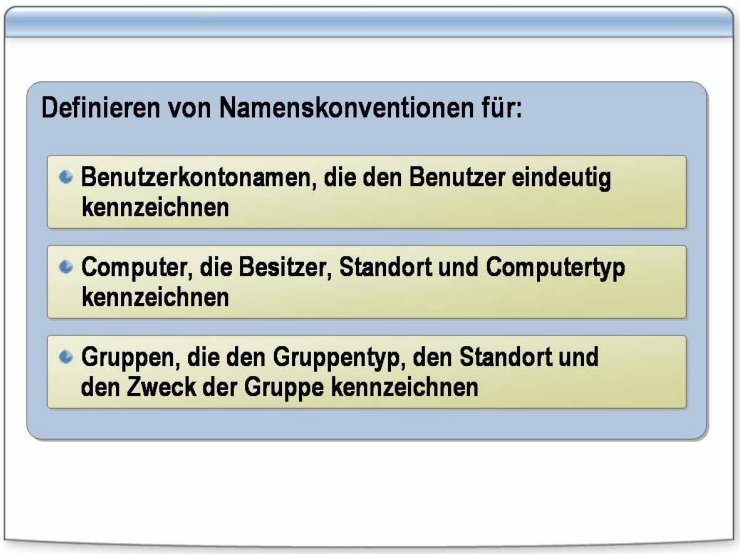
In dieser Lektion werden die Richtlinien zum Planen einer Strategie für Benutzer- und Computerkonten beschrieben. Eine gut geplante Kontenstrategie hilft, Sicherheitsverletzungen in Ihrem Netzwerk zu vermeiden.

Lernziele der Lektion

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Erklären von Richtlinien für die Definition einer Kontenbenennungskonvention.
- Erklären von Richtlinien zum Festlegen einer Kennwortrichtlinie.
- Erklären von Richtlinien für die Authentifizierung, Autorisierung und Verwaltung von Benutzerkonten.
- Erklären der Richtlinien zum Planen einer Strategie für Gruppenkonten.

Richtlinien für die Benennung von Konten



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Wenn Sie eine Kontenstrategie für die Gesamtstrukturen und Domänen im Netzwerk Ihrer Organisation erstellen, müssen Sie Konventionen für die Benennung von Konten festlegen.

Richtlinien

Die folgenden Richtlinien gelten für die Benennung von Benutzer-, Computer- und Gruppenkonten in einem Windows Server 2003-Netzwerk.

- Definieren Sie für Ihre Organisation eine Benennungskonvention für Benutzerkonten, damit die Benutzernamen von anderen Benutzern leicht ermittelt werden können und damit Sie in der Lage sind, Benutzernamenskonflikte für Benutzer mit sehr ähnlichem Namen zu verwalten. Die Benennungskonvention muss Folgendes umfassen:
  - Den Vornamen, die ersten drei Buchstaben vom Vornamen oder den Anfangsbuchstaben des Vornamens des Benutzers. Verwenden Sie z. B. Brenda für den Benutzer Brenda Diaz.
  - Den Anfangsbuchstaben, die ersten Buchstaben des Nachnamens oder den vollständigen Nachnamen des Benutzers. Verwenden Sie z. B. BrendaDiaz für den Benutzer Brenda Diaz.
  - Weitere Zeichen aus dem Vor- oder Nachnamen oder den Anfangsbuchstaben des zweiten Vornamens, um Namenskonflikte zu lösen.

Ziehen Sie die Verwendung von Folgendem in Erwägung:

- Präfixe oder Suffixe zum Kennzeichnen spezieller Benutzerkontotypen, wie z.B. Vertragspartner, Teilzeitarbeitskräfte und Dienstkonten.
- Einen alternativen Domänennamen für den Benutzerprinzipalnamen-Suffix, um die Anmeldesicherheit zu erhöhen und die Anmeldenamen zu vereinfachen.

  Wenn Ihre Organisation z. B. eine tiefe, nach Abteilung und Region organisierte Domänenstruktur besitzt, können die Domänennamen sehr lang werden. Der standardmäßig verwendete Benutzerprinzipalnamen-Suffix für einen Benutzer in einer Domäne könnte sales.example.nwtraders.msft lauten. Der Anmeldename für einen Benutzer mit dem Namen Brenda Diaz in dieser Domäne könnte BDiaz@sales.example.nwtraders.msft sein. Wenn Sie jedoch das Suffix nwtraders oder nwtraders.msft erstellen, kann sich ein Benutzer mit einem viel einfacheren Anmeldenamen anmelden, wie z. B. BDiaz@nwtraders oder BDiaz@nwtraders.msft. Dieses alternative Benutzerprinzipalnamen-Suffix muss kein gültiger DNS-Name sein.

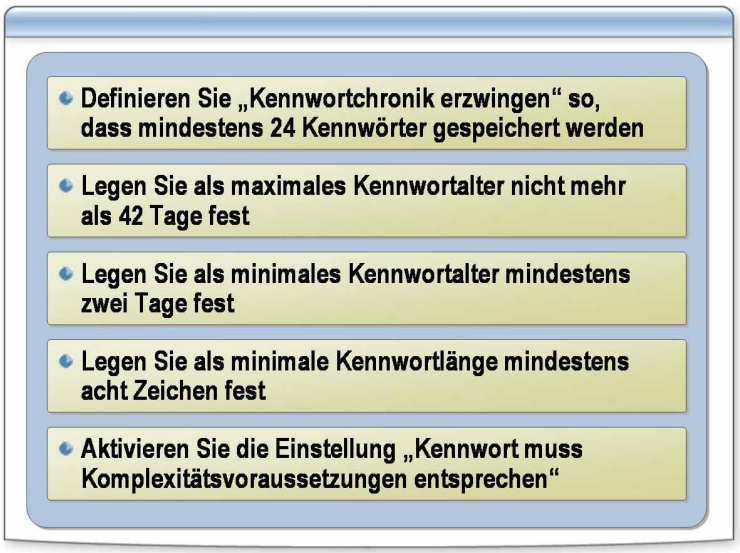
- Definieren Sie eine Benennungskonvention für Computerkonten, die den Besitzer, den Standort und den Computertyp kennzeichnet. Schließen Sie die folgenden Informationen in die Benennungskonvention ein.

Benennungskonvention	Beispiel
Benutzername des Besitzers	BrendaD1
Standort oder Abkürzung	RED oder Redmond
Computertyp oder Abkürzung	SVR oder Server

- Definieren Sie eine Gruppenbenennungskonvention, die den Gruppentyp, den Standort und den Zweck der Gruppe kennzeichnet. Schließen Sie die folgenden Informationen in die Benennungskonvention ein.

Benennungskonvention	Beispiel
Gruppentyp	G für eine globale Gruppe, UN für eine universelle Gruppe, DL für eine lokale Domänengruppe
Standort der Gruppe	Red für Redmond
Zweck der Gruppe	Admins für Administratoren

Richtlinien für das Festlegen einer Kennwortrichtlinie



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Die Rolle von Kennwörtern bei der Sicherung eines Organisationsnetzwerks wird oftmals unterschätzt und übersehen. Kennwörter bilden die erste Verteidigungslinie gegen den nicht autorisierten Zugriff auf Ihre Organisation.

Die Windows Server 2003-Produktfamilie verfügt über ein neues Feature, das die Komplexität von Kennwörtern für das Administratorkonto überprüft. Wenn das Kennwort leer ist oder den Komplexitätsvoraussetzungen nicht entspricht, wird das Dialogfeld **Windows Setup** angezeigt, das vor den Gefahren warnt, die bei der Verwendung eines nicht sicheren Kennworts für das Administratorkonto bestehen. Wenn Sie das Kennwort leer lassen, können Sie nicht über das Netzwerk auf das Konto zugreifen.

Richtlinien

Eine Kennwortrichtlinie stellt sicher, dass alle Benutzer die Kennwortvorgaben befolgen, die Sie für Ihre Organisation als angemessen festlegen. Definieren Sie die folgenden Elemente einer Kennwortrichtlinie:

- Definieren Sie die Richtlinieneinstellung **Kennwortchronik erzwingen**, damit mindestens 24 vorhergehende Kennwörter gespeichert werden. Auf diese Weise können die Benutzer ein abgelaufenes Kennwort nicht noch einmal verwenden.
- Definieren Sie die Richtlinieneinstellung **Maximales Kennwortalter**, so dass die Kennwörter so oft ablaufen, wie für Ihre Umgebung und die Zugriffsebene der Benutzer erforderlich ist. Diese Richtlinieneinstellung verhindert, dass ein Angreifer, der ein Kennwort knackt, bis zum Ablauf des Kennworts auf das Netzwerk zugreifen kann. Für Benutzer mit Domänenadministratorzugriff legen Sie das maximale Kennwortalter niedriger als das für normale Benutzer fest.
- Definieren Sie die Richtlinieneinstellung **Minimales Kennwortalter**, so dass die Benutzer ihr Kennwort erst nach einer bestimmten Anzahl an Tagen ändern können. Wenn Sie ein minimales Kennwortalter definieren, können die Benutzer ihr Kennwort nicht wiederholt ändern, um die Richtlinieneinstellung **Kennwortchronik erzwingen** zu umgehen und ihr ursprüngliches Kennwort zu verwenden.

- Definieren Sie eine Richtlinieneinstellung **Minimale Kennwortlänge**, so dass die Kennwörter aus einer Mindestanzahl an Zeichen bestehen müssen. Lange Kennwörter mit mindestens acht Zeichen sind in der Regel sicherer als kurze Kennwörter. Diese Richtlinieneinstellung verhindert außerdem die Verwendung leerer Kennwörter.
- Aktivieren Sie die Richtlinieneinstellung **Kennwort muss Komplexitätsvoraussetzungen entsprechen**. Diese Einstellung überprüft alle neuen Kennwörter, um sicherzustellen, das sie die Basisanforderungen an sichere Kennwörter erfüllen.

  Ein sicheres Kennwort weist folgende Merkmale auf:

  - Es ist mindestens acht Zeichen lang.
  - Es enthält keinen Benutzernamen, richtigen Namen oder Unternehmensnamen.
  - Es enthält kein vollständiges Wort aus einem Wörterbuch.
  - Es unterscheidet sich erheblich von vorhergehenden Kennwörtern. Inkrementelle Kennwörter (*Kennwort1*, *Kennwort2*, *Kennwort3*...) sind nicht sicher.
  - Es enthält Groß- und Kleinbuchstaben, Zahlen und Symbole.
  - Es enthält erweiterte ASCII-Zeichen. Zu diesen Zeichen gehören Akzentzeichen und spezielle Symbole, die zum Erstellen von Bildern verwendet werden.

  Beispiele für sichere Kennwörter sind: *H!elZl2o* und *J*p2leO4>©F*.

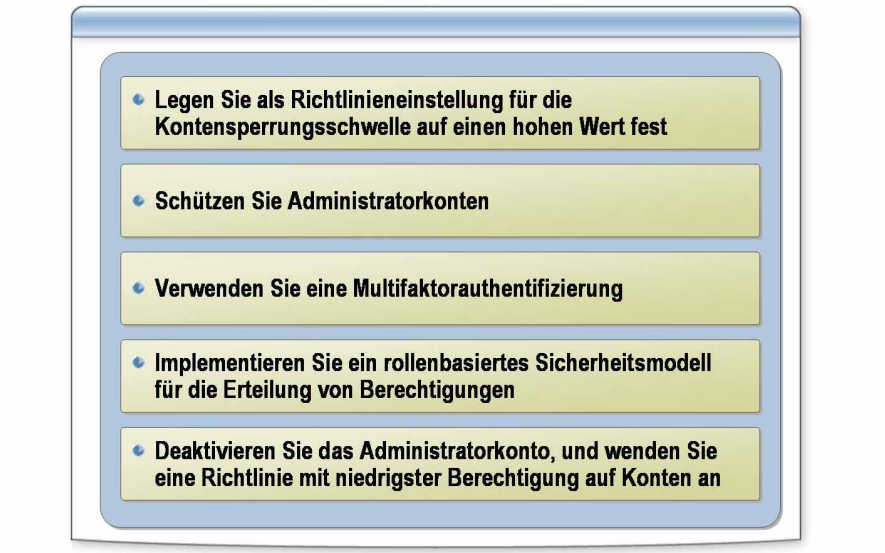
Achtung Potenzielle Angreifer finden erweiterte ASCII-Zeichen in der Zeichentabelle. Verwenden Sie kein erweitertes Zeichen, wenn kein Tastaturanschlag in der rechten unteren Ecke der Zeichentabelle definiert ist. Bevor Sie erweiterte ASCII-Zeichen in Ihrem Kennwort verwenden, müssen Sie diese sorgfältig testen, um sicherzustellen, dass die Kennwörter mit erweiterten ASCII-Zeichen mit den in Ihrer Organisation verwendeten Anwendungen kompatibel sind. Seien Sie besonders vorsichtig bei der Verwendung von erweiterten ASCII-Zeichen in Kennwörtern, wenn Ihre Organisation mehrere Betriebssysteme verwendet.

Die folgende Tabelle zeigt die empfohlenen minimalen Kennwortrichtlinieneinstellungen für sichere Netzwerkumgebungen.

Einstellung	Wert
Kennwortchronik erzwingen	24 gespeicherte Kennwörter
Maximales Kennwortalter	42 Tage
Minimales Kennwortalter	2 Tage
Minimale Kennwortlänge	8 Zeichen
Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
Kennwort mit umkehrbarer Verschlüsselung speichern	Deaktiviert

Tipp Wenn Sie in Ihrer Gesamtstruktur eine Stammdomäne zum Platzieren von Administratorkonten erstellen, müssen Sie bedenken, dass für diese Domäne strengere Kennwortrichtlinieneinstellungen erforderlich sind als für Ihre Kontodomäne. Ziehen Sie z. B. ein maximales Kennwortalter von 30 Tagen, ein minimales Kennwortalter von sieben Tagen und eine minimale Kennwortlänge von 14 Zeichen in Erwägung.

Richtlinien für die Authentifizierung, Autorisierung und Verwaltung von Konten



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Die Planung einer Strategie zur Kontoauthentifizierung, -autorisierung und -verwaltung schützt das Netzwerk Ihrer Organisation. Implementieren Sie beispielsweise eine Kontosperrungsrichtlinie, um einen Angriff auf Ihre Organisation zu verhindern. Seien Sie beim Erstellen von Kontosperrungsrichtlinien jedoch vorsichtig, damit Sie autorisierte Benutzer nicht versehentlich sperren.

Richtlinien

Verwenden Sie die folgenden Richtlinien zum Authentifizieren, Autorisieren und Verwalten von Konten in Ihrer Organisation:

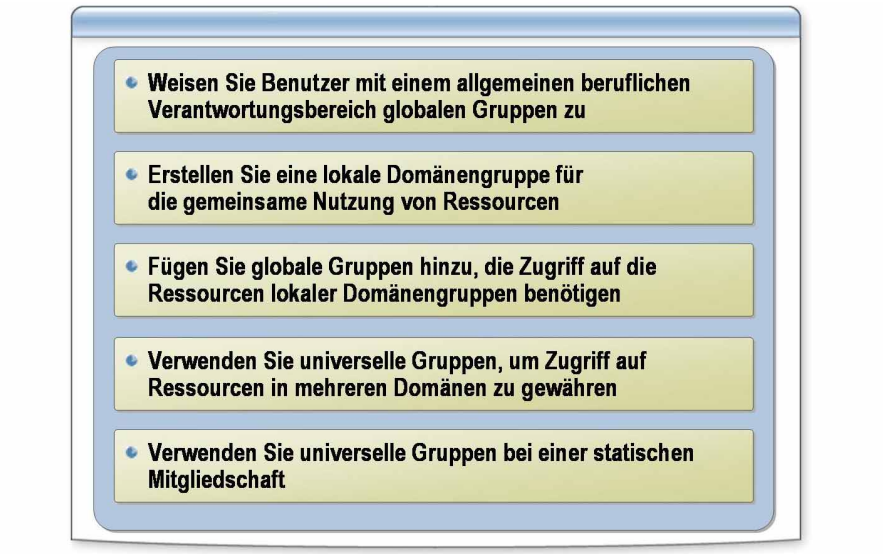
- *Legen Sie die Richtlinieneinstellung für die Kontensperrungsschwelle auf einen hohen Wert fest*. Auf diese Weise werden autorisierte Benutzer nicht für ihre Benutzerkonten gesperrt, wenn sie ein Kennwort falsch eingeben.

  Windows kann autorisierte Benutzer sperren, wenn sie ihr Kennwort auf einem Computer ändern und auf einem anderen nicht. Der Computer, der das alte Kennwort verwendet, versucht kontinuierlich, den Benutzer mit dem falschen Kennwort zu authentifizieren. Schließlich sperrt der Computer das Benutzerkonto so lange, bis es wiederhergestellt ist. Dieses Problem tritt bei den Organisationen nicht auf, die nur Domänencontroller aus der Windows Server 2003-Produktfamilie verwenden.
- *Verwenden Sie keine Administratorkonten zum Durchführen routinemäßiger Datenverarbeitungsaufgaben*. Minimieren Sie außerdem die Anzahl der Administratoren, und erteilen Sie Benutzern keine Administratorrechte. Verlangen Sie von Administratoren, sich unter Verwendung eines normalen Benutzerkontos anzumelden und alle Verwaltungsaufgaben mit dem Befehl **runas** auszuführen.
- *Verwenden Sie eine Multifaktorauthentifizierung*. So können z. B. für Administratorkonten und Remotezugriff Smartcards erforderlich sein, die überprüfen, ob der Benutzer auch der Benutzer ist, für den er sich ausgibt.

- *Verwenden Sie Sicherheitsgruppen auf der Grundlage der A-G-U-DL-P-Strategie*. Diese Strategie bietet die höchste Flexibilität, während sie gleichzeitig die Komplexität beim Zuweisen von Zugriffsberechtigungen zum Netzwerk reduziert. Implementieren Sie darüber hinaus ein rollenbasiertes Sicherheitsmodell für die Erteilung von Berechtigungen. In der A-G-U-DL-P-Strategiedomäne gilt Folgendes:
  - Benutzerkonten (A) werden zu globalen Gruppen (G) hinzugefügt.
  - Globale Gruppen werden zu universellen Gruppen (U) hinzugefügt.
  - Universelle Gruppen werden zu lokalen Domänengruppen (DL) hinzugefügt.
  - Ressourcenberechtigungen (P) werden lokalen Domänengruppen zugewiesen.
- *Deaktivieren Sie das Administratorkonto, und weisen Sie Benutzern und Administratoren die niedrigste Berechtigung zu, die sie zum Ausführen ihrer Aufgaben benötigen*.

  Sie können das Administratorkonto niemals aus der vordefinierten Gruppe Administratoren löschen oder entfernen. Allerdings sollten Sie das Konto deaktivieren. Selbst bei deaktiviertem Administratorkonto kann ein Angreifer oder ein nicht autorisierter Benutzer mit dem abgesicherten Modus auf einen Domänencontroller zugreifen. Dies kann nur verhindert werden, indem Sie die Server physisch sichern.

Richtlinien zum Planen einer Gruppenstrategie



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Beim Planen einer Gruppenstrategie müssen Sie planen, wie globale Gruppen, lokale Domänengruppen und universelle Gruppen verwendet werden, um die Verwaltungsaufgaben zu vereinfachen.

Richtlinien

Verwenden Sie die folgenden Richtlinien zum Planen einer Gruppenstrategie:

- *Weisen Sie Benutzer mit einem allgemeinen beruflichen Verantwortungsbereich globalen Gruppen zu*. Ermitteln Sie die Gruppen auf der Grundlage der Aufgaben, die von den Mitgliedern ausgeführt werden. Erstellen Sie globale Gruppen für diese Benutzer, und fügen Sie Benutzern die allgemeine Aufgaben ausführen, zu diesen Gruppen hinzu.
- *Erstellen Sie eine lokale Domänengruppe für die gemeinsame Nutzung von Ressourcen*. Ermitteln Sie freigegebene Ressourcen, wie Drucker, Dateien und Ordner. Erstellen Sie danach eine lokale Domänengruppe für jede der Ressourcen, und fügen Sie Benutzer hinzu, die Zugriff auf diese Ressourcen benötigen.
- *Fügen Sie globale Gruppen hinzu, die Zugriff auf die Ressourcen lokaler Domänengruppen benötigen*. Wenn Sie eine Ressource in einer Domäne für mehrere globale Gruppen freigeben möchten, fügen Sie diese globalen Gruppen zur lokalen Domänengruppe hinzu, die Zugriff auf die freigegebene Ressource gewährt.
- *Verwenden Sie universelle Gruppen, um Zugriff auf Ressourcen in mehreren Domänen zu gewähren*. Wenn Benutzerkonten Zugriff auf Dateifreigaben benötigen, die sich nicht in der Domäne der Benutzerkonten befinden, erstellen Sie eine universelle Gruppe für diese Benutzer und gewähren für die Dateifreigaben Zugriff auf die universelle Gruppe.
- *Verwenden Sie universelle Gruppen bei einer statischen Mitgliedschaft*. Universelle Gruppen funktionieren am besten, wenn Sie Benutzer hinzufügen, die wahrscheinlich nur selten aus der universellen Gruppe entfernt werden. Active Directory repliziert alle Änderungen in der Mitgliedschaft einer universellen Gruppe, wodurch der Netzwerkdatenverkehr erhöht wird.

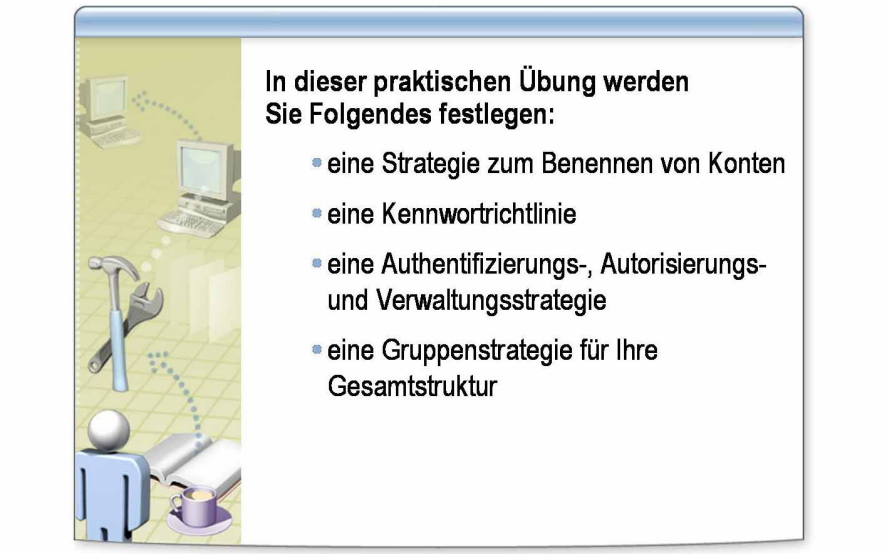
Anmerkung Wenn die Gesamtstrukturfunktionsebene auf Windows 2000 pur festgelegt ist und an der Mitgliedschaft einer universellen Gruppe eine Änderung vorgenommen wird, repliziert Active Directory die gesamte Liste der Mitglieder für alle anderen globalen Katalogserver. Wenn die Gesamtstrukturfunktionsebene auf Windows Server 2003 festgelegt wurde, werden nur die Änderungen für die anderen globalen Katalogserver repliziert. Anders ausgedrückt bedeutet dies, dass häufigere Änderungen an der universellen Gruppenmitgliedschaft geringere Auswirkungen auf das Netzwerk haben als in einer Windows 2000-Gesamtstrukturfunktionsebene.

Planen von Gruppenkonten

Verwenden Sie die folgende Tabelle zum Planen von Gruppenkonten. Die Tabelle enthält Beispieldaten für eine universelle Gruppe mit dem Namen U RedAccts, die in der Domäne Redmond erstellt wird. Die Mitglieder umfassen globale Gruppen der Domänen London, Vancouver und Denver.

Gruppe	Beschreibung	Standort	Typ	Mitglieder
U RedAccts	Buchhaltung	Domäne Redmond	Universelle Gruppe	G LonAccts G VanAccts G DenAccts

Praktische Übung: Planen einer Kontenstrategie



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Lernziele

In dieser praktischen Übung werden Sie folgende Aufgaben ausführen:

- Festlegen der Strategie zum Benennen von Konten.
- Festlegen der Kennwortrichtlinie.
- Festlegen der Authentifizierungs-, Autorisierungs- und Verwaltungsstrategie.
- Festlegen der Gruppenstrategie für Ihre Gesamtstruktur.

Szenario

Ihre Firma befindet sich in einer Unternehmensumgebung, die einem hohen Konkurrenzdruck ausgesetzt ist. Die Sicherheit der Geschäftsdaten und Geschäftsgeheimnisse Ihrer Firma ist äußerst wichtig. Ihre Organisation hat 1.000 Benutzer in einer Active Directory-Gesamtstruktur. Die Gesamtstruktur besteht aus einer leeren Stammdomäne mit dem Namen nwtraders.msft und einer untergeordneten Domäne mit dem Namen corp.nwtraders.msft, die alle Benutzer- und Gruppenkonten enthält. Alle Domänencontroller in Ihrer Gesamtstruktur führen Windows Server 2003 aus. Die Stammdomäne enthält nur Administratorkonten, die Sie zum Ausführen gesamtstrukturübergreifender Verwaltungsaufgaben verwenden.

Praktische Übung

► Planen einer Kontenstrategie

1. Welche Richtlinie zum Benennen von Konten verwenden Sie für die Benutzer in der Domäne corp?

   Die Antworten variieren. Eine mögliche Benennungsstrategie ist die, den Vornamen und den ersten Buchstaben vom Nachnamen der Benutzer zu verwenden. Wenn Namenskonflikte auftreten, lösen Sie diese, indem Sie mindestens zwei Buchstaben des Nachnamens verwenden, um einen eindeutigen Benutzernamen zu erstellen.

2. Welche Kennwortrichtlinieneinstellungen verwenden Sie für die Domäne corp?

   Ihre Richtlinieneinstellungen umfassen mindestens Folgendes:

   - **Kennwortchronik erzwingen** — **24 gespeicherte Kennwörter**
   - **Maximales Kennwortalter** — **42 Tage**
   - **Minimales Kennwortalter** — **2 Tage**
   - **Minimale Kennwortlänge** — **8 Zeichen**
   - **Kennwort muss Komplexitätsvoraussetzungen entsprechen** — **Aktiviert**
   - **Kennwort mit umkehrbarer Verschlüsselung speichern** — **Deaktiviert**

3. Welche Kennwortrichtlinieneinstellungen verwenden Sie für Ihre Stammdomäne?

   Ihre Richtlinieneinstellungen umfassen mindestens Folgendes:

   - **Kennwortchronik erzwingen** — **24 gespeicherte Kennwörter**
   - **Maximales Kennwortalter** — **30 Tage**
   - **Minimales Kennwortalter** — **7 Tage**
   - **Minimale Kennwortlänge** — **14 Zeichen**
   - **Kennwort muss Komplexitätsvoraussetzungen entsprechen** — **Aktiviert**
   - **Kennwort mit umkehrbarer Verschlüsselung speichern** — **Deaktiviert**

4. Was umfasst Ihre Authentifizierungs-, Autorisierungs- und Verwaltungsstrategie?

   Ihre Strategie muss Folgendes umfassen:

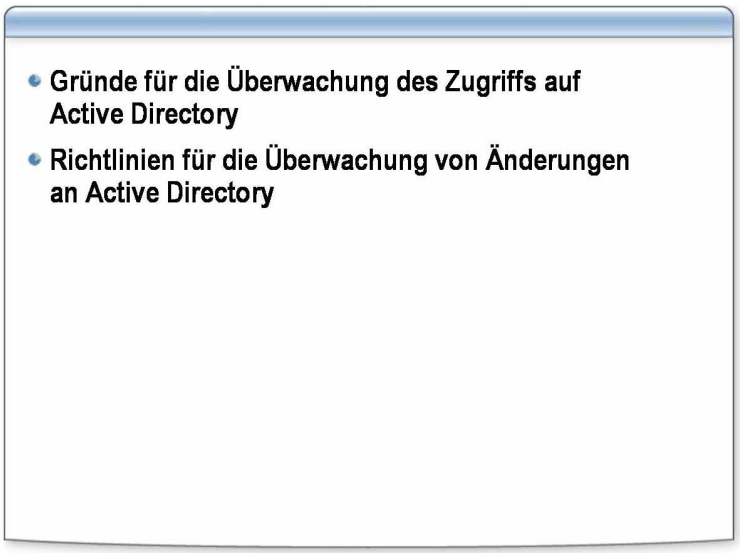
   - **Legen Sie eine Kontosperrungsrichtlinie fest, die Benutzerkonten nach sieben fehlgeschlagenen Anmeldeversuchen 30 Minuten lang sperrt.**
   - **Verlangen Sie von Administratoren, sich unter Verwendung eines normalen Benutzerkontos anzumelden und alle Verwaltungsaufgaben mit dem Befehl „runas“ auszuführen.**
   - **Verlangen Sie eine Smartcardauthentifizierung für alle Remotezugriffe auf Ihr Netzwerk.**
   - **Benennen Sie das Konto „Administrator“ in allen Domänen um, und deaktivieren Sie es.**
   - **Implementieren Sie ein rollenbasiertes Sicherheitsmodell bei der Planung von Gruppen.**

5. Was umfasst Ihre Gruppenstrategie?

   Ihre Strategie muss Folgendes umfassen:

   - **Weisen Sie Benutzer mit allgemeinem Verantwortungsbereich globalen Gruppen zu.**
   - **Erstellen Sie eine lokale Domänengruppe für freigegebene Ressourcen.**
   - **Fügen Sie globale Gruppen hinzu, die Zugriff auf die Ressourcen lokaler Domänengruppen benötigen.**
   - **Verwenden Sie keine universellen Gruppen (außer für die Gruppen „Organisations-Admins“ und „Schema-Admins“ in der Stammdomäne), weil alle Benutzerkonten ohne Administratorrechte, Gruppenkonten und Ressourcen in der Domäne „corp“ enthalten sind.**

Lektion: Planen einer Active Directory-Überwachungsstrategie



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

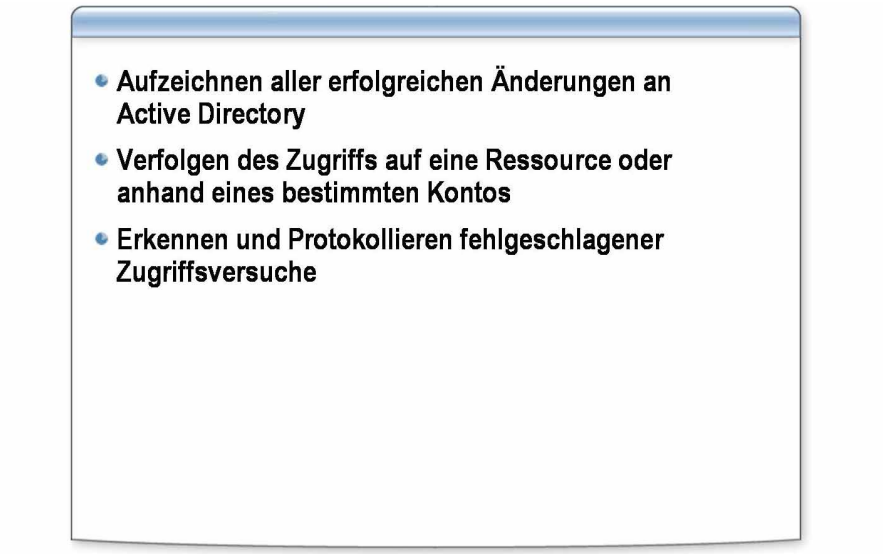
Am Ende dieser Lektion verstehen Sie, warum es wichtig ist, den Benutzerzugriff auf Active Directory zu überwachen und eine Active Directory-Überwachungsstrategie planen zu können.

Lernziele der Lektion

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Erklären, warum der Zugriff auf Active Directory überwacht werden muss.
- Erklären der Richtlinien für die Überwachung von Änderungen an Active Directory.

Gründe für die Überwachung des Zugriffs auf Active Directory



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Sie verwenden die Überwachung, um sicherheitsbezogene Aktivitäten auf einem System zu verfolgen. Da Active Directory Informationen zu allen Objekten in einem Windows Server 2003-Netzwerk speichert, müssen Sie Änderungen an diesen Objekten und deren Attributen verfolgen. So können Sie z. B. Änderungen an einer Gruppenmitgliedschaft oder Änderungen an Active Directory-Infrastrukturkomponenten (z. B. Siteobjekte oder das Active Directory-Schema) überwachen.

Zweck der Überwachung von Active Directory

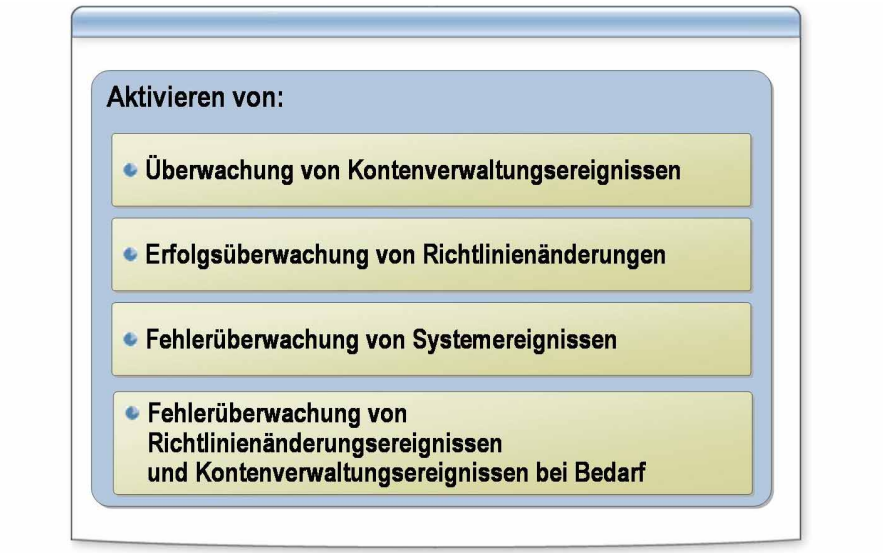
Beim Überwachen von Active Directory zeichnen Sie erfolgreiche Änderungen an Active Directory und fehlgeschlagene Versuche, Active Directory zu ändern, zu folgenden Zwecken auf:

- *Aufzeichnen aller erfolgreichen Änderungen an Active Directory*. Durch die Aufzeichnung aller erfolgreichen Änderungen stellen Sie sicher, dass das autorisierte Personal keine nicht autorisierten Änderungen an Active Directory-Objekten vornimmt. Diese Aufzeichnung ist auch nützlich, um falsche Änderungen an Active Directory zu korrigieren. Wenn beispielsweise Berechtigungen auf die falsche Gruppe angewendet wurden und damit die falsche Personengruppe Zugriff auf Ressourcen erhält, können Sie anhand des Überwachungspfads ermitteln, wann und von wem die Änderung vorgenommen wurde.

- *Verfolgen des Zugriffs auf eine Ressource oder anhand eines bestimmten Kontos*. Durch die Zugriffsverfolgung verstehen Sie Ereignisse, die in Ihrem Netzwerk auftreten. Wenn eine Anwendung z. B. ein Dienstkonto für den Zugriff auf Ressourcen verwendet und die Anwendung nicht richtig funktioniert, kann der Fehler anhand des Überwachungspfads ermittelt werden.
- *Erkennen und Protokollieren fehlgeschlagener Zugriffsversuche*. Durch die Aufzeichnung fehlgeschlagener Versuche, auf Ressourcen zuzugreifen oder Active Directory zu ändern, können Sie sowohl externe als auch interne Sicherheitsrisiken ermitteln.

Um erfolgreiche oder fehlgeschlagene Änderungen an Active Directory-Objekten oder -Attributen zu überwachen, müssen Sie die Überwachung von Verzeichnisdiensten auf allen Domänencontrollern aktivieren und die System Access Control List (SACL) für alle zu überwachenden Objekte oder Attribute konfigurieren.

Richtlinien für die Überwachung von Änderungen an Active Directory



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Einführung

Bei einer erfolgreichen Überwachung wird jedesmal ein Überwachungseintrag generiert, wenn ein Kontenverwaltungsereignis erfolgreich ausgeführt wurde. Obwohl erfolgreiche Kontenverwaltungsereignisse in der Regel harmlos sind, bieten sie eine äußerst wertvolle Aufzeichnung von Aktivitäten, die die Sicherheit eines Netzwerks gefährden können.

Richtlinien

Verwenden Sie die folgenden Richtlinien beim Erstellen einer Überwachungsstrategie:

- *Aktivieren Sie die Überwachung von Kontenverwaltungsereignissen*. Überwachen Sie folgende erfolgreichen Änderungen:
  - Das Erstellen, Ändern oder Löschen von Benutzer- oder Gruppenkonten
  - Das Aktivieren, Deaktivieren oder Umbenennen von Benutzerkonten
  - Das Ändern von Kennwörtern oder der Sicherheitsrichtlinie eines Computers
- *Aktivieren Sie die Erfolgsüberwachung von Richtlinienänderungen*. Wenn die Überwachung dieser Änderungen und der Änderung von Kontenverwaltungsrichtlinien nicht aktiviert ist, könnte ein Angreifer die Sicherheit eines Netzwerks ohne Überwachungspfad unterlaufen.

  Wenn ein Administrator z. B. das Benutzerkonto Sally als Mitglied der Gruppe Sicherungs-Operatoren definiert, würde die Überwachung ein Kontenverwaltungsereignis aufzeichnen. Wenn derselbe Administrator Sallys Konto das erweiterte Benutzerrecht **Dateien und Verzeichnisse sichern** erteilen würde, würde die Überwachung kein Kontenverwaltungsereignis aufzeichnen.

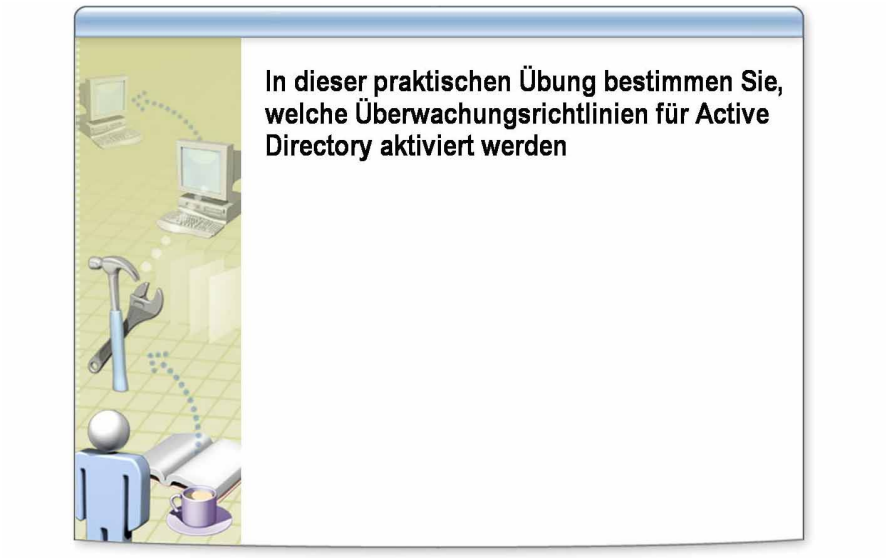
- *Aktivieren Sie die Fehlerüberwachung von Systemereignissen*. Diese Sicherheitseinstellung generiert ein Ereignis beim erfolglosen Versuch eines Benutzers, einen Computer neu zu starten oder herunterzufahren oder die Systemsicherheit oder das Sicherheitsprotokoll zu ändern. Aktivieren Sie diese Überwachungsrichtlinieneinstellung für die gesamte Domäne.

  Fehlerereignisse in der Systemereigniskategorie können ungewöhnliche Ereignisse aufdecken, z. B. einen Eindringling, der versucht, auf Ihren Computer oder Ihr Netzwerk zuzugreifen. Die Anzahl an Überwachungen, die bei aktivierter Einstellung generiert werden, ist relativ gering, und die Qualität der Informationen aus diesen Ereignissen ist relativ hoch.
- *Aktivieren Sie die Fehlerüberwachung von Richtlinienänderungsereignissen und Kontenverwaltungsereignissen nur bei Bedarf*. Die Anzahl der Überwachungen, die bei aktivierten Einstellungen generiert werden, ist sehr hoch. Daher sollten Sie diese Einstellung nur bei Bedarf aktivieren.

Achtung Die Aktivierung von Fehlerüberwachungen für diese Ereignisse kann ein Risiko für Ihre Organisation darstellen. Wenn Benutzer auf eine Ressource zuzugreifen versuchen, für die sie nicht autorisiert sind, können so viele Fehlerüberwachungen erzeugt werden, dass das Sicherheitsprotokoll voll wird und der Computer keine weiteren Überwachungen mehr erfassen kann. Wenn die Richtlinieneinstellung **Überwachung: System sofort herunterfahren, wenn Sicherheitsüberprüfungen nicht protokolliert werden können** aktiviert ist, werden die Server sofort heruntergefahren, wenn das Protokoll voll wird. Eindringlinge können in diesem Fall mithilfe Ihrer Überwachungsrichtlinie einen Dienstverweigerungsangriff initiieren.

Anmerkung Informationen zum Aktivieren der Überwachung finden Sie in der Unterrichtseinheit zum Überwachen von Konten und Ressourcen Unterrichtseinheit 10, „Implementieren von administrativen Vorlagen und Überwachungsrichtlinien“ im Kurs 2145A: *Verwalten einer Microsoft Windows Server 2003-Umgebung*.

Praktische Übung: Planen einer Überwachungsstrategie



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Lernziele

In dieser praktischen Übung bestimmen Sie, welche Überwachungsrichtlinien für Active Directory aktiviert werden.

Szenario

Sie müssen eine Überwachungsrichtlinie für die Firma Northwind Traders planen, die 1.000 Benutzer in einer Active Directory-Gesamtstruktur besitzt. Ihre Gesamtstruktur besteht aus einer leeren Stammdomäne mit dem Namen nwtraders.msft und einer untergeordneten Domäne mit dem Namen corp.nwtraders.msft. Die untergeordnete Domäne enthält alle Benutzer- und Gruppenkonten.

Praktische Übung

► **Planen Sie eine Überwachungsstrategie**

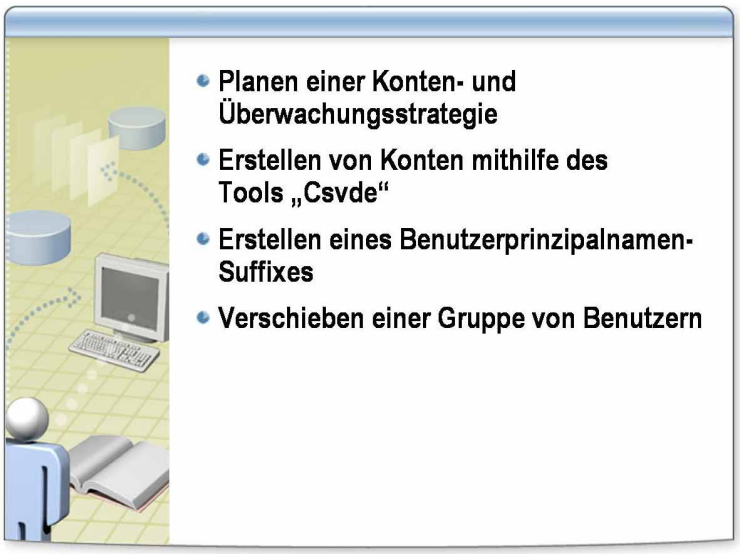
- Für welche Ereignisse aktivieren Sie eine Überwachung?

_____

_____

Die Antworten variieren. Die empfohlene Strategie besteht darin, die Erfolgsüberwachung für System, Richtlinienänderung und Kontenverwaltung sowie die Fehlerüberwachung für Systemereignisse zu aktivieren. Es empfiehlt sich nicht, die Fehlerüberwachung für andere Ereignisse zu aktivieren, es sei denn, Sie führen eine Überwachung zum Zwecke der Angriffserkennung aus.

Übungseinheit A: Implementieren einer Konten- und Überwachungsstrategie



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Lernziele

Am Ende dieser Übungseinheit werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Planen einer Strategie für Benutzer-, Gruppen- und Computerkonten.
- Planen einer Active Directory-Überwachungsstrategie.
- Erstellen mehrerer Benutzer- und Computerkonten.
- Implementieren von Benutzerprinzipalnamen-Suffixen.
- Verschieben von Objekten innerhalb einer Domäne und zwischen den Domänen in einer Gesamtstruktur.

Voraussetzungen

Bevor Sie diese Übungseinheit bearbeiten, müssen Sie folgende Voraussetzungen erfüllen:

- Sie müssen die Richtlinien zum Planen einer Kontenstrategie kennen.
- Sie müssen die Richtlinien zum Planen einer Überwachungsstrategie kennen.

Szenario

Die Firma Northwind Traders implementiert Windows Server 2003 auf ihrem Netzwerk. Sie plant die Verwendung einer Gesamtstruktur mit zwei Domänen, einer leeren Stammdomäne und einer Firmendomäne. Die Firmendomäne enthält die Benutzer-, Gruppen, und Computerkonten.

Veranschlagte Zeit für die Übungseinheit: 60 Minuten

Übung 1
Planen einer Konten- und Überwachungsstrategie

In dieser Übung planen Sie eine Strategie zum Benennen von Konten für die neue Gesamtstruktur der Firma Northwind Traders. Verwenden Sie die Richtlinien, die Ihnen das Entwicklungsteam gegeben hat.

Szenario

Die neue Gesamtstruktur besteht aus einer leeren Stammdomäne mit dem Namen nwtraders.msft und einer untergeordneten Domäne mit dem Namen corp.nwtraders.msft, die alle Benutzerkonten enthält. Die Firma Northwind Traders verfügt über Niederlassungen in sieben Städten.

Ihre Konten- und Überwachungsstrategie muss folgende Anforderungen berücksichtigen:

- Die Strategie zum Benennen von Benutzerkonten muss so gestaltet sein, dass die Mitarbeiter, die nur den Vor- und den Nachnamen eines anderen Benutzers kennen, problemlos die E-Mail-Adresse des gewünschten Benutzers ermitteln können.
- Die Strategie zum Benennen von Computerkonten muss so gestaltet sein, dass die Mitarbeiter den Standort und den Zweck eines Computers leicht ermitteln können.
- Alle Mitarbeiter müssen eine E-Mail-Adresse mit dem Format *Benutzername*@nwtraders.msft besitzen
- Die Überwachungsstrategie muss so beschaffen sein, dass nicht autorisierte Änderungsversuche an Active Directory erkannt werden.

Aufgaben
1. Planen Sie eine Strategie zum Benennen von Benutzerkonten für die Gesamtstruktur nwtraders.msft.
Woraus bestehen die Namen der Benutzerkonten?
Welche Strategie verwenden Sie, um Namenskonflikte bei Benutzerkonten zu lösen?
Was verwenden Sie als Benutzerprinzipalnamen-Suffix für Benutzerkonten?
2. Planen Sie eine Strategie zum Benennen von Computerkonten für die Gesamtstruktur nwtraders.msft.
Welche Benennungskonvention verwenden Sie für Servercomputer?

(*Fortsetzung*)

Aufgaben
Welche Benennungskonvention verwenden Sie für Clientcomputer?
3. Planen Sie eine Kennwortrichtlinie für die Gesamtstruktur nwtraders.msft.
Welche Kennwortrichtlinieneinstellungen wenden Sie auf die Domäne nwtraders.msft an?
Welche Kennwortrichtlinieneinstellungen wenden Sie auf die Domäne corp.nwtraders.msft an?
4. Planen Sie eine Überwachungsstrategie für die Gesamtstruktur nwtraders.msft.
Welche Einstellungen für die Erfolgsüberwachung nehmen Sie in Ihren Plan auf?
Welche Einstellungen für die Fehlerüberwachung nehmen Sie in Ihren Plan auf?

Übung 2
Erstellen von Konten mithilfe des Tools „Csvde“

In dieser Übung verwenden Sie das Befehlszeilenprogramm Csvde, um mehrere Konten aus einer mithilfe von Microsoft Excel erstellten CSV-Importdatei in Active Directory zu importieren.

Szenario

Als einer der Administratoren von Northwind Traders erhalten Sie täglich Anforderungen für neue Benutzerkonten. Ein Teammitglied gibt die Anforderungen in eine Kalkulationstabelle ein, die in einem CSV- (Comma Separated Value-) Format gespeichert wird. Zu Beginn jedes Arbeitstages sind Sie dafür verantwortlich, diese Datei in Active Directory zu importieren, um die Benutzerkonten zu erstellen.

Aufgaben	Spezifische Anweisungen
1. Verwenden Sie das Befehlszeilenprogramm Csvde, um die CSV-Datei in Active Directory zu importieren.	▪ Der Name der CSV-Datei ist mit dem Namen der Domäne Ihres Computers identisch. Sie finden diese Datei im Ordner <*Installationsordner*>Moc\2195A\Labfiles\Lab4 auf Ihrem Computer.
2. Stellen Sie mithilfe von Active Directory-Benutzer und -Computer fest, welche neuen Organisationseinheiten, Benutzer und Gruppen erstellt wurden.	

Welche neuen Organisationseinheiten wurden erstellt?

Welche der neuen Organisationseinheiten enthalten Benutzer- und Gruppenkonten?

Übung 3
Erstellen eines Benutzerprinzipalnamen-Suffixes

In dieser Übung erstellen Sie ein Benutzerprinzipalnamen-Suffix und lösen anschließend einen Benutzerprinzipalnamen-Suffixroutingkonflikt zwischen zwei Gesamtstrukturen.

Szenario

Die Benutzer in Ihrer Domäne möchten sich mit dem Benutzerprinzipalnamen-Suffix, das nur aus dem Namen der Stadt besteht, in der sie sich befinden, an ihrer Domäne anmelden können. Sie erstellen das Benutzerprinzipalnamen-Suffix in der Gesamtstruktur für Ihre Stadt.

Aufgaben	Spezifische Anweisungen
1. Erstellen Sie ein neues Benutzerprinzipalnamen-Suffix in der Gesamtstruktur mit dem Namen *NameIhrerStadt*.	**a.** Melden Sie sich als **Nwtraders***x**ComputerName***User** mit dem Kennwort **P@ssw0rd** an. **b.** Verwenden Sie **Ausführen als**, um die Active Directory-Domänen und -Vertrauensstellungen als *IhreDomäne***Administrator** mit dem Kennwort **P@ssw0rd** zu starten.
2. Aktivieren Sie das Routing des neuen Benutzerprinzipalnamen-Suffixes für die Gesamtstruktur nwtraders.msft.	

Wie lautet der Status des Benutzerprinzipalnamen-Suffixes *NameIhrerStadt* nach seiner Aktivierung?

Wie können Sie diesen Benutzerprinzipalnamen-Suffixroutingkonflikt lösen?

Übung 4
Verschieben einer Gruppe von Benutzern

In dieser Übung erteilen Sie einem freigegebenen Ordner auf Ihrem Server globale Gruppenberechtigungen. Sie verschieben die Gruppe und die zugehörigen Mitglieder anschließend zu einer Organisationseinheit in der anderen Domäne Ihrer Gesamtstruktur. Schließlich überprüfen Sie, ob die verschobene Gruppe immer noch über Berechtigungen für den freigegebenen Ordner auf Ihrem Server verfügt.

Szenario

Auf Grund der vor kurzem durchgeführten Reorganisation der Firma Northwind Traders muss eine Gruppe von Benutzern an einen neuen Standort wechseln. Dieser Verschiebevorgang hat auch Auswirkungen auf Active Directory, da die Gruppe und ihre Benutzerkonten an einen anderen Standort in der Gesamtstruktur verschoben werden müssen. Es wird mehrere Monate dauern, bevor die Server, die die Benutzerdaten enthalten, an einen anderen Ort gebracht werden können. Sie müssen sicherstellen, dass die Benutzer nach dem Verschiebevorgang auf Ihre Dateien zugreifen können.

Aufgaben	Spezifische Anweisungen
1. Erstellen Sie einen Ordner auf Ihrem Server mit dem Namen ITAdmin, und geben Sie ihn frei. Erteilen Sie der globalen Gruppe G IT Admins anschließend sowohl Berechtigungen für den NTFS-Vollzugriff auf den Ordner und Vollzugriff auf die Freigabe.	**a.** Melden Sie sich als **Nwtraders***x**ComputerName***User** mit dem Kennwort **P@ssw0rd** an. **b.** Verwenden Sie **Ausführen als**, um die Computerverwaltung als *IhreDomäne***Administrator** mit dem Kennwort **P@ssw0rd** zu starten.
2. Verwenden Sie Ldp.exe, um SID, SID-Verlauf und GUID des globalen Gruppenobjekts G IT Admins in der Organisationseinheit IT Admin\Groups in der Domäne Ihres Kursteilnehmercomputers zu überprüfen.	
Was ist für die Objekt-GUID-, Objekt-SID- und SID-Verlaufseinträge für die globale Gruppe **G IT Admins** aufgelistet?	
3. Installieren Sie das Active Directory-Migrationsprogramm auf Ihrem Computer.	**a.** Verwenden Sie **Ausführen als**, um eine Eingabeaufforderung als *IhreDomäne***Administrator** mit dem Kennwort **P@ssw0rd** zu starten. **b.** Starten Sie die Installation an der Eingabeaufforderung, indem Sie **\\London\OS\ADMT\ADMIGRATION.MSI** eingeben und dann die EINGABETASTE drücken, um die Installation zu starten.

(***Fortsetzung***)

Aufgaben	
4. Verwenden Sie das Active Directory-Migrationsprogramm, um die globale Gruppe G IT Admins und ihre Mitglieder in die Organisationseinheit IT Test\IT Test Move in der anderen Domäne der Gesamtstruktur zu verschieben.	▪ Verwenden Sie **Ausführen als**, um das Active Directory-Migrationsprogramm als **nwtraders*x*\Administrator** mit dem Kennwort **P@ssw0rd** zu öffnen. **Anmerkung:** Das Dialogfeld **Migrationsstatus** zeigt möglicherweise Fehler an. Die Fehler wurden generiert, als Sie die Benutzer und die Gruppe mit der verschobenen Erweiterung umbenannt haben. Ignorieren Sie diese Fehlermeldungen.
5. Verwenden Sie Ldp.exe, um SID, SID-Verlauf und GUID des globalen Gruppenobjekts G IT Admins in der Organisationseinheit IT Test\IT Test Move der Domäne zu überprüfen, in die es verschoben wurde.	**Anmerkung:** Die Gruppe **G IT Admins** wurde möglicherweise als Teil des Verschiebevorgangs in **G IT Adminsmoved** umbenannt. ▪ Nachdem Sie die Frage unten beantwortet haben, klicken Sie im Menü **Connection** (Verbindung) auf **Exit** (Beenden).
Was ist für die Objekt-GUID-, Objekt-SID- und SID-Verlaufseinträge für die globale Gruppe G IT Admins aufgelistet? _____ _____	
Wurden die Objekt-GUID-, Objekt-SID- oder SID-Verlaufseinträge als Folge des Verschiebevorgangs geändert? _____ _____	
6. Verwenden Sie Windows Explorer, um die Berechtigungen anzuzeigen, die dem Ordner ITAdmin, den Sie in Schritt 1 erstellt und freigegeben haben, zugewiesen wurden.	
Haben die Gruppen, denen Sie in Schritt 1 Berechtigungen für diesen Ordner erteilt haben, immer noch Vollzugriff auf den Ordner? Warum oder warum nicht? _____ _____	