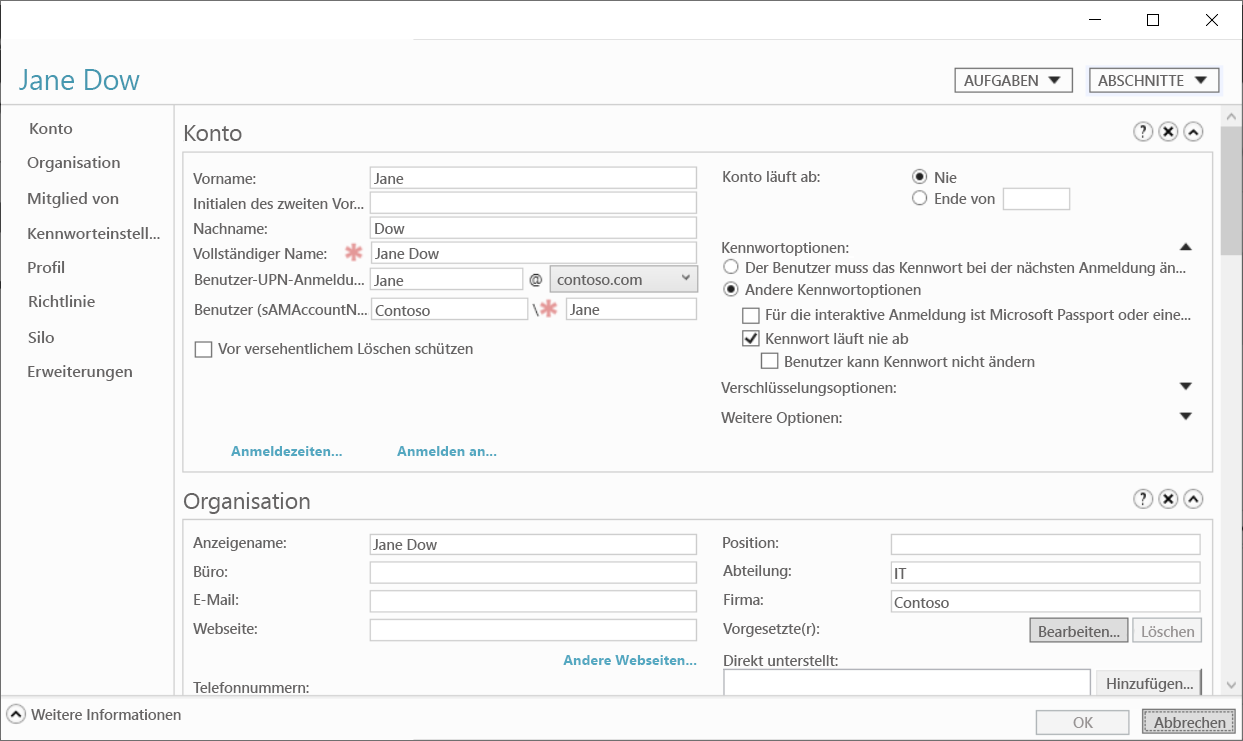
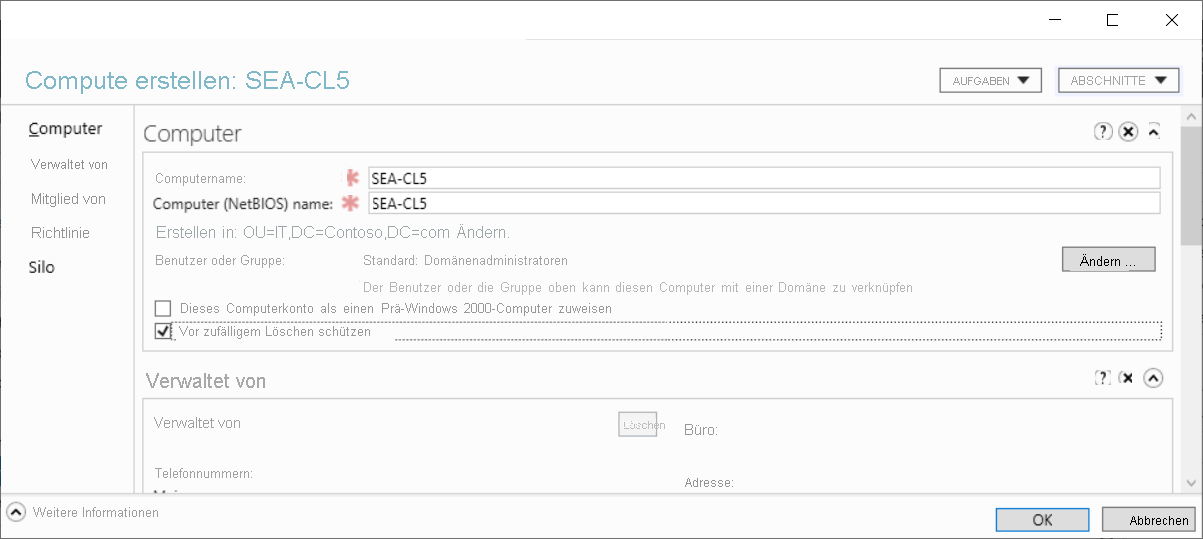
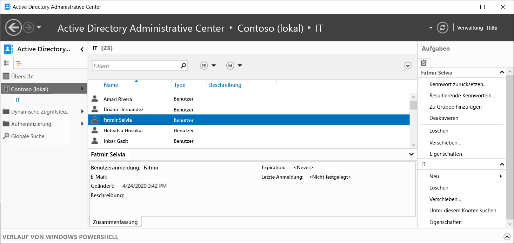
**Active Drectory Domain Services (AD DS)**

Lernziele:

* **Beschreiben von AD DS**
  + AD DS und die zugehörigen Dienste bilden die Grundlage für Unternehmensnetzwerke, in denen Windows-Betriebssysteme ausgeführt werden. Die AD DS-Datenbank ist der zentrale Speicher für alle Domänenobjekte wie Benutzerkonten, Computerkonten und Gruppen. AD DS bietet ein durchsuchbares, hierarchisches Verzeichnis und eine Methode zum Anwenden von Konfigurations- und Sicherheitseinstellungen für Objekte in einem Unternehmen.
  + AD DS-Optionen können Sie zum Ausführen folgender Aktionen verwenden:
    - Installieren, Konfigurieren und Aktualisieren von Apps
    - Verwalten der Sicherheitsinfrastruktur
    - Aktivieren von Remote Access Service und DirectAccess
    - Ausstellen und Verwalten digitaler Zertifikate
  + **Logische Komponenten**. Sind Strukturen, mit denen Sie ein AD DA-Design implementieren, das für eine Organisation geeignet ist. In einer AD DS-Datenbank sind folgende Typen logischer Komponenten enthalten:
    - Partition:
      * Eine Partition bzw. ein Namenskontext ist ein Teil der AD DS-Datenbank. Auch wenn die Datenbank aus nur einer Datei namens „Ntds.dit“ besteht, enthalten unterschiedliche Partitionen unterschiedliche Daten. Die Schemapartition beispielsweise enthält eine Kopie des Active Directory-Schemas. Die Konfigurationspartition enthält die Konfigurationsobjekte für die Gesamtstruktur, und die Domänenpartition enthält die Benutzer, Computer, Gruppen und andere domänenspezifische Objekte. Active Directory speichert Kopien der Partitionen auf mehreren Domänencontrollern und aktualisiert sie mithilfe der Verzeichnisreplikation.
    - Schema:
      * Ein Satz mit Definitionen von Objekttypen und Attributen, mit denen Sie die AD DS erstellten Objekte definieren.
    - Domäne:
      * Ein logischer Verwaltungscontainer für Objekte wie Benutzer und Computer. Eine Domäne ist einer bestimmten Partition zugeordnet und kann mithilfe von über-/untergeordneten Beziehungen zu anderen Domänen organisiert werden.
    - Domänenstruktur:
      * Eine Domänenstruktur ist eine hierarchische Sammlung von Domänen, die eine gemeinsame Stammdomäne und einen zusammenhängenden DNS-Namespace (Domain Name System) verwenden.
    - Gesamtstruktur:
      * Eine Gesamtstruktur ist eine Sammlung von einer oder mehreren Domänen, die über einen gemeinsamen AD DS-Stamm, ein gemeinsames Schema und einen gemeinsamen globalen Katalog verfügen.
    - OE (Organisationseinheit):
      * Ist ein Containerobjekt für Benutzer, Gruppen und Computer und stellt durch die Verknüpfung von Gruppenrichtlinienobjekten ein Framework zum Delegieren von Administratorrechten und Verwaltung bereit.
    - Container:
      * Ist ein Objekt, das ein organisationsbezogenes Framework für die Verwendung in AD DS bereitstellt. Sie können die Standardcontainer verwenden oder benutzerdefinierte Container erstellen. Gruppenrichtlinienobjekte können nicht mit Containern verknüpft werden.
  + **Physische Komponenten** in AD DS sind konkrete Objekte oder Objekte, die konkrete, reale Komponenten Beschreiben. Folgende sind einige davon:
    - Domänencontroller:
      * Enthält eine Kopie der AD DS-Datenbank. Bei den meisten Vorgängen kann jeder Domänencontroller Änderungen verarbeiten und die Änderungen auf alle anderen Domänencontroller in der Domäne replizieren.
    - Datenspeicher:
      * Auf jedem Domänencontroller ist eine Kopie des Datenspeichers vorhanden. Die AD DS-Datenbank verwendet die Microsoft Jet-Datenbanktechnologie und speichert die Verzeichnisinformationen in der Datei „Ntds.dit“ und den zugehörigen Protokolldateien. Diese Dateien werden standardmäßig im Ordner „C:\Windows\NTDS“ gespeichert.
    - Globaler Katalogserver:
      * Ist ein Domänencontroller, der den globalen Katalog hostet. Dabei handelt es sich um eine partielle, schreibgeschützte Kopie aller Objekte in einer Gesamtstruktur mit mehreren Domänen. Ein globaler Katalog beschleunigt die Suche nach Objekten, die möglicherweise auf Domänencontrollern in einer anderen Domäne innerhalb der Gesamtstruktur gespeichert sind.
    - Schreibgeschützter Domänencontroller (RODC):
      * Ist eine besondere, schreibgeschützte Installation von AD DS. RODCs sind üblich in Zweigniederlassungen mit suboptimaler physischer Sicherheit, mit weniger IT-Support als in den Hauptstellen des Unternehmens oder mit Branchenanwendungen, die auf einem Domänencontroller ausgeführt werden müssen.
    - Standort:
      * Ein Container für AD DS-Objekte wie Computer und Dienste, die speziell für einen physischen Standort erforderlich sind. Im Vergleich dazu stellt eine Domäne zusätzlich zu den Computern auch die logische Struktur von Objekten (z.B. Benutzer und Gruppen) dar.
    - Subnetz:
      * Ist ein Bestandteil der IP-Netzwerkadressen einer Organisation, die Computern an einem Standort zugewiesen sind. Ein-Standort kann über mehrere Subnetze verfügen.
* **Beschreiben von Benutzern, Gruppen und Computern**
  + Unter Windows Server ist ein **Benutzerkonto** ein Objekt, das alle Informationen enthält, die einen Benutzer beschreiben. Ein Benutzerkonto umfasst Folgendes:
    - Benutzername
    - Benutzerkennwort
    - Gruppenmitgliedschaften
  + Ein Benutzerkonto enthält auch Einstellungen, die Sie entsprechend den Anforderungen Ihrer Organisation konfigurieren können.
  + Benutzerobjekte in AD DS können an folgenden Stellen erstellt und verwaltet werden:
    - Active Directory-Verwaltungscenter
    - Active Directory-Benutzer und –Computer
    - Windows Admin Center
    - Windows PowerShell
    - Dsadd-Befehlszeilentool
  + **Dienstkonto.** Viele Apps enthalten Dienste, die Sie auf dem Server installieren, der das Programm hostet. Diese Dienste werden in der Regel beim Start des Servers ausgeführt oder durch andere Ereignisse ausgelöst. Dienste werden häufig im Hintergrund ausgeführt und erfordern keine Benutzerinteraktion. Damit ein Dienst gestartet und authentifiziert werden kann, verwenden Sie ein Dienstkonto. Ein Dienstkonto kann ein lokales Konto auf dem Computer sein (z. B. das lokale Dienstkonto, das Netzwerkdienstkonto oder das lokale Systemkonto, die alle bereits integriert sind). Sie können ein Dienstkonto auch so konfigurieren, dass ein domänenbasiertes Konto in AD DS verwendet wird.
  + ---------------------------------------------
  + Wenn beispielsweise mehrere Benutzer die gleiche Zugriffsebene für einen Ordner benötigen, ist es effizienter, eine **Gruppe** zu erstellen, welche die entsprechenden Benutzerkonten enthält, und dann der Gruppe die erforderlichen Berechtigungen zuzuweisen.
  + TIPP: Außerdem ist es ein weiterer Vorteil, dass Sie Dateiberechtigungen von Benutzern durch Hinzufügen des jeweiligen Benutzers zu Gruppe oder Entfernen des Benutzers aus der Gruppe ändern können und sie nicht direkt bearbeiten müssen.
  + In einem Windows Server-Unternehmensnetzwerk gibt es zwei Arten von Gruppen:
    - Sicherheit:
      * Sicherheitsgruppen sind Gruppen mit aktivierter Sicherheit und werden zum Zuweisen von Berechtigungen für verschiedene Ressourcen verwendet. Sie können Sicherheitsgruppen für Berechtigungseinträge in Zugriffssteuerungslisten (Access Control Lists, ACLs) verwenden, um die Sicherheit beim Zugriff auf Ressourcen besser steuern zu können. Wenn Sie eine Gruppe zum Verwalten der Sicherheit verwenden möchten, muss es sich um eine Sicherheitsgruppe handeln.
    - Verteiler:
      * Für E-Mail-Anwendungen werden normalerweise Verteilergruppen ohne aktivierte Sicherheit verwendet. Sie können aber auch Sicherheitsgruppen für die Verteilung von E-Mail-Anwendungen verwenden.
  + Der Gruppentyp bestimmt die Funktion der Gruppe.
  + Der Geltungsbereich einer Gruppe bestimmt sowohl den Umfang der Funktionen der Gruppe als auch die Berechtigungen und die Gruppenmitgliedschaft. Es gibt viel Gruppengeltungsbereiche:
    - **Lokal:**
      * Dieser Gruppentyp wird für eigenständige Server oder Arbeitsstationen, für Server, die Domänenmitglied, aber keine Domänencontroller sind, oder für Arbeitsstationen, die Domänenmitglied sind, verwendet. Lokale Gruppen sind nur auf den Computern verfügbar, auf denen sie vorhanden sind. Die wichtigsten Merkmale einer lokalen Gruppe:
        + Sie können Funktionen und Berechtigungen nur lokalen Ressourcen (d. h. auf dem lokalen Computer) zuweisen.
        + Mitglieder können von jeder Stelle der AD DS-Gesamtstruktur stammen.
    - **Lokal (in Domäne):**
      * Dieser Gruppentyp wird primär zum Verwalten des Zugriffs auf Ressourcen oder zum Zuweisen von Verwaltungsrechten und Zuständigkeiten verwendet. Lokale Domänengruppen befinden sich auf Domänencontrollern in einer AD DS-Domäne. Daher handelt es sich bei dem Geltungsbereich der Gruppe für die Domäne, in der sie sich befindet, um einen lokalen Bereich. Die wichtigsten Merkmale von lokalen Domänengruppen:
        + Sie können Funktionen und Berechtigungen nur lokalen Domänenressourcen (d. h. auf allen Computern in der lokalen Domäne) zuweisen.
        + Mitglieder können von jeder Stelle der AD DS-Gesamtstruktur stammen.
    - **Global:**
      * Dieser Gruppentyp wird hauptsächlich verwendet, um Benutzer mit ähnlichen Merkmalen zu konsolidieren. Beispielsweise können Sie globale Gruppen zum Einbinden von Benutzern verwenden, die zu einer Abteilung oder einem geografischen Standort gehören. Die wichtigsten Merkmale von globalen Gruppen:
        + Sie können überall in der Gesamtstruktur Funktionen und Berechtigungen zuweisen.
        + Mitglieder können nur aus der lokalen Domäne stammen und Benutzer, Computer und globale Gruppen aus der lokalen Domäne beinhalten.
    - **Universell:**
      * Dieser Gruppentyp wird am häufigsten in Netzwerken mit mehreren Domänen verwendet, da er die Merkmale von lokalen Domänengruppen und globalen Gruppen vereint. Zu den wichtigen Merkmalen universeller Gruppen zählen ganz besonders folgende:
        + Sie können überall in der Gesamtstruktur Funktionen und Berechtigungen zuweisen, ähnlich wie bei globalen Gruppen.
        + Mitglieder können von jeder Stelle der AD DS-Gesamtstruktur stammen.
  + **Computer** sind (wie Benutzer) Sicherheitsprinzipale, da sie folgende Merkmale aufweisen:
    - Sie verfügen über ein Konto mit einem Anmeldenamen und einem Kennwort, das von Windows regelmäßig und automatisch geändert wird.
    - Sie authentifizieren sich bei der Domäne.
    - Sie können zu Gruppen gehören, auf Ressourcen zugreifen und mithilfe von Gruppenrichtlinien konfiguriert werden.
  + Der Lebenszyklus eines Computerkontos beginnt, wenn Sie das Computerobjekt erstellen und in die Domäne einbinden. Nach dem Einbinden des Computerkontos in Ihre Domäne zählen folgende Aufgaben zu den alltäglichen Verwaltungsaufgaben:
    - Konfigurieren von Computereigenschaften
    - Verschieben des Computers zwischen Organisationseinheiten
    - Verwalten des Computers selbst
    - Umbenennen, Zurücksetzen, Deaktivieren, Aktivieren und schließlich Löschen des Computerobjekts
  + Ein Computerobjekt wird standartmäßig im „Computer“ Container (integrierter Container in einer AD DS-Domäne) gespeichert, wenn ein Computer der Domäne beitritt.
  + Dieser Container ist keine Organisationseinheit. Stattdessen handelt es sich um ein Objekt der Container-Klasse. Der allgemeine Name lautet „CN=Computers“.
  + Es gibt feine, aber wichtige Unterschiede zwischen einem Container und einer Organisationseinheit. Sie können in einem Container keine Organisationseinheit erstellen, d. h., Sie können den Container „Computer“ nicht unterteilen. Sie können mit einem Container auch kein Gruppenrichtlinienobjekt verknüpfen. Daher empfiehlt es sich, benutzerdefinierte Organisationseinheiten zum Hosten von Computerobjekten zu erstellen und nicht den Container „Computer“ zu verwenden.

* **Identifizieren und Beschreiben von AD DS-Gesamtstrukturen und –Domänen**
  + Eine AD DS-Gesamtstruktur ist eine Sammlung von einer oder mehreren AD DS-Strukturen, die eine oder mehrere AD DS-Domänen enthalten. Für alle Domänen in einer Gesamtstruktur gilt Folgendes:
    - Gemeinsamer Stamm
    - Gemeinsames Schema
    - Globaler Katalog
  + Eine AD DS-Domäne ist ein logischer Verwaltungscontainer für folgende Objekte:
    - Benutzer
    - Gruppen
    - Computer
  + Eine **Gesamtstruktur** ist ein Container der obersten Ebene in AD DS. Jede Gesamtstruktur ist eine Sammlung von einer oder mehreren Domänenstrukturen, die über ein gemeinsames Verzeichnisschema und einen globalen Katalog verfügen. Eine Domänenstruktur ist eine Sammlung von einer oder mehreren Domänen, die gemeinsam einen zusammenhängenden Namespace verwenden. Die Stammdomäne der Gesamtstruktur ist die erste Domäne, die in der Gesamtstruktur erstellt wird.
  + Die folgenden Objekte sind in der Gesamtstruktur-Stammdomäne vorhanden:
    - Schema-Masterrolle
    - Domänennamen-Masterrolle
    - Gruppe „Unternehmensadministratoren“
    - Gruppe „Schemaadministratoren“
  + Eine AD DS-Gesamtstruktur wird häufig wie folgt beschrieben:
    - Sicherheitsgrenze Standardmäßig können keine Benutzer von außerhalb der Gesamtstruktur auf Ressourcen innerhalb der Gesamtstruktur zugreifen. Außerdem vertrauen alle Domänen in einer Gesamtstruktur automatisch den anderen Domänen in der Gesamtstruktur. Dadurch ist es einfach, den Zugriff auf Ressourcen für alle Benutzer in einer Gesamtstruktur zu aktivieren, und zwar unabhängig von der Domäne, zu der sie gehören.
    - Replikationsgrenze Eine AD DS-Gesamtstruktur ist die Replikationsgrenze für die Konfigurations- und Schemapartitionen in der AD DS-Datenbank. Daher müssen Unternehmen, die Anwendungen mit inkompatiblen Schemas bereitstellen möchten, zusätzliche Gesamtstrukturen bereitstellen. Die Gesamtstruktur ist auch die Replikationsgrenze für den globalen Katalog. Der globale Katalog ermöglicht das Auffinden von Objekten in jeder Domäne der Gesamtstruktur.
  + Die folgenden Objekte sind in jeder Domäne vorhanden (einschließlich der Gesamtstruktur-Stammdomäne):
    - RID-Masterrolle
    - Infrastruktur-Masterrolle
    - PDC-Emulator-Masterrolle
    - Gruppe „Domänenadministratoren“
  + Eine AD DS-Domäne ist ein logischer Container für die Verwaltung von Benutzern, Computern, Gruppen und anderen Objekten.
  + Die häufigsten verwendeten Objekte:
    - Benutzerkonten
    - Computerkonten
    - Gruppen
  + Eine AD DS-Domäne wird häufig wie folgt beschrieben:
    - Replikationsgrenze Wenn Sie Änderungen an Objekten in der Domäne vornehmen, repliziert der Domänencontroller, auf dem die Änderung erfolgt ist, diese Änderung auf alle anderen Domänencontroller in der Domäne. Wenn mehrere Domänen in der Gesamtstruktur vorhanden sind, werden nur Teilmengen der Änderungen in andere Domänen repliziert. In AD DS wird ein Multimaster-Replikationsmodell verwendet, das allen Domänencontroller Änderungen an Objekten in der Domäne erlaubt.
    - Verwaltungseinheit Die AD DS-Domäne enthält ein Administratorkonto und die Gruppe „Domänenadministratoren“. Standardmäßig ist das Administratorkonto Mitglied der Gruppe „Domänenadministratoren“, die wiederum Mitglied aller lokalen Administratorgruppen von in die Domäne eingebundenen Computern ist. Außerdem haben die Mitglieder der Gruppe „Domänenadministratoren“ standardmäßig die vollständige Kontrolle über jedes Objekt in der Domäne.
  + Eine AD DS-Domäne ermöglicht Folgendes:
    - Authentifizierung, Wenn ein in eine Domäne eingebundener Computer gestartet wird oder sich ein Benutzer an einem in die Domäne eingebundenen Computer anmeldet, wird er von AD DS authentifiziert. Bei der Authentifizierung wird anhand der Anmeldeinformationen überprüft, ob der Computer oder Benutzer über die richtige Identität in AD DS verfügt.
    - Autorisierung Windows verwendet Technologien für die Autorisierung und Zugriffssteuerung, um zu ermitteln, ob authentifizierten Benutzern der Zugriff auf Ressourcen erlaubt ist.
  + AD DS-Vertrauensstellungen ermöglichen in einer komplexen AD DS-Umgebung den Zugriff auf Ressourcen.
* **Beschreiben von Organisationseinheiten (OEs)**
  + Eine Organisationseinheit ist ein Containerobjekt innerhalb einer Domäne, dass Sie zum Konsolidieren von Benutzern, Computern, Gruppen und anderen Objekten verwenden können.
  + Sie können Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) direkt mit einer Organisationseinheit verknüpfen, um die in der Organisationseinheit enthaltenen Benutzer und Computer zu verwalten.
  + Sie können auch einen Organisationseinheitenmanager zuweisen und einer Organisationseinheit eine COM+-Partition zuordnen.
  + Neue Organisationseinheiten in AD DS können Sie an folgenden Stellen erstellen:
    - Active Directory-Verwaltungscenter
    - Active Directory-Benutzer und -Computer
    - Windows Admin Center
    - Windows PowerShell mit dem Active Directory PowerShell-Modul
  + Es gibt zwei Gründe zum Erstellen einer Organisationseinheit:
    - Zum Konsolidieren von Objekten und zum Vereinfachen der Objektverwaltung, da Gruppenrichtlinienobjekte auf die Gesamtheit angewendet werden. Wenn Sie einer Organisationseinheit Gruppenrichtlinienobjekte zuweisen, gelten die Einstellungen für alle Objekte in der Organisationseinheit. Gruppenrichtlinienobjekte sind Richtlinien, die von Administratoren zum Verwalten und Konfigurieren der Einstellungen für Computer oder Benutzer erstellt werden. Sie stellen die Gruppenrichtlinienobjekte bereit, indem Sie sie mit Organisationseinheiten, Domänen oder Standorten verknüpfen.
    - Zum Delegieren der administrativen Objektkontrolle innerhalb der Organisationseinheit. Sie können Verwaltungsberechtigungen für eine Organisationseinheit zuweisen und somit die Kontrolle dieser Organisationseinheit an einen Benutzer oder eine Gruppe in AD DS (zusätzlich zur Gruppe „Domänenadministratoren“) delegieren.
  + Mithilfe von Organisationseinheiten können Sie die hierarchischen, logischen Strukturen in Ihrer Organisation darstellen.
  + AD DS verfügt über mehrere integrierte bzw. generische Container wie „Benutzer“ und „Computer“. In diesen Containern werden Systemobjekte oder Funktionen als übergeordnete Standardobjekte für neue Objekte, die Sie erstellen, gespeichert.
* **Verwalten von Objekten und deren Eigenschaften in AD DS**
  + Das Active Directory-Verwaltungscenter stellt eine grafische Benutzeroberfläche bereit, die auf Windows PowerShell basiert. Diese erweiterte Oberfläche ermöglicht mithilfe einer aufgabenorientierten Navigation das Ausführen der AD DS-Objektverwaltung und ersetzt die Funktionalität „Active Directory-Benutzer und -Computer“.
  + Zu den Aufgaben, die Sie mit dem Active Directory-Verwaltungscenter ausführen können, gehören:
    - Erstellen und Verwalten von Benutzer-, Computer-und Gruppenkonten
    - Erstellen und Verwalten von Organisationseinheiten
    - Herstellen einer Verbindung zu mehreren Domänen und Verwalten dieser Domänen in einer einzigen Instanz des Active Directory-Verwaltungscenters
    - Suchen und Filtern von AD DS-Daten durch das Erstellen von Abfragen
    - Erstellen und Verwalten differenzierter Kennwortrichtlinien
    - Wiederherstellen von Objekten aus dem Active Directory-Papierkorb
    - Verwalten von Objekten, die für die dynamische Zugriffssteuerungsfunktion erforderlich sind
  + **Windows Admin Center** ist eine webbasierte Konsole, mit der Sie Servercomputer und Computer, auf denen Windows 10 ausgeführt wird, verwalten können. In der Regel verwenden Sie Windows Admin Center anstelle der Remoteserver-Verwaltungstools (RSAT) zum Verwalten von Servern.
  + **RSAT (Remote Server Administration Tools)** ist eine Sammlung von Verwaltungstools, mit deren Hilfe Sie Windows Server-Rollen und -Features remote verwalten können.
  + **Active Directory-Modul für Windows PowerShell** unterstützt die AD DS-Verwaltung und zählt zu den wichtigsten Verwaltungskomponenten. Server-Manager und das Active Directory-Verwaltungscenter basieren auf Windows PowerShell und verwenden Cmdlets zum Ausführen der Aufgaben.
  + **„Active Directory-Benutzer und -Computer“** ist ein MMC-Snap-In (Microsoft Management Console), das die gängigsten Ressourcen (einschließlich Benutzer, Gruppen und Computer) verwaltet. Auch wenn viele Administratoren mit diesem Snap-In vertraut sind, wird es durch das Active Directory-Verwaltungscenter ersetzt, das mehr Funktionen bietet.
  + Mit dem MMC-Snap-In **„Active Directory-Standorte und -Dienste“** werden Replikation, Netzwerktopologie und zugehörige Dienste verwaltet.
  + Mit dem MMC-Snap-In **„Active Directory-Domänen und -Vertrauensstellungen“** werden Vertrauensstellungen auf den Funktionsebenen von Domänen und Gesamtstruktur konfiguriert und verwaltet.
  + Mit dem MMC-Snap-In **„Active Directory-Schema“** werden die Definitionen von AD DS-Attributen und -Objektklassen überprüft und geändert. Diese müssen nur selten überprüft oder geändert werden. Daher ist das Snap-In „Active Directory-Schema“ standardmäßig nicht registriert.

**Zusammenfassung:**

Die IT-Mitarbeiter bei Contoso sind damit beschäftigt, lokale Contoso-Server zu Windows Server 2022 zu migrieren. Im Rahmen der Migration hat Contoso die aktuelle AD DS-Umgebung ausgewertet. Als Windows Server-Administrator sind Sie für die Verwaltung von AD DS-Objekten (z. B. Benutzer, Gruppen und Organisationseinheiten) zuständig. Sie kennen jetzt die grundlegende AD DS-Struktur und wissen, in welcher Beziehung Benutzer, Gruppen und gruppenverwaltete Dienstkonten zu Organisationseinheiten stehen.