

---

# Unterrichtseinheit 1: Einführung in die Infrastruktur von Active Directory

## Inhalt

Übersicht	1
Lektion: Die Architektur von Active Directory	2
Lektion: Die Funktionsweise von Active Directory	11
Lektion: Untersuchen von Active Directory	21
Lektion: Die Entwurfs-, Planungs- und Implementierungsprozesse von Active Directory	32



Die in diesen Unterlagen enthaltenen Angaben und Daten, einschließlich URLs und anderer Verweise auf Internetwebsites, können ohne vorherige Ankündigung geändert werden. Die in den Beispielen genannten Firmen, Organisationen, Produkte, Domännennamen, E-Mail-Adressen, Logos, Personen, Orte und Ereignisse sind frei erfunden und jede Ähnlichkeit mit bestehenden Firmen, Organisationen, Produkten, Domännennamen, E-Mail-Adressen, Logos, Personen, Orten oder Ereignissen ist rein zufällig, soweit nichts anderes angegeben ist. Die Benutzer/innen sind verpflichtet, sich an alle anwendbaren Urheberrechtsgesetze zu halten. Unabhängig von der Anwendbarkeit der entsprechenden Urheberrechtsgesetze darf ohne ausdrückliche schriftliche Erlaubnis der Microsoft Corporation kein Teil dieses Dokuments für irgendwelche Zwecke vervielfältigt oder in einem Datenempfangssystem gespeichert oder darin eingelesen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen, usw.) dies geschieht.

Es ist möglich, dass Microsoft Rechte an Patenten bzw. angemeldeten Patenten, an Marken, Urheberrechten oder sonstigem geistigen Eigentum besitzt, die sich auf den fachlichen Inhalt dieses Dokuments beziehen. Die Bereitstellung dieses Dokuments gewährt keinerlei Lizenzrechte an diesen Patenten, Marken, Urheberrechten oder anderem geistigen Eigentum, es sei denn, dies wurde ausdrücklich durch einen schriftlichen Lizenzvertrag mit der Microsoft Corporation vereinbart.

© 2003 Microsoft Corporation. Alle Rechte vorbehalten.

Microsoft, MS-DOS, Windows, Windows NT, Active Directory, Active X, MSDN, PowerPoint, Visio, Visual Basic, Visual C++ und Windows Media sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Die in diesem Dokument aufgeführten Namen tatsächlicher Firmen und Produkte sind möglicherweise Marken der jeweiligen Eigentümer.

## Hinweise für Kursleiter

**Präsentation:**  
90 Minuten

**Übungseinheit:**  
0 Minuten

Diese Unterrichtseinheit führt die Kursteilnehmer in die Verzeichnisdienststruktur von Active Directory®, seine logische und physische Struktur und seine Funktion als Verzeichnisdienst ein. Außerdem werden in dieser Unterrichtseinheit die MMC-Snap-Ins, die Befehlszeilenprogramme sowie der Windows Script Host vorgestellt, mit denen die Komponenten von Active Directory sowie die Entwurfs-, Planungs- und Implementierungsprozesse von Active Directory untersucht werden können.

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

- Beschreiben der Architektur von Active Directory.
- Beschreiben der Funktionsweise von Active Directory.
- Untersuchen der Active Directory-Komponenten mit den MMC-Verwaltungs-Snap-Ins.
- Beschreiben der Entwurfs-, Planungs- und Implementierungsprozesse von Active Directory.

**Erforderliche  
Unterlagen**

Zur Unterrichtung dieser Unterrichtseinheit benötigen Sie folgende Unterlagen:

- Microsoft® PowerPoint®-Datei 2195A\_01.ppt
- Macromedia Flash-Datei 2195A\_2279a\_01\_a\_logical.swf
- Macromedia Flash-Datei 2195A\_2279a\_01\_a\_physical.swf
- Macromedia Flash-Datei 2195A\_2279a\_1\_a\_SSO.swf

---

**Wichtig** Es wird empfohlen, zum Anzeigen der Folien für diesen Kurs PowerPoint 2002 oder höher zu verwenden. Wenn Sie PowerPoint Viewer oder eine frühere Version von PowerPoint verwenden, werden möglicherweise nicht alle Features der Folien ordnungsgemäß angezeigt.

---

**Vorbereitende  
Aufgaben**

Zur Vorbereitung dieser Unterrichtseinheit gehen Sie folgendermaßen 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.
- Sehen Sie sich die Multimediapräsentationen an.
- 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.

## Vermitteln dieser Unterrichtseinheit

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

---

**Wichtig** Zu jeder Lektion dieser Unterrichtseinheit gehören Bewertungspunkte, die sich auf der Kursteilnehmer-CD befinden. Sie können diese Punkte 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 den Kursleiter 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 zur Durchführung 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: Die Architektur von Active Directory

In diesem Abschnitt werden die didaktischen Methoden zum Unterrichten dieser Lektion beschrieben. Diese Lektion beschreibt die Funktion von Active Directory, seine logische und physische Struktur sowie die Betriebsmasterfunktionen.

Beschreiben Sie bei der Vorstellung des Themas Was macht Active Directory? die Funktion von Active Directory in Microsoft Windows Server™ 2003. Erklären Sie die Funktion von Active Directory als Netzwerkverzeichnisdienst und wie es Administratoren bei der Verwaltung der Netzwerkressourcen hilft.

Stellen Sie die logische Struktur von Active Directory mithilfe der Animation *Die logische Struktur von Active Directory* vor. Führen Sie die Animation dem gesamten Kurs vor, oder bitten Sie die Kursteilnehmer, die Animation alleine anzusehen, sofern sie über Kopfhörer verfügen. Die Übung am Ende der Animation kann gemeinsam oder von jedem Kursteilnehmer alleine durchgeführt werden. Nehmen Sie die Übung als Anlass für eine Diskussion über den Inhalt der Animation. Nach der Einführung können Sie mit den Navigationsschaltflächen zu jedem Thema der Animation gehen.

Stellen Sie die physische Struktur von Active Directory mithilfe der Animation *Die physische Struktur von Active Directory* vor. Erklären Sie anhand dieser Animation, wie sich Active Directory durch das Zusammenwirken der logischen und physischen Struktur an die Anforderungen eines Unternehmens anpassen lässt. Fassen Sie die Kernpunkte der Animation nach der Multimediapräsentation zusammen. Vergewissern Sie sich, dass die Kursteilnehmer folgende Konzepte verstehen:

- Standorte sind physisch eigenständige Objekte. Heben Sie hervor, wie Standorte die Replikation und den Anmeldeverkehr optimieren.
- Domänencontroller sind physisch eigenständige, von Domänen getrennte Objekte.

Achten Sie darauf, dass Sie bei der Vorstellung des Themas Was sind Betriebsmaster? nur die Funktion jeder Rolle beschreiben. Gehen Sie bei der Beschreibung der Schemamasterfunktion nicht zu detailliert auf das Schema selbst ein. Das Schema wird in einer späteren Unterrichtseinheit behandelt. Verweisen Sie die Kursteilnehmer auf die Unterrichtseinheit 9, „Verwalten der Betriebsmaster“, in Kurs 2195A: *Planen, Implementieren und Warten einer Active Directory-Infrastruktur unter Microsoft Windows Server 2003*. Dort wird die Verwaltung von Domänencontrollern, die diese Funktionen verwalten, ausführlich beschrieben.

**Praktische Übung**

Diese Lektion beinhaltet keine praktische Übung.

## Lektion: Die Funktionsweise von Active Directory

Diese Lektion beschreibt die Funktion von Active Directory als Verzeichnisdienst. Die Kursteilnehmer erfahren in dieser Lektion, wie ihnen Active Directory bei der Verwaltung der Ressourcen und bei der Lösung von Problemen hilft, die beim Zugriff auf die Ressourcen auftreten können.

Erklären Sie die Funktion von Active Directory als Verzeichnisdienst. Die Funktion eines Verzeichnisdienstes können Sie mit einem Telefonbuch vergleichen. In einem Telefonbuch finden Sie die Telefonnummer einer bestimmten Person, indem Sie den betreffenden Nachnamen nachschlagen. Genauso kann Active Directory zum Suchen von Ressourcen verwendet werden. Es findet Ressourcen auf der Grundlage von Attributen, die die betreffende Ressource beschreiben.

Stellen Sie bei der Erklärung des globalen Katalogs sicher, dass die Kursteilnehmer verstehen, dass der globale Katalog zur Gesamtstruktur gehört und dass er nur einen Teil der Attribute der in Active Directory gespeicherten Objekte enthält. Die zu jedem Objekt gespeicherten Attribute bieten Active Directory genügend Anhaltspunkte, um die durch das Objekt dargestellte Ressource zu finden.

Stellen Sie bei der Erläuterung des Active Directory-Schemas sicher, dass Kursteilnehmer, die bereits unter Microsoft Windows 2000 mit Active Directory gearbeitet haben, verstehen, wie wichtig es ist, Schemaänderungen zu deaktivieren. Dies ist eine neue Funktionsweise in Windows Server 2003.

Heben Sie bei der Vorstellung des Themas Was sind Distinguished Names und Relative Distinguished Names? die Verwendung von LDAP (Lightweight Directory Access Protocol) für die Kommunikation mit Active Directory hervor. Überprüfen Sie auch, ob die Kursteilnehmer eine LDAP-Abfragezeichenfolge erstellen können.

Zeigen Sie den Kursteilnehmern anhand der Animation *Handhabung einmaliger Anmeldungen durch Active Directory* das Zusammenwirken von Attributwerten, dem globalen Katalog und LDAP bei der Bereitstellung des Ressourcenzugriffs und anderer Active Directory-Funktionen.

**Praktische Übung**

Diese Lektion beinhaltet keine praktische Übung.

## Lektion: Untersuchen von Active Directory

Diese Lektion stellt die MMC-Snap-Ins und Befehlszeilenprogramme für die Verwaltung von Active Directory und die Untersuchung der in Lektion Die Architektur von Active Directory beschriebenen Active Directory-Objekte vor.

Die Kursteilnehmer sollten bereits über Vorkenntnisse der zentralen und dezentralen Verwaltungsmodelle von Active Directory verfügen. Gehen Sie unter dem Thema Verwalten von Active Directory kurz auf diese Modelle ein.

Beschreiben Sie unter dem Thema Snap-Ins und Programme für die Verwaltung von Active Directory die wichtigsten MMC-Snap-Ins für die Verwaltung von Active Directory. Gehen Sie nur kurz auf die Features der einzelnen Programme ein.

Die Kursteilnehmer sollten bereits mit den Verwaltungs-Snap-Ins der grafischen Benutzeroberfläche vertraut sein. Wiederholen Sie deren Funktion nur kurz unter dem Thema Wie wird Active Directory untersucht?. Verweisen Sie die Kursteilnehmer auf die Anhänge. Dort erhalten sie Informationen über die Verwendung von ADSI-Bearbeitung.

### Praktische Übung

Am Ende der Lektion werden die Kursteilnehmer gebeten, die Active Directory-Struktur der Schulungsraum-Gesamtstruktur mithilfe von Active Directory-Benutzer und -Computer, Active Directory-Domänen und -Vertrauensstellungen und Active Directory-Standorte und -Dienste zu untersuchen.

## Lektion: Die Entwurfs-, Planungs- und Implementierungsprozesse von Active Directory

Diese Lektion gibt eine Übersicht über die Entwurfs-, Planungs- und Implementierungsprozesse von Active Directory. Stellen Sie sicher, dass die Kursteilnehmer den Unterschied zwischen Entwurf, Planung und Implementierung verstehen.

### Praktische Übung

Diese Lektion beinhaltet keine praktische Übung.



# Übersicht

- Die Architektur von Active Directory
- Die Funktionsweise von Active Directory
- Untersuchen von Active Directory
- Die Entwurfs-, Planungs- und Implementierungsprozesse von Active Directory

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

## Einführung

Diese Unterrichtseinheit stellt die logische und physische Struktur von Active Directory® und seine Funktion als Verzeichnisdienst vor. Außerdem werden in dieser Unterrichtseinheit die Snap-Ins, die Befehlszeilenprogramme sowie der Windows Script Host vorgestellt, mit denen die Komponenten von Active Directory sowie die Entwurfs-, Planungs- und Implementierungsprozesse von Active Directory verwaltet werden können.

## Lernziele

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

- Beschreiben der Architektur von Active Directory.
- Beschreiben der Funktionsweise von Active Directory.
- Untersuchen der Active Directory-Komponenten mit den Verwaltungs-Snap-Ins.
- Beschreiben der Entwurfs-, Planungs- und Implementierungsprozesse von Active Directory.

# Lektion: Die Architektur von Active Directory

- Was macht Active Directory?
- Multimediapräsentation: Die logische Struktur von Active Directory
- Multimediapräsentation: Die physische Struktur von Active Directory
- Was sind Betriebsmaster?

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

## Einführung

Active Directory besteht aus Komponenten, die eine logische und physische Struktur bilden. Bei der Planung müssen Sie sowohl die logischen als auch die physischen Strukturen von Active Directory an die Anforderungen Ihres Unternehmens anpassen. Zur Verwaltung von Active Directory müssen Sie die Aufgaben der einzelnen Komponenten verstehen und wissen, wie sie angewendet werden.

## Lernziele der Lektion

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

- Beschreiben der Funktion von Active Directory.
- Beschreiben der logischen Struktur von Active Directory.
- Beschreiben der physischen Struktur von Active Directory.
- Beschreiben der Betriebsmasterfunktionen.

## Was macht Active Directory?

- **Zentrale Steuerung der Netzwerkressourcen**
- **Zentralisieren und Dezentralisieren der Ressourcenverwaltung**
- **Sicheres Speichern von Objekten in einer logischen Struktur**
- **Optimieren des Netzwerkdatenverkehrs**

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

### Einführung

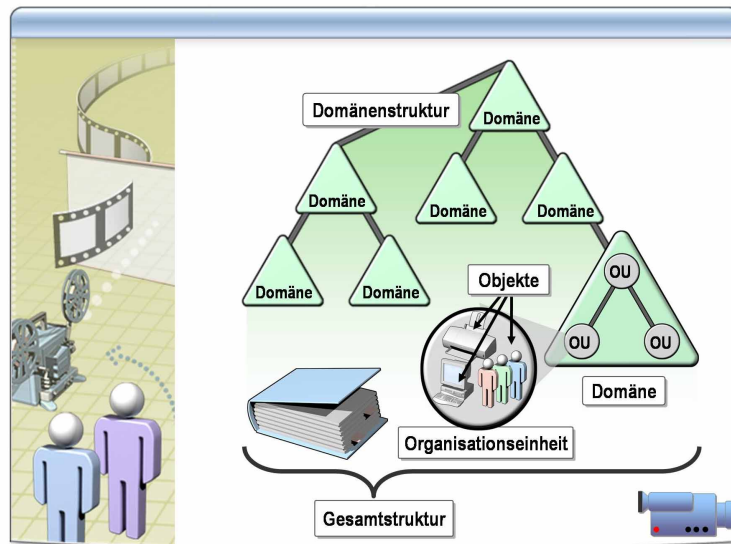
Active Directory speichert Informationen über Benutzer, Computer und Netzwerkressourcen und stellt diese Ressourcen Benutzern und Anwendungen bereit. Es bietet eine konsistente Methode zum Benennen, Beschreiben, Auffinden, Zugreifen, Verwalten und Sichern von Informationen über diese Ressourcen.

### Die Funktion von Active Directory

Active Directory erfüllt folgende Funktionen:

- *Zentrale Steuerung der Netzwerkressourcen.* Durch die zentrale Steuerung der Ressourcen, beispielsweise von Servern, freigegebenen Dateien und Druckern, erhalten in Active Directory nur autorisierte Benutzer Zugriff auf diese Ressourcen.
- *Zentralisieren und Dezentralisieren der Ressourcenverwaltung.* Administratoren können verteilte Clientcomputer, Netzwerkdienste und Anwendungen auf einer einheitlichen Verwaltungsoberfläche von einem zentralen Standort aus verwalten, oder sie können Verwaltungsaufgaben verteilen, indem sie die Kontrolle über die Ressourcen an andere Administratoren abgeben.
- *Sicheres Speichern von Objekten in einer logischen Struktur.* Active Directory speichert alle Ressourcen als Objekte in einer sicheren, hierarchischen logischen Struktur.
- *Optimieren des Netzwerkdatenverkehrs.* Die physische Struktur von Active Directory ermöglicht eine effizientere Nutzung der Netzwerkbandbreite. Wenn sich beispielsweise ein Benutzer beim Netzwerk anmeldet, wird er von der nächstliegenden Authentifizierungsstelle überprüft. Dadurch reduziert sich der Netzwerkdatenverkehr.

## Multimediapräsentation: Die logische Struktur von Active Directory



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

### Speicherort der Datei

Öffnen Sie zum Anzeigen der Präsentation *Die logische Struktur von Active Directory* die Webseite auf der Kursteilnehmer-CD, klicken Sie auf **Multimedia** und anschließend auf den Titel der Präsentation. Starten Sie die Präsentation nur, wenn der Kursleiter Sie dazu auffordert.

### Lernziele

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

- Definieren der Elemente der logischen Struktur von Active Directory.
- Erläutern der Funktionen dieser Elemente.

### Kernpunkte

In der hierarchischen logischen Struktur von Active Directory werden Informationen über Objekte sicher gespeichert. Active Directory-Objekte repräsentieren Benutzer und Ressourcen (z. B. Computer und Drucker). Einige Objekte sind Container für andere Objekte. Wenn Sie die Funktion dieser Objekte verstehen, können Sie eine Vielzahl von Aufgaben wie das Installieren, Konfigurieren, Verwalten und die Fehlerbehebung von Active Directory ausführen.

Die logische Struktur von Active Directory besteht aus folgenden Komponenten:

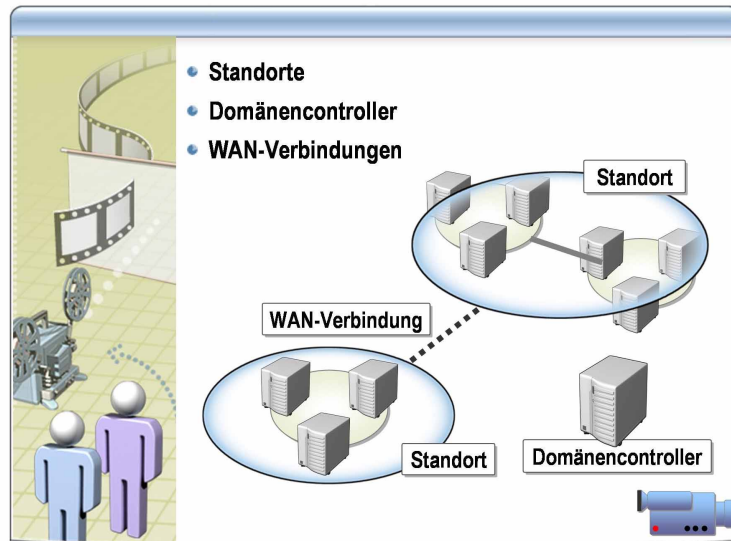
- *Objekte*. Dies sind die Grundkomponenten der logischen Struktur. *Objektklassen* sind Vorlagen oder Blaupausen für die in Active Directory erstellbaren Objekttypen. Jede Objektklasse wird durch eine Gruppe von *Attributen* definiert, die die möglichen Werte eines Objekts festlegen. Jedem Objekt ist eine eindeutige Kombination von Attributwerten zugewiesen.
- *Organisationseinheiten*. Diese Containerobjekte verwenden Sie dazu, andere Objekte entsprechend Ihren Verwaltungsanforderungen zusammenzustellen. Durch Zusammenfassen von Objekten in Organisationseinheiten erleichtern Sie sich das Auffinden und Verwalten der Objekte. Sie können die Berechtigung, eine Organisationseinheit zu verwalten, auch delegieren. Organisationseinheiten können in anderen Organisationseinheiten *verschachtelt* sein, wodurch sich die Objektverwaltung noch mehr vereinfacht.
- *Domänen*. Die wichtigsten funktionalen Einheiten der logischen Struktur von Active Directory sind Domänen. Domänen sind eine Sammlung administrativ definierter Objekte, die sich eine gemeinsame Verzeichnisdatenbank, Sicherheitsrichtlinien und Vertrauensstellungen mit anderen Domänen teilen. Domänen haben folgende drei Funktionen:
  - Sie dienen als administrative Grenze für Objekte.
  - Sie sind ein Mittel, die Sicherheit freigegebener Ressourcen zu verwalten.
  - Sie stellen eine Replikationseinheit für Objekte dar.
- *Domänenstrukturen*. In einer hierarchischen Struktur zusammengefasste Domänen werden als Domänenstruktur bezeichnet. Wenn Sie einer Domänenstruktur eine zweite Domäne hinzufügen, wird diese Domäne zur *untergeordneten Domäne* der Stammdomäne der Struktur. Die Domäne, an der eine untergeordnete Domäne ansetzt, wird als *übergeordnete Domäne* bezeichnet. Einer untergeordneten Domäne können weitere Domänen untergeordnet sein.

Der Name einer untergeordneten Domäne kombiniert mit dem Namen der übergeordneten Domäne ergibt den eindeutigen DNS-Namen (Domain Name System) der Domäne. Zum Beispiel: corp.nwtraders.msft. Eine Domänenstruktur hat also einen *zusammenhängenden Namespace*.

- *Gesamtstrukturen*. Eine Gesamtstruktur ist eine vollständige Instanz von Active Directory. Sie besteht aus mindestens einer Domänenstruktur. In einer aus zwei Ebenen bestehenden Domänenstruktur, die sich für die meisten Unternehmen empfiehlt, sind alle untergeordneten Domänen der Stammdomäne der Gesamtstruktur untergeordnet und bilden so eine zusammenhängende Struktur.

Die erste Domäne einer Gesamtstruktur wird als *Stammdomäne der Gesamtstruktur* bezeichnet. Der Name dieser Domäne verweist auf die Gesamtstruktur (z. B. nwtraders.msft). Die Informationen in Active Directory sind standardmäßig nur innerhalb der Gesamtstruktur freigegeben. Auf diese Weise stellt die Gesamtstruktur eine Sicherheitsgrenze für die in der jeweiligen Instanz von Active Directory enthaltenen Informationen dar.

## Multimediapräsentation: Die physische Struktur von Active Directory



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

**Speicherort der Datei** Öffnen Sie zum Anzeigen der Präsentation *Die physische Struktur von Active Directory* die Webseite auf der Kursteilnehmer-CD, klicken Sie auf **Multimedia** und anschließend auf den Titel der Präsentation. Starten Sie die Präsentation nur, wenn der Kursleiter Sie dazu auffordert.

**Lernziele** Am Ende dieser Präsentation werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Definieren der Elemente der physischen Struktur von Active Directory.
- Erläutern der Funktionen dieser Elemente.

**Kernpunkte** Im Gegensatz zur logischen Struktur, die die administrativen Anforderungen widerspiegelt, dient die physische Struktur von Active Directory dazu, den Netzwerkdatenverkehr zu optimieren. Zu diesem Zweck bestimmt sie, wann und wo Replikation und Anmeldeverkehr stattfinden. Zur Optimierung der Netzwerk-Bandbreitenauslastung von Active Directory müssen Sie die physische Struktur verstehen. Die physische Struktur von Active Directory enthält folgende Elemente:

- *Domänencontroller*. Auf diesen Computern werden Microsoft® Windows Server™ 2003 oder Windows 2000 Server und Active Directory ausgeführt. Jeder Domänencontroller übt Speicher- und Replikationsfunktionen aus. Ein Domänencontroller kann nur eine Domäne unterstützen. Zur Sicherstellung der kontinuierlichen Verfügbarkeit von Active Directory sollte jede Domäne über mehrere Domänencontroller verfügen.

- *Active Directory-Standorte*. Diese Standorte sind Gruppen von optimal miteinander verbundenen Computern. Wenn Sie Standorte einrichten, kommunizieren die Domänencontroller desselben Standortes häufig miteinander. Dadurch verringert sich die *Latenz* an diesem Standort, d. h. die Zeit, die zur Replikation einer Änderung auf einem Domänencontroller zu einem anderen Domänencontroller benötigt wird. Standorte werden erstellt, um die Bandbreitenauslastung zwischen Domänencontrollern zu optimieren, die sich an verschiedenen Standorten befinden.

---

**Anmerkung** Weitere Informationen über Active Directory-Standorte finden Sie in Unterrichtseinheit 7, „Implementieren von Standorten zum Verwalten der Active Directory-Replikation“, in Kurs 2195A: *Planen, Implementieren und Warten einer Active Directory-Infrastruktur unter Microsoft Windows Server 2003*.

---

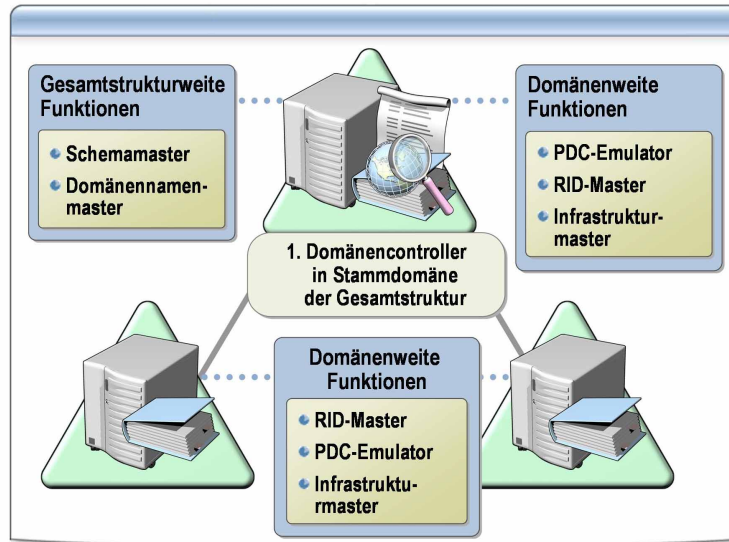
- *Active Directory-Partitionen*. Jeder Domänencontroller enthält die folgenden Active Directory-Partitionen:
  - Eine *Domänenpartition* mit Replikaten aller Objekte dieser Domäne. Die Domänenpartition wird nur auf andere Domänencontroller der gleichen Domäne repliziert.
  - Eine *Konfigurationspartition* mit der Topologie der Gesamtstruktur. Die *Topologie* ist ein Datensatz aller Domänencontroller einer Gesamtstruktur und der Verbindungen zwischen diesen Controllern.
  - Eine *Schemapartition* mit dem Schema der Gesamtstruktur. Jede Gesamtstruktur verfügt nur über ein Schema. So wird sichergestellt, dass die Definitionen der einzelnen Objektklassen konsistent sind. Die Konfigurations- und Schemapartitionen werden auf jeden Domänencontroller der Gesamtstruktur repliziert.
  - Optionale *Anwendungspartitionen* mit Objekten, die nicht für die Sicherheit relevant sind und die von einer oder mehreren Anwendungen verwendet werden. Anwendungspartitionen werden nur auf bestimmte Domänencontroller der Gesamtstruktur repliziert.

---

**Anmerkung** Weitere Informationen über Active Directory-Partitionen finden Sie in Unterrichtseinheit 7, „Implementieren von Standorten zum Verwalten der Active Directory-Replikation“, in Kurs 2195A: *Planen, Implementieren und Warten einer Active Directory-Infrastruktur unter Microsoft Windows Server 2003*.

---

## Was sind Betriebsmaster?



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

### Einführung

Wenn auf einer Domäne eine Änderung vorgenommen wird, wird diese Änderung auf alle Domänencontroller in der Domäne repliziert. Einige Änderungen, zum Beispiel Schemaänderungen, werden auf alle Domänen der Gesamtstruktur repliziert. Diese Replikation wird als *Multimasterreplikation* bezeichnet.

### Singlemasterreplikation

Bei Multimasterreplikationen kann es zu einem Replikationskonflikt kommen, wenn die ursprünglichen Aktualisierungen gleichzeitig auf zwei Domänencontrollern am selben Objektattribut ausgeführt werden. Zur Vermeidung von Replikationskonflikten verwenden Sie die *Singlemasterreplikation*. Bei dieser Art der Replikation können bestimmte Verzeichnisänderungen nur an einem einzigen, designierten Domänencontroller durchgeführt werden. Auf diese Weise können Änderungen nicht gleichzeitig an mehreren Stellen des Netzwerks auftreten. Active Directory verwendet die Singlemasterreplikation für wichtige Änderungen wie das Hinzufügen einer neuen Domäne oder eine Änderung am Schema der Gesamtstruktur.

### Betriebsmasterfunktionen

Vorgänge, die Singlemasterreplikation verwenden, sind in einer Gesamtstruktur oder einer Domäne in speziellen Funktionen zusammengefasst. Diese Funktionen werden als *Betriebsmasterfunktionen* bezeichnet. Nur der einer Betriebsmasterfunktion zugewiesene Domänencontroller kann die zugehörigen Verzeichnisänderungen durchführen. Der für eine bestimmte Funktion zuständige Domänencontroller wird als *Betriebsmaster* dieser Funktion bezeichnet. Active Directory speichert Informationen über die Zuständigkeit von Domänencontrollern für bestimmte Funktionen.

In Active Directory sind fünf Betriebsmasterfunktionen definiert. Jede dieser Funktionen hat einen Standardstandort. Die Betriebsmasterfunktionen beziehen sich entweder auf die Gesamtstruktur oder auf die Domäne.

- *Gesamtstrukturweite Funktionen.* Diese Betriebsmasterfunktionen sind innerhalb einer Gesamtstruktur eindeutig. Hierzu gehören:
  - *Schemamaster.* Steuert alle Schemaaktualisierungen. Das Schema enthält eine Masterliste der Objektklassen und Attribute, die zur Erstellung aller Active Directory-Objekte (Benutzer, Computer, Drucker usw.) verwendet werden.
  - *Domänennamenmaster.* Steuert das Hinzufügen oder Entfernen von Domänen in der Gesamtstruktur. Wenn Sie der Gesamtstruktur eine neue Domäne hinzufügen, kann nur der Domänencontroller, der für die Domänennamenmasterfunktion zuständig ist, die neue Domäne hinzufügen.

Eine Gesamtstruktur kann nur einen Schemamaster und nur einen Domänennamenmaster haben.

- *Domänenweite Funktionen.* Zu diesen innerhalb jeder Domäne einer Gesamtstruktur eindeutigen Funktionen gehören:
  - *Emulator für primären Domänencontroller* (PDC, Primary Domain Controller). Fungiert als Windows NT-PDC und unterstützt alle Reservedomänencontroller (Backup Domain Controllers, BDCs), auf denen Microsoft Windows NT® in einer *Domäne im gemischten Modus* ausgeführt wird. Auf den Domänencontrollern dieses Domänentyps wird Windows NT 4.0 ausgeführt. Der PDC-Emulator ist der erste Domänencontroller, den Sie in einer neuen Domäne erstellen.
  - *RID-Master.* Wenn ein neues Objekt erstellt wird, erstellt der Domänencontroller ein neues Sicherheitsprinzipal, das das Objekt repräsentiert und ihm eine eindeutige Sicherheitskennung (Security Identifier, SID) zuweist. Diese SID besteht aus einer Domänen-SID, die für alle Sicherheitsprinzipale der Domäne gleich ist, und einer relativen Kennung (Relative Identifier, RID), die für jedes Sicherheitsprinzipal der Domäne eindeutig ist. Der RID-Master weist jedem Domänencontroller der Domäne bestimmte RID-Blöcke zu. Aus dem ihm zugewiesenen RID-Block weist der Domänencontroller neu erstellten Objekten RIDs zu.

- *Infrastrukturmaster*. Wenn ein Objekt von einer Domäne in eine andere Domäne verschoben wird, aktualisiert der Infrastrukturmaster die Objektreferenz in seiner Domäne, so dass sie auf das Objekt in der anderen Domäne verweist. Die Objektreferenz enthält die GUID (Globally Unique Identifier), den DN (Distinguished Name) und eine SID (Security Identifier). Active Directory aktualisiert den DN und die SID einer Objektreferenz in regelmäßigen Abständen, um Änderungen am eigentlichen Objekt, wie Verschiebungen innerhalb und zwischen Domänen oder das Löschen des Objekts, widerzuspiegeln.

Jede Domäne in einer Gesamtstruktur hat einen eigenen PDC-Emulator, RID-Master und Infrastrukturmaster.

---

**Anmerkung** Weitere Informationen über Betriebsmasterfunktionen finden Sie in Unterrichtseinheit 9, „Verwalten der Betriebsmaster“, in Kurs 2195A: *Planen, Implementieren und Warten einer Active Directory-Infrastruktur unter Microsoft Windows Server 2003*.

---

## Lektion: Die Funktionsweise von Active Directory

- Was ist ein Verzeichnisdienst?
- Was ist ein Schema?
- Was ist der globale Katalog?
- Was sind Distinguished Names und Relative Distinguished Names?
- Multimediapräsentation: Handhabung einmaliger Anmeldungen durch Active Directory

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

### Einführung

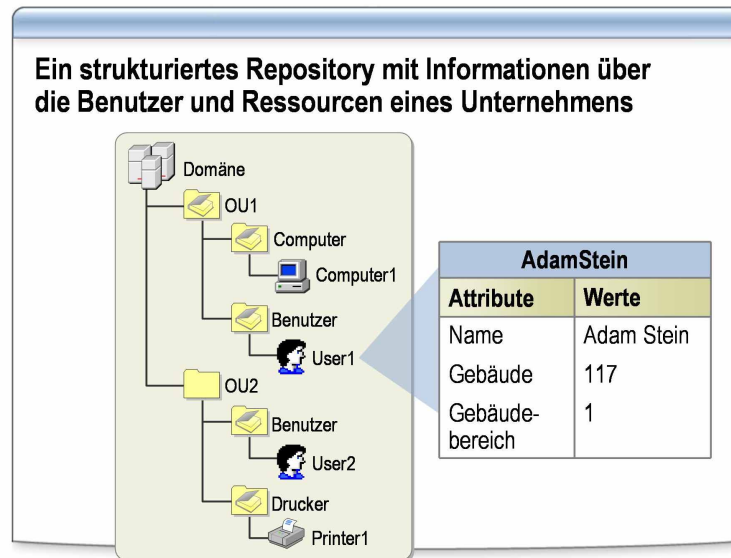
In dieser Lektion wird die Funktion von Active Directory als Verzeichnisdienst beschrieben. Wenn Sie die Funktionsweise von Active Directory verstehen, können Sie Ihre Ressourcen besser verwalten und Probleme im Zusammenhang mit dem Ressourcenzugriff schneller beheben.

### Lernziele der Lektion

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

- Beschreiben der Funktion von Active Directory als Verzeichnisdienst.
- Beschreiben der Funktion und der Verwendung des Active Directory-Schemas.
- Beschreiben der Funktion des globalen Katalogs.
- Unterscheiden zwischen dem DN (Distinguished Name) und RDN (*Relative Distinguished Name*) eines Active Directory-Objekts.
- Beschreiben, wie Active Directory einmalige Anmeldungen handhabt.

## Was ist ein Verzeichnisdienst?



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

### Einführung

In großen Netzwerken teilen sich zahlreiche Benutzer und Anwendungen die gleichen Ressourcen. Damit Benutzer und Anwendungen auf diese Ressourcen und zugehörige Informationen zugreifen können, benötigen Sie eine konsistente Methode, die Informationen über diese Ressourcen zu benennen, zu beschreiben, zu suchen, darauf zuzugreifen, sie zu verwalten und sie zu sichern. Dies ist die Funktion eines Verzeichnisdienstes.

### Was ist ein Verzeichnisdienst?

Ein Verzeichnisdienst ist ein strukturiertes Repository mit Informationen über die Benutzer und Ressourcen eines Unternehmens. In einem Windows Server 2003-Netzwerk ist Active Directory der Verzeichnisdienst.

### Funktionen von Active Directory

Active Directory hat folgende Funktionen:

- *Benutzern und Anwendungen wird der Zugriff auf Informationen über Objekte ermöglicht.* Objektinformationen werden in Form von Attributwerten gespeichert. Objekte können anhand ihrer Objektklasse, ihrer Attribute und Attributwerte, ihres Speicherorts innerhalb der Active Directory-Struktur oder einer Kombination aus diesen Werten gesucht werden.
- *Die physische Netzwerktopologie und Protokolle werden transparent.* Auf diese Weise kann ein Benutzer innerhalb eines Netzwerks auf jede Ressource, zum Beispiel einen Drucker, zugreifen, ohne den Standort der Ressource zu kennen oder zu wissen, wie die Ressource physisch an das Netzwerk angeschlossen ist.

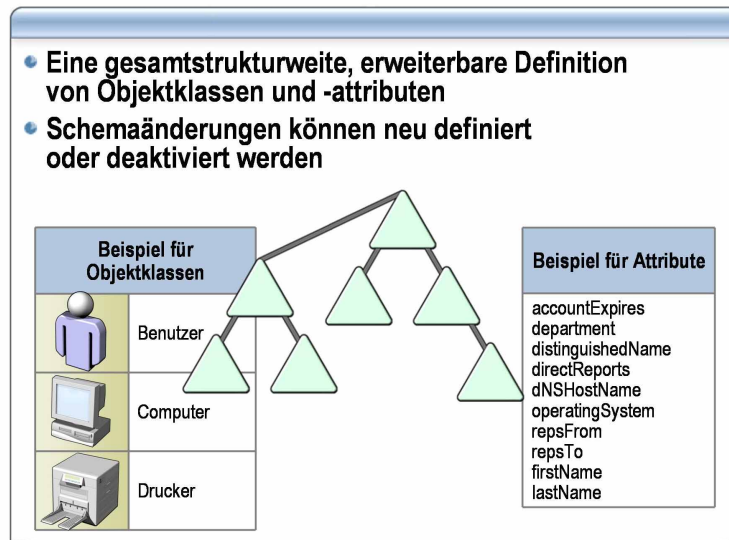
- 
- *Eine sehr große Anzahl von Objekten kann gespeichert werden.* Aufgrund seiner Einteilung in Partitionen kann Active Directory dem wachsenden Unternehmen angepasst werden. Ein Verzeichnis mit einigen hundert Objekten, das auf einem einzigen Server Platz findet, kann beispielsweise zu einem Verzeichnis mit Millionen von Objekten auf Tausenden von Servern anwachsen.
  - *Active Directory kann als vom Betriebssystem unabhängiger Dienst ausgeführt werden.* Active Directory im Anwendungsmodus (AD/AM) ist eine neue Funktion von Active Directory, die bestimmte Bereitstellungsszenarien mit verzeichnisfähigen Anwendungen anspricht. AD/AM wird als betriebssystemunabhängiger Dienst ausgeführt und erfordert als solcher keine Bereitstellung auf einem Domänencontroller. Unabhängig vom Betriebssystem ist AD/AM insofern, als dass auf einem einzigen Server mehrere Instanzen von AD/AM gleichzeitig ausgeführt werden können und jede dieser Instanzen unabhängig voneinander konfiguriert werden kann.

---

**Anmerkung** Weitere Informationen über AD/AM finden Sie unter dem Thema „Introduction to Active Directory in Application Mode“ unter folgender Adresse:  
<http://www.microsoft.com/windowsserver2003/techinfo/overview/adam.msp>  
(nur auf Englisch verfügbar).

---

## Was ist ein Schema?



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

### Einführung

Das Active Directory-Schema legt fest, welche Objekttypen, welche Arten von Informationen über diese Objekte und welche Standardsicherheitskonfiguration für diese Objekte in Active Directory gespeichert werden können.

### Was ist das Active Directory-Schema?

Das Active Directory-Schema enthält die Definitionen aller Objekte (Benutzer, Computer, Drucker usw.), die in Active Directory gespeichert sind. Domänencontroller unter Windows Server 2003 erlauben nur ein Schema für die Gesamtstruktur. Auf diese Weise wird sichergestellt, dass alle in Active Directory erstellten Objekte den gleichen Regeln entsprechen.

Das Schema unterstützt zwei Definitionstypen: Objektklassen und Attribute. *Objektklassen* wie Benutzer, Computer und Drucker legen fest, welche Verzeichnisobjekte erstellt werden können. Jede Objektklasse enthält eine Sammlung von Attributen.

Attribute werden unabhängig von Objektklassen definiert. Ein Attribut wird nur einmal definiert und kann in mehreren Objektklassen verwendet werden. Das Attribut **Beschreibung** kann beispielsweise in mehreren Objektklassen verwendet werden, wird aber nur einmal im Schema definiert, um die Konsistenz sicherzustellen.

### Erweiterbarkeit des Active Directory-Schemas

Durch Schemaerweiterungen können Sie in Active Directory neue Objekttypen erstellen. Für eine E-Mail-Serveranwendung können Sie zum Beispiel der Benutzerklasse in Active Directory neue Attribute hinzufügen, die neue Informationen wie die E-Mail-Adressen der Benutzer speichern.

---

**Anmerkung** Weitere Informationen zur Erweiterung des Active Directory-Schemas finden Sie in der MSDN Library-Onlinereferenz unter dem Thema „Extending the Schema“ (auf Englisch).

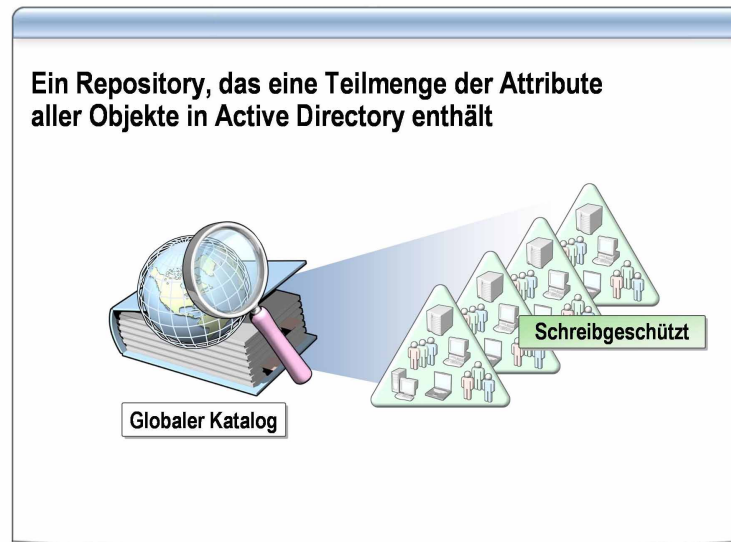
---

**Schemaänderungen  
und Deaktivieren von  
Schemaänderungen**

Auf Windows Server 2003-Domänencontrollern können Schemaänderungen durch Deaktivieren der Änderungen rückgängig gemacht werden. Auf diese Weise lässt sich die Erweiterungsfähigkeit von Active Directory in einem Unternehmen besser nutzen.

Schemaklassen oder Attribute können auch neu definiert werden. Sie können beispielsweise die Unicode-Zeichenfolgensyntax eines Attributs namens „SalesManager“ zu „Distinguished Name“ ändern.

## Was ist der globale Katalog?



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

### Einführung

In Active Directory können Ressourcen domänen- und gesamtstrukturübergreifend freigegeben sein. Der globale Katalog von Active Directory macht die domänen- und gesamtstrukturübergreifende Suche nach Ressourcen für den Benutzer transparent. Wenn Sie beispielsweise alle Drucker innerhalb einer Gesamtstruktur suchen, wird diese Abfrage von einem globalen Katalogserver im globalen Katalog ausgeführt und das Ergebnis zurückgegeben. Gäbe es keine globalen Katalogserver, müssten für diese Abfrage alle Domänen der Gesamtstruktur durchsucht werden.

### Was ist der globale Katalog?

Der *globale Katalog* ist ein Informationsrepository, das eine Teilmenge der Attribute aller in Active Directory gespeicherten Objekte enthält. Welche Attribute im globalen Katalog gespeichert werden, wird von den Mitgliedern der Schema-Admins-Gruppe entsprechend den Anforderungen des Unternehmens festgelegt. Der globale Katalog enthält folgende Informationen:

- Die am häufigsten in Abfragen verwendeten Attribute, beispielsweise Vornamen, Nachnamen und Anmeldenamen der Benutzer.
- Informationen, die zum Auffinden eines Objekts innerhalb des Verzeichnisses erforderlich sind.
- Eine Standard-Teilmenge der Attribute jedes einzelnen Objekttyps.
- Die Zugriffsberechtigungen aller Objekte und Attribute, die im globalen Katalog gespeichert sind. Wenn Sie ein Objekt suchen, für das Sie keine Anzeigeberechtigung besitzen, wird das Objekt nicht im Suchergebnis angezeigt. Zugriffsberechtigungen stellen sicher, dass Benutzer nur Objekte finden, für die sie Zugriffsrechte besitzen.

**Was ist ein globaler Katalogserver?**

Ein *globaler Katalogserver* ist ein Domänencontroller, der im globalen Katalog effizient Abfragen innerhalb der Gesamtstruktur ausführt. Der erste Domänencontroller, den Sie in Active Directory erstellen, ist automatisch ein globaler Katalogserver. Neben diesem Server können Sie weitere globale Katalogserver konfigurieren, auf die der Anmelde- und Abfrageverkehr aufgeteilt wird.

**Funktionen des globalen Katalogs**

Über den globalen Katalog können die Benutzer zwei wichtige Funktionen ausführen:

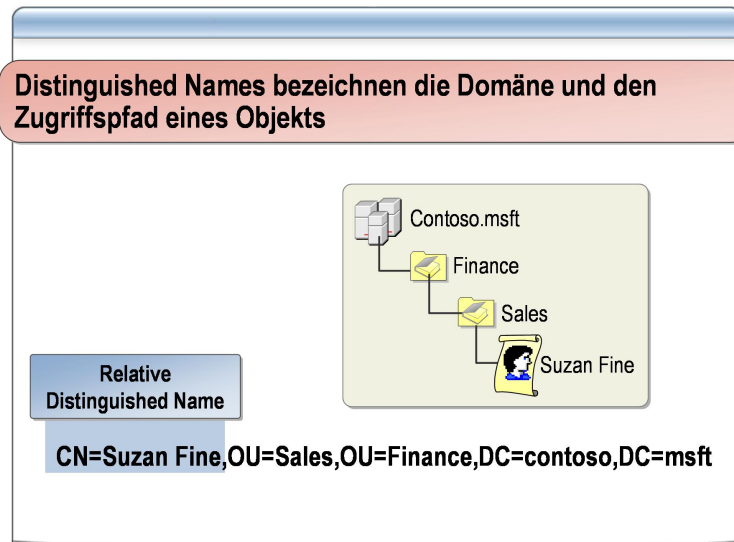
- Suchen nach Active Directory-Informationen innerhalb der Gesamtstruktur, unabhängig vom Speicherort der Daten.
- Anmelden beim Netzwerk auf Grundlage von Daten der universellen Gruppenmitgliedschaft.

---

**Anmerkung** Weitere Informationen über den globalen Katalog finden Sie in Unterrichtseinheit 8, „Implementieren der Domänencontrollerposition“, in Kurs 2195A: *Planen, Implementieren und Warten einer Active Directory-Infrastruktur unter Microsoft Windows Server 2003*.

---

## Was sind Distinguished Names und Relative Distinguished Names?



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

### Einführung

Clientcomputer verwenden das Lightweight Directory Access Protocol (LDAP) zum Suchen und Ändern von Objekten in einer Active Directory-Datenbank. LDAP beinhaltet einen Teil von X.500, einem Industriestandard, der festlegt, wie Verzeichnisse strukturiert werden. LDAP nutzt die Strukturinformationen eines Verzeichnisses für die Suche nach Objekten, die jeweils eindeutige Namen haben.

### Definition

LDAP verwendet einen Namen, der ein Active Directory-Objekt durch eine Reihe von Komponenten definiert, die sich auf die logische Struktur beziehen. Diese Darstellung, auch als *Distinguished Name* (DN) des Objekts bezeichnet, kennzeichnet die Domäne, auf der sich das Objekt befindet, sowie den vollständigen Pfad, über den das Objekt erreicht wird, eindeutig. Ein DN muss innerhalb der Active Directory-Gesamtstruktur eindeutig sein.

Der *Relative Distinguished Name* (RDN) eines Objekts kennzeichnet das Objekt eindeutig innerhalb seines Containers. Kein Objekt innerhalb eines Containers darf den gleichen Namen haben wie ein anderes Objekt im selben Container. Der RDN ist immer die erste Komponente des DN. Es muss sich hierbei jedoch nicht um einen allgemeinen Namen (CN) handeln.

**Beispiel für einen DN**

Der folgende DN gibt jedes einzelne Element der logischen Struktur für eine Benutzerin namens „Suzan Fine“ wieder, die in der Organisationseinheit „Sales“ in der Domäne „Contoso.msft“ arbeitet:

```
CN=Suzan Fine,OU=Sales,DC=contoso,DC=msft
```

- CN ist der allgemeine Name des Objekts innerhalb seines Containers.
- OU ist die Organisationseinheit, in der sich das Objekt befindet. Ein DN kann auch mehrere OU-Werte enthalten, wenn sich das Objekt in einer verschachtelten Organisationseinheit befindet.
- DC ist eine Domänenkomponente wie „com“ oder „msft“. Ein DN enthält immer zwei bzw. bei untergeordneten Domänen auch mehr Domänenkomponenten.

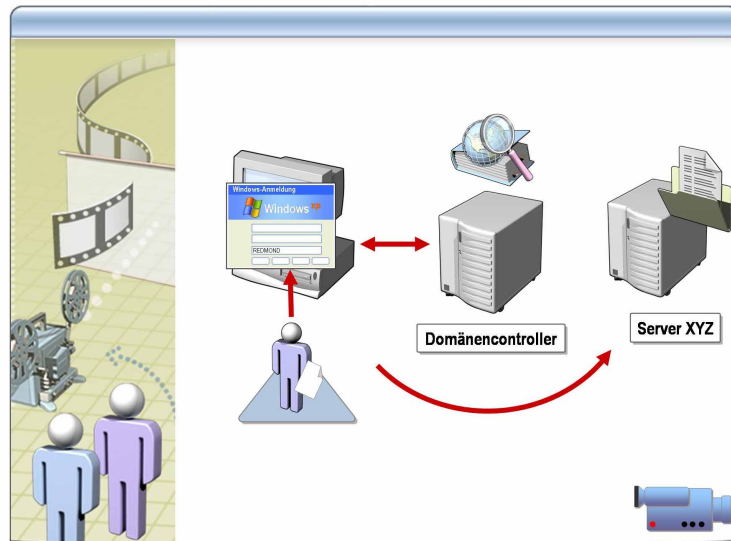
Die Domänenkomponenten eines DN sind im Domain Name System (DNS) definiert.

**Beispiel für einen RDN**

Im folgenden Beispiel ist „Sales“ der RDN einer Organisationseinheit, die durch folgenden LDAP-Namenspfad wiedergegeben wird:

```
OU=Sales,DC=contoso,DC=msft
```

## Multimediapräsentation: Handhabung einmaliger Anmeldungen durch Active Directory



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

### Speicherort der Datei

Öffnen Sie zum Anzeigen der Präsentation *Handhabung einmaliger Anmeldungen durch Active Directory* die Webseite auf der Kursteilnehmer-CD, klicken Sie auf **Multimedia** und anschließend auf den Titel der Präsentation. Starten Sie die Präsentation nur, wenn der Kursleiter Sie dazu auffordert.

### Lernziele

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

- Beschreiben des Prozesses, mit dem Active Directory einmalige Anmeldungen (Single Sign-On) ermöglicht.
- Erklären der Bedeutung von einmaligen Anmeldungen.

### Kernpunkte

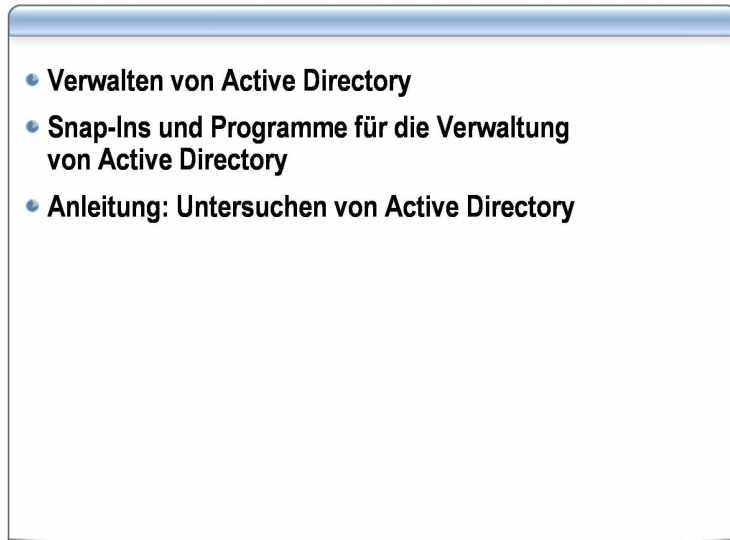
Durch die Möglichkeit der einmaligen Anmeldung macht Active Directory den komplexen Prozess der Authentifizierung und Autorisierung für den Benutzer transparent. Für die Benutzer entfällt dadurch die Verwaltung mehrerer Anmeldeinformationssätze.

Eine einmalige Anmeldung umfasst folgende Prozesse:

- *Authentifizierung*, d. h. die Überprüfung der Anmeldeinformationen des Verbindungsversuchs.
- *Autorisierung*, d. h. die Überprüfung der Zulässigkeit des Verbindungsversuchs.

Als Systemingenieur müssen Sie diese Prozesse verstehen, damit Sie Ihre Active Directory-Struktur optimieren und eventuelle Probleme beheben können.

## Lektion: Untersuchen von Active Directory



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

### Einführung

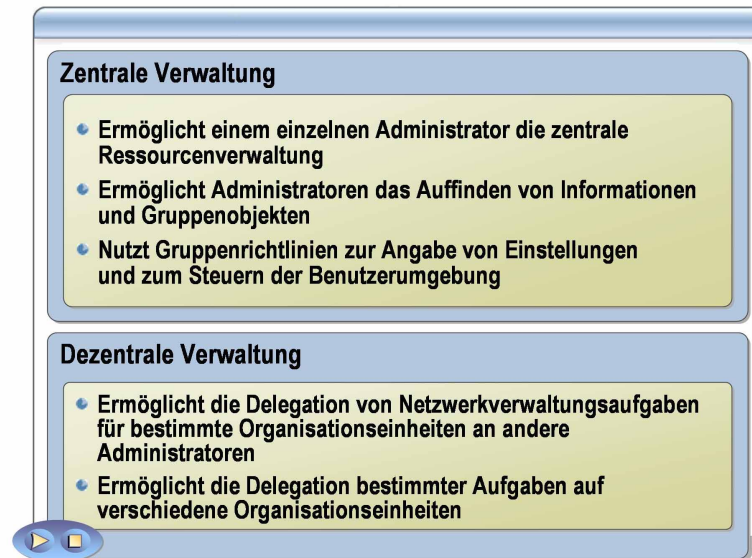
Für Administratoren bietet Windows Server 2003 Snap-Ins und Befehlszeilenprogramme für die Verwaltung von Active Directory. Diese Snap-Ins und Befehlszeilenprogramme werden in dieser Lektion vorgestellt. Sie erfahren außerdem in dieser Lektion, wie Sie diese Programme zur Untersuchung der logischen und physischen Struktur von Active Directory verwenden.

### Lernziele der Lektion

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

- Erklären, wie Active Directory die zentrale und dezentrale Verwaltung ermöglicht.
- Beschreiben der wichtigsten Snap-Ins und Befehlszeilenprogramme für die Verwaltung von Active Directory.
- Untersuchen der logischen und physischen Struktur von Active Directory.

## Verwalten von Active Directory



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

### Einführung

Mit Active Directory können Sie große Mengen an Benutzern, Computern, Druckern und Netzwerkressourcen von einem zentralen Standort aus verwalten. Dazu verwenden Sie die Verwaltungs-Snap-Ins und -Programme von Windows Server 2003. Darüber hinaus unterstützt Active Directory auch die dezentrale Verwaltung. Ein Administrator mit der entsprechenden Berechtigung kann einen ausgewählten Satz von Verwaltungsrechten an andere Benutzer oder Benutzergruppen des Unternehmens delegieren.

### Wie Active Directory die zentrale Verwaltung unterstützt

Active Directory beinhaltet verschiedene Features, die die zentrale Verwaltung unterstützen:

- *Es enthält Informationen über alle Objekte und ihre Attribute.* Die Attributwerte beschreiben die durch das Objekt dargestellte Ressource. Da Active Directory Informationen über alle Netzwerkressourcen speichert, können die Netzwerkressourcen zentral von einem Administrator verwaltet werden.
- *Active Directory kann mit Protokollen wie LDAP abgefragt werden.* Mit Programmen, die LDAP unterstützen, finden Sie Informationen über Objekte problemlos, indem Sie nach ausgewählten Attributen der Objekte suchen.
- *Objekte mit ähnlichen verwaltungs- und sicherheitstechnischen Anforderungen können in Organisationseinheiten zusammengefasst werden.* Organisationseinheiten bieten verschiedene Ebenen der Verwaltungsautorität. Sie können daher Gruppenrichtlinien anwenden und Verwaltungsaufgaben delegieren. Die Möglichkeit der Delegation vereinfacht die Verwaltung der Objekte und ermöglicht es Ihnen, die Struktur von Active Directory an die Anforderungen Ihres Unternehmens anzupassen.
- *Gruppenrichtlinien können für einen Standort, für eine Domäne oder eine Organisationseinheit eingerichtet werden.* Active Directory setzt die Gruppenrichtlinien für alle Benutzer und Computer innerhalb des jeweiligen Containers durch.

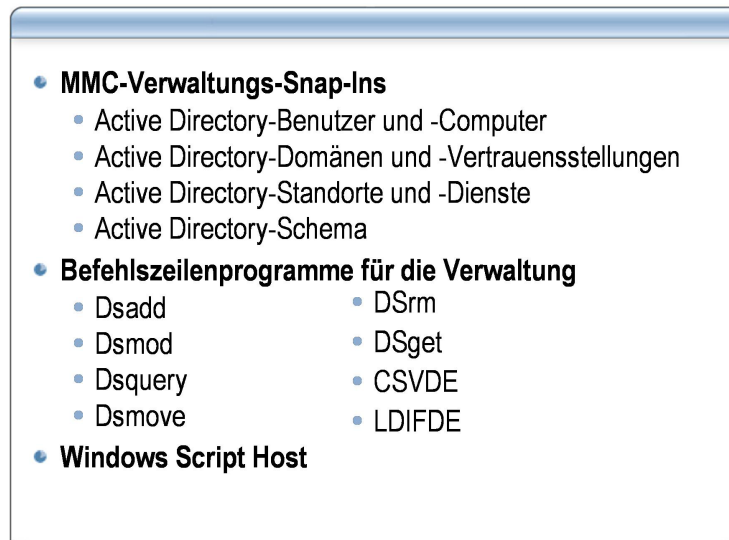
**Wie Active Directory die dezentrale Verwaltung unterstützt**

Neben der zentralen Verwaltung unterstützt Active Directory auch die dezentrale Verwaltung. Berechtigungen und Benutzerrechte können je nach Anforderungen spezifisch zugewiesen werden. So können Sie beispielsweise Verwaltungsberechtigungen für bestimmte Objekte an das Vertriebs- und Marketingteam Ihres Unternehmens abgeben.

Die Zuweisung von Berechtigungen können Sie wie folgt delegieren:

- Für bestimmte Organisationseinheiten an unterschiedliche lokale Gruppen der Domäne. Beispiel: Delegieren der Berechtigung Vollzugriff an die Organisationseinheit „Sales“.
- Berechtigung zur Änderung bestimmter Attribute eines Objekts in einer Organisationseinheit. Beispiel: Zuweisen der Berechtigung, Namen, Adressen und Telefonnummern zu ändern sowie Kennwörter von Benutzerkontoobjekten zurückzusetzen.
- Berechtigung zur Durchführung derselben Aufgabe, beispielsweise Zurücksetzen von Kennwörtern, in allen Organisationseinheiten einer Domäne.

## Snap-Ins und Programme für die Verwaltung von Active Directory



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

### Einführung

Windows Server 2003 bietet eine Reihe von Snap-Ins und Befehlszeilenprogrammen für die Verwaltung von Active Directory. Sie können Active Directory aber auch über Windows Script Host-Skripts mit ADSI-Objekten (Active Directory Service Interfaces) verwalten. ADSI ist eine leistungsstarke und dennoch einfache Schnittstelle zu Active Directory, mit der wiederverwendbare Skripts für die Verwaltung von Active Directory erstellt werden können.

### Verwaltungs-Snap-Ins

In der folgenden Tabelle werden die wichtigsten Snap-Ins für die Verwaltung von Active Directory beschrieben.

Snap-In	Beschreibung
Active Directory-Benutzer und -Computer	Eine Microsoft Management Console (MMC), auf der Sie Active Directory-Informationen verwalten und veröffentlichen. Sie können Benutzerkonten, Gruppen und Computerkonten verwalten, Computer zu Domänen hinzufügen, Kontorichtlinien und Benutzerrechte verwalten sowie Richtlinien überwachen.
Active Directory-Domänen und -Vertrauensstellungen	Eine MMC, auf der Sie Domänen- und Gesamtstruktur-Vertrauensstellungen verwalten, Suffixe zu Benutzerprinzipalnamen hinzufügen und die Funktionsebenen von Domänen und Gesamtstrukturen ändern.
Active Directory-Standorte und -Dienste	Eine MMC, auf der Sie die Replikation der Verzeichnisdaten verwalten.
Active Directory-Schema	Eine MMC, auf der Sie das Schema verwalten. Diese MMC wird nicht automatisch im Menü Verwaltung installiert. Sie müssen sie manuell hinzufügen.

**Anmerkung** Auch mit dem ADSI-Editor können Sie Active Directory-Objekte anzeigen, erstellen, ändern und löschen. Der ADSI-Editor wird nicht standardmäßig installiert. Zur Installation des ADSI-Editors installieren Sie die Supportprogramme von Windows Server 2003 aus dem Ordner \Support\Tools der Produkt-CD.

Die Verwaltungskonsolen können an die an andere Administratoren delegierten Verwaltungsaufgaben angepasst werden. Mehrere für eine Verwaltungsfunktion erforderliche Konsolen können auch zu einer Konsole zusammengefasst werden.

**Befehlszeilenprogramme für die Verwaltung**

In der folgenden Tabelle werden die wichtigsten Befehlszeilenprogramme für die Verwaltung von Active Directory beschrieben.

Programm	Beschreibung
Dsadd	Fügt Objekte wie Computer, Benutzer, Gruppen, Organisationseinheiten und Kontakte zu Active Directory hinzu.
Dsmmod	Ändert Objekte wie Computer, Server, Benutzer, Gruppen, Organisationseinheiten und Kontakte in Active Directory.
Dsquery	Führt in Active Directory Abfragen nach bestimmten Kriterien aus. Abfragen können an Servern, Computern, Gruppen, Benutzern, Standorten, Organisationseinheiten und Partitionen ausgeführt werden.
Dsmove	Verschiebt ein einzelnes Objekt innerhalb einer Domäne an eine andere Stelle in Active Directory oder benennt ein einzelnes Objekt um, ohne es zu verschieben.
Dsrm	Löscht ein Objekt aus Active Directory.
Dsget	Zeigt ausgewählte Attribute von Computern, Kontakten, Gruppen, Organisationseinheiten, Servern oder Benutzern in Active Directory an.
Csvde	Importiert und exportiert Active Directory-Daten in einem Format, in dem Kommas als Trennzeichen verwendet werden.
Ldifde	Erstellt, ändert und löscht Active Directory-Objekte, erweitert das Active Directory-Schema, exportiert Benutzer- und Gruppeninformationen in andere Anwendungen oder Dienste und importiert die Daten anderer Verzeichnisdienste in Active Directory.

**Anmerkung** Weitere Informationen über die Befehlszeilenprogramme von Windows Server 2003 finden Sie in Hilfe und Support unter dem Thema „Verwalten von Active Directory über die Befehlszeile“.

**Windows Script Host**

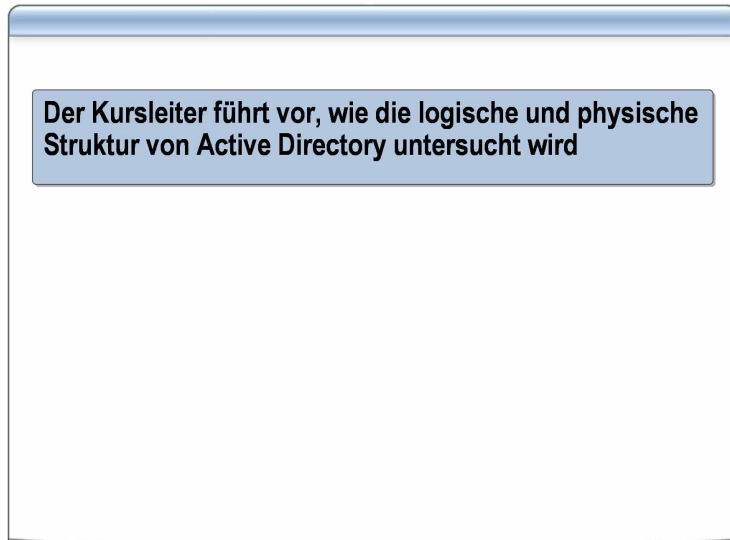
Windows Server 2003 bietet zwar eine Reihe von Snap-Ins und Befehlszeilenprogrammen für die Verwaltung von Active Directory. Diese sind aber nicht für Batchvorgänge geeignet, mit denen komplexe Änderungen in Active Directory durchgeführt werden. In solchen Fällen führen Sie die Änderungen schneller mit einem Skript durch. Mit einem Skript können Sie zum Beispiel für alle Mitarbeiter, die aus Gebäude 3 oder 4 in Gebäude 5 Ihres Unternehmens umziehen, die erste Stelle der Telefondurchwahl von 3 zu 5 bzw. von 4 zu 5 ändern.

Für folgende Aufgaben können Sie Windows Script Host-Skripts mit ADSI-Objekten verwenden:

- Abrufen von Informationen über Active Directory-Objekte.
- Hinzufügen von Objekten zu Active Directory.
- Ändern der Attributwerte von Active Directory-Objekten.
- Löschen von Objekten aus Active Directory.
- Erweitern des Active Directory-Schemas.

Zur Kommunikation mit Active Directory verwendet ADSI das LDAP-Protokoll.

## Anleitung: Untersuchen von Active Directory



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

### Einführung

Die logische und physische Struktur von Active Directory können Sie mit den Verwaltungs-Snap-Ins Active Directory-Benutzer und -Computer, Active Directory-Standorte und -Dienste und Active Directory-Domänen und -Vertrauensstellungen anzeigen.

### Verfahren

Führen Sie die folgenden Schritte aus, um die logische und physische Struktur von Active Directory anzuzeigen:

1. Öffnen Sie das Snap-In Active Directory-Benutzer und -Computer, und zeigen Sie die Organisationseinheiten von Active Directory an. Führen Sie dazu die folgenden Schritte aus:
  - a. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme** und auf **Verwaltung**, und klicken Sie dann auf **Active Directory-Benutzer und -Computer**.
  - b. Erweitern Sie in der Konsolenstruktur den Knoten **Active Directory-Benutzer und -Computer**.
  - c. Erweitern Sie in der Konsolenstruktur die Domäne, deren Organisationseinheiten Sie anzeigen möchten.
  - d. Zeigen Sie für jeden Container der Konsolenstruktur die Seite **Eigenschaften** an.
  - e. Bestimmen Sie den Objekttyp mithilfe der Objektklasseninformationen auf der Registerkarte **Objekt**. Die Objektklasse für Organisationseinheiten lautet *Organisationseinheit*.

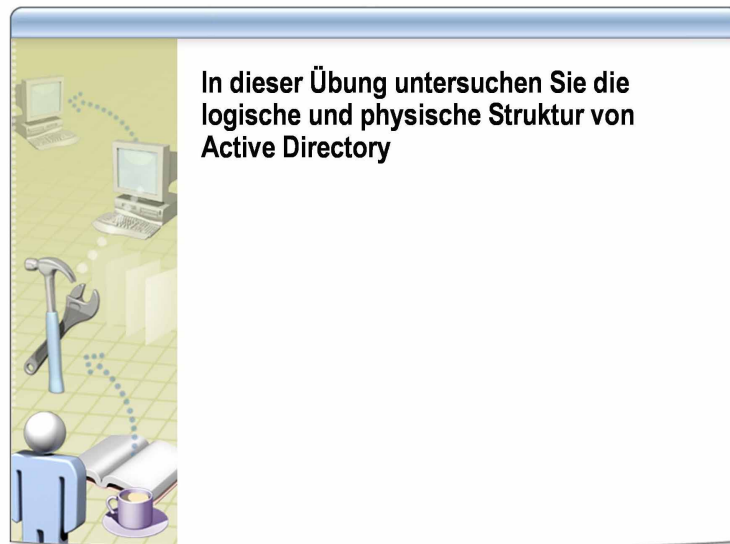
2. Öffnen Sie das Snap-In Active Directory-Domänen und -Vertrauensstellungen, und sehen Sie sich die logische Struktur von Active Directory an. Führen Sie dazu die folgenden Schritte aus:
  - a. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme** und auf **Verwaltung**, und klicken Sie dann auf **Active Directory-Domänen und -Vertrauensstellungen**.
  - b. Erweitern Sie im linken Fensterbereich den Stammdomänenknoten der Gesamtstruktur, um die Domänen anzuzeigen, aus denen die logische Struktur von Active Directory besteht.
3. Öffnen Sie das Snap-In Active Directory-Standorte und -Dienste, und sehen Sie sich die physische Struktur von Active Directory an. Führen Sie dazu die folgenden Schritte aus:
  - a. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme** und auf **Verwaltung**, und klicken Sie dann auf **Active Directory-Standorte und -Dienste**.
  - b. Erweitern Sie in der Konsolenstruktur den Knoten **Standorte** und danach den Ordner des Standorts, dessen Serverliste Sie anzeigen möchten.
  - c. Klicken Sie auf **Server**, um im rechten Fensterbereich eine Liste der Server anzuzeigen.

---

**Anmerkung** Weitere Informationen über die Untersuchung von Active Directory finden Sie im Ordner Anhänge der Kursteilnehmer-CD in Unterrichtseinheit 1 unter dem Thema „Anleitung: Untersuchen von Active Directory“.

---

## Praktische Übung: Untersuchen der Active Directory-Struktur



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

- Lernziele** In dieser Übung untersuchen Sie die logische und physische Struktur von Active Directory.
- Szenario** Heute ist Ihr erster Tag als Systemingenieur bei der Firma Northwind Traders. Ihr Vorgesetzter hat Sie gebeten, sich mit der logischen und physischen Struktur von Active Directory bei Northwind Traders vertraut zu machen.
- Praktische Übung**
- ▶ **Untersuchen Sie die Standardstruktur der Active Directory-Objekte mithilfe des Snap-Ins Active Directory-Benutzer und -Computer**
1. Melden Sie sich als **nwtraders\ComputerNameUser** mit dem Kennwort **P@ssw0rd** an.
  2. Installieren Sie die Verwaltungsprogramme von Windows Server 2003. Führen Sie dazu die folgenden Schritte aus:
    - a. Klicken Sie auf **Start**, klicken Sie mit der rechten Maustaste auf **Eingabeaufforderung**, und klicken Sie dann auf **Ausführen als**.
    - b. Wählen Sie im Dialogfeld **Ausführen als** die Option **Folgender Benutzer** aus, geben Sie als Benutzername **nwtraders\administrator** und als Kennwort **P@ssw0rd** ein, und klicken Sie auf **OK**.
    - c. Geben Sie an der Eingabeaufforderung **\\London\OS\i386\Adminpak.msi** ein, und drücken Sie dann die EINGABETASTE.
    - d. Klicken Sie im Dialogfeld **Dateidownload** auf **Öffnen**, und führen Sie Installation aus.
    - e. Schließen Sie das Eingabeaufforderungsfenster.
  3. Öffnen Sie das Snap-In Active Directory-Benutzer und -Computer.
  4. Aktivieren Sie die erweiterten Funktionen.

5. Erweitern Sie **nwtraders.msft**, und suchen Sie das Objekt Locations. Welchen Objekttyp hat dieses Objekt?

**Das Objekt Locations ist eine Organisationseinheit.**

---

---

6. Erweitern Sie **Locations**. Welche Objekttypen enthält der Ordner?

**Die Organisationseinheit Locations enthält 25 weitere Organisationseinheiten, die jeweils nach einer anderen Stadt benannt sind.**

---

---

7. Die Objekte im Ordner Locations stellen die geographischen Standorte der Organisation dar. Jeder Standort enthält drei Objekte. Welche Funktion haben diese Objekte?

**Jede Organisationseinheit mit einem *Standortnamen* enthält drei Organisationseinheiten mit den Namen Users, Computer und Groups. Diese Organisationseinheiten sind für Benutzer-, Computer- bzw. Gruppenobjekte vorgesehen.**

---

---

8. Öffnen Sie einen beliebigen Standortcontainer und danach den darin enthaltenen Container Users.

Was fällt Ihnen an den Objekten in diesem Container auf?

**Alle Benutzerobjekte sind deaktiviert.**

---

► **Untersuchen Sie die Standardstruktur von Active Directory mithilfe des Snap-Ins „Active Directory-Standorte und -Dienste“**

1. Öffnen Sie das Snap-In Active Directory-Standorte und -Dienste.
2. Erweitern Sie **Standorte**, klicken Sie mit der rechten Maustaste auf **Standardname-des-ersten-Standorts**, und klicken Sie dann auf **Eigenschaften**.

3. Sehen Sie sich auf der Registerkarte **Sicherheit** die Berechtigungen der Gruppe Domänen-Admins an. Welche Berechtigungen hat diese Gruppe?  
**Die Gruppe „Domänen-Admins“ hat die Berechtigungen „Lesen“, „Schreiben“, „Alle untergeordneten Objekte erstellen“, „Connector-Warteschlange öffnen“ sowie „Spezielle Berechtigungen“ für den Standort „Standardname-des-ersten-Standorts“.**
- 
- 

4. Sehen Sie sich die Berechtigungen der Gruppe Domänen-Admins des Objekts **Standardname-des-ersten-Standorts\Servers\London** an. Was fällt Ihnen auf?

**Für das Serverobjekt „London“ hat die Gruppe „Domänen-Admins“ die Berechtigung „Vollzugriff“. Am Standort „Standardname-des-ersten-Standorts“ hat sie jedoch keinen Vollzugriff.**

---

---

► **Untersuchen Sie die Standardstruktur von Active Directory mithilfe des Snap-Ins „Active Directory-Domänen und -Vertrauensstellungen“**

1. Öffnen Sie das Snap-In Active Directory-Domänen und -Vertrauensstellungen.
2. Erweitern Sie **nwtraders.msft**, und zeigen Sie die Eigenschaften von nwtraders.msft an.

Was fällt Ihnen auf?

**Die Vertrauensstellungen dieser Domäne werden angezeigt.**

---

3. Wählen Sie die Domäne corp.nwtraders.msft, und starten Sie die Verwaltung. Was geschieht daraufhin?

**Das Snap-In „Active Directory-Benutzer und -Computer“ wird geöffnet.**

---

# Lektion: Die Entwurfs-, Planungs- und Implementierungsprozesse von Active Directory

- Übersicht über den Entwurf, die Planung und die Implementierung von Active Directory
- Der Entwurfsprozess von Active Directory
- Der Planungsprozess von Active Directory
- Der Implementierungsprozess von Active Directory

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

## Einführung

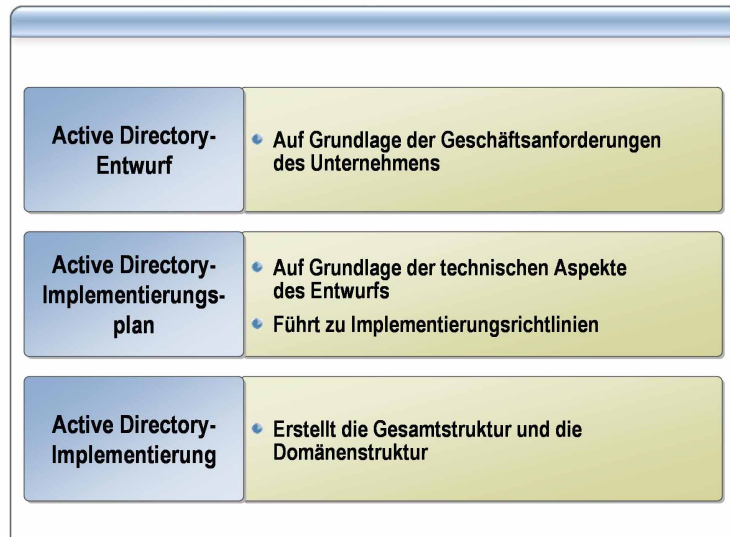
Diese Lektion gibt eine Übersicht über die Entwurfs-, Planungs- und Implementierungsprozesse von Active Directory.

## Lernziele der Lektion

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

- Unterscheiden zwischen Entwurf, Planung und Implementierung von Active Directory.
- Beschreiben der einzelnen Phasen des Entwurfsprozesses von Active Directory.
- Beschreiben der einzelnen Phasen des Planungsprozesses von Active Directory.
- Beschreiben der einzelnen Phasen des Implementierungsprozesses von Active Directory.

## Übersicht über den Entwurf, die Planung und die Implementierung von Active Directory



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

### Einführung

Die Implementierung von Active Directory beginnt mit der Erstellung eines Active Directory-Entwurfs. Diesen Entwurf verwenden Sie zur Planung der Implementierung und schließlich zur Implementierung von Active Directory.

### Active Directory-Entwurf

Der Active Directory-Entwurf wird von einem oder mehreren Systemarchitekten auf Grundlage der Geschäftsanforderungen des Unternehmens entwickelt. Die Geschäftsanforderungen bestimmen die funktionalen Spezifikationen des Entwurfs.

### Active Directory-Implementierungsplan

Der Implementierungsplan für Active Directory legt fest, wie der Active Directory-Entwurf unter den gegebenen Hardwarebedingungen des Unternehmens implementiert wird. Der Active Directory-Entwurf kann beispielsweise die Anzahl der Domänencontroller für jede Domäne auf der Grundlage einer bestimmten Serverkonfiguration vorgeben. Falls diese Konfiguration jedoch nicht zur Verfügung steht, können Sie in der Planungsphase entscheiden, die Anzahl der Server zu ändern und so die Geschäftsanforderungen Ihres Unternehmens zu erfüllen.

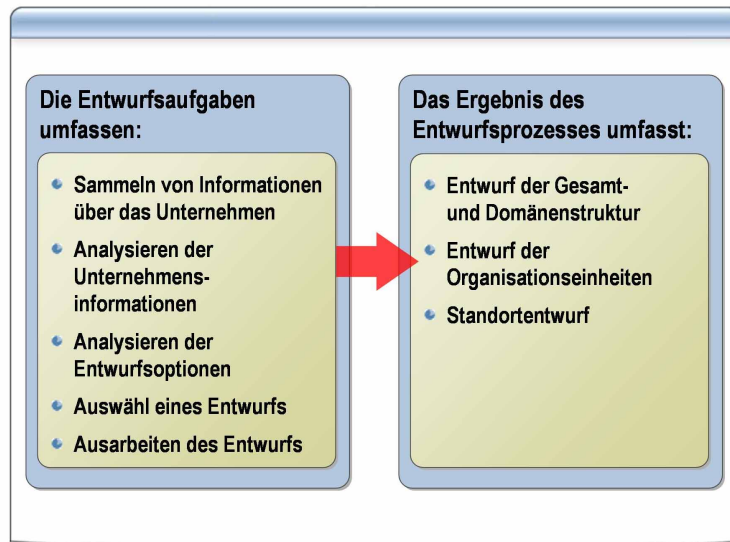
Nach der Implementierung müssen Sie Active Directory verwalten und warten, um seine Verfügbarkeit, Zuverlässigkeit und Netzwerksicherheit zu garantieren. In diesem Kurs wird die Planungs- und Implementierungsphase beschrieben. Eine ausführliche Besprechung der Entwurfsphase würde den Rahmen dieses Kurses sprengen.

**Active Directory-  
Implementierung**

Die Implementierung von Active Directory umfasst folgende Aufgaben:

- Erstellen der Gesamt- und Domänenstruktur sowie die Bereitstellung der Server.
- Erstellen der Struktur der Organisationseinheiten.
- Erstellen der Benutzer- und Computerkonten.
- Erstellen der Sicherheits- und Verteilergruppen.
- Erstellen der Gruppenrichtlinienobjekte (GPOs) und deren Anwendung auf Domänen, Standorte und Organisationseinheiten.
- Erstellen der Verteilerrichtlinie für Software.

## Der Entwurfsprozess von Active Directory



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

### Einführung

Ein Active Directory-Entwurf umfasst mehrere Aufgaben. Jede dieser Aufgaben definiert die funktionalen Anforderungen einer Komponente der Active Directory-Implementierung.

### Aufgaben des Active Directory-Entwurfsprozesses

Der Active Directory-Entwurfsprozess umfasst die folgenden Aufgaben:

- *Sammeln von Informationen über das Unternehmen.* In dieser ersten Aufgabe werden die Anforderungen an den Verzeichnisdienst und die Geschäftsanforderungen des Projekts festgelegt. Informationen über ein Unternehmen beinhalten ein detailliertes Organisationsprofil, Angaben über die geographischen Standorte des Unternehmens, die technische Ausstattung sowie die Infrastruktur des Netzwerks und eventuelle Änderungspläne des Unternehmens.
- *Analysieren der Unternehmensinformationen.* Die gesammelten Informationen über das Unternehmen müssen ausgewertet werden, damit ihre Relevanz und Wichtigkeit für den Entwurfsprozess bestimmt werden kann. Sie legen fest, welche Informationen wichtig sind und auf welche Komponenten des Active Directory-Entwurfs sich diese Vorgaben auswirken. Bedenken Sie, dass Sie diese Vorgaben während des gesamten Entwurfsprozesses berücksichtigen müssen.
- *Analysieren der Entwurfsoptionen.* Bei der Auswertung der Unternehmensinformationen stellen Sie vermutlich fest, dass es verschiedene Entwurfsoptionen gibt, die die Geschäftsanforderungen erfüllen. Eine verwaltungstechnisch vorgegebene Anforderung lässt sich zum Beispiel durch einen Domänenentwurf oder durch Organisationseinheiten lösen. Jede Entscheidung, die Sie treffen, wirkt sich auf andere Entwurfskomponenten aus. Bleiben Sie also in der gesamten Entwurfsphase flexibel.

- *Auswahl eines Entwurfs.* Entwickeln Sie mehrere Active Directory-Entwürfe und vergleichen Sie ihre Stärken und Schwächen. Überprüfen Sie bei der Auswahl eines Entwurfs, ob es Konflikte zwischen Geschäftsanforderungen gibt, und überdenken Sie deren Auswirkungen auf Ihre Entwurfsoptionen. Möglicherweise gibt es unter allen Entwurfsoptionen keinen eindeutigen Sieger. Wählen Sie den Entwurf aus, der die meisten Geschäftsanforderungen erfüllt und zum besten Gesamtergebnis führt.
- *Ausarbeiten des Entwurfs.* Die erste Version Ihres Entwurfs wird sich sicherlich bis zur Pilotphase der Implementierung ändern. Bei der Entwicklung einer Active Directory-Infrastruktur müssen zahlreiche Variablen berücksichtigt werden, die eine ständige Überarbeitung des Entwurfs erfordern. Überprüfen und verbessern Sie jedes Entwurfskonzept mehrmals, bis alle Geschäftsanforderungen erfüllt sind.

### Ergebnis des Active Directory- Entwurfsprozesses

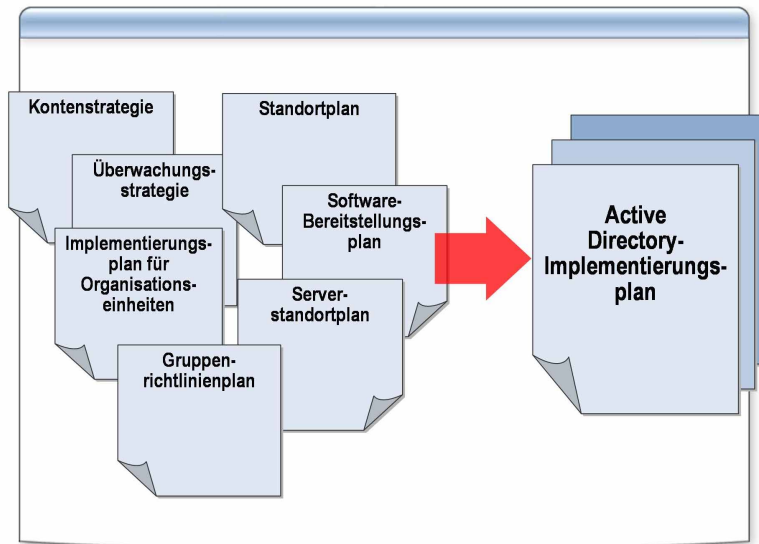
Am Ende des Active Directory-Entwurfsprozesses haben Sie folgende Einzelentwürfe:

- *Entwurf der Gesamt- und Domänenstruktur.* Der Gesamtstrukturentwurf beinhaltet Informationen wie die Anzahl der erforderlichen Gesamtstrukturen, die Richtlinien für die Erstellung von Vertrauensstellungen und die vollqualifizierten Domännennamen der Stammdomäne jeder Gesamtstruktur. Dieser Entwurf enthält unter anderem auch eine Steuerungsrichtlinie für Gesamtstrukturänderungen. Diese Richtlinie bestimmt die Besitzer- und Zulassungsprozesse für Konfigurationsänderungen, die sich auf die gesamte Struktur auswirken. Geben Sie an, welche Personen innerhalb der einzelnen Gesamtstrukturen für die Festlegung der Steuerungsrichtlinie für Gesamtstrukturänderungen verantwortlich sind. Falls Ihr Entwurf mehrere Gesamtstrukturen enthält, können Sie zwischen den Gesamtstrukturen Vertrauensstellungen einrichten, über die Netzwerkressourcen zwischen den Gesamtstrukturen ausgetauscht werden können.

Der Domänenentwurf legt die Anzahl der in jeder Gesamtstruktur erforderlichen Domänen, die Stammdomäne der einzelnen Gesamtstrukturen sowie die Domänenhierarchie fest (wenn der Entwurf mehrere Domänen enthält). Außerdem legt der Domänenentwurf die DNS-Namen der einzelnen Domänen sowie die Vertrauensstellungen zwischen den Domänen fest.

- *Entwurf der Organisationseinheiten.* Dieser Entwurf gibt an, wie die Organisationseinheiten der einzelnen Domänen in der Gesamtstruktur erstellt werden. Der Entwurf beschreibt die Verwaltungsautorität der einzelnen Organisationseinheiten und bestimmt die Personen, an die die Verwaltungsautorität delegiert wird. Außerdem enthält der Entwurf eine Strategie für die Anwendung der Gruppenrichtlinie auf die Struktur der Organisationseinheiten.
- *Standortentwurf.* Dieser Entwurf beschreibt die Anzahl und die Position der Unternehmensstandorte, die erforderlichen Standortverknüpfungen sowie die Kosten der Verknüpfungen.

## Der Planungsprozess von Active Directory



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

### Einführung

Das Ergebnis des Planungsprozesses ist der Implementierungsplan für Active Directory. Dieser Plan umfasst mehrere Einzelpläne, die jeweils die funktionalen Anforderungen einer bestimmten Komponente der Active Directory-Implementierung definieren.

### Komponenten eines Active Directory-Plans

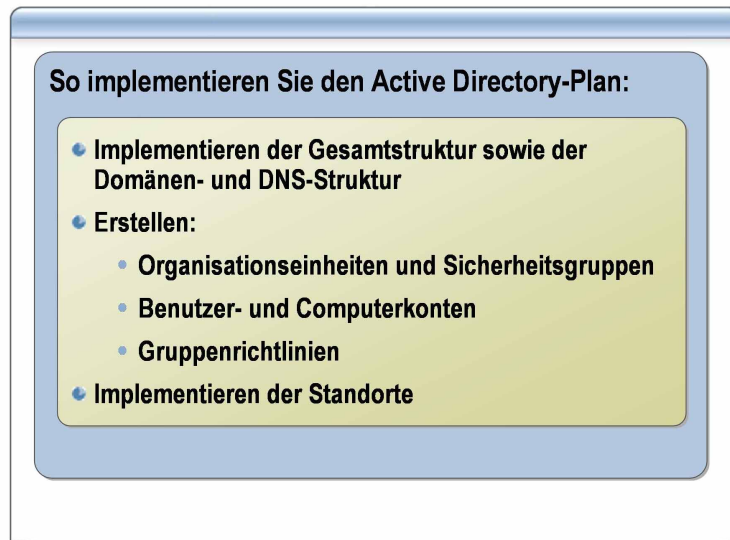
Ein Active Directory-Plan enthält die folgenden Komponenten:

- *Kontenstrategie*. Dieser Plan beinhaltet Informationen wie die Kontonamen- und Kontosperrungsrichtlinien, die Kennwortrichtlinie und Sicherheitsrichtlinien für Objekte.
- *Überwachungsstrategie*. Dieser Plan legt fest, wie Änderungen an Active Directory-Objekten überwacht werden.
- *Implementierungsplan für Organisationseinheiten*. Dieser Plan legt fest, wie und welche Organisationseinheiten erstellt werden. Wenn der Entwurf für die Organisationseinheiten beispielsweise festlegt, dass die Organisationseinheiten nach geographischer Region erstellt und innerhalb jeder Region nach Geschäftsbereichen eingeteilt werden sollen, definiert der Implementierungsplan die zu implementierenden Organisationseinheiten, zum Beispiel „Vertrieb“, „Personal“ und „Produktion“. Darüber hinaus enthält der Plan Richtlinien für die Delegation der Autorität.
- *Gruppenrichtlinienplan*. Dieser Plan legt fest, wer Gruppenrichtlinienobjekte erstellt, verknüpft und verwaltet und wie die Gruppenrichtlinie implementiert wird.
- *Standortplan*. Dieser Plan bestimmt die Standorte, die Standortverknüpfungen und den Verknüpfungszeitplan. Außerdem definiert er den Replikationszeitplan und das Replikationsintervall sowie die Richtlinien für die Sicherheit und die Konfiguration der Replikation zwischen den Standorten.

- *Softwarebereitstellungsplan*. Dieser Plan bestimmt, wie die Gruppenrichtlinie zur Bereitstellung neuer Software bzw. zur Bereitstellung von Softwareupdates verwendet wird. Der Plan kann beispielsweise festlegen, ob Softwareupdates zwingend erforderlich oder optional sind.
- *Serverstandortplan*. Legt die Standorte von Domänencontrollern, globalen Katalogservern, in Active Directory integrierten DNS-Servern und Betriebsmastern fest. Außerdem gibt dieser Plan an, ob für Standorte, die über keinen globalen Katalogserver verfügen, die Zwischenspeicherung der universellen Gruppenmitgliedschaft aktiviert wird.

Die fertiggestellten Einzelpläne fassen Sie zum Schluss zum vollständigen Active Directory-Implementierungsplan zusammen.

## Der Implementierungsprozess von Active Directory



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

### Einführung

Nach der Fertigstellung des Active Directory-Implementierungsplans können Sie beginnen, Active Directory entsprechend Ihrem Entwurf zu implementieren.

### Der Implementierungsprozess

Die Implementierung von Active Directory umfasst die folgenden Aufgaben:

- *Implementieren der Gesamtstruktur sowie der Domänen- und DNS-Struktur.* Diese Aufgabe umfasst die Erstellung der Stammdomäne der Gesamtstruktur, der Domänenstrukturen sowie der untergeordneten Domänen, aus denen sich die Gesamt- und Domänenhierarchie zusammensetzt.
- *Erstellen von Organisationseinheiten und Sicherheitsgruppen.* Diese Aufgabe umfasst die Erstellung der Organisationseinheitenstruktur für jede Domäne in allen Gesamtstrukturen, die Erstellen von Sicherheitsgruppen sowie die Delegation der Verwaltungsautorität an administrative Gruppen in jeder Organisationseinheit.
- *Erstellen von Benutzer- und Computerkonten.* Diese Aufgabe umfasst den Import von Benutzerkonten in Active Directory.
- *Erstellen von Gruppenrichtlinienobjekten.* Diese Aufgabe umfasst die Erstellung von Gruppenrichtlinienobjekten entsprechend der Gruppenrichtlinienstrategie sowie die Verknüpfung der Gruppenrichtlinienobjekte mit Standorten, Domänen und Organisationseinheiten.
- *Implementieren der Standorte.* Diese Aufgabe umfasst die Erstellung von Standorten entsprechend dem Standortplan, die Erstellung von Standortverknüpfungen, die Festlegung der Verknüpfungszeitpläne sowie die Bereitstellung von Domänencontrollern, globalen Katalogservern, DNS-Servern und Betriebsmastern an den einzelnen Standorten.

