Einführung in das Active Directory im Anwendungsmodus

Microsoft GmbH

Veröffentlich August 2002

Übersicht

Der Active Directory®-Dienst von Microsoft® Windows® ist der am schnellsten wachsende Verzeichnisdienst für Intra- und Extranet. Dies rührt daher, dass er eine reichhaltige Integration von Verzeichnis, Sicherheit und Skalierbarkeit bietet und das Lightweight Directory Access Protokoll (LDAP) direkt unterstützt. Windows Server 2003 baut auf diesen Erfolg auf, indem es eine Reihe neuer Möglichkeiten von LDAP unterstützt, die auf IT-Professionals und Anwendungsentwickler ausgerichtet sind. Der Anwendungsmodus des Active Directorys (AD/AM) ist eine dieser neuen Möglichkeiten, die Teil des von Microsoft vollständig in die Windows Server 2003 integrierten Verzeichnisdiensts sind. Unternehmen, Independent Software Vendors (ISVs) und Anwendungsentwickler, die ihre Anwendungen in den Verzeichnisdienst integrieren möchten, verfügen nun über eine zusätzliche Möglichkeit, die ihnen eine Reihe von Vorteilen bietet. Dieser Artikel bietet eine Einführung in AD/AM und beschreibt, welche Vorteile dieser für Unternehmen bietet.

Hinweis auf Betaversion

Bei diesem Dokument handelt es sich um ein vorläufiges Dokument, das bis zur endgültigen Handelsausgabe der hier beschriebenen Software wesentlichen Änderungen unterliegen kann.

Die in diesem Dokument enthaltenen Informationen stellen die behandelten Themen aus der Sicht der Microsoft Deutschland GmbH zum Zeitpunkt der Veröffentlichung dar. Da Microsoft Deutschland auf sich ändernde Marktanforderungen reagieren muss, stellt dies keine Verpflichtung seitens der Microsoft Deutschland GmbH dar und Microsoft kann die Richtigkeit der hier dargelegten Informationen nach dem Zeitpunkt der Veröffentlichung nicht garantieren. Dieses Dokument dient ausschließlich informativen Zwecken. Microsoft schließt für dieses Dokument jede Gewährleistung aus, sei sie ausdrücklich oder konkludent.

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 Deutschland GmbH 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.

Soweit nicht anders vermerkt, sind alle in diesem Dokument genannten Unternehmen, Namen, Adressen, Produkte, Domänennamen, E-Mail-Adressen, Logos und Orte frei erfunden und stehen in keinerlei Verbindung zu einem real existierenden Unternehmen, Namen, einer Adresse, einem Produkt, Domänennamen, einer E-Mail-Adresse, einem Logo oder Ort.

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. Das Bereitstellen dieses Dokuments gibt Ihnen jedoch keinen Anspruch auf diese Patente, Marken, Urheberrechte oder auf sonstiges geistiges Eigentum, es sei denn, dies wird ausdrücklich in den schriftlichen Lizenzverträgen von Microsoft eingeräumt.

Active Accessibility, Active Channel, Active Client, Active Desktop, Active Directory, ActiveMovie, ActiveX, Authenticode, BackOffice, Direct3D, DirectAnimation, DirectDraw, DirectInput, DirectMusic, DirectPlay, DirectShow, DirectSound, DirectX, DoubleSpace, DriveSpace, FrontPage, IntelliMirror, IntelliMouse, IntelliSense, JScript, Links, Microsoft, Microsoft Press, Microsoft QuickBasic, MSDN, MS-DOS, MSN, Natural, NetMeeting, NetShow, OpenType, Outlook, PowerPoint, SideWinder, Slate, TrueImage, Verdana, Visual Basic, Visual C++, Visual FoxPro, Visual InterDev, Visual J++, Visual Studio, WebBot, Win32, Windows, Windows Media, Windows NT sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Weitere in diesem Dokument aufgeführte tatsächliche Produkt- und Firmennamen können geschützte Marken ihrer jeweiligen Inhaber sein.

Inhaltsverzeichnis

Einleitung

Ursprünglich inspiriert durch das Auftauchen von Lösungen, die auf dem Lightweight Directory Access Protocol (LDAP) basierten (Mitte der 90er Jahre), begannen Unternehmen damit, Lösungen einzusetzen, die in der Lage waren, auf das Verzeichnis zuzugreifen. Diese stellten Lösungen für wichtige Probleme wie z. B. den Zugriff auf ein Telefon- oder Branchenbuch, Single Sign-On bei Extranet- oder Webzugriff, die Infrastruktur für das Verwenden von öffentlichen Schlüsseln, Unterstützung von Netzwerkbetriebssystemen und Geschäftsanwendungen, bereit.

Die Folge ist, dass in den meisten Unternehmen heute mehrere Verzeichnisdienste vorzufinden sind: Ein Verzeichnisdienst regelt die Authentifizierung und Berechtigung der Benutzer (Unterstützung des Netzwerkbetriebsystems, NOS), ein anderer ist für öffentliche Schlüssel zuständig (PKI), die von einer Anwendung für den Remotezugriff benutzt werden, ein Verzeichnis ist ein Telefonbuch und ein weiterer ist für das Single-Sign-On bei Extranet- oder Webzugriffen zuständig. Darüber hinaus stellt man auch immer häufiger fest, dass es nicht nur unterschiedliche Verzeichnisdienste innerhalb eines Unternehmens gibt, sondern dass diese auch auf unterschiedlichen Technologien beruhen. So kann es sich z. B. bei dem Verzeichnis, das für das NOS zuständig ist, um ein Verzeichnis auf der Basis von Microsoft Active Directory® handeln, während die Infrastruktur für die öffentlichen Schlüsseln auf der Basis eines X.500-Verzeichnisses gelöst ist und Telefonbuch und Verzeichnis für die Geschäftsanwendungen dann wieder auf anderen Technologien basieren.

Basiert dann noch jeder dieser unterschiedlichen Verzeichnisdienste auf LDAP, stellt sich offensichtlich die Frage, warum die Unternehmen nicht in der Lage waren, sich auf eine Verzeichnistechnologie zu einigen. Die Antwort liegt in den einzelnen Faktoren, die zu diesem Phänomen geführt haben:

- **Fehlende Interoperabilität der Verzeichnisse –** Viele Verzeichnisdienste arbeiten schlichtweg nicht mit anderen zusammen. Ein historisches Beispiel dafür ist das originale X.500-Verzeichnis, das das LDAP-Protokoll nicht unterstützt. Auch heute unterstützen einige Produkte, die ein Verzeichnis als Teil der Lösung implementieren, LDAP oder andere gängige Protokolle nicht.
- **Geringe Auswahl –** Einige Hersteller liefern ihre Lösungen aus, die nur darauf zertifiziert sind, mit einem eingeschränkten Subset von Verzeichnisdiensten, die heute verfügbar sind, zusammen zuarbeiten. Dadurch sind Kunden, die diese Anwendung einsetzen möchten, dazu gezwungen, einen Verzeichnisdienst zu installieren, der anderweitig im Unternehmen nicht benötigt wird.
- **Fehlende Koordination –** In einigen Fällen haben voneinander losgelöste Gruppen unterschiedliche Lösungen installiert. Dies führte zur Nutzung unterschiedlicher Verzeichnistechniken.
- **Fehlende Zusammenarbeit im Bereich Sicherheit –** Geschäftslösungen erlauben es selten, sich mit Benutzerinformationen zu identifizieren, die im Verzeichnis gespeichert und nicht direkt mit der entsprechenden Lösung verbunden sind. Dies bedeutet einmal mehr, dass man mehrere Verzeichnisse anlegen muss, die als Speicher für Benutzerinformationen für jede einzelne Anwendung dienen.

  Viele Unternehmen erkennen erst jetzt, welche enorm hohen, verdeckten Kosten mit diesen vielen unterschiedlichen Verzeichnisdiensten verbunden sind:

- **Erhöhte Sicherheitsrisiken –** Im Bereich der Geschäftlösungen, die auf den unterschiedlichen Verzeichnisdiensten beruhen, ist es enorm schwierig, sicherzustellen, dass diese Lösungen auch effektiv in einen Geschäftsprozess integriert werden können. Wenn Angestellte, Partner, Vertragspartner oder Kunden eine Geschäftsbeziehung aufnehmen oder beenden, ist es von hoher Wichtigkeit, dass der Zugriff auf VPN, PKI, NOS oder andere Geschäftslösungen sofort eingerichtet bzw. beendet werden kann. Ist der Verwaltungsaufwand dagegen hoch, leidet darunter auch die Produktivität. Werden auf der anderen Seite die Zugriffsmöglichkeiten nicht schnellstens beendet, entstehen Sicherheitsrisiken, die es einer Person, die nicht dazu berechtigt ist, ermöglicht, auf eine Geschäftslösung weiterhin zuzugreifen.

- **Hohe Gesamtbetriebskosten –** Jede Lösung, die auf einer unterschiedlichen Verzeichnistechnik beruht benötigt:
- Personen, die auf diese Technik trainiert wurden.
- Unterschiedliche Administrations- und Verwaltungsprozeduren.
- Zusätzliche Lizenzen und Supportvereinbarungen
- **Steigende Kosten im „Erfolgsfall“ –** Einige Verzeichnisse werden nach der Anzahl der Objekte, die innerhalb des Verzeichnisses abgelegt werden, lizenziert. Dies bedeutet, dass die Kosten für Lizenzen und Betrieb sich mit dem Erfolg, die eine Lösung mit der Zeit hat, in einer Spirale nach oben schrauben. Diese unglückliche Situation betrifft gerade Firmen, die eine Lösung einsetzen möchten, die Extranetzugriffe verwaltet und mehrere Millionen von Kunden verwalten soll.
- **Fehlende Integration in den Geschäftsprozess –** Verzeichnisinformationen können flüchtig sein. Wenn ein Benutzer von einer Gruppe in die nächste wechselt, sich die Adresse des Büros oder die Telefonnummer ändert, der Name oder die Position sich verändern, müssen die Informationen innerhalb des Verzeichnisses aktualisiert werden. Werden diese Informationen nun auch in anderen Lösungen benötigt, die ein anderes Verzeichnis einsetzen, dann müssen diese ebenfalls aktualisiert werden. Ist dieser Prozess nicht automatisiert, werden die Daten instabil und können in den einzelnen Verzeichnissen voneinander abweichen.

Was die Kunden an dieser Stelle benötigen, ist ein Verzeichnis, das es ihnen erlaubt, dieses sowohl im Bereich des Netzwerkbetriebssystems – wie z. B. das Active Directory – als auch im Bereich der Anwendungen einzusetzen. Gleichzeitig muss es sich dazu eignen, die Sicherheit, die in die Netzwerkbetriebssyteminfrastruktur eingebaut wurde, für Anwendungen zu benutzen.
Der Anwendungsmodus des Active Directorys erreicht genau dieses Ziel. Hierbei entfallen zusätzliche Kosten für weitere Lizenzen oder teuere Trainings. Gleichfalls entfallen auch die Kosten, die durch die Installation von unterschiedlichen Verzeichnissen zur Unterstützung von verzeichnisfähigen Anwendungen entstehen.

Der Anwendungsmodus des Active Directorys (AD/AM) stellt eine neue Fähigkeit von Microsoft Active Directory dar, die auf bestimmte Einsatzszenarien ausgerichtet ist, die mit verzeichnisfähigen Anwendungen zusammen hängen. AD/AM wird als Dienst, der unabhängig vom Betriebssystem ist, ausgeführt und muss nicht auf einem Domänencontroller ausgeführt werden. Dies bedeutet, dass mehrere Instanzen von AD/AM auf einem einzigen Server ausgeführt werden können und jede einzelne Instanz unabhängig konfiguriert werden kann.

Wenn auch die Vision eines einzigen Verzeichnisdienstes für Unternehmen noch immer nicht erfüllt werden kann, so stellt der Anwendungsmodus des Active Directorys doch einen Durchbruch im Bereich der Verzeichnisdienste dar, der die oben beschriebenen Probleme löst und Flexibilität erlaubt. Er unterstützt Unternehmen bei der Einsparung von Kosten, die aus einer komplexen Infrastruktur entstehen.

Einfachheit des Anwendungsmodus

Viele Anwendungen benötigen nur ein einfaches Anwendungsverzeichnis. Die Informationen, die in diesem Verzeichnis abgespeichert werden, müssen nicht unbedingt global von Interesse sein und benötigen auch keine umfangreiche Replikation. Sie benötigen nicht unbedingt die gleiche Stufe eines Dienstes, wie er von den bestehenden Domänencontrollern, die das NOS-Verzeichnis speichern, angeboten wird. So können die Daten einer Anwendung sich sehr häufig ändern. Dies würde einen relativ hohen Replikationsverkehr verursachen, der Auswirkungen auf die Netzwerkressourcen haben könnte, wenn die Daten innerhalb des NOS-Verzeichnisses gespeichert würden. Für diese Fälle stellt AD/ADM einen Speicherort zur Verfügung und erfüllt damit genau die Anforderungen, die eine Anwendung an die Speicherung von Informationen stellt.

Anwendungsverzeichnisse entwickeln sich im Laufe der Zeit – die Anforderungen des Geschäftsbetriebes ändern sich fortwährend und führen zu Änderungen im Verzeichnisschema oder der Verzeichniskonfiguration. Der Anwendungsmodus des Active Directorys wird im Gegensatz zu

Diensten des Betriebssystems als unabhängiger Dienst ausgeführt. Hierdurch können Sie lokale oder bestimmte Instanzen von AD/AM verändern, ohne eine Änderung an der unternehmensweiten Verzeichnisinfrastruktur zu erzwingen.

AD/AM kann einfach auf einem Entwicklerarbeitsplatz installiert und wieder deinstalliert werden. Dies ermöglicht es im Entwicklungsprozess einer Anwendung, sehr schnell auf einen bereinigten Zustand zurückzukehren.

Darüber hinaus können Sie, wie es im kommenden Abschnitt beschrieben wird, AD/AM effektiv in den folgenden Szenarien einsetzen:

- Anwendungsspezifische Verzeichnisszenarien
- Anwendungsentwicklerszenarien
- Szenarien, bei denen es um die Verwaltung von Extranetzugriffen geht (Extranet Access Management, EAM)
- Migrationsszenarien

Szenarien für den Einsatz von AD/AM

Als ein Infrastrukturverzeichnis kann das Active Directory innerhalb eines Unternehmens ganz unterschiedliche Rollen spielen. Diese reichen von der NOS-Rolle für das Verwalten eines Windows®-Netzwerks bis hin zur Unterstützung von verzeichnisfähigen E-Commerce-Anwendungen. Active Directory muss eingesetzt werden, um Sicherheitsidentitäten unter Windows zu verwalten und um Netzwerke zu verwalten, die aus Windows-basierten Clients, Windows-basierten Servern und sicherheitsintegrierten Anwendungen wie Microsoft Exchange bestehen. Active Directory kann auch für Daten benutzt werden, die zwischen den einzelnen Anwendungen über das Netzwerk hinweg ausgetauscht werden müssen.

Independent Software Vendors (ISVs) und Entwickler von Unternehmensanwendungen sehen sich beim Einsatz von verzeichnisfähigen Anwendungen dann einer Vielzahl von Herausforderungen ausgesetzt, wenn kein Verzeichnisdienst genutzt wird oder aber die Unternehmen bereits ein vollständiges Verzeichnis im Einsatz haben. Hier eine Reihe typischer Aufgaben:

- Entwickler von verzeichnisfähigen Anwendungen sehen sich bisweilen der Herausforderung ausgesetzt, ihr Produkt in ein bestehendes NOS-Verzeichnis zu integrieren, was intensive Planung und viel Zeit bei der Implementierung erfordert.
- Unternehmen, die einen unternehmensweiten Verzeichnisdienst einsetzen, benötigen Flexibilität zwischen den einzelnen Abteilungen, wenn die Geschäftziele oder Geschäftsstrategien voneinander abweichen. Änderungen wie z. B. die Erweiterungen im Schema führen zu Brüchen und haben Auswirkungen auf den unternehmensweiten Einsatz des Verzeichnisses.
- ISVs sind nicht in der Lage, verzeichnisfähige Anwendungen in Unternehmen, die kein Verzeichnisdienst nutzen, einzuführen. Sie müssen entweder abwarten, bis ein Verzeichnisdienst eingerichtet wird, oder riskieren es, den Auftrag an ein Konkurrenzunternehmen zu verlieren, das einen anderen Ort für das Speichern der Informationen nutzt.
- Entwickler wünschen sich ein einfaches Verzeichnis, das sie einfach programmieren können, ohne eine umständliche Installation durchführen zu müssen oder aufwändigen Hardwaresupport während der Entwicklung der Anwendung leisten zu müssen.

Die nachfolgend aufgeführten Szenarien illustrieren die Lösungen, die AD/AM einsetzen, um sich diesen Herausforderungen zu stellen.

Anwendungspezifische Verzeichnisszenarien

Stellen Sie sich ein Szenario vor, bei dem eine Portalanwendung persönliche Daten benötigt, die mit Benutzern zusammenhängen, welche durch das Active Directory des Netzwerkbetriebssystems authentifiziert wurden. Das Speichern von persönlichen Daten innerhalb des NOS-Verzeichnises würde eine Erweiterung der Benutzerklasse des Schemas erfordern. Durch den Einsatz von AD/AM kann die Anwendung das Active Directory dafür nutzen, den Benutzer zu authentifizieren und Dienste zu veröffentlichen, und kann im AD/AM die persönlichen Daten ablegen. Abbildung 1 zeigt die Architektur dieser Lösung:

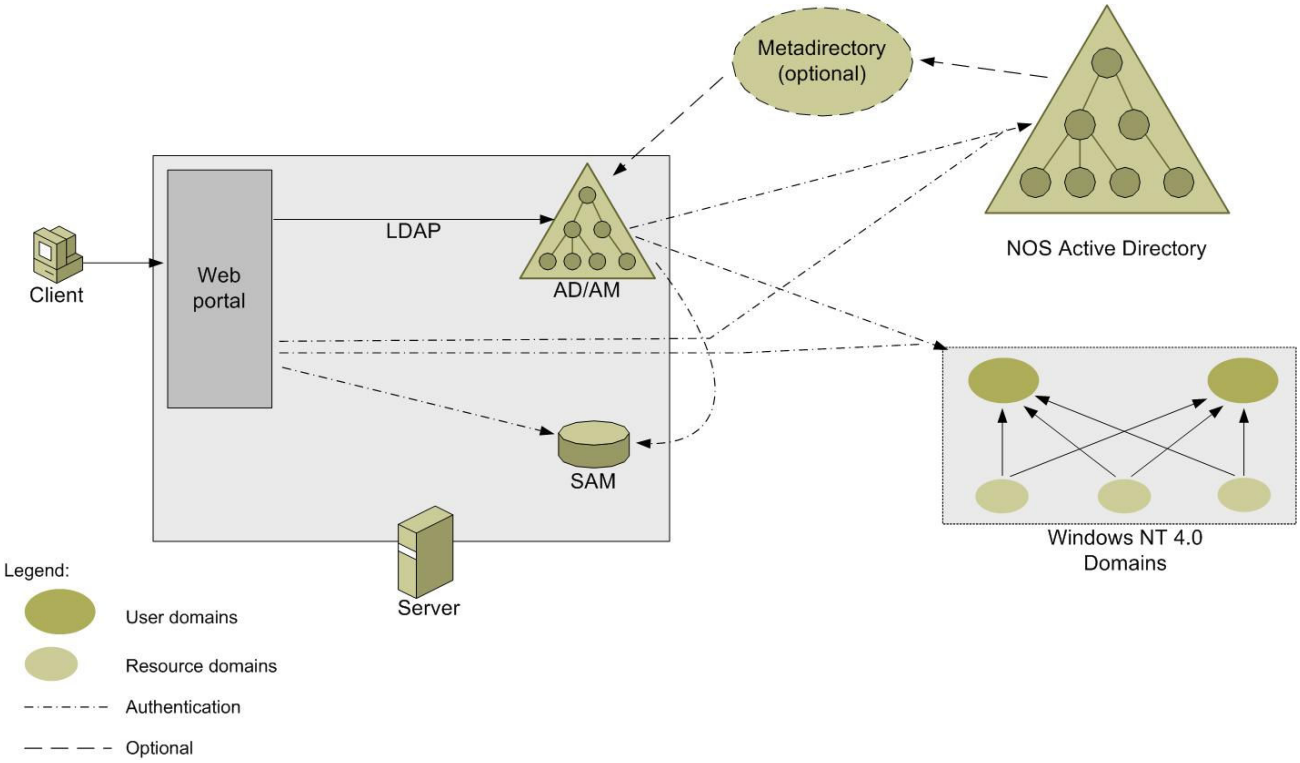

Abbildung 1: Anwendungsspezifische Lösung

AD/AM erlaubt es einer Anwendung, eigene Verzeichnisinformationen, die nur für diese Anwendung relevant sind, in einem lokalen Verzeichnisdienst, z. B. auf dem gleichen Server wie die Anwendung, zu speichern, ohne dass eine zusätzliche Konfiguration des NOS-Verzeichnisses erforderlich wäre. Die benutzerbezogenen Daten, welche nur für die Portalanwendung wichtig sind und nicht umfassend repliziert werden müssen, werden nun nur im AD/AM-Verzeichnis, das mit der Anwendung verbunden ist, gespeichert. Diese Lösung vermindert den Replikationsverkehr auf dem Netzwerk zwischen den einzelnen Domänencontrollern.

Die Anwendungen können natürlich auch weiterhin ihre Daten im Active Directory oder aber in AD/AM ablegen. Wenn die Daten für alle Benutzer aus dem NOS-Verzeichnis interessant sind, können diese auch im Active Directory der Domäne gespeichert werden und über den globalen Katalog bereit gestellt werden. Wenn Sie aber Daten wie z. B. Richtlinien ablegen möchten, die nur für die einzelne Anwendung genutzt werden, können Sie diese im AD/AM ablegen und die Principals des Active Directorys für die Authentifizierung und Zugriffskontrolle auf Objekte des AD/AM nutzen. Dies verhindert, dass für jedes AD/AM-Verzeichnis eine eigene Benutzerdatenbank benötigt wird. Damit wird das Wuchern von Benutzer-IDs und Passworten, das sonst bei jedem Einsatz einer neuen, verzeichnisfähigen Anwendung auf dem Netzwerk entstehen würde, eingedämmt.

Zugeschnittenes Schema

Geschäftsdaten sind oft auf ein bestimmtes Unternehmen oder eine Abteilung zugeschnitten. Wenn ein Unternehmen eine verzeichnisfähige Anwendung einsetzt, die auf einer bestimmten Geschäftslogik oder einem bestimmten Geschäftsschema aufbaut, kann AD/AM diese Rolle ausfüllen. So könnte ein Anwendungsentwickler z. B. Daten über LDAP zur Verfügung stellen, die allerdings nur von den Clients der Anwendung benötigt werden und auch speziell auf diese Anwendung abgestimmt sind. Die Anwendung erfordert ein Schema, das von dem bestehenden Schema des NOS-Verzeichnisses abweicht. Ohne die Konfiguration des NOS-Verzeichnisses ändern zu müssen, kann der ISV eine AD/AM-basierte Anwendung zur Verfügung stellen, die genau an die Anforderungen des Geschäftsvorganges, der Daten und des Arbeitsablaufs angepasst ist. Diese Möglichkeit erlaubt es, den Workflow und damit zusammenhängende Daten, auf die einfachste Weise in einem Anwendungsverzeichnis zu speichern, und erlaubt gleichzeitig Unabhängigkeit von der Struktur des NOS-Verzeichnisses.

Zusätzlich können Schemakonflikte auftreten, wenn mehrere Lösungen vorhanden sind, die verzeichnisbasiert sind. AD/AM vermeidet Konflikte durch die Isolation der einzelnen Instanzen.

Lokale Verwaltung innerhalb eines Unternehmens

Innerhalb jedes Unternehmens betreiben einzelne Abteilungen Anwendungen, die für die Arbeit der Abteilung notwendig sind. Da diese Anwendungen abteilungsspezifisch sind, kann es sein, dass die Informationen, die für diese Anwendungen gespeichert werden, für den Rest des Unternehmens nicht relevant sind. Die Abteilung könnte ihren eigenen lokalen Verzeichnisdienst verwalten, da die Ansprüche an die entsprechenden Dienste – wie z. B. Replikation – von den Anforderungen, die an das Verzeichnis des Unternehmens gestellt werden, abweichen. Der Anwendungsmodus des Active Directory ist eine Verzeichnislösung die schnell und einfach lokal in einem solchen Szenario eingesetzt werden kann.

Optional – zentralisierte Verwaltung

Sie können die Instanz von AD/AM auf einem lokal verwalteten Abteilungsserver oder auf einem zentral verwalteten Server ausführen. Im zweiten Fall können Sie die Verwaltung an die zentrale IT-Abteilung delegieren. Der zentral verwaltete Server kann viele unterschiedliche, unabhängig voneinander konfigurierte Instanzen von AD/AM auf dem gleichen Computer ausführen. Hiermit wird eine größere Effizienz durch die Konsolidierung der Serverumgebung und vereinfachte Verwaltung erzielt. Die unterschiedlichen Instanzen von AD/AM können von verschiedenen verzeichnisfähigen Anwendungen genutzt werden. Diese AD/AM-Instanzen können ihre Daten auch an andere Replikate replizieren, unabhängig von den anderen Instanzen. Hierdurch werden die Daten dort verfügbar, wo sie benötigt werden.

Microsoft Windows NT 4.0-Domänen

Verzeichnisfähige Anwendungen, die AD/AM einsetzen, können auch in Windows NT® 4.0-Domänen eingesetzt werden. Sie können AD/AM auf einem Windows-Server installieren, der als Mitgliedsserver in einer Windows NT 4.0-Domäne betrieben wird und für diese Anwendung als AD/AM eingesetzt wird. Da AD/AM mit der Windows-integrierten Sicherheit arbeitet, kann AD/AM auch Benutzer aus Windows NT 4.0-Domänen authentifizieren.

Szenario für Anwendungsentwickler

AD/AM ist das perfekte Tool für Entwickler, die eine Anwendung für das Active Directory entwickeln, da AD/AM das gleiche Programmmodell verwendet und die gleiche Administratorerfahrung vermittelt wie Active Directory. Der Vorteil besteht darin, dass ein Entwickler mit lokalen Instanzen von AD/AM auf einem Entwicklungsrechner arbeiten kann und dann die Anwendung zu einem späteren Zeitpunkt auf Active Directory übertragen kann.

Einfache Installation und Einrichtung

Die Installation von AD/AM besteht aus einem einfachen Installationsassistenten, der nur wenige Eingaben benötigt. Die Installation kann auch einfach geskriptet werden, was für eine unbeaufsichtigte Installation oder eine Silent-Installation einer Anwendung genutzt werden kann. Damit kann der Entwickler einzelne Instanzen von AD/AM installieren, deinstallieren oder auch mehrere Instanzen während der Entwicklung seiner Anwendung nutzen. Ein Entwickler kann durch die Verwendung mehrerer Instanzen unterschiedliche Konfigurationen austesten und einfach zwischen diesen Instanzen hin- und herwechseln, ohne das Verzeichnis neu installieren zu müssen. Es wird auch kein Neustart notwendig, weder während der Installation noch bei der Konfiguration.

Lokal installiert, lokal verwaltet

Stellen Sie sich ein Szenario vor, bei welchem ein Anwendungsentwickler eine verzeichnisfähige Anwendung entwickelt. Bestehende Regeln erfordern, dass das Verzeichnis auf einem Server oder einem Domänencontroller installiert sein muss. Dies kann zu Komplikationen innerhalb eines Unternehmens führen, da das Unternehmen einen Server für die Entwicklung bereitstellen und verwalten muss. Darüber hinaus kann das Installieren oder Deinstallieren des Verzeichnisses auch Auswirkungen auf andere Benutzer haben. AD/AM dagegen muss nicht auf einem Server oder Domänencontroller installiert sein und kann auch effektiv auf Clientrechnern ausgeführt werden. So können Sie eine verzeichnisfähige Anwendung ausführen, ohne auf Personen der IT-Abteilung zurückgreifen zu müssen. Sie können AD/AM unter Microsoft Windows XP oder Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition oder Microsoft Windows Server 2003 Datacenter Edition ausführen.

Szenario mit Verwaltung von Extranetzugriffen

Stellen Sie sich ein Szenario vor, in welchem eine Webportalanwendung mit der Verwaltung von Extranetzugriffen umgehen muss. Lösungen wie OpenNetwork's DirectorySmart oder Netegrity's SiteMinder sind dafür exzellente Beispiele. Das Webportal speichert die Anmeldeinformationen innerhalb des Verzeichnisses und benutzt das Verzeichnis nur für die Authentifizierung.

Abbildung 2 zeigt dieses Extranetszenario.

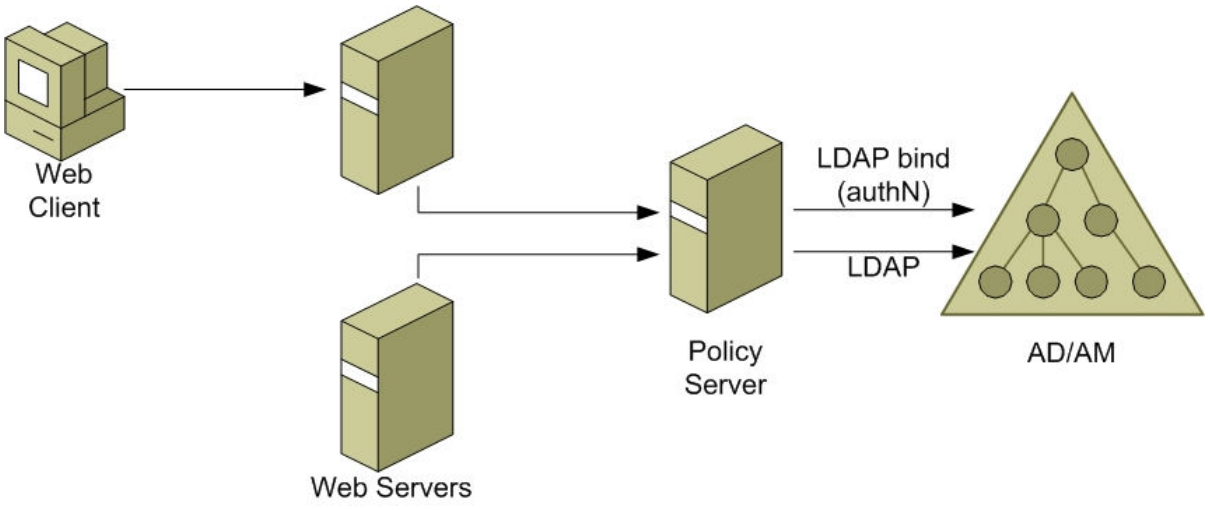

Abbildung 2: Verwaltung von Extranetzugriffen

In solchen Fällen ist AD/AM die optimale Lösung. Da AD/AM auch Benutzerobjekte aufnehmen kann, die keine Windows-Sicherheitsprincipals sind, aber über einfache LDAP-Binds authentifiziert werden können, können alle Benutzerinformationen sowie die für die Berechtigungen notwendigen Daten für diese Anwendungen innerhalb von AD/AM abgelegt werden. Diese Konfiguration kann auch sehr gut in heterogenen Umgebungen eingesetzt werden und selbst dann genutzt werden, wenn Active Directory nicht als Infrastrukturanbieter für das Netzwerkbetriebssystem eingesetzt wird. Webclients

werden durch die Portalanwendung bedient, welche auf einer beliebigen Plattform ausgeführt wird und das AD/AM als einfachen LDAP-Speicher nutzt.

Migrationsszenarien

Stellen Sie sich ein Szenario vor, in welchem ein Unternehmen bereits ein Verzeichnis einsetzt, das nach Art eines X.500-Verzeichnisses die Namen “O=<Unternehmen>, C=<Land>” verwendet und das dieses Verzeichnis für bestehende Anwendungen einsetzt. Abbildung 3 zeigt die Migrationsmöglichkeiten auf Active Directory. Hierbei wird AD/AM als eine Zwischenlösung eingesetzt.

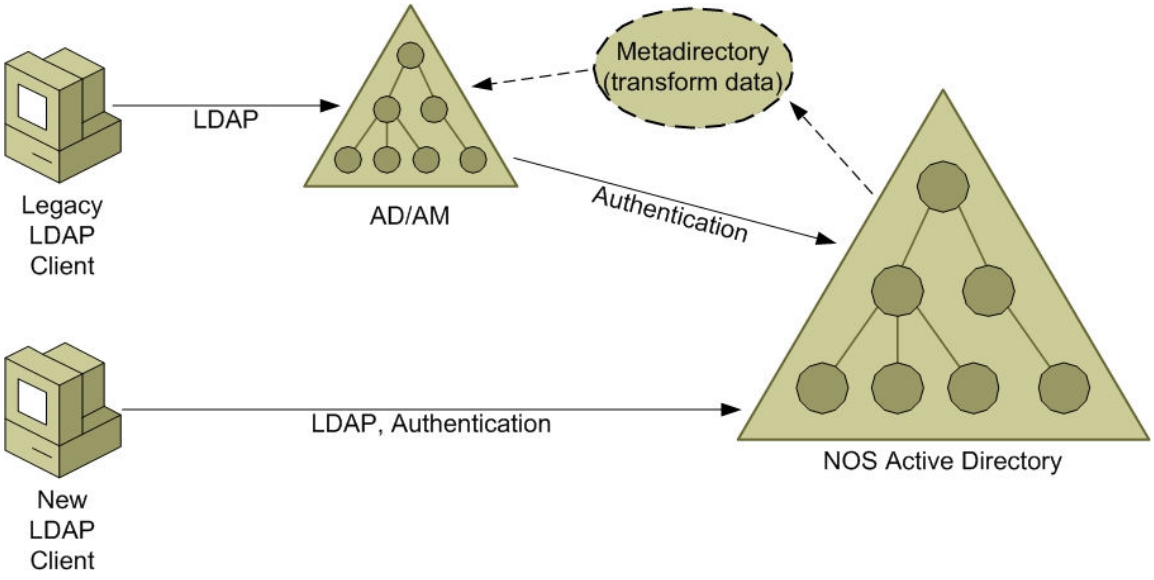

Abbildung 3: Migration zu Active Directory

In Fällen, in welchen eine Migration auf Active Directory vorgenommen wird, kann AD/AM eingesetzt werden, um Anwendungen zu bedienen, die auf Verzeichnisse mit X.500-Benennung beruhen. Sie können dann Active Directory als das Verzeichnis für das Netzwerkbetriebssystem einsetzen, das eine gemeinsame Sicherheitsinfrastruktur im Netzwerk zur Verfügung stellt, und AD/AM dazu nutzen, alten Anwendungen das notwendige Verzeichnis zur Verfügung zu stellen.

Wenn Sie Anwendungen auf das Active Directory umstellen, können Sie diese auf das NOS-Active Directory ausrichten. Sie können auch ein Metadirectory wie z. B. die Microsoft Metadirectory-Dienste einsetzen, um die Daten im Active Directory und AD/AM automatisch zu synchronisieren. Dies ermöglicht eine reibungslose Umstellung.

Vorteile für die Benutzer

AD/AM stellt eine erweiterte Möglichkeit des Active Directorys dar, das es erlaubt, das Active Directory als einen Lightweight-Verzeichnisdienst zu nutzen. Damit kann für Anwendungen schnell und flexibel ein Verzeichnisdienst zur Verfügung gestellt werden.

Reichhaltiger und erweiterbarer Speicher

AD/AM unterstützt ein flexibles und erweiterbares Schema, das es Ihnen ermöglicht, dieses einfach mit den bekannten Windows-basierten Tools wie z. B. LDIFDE, dem Active Dircectory Snap-In oder aber ADSIEdit, anzupassen. Jede Instanz von AD/AM, die auf einem Computer ausgeführt wird, kann dabei ein unterschiedliches Schema besitzen.

Eine einzelne Instanz von AD/AM kann mehrere Datenpartitionen beherbergen. Dies erlaubt es Ihnen, die einzelnen Speicher, die Verteilung und auch den Replikationsrahmen für die Partitionsdaten

festzulegen. Der Speicher verfügt über einen flexiblen Namensraum, der den Einsatz sowohl von Namen im DNS-Stil als auch von X.500-Distinguished-Namen erlaubt.

Hieraus ergibt sich ein deutlich schnellerer Einsatz eines Verzeichnisses, der auch gleichzeitig deutlich weniger Planung für das damit zusammenhängende Schema oder die Namenskonventionen benötigt.

Replikation

AD/AM benutzt die gleiche Multi-Master-Replikation, die auch von Active Directory genutzt wird. Diese stellt sicher, dass jede Instanz, die an einem Replikationsset beteiligt ist, Daten verändern kann und somit das Ändern von Daten nicht auf die primäre Replikationsquelle beschränkt bleibt. AD/AM-Replikation nutzt das gleiche Standortmodell, das auch von Active Directory genutzt wird. Damit stehen auch die Funktionen wie zeitgesteuerte, komprimierte Intersite-Replikation zur Verfügung. Sie können diese mit den bekannten Tools wie *Repadmin.exe* verwalten.

Unter Active Directory wird die Replikation von Anwendungsdaten mit der Replikation von NOS-Daten verbunden. Administratoren von unternehmensweiten Verzeichnissen legen normalerweise die Replikationszyklen für das NOS-Verzeichnis fest, so dass diese am besten für alle Anwendungen geeignet sind. Durch die Verwendung von AD/AM können die Zeiten für die Replikation so festgelegt werden, dass diese optimal auf die einzelnen Anwendungen abgestimmt sind.

Zusätzlich können Sie auch die Anwendungsdaten zwischen verschiedenen AD/AM-Instanzen replizieren. Sie können Instanzen von AD/AM auf Servern, die Mitgliedsserver einer Active-Directory-Domäne sind, Mitglieder von unterschiedlichen Active Directory-Gesamtstrukturen sind oder aber auf Arbeitsstationen, die Mitglieder einer Arbeitsgruppe sind, ausführen.

Einrichtung und Entfernen

AD/AM nutzt den vertrauten Windows-basierten Installer. Es sind nur wenige Eingaben erforderlich und die Installation kann außerdem geskriptet werden. Dies ist von Vorteil, wenn unbeaufsichtigte oder aber Silent-Installationen als Teil einer Anwendungsinstallation ausgeführt werden sollen. Der Installationsassistent erlaubt es Ihnen auch, eine neue Instanz oder ein Replikat einer bestehenden Instanz anzulegen.

Der Assistent zur Deinstallation entfernt:

- Von Ihnen ausgewählte Instanzen.
- Alle Dateien, die Konfigurationsdaten enthalten.
- Die mit den Instanzen verbundenen Partitionen.

Die einfache Installation, Einrichtung und Entfernung spart Administratoren Zeit und macht es relativ einfach, eine Testinstallation von AD/AM zu entfernen.

Unterstützung von mehreren Instanzen

Mehrere Instanzen von AD/AM können gleichzeitig auf einem einzigen Server ausgeführt werden, wobei jede Instanz unabhängig von anderen Instanzen konfiguriert werden kann und isoliert von anderen Instanzen ist, die auf der gleichen Maschine ausgeführt werden. Jede Instanz von AD/AM wird durch einen eindeutigen Namen und Port gekennzeichnet und verfügt über getrennt installierte Binärdateien.

Die Nutzung von mehreren Instanzen von AD/AM bietet wichtige Vorteile für Unternehmen. Darunter fallen z. B. die Konsolidierung von Serverstrukturen, die Entwicklung von Line-Of-Business (LOB)-Anwendungen und die Möglichkeit, Unternehmensanwendungen inkrementell zu aktualisieren. In kleineren Unternehmen wird durch den Einsatz von mehreren Instanzen die Möglichkeit geschaffen, einzelne Instanzen für die spezifischen Anforderungen einzelner Anwendungen zu konfigurieren, und es können unterschiedliche Datenspeicher auf dem gleichen Computer abgefragt werden.

Sicherung und Wiederherstellung

AD/AM ist auch in die durch das Windows-Betriebssystem bereitgestellten Sicherungs- und Wiederherstellungsmöglichkeiten integriert. Jede Instanz wird durch einen konfigurierbaren, automatisierten Onlineprozess gesichert, der auch den unmittelbaren Zugriff auf kritische Daten erlaubt. AD/AM ermöglicht ein Online-Backup und Offline-Restore unter Verwendung der NTBackup-Utility.

Unterstützung von Tools

Da es sich bei AD/AM um einen Modus des Active Directorys handelt, kann der Administrator auch ähnlich damit umgehen. Auch die Tools sind vergleichbar:

- LDP (LDP.EXE) erlaubt LDAP-Operationen, die gegen AD/AM ausgeführt werden, und ist Bestandteil der Supporttools der Windows 2000- und der Windows Server 2003-Familie. LDP setzt eine grafische Benutzerschnittstelle ein.
- ADSIEdit ist ein bekanntes Tool, das benutzt wird, um alle Objekte innerhalb des Verzeichnisses anzuzeigen (auch die Schema- und die Konfigurationsinformationen), Objekte zu verändern und um Zugriffsberechtigungen für Objekte zu setzen. Es ist Bestandteil der Windows Support Tools und ist ein Snap-In für die Microsoft Management Console (MMC).
- Andere vertraute Tools wie PerfMon können benutzt werden, um die Netzwerk- und Systemperformance unter AD/AM zu analysieren. Sie können Informationen über die einzelnen Instanzen von AD/AM in einzelnen Leistungsindikatoren und Trace-Logs sammeln und entsprechend angepasste Ansichten in der Microsoft Management Console darstellen.
- Tools wie NTDSUtil können genutzt werden, um die Datenbank zu warten, Singel-Master-Operationen zu kontrollieren und zu verwalten, unerwünschte Metadaten zu entfernen und Verzeichnispartitionen anzulegen.

Durch die Verwendung der gleichen Tools für AD/AM wie für das Active Directory können Kosten, die sonst für Schulung aufgewendet werden müssten, eingespart werden.

Sicherheit

AD/AM erhöht das Sicherheitsmodel des Windows-Betriebssystems. Sie können Zugriffe auf Objekte innerhalb von AD/AM und der Dienste unter Verwendung der folgender Mittel kontrollieren:

- Benutzer aus dem Netzwerkverzeichnisdienst
- Einer Windows NT 4.0 Domänenstruktur
- Konten auf dem lokalen Computer

AD/AM unterstützt LDAP-Authentifizierung unter Verwendung von Anmeldeinformationen einer externen verteilten Sicherheitsinfrastruktur, so eine entsprechende Infrastruktur vorhanden ist. Sicherheitsprincipals können von der lokalen Plattform oder vom Netzwerkverzeichnisdienst genutzt werden. Sie können auch Benutzerkonten innerhalb von AD/AM anlegen. Dies erlaubt es Anwendungen, sich auf dieses Verzeichnis für den Umgang mit Authentifizierungen zu verlassen, während die Anwendungen sich dann um die Berechtigungen kümmern. In diesen Fällen bietet AD/AM Authentifizierung auf der Grundlage des LDAP Simple Bind-Mechanismus.

Berechtigungen für den Zugriff auf die Objekte des Verzeichnisses beruhen auf Access Control Lists (ACLs), wie sie unter Windows üblich sind. Dieser Mechanismus für die Kontrolle von Zugriffen erlaubt es Ihnen, detailliert den Zugriff auf jedes einzelne Objekt in jeder Instanz festzulegen. Er basiert auf Sicherheitsdeskriptoren für Sicherheitsprincipals, die bereits innerhalb der Windows-Infrastruktur vorhanden sind. Anwendungen können diese für Ihr eigenes Berechtigungsframework erweitern und dabei den Verzeichnisdienst für die Authentifizierung nutzen.

Unterstützte Plattformen

AD/AM kann auf den folgenden Plattformen ausgeführt werden:

- Windows Server 2003 Standard Edition
- Windows Server 2003 Enterprise Edition
- Windows Server 2003 Datacenter Edition
- Windows XP Professional

Zusammenfassung

Firmen, Independent Software Vendors (ISVs) und Entwickler, die ihre Anwendungen in einen Verzeichnisdienst integrieren möchten, haben nun unter Active Directory Möglichkeiten, die ihnen die folgenden Vorteile bieten:

- **Einfacher Einsatz -** Entwickler, Endnutzer und ISVs können AD/AM einfach als einen Lightweight-Verzeichnisdienst auf fast allen Windows Server 2003-Betriebssystemen und Windows XP Professional einsetzen. Er ist einfach zu installieren und wieder zu entfernen und macht ihn damit zu dem geeigneten Verzeichnisdienst für Anwendungen.
- **Reduzierte Kosten für die Infrastruktur** – Durch den Einsatz einer einheitlichen Technologie sowohl für das Netzwerkverzeichnis als auch für das Anwendungsverzeichnis, können die Kosten für die gesamte Infrastruktur gesenkt werden. Zusätzliche Investitionen für Training, Verwaltung oder Administration des Awendungsverzeichnisses fallen nicht an. Auch die Application Programming Interfaces (LDAP, ADSI, DSML) sind gleich, so dass Sie Anwendungen auf AD/AM entwickeln und danach auf das firmenweite Netzwerkverzeichnis übertragen können. Dabei werden nur geringfügige Anpassungen notwendig.
- **Erhöhte Sicherheit** – Die Integration in das Windows-Sicherheitsmodell erlaubt es jeder Anwendung, die AD/AM einsetzt, eine Authentifizierung gegenüber dem firmenweit eingesetzten Active Directory durchzuführen.
- **Erhöhte Flexibilität** – Der Besitzer einer Anwendung kann damit auf einfache Weise verzeichnisfähige Anwendungen zur Verfügung stellen, ohne das firmenweite Verzeichnisschema zu verändern. Dabei werden aber einzelne Informationen weiterhin aus dem Netzwerkverzeichnis genutzt.
- **Zuverlässigkeit und Skalierbarkeit** – Anwendungen, die AD/AM nutzen, verfügen über die gleiche Zuverlässigkeit, Skalierbarkeit und Leistung, über die sie auch verfügen würden, wenn Sie direkt im Active Directory des Netzwerks ausgeführt würden.

Zum ersten Mal sind Sie damit in der Lage, eine einheitliche Verzeichnistechnologie in unterschiedlichen Rollen auszuführen und gleichzeitig Investitionen zu sichern, die Sie in die Ausbildung Ihrer Administratoren, Operationen, Lizenzierung und Sicherheit getätigt haben. Firmen, ISVs und Entwickler können Active Directory damit in unterschiedlichen Rollen einsetzen, ohne sich den erhöhten Kosten, die sich durch den Einsatz von unterschiedlichen Technologien für Netzwerk- und Anwendungsverzeichnisse ergeben, auszusetzen.

Weiterführende Links

Die neuesten Informationen über Windows Server 2003 finden Sie auf der Windows Server 2003-Website unter http://www.microsoft.com/windows.netserver.