KAPITEL 14

Active Directory Lightweight Directory Services

Von den fünf Active Directory-Technologien unter Windows Server 2008 R2 ist die Active Directory Lightweight Directory Services (AD LDS) die Technologie, die den Active Directory-Domänendiensten (Active Directory Domain Services, AD DS) am stärksten ähnelt. Der Grund ist, dass die AD LDS im Wesentlichen nur als eine Untermenge des AD DS-Funktionsumfangs bieten. Beide arbeiten mit demselben Kerncode und bieten einen sehr ähnlichen Funktionsumfang.

Die AD LDS, früher Active Directory Application Mode (ADAM) genannt, sind eine Technologie zur Unterstützung verzeichnisfähiger Anwendungen auf Anwendungsbasis. Sie erfordern keine Änderung am Datenbankschema des Verzeichnisses des Netzwerkbetriebssystems, das unter den AD DS ausgeführt wird. Die AD LDS eignen sich besonders für Administratoren, die mit verzeichnisfähigen Anwendungen arbeiten möchten, ohne sie in das Verzeichnis ihres Netzwerkbetriebssystems zu integrieren.

Die Active Directory-Domänendienste unterstützen ebenfalls verzeichnisfähige Anwendungen. Ein sehr gutes Beispiel ist Microsoft Exchange Server 2007. Alle Benutzerinformationen in Exchange Server werden vom Verzeichnis bereitgestellt. Wenn Sie Exchange Server in Ihrem Netzwerk installieren, wird erst einmal das AD DS-Schema erweitert, dessen Größe sich praktisch verdoppelt. Wie Sie wissen, dürfen Schemaänderungen nicht auf die leichte Schulter genommen werden, da ein Objekt oder Attribut, das Sie einmal zum AD DS-Schema hinzugefügt haben, nicht mehr entfernt werden kann. Sie können solche Objekte deaktivieren oder umbenennen und weiterverwenden, doch wer möchte schon nicht mehr benötigte Objekte im Verzeichnis seines Netzwerkbetriebssystems? Das Erweitern des Schemas für eine Anwendung wie Exchange Server ist dagegen sinnvoll, weil sie einen wichtigen Netzwerkdienst bereitstellt: E-Mail.

Weitere Informationen **Empfohlene Vorgehensweisen für den Active Directory-Entwurf**

Informationen zu den empfohlenen Vorgehensweisen beim Entwurf von Active Directory sowie Richtlinien zur AD DS-Schemaverwaltung erhalten Sie in Kapitel 3, »Designing the Active Directory«, des Handbuchs *Windows Server 2003, Best Practices for Enterprise Deployments*, das Sie kostenlos von *http://www.reso-net.com/Documents/007222343X_Ch03.pdf* herunterladen können.

Informationen zum Erstellen einer neuen Gesamtstruktur sowie zum Migrieren des Inhalts einer Gesamtstruktur in eine andere finden Sie in *Windows Server 2008: The Complete Reference* von Danielle und Nelson Ruest (McGraw-Hill Osborne, 2008). In diesem Buch wird der Aufbau einer vollständigen auf Microsoft Windows Server basierenden Infrastruktur und das Migrieren ihres Inhalts beschrieben.

Doch was andere Anwendungen betrifft, insbesondere Anwendungen anderer Softwarehersteller, sollten Sie sorgfältig prüfen, ob sie in Ihr AD DS-Verzeichnis integriert werden sollten. Bedenken Sie stets, dass Sie sehr lange mit Ihrer AD DS-Produktivstruktur arbeiten werden. Wenig wünschenswert ist es, dass Sie ein Produkt in Ihr Verzeichnis integrieren, um Jahre später, nachdem der Softwarehersteller nicht mehr auf dem Markt aktiv ist, überlegen zu müssen, was Sie mit den zu Ihrer AD DS-Struktur hinzugefügten Erweiterungen dieses Produkts anfangen sollen, die die Replikationszeiten verlängern und das Verzeichnis durch ungenutzte Inhalte aufblähen.

Aus diesem Grund sind die AD LDS ein wahrer Segen. Da mehrere AD LDS-Instanzen auf demselben Server unterstützt werden können (im Gegensatz zu den AD DS, die nur eine Instanz eines Verzeichnisses auf einem beliebigen Server unterstützen), können die AD LDS die Anforderungen verzeichnisfähiger Anwendungen erfüllen und sogar Instanzen auf Anwendungsbasis bereitstellen. Darüber hinaus benötigen Sie zum Arbeiten mit den AD LDS nicht wie bei den AD DS die Berechtigungen eines Organisations- oder Schemaadministrators. Die AD LDS können auf Mitglieds- oder eigenständigen Servern ausgeführt werden, und für ihre Verwaltung sind nur lokale Administratorrechte erforderlich. Aus diesem Grund können sie in einem Umkreisnetzwerk eingesetzt werden, um Anwendungs- oder Webauthentifizierungsdienste bereitzustellen. Die AD LDS sind eine der vier Active Directory-Technologien, mit denen Sie den Einflussbereich Ihres Unternehmens über die Firewall hinaus auf das Internet ausdehnen können (Abbildung 14.1).

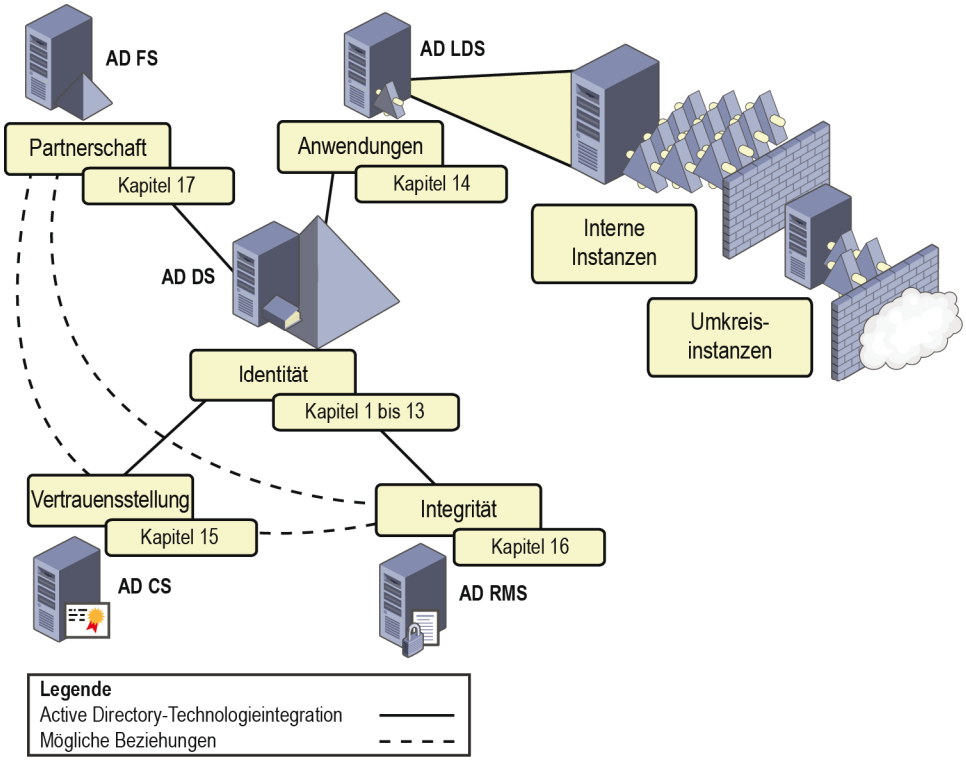

Abbildung 14.1 Die AD LDS können zur Unterstützung von Anwendungen intern und extern eingesetzt werden

In diesem Kapitel abgedeckte Prüfungsziele:

- Konfigurieren von AD LDS (Active Directory Lightweight Directory Services)

Lektionen in diesem Kapitel:

Bevor Sie beginnen

Damit Sie die Lektionen in diesem Kapitel durcharbeiten können, müssen Sie Windows Server 2008 R2 auf folgenden Computern installiert haben:

- Einem physischen oder virtuellen Computer, der den Namen *SERVER01* trägt und als Domänencontroller in der Domäne *contoso.com* konfiguriert ist. Einzelheiten zu dieser Bereitstellung finden Sie in Kapitel 1, »Erstellen einer Active Directory-Domäne«. Verwenden Sie die dort angegebenen Einstellungen für die IP-Adressen.
- Einem weiteren physischen oder virtuellen Computer. Der Computer muss den Namen *SERVER03* tragen und Mitgliedsserver der Domäne *contoso.com* sein. Dieser Computer dient als Host der AD LDS-Instanzen, die Sie in den Übungen in diesem Kapitel installieren und erstellen. Stellen Sie sicher, dass dieser Computer auch über ein Laufwerk *D:* zum Speichern der Daten der AD LDS-Instanzen verfügt. Für dieses Laufwerk wird eine Größe von 10 GByte empfohlen. Konfigurieren Sie dieses Laufwerk in der Datenträgerverwaltung des Server-Managers.
- Einem dritten physischen oder virtuellen Computer. Der Computer sollte den Namen *SERVER04* tragen und Mitgliedsserver der Domäne *contoso.com* sein. Dieser Computer dient zum Konfigurieren von Replikationsbereichen für die AD LDS. Stellen Sie sicher, dass dieser Computer auch über ein Laufwerk *D:* zum Speichern der Daten der AD LDS-Instanzen verfügt. Für dieses Laufwerk wird eine Größe von 10 GByte empfohlen.

Praxistipp

Danielle und Nelson Ruest

Ende 2003 wurden wir vom Redmond Magazine (vormals MCP Magazine) gebeten, eine Übersicht der verschiedenen Produkte auf dem Markt zusammenzustellen, die Systemadministratoren bei der Verwaltung von Active Directory-Umgebungen unterstützen. Wir waren von der Aufgabe angetan, da Active Directory eine unserer Lieblingstechnologien ist. Active Directory ist nicht nur ein echter LDAP-Verzeichnisdienst (Lightweight Directory Access Protocol), sondern auch ein sehr leistungsfähiges Verzeichnis des Netzwerkbetriebssystems, das Millionen von Objekten verwalten kann. Außerdem unterstützt Active Directory mit Gruppenrichtlinien eine überaus leistungsstarke Objektverwaltungsplattform, die die Funktionen des Verzeichnisdienstes des Netzwerkbetriebssystems erweitert. Schließlich kann mittels der über Gruppenrichtlinien gesteuerten Softwareübermittlung die Bereitstellung von Windows Installer-basierten Softwarepaketen in der gesamten Verzeichnisstruktur verwaltet werden. Für uns gibt es keinen Zweifel, dass Active Directory eines der besten Produkte ist, die jemals die Entwicklungszentren in Redmond verlassen haben.

Nachdem wir im Internet recherchiert und unsere Kunden befragt haben, kamen wir auf sechs Produkte:

- Quest FastLane Active Roles
- Aelita Enterprise Directory Manager
- NetIQ Security Administration Suite
- Javelina ADvantage
- NetPro Active Directory Lifecycle Suite
- Bindview Secure Active Directory LifeCycle Suite

Von den sechs Produkten standen uns für den Artikel nur vier zur Verfügung. Bindview weigerte sich, uns eine Testversion ihres Produkts zu überlassen, sodass dieser Anbieter von vornherein gestrichen wurde. Bei NetPro, das dem Anschein nach eine überzeugende Lösung anbietet, verzögerte sich die Markteinführung, weshalb wir auch auf dieses Produkt verzichten mussten. Später hatten wir dennoch eine Chance, über die NetPro-Suite von Active Directory-Produkten zu schreiben (siehe *http://mcpmag.com/reviews/products/article.asp?EditorialsID=454*), wobei die Lösung sehr gut abschnitt. So blieben uns also vier zu untersuchende Produkte. Das Ergebnis war ein Artikel mit dem Titel »The 12 Mighty Labors of Active Directory Management« (siehe *http://mcpmag.com/Features/article.asp?EditorialsID=359*). Der Artikel stieß bei der Leserschaft auf gute Resonanz. Doch wir erhielten aus verschiedenen Quellen auch einige sehr bissige Kommentare zu einem der Hauptpunkte in unserem Artikel.

Zwei der vier untersuchten Produkte, NetIQ Security Administration Suite und Quest FastLane Active Roles, änderten das Datenbankschema von Active Directory. Bis zu diesem Zeitpunkt hatten wir als Berater an verschiedenen Active Directory-Implementierungen mitgewirkt, wobei sich stets die eine Frage stellte, wie Schemaänderungen verwaltet werden sollen. Denn wenn das Schema einmal geändert wurde, kann dieser Schritt nicht rückgängig gemacht werden.

Unter Windows Server 2003 ermöglichte Microsoft die Deaktivierung beziehungsweise Umbenennung und Wiederverwendung von Schemaänderungen, doch für unsere Kunden und für uns war dies nur die dürftige zweite Wahl. Nach Möglichkeit sollte das Schema unangetastet bleiben. Darüber hinaus hatte Microsoft gerade ADAM zur Unterstützung von Unternehmen veröffentlicht, die Anwendungen in einen Verzeichnisdienst integrierten wollten, ohne das Schema des Verzeichnisses ihres Netzwerkbetriebsystems zu ändern.

Schlussendlich kürten wir das Aelita-Produkt aus einem bestimmten Grund zum Testsieger: Aelita hatte sich für die Speicherung all seiner Datenbankanforderungen in Microsoft SQL Server anstatt für die Änderung des Active Directory-Schemas entschieden, aber dennoch war Enterprise Directory Manager genauso leistungsfähig wie die anderen Hauptkonkurrenten.

Zwei Monate nach der Veröffentlichung unseres Artikels wurde Aelita von Quest gekauft und Enterprise Directory Manager (EDM) in die nächste Version von Active Roles transformiert. Das ursprüngliche Active Roles, das von FastLane, einem kleinen Unternehmen aus Ottawa in Kanada, produziert und ebenfalls von Quest gekauft wurde, floss in EDM ein. Die neue Version von Active Roles erforderte nicht mehr die Implementierung von Schemaänderungen, bot aber dennoch verschiedene leistungsstarke Active Directory-Verwaltungsfunktionen. Ob unser Artikel damit etwas zu tun hatte? Wer weiß? Eines ist jedoch sicher: Niemand sollte sich leichtfertig entscheiden, das Schema des Verzeichnisses des Netzwerkbetriebssystems zu ändern, wenn doch leistungsfähige Tools wie ADAM (nun AD LDS) zur Verfügung stehen.

Lektion 1: Grundlagen und Installieren der AD LDS

Obwohl die AD LDS auf demselben Code wie die AD DS basieren, ist die Arbeit mit den AD LDS wesentlich einfacher. Wenn Sie beispielsweise die AD LDS auf einem Server installieren, ändert sich die Konfiguration des Servers nicht so wie bei den AD DS, wenn Sie einen Domänencontroller erstellen. Die AD LDS sind lediglich eine Anwendung und nichts weiter. Bei der Installation müssen Sie den Server nicht neu starten, da die Anwendungsinstallation lediglich weitere Funktionen zum Server hinzufügt, ohne sein Wesen zu ändern.

Doch bevor Sie beginnen, müssen Sie wissen, woraus eine AD LDS-Instanz besteht, wie AD LDS-Instanzen verwendet werden sollen und wie ihr Verhältnis zu AD DS-Verzeichnissen ist oder sein kann. Anschließend können Sie mit der Installation der AD LDS fortfahren.

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

- Beschreiben, wann die AD LDS eingesetzt werden sollten
- Installieren der AD LDS auf einem Mitgliedsserver
- Finden und Anzeigen des AD LDS-Verzeichnisspeichers

Veranschlagte Zeit für diese Lektion: 30 Minuten

Grundlagen der AD LDS

Wie die AD DS basieren AD LDS-Instanzen auf LDAP (Lightweight Directory Access Protocol) und stellen hierarchische Datenbankdienste bereit. Im Gegensatz zu relationalen Datenbanken sind LDAP-Verzeichnisse für bestimmte Zwecke optimiert und sollten zum Einsatz kommen, wenn zur Unterstützung bestimmter Anwendungen eine schnelle Informationssuche erforderlich ist. In Tabelle 14.1 werden die Hauptunterschiede zwischen einem LDAP-Verzeichnis und einer relationalen Datenbank wie Microsoft SQL Server vorgestellt. Anhand dieses Vergleichs können Sie bestimmen, wann Sie sich zur Unterstützung einer Anwendung für ein LDAP-Verzeichnis und nicht für eine relationale Datenbank entscheiden sollten.

Die AD LDS basieren zwar auf den AD DS, bieten aber nicht alle ihre Features. Die Unterschiede zwischen den Features in AD LDS und AD DS sind in Tabelle 14.2 aufgeschlüsselt.

Tabelle 14.1 LDAP-Verzeichnisse und relationale Datenbanken im Vergleich

LDAP-Verzeichnisse	Relationale Datenbanken
Schnelle Lese- und Suchvorgänge.	Schnelle Schreibvorgänge.
Hierarchischer Datenbankentwurf, der häufig auf DNS (Domain Name System) oder dem Benennungssystem X.500 basiert.	Strukturierter Datenentwurf auf Basis von Tabellen mit Zeilen und Spalten. Tabellen können verknüpft werden.
Basiert auf einer standardmäßigen Schemastruktur bei erweiterbarem Schema.	Basiert nicht auf Schemas.
Dezentrale Verteilung und Replikation zur Erhaltung der Datenkonsistenz.	Zentrale Datenspeicher.
Sicherheitseinstellungen werden auf Objektebene angewendet.	Sicherheitseinstellungen werden auf Zeilen- oder Spaltenebene angewendet. ▶

LDAP-Verzeichnisse	Relationale Datenbanken
Da die Datenbank verteilt ist, gibt es keine absolute Datenkonsistenz, zumindest nicht bis die Replikationsdurchgänge abgeschlossen sind.	Da die Dateneingabe transaktionsgesteuert ist, gibt es stets eine absolute Datenkonsistenz.
Datensätze werden nicht gesperrt und können von zwei Benutzern gleichzeitig geändert werden. Konflikte werden mithilfe von USNs (Update Sequence Numbers) gelöst.	Datensätze werden gesperrt und können immer nur von einem Benutzer gleichzeitig bearbeitet werden.

Tabelle 14.2 AD LDS und AD DS im Vergleich

Feature	AD LDS	AD DS
Mehrere Instanzen auf einem Server möglich	☑	☐
Unabhängiges Schema für jede Instanz	☑	☐
Ausführung unter Clientbetriebssystemen wie Windows 7 oder auf Windows Server 2008 R2-Mitgliedsservern	☑	☐
Ausführung auf Domänencontrollern	☑	☑
Verzeichnispartitionen können auf X.500-Benennungskonventionen basieren	☑	☐
Installation oder Entfernen ohne Neustart möglich	☑	☐
Dienst kann ohne Neustart beendet beziehungsweise gestartet werden	☑	☑
Gruppenrichtlinien werden unterstützt	☐	☑
Globaler Katalog	☐	☑
Verwaltung von Objekten wie Arbeitsstationen, Mitgliedsservern und Domänencontrollern	☐	☑
Unterstützung von Vertrauensstellungen zwischen Domänen und Gesamtstrukturen	☐	☑
Unterstützung von und Integration mit Infrastrukturen öffentlicher Schlüssel (Public Key Infrastructures, PKIs) und X.509-Zertifikaten	☐	☑
Unterstützung von SRV-Einträgen des DNS-Dienstes zum Auffinden von Verzeichnisdiensten	☐	☑
Unterstützung von LDAP-APIs (Application Programming Interfaces, Anwendungsprogrammierschnittstellen)	☑	☑
Unterstützung der ADSI-API (Active Directory Services Interface)	☑	☑
Unterstützung der MAPI (Messaging API)	☐	☑
Unterstützung von Sicherheitseinstellungen auf Objektebene und Delegierung der Verwaltung	☑	☑
Multimasterreplikation für die Erhaltung der Datenkonsistenz	☑	☑
Unterstützung von Schemaerweiterungen und Anwendungsverzeichnispartitionen	☑	☑
Möglichkeit der Installation eines Replikats von einem Wechseldatenträger	☑	☑
Möglichkeit, über Sicherheitsprinzipale Zugriff auf ein Windows Server-Netzwerk bereitzustellen	☐	☑
Möglichkeit, über Sicherheitsprinzipale Zugriff auf Anwendungen und Webdienste bereitzustellen	☑	☑
Integration in die Windows Server 2008 R2-Sicherungsprogramme	☑	☑

Wie Sie anhand von Tabelle 14.2 erkennen können, gibt es mehrere Ähnlichkeiten und Unterschiede zwischen den AD LDS und AD DS. Es ist beispielsweise einfach nachzuvollziehen, warum Exchange Server mit den AD DS integriert werden muss und nicht mit den AD LDS zusammenarbeiten kann, da Exchange Server für seinen Betrieb Zugriff auf den globalen Katalogserver braucht. Ohne diesen können E-Mail-Benutzer keine Empfänger nachschlagen. Da die AD LDS nicht den globalen Katalog unterstützen, kann Exchange Server nicht darauf basieren. Exchange Server ist jedoch eine Anwendung, die an allen Standorten der Domäne oder Gesamtstruktur Zugriff auf Verzeichnisdaten benötigt. Deshalb ist Exchange Server von der Platzierung Ihrer Domänencontroller abhängig, um sicherzustellen, dass alle Benutzer E-Mails ordnungsgemäß adressieren können.

Dennoch bieten die AD LDS einen Großteil des Funktionsumfangs der AD DS. Sie können beispielsweise ähnlich wie bei der Platzierung von Domänencontrollern Instanzen mit an verschiedenen Stellen in Ihrem Netzwerk verteilten Replikaten erstellen und anschließend zum Sicherstellen der Datenkonsistenz die Multimasterreplikation verwenden. Zusammengefasst stellen die AD LDS eine abgespeckte, portierbare und flexiblere Version des von den AD DS gebotenen Verzeichnisdienstes dar.

AD LDS-Szenarien

Nachdem Sie sich mit den AD LDS und ihren Features vertraut gemacht haben, können Sie beginnen, Szenarien zu ermitteln, für die sich diese Technologie eignet. Untersuchen Sie die folgenden Szenarien, wenn Sie entscheiden müssen, ob Sie die AD LDS oder die AD DS einsetzen:

- Wenn Ihre Anwendungen mit einem LDAP-Verzeichnis zusammenarbeiten müssen, sollten Sie den AD LDS den Vorzug gegenüber den AD DS geben. Die AD LDS können häufig auf demselben Server wie die Anwendung ausgeführt werden, was einen sehr schnellen lokalen Zugriff auf Verzeichnisdaten ermöglicht. Außerdem wird dadurch der Replikationsdatenverkehr reduziert, da alle benötigten Daten lokal sind. Darüber hinaus können Sie für die Bereitstellung die AD LDS-Instanz mit der Anwendung in einem Paket bündeln. Angenommen, Sie verfügen über eine Anwendung für das Personalwesen, die mit benutzerdefinierten Richtlinien arbeitet, um sicherzustellen, dass Benutzer nur auf bestimmte Inhalte zugreifen dürfen, wenn ihr Benutzerobjekt bestimmte Attribute enthält. Dann können Sie diese Attribute und Richtlinien in den AD LDS speichern.
- Verwenden Sie die AD LDS, um mit Benutzerkonten in den AD DS verknüpfte Daten bereitzustellen, für deren Unterstützung aber Erweiterungen am AD DS-Schema erforderlich sind. Durch Verwenden der AD LDS in diesem Szenario werden die zusätzlichen Benutzerdaten bereitgestellt, ohne das AD DS-Schema ändern zu müssen. Beispiel: Wenn Sie über eine zentrale Anwendung verfügen, die ein Foto jedes Mitarbeiters im Unternehmen bereitstellt, und dieses Foto mit dem AD DS-Konto des Benutzers verknüpft ist, können Sie die Fotos in einer AD LDS-Instanz speichern. Durch Speichern der Fotos in den AD LDS an einem zentralen Speicherort sind sie mit den Benutzerkonten in den AD DS verknüpft, doch da sie in den AD LDS enthalten sind, werden sie nicht mit allen anderen AD DS-Daten repliziert, wodurch sich die Bandbreitenanforderungen an die Replikation verringern.
- Sie können eine AD LDS-Instanz zum Bereitstellen von Authentifizierungsdiensten für eine Webanwendung wie Microsoft SharePoint Server in einem Umkreisnetzwerk oder Extranet einsetzen. Die AD LDS können die interne AD DS-Struktur durch eine Firewall

hindurch abfragen, um Benutzerkontendaten abzurufen und sicher im Umkreisnetzwerk zu speichern. Dadurch müssen die AD DS nicht im Umkreisnetzwerk bereitgestellt beziehungsweise Domänencontroller aus dem internen Netzwerk nicht in das Umkreisnetzwerk einbezogen werden. Sie können auch mit den Active Directory-Verbunddiensten (Active Directory Federation Services, AD FS) arbeiten, um diesen Zugriff bereitzustellen. Die AD FS werden detailliert in Kapitel 17, »Active Directory-Verbunddienste«, behandelt.

- Sie können mehrere Identitätsdatenspeicher zu einem einzelnen Verzeichnisspeicher zusammenfassen. Mithilfe eines Metaverzeichnisdienstes wie Forefront Identity Manager (FIM) oder dem kostenlosen Identity Integration Feature Pack (IIFP) können Sie Daten aus verschiedenen Quellen abrufen und in einer AD LDS-Instanz zusammenführen. FIM und IIFP unterstützen die Bereitstellung von Daten aus einer Vielzahl von Quellen wie AD DS-Gesamtstrukturen, SQL Server-Datenbanken, LDAP-Diensten anderer Anbieter und vieles mehr. IIFP ist eine Untermenge von Microsoft Identity Integration Server (MIIS) und unterstützt die Datenintegration zwischen den AD DS, AD LDS und Exchange Server. Mittels dieser Lösungen können Sie den Aufwand für die Identitätsverwaltung reduzieren, indem Sie eine zentrale Quelle bestimmen und alle anderen Datenspeicher mit Daten aus dieser Quelle versorgen.

Weitere Informationen FIM und IIFP

Weitere Informationen zu FIM finden Sie unter *http://www.microsoft.com/forefront/identitymanager/en/us/default.aspx*.

Weitere Informationen zu IIFP und die Möglichkeit zum Download finden Sie unter *http://www.microsoft.com/downloads/details.aspx?familyid=d9143610-c04d-41c4-b7ea-6f56819769d5*.

- Stellen Sie Unterstützung für abteilungsspezifische Anwendungen bereit. Mitunter benötigen Abteilungen besondere Identitätsdaten, die nur für die jeweilige Abteilung innerhalb des Unternehmens von Bedeutung sind. Durch Integrieren dieser Daten in eine AD LDS-Instanz hat die Abteilung Zugriff darauf, ohne den Verzeichnisdienst des gesamten Unternehmens zu beeinträchtigen.
- Sie können Unterstützung für verteilte Anwendungen bereitstellen. Wenn Ihre Anwendung verteilt ist und Zugriff auf Daten an mehreren Speicherorten benötigt, können Sie auch mit den AD LDS arbeiten, da sie dieselben Multimaster-Replikationsfunktionen wie die AD DS bieten.
- Sie können ältere Verzeichnisanwendungen in die AD LDS migrieren. Wenn in Ihrem Unternehmen ältere Anwendungen ausgeführt werden, die ein LDAP-Verzeichnis verwenden, können Sie die Daten in eine AD LDS-Instanz migrieren und an Active Directory-Verzeichnistechnologien anpassen.
- Stellen Sie Unterstützung für die lokale Entwicklung bereit. Da die AD LDS auf Clientarbeitsstationen installierbar sind, können Sie Entwicklern portierbare Einzelinstanzverzeichnisse zur Verfügung stellen, mit deren Hilfe sie benutzerdefinierte Anwendungen entwickeln können, die Zugriff auf Identitätsdaten benötigen. Die Softwareentwicklung mithilfe der AD LDS ist wesentlich einfacher zu verwalten und zu kontrollieren als die Entwicklung mithilfe der AD DS.

- Darüber hinaus sollten Sie beim Überprüfen verzeichnisfähiger Anwendungen auf dem Markt stets Anwendungen den Vorzug geben, die mit den AD LDS oder ihrem Vorgänger ADAM zusammenarbeiten, bevor Sie eine Anwendung wählen, die Änderungen am AD DS-Schema erfordert. Das Bereitstellen von Anwendungen mit portierbaren Verzeichnissen ist wesentlich einfacher und hat weit weniger Auswirkungen auf Ihr Netzwerk als das Bereitstellen von Anwendungen, die das Schema des Verzeichnisses ihres Netzwerkbetriebssystems unwiderruflich ändern.

Jedes dieser Szenarien stellt eine Einsatzmöglichkeit der AD LDS dar. Zu den typischen Anwendungsbereichen zählen Telefon- und Adressbücher, sicherheitsorientierte Anwendungen sowie Netzwerkkonfigurations- und Richtlinienspeicheranwendungen.

Wie Sie sehen, sind die AD LDS wesentlich portierbarer und flexibler, als es die AD DS je sein werden. Immer wenn Sie Schemaänderungen in den AD DS erwägen, sollten Sie die AD LDS in Betracht ziehen. Nahezu fast immer stellen die AD LDS die bessere Wahl dar, da die AD DS stets als Verzeichnis des Netzwerkbetriebssystems reserviert sind und eine Integration nur mit Anwendungen zulassen sollten, die den Funktionsumfang des Verzeichnisses des Netzwerkbetriebssystems ergänzen.

Weitere Informationen AD LDS

Weitere Informationen zu den AD LDS finden Sie unter *http://technet.microsoft.com/de-de/library/cc731868(WS.10).aspx*.

Prüfungstipp

Prägen Sie sich die Szenarien aus dem letzten Abschnitt ein. Es gibt zwar nur wenige Prüfungsfragen zu den AD LDS, aber Sie können davon ausgehen, dass sie sich auf das bevorzugte Auswählen der AD LDS gegenüber anderen Active Directory-Technologien beziehen.

Neue AD LDS-Features in Windows Server 2008 R2

Microsoft hat die AD LDS in Windows Server 2008 R2 um mehrere Features erweitert. All diese Features sind auch in AD DS verfügbar, daher wurden einige bereits in früheren Kapiteln vorgestellt.

- **Active Directory-Papierkorb** Dieses Feature wird über eine Schemaaktualisierung verfügbar gemacht. Es bietet Administratoren die Möglichkeit, versehentlich gelöschte Elemente wiederherzustellen. Das Feature ist auch in AD DS enthalten, es wurde in Kapitel 13, »Business Continuity«, behandelt.
- **Active Directory-Webdienste (Active Directory Web Services, ADWS)** Dieses Feature stellt eine Webdienstschnittstelle zur Verfügung, die Verbindungen zu AD LDS-Instanzen herstellt. Das Feature wird automatisch installiert und steht zur Verfügung, sobald Sie die Rolle *Active Directory Lightweight Directory Services* installiert haben. Dieses Feature ist auch in AD DS verfügbar, es wurde in Kapitel 3, »Verwalten von Benutzerkonten«, beschrieben.

- **Active Directory-Modul für Windows PowerShell** Dieses Feature stellt eine Befehlszeilenoberfläche für Administratoren zur Verfügung. Sie können mit PowerShell administrative Aufgaben interaktiv durchführen oder häufiger benötigte Vorgänge automatisieren. Dieses Feature steht auch für AD DS zur Verfügung, es wurde ebenfalls in Kapitel 3 vorgestellt.

Alle drei Neuerungen wurden bereits beschrieben. Sie können für die AD LDS praktisch genauso genutzt werden wie für die AD DS.

Installieren der AD LDS

Die AD LDS können als Teil von Windows Server 2008 R2 sowohl im Rahmen der vollständigen Installation als auch der Server Core-Installation installiert und konfiguriert werden. Darüber hinaus eignen sich die AD LDS ideal für die Virtualisierung mithilfe von Windows Server 2008 R2 Hyper-V. Aufgrund ihrer geringen Anforderungen können die AD LDS problemlos in einer virtuellen Instanz des Betriebssystems Windows Server 2008 R2 ausgeführt werden, es sei denn die Anwendung, die an die AD LDS-Instanz gebunden ist, setzt eine physische Installation voraus.

Vermeiden Sie möglichst die Installation der AD LDS auf Domänencontrollern. Auch wenn die AD LDS parallel zur Rolle eines Domänencontrollers und sogar eines schreibgeschützten Domänencontrollers ausgeführt werden können, sollten Domänencontroller als besondere Funktionsträger im Netzwerk angesehen werden und nach Möglichkeit ausschließlich an den DNS-Dienst gebunden werden. Da sich auch Domänencontroller gut für die Virtualisierung eignen, sollten in Netzwerken, die auf Hostservern aufbauen, auf denen Hyper-V und virtualisierte Instanzen anderer Dienste ausgeführt werden, Domänencontroller so umfassend wie möglich virtualisiert werden. Bei einem virtuellen Domänencontroller ist es wesentlich einfacher sicherzustellen, dass keine anderen Rollen auf dem Server ausgeführt werden, da alle anderen Rollen ebenfalls in ihren eigenen Instanzen von Windows Server 2008 R2 virtualisiert werden können.

Erwägen Sie außerdem, die AD LDS in Szenarien auszuführen, in denen eine hohe Sicherheit erforderlich ist. Als Beispiel bietet sich die Ausführung eines Authentifizierungsverzeichnisdienstes in Extranets oder Umkreisnetzwerken an. Das Arbeiten mit Server Core-Installationen in solchen Umgebungen kann die Angriffsfläche von Servern verkleinern, auf die von außerhalb Ihres Firmennetzwerks zugegriffen werden kann.

Ermitteln der AD LDS-Anforderungen

Wie zuvor erwähnt, haben die AD LDS sehr geringe Installationsanforderungen:

- Ein unterstütztes Betriebssystem wie beispielsweise Windows Server 2008 R2 Standard Edition, Enterprise Edition oder Datacenter Edition
- Ein Konto mit lokalen Administratorberechtigungen

Das Entfernen der AD LDS von einem Server umfasst zwei Aufgaben:

- Um eine AD LDS-Instanz zu entfernen, die Sie nach Installation der Rolle erstellt haben, öffnen Sie in der Systemsteuerung *Programme und Funktionen*.
- Entfernen Sie anschließend im Server-Manager die Rolle *Active Directory Lightweight Directory Services*.

Wie Sie sehen, sind die Installations- und Deinstallationsanforderungen sehr niedrig. Unbedingt zu erwähnen ist, dass Sie vor Entfernen der Rolle sicherstellen müssen, dass alle Instanzen von einem Server entfernt wurden.

Prüfungstipp

Sie müssen alle AD LDS-Instanzen von einem Server entfernen, bevor Sie die Rolle vom Server entfernen können.

Installieren der AD LDS unter Server Core

Die Installation der AD LDS entspricht nahezu der Installation der AD DS. Zuerst müssen Sie die Serverrolle und anschließend die gewünschten AD LDS-Instanzen installieren. Das Installieren der AD LDS unter der vollständigen Installation von Windows Server 2008 R2 wird in der Übung am Ende dieser Lektion behandelt.

Der Installationsprozess für die AD LDS ist unter Server Core ebenso einfach wie bei einer vollständigen Installation von Windows Server 2008 R2. Gehen Sie wie folgt vor:

1. Melden Sie sich mit lokalen Administratorberechtigungen an einem eigenständigen oder Mitgliedsserver mit Windows Server 2008 R2 an, auf dem Server Core ausgeführt wird.
2. Beginnen Sie mit dem Bestimmen des Dienstnamens der AD LDS. Geben Sie den folgenden Befehl ein:

   ```
   oclist | more
   ```

   Der Name sollte weiter unten in der Liste auftauchen und *DirectoryServices-ADAM-ServerCore* lauten.
3. Fahren Sie mit der Installation der Rolle fort. Geben Sie den folgenden Befehl ein:

   ```
   start /w ocsetup DirectoryServices-ADAM-ServerCore
   ```

   Bei Rollennamen wird zwischen Groß- und Kleinschreibung unterschieden, weshalb Sie den Namen exakt wie gezeigt eingeben müssen, da der Befehl sonst fehlschlägt. Außerdem stellt das Angeben des Befehls `start /w` sicher, dass die Eingabeaufforderung erst dann eine Rückgabe liefert, wenn die Rolleninstallation abgeschlossen ist.

Wenn Sie den Befehl `oclist` nochmals ausführen, werden Sie erkennen, dass die Rolle *Active Directory Lightweight Directory Services* zu diesem Server hinzugefügt wurde. Sie können auch zum Ordner *%SystemRoot%\ADAM* wechseln, um die neuen AD LDS-Dateien anzuzeigen. Ihr Server ist nun bereit, AD LDS-Instanzen bereitzustellen.

Wichtig Installierte AD LDS-Dateien

Die AD LDS installieren automatisch die Komponenten für das Active Directory-Modul für Windows PowerShell. Dazu gehören das .NET Framework 3.5.1, Windows PowerShell und die Active Directory-Webdienste.

Übung Installieren der AD LDS

In dieser Übung installieren Sie die Rolle *Active Directory Lightweight Directory Services* auf einem Server mit vollständiger Installation von Windows Server 2008 R2. Anschließend untersuchen Sie den Inhalt des Installationsordners, um zu bestimmen, welche Dateien installiert wurden.

▶ Übung 1 Installieren der AD LDS

In dieser Übung installieren Sie die Serverrolle *Active Directory Lightweight Directory Services*.

1. Vergewissern Sie sich, dass der Active Directory-Domänencontroller *SERVER01.contoso.com* ausgeführt wird, und starten Sie die Mitgliedsserver *SERVER03.contoso.com* und *SERVER04.contoso.com*.
2. Melden Sie sich mit dem Konto *CONTOSO\Administrator* an *SERVER03.contoso.com* an.

   Für das Arbeiten mit den AD LDS sind keine Domänenadministratorberechtigungen erforderlich. Da jede AD LDS-Installation von den AD DS unabhängig ist, benötigen Sie dafür nur lokale Administratorrechte, doch für diese Übung kann auch das Domänenadministratorkonto verwendet werden.
3. Klicken Sie im Server-Manager mit der rechten Maustaste auf den Knoten *Rollen* und wählen Sie den Befehl *Rollen hinzufügen*.
4. Lesen Sie die Seite *Vorbemerkungen* und klicken Sie auf *Weiter*.
5. Aktivieren Sie im Dialogfeld *Serverrollen auswählen* das Kontrollkästchen *Active Directory Lightweight Directory Services*, klicken Sie auf *Erforderliche Features hinzufügen* und klicken Sie auf *Weiter*.
6. Lesen Sie die Informationen im Fenster *Active Directory Lightweight Directory Services* und klicken Sie auf *Weiter*.
7. Überprüfen Sie die ausgewählten Optionen und klicken Sie dann auf *Installieren*.
8. Überprüfen Sie die Installationsergebnisse und klicken Sie auf *Schließen*.
9. Wiederholen Sie den Vorgang auf *SERVER04.contoso.com*.

Die AD LDS sind nun auf beiden Mitgliedsservern installiert.

Bei der AD LDS-Installation wird der Dienst installiert, und es wird ein Verzeichnisspeicher mit dem Namen *Adamntds.dit* im Ordner *%SystemRoot%\ADAM* erzeugt. Außerdem werden die Tools zum Konfigurieren und Verwalten der AD LDS und das Active Directory-Modul für PowerShell hinzugefügt.

Weitere Informationen AD LDS-Installationsprozess

Schrittweise Anleitungen zur Installation der AD LDS finden Sie unter *http://technet.microsoft.com/de-de/library/cc770639(WS.10).aspx*.

Nach Abschluss der Installation wird die Rolle im Server-Manager angezeigt (Abbildung 14.2).

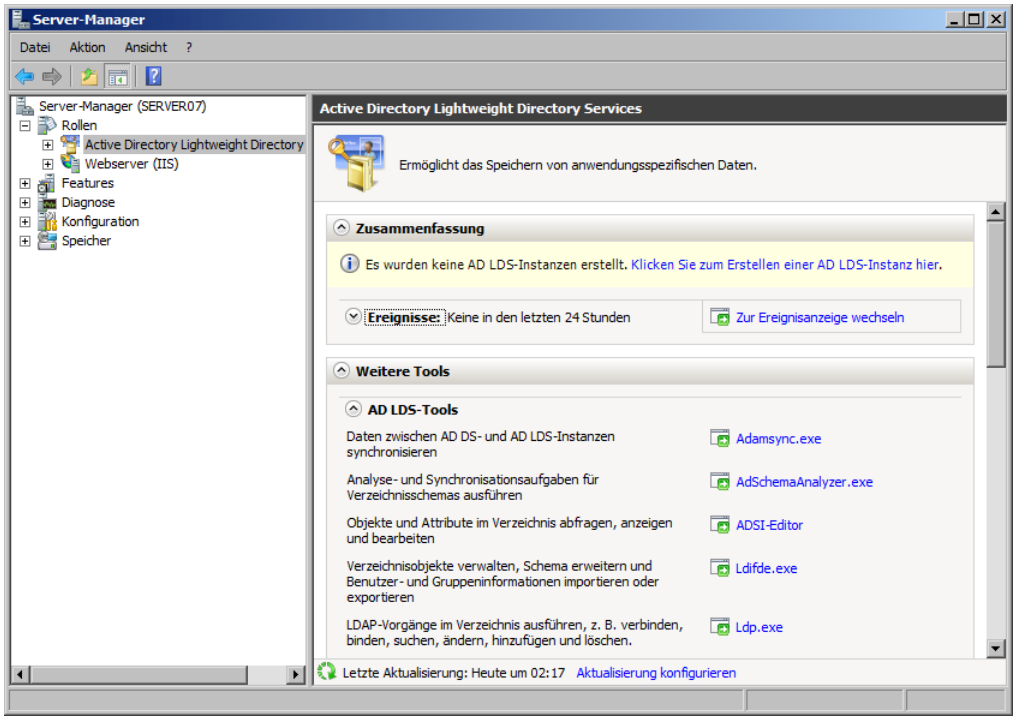

Abbildung 14.2 Anzeigen der Rolle *Active Directory Lightweight Directory Services* im Server-Manager

▶ Übung 2 Überprüfen der installierten AD LDS-Dateien

In dieser Übung überprüfen Sie die Dateien, die bei der AD LDS-Installation auf Servern installiert werden.

1. Melden Sie sich mit dem Konto *CONTOSO\Administrator* am Mitgliedsserver *SERVER03.contoso.com* an.
2. Klicken Sie im Menü *Start* mit der rechten Maustaste auf *Computer* und wählen Sie *Öffnen*, um ein Windows Explorer-Fenster zu öffnen.
3. Wechseln Sie zum Ordner *%SystemRoot%\ADAM*.
4. Überprüfen Sie die Dateien, die beim AD LDS-Installationsprozess erstellt wurden.

   Bei einer vollständigen Installation von Windows Server 2008 R2 wird bei der AD LDS-Installation der Ordner *ADAM* erstellt, in den 21 Dateien und zwei Unterordner eingefügt werden. Die beiden Unterordner enthalten Informationen zur Lokalisierung. Der Ordner *ADAM* enthält die folgenden Ordner (Abbildung 14.3):

   - Die AD LDS-Programmdateien, darunter DLL-, EXE-, CAT-, INI- und XML-Dateien
   - Den AD LDS-Verzeichnisspeicher *Adamntds.dit*
   - LDF-Dateien (Lightweight Directory Format), die zum Auffüllen von AD LDS-Instanzen dienen, wenn diese erstellt werden

In der nächsten Lektion werden Sie bei der Konfiguration der AD LDS mit diesen Dateitypen arbeiten.

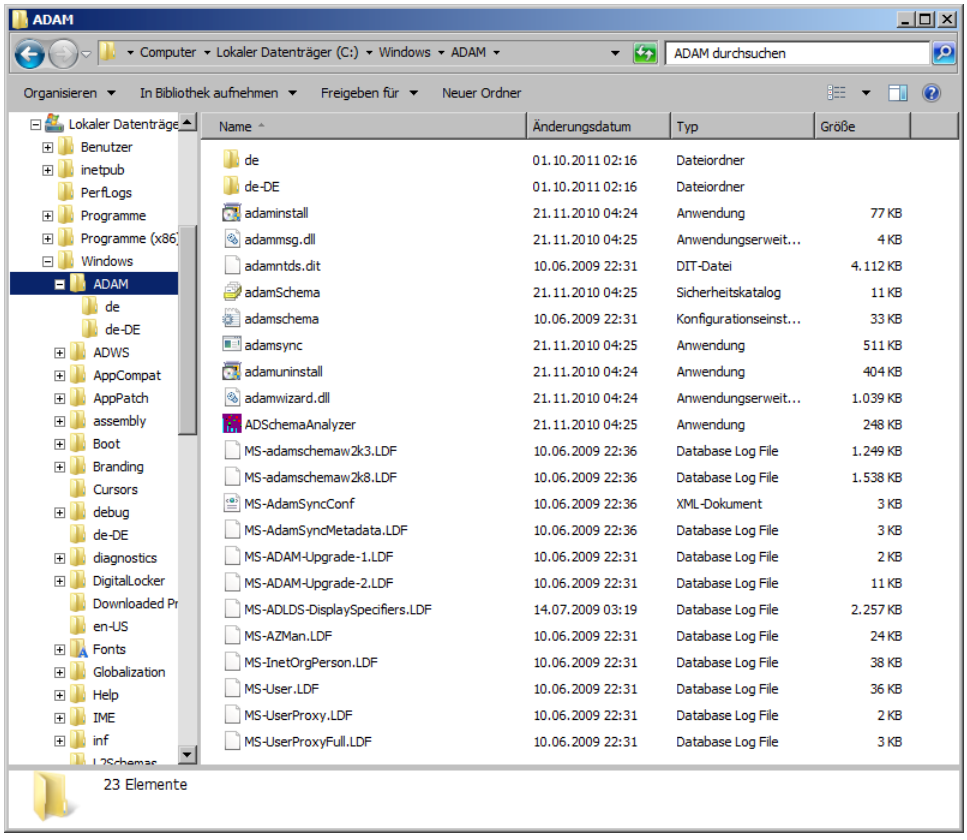

Abbildung 14.3 Bei der AD LDS-Installation wird der Ordner *%SystemRoot%\ADAM* erstellt und die AD LDS-Datenbank erzeugt

Die Installation der AD LDS unter Server Core umfasst nicht dieselben Dateien und Ordner wie die Installation bei einer vollständigen Installation von Windows Server 2008 R2. Server Core erstellt nur einen Ordner für die Lokalisierung im Vergleich zu zweien bei der vollständigen Installation. Darüber hinaus bietet die vollständige Installation mit dem Active Directory Schema Analyzer ein Tool, das unter Server Core nicht installiert wird.

Zusammenfassung der Lektion

- Wie der Name andeutet, sind die AD LDS eine abgespeckte Version der AD DS. Die AD LDS unterstützen mit Ausnahme der Netzwerkbetriebssystemfunktionen alle Features der AD DS. Sie stellen einen Verzeichnisdienst dar, der an Anwendungen gebunden werden kann und deren Bedarf an benutzerdefinierten Konfigurationen und Authentifizierungsdiensten in unsicheren Umgebungen wie Umkreisnetzwerken erfüllt.

- Die Installationsanforderungen der AD LDS sind sehr gering, da nur ein Server benötigt wird, auf dem eine unterstützte Version von Windows Server 2008 R2 läuft. Dabei kann es sich um einen eigenständigen oder Mitgliedsserver oder sogar um einen Domänencontroller handeln, obwohl Sie bestrebt sein sollten, Domänencontroller von allen anderen Rollen getrennt auszuführen.
- Um die AD LDS zu installieren, wählen Sie die Rolle im Assistenten zum Hinzufügen von Rollen aus. Der Installationsprozess ist der wahrscheinlich einfachste aller Rollen unter Windows Server 2008 R2.
- Zum Entfernen der AD LDS müssen Sie zuerst über die Systemsteuerung in der Konsole *Programme und Funktionen* alle Instanzen und anschließend die Rolle aus dem Server-Manager entfernen.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen aus Lektion 1, »Grundlagen und Installieren der AD LDS«, testen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.

Hinweis Die Antworten

Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Buchs.

1. Sie sind Serveradministrator für *contoso.com*. Ihr Chef hat Sie beauftragt, *SERVER04* so schnell wie möglich eine neue Rolle zuzuweisen. Auf *SERVER04* werden gegenwärtig fünf AD LDS-Instanzen ausgeführt. Sie müssen die AD LDS von diesem Server deinstallieren. Sie melden sich mit lokalen Administratorrechten an *SERVER04* an und öffnen eine Eingabeaufforderung mit erhöhten Rechten. Sie rufen den Befehl `ocsetup` mit dem Parameter `/uninstall` auf, doch er schlägt fehl. Welchen der folgenden Schritte müssen Sie zur Lösung dieses Problems unternehmen?
   A. Sie müssen den Server neu starten, um sicherzustellen, dass alle ausgeführten Setupvorgänge abgeschlossen sind, und dann den Befehl `ocsetup /uninstall` nochmals aufrufen.
   B. Sie müssen im Server-Manager alle AD LDS-Instanzen und die Rolle entfernen.
   C. Sie müssen zuerst über die Systemsteuerungsoption *Programme und Funktionen* alle vorhandenen AD LDS-Instanzen deinstallieren und anschließend `ocsetup /uninstall` an der Eingabeaufforderung aufrufen.
   D. Sie müssen über den Befehl `oclist` die Syntax der Option überprüfen, die Sie mit dem Befehl `ocsetup` entfernen möchten. Führen Sie anschließend den Befehl `ocsetup` mit ordnungsgemäßer Syntax aus.

Lektion 2: Konfigurieren und Verwenden der AD LDS

Nachdem Sie die AD LDS installiert haben, können Sie sie zum Speichern verzeichnisbezogener Daten verschiedener Anwendungen einsetzen. Doch zuerst sollten Sie sich mit den Tools zum Verwalten der AD LDS vertraut machen. Im Anschluss können Sie beginnen, die ersten Instanzen zu erstellen. Nachdem Sie Instanzen erstellt haben, können Sie sie absichern, um ihren ordnungsgemäßen Schutz sicherzustellen. Im nächsten Schritt erstellen Sie Replikate dieser Instanzen, damit Sie sie auf verschiedenen anderen Systemen installieren können, und steuern die Replikation, damit Instanzen auf verschiedenen Computern mithilfe der Multimasterreplikation aktualisiert werden können.

In dieser Lektion soll der Nutzen der AD LDS veranschaulicht werden, wenn Sie sie mit Anwendungen kombinieren und mit anderen Active Directory-Technologien von Windows Server 2008 R2 integrieren.

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

- Erstellen von AD LDS-Instanzen
- Arbeiten mit AD LDS-Tools
- Arbeiten mit Anwendungspartitionen
- Verwalten der Replikation zwischen AD LDS-Instanzen

Veranschlagte Zeit für diese Lektion: 30 Minuten

Arbeiten mit AD LDS-Tools

Sie können zum Arbeiten mit den AD LDS verschiedene Tools verwenden, von denen Sie schon viele von der Verwaltung der AD DS kennen. In Tabelle 14.3 werden diese Tools und ihr Zweck bei der Verwaltung des AD LDS-Dienstes beschrieben.

Beim Ausführen der AD LDS-Dienste verwenden Sie verschiedene der Tools in Tabelle 14.3, um die erforderlichen Konfigurations- und Verwaltungsaufgaben zu erledigen.

Weitere Informationen AD LDS-Überwachung

Weitere Informationen zum Überwachen von AD LDS-Instanzen beziehungsweise AD DS-Domänen finden Sie unter *http://technet.microsoft.com/de-de/library/cc731764(WS.10).aspx*.

Erstellen von AD LDS-Instanzen

Der Prozess zur Installation der Rolle *Active Directory Lightweight Directory Services* entspricht nahezu dem AD-DS-Installationsprozess. Sie beginnen mit der Installation der AD LDS-Binärdateien und erstellen nach deren Installation AD LDS-Instanzen, um mit dem Dienst zu arbeiten. Auch beim Bereitstellen der AD DS beginnen Sie mit der Installation der Binärdateien und erstellen anschließend mit dem Assistenten zum Installieren von Active Directory-Domänendiensten die zu verwendende AD DS-Instanz. Aufgrund der gleichen Codebasis sind viele Verwaltungstools identisch.

Tabelle 14.3 AD LDS-Tools und AD DS-Tools

Toolname	Zweck	Speicherort
Snap-In *Active Directory-Schema*	Dient zum Ändern des Schemas von AD LDS-Instanzen. Sie müssen allerdings zuerst über den Befehl *Regsvr32.exe* die Datei *Schmmgnt.dll* registrieren.	Benutzerdefinierte MMC
Snap-In *Active Directory-Standorte und -Dienste*	Dient zum Konfigurieren und Verwalten von Replikationsbereichen von AD LDS-Instanzen. AD LDS-Instanzen müssen zuerst aktualisiert werden, um Replikationsobjekte zu unterstützen.	Programmgruppe *Verwaltung*
AD LDS-Setup	Dient zum Erstellen von AD LDS-Instanzen.	Programmgruppe *Verwaltung*
ADAMInstall.exe	Befehlszeilenprogramm für die Erstellung von AD LDS-Instanzen.	Ordner *%SystemRoot%\ADAM*
ADAMSync.exe	Befehlszeilenprogramm für die Synchronisierung von Daten zwischen AD DS-Gesamtstruktur und AD LDS-Instanz. Die AD LDS-Instanz muss zuerst auf das AD DS-Schema aktualisiert werden.	Ordner *%SystemRoot%\ADAM*
ADAMUninstall.exe	Befehlszeilenprogramm zum Entfernen von AD LDS-Instanzen.	Ordner *%SystemRoot%\ADAM*
ADSchemaAnalyzer.exe	Befehlszeilenprogramm für das Kopieren von Schemainhalten aus den AD DS in die AD LDS beziehungsweise aus einer AD LDS-Instanz in eine andere. Unterstützt Kopiervorgänge für LDAP-Verzeichnisschemas anderer Anbieter.	Ordner *%SystemRoot%\ADAM*
ADSI-Editor	Dient zur interaktiven Verwaltung der AD LDS über ADSI.	Programmgruppe *Verwaltung*
CSVDE.exe	Dient zum Importieren von Dateien in AD LDS-Instanzen.	Befehlszeile
DSACLS.exe	Dient zum Steuern von Zugriffssteuerungslisten für AD LDS-Objekte.	Befehlszeile
DSAMain.exe	Dient zum Bereitstellen von Sicherungen und Snapshots des Active Directory-Speichers (*.dit*), um deren Inhalt zu ermitteln.	Befehlszeile
DSDBUtil.exe	Dient zum Ausführen der Datenbankwartung, zum Konfigurieren von AD LDS-Ports und zum Anzeigen vorhandener Instanzen. Dient auch zum Generieren von Ein-Schritt-Installationen für den Transport von AD LDS-Instanzen über den Erstellungsprozess *Installieren von Medium (IFM)*.	Befehlszeile
Dcdiag.exe	Dient zum Untersuchen von AD LDS-Instanzen. Der Parameter `/n:<Namenskontext>` muss angegeben werden, um die zu untersuchende Instanz zu benennen.	Befehlszeile
DSMgmt.exe	Unterstützt Anwendungspartitionen und die AD LDS-Richtlinienverwaltung.	Befehlszeile

▶

Toolname	Zweck	Speicherort
Ereignisanzeige	Dient zum Überwachen von AD LDS-Änderungen und zum Protokollieren alter und neuer Werte sowohl für Objekte als auch für Attribute.	Programmgruppe *Verwaltung*
LDIF-Dateien (LDAP Data Interchange Format)	AD LDS-Installationen können LDIF-Dateien (*.ldp*) während der Instanzerstellung dynamisch importieren, um die Instanz automatisch zu konfigurieren.	Ordner *%SystemRoot%\ADAM*
LDIFDE.exe	Dient zum Importieren von Dateien in AD LDS-Instanzen.	Befehlszeile
LDP.exe	Dient zum interaktiven Ändern von Inhalten beziehungsweise AD LDS-Instanzen über LDAP.	Befehlszeile
Ntdsutil.exe	Dient zum Verwalten von AD LDS-Instanzen, jedoch nur, wenn die AD DS ebenfalls installiert sind. (Nicht empfohlen. Arbeiten Sie stattdessen mit *DSDBUtil.exe*.)	Befehlszeile
RepAdmin.exe	Dient zum Analysieren der Replikation, um potenzielle Probleme anzuzeigen.	Befehlszeile
Server-Manager	Dient zum Verwalten vorhandener AD LDS-Instanzen.	Programmgruppe *Verwaltung*
Windows PowerShell	Dient zum Erstellen, Verwalten und Löschen von AD LDS-Instanzen.	Programmgruppe *Verwaltung*
Windows Server-Sicherungsprogramm	Dient zum Sichern und Wiederherstellen von AD LDS-Instanzen und ihrem Inhalt.	Programmgruppe *Verwaltung*

Vorbereiten der Erstellung von AD LDS-Instanzen

AD LDS-Instanzen werden mit dem Setup-Assistenten für Active Directory Lightweight Directory Services erstellt. Sie müssen jedoch die folgenden Komponenten vorbereiten, bevor Sie eine Instanz erstellen. Notieren Sie sich die Werte, die Sie beim Vorbereiten jedes Elements wählen. Sie brauchen diese Werte später, um die Instanz zu erstellen und zu verwalten. Folgende Elemente müssen Sie vorbereiten:

- Ein für Ihren Server erstelltes Datenlaufwerk. Da auf diesem Server Verzeichnisspeicher betrieben werden, sollten Sie diese Speicher auf ein vom Betriebssystem getrenntes Laufwerk legen.
- Den Namen, den Sie bei der Erstellung der Instanz angeben. Wählen Sie einen aussagekräftigen Namen, zum Beispiel den Namen der Anwendung, die an diese Instanz gebunden wird, um Instanzen zu benennen. Dieser Name wird verwendet zum Benennen der Instanz auf dem lokalen Computer sowie der Dateien, die die Instanz bilden, und des Dienstes, der diese unterstützt.
- Die Ports für die Kommunikation mit der Instanz. Die AD LDS und AD DS nutzen für die Kommunikation dieselben Ports. Diese Ports sind standardmäßig für LDAP 389 und für LDAP über Secure Sockets Layer (SSL) beziehungsweise Secure LDAP 636. Die AD DS nutzen zwei weitere Ports: 3268, der LDAP für den Zugriff auf den globalen Katalog verwendet, und 3269, der Secure LDAP für den Zugriff auf den globalen Katalog verwendet. Dass die AD DS und AD LDS dieselben Ports nutzen, ist ein weiterer guter Grund, beide Rollen nicht auf demselben Server auszuführen. Wenn der Assistent aller-

dings erkennt, dass die Ports 389 and 636 bereits belegt sind, schlägt er die Ports 50.000 und 50.001 vor und nutzt für weitere Instanzen andere Ports im 50.000-er-Bereich.

Schnelltest

1. Welche Ports werden für AD LDS-Instanzen verwendet?
2. Wie unterscheiden sich die Ports in einer AD LDS-Instanz von denen, die von den AD DS verwendet werden?

Antworten zum Schnelltest

1. Die von einer AD LDS-Instanz verwendeten Ports können die Standardports für LDAP (389) oder für LDAP über SSL beziehungsweise Secure LDAP (636) sein. Darüber hinaus können die AD LDS alle Ports über 1025 verwenden. Empfohlen wird hingegen die Verwendung von Ports im 50.000-er-Bereich.
2. Sowohl die AD DS als auch die AD LDS können die Ports 389 (LDAP) oder 636 (Secure LDAP) verwenden. Darüber hinaus verwenden die AD DS die Ports 3268 (LDAP) und 3269 (Secure LDAP) zur Kommunikation mit dem globalen Katalogserver. Empfohlen wird jedoch die Reservierung der Ports 389 und 636 für die AD DS.

Wichtig **Verwenden der Ports 389 und 636**

Wenn Sie AD LDS-Instanzen in einer Domäne einrichten, sollten Sie nicht die Ports 389 und 636 wählen, selbst wenn Sie nicht die erste Instanz auf einem Domänencontroller erstellen. Die AD DS verwenden diese Ports standardmäßig. Aus diesem Grund stellen einige Konsolen, zum Beispiel diejenigen, die das Snap-In *Active Directory-Schema* verwenden, keine Bindung zu lokalen Instanzen her, da sie standardmäßig eine Bindung zum AD DS-Verzeichnis herstellen. Als empfohlene Vorgehensweise sollten Sie stets Ports im 50.000-er-Bereich für Ihre AD LDS-Instanzen wählen.

Prüfungstipp

Merken Sie sich die Standardports, da sie mit Sicherheit in der Prüfung abgefragt werden, obwohl Sie sie in Produktivumgebungen vermeiden sollten.

- Den Namen der Active Directory-Anwendungspartition, den Sie für die Instanz wählen möchten. Zum Erstellen der Partition müssen Sie einen definierten Namen (Distinguished Name, DN) angeben, zum Beispiel *CN=AnwPartition1,DC=Contoso,DC=com*. Abhängig davon, wie Sie die Instanz nutzen möchten, benötigen Sie die Anwendungspartition. Anwendungspartitionen steuern den Replikationsbereich eines Verzeichnisspeichers. Wenn Sie beispielsweise DNS-Daten im Verzeichnis integrieren, erstellen die AD DS eine Anwendungspartition, um den gewünschten Domänencontrollern DNS-Daten zur Verfügung zu stellen. Es gibt drei Möglichkeiten zum Erstellen von Anwendungspartitionen für die AD LDS: beim Erstellen der Instanz, beim Installieren der Anwendung, die an die Instanz gebunden wird, oder beim manuellen Erstellen der Partition mit dem Programm *LDP.exe*. Wenn Ihre Anwendung Anwendungspartitionen nicht automatisch erstellt, müssen Sie sie mithilfe des Assistenten einrichten.

- Ein Dienstkonto zum Ausführen der Instanz. Sie können das Konto *NETZWERKDIENST* verwenden, doch wenn Sie mehrere Instanzen ausführen möchten, empfiehlt es sich, benannte Dienstkonten für jede Instanz zu verwenden. Wenn Sie kein verwaltetes Dienstkonto benutzen, sondern Ihre Dienstkonten von Hand einrichten, sollten Sie die nachfolgenden Anweisungen zu und Anforderungen an Dienstkonten befolgen:

Hinweis Verwaltete Dienstkonten

Wie Sie ein verwaltetes Dienstkonto erstellen, ist in Kapitel 8, Lektion 4, ausführlich beschrieben.

  - Wenn Sie in einer Domäne arbeiten, sollten Sie ein Domänenkonto erstellen, andernfalls ein lokales Konto (zum Beispiel in einem Umkreisnetzwerk).
  - Geben Sie dem Konto den Namen der Instanz.
  - Weisen Sie diesem Konto ein komplexes Kennwort zu.
  - Aktivieren Sie in den Kontoeigenschaften *Benutzer kann Kennwort nicht ändern*. Sie weisen diese Eigenschaft zu, damit niemand das Kennwort bestimmen kann.
  - Aktivieren Sie in den Kontoeigenschaften *Kennwort läuft nie ab*. Sie weisen diese Eigenschaft zu, um sicherzustellen, dass der Dienst nicht aufgrund einer Kennwortrichtlinie ausfällt.
  - Weisen Sie das Benutzerrecht *Anmelden als Dienst* in der lokalen Sicherheitsrichtlinie aller Computer zu, auf denen diese Instanz ausgeführt wird.
  - Weisen Sie das Benutzerrecht *Generieren von Sicherheitsüberwachungen* in der lokalen Sicherheitsrichtlinie aller Computer zu, auf denen diese Instanz ausgeführt wird, um die Kontoüberwachung zu unterstützen.
- Eine Gruppe mit den Benutzerkonten, die die Instanz verwalten. Die empfohlene Vorgehensweise für die Zuweisung von Berechtigungen ist das Verwenden von Gruppen, selbst wenn nur ein Konto Mitglied einer Gruppe ist. Wenn sich Personal verändert, können Sie stets Gruppenmitglieder hinzufügen oder ändern, ohne Berechtigungen hinzufügen oder ändern zu müssen. Wenn Sie in einer Domäne arbeiten, sollten Sie eine Domänengruppe erstellen, ansonsten eine lokale Gruppe. Geben Sie der Gruppe den Namen der Instanz. Auf diese Weise erschließt sich schnell der Zweck der Gruppe. Fügen Sie zu der Gruppe Ihr eigenes Konto sowie das zuvor erstellte Dienstkonto hinzu.
- Zusätzliche LDIF-Dateien, die Sie für die Instanz benötigen. Legen Sie diese Dateien im Ordner *%SystemRoot%\ADAM* ab. Diese Dateien werden bei der Erstellung der Instanz importiert. Beim Importieren von LDIF-Dateien wird das Schema der Instanz, die Sie erstellen, so erweitert, dass zusätzliche Vorgänge unterstützt werden. Um beispielsweise die AD DS mit den AD LDS zu synchronisieren, importieren Sie die Datei *MS-AdamSyncMetadata.ldf*. Falls Ihre Anwendung benutzerdefinierte Schemaänderungen erfordert, erstellen Sie die LDIF-Datei im Vorfeld und importieren sie beim Erstellen der Instanz. Sie können LDIF-Dateien auch stets importieren, nachdem die Instanz erstellt wurde. Standardmäßige LDIF-Dateien finden Sie in Tabelle 14.4.

Tabelle 14.4 Standardmäßige LDIF-Dateien für die AD LDS

Dateiname	Zweck
MS-ADAM-Upgrade-1.ldf	Dient zum Aktualisieren des AD LDS-Schemas auf die neueste Version.
MS-ADAM-Upgrade-2.ldf	Dient zum Aktualisieren des AD LDS-Schemas, damit es den Active Directory-Papierkorb unterstützt.
MS-adamschemaw2k3.ldf	Als Voraussetzung für das Synchronisieren einer Instanz mit Active Directory unter Windows Server 2003 erforderlich.
MS-adamschemaw2k8.ldf	Als Voraussetzung für das Synchronisieren einer Instanz mit Active Directory unter Windows Server 2008 oder Windows Server 2008 R2 erforderlich.
MS-AdamSyncMetadata.ldf	Für die Synchronisierung von Daten zwischen einer AD DS-Gesamtstruktur und einer AD LDS-Instanz über ADAMSync erforderlich.
MS-ADLDS-DisplaySpecifiers.ldf	Für den Betrieb des Snap-Ins *Active Directory-Standorte und -Dienste* erforderlich.
MS-AZMan.ldf	Zur Unterstützung des Windows-Autorisierungs-Managers erforderlich.
MS-InetOrgPerson.ldf	Zur Erstellung von Benutzerklassen und Attributen für `inetOrgPerson` erforderlich.
MS-User.ldf	Zur Erstellung von Benutzerklassen und Attributen erforderlich.
MS-UserProxy.ldf	Zur Erstellung einer einfachen Benutzerklasse für `userProxy` erforderlich.
MS-UserProxyFull.ldf	Zur Erstellung einer vollständigen Klasse für `userProxy` erforderlich. *MS-UserProxy.ldf* muss zuerst importiert werden.

Sobald Sie alle diese Komponenten beisammen haben, können Sie mit der Erstellung Ihrer ersten Instanz beginnen. Vergewissern Sie sich, dass das verwendete Konto über lokale Administratorrechte verfügt. Es gibt zwei Möglichkeiten, eine Instanz zu erstellen: Erstens über den Setup-Assistenten für Active Directory Lightweight Directory Services und zweitens über die Befehlszeile. In der Übung in dieser Lektion arbeiten Sie mit dem Assistenten. Die Befehlszeile wird im nächsten Abschnitt erläutert.

Wichtig AD LDS-Protokolldateien

Die AD LDS generieren Protokolldateien, während sie eine Instanz erstellen. Diese Dateien liegen im Ordner *%SystemRoot%\Debug*, sie heißen *ADAMSetup.log* und *ADAMSetup_loader.log*. Sie können sich den Inhalt dieser Dateien ansehen, falls Probleme beim Erstellen einer Instanz auftreten.

Ausführen einer unbeaufsichtigten Erstellung einer AD LDS-Instanz

Sie können die Erstellung von AD LDS-Instanzen unbeaufsichtigt ausführen. Um beispielsweise Instanzen für Server Core-Installationen zu erstellen, müssen Sie einen unbeaufsichtigten Instanzerstellungsprozess wählen, da es keine grafische Benutzeroberfläche zum Ausführen des Assistenten gibt. Die unbeaufsichtigte Instanzerstellung ist auch nützlich, wenn Sie eine Instanz für eine auf mehrere Server verteilte Anwendung erstellen müssen. Stellen

Sie sicher, dass alle zuvor in dieser Lektion genannten Voraussetzungen im Abschnitt »Vorbereiten der Erstellung von AD LDS-Instanzen« erfüllt sind.

Der Ordner *%SystemRoot%\ADAM* enthält das zusätzliche Tool *AdamInstall.exe*, mit dem unbeaufsichtigte Instanzeinrichtungen ausgeführt werden können. Wie das Tool *Dcpromo.exe* benötigt dieses Tool für die Erstellung der Instanz eine Textdatei als Eingabe. Sie können *AdamInstall.exe* entweder unter einer vollständigen Installation oder unter Server Core ausführen. Erstellen Sie zunächst eine Antwortdatei:

1. Öffnen Sie den Editor.
2. Geben Sie den folgenden Text für die Antwortdatei ein:

```
[ADAMInstall]
InstallType=Unique
InstanceName=<Instanzname>
LocalLDAPPortToListenOn=<Portnummer>
LocalSSLPortToListenOn=<Portnummer>
NewApplicationPartitionToCreate=<Partitionsname> DataFilesPath=D:\ADAMInstances\
<Instanzname>\Data LogFilesPath=D:\ADAMInstances\<Instanzname>\Data
ServiceAccount=<Domänen- oder Computername>\<Kontoname>
ServicePassword=<Kennwort>
Administrator=<Domänen- oder Computername>\<Kontoname>\<Gruppenname>
ImportLDIFFiles="LDIFFilename1" "LDIFFilename2" "LDIFFilename3"
SourceUserName=<Domänen- oder Computername>\<Kontoname>
SourcePassword=<Kennwort>
```

   Ersetzen Sie alle kursiven Angaben durch die entsprechenden Werte. Die benötigten Werte finden Sie weiter oben in dieser Lektion unter »Vorbereiten der Erstellung von AD LDS-Instanzen«. Gehen Sie sorgsam mit dieser Datei um, da sie Kennwörter im Klartext enthält. Die Kennwörter werden entfernt, sobald die Datei vom Tool zur Erstellung von AD LDS-Instanzen verwendet wird.
3. Speichern Sie die Datei im Ordner *%SystemRoot%\ADAM* und benennen Sie sie mit dem Namen der zu erstellenden Instanz.
4. Schließen Sie den Editor.

Weitere Informationen Erstellen von AD LDS-Instanzen

Weitere Informationen zur Erstellung von AD LDS-Instanzen finden Sie unter *http://technet.microsoft.com/de-de/library/cc770639(WS.10).aspx*.

Nun können Sie mit dem Erstellen einer Instanz beginnen. Bedenken Sie, dass Sie lokale Administratorrechte benötigen.

1. Öffnen Sie im Menü *Start* eine Eingabeaufforderung mit erhöhten Rechten, indem Sie mit der rechten Maustaste auf *Eingabeaufforderung* klicken und *Als Administrator ausführen* wählen.
2. Wechseln Sie im Eingabeaufforderungsfenster zum Ordner *%SystemRoot%\ADAM*. Geben Sie den folgenden Befehl ein und drücken Sie die EINGABETASTE.

```
cd windows\adam
```

3. Geben Sie den folgenden Befehl ein. Setzen Sie den Dateinamen in Anführungszeichen, falls er Leerzeichen enthält.

   ```
   adaminstall /answer:<Dateiname.txt>
   ```

4. Schließen Sie das Eingabeaufforderungsfenster.

Ihre Instanz ist fertig. Sie können nun prüfen, ob die Instanzdateien erstellt wurden, indem Sie zum Zielordner wechseln und dessen Inhalt anzeigen.

Migrieren vorheriger LDAP-Instanzen in die AD LDS

Sie können auch vorhandene LDAP-Verzeichnisse in die AD LDS migrieren oder Instanzen von ADAM in die AD LDS aktualisieren. Importieren Sie dazu den Inhalt der älteren Instanzen in eine neue Instanz der AD LDS.

Das Importieren der Daten kann bei der Erstellung der Instanz oder danach erfolgen. Beide Prozesse befolgen denselben Ansatz, da beide mit LDIF-Dateien beziehungsweise Dateien mit der Erweiterung *.ldf* arbeiten. Wenn Sie Daten importieren möchten, nachdem die Instanz erstellt wurde, müssen Sie das Tool *LDIFDE.exe* verwenden. Sie müssen die Daten zuerst aus der vorherigen Instanz exportieren und in einer Datei im LDIF-Format ablegen, bevor Sie sie importieren können.

Über *LDIFDE.exe* exportieren Sie Inhalte aus vorhandenen Instanzen. Sie benötigen lokale Administratorrechte sowie Administratorrechte für die Instanz, um diese Schritte ausführen zu können. Außerdem müssen Sie die Eingabeaufforderung mit erhöhten Rechten verwenden. Verwenden Sie die folgende Syntax:

```
ldifde -f <Dateiname> -s <Servername>:<Portnummer> -m -b <Benutzername> <Domänenname>
   <Kennwort>
```

In diesem Befehl ist *<Dateiname>* der Name der zu erstellenden Datei (geben Sie Anführungszeichen ein, wenn der Pfad Leerzeichen enthält). *<Servername>* ist der Name des Servers, auf dem die Instanz ausgeführt wird. *<Portnummer>* ist der Kommunikationsport. *<Benutzername>*, *<Domänenname>* und *<Kennwort>* sind die Anmeldeinformationen des Instanzadministrators.

Zum Importieren der Daten in die neue Instanz verwenden Sie einen ähnlichen Befehl:

```
ldifde -i -f <Dateiname> -s <Servername>:<Portnummer> -m -b <Benutzername> <Domänenname>
   <Kennwort>
```

Um Kennwörter aus der vorhandenen Instanz zu importieren, müssen Sie den Parameter `-h` angeben, der unter Verwendung von SASL (Simple Authentication And Security Layer) alle Kennwörter verschlüsselt.

Aktivieren des Active Directory-Papierkorbs in AD LDS

In der Standardeinstellung ist der Active Directory-Papierkorb in AD LDS-Instanzen nicht aktiviert; auch in den AD DS steht er erst zur Verfügung, nachdem er aktiviert wurde. Wenn Sie den Papierkorb in den AD LDS aktivieren wollen, müssen Sie das Schema aktualisieren. Verwenden Sie für diese Schemaaktualisierung den folgenden Befehl:

```
ldifde -i -f MS-ADAM-Upgrade-2.kdf -s <Servername>:<Portnumber> -b <Benutzername>
   <Domänenname> <Kennwort> -j . -$ adamschema.cat
```

Diese Aktion kann nicht wieder rückgängig gemacht werden. Es ist am einfachsten, diese Aktualisierung durchzuführen, nachdem Windows Server 2008 R2 installiert ist und die Rolle *Active Directory Lightweight Directory Services* aktiviert wurde, weil die benötigten

LDF- und CAT-Dateien dann einfach zu finden sind (im Ordner *%SystemRoot%\ADAM*). Wenn Sie versuchen, eine AD LDS-Instanz zu aktualisieren, bevor Sie den Server auf Windows Server 2008 R2 aktualisieren, müssen Sie diese Dateien auf einem anderen Server suchen und auf den Server kopieren, auf dem Sie die Aktualisierung durchführen.

Schnelltest

1. Welche drei Möglichkeiten gibt es zum Erstellen von Anwendungspartitionen für AD LDS-Instanzen?
2. Was ist der Zweck der zu den AD LDS gehörenden LDIF-Dateien?
3. Wie können Sie den Prozess der AD LDS-Instanzerstellung analysieren, wenn etwas schiefgeht?

Antworten zum Schnelltest

1. Es gibt drei Möglichkeiten zum Erstellen von Anwendungspartitionen für AD LDS-Instanzen:
   - Bei der Erstellung einer Installation während der AD LDS-Einrichtung
   - Während der Installation der Anwendung, die an eine AD LDS-Instanz gebunden wird
   - Manuell mit dem Tool *LDP.exe*
2. Die zu den AD LDS gehörenden LDIF-Dateien dienen (je nach Datei) mehreren Zwecken, doch im Allgemeinen sollen sie das Schema einer Instanz erweitern, um spezifische Funktionen zur Verfügung zu stellen.
3. Die AD LDS generieren während der Erstellung der Instanz Protokolldateien. Diese Dateien befinden sich im Ordner *%SystemRoot%\Debug* und haben die Namen *ADAMSetup.log* und *ADAMSetup_loader.log*. Sie können diese Dateien überprüfen, um während der Erstellung der Instanz aufgetretene Probleme zu suchen und zu beheben.

Weitere Informationen LDIFDE

Weitere Informationen zum Tool *LDIFDE.exe* finden Sie in Kapitel 3.

Arbeiten mit AD LDS-Instanzen

Tabelle 14.3 weiter oben enthält alle Tools für die Verwaltung von AD LDS-Instanzen. Darunter sind die grafischen Tools wie ADSI-Editor, *LDP.exe*, das Snap-In *Active Directory-Schema* und *Active Directory-Standorte und -Dienste* am nützlichsten. Sie steuern, wie Sie den Inhalt Ihrer Instanzen anzeigen und bearbeiten können. Befehlszeilenprogramme eignen sich besser für die Automatisierung von Prozessen und die Dateneingabe für AD LDS-Instanzen.

Verwalten von Instanzen mit ADSI-Editor

ADSI-Editor ist ein allgemeines Verwaltungsprogramm für AD LDS-Instanzen. Immer wenn Sie mit einer Instanz arbeiten möchten, müssen Sie zuerst eine Verbindung beziehungsweise Bindung zur Instanz herstellen. Außerdem müssen Sie Administrator der Instanz sein, um dazugehörige Verwaltungsaufgaben ausführen zu können. Gehen Sie wie folgt vor:

1. Öffnen Sie den ADSI-Editor in der Programmgruppe *Verwaltung*.
2. Klicken Sie im Strukturbereich mit der rechten Maustaste auf *ADSI-Editor* und wählen Sie *Verbindung herstellen*. Das Dialogfeld *Verbindungseinstellungen* wird geöffnet (Abbildung 14.4). Geben Sie die folgenden Werte ein:
   - *Name*: Muss dem Namen der Instanz entsprechen, mit der Sie eine Verbindung herstellen möchten.
   - *Verbindungspunkt*: Wählen Sie *Definierten Namen oder Namenskontext auswählen oder eingeben* aus und geben Sie den definierten Namen der Instanz ein.
   - *Computer*: Wählen Sie *Domäne oder Server auswählen oder eingeben* aus und geben Sie den Servernamen und die Portnummer ein. Beispiel: **SERVER03:50000**.
   - *Computer*: Aktivieren Sie das Kontrollkästchen *SSL-basierte Verschlüsselung verwenden*, wenn Sie einen Secure LDAP-Port verwenden.

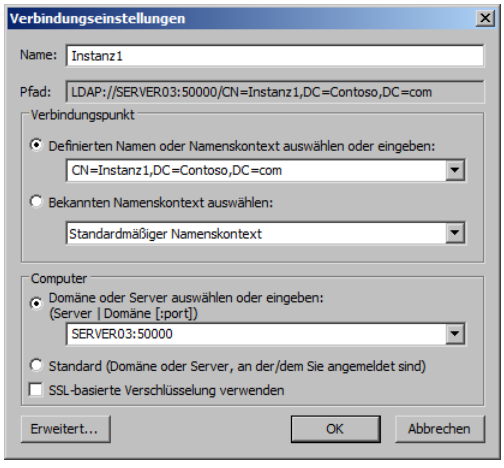

Abbildung 14.4 Verbinden mit einer AD LDS-Instanz mithilfe des ADSI-Editors

3. Klicken Sie auf *OK*.

   Die Verbindung zur Instanz ist hergestellt. Erweitern Sie alle Einträge, um den Inhalt der Instanz anzuzeigen. Untersuchen Sie die Kontextmenüs, um sich mit den Vorgängen vertraut zu machen, die Sie mit ADSI-Editor auf AD LDS-Instanzen anwenden können.

Sobald Sie die Bindung zur Instanz hergestellt haben, können Sie Objekte in der Instanz erstellen und verwalten. Gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf den definierten Namen der Anwendungspartition, wählen Sie *Neu* aus und klicken Sie auf *Objekt*. Das Dialogfeld *Objekt erstellen* wird geöffnet, das alle verfügbaren Objektklassen im Schema der Instanz angezeigt.

2. Beginnen Sie mit dem Erstellen einer Benutzergruppe. Wechseln Sie zum Objekt *group*, wählen Sie es aus und klicken Sie auf *Weiter*.
3. Geben Sie den Namen der Gruppe ein, zum Beispiel AD **LDS-Benutzer**, und klicken Sie auf *Weiter*.
4. Auf dem nächsten Bildschirm des Dialogfelds können Sie auf *Weitere Attribute* klicken, um diesem neuen Objekt weitere Werte zuzuweisen, zum Beispiel eine Beschreibung der Gruppe. Wählen Sie in der Dropdownliste *Anzuzeigende Eigenschaft* den Eintrag *admin-Description* aus. Geben Sie in das Feld *Attribut bearbeiten* eine Beschreibung ein, zum Beispiel **Gruppe für AD LDS-Benutzer**, klicken Sie auf *Festlegen* und anschließend auf *OK*.
5. Klicken Sie auf *Fertig stellen*, um die Gruppe zu erstellen. Dadurch wird standardmäßig eine Sicherheitsgruppe erstellt.
6. Erstellen Sie nun einen Benutzer. Klicken Sie mit der rechten Maustaste auf den definierten Namen der Anwendungspartition, wählen Sie *Neu* aus und klicken Sie auf *Objekt*.
7. Wechseln Sie zum Objekt *user*, wählen Sie es aus und klicken Sie auf *Weiter*.
8. Geben Sie den Namen des Benutzers ein und klicken Sie auf *Weiter*.
9. Klicken Sie auch hier wieder auf *Weitere Attribute*, um diesem neuen Objekt weitere Einstellungen zuzuweisen.
10. Klicken Sie auf *Fertig stellen*, um den Benutzer zu erstellen.
11. Fügen Sie nun den Benutzer zur Gruppe hinzu. Wählen Sie die Partition in der Konsolenstruktur aus, klicken Sie im Detailbereich mit der rechten Maustaste auf die Gruppe und wählen Sie *Eigenschaften*.
12. Wechseln Sie im Dialogfeld *Eigenschaften* zur Eigenschaft *member* und klicken Sie anschließend auf *Bearbeiten*.
13. Klicken Sie im Dialogfeld *Editor für mehrwertige definierte Namen mit Sicherheitsprinzipal* auf *DN hinzufügen*.
14. Geben Sie im Dialogfeld *Definierten Namen (DN) hinzufügen* den definierten Namen des erstellten Benutzers ein, zum Beispiel **cn=John Kane,cn=Instance1,dc=contoso, dc=com**. Klicken Sie auf *OK*. Der Benutzer wird nun in der Mitgliederliste aufgeführt.
15. Klicken Sie auf *OK*, um den Vorgang abzuschließen.

Wenn Sie die Eigenschaften der Gruppe erneut anzeigen, werden Sie sehen, dass der Benutzer zur Gruppe hinzugefügt wurde. Diese Methode ist recht mühsam, um Benutzer und Gruppen auf diese Weise zu einer Instanz hinzuzufügen, eignet sich aber für einzelne Änderungen. Im Idealfall erstellen Sie Benutzer- und Gruppenlisten, die Sie dann in einem Massenvorgang über *CS-VDE.exe* oder *LDIFDE.exe* hinzufügen. In Kapitel 3 können Sie Informationen zur Automatisierung der Benutzererstellung und in Kapitel 4, »Verwalten von Gruppen«, Informationen zur Automatisierung der Gruppenerstellung nachlesen.

Verwenden von *LDP.exe* zum Arbeiten mit Instanzen

Auch über die Konsole *LDP.exe* können Sie den Inhalt von Instanzen anzeigen und bearbeiten. Wie bei ADSI-Editor müssen Sie zuerst eine Verbindung und anschließend eine Bindung zur Instanz herstellen, mit der Sie arbeiten möchten. Außerdem müssen Sie Administrator der Instanz sein, um Verwaltungsaufgaben dafür ausführen zu können. Gehen Sie wie folgt vor:

1. Starten Sie *LDP.exe* über die Befehlszeile oder den Server-Manager unter dem Abschnitt *Active Directory Lightweight Directory Service*, *Weitere Tools*.
2. Klicken Sie im Menü *Remotedesktopverbindung* auf *Verbinden*.
3. Geben Sie den Namen des Servers, zu dem die Verbindung hergestellt werden soll, und die gewünschte Portnummer ein. Aktivieren Sie *SSL*, wenn Sie einen Secure LDAP-Port verwenden. Klicken Sie auf *OK*.
4. Klicken Sie im Menü *Remotedesktopverbindung* auf *Gebunden*.
5. Falls Ihr Konto über die benötigten Berechtigungen verfügt, wählen Sie *Bindung als aktuell angemeldeter Benutzer* aus. Falls nicht, wählen Sie *Bindung mit Anmeldeinformationen* aus und geben die entsprechenden Anmeldeinformationen ein. Klicken Sie auf *OK*.
6. Klicken Sie im Menü *Ansicht* auf *Struktur*. Dadurch wird die Baumstruktur aufgefüllt.
7. Klicken Sie in der Dropdownliste *Basis-DN* auf den nach unten weisenden Pfeil, um die Liste der definierten Namen anzuzeigen, und wählen Sie den Namen Ihrer Instanz aus. Klicken Sie auf *OK*.

   Ab dieser Stelle können Sie im Strukturbereich auswählen, wo Sie in der Instanz arbeiten möchten. Untersuchen Sie die verschiedenen Menüs, um zu prüfen, welche Vorgänge Sie mithilfe von *LDP.exe* anwenden können, und schließen Sie *LDP.exe*.

Weitere Informationen **Anwenden von *LDP.exe* auf AD LDS-Instanzen**

Weitere Informationen zum Anwenden von *LDP.exe* auf AD LDS-Instanzen finden Sie unter *http://technet.microsoft.com/de-de/library/cc770639(WS.10).aspx*.

Verwenden des Snap-Ins *Active Directory-Schema* zum Arbeiten mit Instanzen

Sie können auch mit dem Snap-In *Active Directory-Schema* benutzerdefinierte Konsolen für die Verwaltung von AD LDS-Instanzschemas erstellen. Wenn Sie dieses Snap-In verwenden möchten, müssen Sie es zuerst auf dem Server registrieren (dies wurde bereits in Kapitel 2, »Verwalten der Active Directory-Domänendienste«, beschrieben). Geben Sie dazu in einer Eingabeaufforderung mit erhöhten Rechten folgenden Befehl ein:

```
regsvr32 schmmgmt.dll
```

Sie können nun das Snap-In *Active Directory-Schema* laden, um das Schema Ihrer Instanzen anzuzeigen. Sie benötigen Administratorberechtigungen für die Instanz.

1. Klicken Sie auf *Start* und geben Sie im Suchfeld **mmc** ein. Drücken Sie die EINGABETASTE.
2. Klicken Sie im Menü *Datei* der leeren MMC auf *Snap-In hinzufügen/entfernen*.
3. Wählen Sie in der Liste *Verfügbare Snap-Ins* den Eintrag *Active Directory-Schema* aus, klicken Sie auf *Hinzufügen* und anschließend auf *OK*.
4. Speichern Sie die Konsole unter einem geeigneten Namen am gewünschten Speicherort.
5. Das Snap-In *Active Directory-Schema* stellt standardmäßig eine Bindung zum Verzeichnis der Active Directory-Domänendienste her. Um eine Bindung zu einer AD LDS-Instanz herzustellen, klicken Sie mit der rechten Maustaste im Strukturbereich auf *Active Directory-Schema* und wählen *Active Directory-Domänencontroller ändern* aus.

6. Wählen Sie im Dialogfeld *Verzeichnisserver ändern* die Option *Bestimmter Domänencontroller oder AD LDS-Instanz* aus, klicken Sie auf *<Verzeichnisservername[:port] hier eingeben>*, geben Sie den Servernamen, einen Doppelpunkt und die Portnummer ein und drücken Sie die EINGABETASTE. Klicken Sie auf *OK*.
7. Klicken Sie im Warndialogfeld auf *Ja*, um die Server zu ändern.

   Sie können nun das Schema dieser Instanz anzeigen. Speichern Sie nochmals die Konsole, um diese Einstellungen zu speichern. Achten Sie auf die Ähnlichkeiten zwischen dem Schema einer AD LDS-Instanz und dem eines AD DS-Verzeichnisses.

Hinweis Erstellen einer Konsole für mehrere AD LDS-Instanzschemas

Wenn Sie nur eine Konsole mit mehreren AD LDS-Instanzschemas erstellen möchten, müssen Sie zur Konsole lediglich weitere *Active Directory-Schema*-Snap-Ins hinzufügen. Verwenden Sie ein Snap-In für jede Instanz, mit der Sie sich verbinden möchten. Wenn Sie die Konsole erneut öffnet, verbindet sie sich mit den einzelnen Instanzen, wodurch Sie Zeit sparen.

Verwenden von *Active Directory-Standorte und -Dienste* zum Arbeiten mit Instanzen

Wie bei den anderen Active Directory-Tools können Sie AD LDS-Instanzen mit der Konsole *Active Directory-Standorte und -Dienste* verwalten. Zuvor müssen Sie allerdings die Datei *MS-ADLDS-DisplaySpecifiers.ldf* importieren, um das Schema der Instanz für die Unterstützung der entsprechenden Objekte zu aktualisieren. Das müssen Sie für jede Instanz erledigen, die Sie in dieser Konsole verwalten wollen. Führen Sie dazu die folgenden Schritte durch:

1. Fügen Sie, falls noch nicht geschehen, die LDIF-Datei zu Ihrer Instanz hinzu. Öffnen Sie dazu eine Eingabeaufforderung mit erhöhten Rechten.
2. Wechseln Sie zum Ordner *%SystemRoot%\ADAM*, in dem Sie **cd \windows\adam** eingeben.
3. Importieren Sie die LDIF-Datei in die Instanz:

   ```
   ldifde -i -f MS-ADLDS-DisplaySpecifiers.ldf -s <Servername>:<Portnummer> -m
      -a <Benutzername> <Domänenname> <Kennwort>
   ```

4. Schließen Sie die Eingabeaufforderung.
5. Öffnen Sie die Konsole *Active Directory-Standorte und -Dienste* über die Programmgruppe *Verwaltung*.
6. Die Konsole stellt standardmäßig eine Bindung zum Verzeichnis der Active Directory-Domänendienste her. Um eine Bindung zu einer AD LDS-Instanz herzustellen, klicken Sie mit der rechten Maustaste im Strukturbereich auf *Active Directory-Standorte und -Dienste* und wählen *Domänencontroller ändern* aus.
7. Wählen Sie im Dialogfeld *Verzeichnisserver ändern* die Option *Bestimmter Domänencontroller oder AD LDS-Instanz* aus, klicken Sie auf *<Verzeichnisservername[:port] hier eingeben>*, geben Sie den Servernamen, einen Doppelpunkt und die Portnummer ein, und drücken Sie die EINGABETASTE. Klicken Sie auf *OK*.
8. Klicken Sie im Warndialogfeld auf *Ja*, um die Server zu ändern.

Sie können nun mit den Replikationsparametern für die Instanz arbeiten. Beachten Sie, dass der Server im Format *Servername$Instanzname* angegeben ist, um zu verdeutlichen, dass es sich nicht um einen Domänencontroller handelt.

Weitere Informationen AD LDS-Tools und -Instanzen

Weitere Informationen zu AD LDS-Tools und -Instanzen finden Sie unter *http://technet.microsoft.com/de-de/library/cc770639(WS.10).aspx*.

Prüfungstipp

Denken Sie daran, dass Sie unter Server Core keine grafischen Programme nutzen können. Verwenden Sie die grafischen Programme auf einer vollständigen Windows-Installation oder auf einem Clientsystem, auf dem die Remoteserver-Verwaltungstools ausgeführt werden, um die Instanzen in Server Core-Installationen zu verwalten.

Das Arbeiten mit AD LDS-Instanzen erfordert Sorgfalt und Aufmerksamkeit, da nahezu jede Aktivität entweder über die Befehlszeile oder unter Verwendung definierter Namen erfolgt. Wie Sie bei der Arbeit mit den AD DS gesehen haben, sind Tippfehler der Fluch eines jeden Administrators, der mit diesen Tools arbeitet. Dasselbe gilt für die AD LDS. Prüfen Sie alle Angaben sehr sorgfältig, bevor Sie einen Befehl ausführen oder ein Objekt unter Verwendung seines definierten Namens erstellen oder verwalten.

Verwenden von *Active Directory-Modul für Windows PowerShell* zum Arbeiten mit Instanzen

Sie können auch Windows PowerShell einsetzen, um die AD LDS-Administration durchzuführen oder zu automatisieren. Die AD LDS-Administration mit PowerShell ähnelt der AD DS-Administration mit demselben Tool. Es stehen viele derselben Cmdlets zur Verfügung. Gehen Sie folgendermaßen vor, um AD LDS mit PowerShell zu verwalten:

1. Starten Sie Windows PowerShell. Öffnen Sie dazu *Active Directory-Modul für Windows PowerShell* aus der Programmgruppe *Verwaltung*.
2. Sie können nun auf eine AD LDS-Instanz zugreifen und verschiedene Operationen ausführen. Das sind zum Beispiel:
   - Informationen aus einer AD LDS-Instanz abrufen:

     ```
     Get-ADGroupMember -identity '<DN der Gruppe>' -server '<Servername>:<Port>'
        -partition '<DN der Partition>' |
        FT Name,DistinguishedName -A
     ```

     Dieser Befehl liefert eine Liste aller Mitglieder einer bestimmten Gruppe innerhalb der Instanz. Denken Sie daran, dass Sie den Namen der Gruppe, den Servernamen und den Port für die AD LDS-Instanz sowie den Namen der Partition angeben müssen, in der die Gruppe liegt. Beachten Sie außerdem, dass alle Namen definierte Namen sind.
   - Objekte innerhalb einer AD LDS-Instanz erstellen:

     ```
     New-ADUser -name '<Benutzername>' -DisplayName '<Anzeigename>'
        -server '<Servername>:<Port>'
        -path '<DN des Pfads, in dem der Benutzer liegt>'
     ```

Dieser Befehl erstellt einen neuen Benutzer an einem bestimmten Ort innerhalb einer AD LDS-Instanz. Sie müssen den Namen des Benutzers, den Anzeigenamen für den Benutzer, den Servernamen und den Port für die AD LDS-Instanz sowie den Namen des Orts für den Benutzer angeben. Alle Namen sind definierte Namen.

- Objekte aus einer AD LDS-Instanz entfernen:

```
Remove-ADUser -identity '<Benutzername>' -server '<servername>:<port>'
   -path '<DN des Pfads, in dem der Benutzer liegt>'
```

Dieser Befehl entfernt einen Benutzer aus dem angegebenen Ort innerhalb einer AD LDS-Instanz. Sie müssen den Namen des Benutzers, den Servernamen und den Port für die AD LDS-Instanz sowie den Namen des Orts für den Benutzer angeben. Alle Namen sind definierte Namen.

Wie Sie sehen, können Sie viele der AD DS-PowerShell-Cmdlets verwenden, um mit AD LDS-Instanzen zu arbeiten. Der größte Unterschied besteht darin, dass Sie den Pfad der Instanz (Servername und Portnummer) angeben müssen, um mit PowerShell darauf zuzugreifen.

Übung Arbeiten mit AD LDS-Instanzen

In dieser Übung erstellen Sie Ihre erste AD LDS-Instanz sowie ein Replikat. Anschließend verwalten Sie die Replikation zwischen den beiden Instanzen. Zu diesem Zweck benötigen Sie die beiden im Abschnitt »Bevor Sie beginnen« in diesem Kapitel angegebenen Server.

▶ Übung 1 Erstellen einer AD LDS-Instanz

In dieser Übung erstellen Sie Ihre erste AD LDS-Instanz. Wie im Abschnitt »Bevor Sie beginnen« in diesem Kapitel angegeben, haben Sie zuvor den AD LDS-Dienst auf beiden Mitgliedsservern installiert. Sie arbeiten in dieser Übung mit den Werten in Tabelle 14.5.

Tabelle 14.5 Werte für die Erstellung der Instanz

Element	Wert
Instanzname	*ADLDSInstanz*
Ports	50004 für LDAP 50005 für Secure LDAP
Name der Anwendungspartition	*CN=ADLDSInstanz,dc=contoso,dc=com*
Datenpfade	*D:\ADLDS\ADLDSInstanz\Data*
Dienstkonto	*NETZWERKDIENST*
Verwaltungskonto	*CONTOSO\Administrator*
Zu importierende LDIF-Dateien	*MS-AdamSyncMetadata.ldf* *MS-ADLDS-DisplaySpecifiers.ldf* *MS-AZMan.ldf* *MS-InetOrgPerson.ldf* *MS-User.ldf* *MS-UserProxy.ldf* *MS-UserProxyFull.ldf*

Füllen Sie am besten stets eine Tabelle ähnlich wie Tabelle 14.5 aus, wenn Sie eine neue AD LDS-Instanz erstellen. Da es auf einem Server mehrere AD LDS-Instanzen geben kann, empfiehlt es sich, jede einzeln zu dokumentieren.

1. Vergewissern Sie sich, dass der Domänencontroller *SERVER01.contoso.com* und die Mitgliedsserver *SERVER03.contoso.com* und *SERVER04.contoso.com* ausgeführt werden.
2. Melden Sie sich an *SERVER03.contoso.com* mit dem Domänenadministratorkonto an.

   Denken Sie daran, dass Sie in Produktivumgebungen nur lokale Administratorrechte für das Arbeiten mit den AD LDS benötigen.
3. Öffnen Sie über die Programmgruppe *Verwaltung* den Setup-Assistenten für Active Directory Lightweight Directory Services.
4. Lesen Sie die Informationen auf der Begrüßungsseite und klicken Sie auf *Weiter*.
5. Aktivieren Sie auf der Seite *Setupoptionen* die Option *Eine eindeutige Instanz installieren* und klicken Sie auf *Weiter*.
6. Geben Sie auf der Seite *Instanzname* den Namen **ADLDSInstanz** ein und klicken Sie auf *Weiter*.

   Beim Benennen der Instanz benennen Sie auch den Dienst, der diese Instanz ausführen wird. Dieser Name lautet *ADAM_<Instanzname>*, doch der in der Konsole *Dienste* angezeigte Name lautet nur *<Instanzname>*.
7. Geben Sie auf der Seite *Anschlüsse* die Ports für die Kommunikation mit dieser Instanz ein. Geben Sie **50004** für LDAP und **50005** für Secure LDAP ein. Klicken Sie auf *Weiter*.
8. Wählen Sie auf der Seite *Anwendungsverzeichnispartition* die Option *Ja, eine Anwendungsverzeichnispartition erstellen*. Geben Sie den Namen der Anwendungspartition ein, in diesem Fall **CN=ADLDSInstanz,dc=contoso,dc=com**, und klicken Sie auf *Weiter*.

   Sie müssen stets einen definierten Namen angeben.
9. Ändern Sie auf der Seite *Speicherort* die Pfade in *D:\ADLDS\ADLDSInstanz\Data* und klicken Sie auf *Weiter*.

   Da es sich um einen Verzeichnisspeicher handelt, sollte er auf einem vom Betriebssystem getrennten Datenträger abgelegt werden, zum Beispiel auf Laufwerk D. Sie können auch getrennte Unterordner für die Datendateien und die Datenwiederherstellungsdateien verwenden.
10. Wählen Sie auf der Seite *Dienstkontoauswahl* die Option *Netzwerkdienstkonto* aus und klicken Sie auf *Weiter*.

    Microsoft Windows wählt standardmäßig das Konto *NETZWERKDIENST* aus. Dieses Konto hat begrenzte lokale Zugriffsrechte und ist geschützt. Sie sollten normalerweise ein ordnungsgemäßes Dienstkonto verwenden, doch für den Zweck dieser Übung ist *NETZWERKDIENST* ausreichend.
11. Wählen Sie auf der Seite *AD LDS-Administratoren* die Option *Zurzeit angemeldeter Benutzer* aus und klicken Sie auf *Weiter*.

    Sie sollten normalerweise eine vorbereitete Gruppe verwenden, doch für den Zweck dieser Übung ist das Konto *Administrator* ausreichend.

12. Wählen Sie auf der Seite *Importieren von LDIF-Dateien* alle aufgeführten LDIF-Dateien aus und klicken Sie auf *Weiter*.
13. Prüfen Sie auf der Seite *Installationsbereit* die gewählten Installationsoptionen und klicken Sie auf *Weiter*.

    Die neue AD LDS-Instanz wird installiert.
14. Klicken Sie auf *Fertig stellen*.

    Sie haben soeben Ihre erste Instanz erstellt. Öffnen Sie den Server-Manager und erweitern Sie den Knoten *Rollen\Active Directory Lightweight Directory Services*, um die entsprechenden Ergebnisse anzuzeigen.

    Die AD LDS generieren während der Erstellung der Instanz Protokolldateien. Diese Dateien befinden sich im Ordner *%SystemRoot%\Debug* und haben die Namen *ADAM-Setup.log* und *ADAMSetup_loader.log*. Sie können diese Dateien überprüfen, um während der Erstellung der Instanz aufgetretene Probleme zu suchen und zu beheben. Außerdem wird beim Erstellen einer Instanz ein Dienst für die Instanz eingerichtet. Sie können in der Programmgruppe *Verwaltung* die Konsole *Dienste* öffnen, um das Vorhandensein dieses Dienstes zu bestätigen.

▶ Übung 2 Erstellen eines Replikats einer AD LDS-Instanz

In dieser Übung erstellen Sie Ihr erstes Replikat einer AD LDS-Instanz, und zwar auf dem zweiten eingerichteten Mitgliedsserver.

1. Vergewissern Sie sich, dass der Domänencontroller *SERVER01.contoso.com* und die Mitgliedsserver *SERVER03.contoso.com* und *SERVER04.contoso.com* laufen.
2. Melden Sie sich an *SERVER04.contoso.com* mit dem Domänenadministratorkonto an.
3. Öffnen Sie über die Programmgruppe *Verwaltung* den Setup-Assistenten für Active Directory Lightweight Directory Services.
4. Lesen Sie die Informationen auf der Begrüßungsseite und klicken Sie auf *Weiter*.
5. Wählen Sie unter *Setupoptionen* die Option *Ein Replikat einer vorhandenen Instanz installieren* aus und klicken Sie auf *Weiter*.
6. Geben Sie auf der Seite *Instanzname* den Namen **ADLDSInstanz** ein und klicken Sie auf *Weiter*.
7. Geben Sie auf der Seite *Anschlüsse* die Ports für die Kommunikation mit dieser Instanz ein. Geben Sie **50004** für LDAP und **50005** für Secure LDAP ein. Klicken Sie auf *Weiter*.
8. Klicken Sie auf der Seite *Einem Konfigurationssatz beitreten* neben *Server* auf *Durchsuchen*, um *Server03* zu suchen. Geben Sie **SERVER03** ein und klicken Sie dann auf *Namen überprüfen*. Klicken Sie auf *OK* und geben Sie **50004** in das Feld *LDAP-Port* ein. Klicken Sie auf *Weiter*.
9. Wählen Sie auf der Seite *Administratorberechtigungen für den Konfigurationssatz* die Option *Zurzeit angemeldeter Benutzer* aus und klicken Sie auf *Weiter*.

    Sie sollten normalerweise eine Gruppe verwenden, doch für den Zweck dieser Übung ist das Konto *Administrator* ausreichend.
10. Wählen Sie auf der Seite *Kopieren von Anwendungsverzeichnispartitionen* die Partition *CN=ADLDSInstanz,dc=contoso,dc=com* aus und klicken Sie auf *Weiter*.

11. Ändern Sie auf der Seite *Speicherort* die Pfade in *D:\ADLDS\ADLDSInstanz\Data* und klicken Sie auf *Weiter*.
12. Wählen Sie auf der Seite *Dienstkontoauswahl* die Option *Netzwerkdienstkonto* aus und klicken Sie auf *Weiter*.

    Sie sollten normalerweise ein ordnungsgemäßes Dienstkonto verwenden, doch für den Zweck dieser Übung ist *NETZWERKDIENST* ausreichend.
13. Wählen Sie auf der Seite *AD LDS-Administratoren* die Option *Zurzeit angemeldeter Benutzer* aus und klicken Sie auf *Weiter*.

    Sie sollten normalerweise eine Gruppe verwenden, doch für den Zweck dieser Übung ist das Konto *Administrator* ausreichend.
14. Prüfen Sie auf der Seite *Installationsbereit* die gewählten Installationsoptionen und klicken Sie auf *Weiter*.

    Die neue AD LDS-Instanz wird installiert.
15. Klicken Sie auf *Fertig stellen*.

    Sie haben soeben das Replikat erstellt.

▶ Übung 3 Verwalten der Replikation zwischen AD LDS-Replikaten

In dieser Übung zeigen Sie die Replikationsparameter zwischen Ihren beiden Instanzen an. Sie müssen die Instanzen nicht für die Unterstützung von *Active Directory-Standorte- und Dienste*-Objekten aktualisieren, da Sie beim Erstellen der Quellinstanz in der Übung 1 alle LDIF-Dateien importiert haben.

1. Vergewissern Sie sich, dass der Domänencontroller *SERVER01.contoso.com* und die Mitgliedsserver *SERVER03.contoso.com* und *SERVER04.contoso.com* laufen.
2. Melden Sie sich an *SERVER04.contoso.com* mit dem Domänenadministratorkonto an.
3. Öffnen Sie die Konsole *Active Directory-Standorte und -Dienste* über die Programmgruppe *Verwaltung*.

    Die Konsole stellt standardmäßig eine Bindung zum Verzeichnis der Active Directory-Domänendienste her.
4. Um eine Bindung zu einer AD LDS-Instanz herzustellen, klicken Sie mit der rechten Maustaste im Strukturbereich auf *Active Directory-Standorte und -Dienste* und wählen *Domänencontroller ändern* aus.
5. Wählen Sie im Dialogfeld *Verzeichnisserver ändern* die Option *Bestimmter Domänencontroller oder AD LDS-Instanz* aus, klicken Sie auf *<Verzeichnisservername[:port] hier eingeben>*, geben Sie **SERVER03:50004** ein, und drücken Sie die EINGABETASTE. Klicken Sie auf *OK*.
6. Klicken Sie im Warndialogfeld auf *Ja*, um die Server zu ändern.
7. Blenden Sie nun die Struktur von *Active Directory-Standorte und -Dienste* vollständig ein. Drücken Sie dazu mehrmals die Sternchentaste (*) auf der Zehnertastatur. Dadurch wird die Replikationsstruktur für diese Instanz angezeigt.

    Nun erstellen Sie einen neuen Standort, an den Sie eines der Instanzobjekte verschieben.
8. Klicken Sie mit der rechten Maustaste im Strukturbereich auf *Sites* und wählen Sie den Befehl *Neuer Standort*.

9. Nennen Sie den Standort **Replikation01**, wählen Sie das Objekt *DEFAULTIPSITELINK* aus und klicken Sie auf *OK*.

   Die neue Standortverknüpfung wurde erstellt. Im Dialogfeld *Active Directory-Standorte und -Dienste* werden die nächsten auszuführenden Schritte aufgeführt (Abbildung 14.5).

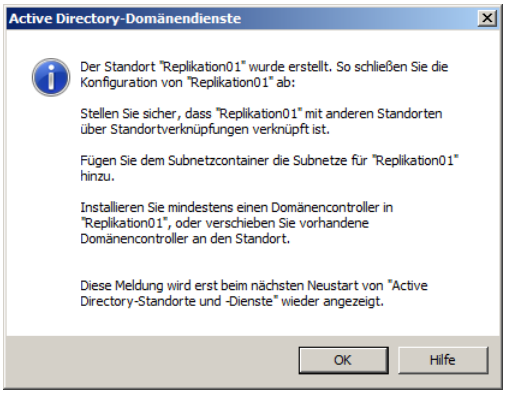

Abbildung 14.5 Zum Erstellen einer Replikationspartnerschaft auszuführende Aufgaben

10. Klicken Sie auf *OK*, um das Dialogfeld zu schließen.

    In diesem Fall führen Sie nicht alle Aktivitäten aus. Sie verschieben nur *SERVER04* zur neuen Standortverknüpfung.
11. Erweitern Sie den Knoten *Replikation01*.
12. Klicken Sie unter *Default-First-Site-Name* auf *SERVER04$ADLDSInstanz* und ziehen Sie diesen Knoten in den Container *Servers* unter *Replikation01*.
13. Klicken Sie im Warnfeld zum Verschieben von Objekten auf *Ja*, um das Objekt zu verschieben. Das Objekt wird nun unter dem Standort *Replikation01* angezeigt.

In dieser Übung wurde das Arbeiten mit Instanzen und das Steuern der Replikation demonstriert. In der Praxis müssen Sie alle in Abbildung 14.5 angegebenen Aufgaben ausführen, um eine ordnungsgemäße Replikationspartnerschaft einzurichten.

Weitere Informationen AD LDS-Replikation

Weitere Informationen zur AD LDS-Replikation finden Sie unter *http://technet.microsoft.com/de-de/library/cc731246(WS.10).aspx*.

Zusammenfassung der Lektion

- Die Tools zum Steuern von AD LDS-Instanzen entsprechen nahezu den für die AD DS verwendeten Tools. In Tabelle 14.3 finden Sie eine vollständige Liste der Tools, mit denen Sie AD LDS-Instanzen verwalten können.
- Sie können Instanzen sowohl auf der grafischen Benutzeroberfläche über den Setup-Assistenten für Active Directory Lightweight Directory Services AD LDS als auch über die Befehlszeile mit dem Befehl *ADAMInstall.exe* erstellen. In beiden Fällen müssen Sie im Vorfeld alle Voraussetzungen für die Instanz erfüllen. Bei Verwenden des Programms

ADAMInstall.exe müssen Sie im Voraus eine Antwortdatei mit den entsprechenden Werten vorbereiten.

- Das Arbeiten mit AD LDS-Instanzen ist mit der Angabe definierter Namen verbunden. Definierte Namen nutzen eine hierarchische Struktur, die der hierarchischen Struktur von AD DS-Gesamtstrukturen ähnelt.
- Das Arbeiten mit AD LDS-Instanzen ist mit der Angabe von Servernamen und Portnummern verbunden. Es empfiehlt sich stets, alle für die erstellten Instanzen gewählten Werte zu notieren, so auch Servernamen und Portnummern.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen aus Lektion 2, »Konfigurieren und Verwenden der AD LDS«, testen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.

Hinweis Die Antworten

Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Buchs.

1. Sie sind ein lokaler Serveradministrator für *contoso.com*. Eine Ihrer Aufgaben ist das Verwalten von AD LDS-Instanzen auf *SERVER03*. Vor Kurzem haben Sie vier Instanzen auf *SERVER03* installiert, einem Mitgliedsserver in Ihrer Domäne. Sie haben dabei mit den Standardeinstellungen für die Portauswahl für jede Instanz begonnen. Nun müssen Sie das Schema der erstellten installierten Instanz (*Instanz1*) ändern. Sie registrieren das Snap-In *Active Directory-Schema* auf dem Server und erstellen die benutzerdefinierte Konsole *Active Directory-Schema*. Wenn Sie versuchen, eine Verbindung zum Schema der ersten Instanz herzustellen, wird jedoch immer wieder eine Fehlermeldung angezeigt. Was ist wahrscheinlich die Ursache des Problems?
   A. *Instanz1* enthält kein Schema, das Sie bearbeiten könnten.
   B. Sie können das Schema einer Instanz nicht mit dem Snap-In *Active Directory-Schema* ändern. Sie müssen dazu den Befehl *LDP.exe* ausführen.
   C. Sie können das Schema einer Instanz nicht mit dem Snap-In *Active Directory-Schema* ändern. Das Ändern des Schemas einer Instanz erfolgt durch Importieren von LDIF-Dateien über den Befehl *LDIFDE.exe*.
   D. Sie können über das Snap-In *Active Directory-Schema* keine Verbindung zur Instanz herstellen, da sie standardmäßig denselben Port wie Ihr AD DS-Verzeichnis verwendet.

Rückblick auf dieses Kapitel

Um die in diesem Kapitel vermittelten Kenntnisse weiter zu vertiefen, können Sie die folgenden Aufgaben ausführen:

- Lesen Sie die Zusammenfassung des Kapitels sorgfältig durch.
- Lesen Sie die Liste der Schlüsselbegriffe durch, die in diesem Kapitel eingeführt wurden.
- Arbeiten Sie die Übung mit Fallbeispiel durch. Diese Szenarien beschreiben Fälle aus der Praxis, in denen die Themen dieses Kapitels zur Anwendung kommen. Sie werden aufgefordert, eine Lösung zu entwickeln.
- Führen Sie die vorgeschlagenen Übungen durch.
- Machen Sie einen Übungstest.

Zusammenfassung des Kapitels

- Wie der Name andeutet, sind die AD LDS ein überaus flexibler Verzeichnisdienst. Die AD LDS sollten stets zuerst in Erwägung gezogen werden, wenn Sie mit einer Änderung des Schemas Ihres Netzwerkbetriebssystems, den AD DS, konfrontiert sind. Sollte es möglich sein, eine Anwendung über die AD LDS anstatt über die AD DS zu integrieren, verwenden Sie die AD LDS. Es gibt allerdings Situationen, in denen Sie die AD DS nicht durch die AD LDS ersetzen können.
- Die AD LDS können unter der vollständigen Installation und der Server Core-Installation von Windows Server 2008 R2 ausgeführt werden. Aufgrund ihrer »abgespeckten« Natur eignen sich die AD LDS sehr gut für eine Virtualisierung per Hyper-V.
- Die AD DS und AD LDS haben denselben Installationsprozess. Beginnen Sie mit der Installation der Rolle und erstellen Sie anschließend über einen benutzerdefinierten Assistenten oder unbeaufsichtigten Setupprozess die Verzeichnisdienstinstanz. Um die AD LDS zu entfernen, müssen Sie zuerst die erstellten Instanzen und anschließend die Rolle vom Server entfernen.
- Nachdem Sie die AD LDS installiert haben, können Sie sie zum Speichern verzeichnisbezogener Daten verschiedener Anwendungen einsetzen. Machen Sie sich zuerst mit den AD LDS-Tools vertraut. Im Anschluss können Sie beginnen, die ersten Instanzen zu erstellen. Nachdem Sie Instanzen erstellt haben, können Sie sie absichern, um ihren ordnungsgemäßen Schutz sicherzustellen. Im nächsten Schritt erstellen Sie Replikate dieser Instanzen, damit Sie sie auf verschiedenen anderen Systemen installieren können, und steuern die Replikation, damit Instanzen auf verschiedenen Computern mithilfe der Multimasterreplikation aktualisiert werden können.

Schlüsselbegriffe

Die folgenden Begriffe wurden in diesem Kapitel neu eingeführt. Wissen Sie, was sie bedeuten?

- Anwendungspartitionen
- Instanzen

Übung mit Fallbeispiel

In der folgenden Übung mit Fallbeispiel wenden Sie das Gelernte zu den Active Directory Lightweight Directory Services an. Antworten zu den gestellten Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Buchs.

Übung mit Fallbeispiel: Bestimmen der Voraussetzungen für AD LDS-Instanzen

Contoso hat bislang mit mehreren benutzerdefinierten Anwendungen gearbeitet, die eigene Informationsspeicher nutzen. Kürzlich hat sich die Contoso-Geschäftsführung für einen Wechsel zu den Active Directory-Domänendiensten und für eine Standardisierung basierend auf Windows Server 2008 R2-Technologien entschlossen. Nun sollen die Informationsspeicher in den bisherigen Anwendungen in Active Directory Lightweight Directory Services-Instanzen verschoben werden.

Das Unternehmen tritt an Sie als potenziellen Administrator der AD LDS im Unternehmen heran, um den Verantwortlichen bei der Beantwortung bestimmter Fragen zu den Voraussetzungen von Instanzen zu helfen. Folgende Fragen werden an Sie gerichtet:

1. Wo sollen die Dateien der einzelnen Instanzen gespeichert werden?
2. Wie sollen die einzelnen Instanzen benannt werden?
3. Welche Ports sollen zum Verbinden mit den Instanzen verwendet werden?
4. Müssen Anwendungsverzeichnispartitionen verwendet werden? Falls ja, warum?
5. Wie sollen die einzelnen Instanzen ausgeführt werden?

Vorgeschlagene Übungen

Führen Sie zur Vertiefung der in diesem Kapitel behandelten Prüfungsziele die folgenden Aufgaben aus.

Arbeiten mit AD LDS-Instanzen

Da es in diesem Thema nur ein Prüfungsziel gibt, konzentrieren Sie sich zur Vorbereitung auf die Prüfung auf drei Hauptaufgaben:

- Installieren der Serverrolle *Active Directory Lightweight Directory Services*
- Konfigurieren einer AD LDS-Instanz
- Zugreifen auf die AD LDS-Instanz über ihre Verwaltungstools

Führen Sie zu diesen Themen folgende Übungen aus:

- **Übung 1** Installieren Sie auf einem physischen oder virtuellen Server, auf dem entweder Windows Server 2008 R2 Standard Edition oder Windows Server 2008 R2 Enterprise Edition ausgeführt wird, die Serverrolle *Active Directory Lightweight Directory Services*. Der Server darf kein Domänencontroller sein, sondern muss ein Mitgliedsserver in einer Active Directory-Domänendienste-Domäne sein.
- **Übung 2** Erstellen Sie die AD LDS-Instanz *MeineADLDSInstanz*. Durchlaufen Sie zuerst die Vorbereitungen zum Erfüllen der Voraussetzungen einer AD LDS-Instanz, bevor Sie die Instanz erstellen. Wählen Sie für die Instanz die Ports 50.010 und 50.011.

Erstellen Sie in der Instanz eine Anwendungspartition und weisen Sie ihr ein Dienstkonto zu. Verwalten Sie die Instanz mithilfe einer AD DS-Sicherheitsgruppe und stellen Sie sicher, dass Ihr Konto zu dieser Gruppe gehört. Speichern Sie die Instanz auf einem vom Betriebssystem getrennten Datenlaufwerk. Importieren Sie beim Erstellen der Instanz alle LDIF-Dateien.

- **Übung 3** Üben Sie nach der Erstellung der Instanz das Verbinden und Arbeiten mit der Instanz. Arbeiten Sie mit den folgenden Tools:
  - Snap-In *Active Directory-Schema*
  - Snap-In *Active Directory-Standorte und -Dienste*
  - *LDP.exe*
  - ADSI-Editor
  - Windows PowerShell

  Mit diesen Tools können Sie die Instanz untersuchen und ihren Inhalt anzeigen. Sie können auch innerhalb der Instanz das Erstellen von Objekten üben. Erstellen Sie beispielsweise eine Organisationseinheit und fügen Sie eine Gruppe und einen Benutzer hinzu.

Machen Sie einen Übungstest

Die Übungstests (in englischer Sprache) auf der Begleit-CD zu diesem Buch bieten zahlreiche Möglichkeiten. Zum Beispiel können Sie einen Test machen, der ausschließlich die Themen aus einem Prüfungslernziel behandelt, oder Sie können sich selbst mit dem gesamten Inhalt der Prüfung 70-640 testen. Sie können den Test so konfigurieren, dass er dem Ablauf einer echten Prüfung entspricht, oder Sie können einen Lernmodus verwenden, in dem Sie sich nach dem Beantworten einer Frage jeweils sofort die richtige Antwort und Erklärungen ansehen können.

Weitere Informationen Übungstests

Einzelheiten zu allen Optionen, die bei den Übungstests zur Verfügung stehen, finden Sie im Abschnitt »So benutzen Sie die Übungstests« in der Einführung am Anfang dieses Buchs.