KAPITEL 5

Identitätsverbund und Zugriffslösungen

Windows Server 2016 bietet verschiedene Merkmale und Dienste an, mit denen Sie die Inhalte Ihrer Organisation auf sichere Weise den Benutzern in anderen Organisationen, Benutzern im Internet und Benutzern mit einem Azure AD-Konto (Microsoft Azure Active Directory) bereitstellen können. Dazu gehören die Active Directory-Verbunddienste, die Active Directory-Rechteverwaltungsdienste und der Webanwendungsproxy. Um Benutzern außerhalb Ihrer Organisation auf sichere Weise Zugriff auf Ihre Ressourcen zu gewähren, müssen Sie wissen, wie Sie diese Dienste bereitstellen und einrichten.

In diesem Kapitel behandelte Prüfungsziele:

- Installieren und Einrichten der Active Directory-Verbunddienste
- Verwenden des Webanwendungsproxys
- Installieren und Einrichten der Active Directory-Rechteverwaltungsdienste

Prüfungsziel 5.1: Installieren und Einrichten der Active Directory-Verbunddienste

Durch die Bereitstellung der Active Directory-Verbunddienste ermöglichen Sie Ihren Benutzern, sich mit einer einmaligen Anmeldung (Single Sign-On, SSO) für die Anwendungen und Dienste in Azure, die Netzwerkinfrastruktur Ihres Geschäftsstandorts oder das Netzwerk einer Partnerorganisation zu authentifizieren (abhängig von der Einrichtung).

Die Verbunddienste stützen sich auf Vertrauensbeziehungen, die Sie zwischen Organisationen einrichten, um die gemeinsame Nutzung von Ressourcen zu ermöglichen. Sie werden als *Verbundvertrauensstellungen* bezeichnet und können nach den geschäftlichen Bedürfnissen über die Grenzen von Gesamtstrukturen hinweg und zwischen Organisationen eingerichtet werden.

In jeder der Organisationen definiert der Administrator, welche Ressourcen über die Vertrauensstellung zugänglich sind und wer Zugriff auf sie hat.

PRÜFUNGSTIPP

Verbundvertrauensstellungen haben nichts mit Gesamtstrukturvertrauensstellungen in AD DS zu tun. Es ist auch nicht erforderlich, dass die Verbunddienstserver der Organisationen direkt miteinander kommunizieren.

Nehmen Sie als Beispiel an, die Mitarbeiter eines Theaters wollen die Kartenverkäufe für eine kommende Vorstellung einsehen, die von einer externen Organisation abgewickelt werden. Der Netzwerkadministrator des Theaters muss dazu alle Benutzerkonten, die Zugriff auf diese Informationen benötigen, in eine Gruppe stellen, und der Administrator des Kartenverkäufers muss dieser Gruppe über die Vertrauensstellung den erforderlichen Zugriff auf die Verkaufsdatenbank gewähren. Dabei muss der Administrator des Kartenverkäufers dafür sorgen, dass lediglich die entsprechenden Mitarbeiter des Theaters Zugriff auf die Kartendaten für ihr Theater und auf keine anderen erhalten.

Bei der Einrichtung von Verbundvertrauensstellungen ist es wichtig, dass sich jede der Parteien darüber im Klaren ist, wie die Benutzeridentitäten verwendet werden. Insbesondere muss ihnen bekannt sein, welche Arten von Anmeldeinformationen erforderlich sind und wie sie gespeichert und genutzt werden. Des Weiteren müssen alle beteiligten Organisationen eine Richtlinie festlegen, um die Vertraulichkeit von Daten zu gewährleisten, die nicht über die Vertrauensstellung bereitgestellt werden sollen.

WEITERE INFORMATIONEN **Überblick über Active Directory-Verbunddienste**

Weitere Informationen über Active Directory-Verbunddienste finden Sie auf der Microsoft TechNet-Website unter:

https://technet.microsoft.com/library/hh831502(v=ws.11).aspx

Inhalt dieses Abschnitts:

- Überprüfen der Voraussetzungen für Verbunddienste
- Installieren der Verbunddienste
- Einrichten der Verbunddienste
- Einrichten der anspruchsgestützten Authentifizierung
- Einrichten von Authentifizierungsrichtlinien
- Einrichten der Geräteregistrierung
- Einrichtung zur Verwendung von Microsoft Azure und Microsoft Office 365
- Einrichten der Verbunddienste zur Authentifizierung von Benutzern in LDAP-Verzeichnissen
- Aktualisieren und Migrieren von früheren Verbunddienst-Bereitstellungen auf Windows Server 2016

Überprüfen der Voraussetzungen für Verbunddienste

Zur Einrichtung von Verbünden gibt es in Windows Server 2016 die Serverrolle *Active Directory-Verbunddienste* (Active Directory Federation Services, AD FS) mit folgenden Komponenten:

- **Verbundserver** Jede Partei benötigt mindestens einen Verbundserver. Diese Komponente stellt das Herz der Verbunddienste dar und ist für die Ausgabe und Überprüfung von Identitätsansprüchen zuständig.
- **Webanwendungsproxy** Diese Komponente ist optional. Sie wird gewöhnlich in einem Umkreisnetzwerk bereitgestellt, wo sie als Webproxy sowie als umgekehrter Webproxy für die Verbunddienste fungiert. In der letztgenannten Rolle wird sie als Verbundproxy bezeichnet.

PRÜFUNGSTIPP

Der Webanwendungsproxy wird als Rollendienst der Serverrolle *Remotezugriff* installiert.

- **Ansprüche** Eine vertrauenswürdige Partei in einer Verbundvertrauensstellung macht eine Aussage über einen Sicherheitsprinzipal, z. B. einen Benutzer, die zur Authentifizierung über die Vertrauensstellung genutzt wird. Dieser Anspruch kann ein oder mehrere Attribute des Objekts enthalten, z. B. den Benutzernamen oder die Abteilung.
- **Anspruchsregeln** Die vertrauende Partei verwendet Anspruchsregeln, um zu bestimmen, wie sie Ansprüche verarbeiten soll. Beispielsweise kann eine Anspruchsregel besagen, dass ein Benutzerprinzipalname (User Principal Name, UPN) ein gültiger Anspruch ist.
- **Anspruchsanbieter** Ein Anspruchsanbieter ist eine Komponente der vertrauenswürdigen Partei. Sie ist für die Verwaltung der Benutzerauthentifizierung und die Ausgabe von Ansprüchen zuständig, die den Benutzer darstellen.
- **Anspruchsanbieter-Vertrauensstellung** Legt die Regeln dafür fest, wann ein Client Ansprüche von einem Anspruchsanbieter anfordern kann, die der Client dann an eine vertrauende Partei überträgt.
- **Attributspeicher** Ein Attributspeicher, etwa AD DS, enthält Anspruchswerte. Einfach ausgedrückt, handelt es sich um einen Verzeichnisdienst, der Benutzerobjekte mit geeigneten Eigenschaften wie UPNs oder E-Mail-Adressen enthält. AD DS ist die übliche Wahl bei der Bereitstellung der Verbunddienste, da jeder AD FS-Server Mitglied einer Domäne sein muss, weshalb AD DS als Attributspeicher gut zugänglich ist.

PRÜFUNGSTIPP

AD DS ist auf Ihren AD FS-Servern automatisch und ohne Einrichtung durch einen Administrator als Attributspeicher verfügbar.

- **Vertrauende Seiten** Die vertrauenden Seiten befinden sich am vertrauenden Ende der Verbundvertrauensstellung, also dem Ende mit der Ressource. Sie werden durch einen Webdienst bereitgestellt, in dem WIF (Windows Identity Foundation) installiert ist. Als Alternative zu WIF können vertrauende Seiten auch den anspruchsfähigen Agent AD FS 1.0 verwenden.

> ***WEITERE INFORMATIONEN*** **Windows Identity Foundation**
>
> Weitere Informationen über Windows Identity Foundation finden Sie auf der Microsoft MSDN-Website unter:
>
> *https://msdn.microsoft.com/library/ee748475.aspx*

- **Vertrauensstellung der vertrauenden Seite** Sie besteht aus Regeln und Bezeichnern und dient dazu, einer vertrauenden Seite Ansprüche bereitzustellen.
- **Zertifikate** In der AD FS-Architektur werden Zertifikate ausgiebig als Sicherheitsmaßnahme genutzt. AD FS-Server verwenden folgende Zertifikate:
  - Selbst signierte Zertifikate
  - Zertifikate von einer internen Zertifizierungsstelle
  - Zertifikate von einer externen Zertifizierungsstelle

  Unabhängig von der Art der verwendeten Zertifikate müssen ihnen alle kommunizierenden Seiten vertrauen. Bei der Einrichtung einer Verbundvertrauensstellung zwischen zwei getrennten Organisationen müssen Sie daher sehr wahrscheinlich eine PKI auf der Grundlage öffentlicher Zertifikate für die AD FS-Architektur einrichten.

> ***HINWEIS*** **Verwenden einer internen Zertifizierungsstelle**
>
> Wenn Sie AD FS ausschließlich in Ihrer eigenen Organisation nutzen, um eine einmalige Anmeldung für mehrere Webanwendungen zu ermöglichen, können Sie zur Bereitstellung und Verwaltung der erforderlichen Zertifikate eine interne Unternehmenszertifizierungsstelle verwenden. Die benötigten Zertifikate können Sie dann mithilfe von Gruppenrichtlinienobjekten bereitstellen.

Um sich klar zu machen, wozu die einzelnen Komponenten gut sind, betrachten Sie das folgende Beispiel. Die beiden Organisationen Adatum und Contoso möchten ihre Ressourcen gemeinsam nutzen. Insbesondere benötigt Adatum Zugriff auf eine Webanwendung von Contoso. Dazu stellt die IT-Abteilung AD FS und die entsprechenden Komponenten bereit. In diesem Beispiel ist Contoso die Organisation mit der Ressource und Adatum die mit den Konten. In der Terminologie der Verbunddienste handelt es sich bei Adatum also um einen Anspruchsanbieter und bei Contoso um die vertrauende Seite. In Abbildung 5–1 können Sie erkennen, dass der folgende Vorgang abläuft, wenn ein Benutzer aus Adatum versucht, auf die Webanwendung von Contoso zuzugreifen:

1. Ein Benutzer in Adatum öffnet im Internet Explorer eine Verbindung zum Webserver von Contoso. Die Webanwendung erkennt, dass der Benutzer nicht authentifiziert ist, und leitet den Client an den Verbundserver von Contoso weiter.
2. Der Clientcomputer sendet eine Anforderung an den Verbundserver von Contoso. Der Verbundserver erkennt, dass der Benutzer zu Adatum gehört. Jetzt leitet der Webserver den Client zum Verbundserver von Adatum weiter.
3. Der Client sendet eine Anforderung an den Verbundserver von Adatum.
4. Der Domänencontroller von Adatum authentifiziert den Benutzer und meldet diesen Erfolg an den Verbundserver von Adatum.
5. Der Verbundserver von Adatum erstellt einen Anspruch für den Benutzer. Dies geschieht auf der Grundlage der Regeln, die für den Verbundpartner definiert sind, also für Contoso. Anschließend sendet der Verbundserver den Anspruch an den Clientcomputer.
6. Der Clientcomputer sendet den Anspruch an den Verbundserver von Contoso.
7. Der Verbundserver von Contoso überprüft die Vertrauensstellung im Token und erstellt und signiert ein neues Token, das er an den Clientcomputer sendet.
8. Der Clientcomputer sendet das neue Token an den ursprünglichen Webserver.
9. Die Anwendung auf dem Webserver überprüft das Token und gewährt aufgrund des Anspruchs in dem Token Zugriff auf die Anwendung.

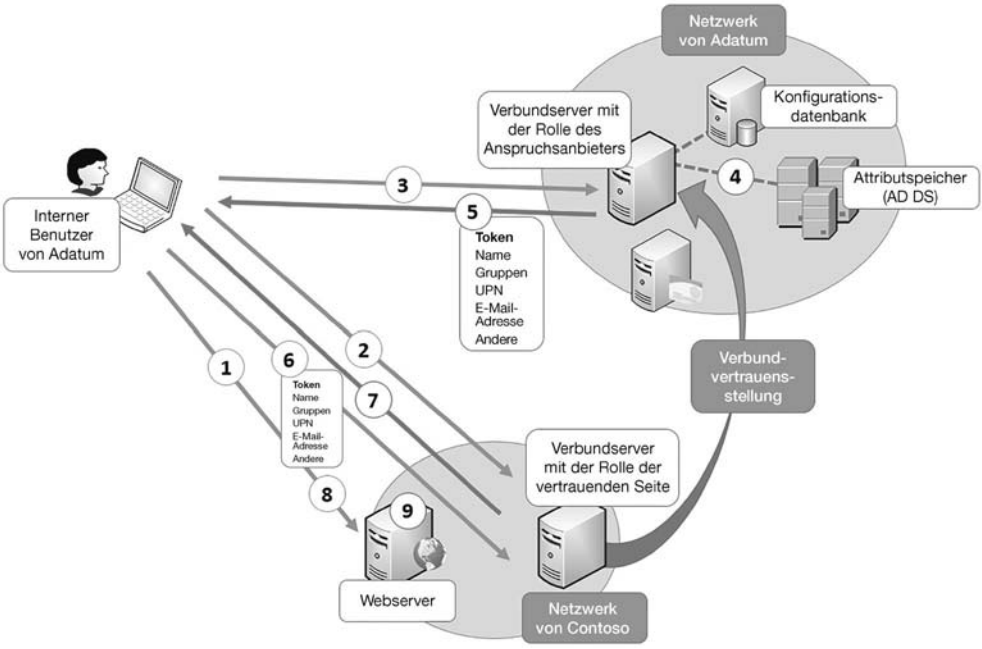

Abb. 5–1 Komponenten der Active Directory-Verbunddienste

Voraussetzungen für Active Directory-Verbunddienste

Damit Sie die Active Directory-Verbunddienste bereitstellen können, muss Ihre Netzwerkinfrastruktur die folgenden Voraussetzungen erfüllen:

- **Active Directory-Domänendienste** Alle Verbundserver müssen Mitglieder einer Domäne sein.
- **Attributspeicher** Enthält die Attribute von Sicherheitsprinzipalen.
- **Namensauflösung** Die Namensauflösung erfolgt durch DNS (Domain Name System). Interne Clientcomputer müssen den DNS-Namen des Verbundservers (oder der Serverfarm) auflösen können, externe Clientcomputer den Namen des Verbundproxys in ihrem Umkreisnetzwerk.
- **Netzwerk** Clientcomputer benötigen Netzwerkverbindungen zum Verbundserver oder Verbundproxy, Verbundserver brauchen Verbindungen zu Domänencontroller und der Verbundproxy muss eine Verbindung zum Verbundserver haben.

PRÜFUNGSTIPP

Die Kommunikation in den Verbunddiensten erfolgt über HTTPS (Hypertext Transfer Protocol über Secure Sockets Layer).

Installieren der Verbunddienste

Grundlage der Verbunddienste ist die Bereitstellung der Serverrolle *Active Directory-Verbunddienste*. Gehen Sie zu ihrer Installation wie folgt vor:

1. Melden Sie sich an einem Servercomputer in Ihrer Domäne als Mitglied der globalen Sicherheitsgruppe *Domänen-Admins* an.
2. Öffnen Sie den Server-Manager, klicken Sie auf *Verwalten* und dann auf *Rollen und Features hinzufügen*.
3. Aktivieren Sie in der Liste *Rollen* auf der Seite *Serverrollen auswählen* das Kontrollkästchen *Active Directory-Verbunddienste* und klicken Sie auf *Weiter* (siehe Abbildung 5–2).

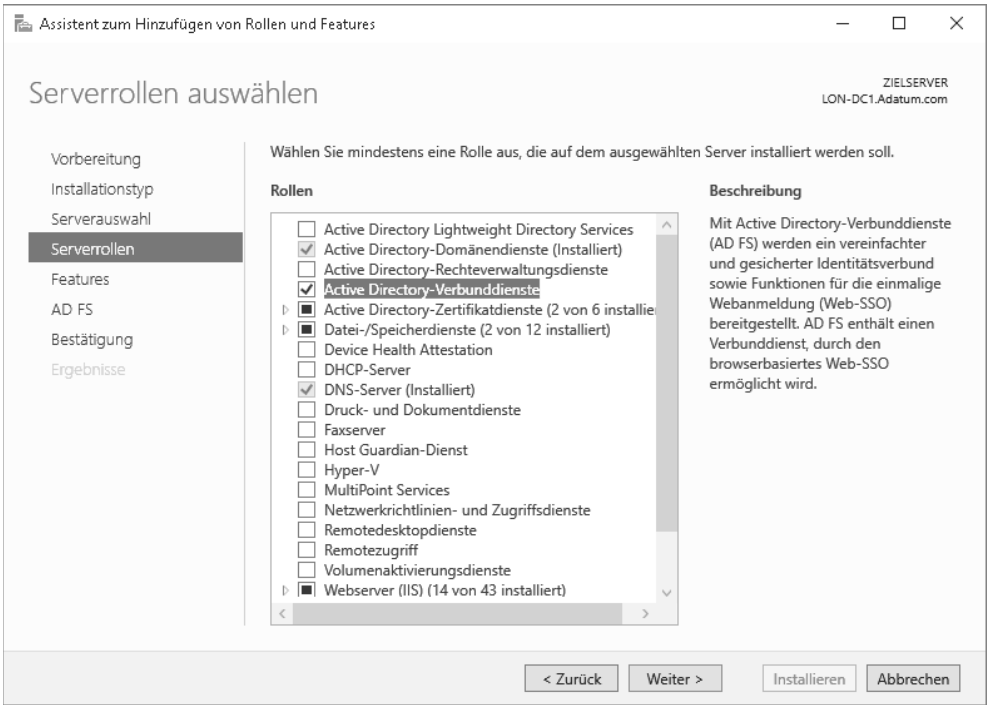

Abb. 5–2 Installieren der Serverrolle *Active Directory-Verbunddienste*

4. Klicken Sie sich durch den Rest des Assistenten und schließlich auf *Installieren*.
5. Klicken Sie nach Abschluss des Vorgangs auf *Schließen*.

Zur Installation der Active Directory-Verbunddienste können Sie auch das Windows PowerShell-Cmdlet `Install-WindowsFeatures` verwenden. Um die Serverrolle einschließlich aller Verwaltungswerkzeuge bereitzustellen, führen Sie folgenden Befehl aus:

```
Install-WindowsFeature -Name adfs-federation -IncludeManagementTools
```

Einrichten der Verbunddienste

Nachdem Sie die Serverrolle installiert haben, müssen Sie sie einrichten. Dazu müssen Sie das Dienstkonto, die Konfigurationsdatenbank, die Zertifikate und den Verzeichnisdienst angeben. Dazu gehen Sie folgendermaßen vor:

1. Klicken Sie im Server-Manager auf das Benachrichtigungssymbol und dann auf *Konfigurieren Sie den Verbunddienst auf diesem Server*.
2. Klicken Sie auf der Willkommensseite auf eine der beiden folgenden Optionen und dann auf *Weiter*:
   - *Erstellt den ersten Verbundserver in einer Verbundserverfarm*
   - *Fügt einer Verbundserverfarm einen Verbundserver hinzu*

3. Geben Sie auf der Seite *Mit Active Directory-Domänendiensten verbinden* die erforderlichen Anmeldeinformationen ein, gewöhnlich die eines Mitglieds der Gruppe *Domänen-Admins*. Klicken Sie auf *Weiter*.
4. Wählen Sie auf der Seite *Diensteigenschaften angeben* aus Abbildung 5–3 das geeignete SSL-Zertifikat, überprüfen Sie den Verbunddienstnamen und geben Sie den Anzeigenamen für die Verbunddienste ein. Klicken Sie auf *Weiter*.

> ***HINWEIS*** **Auswählen des Zertifikats**
>
> Der Verbunddienstname entspricht dem Namen des von Ihnen ausgewählten Zertifikats und sollte auch mit dem vollqualifizierten Domänennamen des Verbundservers identisch sein. Bevor Sie den Konfigurations-Assistenten für die Active Directory-Verbunddienste starten, müssen Sie das erforderliche Zertifikat mit dem entsprechenden Antragstellernamen installieren.

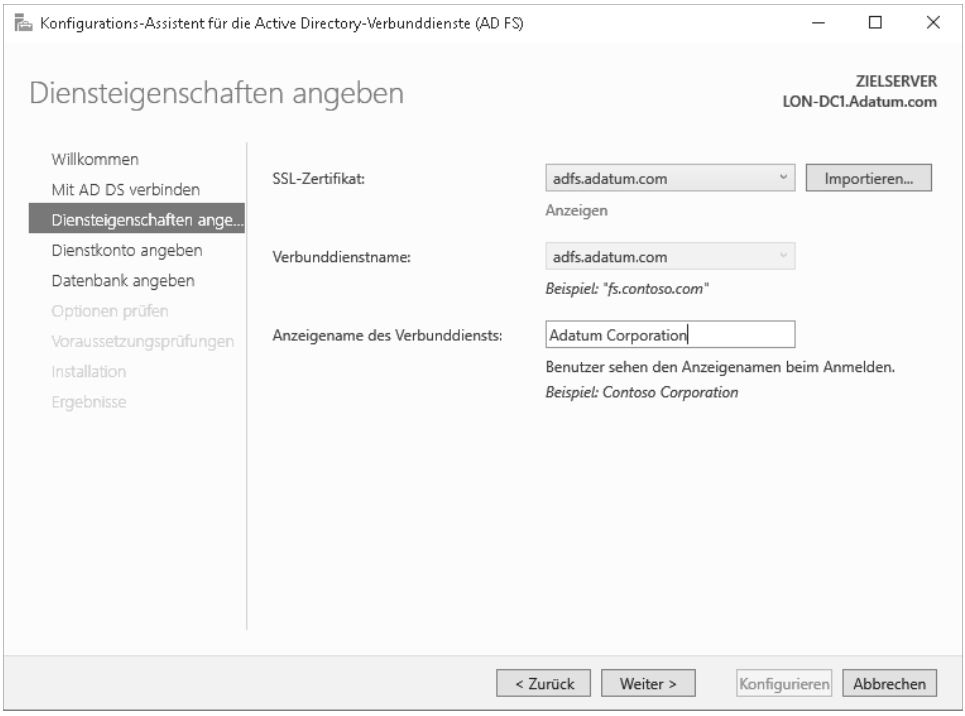

Abb. 5–3 Auswählen des Zertifikats und des Anzeigenamens für die Verbunddienste

5. Geben Sie auf der Seite *Dienstkonto angeben* aus Abbildung 5–4 ein geeignetes Dienstkonto an, am besten ein gruppenverwaltetes Dienstkonto. Klicken Sie danach auf *Weiter*.

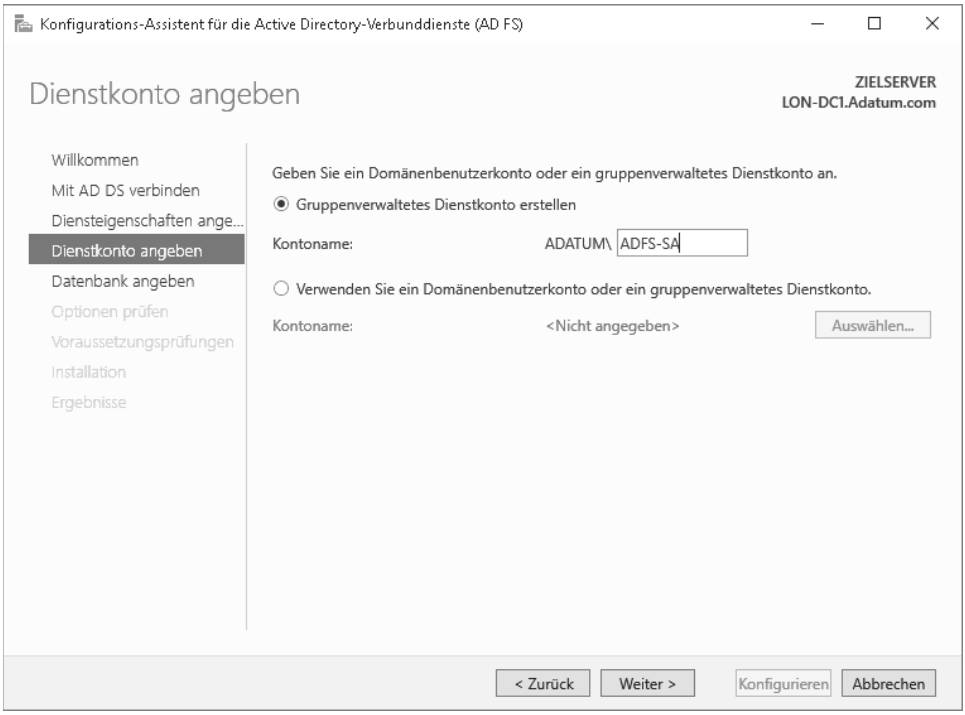

Abb. 5–4 Erstellen des Dienstkontos für die Verbunddienste

6. Behalten Sie auf der Seite *Konfigurationsdatenbank angeben* entweder die Standardauswahl der internen Windows-Datenbank bei oder aktivieren Sie die Option *Geben Sie den Ort einer SQL Server-Datenbank ein*. In letzterem Fall müssen Sie den Host- und den Instanznamen der Datenbank angeben. Klicken Sie anschließend auf *Weiter*.
7. Schauen Sie sich Ihre Auswahl auf der Seite *Optionen prüfen* noch einmal an und klicken Sie auf *Weiter*.
8. Die Voraussetzungen werden überprüft. Wenn sie erfüllt sind, klicken Sie auf *Konfigurieren*. Klicken Sie sich anschließend durch den Rest des Assistenten, um die Einrichtung abzuschließen.

Zur Einrichtung und Verwaltung der Verbunddienste können Sie auch das Windows PowerShell-Cmdlet `Install-ADFSFarm` verwenden. Um beispielsweise den ersten Server einer Verbundserverfarm in der Organisation *Adatum.com* bereitzustellen, führen Sie folgenden Befehl aus:

```
Install-AdfsFarm -CertificateThumbprint 8d4ece8e4397923563868d3f61b944103573a248
-FederationServiceName adfs.adatum.com -GroupServiceAccountIdentifier ADATUM\ADFS-SA
```

Um sich den Fingerabdruck des Zertifikats zu beschaffen, rufen Sie die Eigenschaften des betreffenden Zertifikats auf und kopieren den Wert in die Zwischenablage.

WEITERE INFORMATIONEN **Windows PowerShell-Cmdlets für Active Directory-Verbunddienste**

Weitere Informationen über die Einrichtung der Active Directory-Verbunddienste mithilfe der Windows PowerShell finden Sie auf der Microsoft TechNet-Website unter:

https://technet.microsoft.com/library/dn479343.aspx

Nach der Bereitstellung des Verbundservers müssen Sie ihn für eine oder beide der folgenden Funktionen einrichten:

- Anspruchsanbieter
- Vertrauende Seite

Wenn im B2B-Verkehr die Benutzerkonten einer Organisation auf Ressourcen in der anderen zugreifen müssen, richten Sie die Anspruchsanbieterfunktion in der Organisation mit den Konten ein und die Funktion der vertrauenden Seite in der Organisation mit der Ressource. Es ist aber auch möglich, Verbunddienste innerhalb einer einzigen Organisation bereitzustellen, sodass die Benutzer und die Ressourcen zur selben Organisation gehören. Daher kann ein einzelner Verbundserver sowohl als Anspruchsanbieter als auch als vertrauende Seite fungieren. Im nächsten Abschnitt sehen wir uns an, wie Sie den Anspruchsanbieter und die vertrauende Seite einrichten.

Einrichten der anspruchsgestützten Authentifizierung

Um die anspruchsgestützte Authentifizierung einzurichten, müssen Sie die beiden folgenden Ausgaben ausführen:

- Einrichten einer Anspruchsanbieter-Vertrauensstellung
- Einrichten einer Vertrauensstellung der vertrauenden Seite

Einrichten einer Anspruchsanbieter-Vertrauensstellung

Um eine Anspruchsanbieter-Vertrauensstellung einzurichten, führen Sie auf dem Verbundserver mit der Funktion des Anspruchsanbieters den folgenden Vorgang aus:

1. Klicken Sie im Server-Manager auf *Tools* und dann auf *AD FS-Verwaltung*.
2. Klicken Sie im Navigationsbereich der AD FS-Verwaltungskonsole auf *Anspruchsanbieter-Vertrauensstellungen*. Im Detailbereich wird das Standardobjekt *Active Directory* angezeigt.
3. Klicken Sie im Aktionsbereich unter *Active Directory* auf *Anspruchsregeln bearbeiten*.
4. Klicken Sie auf der Registerkarte *Akzeptanztransformationsregeln* des Dialogfelds *Anspruchsregeln für Active Directory bearbeiten* auf *Regel hinzufügen* (siehe Abbildung 5–5).

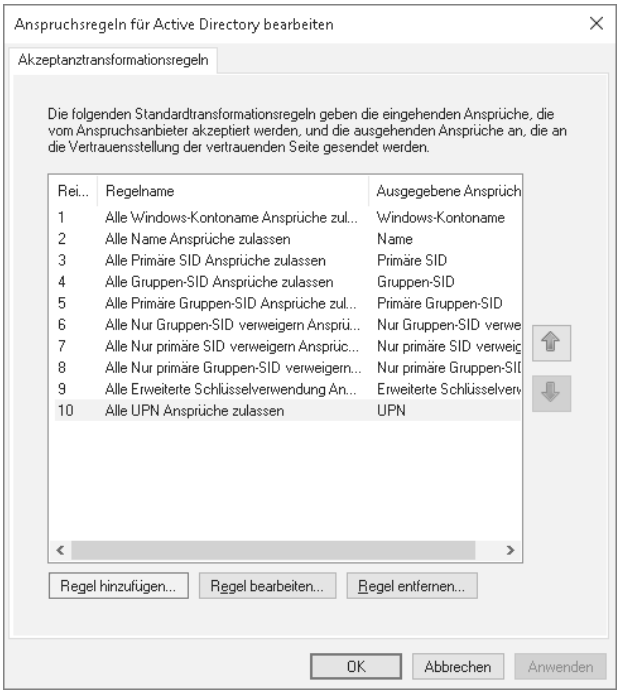

Abb. 5–5 Anzeigen der Akzeptanztransformationsregeln

5. Wählen Sie auf der Seite *Regelvorlage auswählen* des Assistenten zum Hinzufügen einer Transformationsanspruchsregel eine der folgenden Optionen aus der Liste *Anspruchsregelvorlage* (siehe Abbildung 5–6):
   - **LDAP-Attribute als Ansprüche senden** Verwenden Sie diese Vorlage, um ein oder mehrere LDAP-Attribute (Lightweight Directory Access Protocol) aus dem LDAP-Speicher auszuwählen, z. B. aus AD DS oder AD LDS (Lightweight Directory Service). Die Regel entnimmt dem Speicher die angegebenen Werte und sendet sie als Claims.
   - **Gruppenmitgliedschaft als Anspruch senden** Verwenden Sie diese Vorlage, um die Mitgliedschaft in einer AD DS-Sicherheitsgruppe als Anspruch zu verwenden.
   - **Eingehenden Anspruch transformieren** Mit dieser Vorlage erstellen Sie eine Regel, die eingehende Ansprüche umwandelt, indem sie die Regeltypen und optional auch die Werte ändert.
   - **Eingehenden Anspruch filtern oder zulassen** Mit dieser Vorlage können Sie eingehende Ansprüche filtern und nur diejenigen durchlassen, die bestimmte Kriterien erfüllen. Beispielsweise können Sie damit eine Regel erstellen, die nur Ansprüche auf der Grundlage von UPNs mit dem Suffix *@Adatum.com* durchlässt.
   - **Ansprüche mithilfe einer benutzerdefinierten Regel senden** Verwenden Sie diese Vorlage, wenn keine der anderen Ihre Bedürfnisse erfüllt.

6. Wählen Sie beispielsweise *LDAP-Attribute als Ansprüche senden* aus und klicken Sie auf *Weiter*.

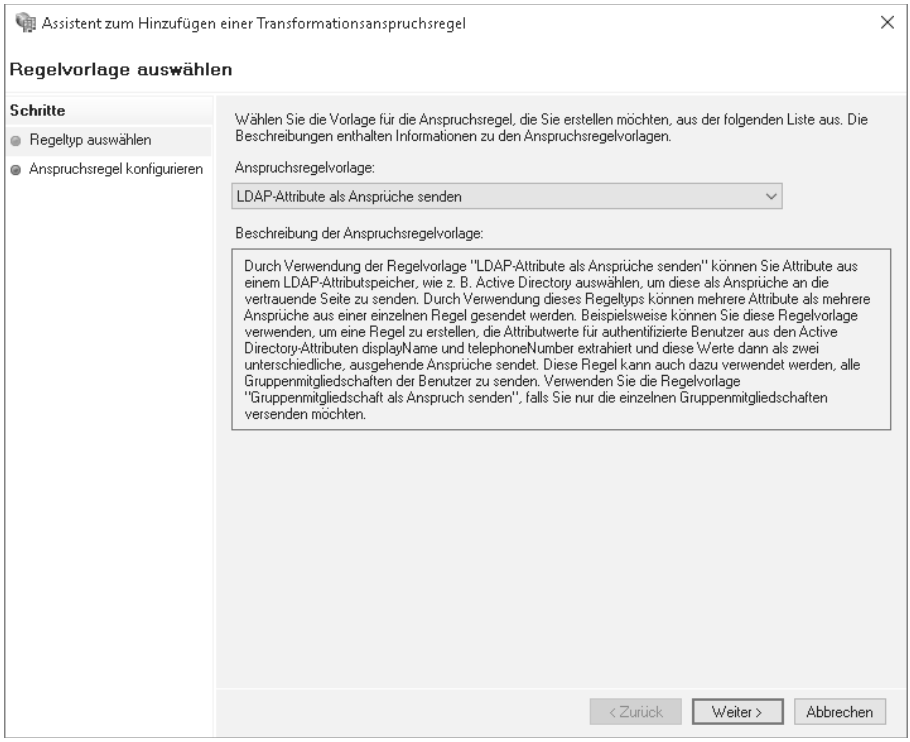

Abb. 5–6 Auswählen einer Regelvorlage

7. Geben Sie auf der Seite *Regel konfigurieren* aus Abbildung 5–7 einen Namen in das Feld *Anspruchsregelname* ein, in unserem Beispiel *Ausgehende LDAP-Regel*.
8. Wählen Sie *Active Directory* aus der Liste *Attributspeicher* aus.
9. Wählen Sie im Bereich *Zuordnung von LDAP-Attributen zu Typen ausgehender Ansprüche* geeignete Werte für die LDAP-Attribute und die zugehörigen ausgehenden Anspruchstypen aus. In Abbildung 5–7 sehen Sie als Beispiel die folgenden Zuordnungen:
   - *E-Mail-Addresses* > *E-Mail-Adresse*
   - *User-Principal-Name* > *UPN*
10. Klicken Sie auf *Fertig stellen* und dann auf *OK*.

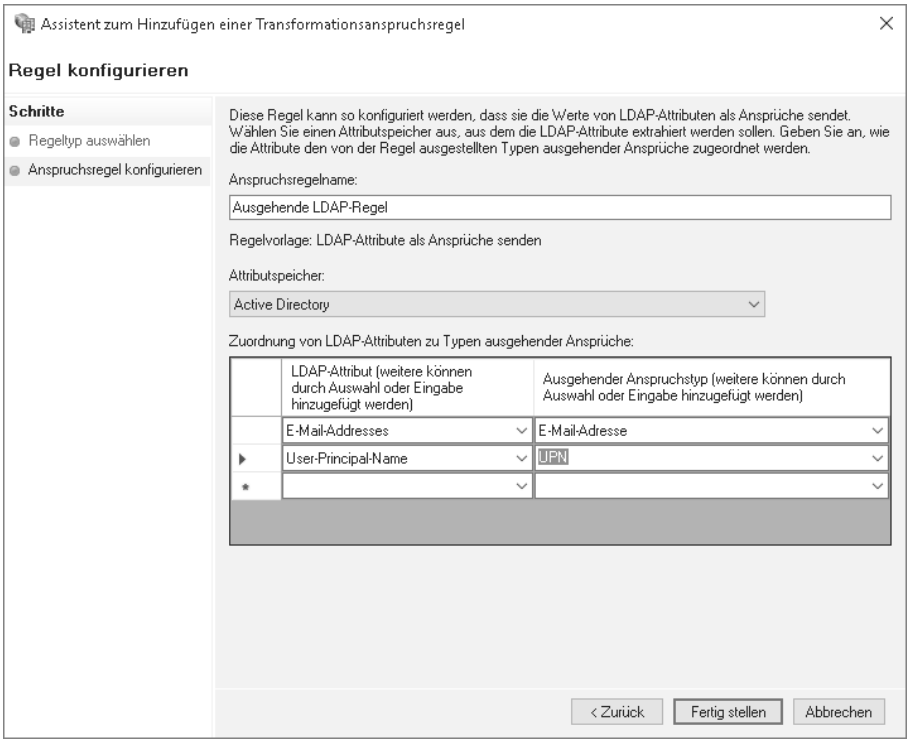

Abb. 5–7 Einrichten einer ausgehenden LDAP-Anspruchsregel

WEITERE INFORMATIONEN **Einrichten einer Anspruchsanbieter-Vertrauensstellung**

Weitere Informationen darüber, wie Sie eine Anspruchsanbieter-Vertrauensstellung anlegen können, finden Sie auf der Microsoft TechNet-Website unter:

https://technet.microsoft.com/library/dn486771(v=ws.11).aspx

Einrichten einer Vertrauensstellung der vertrauenden Seite

Nachdem Sie die Anspruchsanbieter-Vertrauensstellung eingerichtet haben, müssen Sie auf dem Verbundserver, der als vertrauende Seite dient, eine Vertrauensstellung der vertrauenden Seite anlegen. Bei einem Verbund innerhalb derselben Organisation kann dies auf demselben Verbundserver geschehen, bei einem Verbund zwischen zwei Unternehmen erfolgt dieser Vorgang auf einem Verbundserver in der anderen Organisation. Zur Einrichtung der Vertrauensstellung gehen Sie wie folgt vor:

1. Öffnen Sie auf dem Verbundserver die AD FS-Verwaltungskonsole.
2. Rechtsklicken Sie auf *Vertrauensstellungen der vertrauenden Seite* und wählen Sie *Vertrauensstellung der vertrauenden Seite hinzufügen*.

3. Aktivieren Sie auf der Willkommensseite des Assistenten zum Hinzufügen von Vertrauensstellungen der vertrauenden Seite die Option *Ansprüche unterstützend* und klicken Sie auf *Start*.
4. Machen Sie auf der Seite *Datenquelle auswählen* aus Abbildung 5–8 die erforderlichen Angaben, damit der Konfigurations-Assistent die Informationen über die vertrauende Seite finden kann. Folgende Möglichkeiten stehen zur Auswahl:
   - *Online oder in einem lokalen Netzwerk veröffentlichte Daten über die vertrauende Seite importieren*
   - *Daten über die vertrauende Seite aus einer Datei importieren*
   - *Daten über die vertrauende Seite manuell eingeben*
5. Wenn Sie auf *Online oder in einem lokalen Netzwerk veröffentlichte Daten über die vertrauende Seite importieren* geklickt haben, müssen Sie im Textfeld *Verbundmetadaten-Adresse (Hostname oder URL)* den Pfad zu der Anwendung mit den Metadaten über die vertrauende Seite eingeben. Klicken Sie anschließend auf *Weiter*.

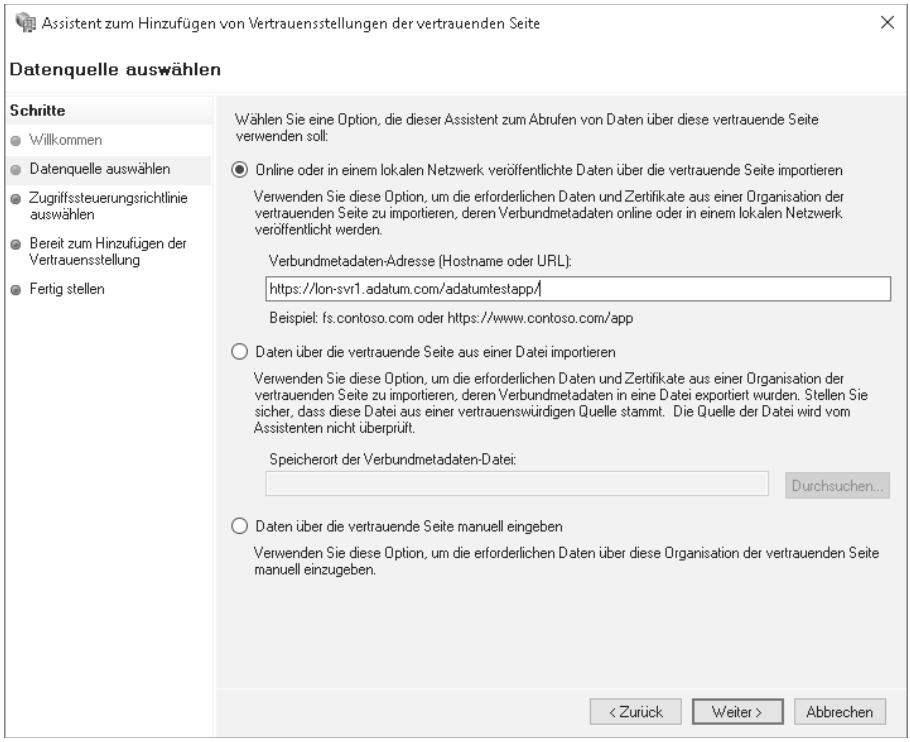

Abb. 5–8 Angeben der Datenquelle für die Vertrauensstellung der vertrauenden Seite

6. Geben Sie auf der Seite *Anzeigename angeben* einen Namen für die Vertrauensstellung in das Feld *Anzeigename* ein und klicken Sie auf *Weiter*.

7. Wählen Sie auf der Seite *Zugriffssteuerungsrichtlinie auswählen* eine passende Richtlinie unter den folgenden aus:
   - *Jedem Einzelnen Zugriff gewähren*
   - *Jedem Einzelnen Zugriff gewähren und MFA verlangen*
   - *Jedem Einzelnen Zugriff gewähren und MFA für bestimmte Gruppe verlangen*
   - *Jedem Einzelnen Zugriff gewähren und MFA für Extranetzugriffe verlangen*
   - *Jedem Einzelnen Zugriff gewähren und MFA für nicht authentifizierte Geräte verlangen*
   - *Jedem Einzelnen Zugriff gewähren und MFA verlangen, automatische Geräteregistrierung zulassen*
   - *Jedem Einzelnen Intranetzugriff gewähren*
   - *Bestimmter Gruppe Zugriff gewähren*
8. Klicken Sie beispielsweise auf *Jedem Einzelnen Zugriff gewähren* und dann auf *Weiter*.
9. Um die Konfiguration abzuschließen, klicken Sie auf der Seite *Bereit zum Hinzufügen der Vertrauensstellung* auf *Weiter* und nach Fertigstellung auf *Schließen*.

> ***WEITERE INFORMATIONEN*** **Einrichten einer Vertrauensstellung der vertrauenden Seite**
>
> Weitere Informationen darüber, wie Sie eine Vertrauensstellung der vertrauenden Seite anlegen können, finden Sie auf der Microsoft TechNet-Website unter:
>
> *https://technet.microsoft.com/library/dn486828(v=ws.11).aspx*

Als Nächstes müssen Sie die Ausstellungsrichtlinien festlegen:

1. Rechtsklicken Sie in der Liste der Vertrauensstellungen der vertrauenden Seite auf die gewünschte Vertrauensstellung und wählen Sie *Anspruchsausstellungsrichtlinie bearbeiten*.
2. Klicken Sie auf der Registerkarte *Ausstellungstransformationsregeln* auf *Regel hinzufügen*.
3. Wählen Sie in der Liste *Anspruchsregelvorlage* des Dialogfelds *Regelvorlage auswählen* eine der folgenden Vorlagen aus:
   - *LDAP-Attribute als Ansprüche senden*
   - *Gruppenmitgliedschaft als Anspruch senden*
   - *Eingehenden Anspruch transformieren*
   - *Eingehenden Anspruch filtern oder zulassen*
   - *Ansprüche mithilfe einer benutzerdefinierten Regel senden*
4. Klicken Sie beispielsweise auf *Eingehenden Anspruch filtern oder zulassen* und dann auf *Weiter*.

5. Geben Sie auf der Seite *Regel konfigurieren* einen Namen für die Regel in das Feld *Anspruchsregelname* ein und wählen Sie das gewünschte Attribut aus der Liste *Typ des eingehenden Anspruchs* aus, z. B. *Windows-Kontoname* (siehe Abbildung 5–9).

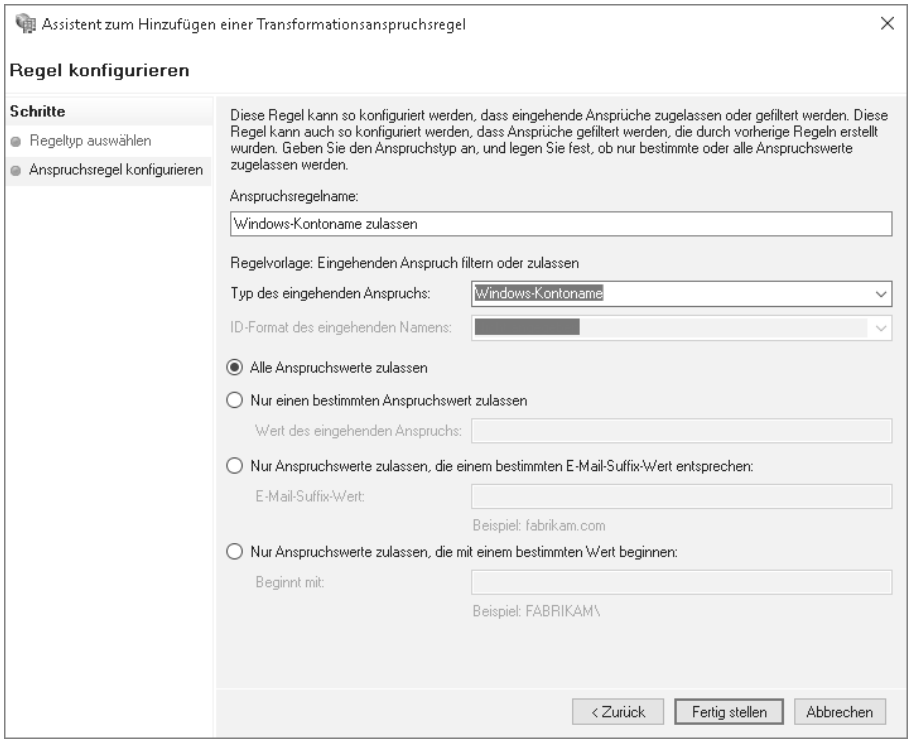

Abb. 5–9 Festlegen einer Transformationsanspruchsregel für eine Ausstellungsrichtlinie

6. Wählen Sie aus, wie mit dem Anspruch umgegangen werden soll:
   - *Alle Anspruchswerte zulassen*
   - *Nur einen bestimmten Anspruchswert zulassen*
   - *Nur Anspruchswerte zulassen, die einem bestimmten E-Mail-Suffix-Wert entsprechen*
   - *Nur Anspruchswerte zulassen, die mit einem bestimmten Wert beginnen*
7. Klicken Sie auf *Fertig stellen*.
8. Definieren Sie nun weitere Transformationsregeln, indem Sie den Vorgang wiederholen. So können Sie beispielsweise eine Regel zum Zulassen von Ansprüchen auf der Grundlage der E-Mail-Adresse oder des UPN hinzufügen (siehe Abbildung 5–10). Klicken Sie danach auf *OK*, um die Einrichtung der Ausstellungsrichtlinie abzuschließen.

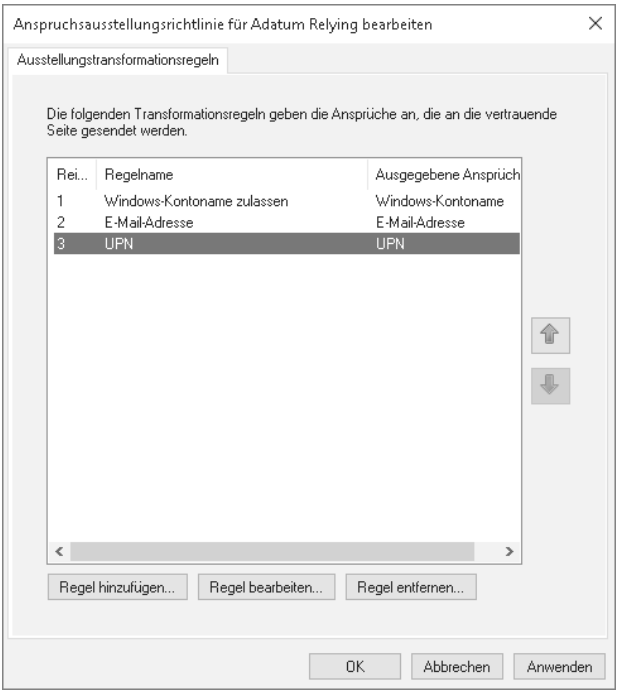

Abb. 5–10 Anzeige der Ausstellungstransformationsregeln

WEITERE INFORMATIONEN **Einrichten von Anspruchsregeln**

Weitere Informationen darüber, wie Sie Anspruchsregeln in AD FS erstellen können, finden Sie auf der Microsoft TechNet-Website unter:

https://technet.microsoft.com/library/dn486796(v=ws.11).aspx

Einrichten von Authentifizierungsrichtlinien

Mit Authentifizierungsrichtlinien können Sie festlegen, welche Authentifizierungsmechanismen akzeptabel sind, um den Zugriff auf Ihre Ressourcen über eine Verbundvertrauensstellung abzusichern. Authentifizierungsrichtlinien lassen sich auf zwei Ebenen festlegen:

- **Global** Eine globale Authentifizierungsrichtlinie gilt für alle Dienste und Anwendungen, die von den Verbunddiensten geschützt werden. Sie wird verwendet, wenn es keine spezifische Richtlinie für eine Vertrauensstellung der vertrauenden Seite gibt.
- **Spezifisch** Sie können eine Authentifizierungsrichtlinie für einen einzelnen geschützten Dienst oder eine einzelne Anwendung einrichten, indem Sie sie für eine einzelne Vertrauensstellung der vertrauenden Seite erstellen. Eine solche spezifische Richtlinie überschreibt nicht die von Ihnen festgelegten globalen Authentifizierungsrichtlinien.

PRÜFUNGSTIPP

Wenn eine Authentifizierungsrichtlinie eine mehrstufige Authentifizierung (Multi-Factor Authentication, MFA) verlangt, dann wird MFA ausgelöst, sobald ein Benutzer versucht, sich zu authentifizieren.

Um eine globale Authentifizierungsrichtlinie einzurichten, gehen Sie wie folgt vor:

1. Erweitern Sie im Navigationsbereich der AD FS-Konsole den Knoten *Dienst*.
2. Klicken Sie auf Authentifizierungsmethoden.
3. Klicken Sie auf den Link *Bearbeiten* unter der Überschrift *Primäre Authentifizierungsmethoden* (siehe Abbildung 5–11).

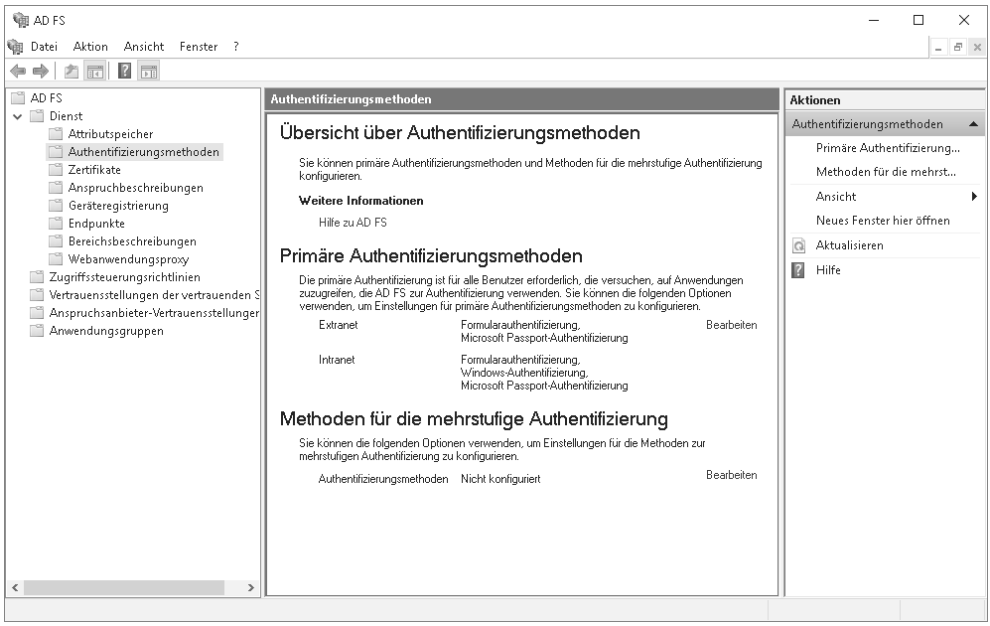

Abb. 5–11 Einrichten von Authentifizierungsmethoden

4. Richten Sie auf der Registerkarte *Primär* des Dialogfelds *Authentifizierungsmethoden bearbeiten* die gewünschten Methoden für Ihre Organisation ein (siehe Abbildung 5–12). Dabei können Sie Einstellungen für Intranet- und Extranetbenutzer wählen. Folgende Methoden sind verfügbar:
   - *Formularauthentifizierung*
   - *Windows-Authentifizierung* (nur für *Intranet*)
   - *Zertifikatsauthentifizierung*
   - *Geräteauthentifizierung*
   - *Microsoft Passport-Authentifizierung*

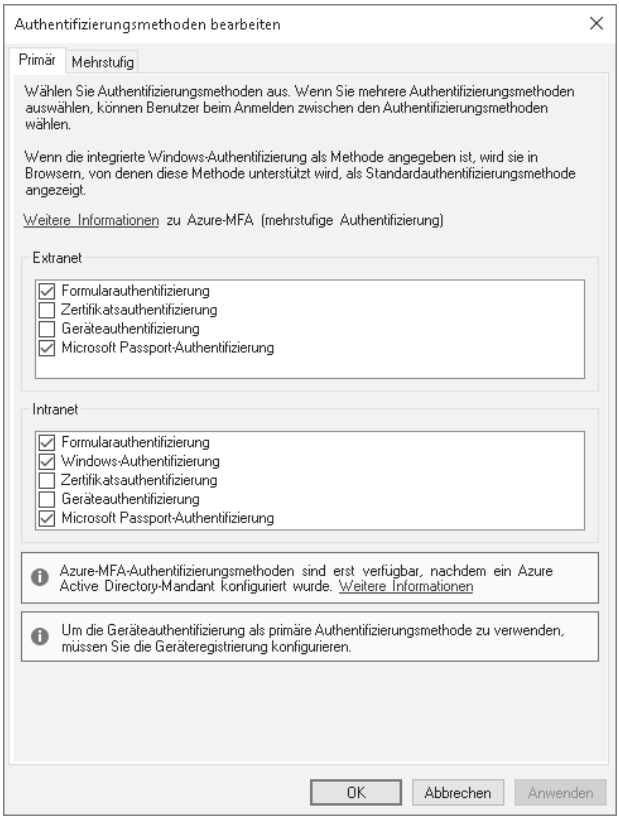

Abb. 5–12 Einrichten der primären Authentifizierungsmethoden

Einrichten von MFA

Bei der herkömmlichen Computerauthentifizierung werden Benutzername und Kennwort gegenüber einer Authentifizierungsstelle angegeben. Eine solche Kennwortauthentifizierung ist zwar in vielen Situationen akzeptabel, doch die Verbunddienste von Windows Server 2016 stellen eine Reihe weiterer, sichererer Methoden zur Verfügung, darunter auch eine mehrstufige Authentifizierung (MFA).

Bei MFA müssen sich die Benutzer anhand mehrerer Faktoren identifizieren: Sie müssen etwas wissen, etwas haben und etwas sein. Beispielsweise kann verlangt werden, dass ein Benutzer ein Kennwort weiß, ein Sicherheitstoken hat (in der Form eines digitalen Zertifikats) und seine Identität mit einem biometrischen Merkmal nachweisen kann, z. B. einem Fingerabdruck.

Um MFA in den Verbunddiensten von Windows Server 2016 zu aktivieren, müssen Sie mindestens eine weitere Authentifizierungsmethode auswählen. Standardmäßig stehen die Zertifikatsauthentifizierung und Azure MFA zur Verfügung. Gehen Sie zur Einrichtung von MFA wie folgt vor:

1. Erweitern Sie im Navigationsbereich der AD FS-Konsole den Knoten *Dienste*.
2. Klicken Sie auf *Authentifizierungsmethoden* und unter *Primäre Authentifizierungsmethoden* auf *Bearbeiten*.
3. Öffnen Sie im Dialogfeld *Authentifizierungsmethoden bearbeiten* die Registerkarte *Mehrstufig*, legen Sie die gewünschten Methoden fest und klicken Sie auf *OK* (siehe Abbildung 5–13). Zur Auswahl stehen:
   - *Zertifikatsauthentifizierung*
   - *Azure MFA*

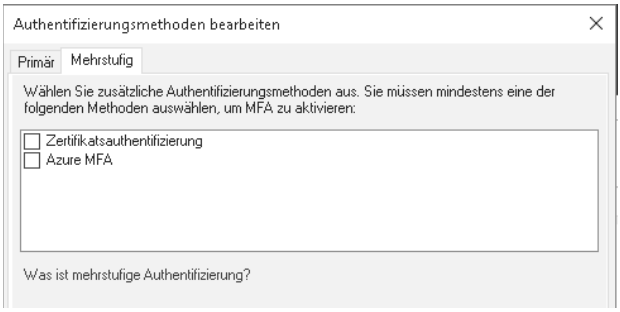

Abb. 5–13 Einrichten der Mehrfaktor-Authentifizierung

WEITERE INFORMATIONEN **Mehrstufige Authentifizierung mit Azure**

Weitere Informationen über Azure MFA finden Sie auf der Microsoft-Website unter:

https://docs.microsoft.com/azure/multi-factor-authentication/multi-factor-authentication-get-started-adfs-w2k12

Einrichten der Geräteregistrierung

Heutzutage greifen viele Benutzer von ihren eigenen Geräten aus auf Firmenressourcen zu. Der Anschluss privater Geräte an das Unternehmensnetzwerk stellt jedoch ein Sicherheitsrisiko dar und erfordert ein gewisses Maß an administrativer Arbeit.

Durch die Verwendung der Geräteregistrierung in den Verbunddiensten können Sie einige der Funktionen, die für Geräte in der Domäne zur Verfügung stehen, auch auf andere Geräte ausweiten und dabei gleichzeitig die Sicherheit Ihrer Organisation wahren.

HINWEIS **Gesamtstrukturfunktionsebene**

Um die Geräteregistrierung und die Einbindung von Microsoft Passport nutzen zu können, muss die Gesamtstruktur mindestens die Funktionsebene Windows Server 2016 aufweisen.

Wenn Sie die Geräteregistrierung einrichten, können Benutzer von ihren eigenen Geräten beispielsweise über SSO auf Ressourcen und Anwendungen des Unternehmens zugreifen.

HINWEIS **Zertifikate**

Die Benutzergeräte müssen der Zertifizierungsstelle vertrauen, die die SSL-Zertifikate Ihren Verbundservern ausgibt. Wenn Sie eine interne private Zertifizierungsstelle verwenden, müssen die Benutzergeräte das Zertifikat der Stammzertifizierungsstelle haben. Da diese Geräte nicht der Domäne angehören, können Sie für diesen Zweck keine Gruppenrichtlinien einsetzen, sondern müssen das Zertifikat anderweitig verteilen.

Um die Geräteregistrierung der Verbunddienste einzuschalten, gehen Sie wie folgt vor:

1. Erweitern Sie in der AD FS-Konsole den Knoten *Dienste* und klicken Sie auf *Geräteregistrierung*.
2. Klicken Sie im Detailbereich auf *Geräteregistrierung wird konfiguriert* und dann auf *OK*.

Sie können diese Aufgabe auch mit dem Windows PowerShell-Cmdlet `Initialize-ADDeviceRegistration` durchführen.

WEITERE INFORMATIONEN **Planen des bedingten Zugriffs von Geräten auf Unternehmensressourcen**

Weitere Informationen über die Planung der Geräteregistrierung finden Sie auf der Microsoft-Website unter:

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/plan-device-based-conditional-access-on-premises

Einbindung von Microsoft Passport in die Verbunddienste

Mit Passport bietet Microsoft ein Authentifizierungssystem an, bei dem keine Kennwörter mehr an eine Authentifizierungsstelle, etwa einen Domänencontroller, gesendet werden müssen. Es handelt sich dabei um eine zweistufige Authentifizierung, bei der biometrische Daten auf der Grundlage von Windows Hello (oder ein PIN) den einen Faktor bilden und der Besitz eines bestimmten Geräts den zweiten.

PRÜFUNGSTIPP

Windows Hello ist ein biometrischer Authentifizierungsmechanismus. Er gehört zum Lieferumfang von Windows 10 und ermöglicht Benutzern, ihre Identität durch ein eindeutig zu ihnen gehörendes Merkmal nachzuweisen. Bei der Verwendung von Windows Hello können Benutzer ihre Geräte durch Gesichtserkennung oder eine Abtastung der Fingerabdrücke entsperren. In den ersten Versionen von Windows 10 waren Windows Hello und Microsoft Passport noch zwei verwandte, aber getrennte Sicherheitsfunktionen. Microsoft hat sie jedoch inzwischen unter dem Namen Windows Hello zusammengefasst.

Die Verwendung von Windows Hello bietet Ihrer Organisation die beiden folgenden Vorteile:

- **Komfort für die Benutzer** Nach der Einrichtung von Windows Hello können die Benutzer auf Unternehmensressourcen zugreifen, ohne sich Benutzernamen und Kennwörter merken zu müssen.
- **Sicherheit** Da bei Microsoft Passport keine Kennwörter verwendet werden, sind die Identitäten der Benutzer und ihre Anmeldeinformationen besser geschützt.

> ***WEITERE INFORMATIONEN*** **Windows Hello für Unternehmen**
>
> Weitere Informationen über Microsoft Passport und Windows Hello finden Sie auf der Microsoft TechNet-Website unter:
>
> *https://technet.microsoft.com/itpro/windows/keep-secure/microsoft-passport-guide*

Zur Einbindung von Microsoft Passport in die Verbunddienste führen Sie den weiter vorn beschriebenen Vorgang zur Geräteregistrierung aus und gehen anschließend wie folgt vor:

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Erstellen Sie ein neues Gruppenrichtlinienobjekt und öffnen Sie es zur Bearbeitung.
3. Öffnen Sie im Gruppenrichtlinienverwaltungs-Editor *Computerkonfiguration*, *Richtlinien*, *Administrative Vorlagen*, *Windows-Komponenten* und *Geräteregistrierung*.
4. Doppelklicken Sie im Detailbereich auf *In die Domäne eingebundene Computer als Geräte registrieren*.
5. Klicken Sie im Dialogfeld *In die Domäne eingebundene Computer als Geräte registrieren* auf *Aktiviert* und dann auf *OK* (siehe Abbildung 5–14).

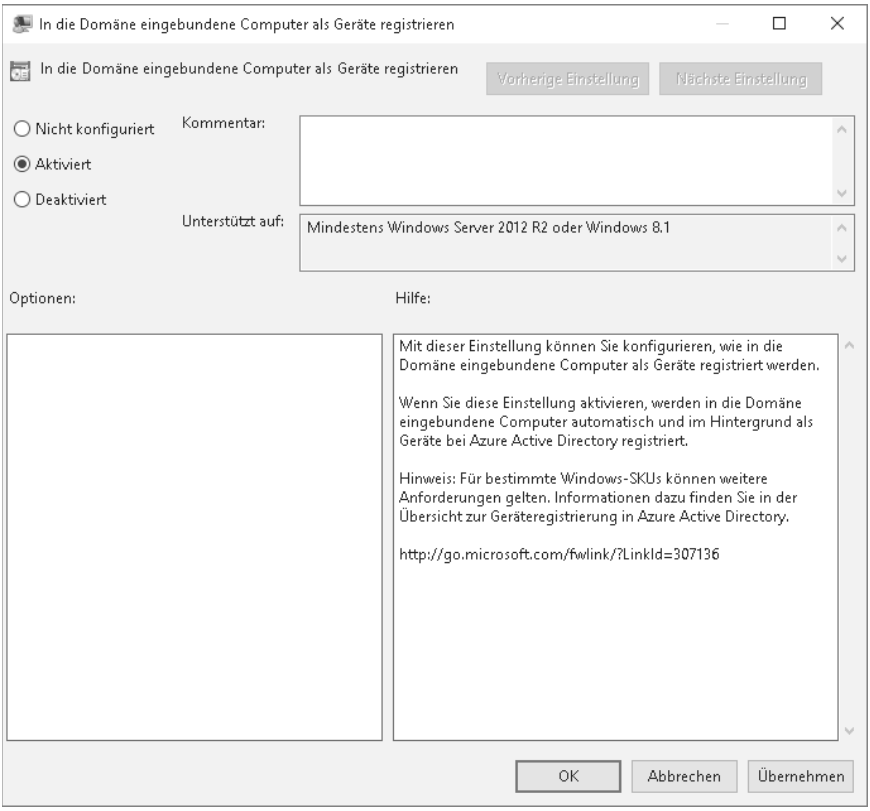

Abb. 5–14 Aktivieren der Gruppenrichtlinieneinstellung *In die Domäne eingebundene Computer als Geräte registrieren*

6. Öffnen Sie im Navigationsbereich *Computerkonfiguration*, *Richtlinien*, *Administrative Vorlagen*, *Windows-Komponenten* und *Windows Hello for Business*.
7. Doppelklicken Sie im Detailbereich auf *Windows Hello for Business*.
8. Klicken Sie im Dialogfeld *Windows Hello for Business* auf *Aktiviert* und dann auf *OK*.
9. Verknüpfen Sie das Gruppenrichtlinienobjekt mit dem passenden Container, beispielsweise mit dem Domänencontainer, wenn Sie die Einstellung für alle Geräte aktivieren möchten.

WEITERE INFORMATIONEN **Einrichten der Verbunddienste zur Nutzung von Microsoft Passport im Unternehmen**

Weitere Informationen darüber, wie Sie die Verbunddienste zur Nutzung von Microsoft Passport einrichten, finden Sie auf der Microsoft TechNet-Website unter:

https://technet.microsoft.com/library/mt732271.aspx

Einrichtung zur Verwendung von Microsoft Azure und Microsoft Office 365

Viele Organisationen verlagern einige oder alle ihre Anwendungen und Dienste auf Onlineplattformen wie Microsoft Azure oder Microsoft Office 365. Sie können die Active Directory-Verbunddienste auch darin einbinden, sodass die Benutzer mit einer einzigen Anmeldung auf Anwendungen und Dienste sowohl in ihrer eigenen Infrastruktur als auch auf den Onlineplattformen zugreifen können.

PRÜFUNGSTIPP

Die Verbunddienste können nicht nur mit Onlinediensten von Microsoft, sondern auch mit verschiedenen anderen Cloud-Anbietern verzahnt werden.

Um die einmalige Anmeldung (Single-Sign On, SSO) für Microsoft-Onlinedienste in den Verbunddiensten einzurichten, gehen Sie wie folgt vor:

1. Richten Sie den Extranetzugriff über die Verbunddienste ein. Dazu müssen Sie auf einem Server in Ihrem Umkreisnetzwerk die Rolle *Webanwendungsproxy* bereitstellen. Mehr dazu erfahren Sie in »Prüfungsziel 5.2: Verwenden des Webanwendungsproxys«.
2. Richten Sie mit dem Windows PowerShell-Cmdlet `New-MsolFederatedDomain` eine Vertrauensstellung zwischen AD FS und Azure AD ein.

PRÜFUNGSTIPP

Bevor Sie dieses Cmdlet nutzen können, müssen Sie Microsoft Azure Active Directory Module installieren.

3. Richten Sie die Verzeichnissynchronisation Ihrer AD DS-Domäne mit Microsoft Azure ein, indem Sie Azure AD Connect herunterladen und installieren.

WEITERE INFORMATIONEN **Verbinden von Active Directory mit Azure AD**

Weitere Informationen über die Verbindung mit Azure AD finden Sie auf der Microsoft-Website unter:

https://docs.microsoft.com/azure/active-directory/connect/active-directory-aadconnect

4. Vergewissern Sie sich, dass Sie SSO korrekt eingerichtet haben:
   - Melden Sie sich auf einem Computer in der Domäne mit Ihren Domänenanmeldeinformationen an dem Microsoft-Cloud-Dienst an. Wenn die einmalige Anmeldung eingerichtet ist, so wird das Kennwortfeld grau dargestellt und zeigt die folgende Meldung an:

     Eine Anmeldung an <Ihr Unternehmen> ist erforderlich.
   - Klicken Sie auf den Link *Anmeldung an <Ihr Unternehmen>*. Wenn die Anmeldung erfolgreich verläuft, haben Sie SSO korrekt eingerichtet.

Einrichten der Verbunddienste zur Authentifizierung von Benutzern in LDAP-Verzeichnissen

Die Verbunddienste ermöglichen auch eine Authentifizierung von Objekten, die in LDAP-Verzeichnissen gespeichert sind, z. B. in AD LDS. Um ein LDAP-Verzeichnis als Attributspeicher einzurichten, gehen Sie wie folgt vor:

1. Öffnen Sie die AD FS-Konsole.
2. Klicken Sie unter dem Knoten *Dienst* auf *Attributspeicher*. Im Detailbereich wird *Active Directory* angezeigt.
3. Rechtsklicken Sie auf *Attributspeicher* und wählen Sie *Attributspeicher hinzufügen*.
4. Geben Sie im Feld *Anzeigename* des Dialogfelds *Attributspeicher hinzufügen* einen Namen ein und wählen Sie *LDAP* aus der Liste *Attributspeichertyp* (siehe Abbildung 5–15).

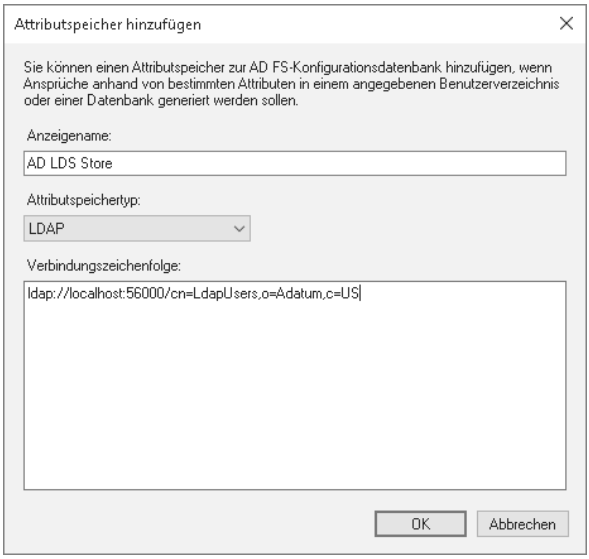

Abb. 5–15 Einrichten eines LDAP-Attributspeichers

5. Geben Sie in das Feld *Verbindungszeichenfolge* die Verbindungszeichenfolge ein und klicken Sie auf *OK*. Diese Zeichenfolge sieht beispielsweise wie folgt aus: `ldap://localhost:56000/cn=LdapUsers,o=Adatum,c=US`. Die genaue Angabe hängt jedoch davon ab, wo das LDAP-Verzeichnis untergebracht ist. In diesem Beispiel wird die AD LDS-Serverrolle vom lokalen Host ausgeführt und ist über Port 56000 erreichbar.

WEITERE INFORMATIONEN **Einrichten der Verbunddienste zur Authentifizierung von Benutzern in LDAP-Verzeichnissen**

Weitere Informationen darüber, wie Sie die Verbunddienste zur Authentifizierung von Benutzern in LDAP-Verzeichnissen einrichten, finden Sie auf der Microsoft TechNet-Website unter:

https://technet.microsoft.com/library/dn823754(v=ws.11).aspx

Nachdem Sie den Attributspeicher erstellt haben, müssen Sie eine neue Anspruchsanbietervertrauensstellung einrichten. Bei der Definition der Regeln für diese Vertrauensstellung wählen Sie dann den neuen Attributspeicher aus.

Aktualisieren und Migrieren von früheren Verbunddienst-Bereitstellungen auf Windows Server 2016

In Windows Server 2016 wurden einige neue und verbesserte Merkmale in den Active Directory-Verbunddiensten eingeführt:

- Unterstützung für LDAP-3-konforme Verzeichnisse
- Unterstützung von Azure MFA
- Einführung von Anwendungsrichtlinien und delegierte Dienstverwaltung
- Verbesserungen bei der Geräteregistrierung

Haben Sie die Verbunddienste in Windows Server 2012 R2 oder früher bereitgestellt, sollten Sie eine Aktualisierung oder Migration auf Windows Server 2016 ernsthaft in Betracht ziehen. Wenn Sie einen neuen Verbundserver mit Windows Server 2016 zu einer Verbundserverfarm mit Windows Server 2012 R2 hinzufügen, bietet die Farm weiterhin die alten Merkmale an, das heißt, sie wird weiterhin auf der alten Farmverhaltensebene Windows Server 2012 R2 betrieben.

PRÜFUNGSTIPP

Die Farmverhaltensebene ist ein Windows Server 2016-Merkmal, das den Funktionsumfang einer AD FS-Farm bestimmt.

Dadurch können Sie Ihrer Farm weitere AD FS-Server hinzufügen, ohne deren Funktionsumfang zu ändern. Anschließend können Sie die Verbunddienstrolle auf den verbliebenen Computern mit Windows Server 2012 R2 abschalten und die Farmverhaltensebene auf Windows Server 2016 anheben, um die neuen und verbesserten Verbunddienstfunktionen zu nutzen.

Zur Aktualisierung oder Migration der Verbunddienste auf Windows Server 2016 gehen Sie folgendermaßen vor:

1. Stellen Sie die Verbunddienste auf Windows Server 2016 bereit. Wählen Sie bei der Konfiguration die Option *Fügt einer Verbundserverfarm einen Verbundserver hinzu*.

2. Richten Sie den Verbundserver mit Windows Server 2016 als primären Verbundserver ein. Dazu führen Sie das Windows PowerShell-Cmdlet `Set-AdfsSyncProperties -Role PrimaryComputer` aus.
3. Führen Sie auf einem der Computer mit Windows Server 2012 R2 das Windows PowerShell-Cmdlet `Set-AdfsSyncProperties -Role SecondaryComputer -PrimaryComputerName {FQDN}` aus.
4. Öffnen Sie auf dem Verbundserver mit Windows Server 2016 eine Eingabeaufforderung mit erhöhten Rechten und führen Sie die Befehle `adprep /forestprep` und `adprep /domainprep` aus, die Sie auf der Windows Server 2016-DVD im Ordner *support\adprep* finden. Dadurch werden die Gesamtstruktur und die Domäne auf das Vorhandensein eines Verbundservers mit Windows Server 2016 vorbereitet.
5. Wenn Sie alles eingerichtet haben, können Sie die Verbundserver mit Windows Server 2012 R2 außer Betrieb nehmen.

WEITERE INFORMATIONEN **Aktualisieren auf die Verbunddienste von Windows Server 2016**

Weitere Informationen darüber, wie Sie eine Verbunddienst-Bereitstellung auf Windows Server 2016 aktualisieren, finden Sie auf der Microsoft TechNet-Website unter:

https://technet.microsoft.com/windows-serverdocs/identity/ad-fs/deployment/upgrading-to-ad-fs-in-windows-server-2016

Prüfungsziel 5.2: Verwenden des Webanwendungsproxys

Viele Organisationen möchten ihre Anwendungen und Dienste auch für Benutzer außerhalb ihres Intranets bereitstellen. Das erfordert es gewöhnlich, Verbindungen von Remotebenutzern über das Internet zu ermöglichen. Sie können dazu den Rollendienst *Webanwendungsproxy* auf einem Servercomputer einrichten, den Sie in Ihrem Umkreisnetzwerk bereitstellen. Der Webanwendungsproxy ermöglicht es Ihnen, Anwendungen und Dienste Ihres internen Netzwerks für Benutzer in externen Netzwerken zu veröffentlichen.

Inhalt dieses Abschnitts:

- Installieren und Einrichten des Webanwendungsproxys
- Einbinden des Webanwendungsproxys in Active Directory-Verbunddienste
- Einrichten des Webanwendungsproxys im Pass-through-Modus
- Veröffentlichen von Remotedesktopgateway-Anwendungen