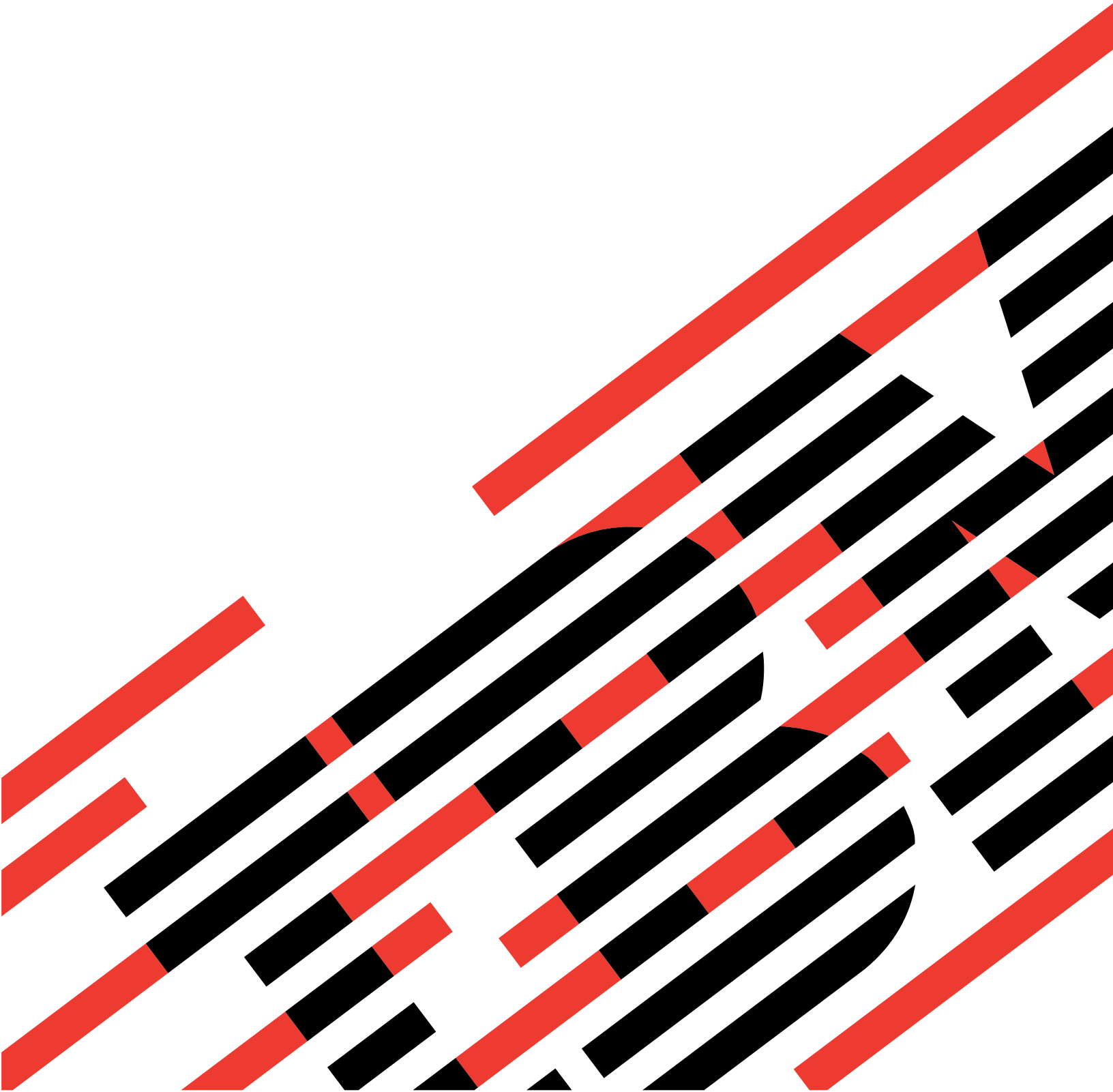
IBM Systems - iSeries

Enterprise Identity Mapping

Version 5 Release 4



IBM Systems - iSeries

Enterprise Identity Mapping

Version 5 Release 4

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die allgemeinen Informationen unter „Bemerkungen", auf Seite 141 gelesen werden.

Fünfte Ausgabe (Februar 2006)

Diese Ausgabe bezieht sich auf Version 5, Release 4, Modifikation 0 von IBM i5/OS (Produktnummer 5722–SS1) und alle nachfolgenden Releases und Modifikationen, es sei denn, es erfolgen anders lautende Angaben in neuen Ausgaben. Diese Version kann nicht auf allen RISC-Modellen (Reduced Instruction Set Computer) ausgeführt werden. Auf CICS-Modellen ist sie nicht ausführbar.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Systems - iSeries Enterprise Identity Mapping, Version 5 Release 4,
herausgegeben von International Business Machines Corporation, USA

Herausgegeben von:
SW TSC Germany
Kst. 2877
Februar 2006

Inhaltsverzeichnis

Enterprise Identity Mapping

Enterprise Identity Mapping (EIM) für iSeries ist die i5/OS-Implementierung einer IBM @server -Infrastruktur, die Administratoren und Anwendungsentwicklern die Verwaltung von mehreren Benutzerregistern innerhalb des Unternehmens ermöglicht. Die meisten Unternehmen mit Netzwerken kennen das Problem mehrerer Benutzerregister, d. h., dass jede Person oder Entität innerhalb des Unternehmens eine Benutzeridentität in jedem Register besitzen muss. Wenn der Bedarf an Benutzerregistern zunimmt, entsteht schnell ein großes Verwaltungsproblem, das Benutzer, Administratoren und Anwendungsentwickler betrifft. Enterprise Identity Mapping (EIM) ermöglicht kosteneffiziente Lösungen für eine einfachere Verwaltung mehrerer Benutzerregister und Benutzeridentitäten in Ihrem Unternehmen.

EIM bietet Ihnen die Möglichkeit, für eine Person in Ihrem Unternehmen ein System von Identitätsabgleichen, so genannten Zuordnungen, zwischen den verschiedenen Benutzeridentitäten in verschiedenen Benutzerregistern zu erstellen. EIM stellt einen allgemeinen API-Satz zur Verfügung, mit dem plattformübergreifend Anwendungen entwickelt werden können, die in der Lage sind, anhand der von Ihnen erstellten Identitätsabgleiche die Beziehungen zwischen Benutzeridentitäten zu ermitteln. Außerdem können Sie EIM in Verbindung mit dem Netzwerkauthentifizierungsservice (i5/OS-Implementierung von Kerberos) verwenden, um eine Umgebung für die Einzelanmeldung aufzubauen.

Sie können EIM über den iSeries Navigator, die grafische iSeries-Benutzeroberfläche, konfigurieren und verwalten. Der iSeries-Server verwendet EIM, um i5/OS-Schnittstellen für die Authentifizierung von Benutzern über den Netzwerkauthentifizierungsservice zu aktivieren. Sowohl Anwendungen als auch i5/OS können Kerberos-Tickets akzeptieren und mit EIM das Benutzerprofil ermitteln, das dieselbe Person repräsentiert wie das Kerberos-Ticket.

Weitere Informationen zur Funktionsweise von EIM, zu den EIM-Konzepten und zur Verwendung von EIM in Ihrem Unternehmen erhalten Sie in den folgenden Abschnitten:

Neuerungen in V5R4

Im folgenden Abschnitt werden die Änderungen beschrieben, die in V5R4 an EIM (EIM = Enterprise Identity Mapping) für iSeries durchgeführt wurden.

Neue oder erweiterte Funktionen für EIM

- Gruppenregisterdefinitionen Sie können nun Gruppenregisterdefinitionen erstellen, mit deren Hilfe Sie den Arbeitsaufwand für die Konfiguration von EIM-Abgleichen reduzieren können. Sie können eine Gruppenregisterdefinition in ähnlicher Weise verwalten wie eine einzelne Registerdefinition.
- Gruppenregisterdefinition hinzufügen Führen Sie die hier aufgeführten Anweisungen durch, um eine Gruppenregisterdefinition zu erstellen und diese zu einer EIM-Domäne hinzuzufügen.
- Mitglied zu einer Gruppenregisterdefinition hinzufügen Wenn Sie eine Verbindung zu der EIM-Domäne herstellen, in der die Gruppenregisterdefinition gespeichert ist, können Sie ein Mitglied zur Gruppenregisterdefinition hinzufügen, indem Sie die hier aufgeführten Anweisungen befolgen.

Erweiterungen der EIM-Informationen

Im aktuellen Release wurden zahlreiche Aktualisierungen an der Vorgehensweise zur Implementierung von Gruppenregisterdefinitionen für verschiedene EIM-Situationen durchgeführt.

- Richtlinienzuordnungen In diesen Informationen erfahren Sie, unter welchen Bedingungen die Verwendung von Gruppenregisterdefinitionen zur Einrichtung einer Abgleichsbeziehung für alle Benutzeridentitäten in einem einzelnen Register und einer Domäne sinnvoll ist.

- SuchoperationenIn diesen Informationen wird der Suchablauf einer Suchoperation erläutert, die eine Zielbenutzeridentität in einem Benutzerregister zurückgibt, das Mitglied einer Gruppenregisterdefinition ist.
- Mehrdeutige Ergebnisse In diesen Informationen wird erläutert, wann Suchoperationen mehrdeutige Ergebnisse zurückgeben können, wenn Sie eine einzelne Benutzerregisterdefinition als Mitglieder mehrerer Gruppenregisterdefinitionen angeben.

Darüber hinaus wurde der Abschnitt zur Einzelanmeldung aktualisiert und enthält nun Informationen zur Implementierung von EIM in einer Einzelanmeldungsumgebung, um den Aufwand für die Kennwortverwaltung zu reduzieren. Dieses Thema enthält eine Reihe von Szenarios mit allgemeinen Situationen zur Einzelanmeldung. Jede Situation ist mit detaillierten Konfigurationsanweisungen zur Implementierung der Szenarios versehen.

Neuerungen und Änderungen anzeigen

Um technische Änderungen zu markieren, werden im vorliegenden Dokument die folgenden Symbole verwendet:

- Das Grafiksymbol » markiert den Anfang der neuen oder geänderten Informationen.
- Das Grafiksymbol « markiert das Ende der neuen oder geänderten Informationen.

Weitere Informationen zu den Änderungen und Neuerungen im aktuellen Release finden Sie Memorandum für Benutzer.

Druckbare PDF-Datei

Gehen Sie wie im Folgenden beschrieben vor, um die hier aufgeführten Informationen im PDF-Format (PDF = Portable Document Format) anzuzeigen oder zu drucken.

Zum Anzeigen oder Herunterladen der PDF-Version dieses Dokuments wählen Sie Enterprise Identity Mapping (ca. 1.820 KB) aus.

Sie können die folgenden zugehörigen Themen anzeigen oder herunterladen:

- Netzwerkauthentifizierungsservice (circa 1.398 KB) veranschaulicht, wie der Netzwerkauthentifizierungsservice in Verbindung mit EIM konfiguriert wird, um eine Einzelanmeldungsumgebung zu erstellen.
- Directory Server (LDAP) (circa 1.700 KB) veranschaulicht, wie der LDAP-Server, den Sie als EIM-Domänencontroller verwenden können, konfiguriert wird und enthält Informationen zur erweiterten LDAP-Konfiguration.

PDF-Dateien speichern

So können Sie eine PDF-Datei auf Ihrer Workstation speichern, um diese anzuzeigen oder zu drucken:

1. Klicken Sie im Browser mit der rechten Maustaste auf die PDF-Datei (klicken Sie auf den o. a. Link).
2. Klicken Sie auf die Auswahl zum lokalen Speichern der PDF-Datei.
3. Navigieren Sie zu dem Verzeichnis, in dem die PDF-Datei gespeichert werden soll.
4. Klicken Sie auf **Speichern**.

Adobe Reader herunterladen

Zum Anzeigen oder Drucken der PDF-Dateien benötigen Sie Adobe Reader. Von der Adobe-Website (www.adobe.com/products/acrobat/readstep.html)  können Sie eine kostenlose Kopie dieses Programms herunterladen.

Enterprise Identity Mapping - Übersicht

Im Folgenden werden die Probleme erläutert, die Sie mit EIM (Enterprise Identity Mapping) beheben können. Darüber hinaus finden Sie hier Informationen zu den branchenspezifischen Lösungsansätzen für diese Probleme und erfahren, welche Vorteile der EIM-Ansatz bietet.

Heutige Netzwerkumgebungen bestehen aus einer komplexen Gruppe von Systemen und Anwendungen, was zur Folge hat, dass mehrere Benutzerregister verwaltet werden müssen. Daraus kann schnell ein großes Verwaltungsproblem entstehen, das sowohl Benutzer und Administratoren als auch Anwendungsentwickler betrifft. Für zahlreiche Unternehmen ist daher die sichere Verwaltung von Authentifizierungen und Berechtigungen für Systeme und Anwendungen problematisch. Enterprise Identity Mapping (EIM) ist eine IBM @server -Infrastrukturtechnologie, mit der Administratoren und Anwendungsentwickler dieses Problem einfacher und kosteneffizienter als je zuvor beheben können.

Im Folgenden werden die Probleme, die mit EIM gelöst werden können, aktuelle branchenspezifische Ansätze und die Vorzüge des EIM-Ansatzes beschrieben.

Verwaltung von mehreren Benutzerregistern

Viele Administratoren verwalten Netzwerke mit unterschiedlichen Systemen und Servern, die alle eine eigene Methode für die Verwaltung von Benutzern über verschiedene Benutzerregister verwenden. In diesen komplexen Netzwerken sind Administratoren für die Verwaltung der Identitäten und Kennwörter der einzelnen Benutzer in unterschiedlichen Systemen verantwortlich. Darüber hinaus müssen Administratoren häufig diese Identitäten und Kennwörter synchronisieren, während die Benutzer zahlreiche Identitäten und Kennwörter behalten sowie synchronisieren müssen. Der Aufwand für Administratoren und Benutzer ist in dieser Umgebung erheblich. Administratoren verbringen somit kostbare Zeit mit der Fehlerbehebung nach fehlgeschlagenen Anmeldeversuchen und dem Zurücksetzen vergessener Kennwörter, anstatt sich der Unternehmensverwaltung zu widmen.

Die Probleme bei der Verwaltung mehrerer Benutzerregister wirken sich zudem auf Anwendungsentwickler aus, die vielschichtige (Multiple-Tier-) bzw. heterogene Anwendungen zur Verfügung stellen möchten. Diese Anwendungsentwickler wissen, dass die wichtigen Geschäftsdaten der Kunden auf unterschiedlichen Systemtypen verteilt sind und dass jedes System über ein eigenes Benutzerregister verfügt. Aus diesem Grund müssen die Anwendungsentwickler proprietäre Benutzerregister und die zugehörige Sicherheitssemantik für ihre Anwendungen erstellen. Auf diese Weise wird das Problem der Anwendungsentwickler zwar gelöst, der Aufwand für Benutzer und Administratoren nimmt jedoch weiter zu.

Aktuelle Ansätze

Um die Probleme bei der Verwaltung mehrerer Benutzerregister zu lösen, stehen zahlreiche aktuelle branchenspezifische Ansätze zur Verfügung. Sie bieten jedoch alle nur unvollständige Lösungen. Lightweight Directory Access Protocol (LDAP) stellt beispielsweise eine Lösung mit einem verteilten Benutzerregister zur Verfügung. Die Verwendung von LDAP (oder einer anderen bekannten Lösung wie Microsoft Passport) bedeutet jedoch, dass Administratoren noch ein weiteres Benutzerregister und die entsprechende Sicherheitssemantik verwalten oder vorhandene Anwendungen, die diese Register verwenden, ersetzen müssen.

Bei Einsatz einer derartigen Lösung müssen Administratoren unterschiedliche Sicherheitsmechanismen für einzelne Ressourcen verwalten, wodurch sich der Verwaltungsaufwand und ggf. sogar die Sicherheitsrisiken erhöhen. Wenn mehrere Mechanismen eine einzige Ressource unterstützen, ist die Wahrscheinlichkeit, dass eine Berechtigung für einen Mechanismus geändert, die Änderung für einen oder mehrere der anderen Mechanismen jedoch vergessen wird, wesentlich höher. Ein Sicherheitsrisiko wäre beispielsweise, wenn einem Benutzer über eine Schnittstelle der Zugriff rechtmäßig verweigert wird, er jedoch über eine oder mehrere andere Schnittstellen Zugriff erhält.

Nach der Bewältigung dieses zusätzlichen Aufwands werden die Administratoren feststellen, dass das Problem nicht endgültig behoben wurde. Zumeist haben Unternehmen zu viel in die aktuellen Benutzerregister und die zugehörige Sicherheitssemantik investiert, um diese Art von Lösung umzusetzen. Die Erstellung eines weiteren Benutzerregisters und der zugehörigen Sicherheitssemantik löst das Problem zwar für den Anwendungslieferanten, nicht jedoch für die Benutzer oder Administratoren.

Eine andere potenzielle Lösung ist die Verwendung der Einzelanmeldung. Es sind zahlreiche Produkte erhältlich, mit denen Administratoren Dateien verwalten können, die alle Identitäten und Kennwörter der Benutzer enthalten. Dieser Ansatz hat jedoch gewisse Schwächen:

- Er behebt nur eines der Probleme, denen die Benutzer gegenüberstehen. Benutzer können sich zwar durch die Eingabe nur einer Identität und eines Kennworts an mehreren Systemen anmelden, sie benötigen aber weiterhin Kennwörter auf anderen Systemen und müssen diese verwalten.
- Vielmehr wird ein neues Problem geschaffen, da unverschlüsselte oder entschlüsselbare Kennwörter in diesen Dateien gespeichert werden und somit ein Sicherheitsrisiko darstellen. Kennwörter sollten keinesfalls in unverschlüsselten Dateien oder leicht zugänglich für Dritte (Administratoren eingeschlossen) gespeichert werden.
- Die Probleme von externen Anwendungsentwicklern, die heterogene, vielschichtige Anwendungen (Multiple-Tier-Anwendungen) liefern, werden nicht behoben. Sie müssen auch weiterhin proprietäre Benutzerregister für ihre Anwendungen liefern.

Trotz der genannten Schwächen haben einige Unternehmen diese Ansätze eingeführt, da sie die Probleme mit mehreren Benutzerregistern zumindest teilweise lösen.

EIM-Ansatz

EIM bietet einen neuen Ansatz, um kosteneffiziente Lösungen für eine einfachere Verwaltung mehrerer Benutzerregister und Benutzeridentitäten in einer mehrschichtigen, heterogenen Unternehmensumgebung zu realisieren. EIM ist eine Architektur, mit der in einem Unternehmen die Beziehungen zwischen Personen bzw. Entitäten (wie Dateiservern und Druckservern) und den zahlreichen Identitäten, die sie repräsentieren, beschrieben werden können. Darüber hinaus beinhaltet EIM eine Reihe von APIs, die Anwendungen die Möglichkeit bieten, Fragen zu diesen Beziehungen zu stellen.

Beispiel: Anhand der Benutzeridentität einer Person in einem einzigen Benutzerregister können Sie feststellen, welche Benutzeridentität diese Person in einem anderen Benutzerregister repräsentiert. Wenn der Benutzer sich mit einer Benutzeridentität authentifiziert hat und diese Benutzeridentität mit der entsprechenden Identität in einem anderen Benutzerregister abgeglichen werden kann, muss der Benutzer keine weiteren Identitätsnachweise zur Authentifizierung angeben. Sie kennen den Benutzer und müssen lediglich wissen, welche Benutzeridentität diesen Benutzer in einem anderen Benutzerregister repräsentiert. EIM bietet somit eine allgemeine Identitätsabgleichfunktion für das Unternehmen.

EIM ermöglicht 1:n-Abgleiche (d. h. ein Benutzer mit mehreren Benutzeridentitäten in einem einzigen Benutzerregister). Zudem müssen nicht für alle Identitäten in einem Benutzerregister spezifische Abgleiche vorhanden sein. Des Weiteren lässt EIM 1:n-Abgleiche zu (d. h., mehrere Benutzer verwenden eine einzige Benutzeridentität in einem einzigen Benutzerregister).

Die Möglichkeit, die Identitäten eines Benutzers über mehrere Benutzerregister hinweg abzugleichen, bietet zahlreiche Vorteile. Der Hauptvorteil besteht darin, dass Anwendungen ein Benutzerregister für Authentifizierungen und ein anderes Benutzerregister für Berechtigungen nutzen können. Beispielsweise kann ein Administrator eine Windows-Benutzeridentität in einem Kerberos-Register mit einem i5/OS-Benutzerprofil in einem anderen Benutzerregister abgleichen, um auf i5/OS-Ressourcen zuzugreifen, für die das i5/OS-Benutzerprofil eine Berechtigung hat.

EIM ist eine offene Architektur, in der Administratoren Identitätsabgleichbeziehungen für alle Register darstellen können. Es ist nicht erforderlich, die vorhandenen Daten in ein neues Repository zu kopieren und beide Kopien zu synchronisieren. Die einzigen neuen Daten, die durch EIM hinzugefügt werden,

sind die Beziehungsinformationen. EIM speichert diese Daten in einem LDAP-Verzeichnis. So können die Daten an einem Ort verwaltet werden, gleichzeitig können überall dort Replikate zur Verfügung stehen, wo die Daten verwendet werden. EIM ermöglicht Unternehmen und Anwendungsentwicklern zudem die Verwendung einer breiteren Palette von Umgebungen bei geringeren Kosten, was ohne diese Unterstützung unmöglich wäre.

EIM wird in Verbindung mit dem Netzwerkauthentifizierungsservice (i5/OS-Implementierung von Kerberos) verwendet und stellt zusammen mit diesem Produkt eine Einzelanmeldungslösung zur Verfügung. Es besteht die Möglichkeit, Anwendungen zu schreiben, die GSS-APIs und EIM verwenden, um Kerberos-Tickets zu akzeptieren und Abgleiche mit anderen zugeordneten Benutzeridentitäten in einem anderen Benutzerregister durchzuführen. Die Zuordnung zwischen Benutzeridentitäten mit diesem Identitätsabgleich kann wie folgt durchgeführt werden: durch die Erstellung von Kennungszuordnungen, die über eine EIM-Kennung eine Benutzeridentität indirekt einer anderen zuordnen, oder durch die Erstellung von Richtlinienzuordnungen, die eine Benutzeridentität in einer Gruppe einer einzigen spezifischen Benutzeridentität direkt zuordnen.

Zum Einsatz von Identitätsabgleichen muss der Administrator die folgenden Aufgaben ausführen:

1. Eine EIM-Domäne im Netzwerk konfigurieren. Sie können mit dem EIM-Konfigurationsassistenten für iSeries einen Domänencontroller für die Domäne erstellen und den Zugriff auf diese Domäne konfigurieren. Mit dem Assistenten können Sie festlegen, dass eine neue EIM-Domäne erstellt und ein Domänencontroller auf dem lokalen oder einem fernen System erstellt werden soll. Ist eine EIM-Domäne bereits vorhanden, können Sie festlegen, dass das System zu einer vorhandenen EIM-Domäne gehören soll.
2. Die auf dem Directory-Server mit dem EIM-Domänencontroller definierten Benutzer bestimmen, die über die Berechtigung zur Verwaltung und zum Zugriff auf spezielle Informationen in der EIM-Domäne verfügen, und diese entsprechenden EIM-Zugriffssteuerungsgruppen zuordnen.
3. EIM-Registerdefinitionen für die Benutzerregister, die zur EIM-Domäne gehören, erstellen. Sie können zwar alle Benutzerregister in einer EIM-Domäne definieren, es müssen jedoch Benutzerregister für die EIM-fähigen Anwendungen und Betriebssysteme definiert werden.
4. Basierend auf dem EIM-Implementierungsbedarf festlegen, welche der folgenden Tasks für die EIM-Konfiguration ausgeführt werden sollen:
   - EIM-Kennungen für jeden eindeutigen Benutzer in der Domäne und Kennungszuordnungen für diese Benutzer erstellen.
   - Richtlinienzuordnungen erstellen.
   - Eine Kombination dieser Zuordnungen erstellen.

   Zugehörige Informationen

   Einzelanmeldung

Enterprise Identity Mapping - Konzepte

In diesem Abschnitt werden wichtige EIM-Konzepte erläutert, die Sie für eine erfolgreiche Implementierung von EIM benötigen.

Sie müssen die in Enterprise Identity Mapping (EIM) verwendeten Konzepte kennen, um zu verstehen, wie Sie EIM in Ihrem Unternehmen einsetzen können. Obwohl die Konfiguration und Implementierung von EIM-APIs abhängig von der Serverplattform variieren kann, sind die EIM-Konzepte auf allen IBM @server -Plattformen gleich.

Abbildung 1 stellt eine mögliche EIM-Implementierung in einem Unternehmen dar. Dabei arbeiten drei Server als EIM-Clients und enthalten EIM-fähige Anwendungen, die mit Hilfe von EIM-Suchoperationen EIM-Daten anfordern 6 . Der Domänencontroller 1 dient zur Speicherung von Informationen zur

EIM-Domäne 2 . Hierzu gehören EIM-Kennungen 3 , Zuordnungen 4 zwischen diesen EIM-Kennungen und Benutzeridentitäten sowie EIM-Registerdefinitionen 5 .

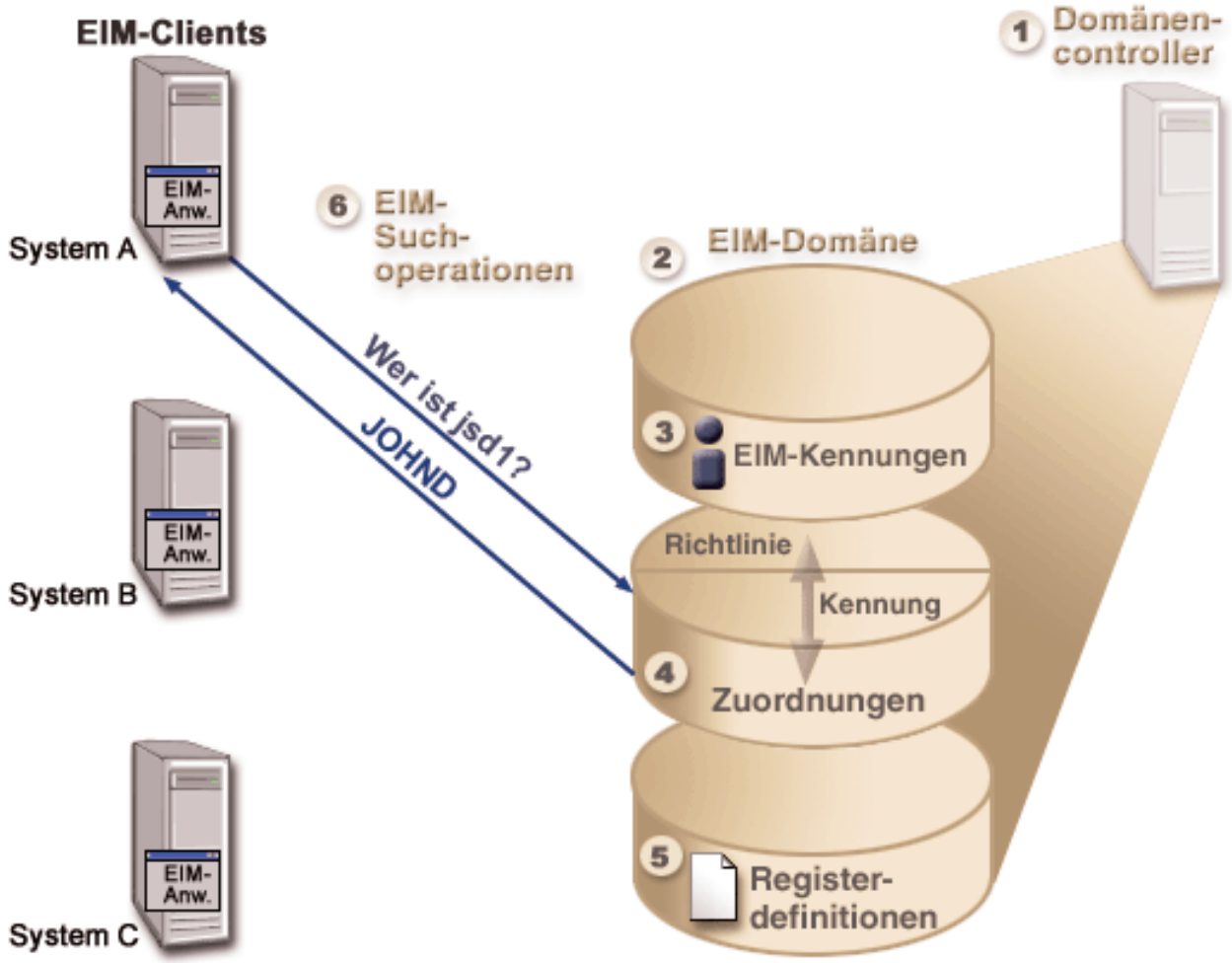


Abbildung 1. Beispiel für eine EIM-Implementierung

Die folgenden Abschnitte enthalten weitere Informationen über diese EIM-@server -Konzepte:

Zugehörige Konzepte

„LDAP-Konzepte für EIM" auf Seite 50
In diesem Abschnitt wird erläutert, wie Sie LDAP (Lightweight Directory Access Protocol) zusammen mit EIM (EIM = Enterprise Identity Mapping) verwenden können.

„iSeries-Konzepte für EIM" auf Seite 53
In diesem Abschnitt werden alle Anwendungen für Enterprise Identity Mapping (EIM) aufgelistet.

EIM-Domänencontroller

Im Folgenden wird erläutert, in welchen Situationen der Einsatz eines EIM-Domänencontrollers (EIM = Enterprise Identity Mapping) sinnvoll ist.

Ein *EIM-Domänencontroller* ist ein LDAP-Server (LDAP = Lightweight Directory Access Protocol), der für die Verwaltung von mindestens einer EIM-Domäne konfiguriert ist. Eine *EIM-Domäne* ist ein LDAP-Ver-

zeichnis mit allen EIM-Kennungen, EIM-Zuordnungen und Benutzerregistern, die in dieser Domäne definiert sind. Systeme (EIM-Clients) werden in die EIM-Domäne integriert, indem sie die Domänendaten für EIM-Suchoperationen verwenden.

Momentan können Sie den IBM Directory Server auf einigen IBM @server -Plattformen so konfigurieren, dass er als EIM-Domänencontroller eingesetzt werden kann. Der Domäne können alle Systeme, die die EIM-APIs unterstützen, als Clients hinzugefügt werden. Diese Clientsysteme verwenden die EIM-APIs, um eine Verbindung zu einem EIM-Domänencontroller herzustellen und EIM-Suchoperationen durchzuführen. Der Standort des EIM-Clients legt fest, ob es sich bei dem EIM-Domänencontroller um ein lokales oder fernes System handelt. Der Domänencontroller ist *lokal*, wenn der EIM-Client auf dem gleichen System wie der Domänencontroller ausgeführt wird. Der Domänencontroller ist *fern*, wenn der EIM-Client auf einem anderen System als der Domänencontroller ausgeführt wird.

Anmerkung: Wenn Sie planen, einen Directory-Server auf einem fernen System zu konfigurieren, muss der Directory-Server EIM-Unterstützung zur Verfügung stellen. EIM setzt voraus, dass sich der Domänencontroller auf einem Directory-Server befindet, der Lightweight Directory Access Protocol (LDAP) Version 3 unterstützt. Darüber hinaus muss das Directory-Server-Produkt so konfiguriert werden, dass es das EIM-Schema akzeptiert. Diese Unterstützung wird von IBM Directory Server for iSeries und IBM Directory Server V5.1 bereitgestellt.

EIM-Domäne

In diesem Abschnitt wird erläutert, wie eine Domäne zur Speicherung aller vorhandenen Kennungen verwendet werden kann.

In EIM (Enterprise Identity Mapping) wird als *Domäne* ein Verzeichnis innerhalb eines LDAP-Servers (Lightweight Directory Access Protocol) bezeichnet, in dem sich EIM-Daten eines Unternehmens befinden. Eine EIM-Domäne enthält alle EIM-Kennungen, EIM-Zuordnungen und Benutzerregister, die in dieser Domäne definiert sind, sowie die Zugriffssteuerung für die Daten. Systeme (EIM-Clients) werden in die Domäne integriert, indem sie die Domänendaten für EIM-Suchoperationen verwenden.

Eine EIM-Domäne ist nicht mit einem Benutzerregister zu verwechseln. Ein Benutzerregister definiert eine Gruppe von Benutzeridentitäten, die von einer bestimmten Betriebssystem- oder Anwendungsinstanz erkannt und als vertrauenswürdig eingestuft werden. Darüber hinaus enthält ein Benutzerregister die erforderlichen Informationen, um den Benutzer der Identität zu authentifizieren. Des Weiteren beinhaltet ein Benutzerregister häufig zusätzliche Attribute, z. B. Benutzereinstellungen, Systemberechtigungen oder persönliche Daten für die Identität.

Eine EIM-Domäne *verweist* hingegen auf Benutzeridentitäten, die in Benutzerregistern definiert sind. Die EIM-Domäne enthält Informationen über die *Beziehung* zwischen den Identitäten in unterschiedlichen Benutzerregistern (Benutzername, Registertyp und Registerinstanz) und den eigentlichen Personen oder Entitäten, die diese Identitäten repräsentieren.

In Abbildung 2 werden die Daten dargestellt, die in einer EIM-Domäne gespeichert sind. Hierzu zählen EIM-Kennungen, EIM-Registerdefinitionen und EIM-Zuordnungen. Die EIM-Daten definieren die Beziehungen zwischen Benutzeridentitäten und den Personen oder Entitäten, die von diesen Identitäten im Unternehmen repräsentiert werden.

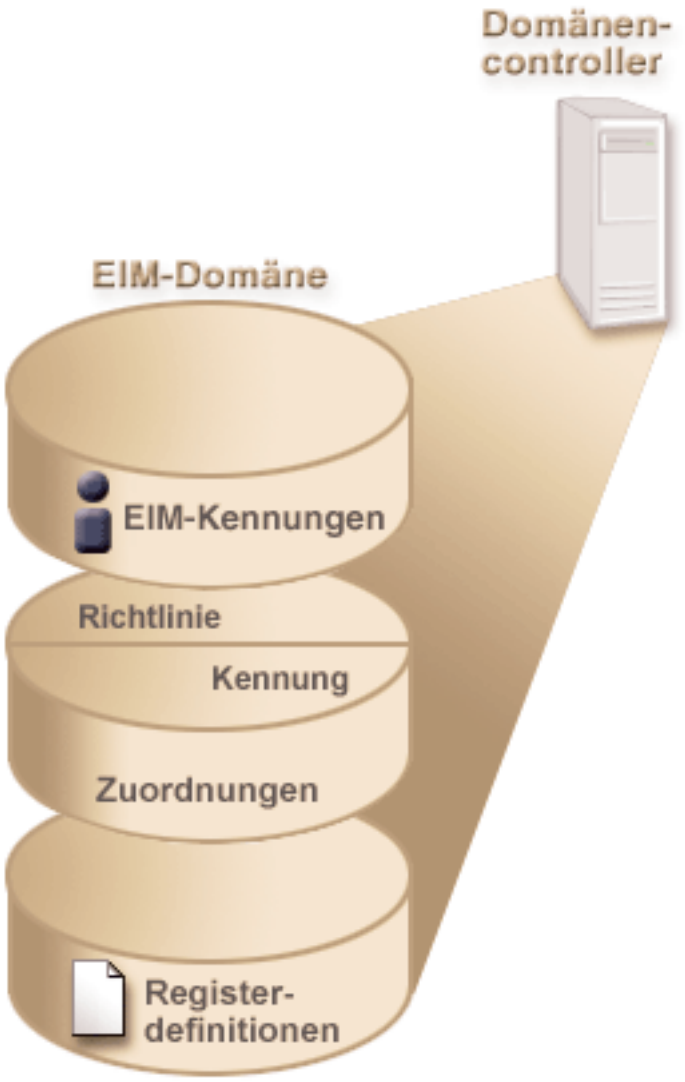


Abbildung 2. EIM-Domäne und in der Domäne gespeicherte Daten

EIM-Daten:

EIM-Registerdefinitionen
Jede von Ihnen erstellte EIM-Registerdefinition repräsentiert ein Benutzerregister (sowie die enthaltenen Benutzeridentitätsdaten), das auf einem System innerhalb des Unternehmens vorhanden ist. Sobald Sie ein bestimmtes Benutzerregister in EIM definieren, kann dieses der EIM-Domäne hinzugefügt werden. Sie können zwei Arten von Registerdefinitionen erstellen: für Systembenutzerregister und für Anwendungsbenutzerregister.

EIM-Kennungen
Jede von Ihnen erstellte EIM-Kennung stellt eine eindeutige Identifikation einer Person oder Entität (z. B. einen Druck- oder einen Dateiserver) innerhalb des Unternehmens dar. Sie können eine EIM-Kennung erstellen, wenn Sie 1:1-Abgleiche zwischen den Benutzeridentitäten für eine Person oder Entität, der die EIM-Kennung entspricht, durchführen möchten.

EIM-Zuordnungen
Die von Ihnen erstellten EIM-Zuordnungen repräsentieren Beziehungen zwischen Benutzeridentitäten. Zuordnungen müssen definiert werden, damit EIM-Clients mit EIM-APIs erfolgreich EIM-Suchoperationen ausführen können. Bei diesen EIM-Suchoperationen wird eine EIM-Domäne nach definierten Zuordnungen durchsucht. Sie können zwei Zuordnungstypen erstellen:

Kennungszuordnungen

Kennungszuordnungen ermöglichen es Ihnen, über eine EIM-Kennung, die für eine Person festgelegt wurde, eine 1:1-Beziehung zwischen Benutzeridentitäten zu definieren. Jede von Ihnen erstellte EIM-Kennungszuordnung repräsentiert eine einzelne, spezifische Beziehung zwischen einer EIM-Kennung und einer zugeordneten Benutzeridentität innerhalb des Unternehmens. Kennungszuordnungen stellen die erforderlichen Informationen zur Verfügung, die eine EIM-Kennung einer bestimmten Benutzeridentität in einem bestimmten Benutzerregister zuordnen und dem Benutzer die Möglichkeit bieten, einen 1:1-Identitätsabgleich für einen Benutzer durchzuführen. Kennungszuordnungen sind besonders nützlich, wenn Einzelpersonen Benutzeridentitäten mit Sonderberechtigungen und anderen Berechtigungen besitzen, die Sie durch die Erstellung von 1:1-Abgleichen zwischen deren Benutzeridentitäten gesondert steuern möchten.

Richtlinienzuordnungen

Mit Richtlinienzuordnungen können Sie eine Beziehung zwischen einer Gruppe von Benutzeridentitäten in einem oder mehreren Benutzerregistern und einer einzelnen Benutzeridentität in einem anderen Benutzerregister definieren. Jede EIM-Richtlinienzuordnung, die Sie erstellen, resultiert in einem n:1-Abgleich zwischen der Quellengruppe von Benutzeridentitäten in einem Benutzerregister und einer einzelnen Zielbenutzeridentität. Normalerweise erstellen Sie Richtlinienzuordnungen, um eine Gruppe von Benutzern, die alle dieselbe Berechtigungsstufe benötigen, einer einzelnen Benutzeridentität zuzuordnen, die über diese Berechtigungsstufe verfügt.

Zugehörige Konzepte

„EIM-Registerdefinitionen" auf Seite 12
In diesem Abschnitt wird erläutert, wie Sie eine Registerdefinition erstellen können, in der alle Benutzerregister Ihres Systems gespeichert werden.

„EIM-Kennung"
In diesem Abschnitt wird erläutert, wie Kennungen für einen Benutzer oder eine Entität innerhalb Ihres Unternehmens erstellt werden können.

„EIM-Suchoperationen" auf Seite 29
In diesem Abschnitt wird der Prozess des EIM-Abgleichs (EIM = Enterprise Identity Mapping) erläutert. Außerdem werden in diesem Abschnitt entsprechende Beispiele dargestellt.

EIM-Kennung

In diesem Abschnitt wird erläutert, wie Kennungen für einen Benutzer oder eine Entität innerhalb Ihres Unternehmens erstellt werden können.

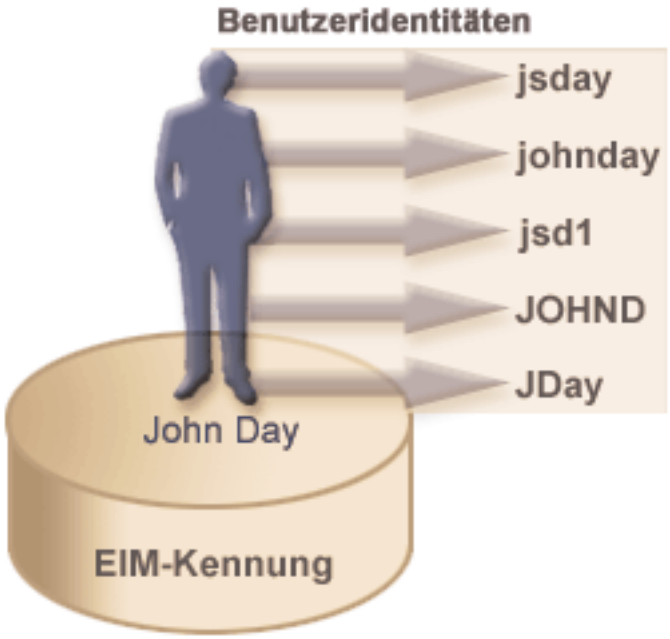
In EIM (Enterprise Identity Mapping) steht eine *Kennung* für eine Person oder Entität innerhalb eines Unternehmens. Ein typisches Netzwerk besteht aus verschiedenen Hardwareplattformen und Anwendungen sowie den zugehörigen Benutzerregistern. Die meisten Plattformen und zahlreiche Anwendungen verwenden plattform- bzw. anwendungsspezifische Benutzerregister. Diese Benutzerregister enthalten alle Identifikationsdaten für die Benutzer, die diese Server oder Anwendungen nutzen.

Sie können mit EIM eindeutige EIM-Kennungen für Personen oder Entitäten in Ihrem Unternehmen erstellen. Anschließend können Sie Kennungszuordnungen bzw. 1:1-Identitätsabgleiche zwischen der EIM-Kennung und den verschiedenen Benutzeridentitäten für die Person oder Entität, die die EIM-Kennung repräsentiert, erstellen. Dieser Prozess vereinfacht die Erstellung heterogener, vielschichtiger Anwendungen. Darüber hinaus vereinfacht die Erstellung von EIM-Kennungen und Zuordnungen die Entwicklung und Verwendung von Tools für die Verwaltung der einzelnen Benutzeridentitäten einer Person oder Entität innerhalb des Unternehmens.

EIM-Kennung für eine Person

In Abbildung 3 ist ein Beispiel für eine EIM-Kennung zu sehen, die die Person *John Day* und deren verschiedene Benutzeridentitäten im Unternehmen repräsentiert. In diesem Beispiel besitzt die Person *John Day* fünf Benutzeridentitäten in vier verschiedenen Benutzerregistern: `johnday`, `jsd1`, `JOHND`, `jsday` und `JDay`.

Abbildung 3: Beziehung zwischen der EIM-Kennung für *John Day* und dessen Benutzeridentitäten

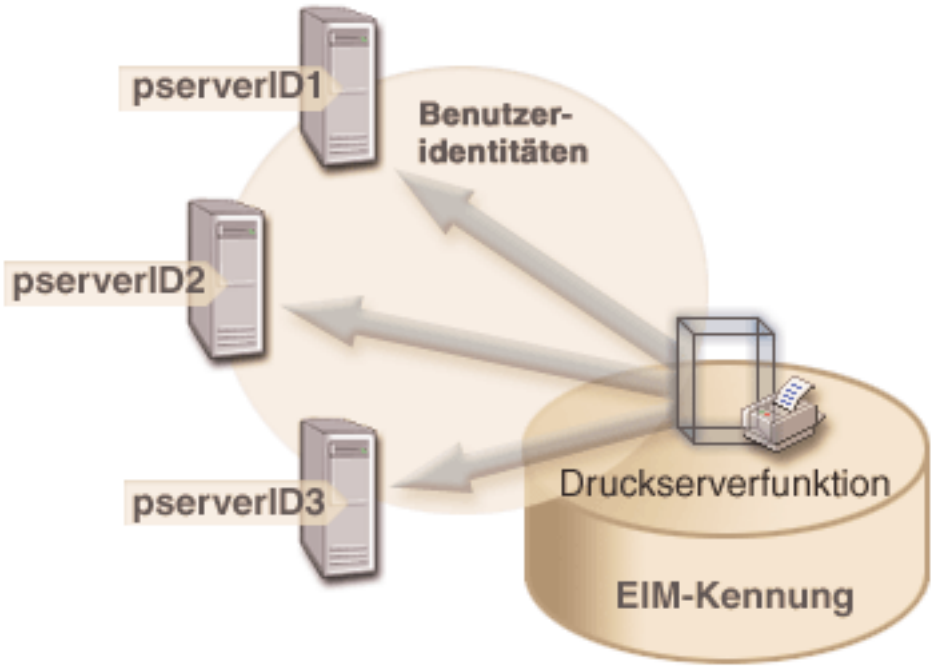


In EIM können Sie Zuordnungen erstellen, die die Beziehung zwischen der Kennung `John Day` und den einzelnen Benutzeridentitäten für *John Day* definieren. Durch die Erstellung von Zuordnungen, die die Beziehungen definieren, können Sie sowie andere Personen Anwendungen entwickeln, die mit Hilfe der EIM-APIs eine benötigte, aber unbekannte Benutzeridentität anhand einer bekannten Benutzeridentität suchen.

EIM-Kennung für eine Entität

EIM-Kennungen können jedoch nicht nur Personen, sondern auch Entitäten innerhalb des Unternehmens repräsentieren (siehe Abbildung 4). Die Druckserverfunktion wird in einem Unternehmen beispielsweise häufig auf verschiedenen Systemen ausgeführt. In Abbildung 4 wird die Druckserverfunktion in einem Unternehmen auf drei unterschiedlichen Systemen und mit drei unterschiedlichen Benutzeridentitäten (`pserverID1`, `pserverID2` und `pserverID3`) ausgeführt.

Abbildung 4: Beziehung zwischen der EIM-Kennung für die Druckserverfunktion und den verschiedenen Benutzeridentitäten für diese Funktion



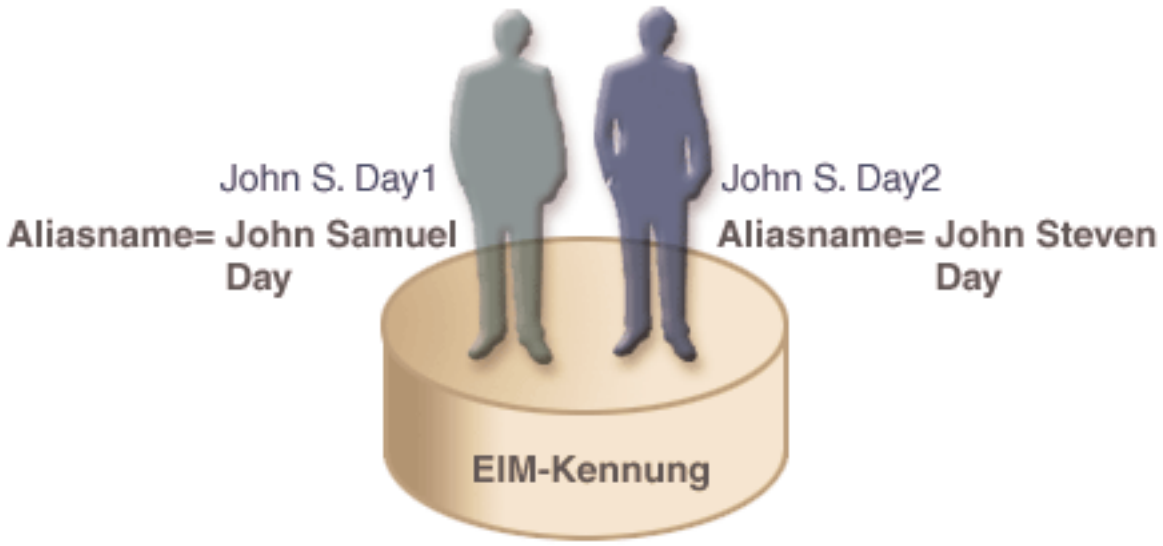
Mit EIM können Sie eine einzige Kennung für die Druckserverfunktion im gesamten Unternehmen erstellen. In diesem Beispiel stellt die EIM-Kennung `Druckserverfunktion` die Entität Druckserverfunktion im Unternehmen dar. Um die Beziehungen zwischen der EIM-Kennung (`Druckserverfunktion`) und den einzelnen Benutzeridentitäten für diese Funktion (`pserverID1`, `pserverID2` und `pserverID3`) zu definieren, werden Zuordnungen erstellt. Diese Zuordnungen ermöglichen Anwendungsentwicklern, mit Hilfe von EIM-Suchoperationen eine bestimmte Druckserverfunktion zu suchen. Anwendungslieferanten können anschließend verteilte Anwendungen schreiben, die eine einfachere Verwaltung der Druckserverfunktion im gesamten Unternehmen ermöglichen.

EIM-Kennungen und Aliasnamen

Die Namen von EIM-Kennungen müssen innerhalb der EIM-Domäne eindeutig sein. Aliasnamen sind daher in Situationen hilfreich, in denen die Verwendung eindeutiger Kennungsnamen problematisch ist. Aliasnamen für EIM-Kennungen sind beispielsweise hilfreich, wenn der rechtsgültige Name sich von dem verwendeten Namen einer Person unterscheidet. Gibt es in einem Unternehmen beispielsweise mehrere Mitarbeiter mit dem gleichen Namen, kann die Verwendung von Eigennamen als EIM-Kennung zu Verwechslungen führen.

In dem Beispiel in Abbildung 5 gibt es in einem Unternehmen zwei Benutzer mit dem Namen *John S. Day*. Der EIM-Administrator erstellt zwei unterschiedliche EIM-Kennungen, um diese zu unterscheiden: `John S. Day1` und `John S. Day2`. Es ist jedoch nicht sofort ersichtlich, welche Kennung für welchen *John S. Day* eingerichtet wurde.

Abbildung 5: Aliasnamen für zwei EIM-Kennungen mit demselben Eigennamen *John S. Day*



Durch die Verwendung von Aliasnamen kann der EIM-Administrator weitere Informationen zu der Person angeben, die der jeweiligen EIM-Kennung zugeordnet ist. Jede EIM-Kennung kann über mehrere Aliasnamen verfügen, die angeben, für welchen *John S. Day* die EIM-Kennung verwendet wird. Dieser zusätzliche Aliasname könnte beispielsweise die Personalnummer, die Abteilungsnummer, die Positionsbezeichnung oder ein anderes Attribut enthalten. Beispiel: Der Aliasname für `John S. Day1` könnte `John Samuel Day` und der Aliasname für `John S. Day2` könnte `John Steven Day` lauten.

Sie können die Aliasinformationen verwenden, um eine spezifische EIM-Kennung leichter zu finden. Eine Anwendung, die EIM verwendet, kann einen Aliasnamen angeben, um die entsprechende EIM-Kennung für die Anwendung zu suchen. Ein Administrator kann diesen Aliasnamen einer EIM-Kennung hinzufügen, damit die Anwendung für EIM-Operationen den Aliasnamen an Stelle des eindeutigen Kennungsnamens verwenden kann. Eine Anwendung kann diese Informationen bei Verwendung der API "Get EIM Target Identities from the Identifier" (`eimGetTargetFromIdentifier()`) angeben, um eine EIM-Suchoperation für die zugehörige Benutzeridentität auszuführen und die entsprechende benötigte Benutzeridentität zu suchen.

Zugehörige Konzepte

„EIM-Domäne" auf Seite 7
In diesem Abschnitt wird erläutert, wie eine Domäne zur Speicherung aller vorhandenen Kennungen verwendet werden kann.

EIM-Registerdefinitionen

In diesem Abschnitt wird erläutert, wie Sie eine Registerdefinition erstellen können, in der alle Benutzerregister Ihres Systems gespeichert werden.

Eine EIM-*Registerdefinition* (EIM = Enterprise Identity Mapping) ist ein Eintrag in EIM, den Sie erstellen, um ein reales Benutzerregister darzustellen, das auf einem System im Unternehmen vorhanden ist. Ein Benutzerregister funktioniert wie ein Verzeichnis und enthält eine Liste der gültigen Benutzeridentitäten für ein bestimmtes System oder eine bestimmte Anwendung. Ein Basisbenutzerregister enthält Benutzeridentitäten und die zugehörigen Kennwörter. Ein Beispiel hierfür ist das Register für z/OS Security Server Resource Access Control Facility (RACF). Darüber hinaus können Benutzerregister weitere Informationen enthalten. Ein LDAP-Verzeichnis (Lightweight Directory Access Protocol) enthält beispielsweise registrierte Namen (Distinguished Name, DN) für Bindevorgänge, Kennwörter und Zugriffssteuerungen für die in LDAP gespeicherten Daten. Weitere Beispiele für häufig verwendete Benutzerregister sind die Principals in einem Kerberos-Realm oder die Benutzeridentitäten in einer Windows Active Directory-Domäne und das i5/OS-Benutzerprofilregister.

Des Weiteren können Sie Benutzerregister innerhalb anderer Benutzerregister definieren. Manche Anwendungen verwenden eine Untergruppe der Benutzeridentitäten aus einer einzelnen Instanz eines Benutzerregisters. Das Register von z/OS Security Server (RACF) kann beispielsweise bestimmte Benutzerregister enthalten, die eine Untergruppe der Benutzer innerhalb des RACF-Benutzerregisters umfassen.

EIM-Registerdefinitionen liefern Informationen über die Benutzerregister in einem Unternehmen. Der Administrator definiert diese Register in EIM, indem er folgende Informationen angibt:

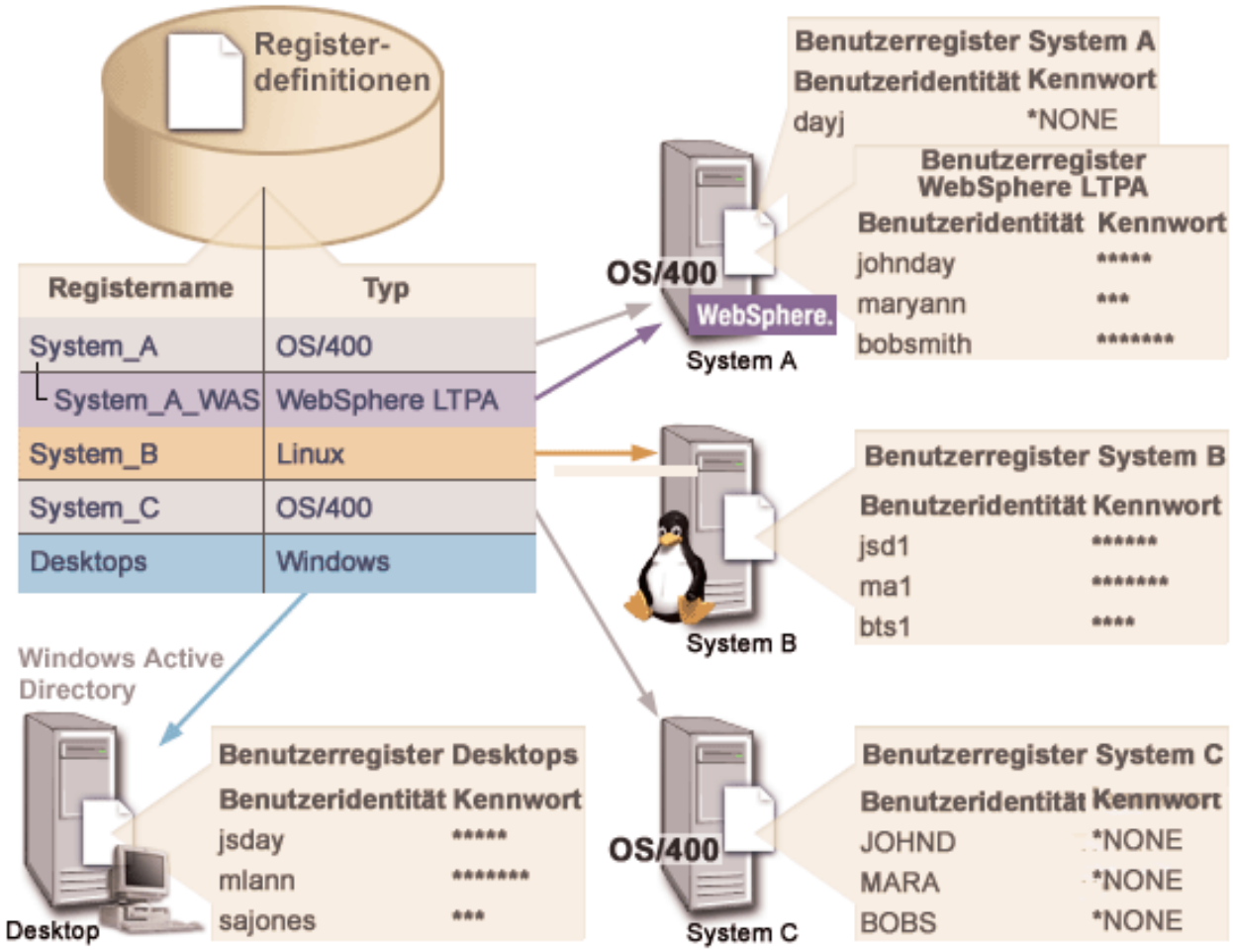
- Einen willkürlichen eindeutigen Namen für das EIM-Register. Jede Registerdefinition stellt eine einzelne Instanz eines Benutzerregisters dar. Sie sollten daher für die EIM-Registerdefinition einen Namen wählen, der die Identifikation der jeweiligen Benutzerregisterinstanz erleichtert. Verwenden Sie beispielsweise den TCP/IP-Hostnamen für ein Systembenutzerregister oder den Hostnamen zusammen mit dem Anwendungsnamen für ein Anwendungsbenutzerregister. Es können beliebige Kombinationen alphanumerischer Zeichen in Groß- und Kleinschreibung sowie Leerzeichen verwendet werden, um einen eindeutigen EIM-Registerdefinitionsnamen zu erstellen.
- Den Typ des Benutzerregisters. EIM stellt eine Reihe vordefinierter Benutzerregistertypen zur Verfügung, die die Benutzerregister der meisten Betriebssysteme abdecken. Dazu gehören:
  - AIX
  - Domino - ausgeschriebener Name
  - Domino - Kurzname
  - Kerberos
  - Kerberos - Beachtung der Groß-/Kleinschreibung erforderlich
  - LDAP
  - LDAP - Kurzname
  - Linux
  - Novell Directory Server
  - Andere
  - Andere - Beachtung der Groß-/Kleinschreibung erforderlich
  - i5/OS (oder OS/400)
  - Tivoli Access Manager
  - RACF
  - Windows - lokal
  - Windows-Domäne (Kerberos) - Beachtung der Groß-/Kleinschreibung erforderlich
  - X.509

Anmerkung: Obwohl die vordefinierten Registerdefinitionstypen die meisten Benutzerregister der Betriebssysteme abdecken, müssen Sie möglicherweise eine Registerdefinition erstellen, für die EIM keinen vordefinierten Registertyp beinhaltet. In dieser Situation haben Sie zwei Optionen. Sie können entweder eine vorhandene Registerdefinition verwenden, die mit den Kenndaten Ihres Registers übereinstimmt, oder Sie können einen privaten Benutzerregistertyp definieren. Beispiel: In Abbildung 6 hat der Administrator den erforderlichen Prozess ausgeführt und den Registertyp für die Anwendungsregisterdefinition `System_A_WAS` als `WebSphere LTPA` definiert.

In Abbildung 6 hat der Administrator EIM-Systemregisterdefinitionen für die Benutzerregister von System A, System B und System C sowie für eine Windows Active Directory-Komponente mit den Kerberos-Principals erstellt, die die Benutzer zur Anmeldung an ihren Desktop-Workstations verwenden. Außerdem hat der Administrator eine Anwendungsregisterdefinition für WebSphere (R) Lightweight Third-Party Authentication (LTPA) erstellt, die auf System A ausgeführt wird. Der Registerdefinitionsname, den der Administrator verwendet, erleichtert die Identifikation der jeweiligen Instanz dieses Benutzerregistertyps. Eine IP-Adresse oder ein Hostname reicht für viele Typen von Benutzerregistern häufig aus. In diesem Beispiel verwendet der Administrator `System_A_WAS` als Namen der Anwendungsregisterdefinition,

um diese spezifische Instanz der Anwendung WebSphere LTPA anzugeben. Er gibt auch an, dass das übergeordnete Systemregister für die Anwendungsregisterdefinition das Register `System_A` ist.

Abbildung 6: EIM-Registerdefinitionen für fünf Benutzerregister in einem Unternehmen



Anmerkung: Soll der Aufwand für die Kennwortverwaltung weiter reduziert werden, definiert der Administrator in Abbildung 6 für die Kennwörter des i5/OS-Benutzerprofils auf System A und System C den Wert *NONE. In diesem Fall konfiguriert der Administrator eine Einzelanmeldungsumgebung, und die Benutzer arbeiten ausschließlich mit EIM-fähigen Anwendungen wie z. B. iSeries Navigator. Aus diesem Grund möchte der Administrator die Kennwörter aus den entsprechenden i5/OS-Benutzerprofilen entfernen, so dass sowohl er als auch die Benutzer weniger Kennwörter verwalten müssen.

Zugehörige Konzepte

„EIM-Domäne" auf Seite 7
In diesem Abschnitt wird erläutert, wie eine Domäne zur Speicherung aller vorhandenen Kennungen verwendet werden kann.

Systemregisterdefinitionen

Im Folgenden finden Sie Informationen zur Erstellung eines Benutzerregisters für bestimmte Systeme.

Eine Systemregisterdefinition ist ein Eintrag, den Sie in EIM (Enterprise Identity Mapping) erstellen, um ein bestimmtes Benutzerregister auf einer Workstation oder einem Server darzustellen und zu beschrei-

ben. Sie können eine EIM-Systemregisterdefinition für ein Benutzerregister erstellen, wenn das Register im Unternehmen eine der folgenden Eigenschaften aufweist:

- Das Register wird von einem Betriebssystem wie AIX, i5/OS oder von einem Produkt zur Sicherheitsverwaltung wie z/OS Security Server Resource Access Control Facility (RACF) zur Verfügung gestellt.
- Das Register enthält Benutzeridentitäten, die in einer bestimmten Anwendung wie Lotus Notes eindeutig sind.
- Das Register enthält verteilte Benutzeridentitäten, z. B. Kerberos-Principals oder registrierte LDAP-Namen (Lightweight Directory Access Protocol).

EIM-Suchoperationen werden unabhängig davon, ob ein EIM-Administrator ein Register als System oder Anwendung definiert, korrekt ausgeführt. Separate Registerdefinitionen ermöglichen jedoch die Verwaltung von Abgleichdaten auf Anwendungsbasis. Die Verantwortung für die Verwaltung anwendungsspezifischer Abgleiche kann einem Administrator für ein bestimmtes Register übertragen werden.

Anwendungsregisterdefinitionen

Im Folgenden wird erläutert, wie Benutzerregister für bestimmte Anwendungen erstellt werden können.

Eine Anwendungsregisterdefinition ist ein EIM-Eintrag, den Sie erstellen, um eine Untergruppe der Benutzeridentitäten zu beschreiben und darzustellen, die in einem Systemregister definiert sind. Diese Benutzeridentitäten verwenden eine gemeinsame Gruppe von Attributen oder Merkmalen, mit denen sie eine bestimmte Anwendung oder Anwendungsgruppe nutzen können. Anwendungsregisterdefinitionen repräsentieren Benutzerregister, die in anderen Benutzerregistern vorhanden sind. Das Register von z/OS Security Server (RACF) kann beispielsweise bestimmte Benutzerregister enthalten, die eine Teilmenge von Benutzern innerhalb des RACF-Gesamtbenutzerregisters darstellen. Auf Grund dieser Beziehung müssen Sie für jede Anwendungsregisterdefinition, die Sie erstellen, den Namen des übergeordneten Systemregisters angeben.

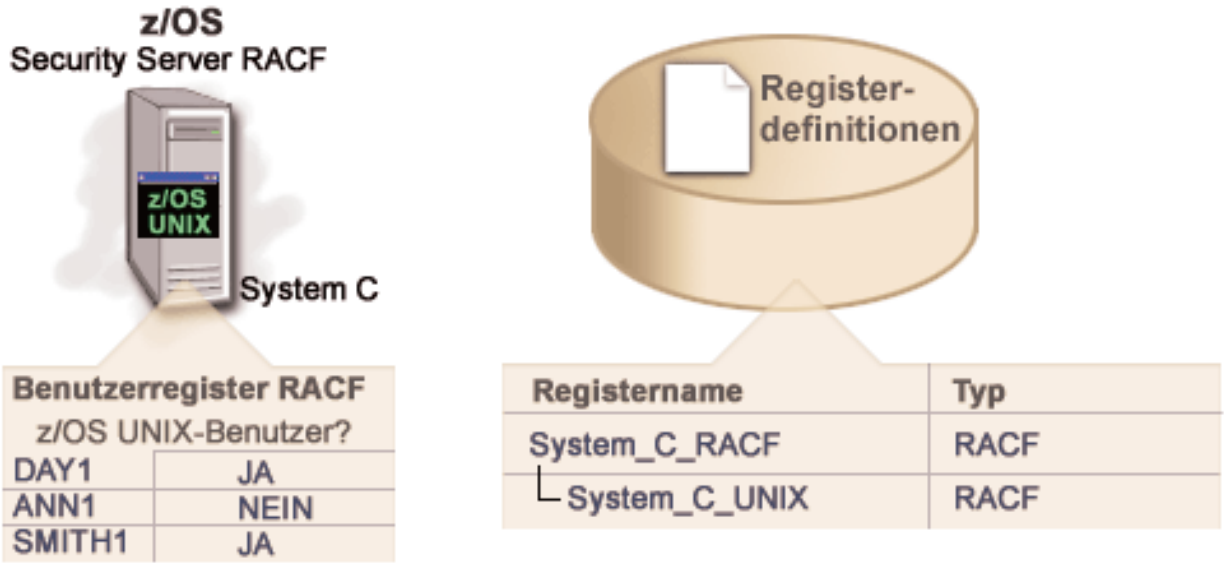
Sie können eine EIM-Anwendungsregisterdefinition für ein Benutzerregister erstellen, wenn die Benutzeridentitäten im Register die folgenden Eigenschaften besitzen:

- Die Benutzeridentitäten für eine Anwendung sind nicht in einem für die Anwendung spezifischen Benutzerregister gespeichert.
- Die Benutzeridentitäten für eine Anwendung sind in einem Systemregister gespeichert, das Benutzeridentitäten für andere Anwendungen enthält.

EIM-Suchoperationen werden unabhängig davon, ob ein EIM-Administrator eine Anwendungs- oder Systemregisterdefinition für ein Benutzerregister erstellt, korrekt ausgeführt. Separate Registerdefinitionen ermöglichen jedoch die Verwaltung von Abgleichdaten auf Anwendungsbasis. Die Verantwortung für die Verwaltung anwendungsspezifischer Abgleiche kann einem Administrator für ein bestimmtes Register übertragen werden.

Beispiel: In Abbildung 7 ist zu sehen, wie ein EIM-Administrator eine Systemregisterdefinition für ein z/OS Security Server RACF-Register erstellt hat. Darüber hinaus hat der Administrator eine Anwendungsregisterdefinition für die Benutzeridentitäten innerhalb des RACF-Registers erstellt, die z/OS(TM) UNIX System Services (z/OS UNIX) verwenden. System C enthält ein RACF-Benutzerregister mit Informationen für drei Benutzeridentitäten, `DAY1`, `ANN1` und `SMITH1`. Zwei dieser Benutzeridentitäten (`DAY1` und `SMITH1`) greifen auf z/OS UNIX auf System C zu. Diese Benutzeridentitäten sind RACF-Benutzer mit eindeutigen Attributen, durch die sie als Benutzer von z/OS UNIX identifiziert werden. Innerhalb der EIM-Registerdefinitionen hat der EIM-Administrator `System_C_RACF` als RACF-Gesamtbenutzerregister definiert. Darüber hinaus hat der Administrator festgelegt, dass `System_C_UNIX` die Benutzeridentitäten mit z/OS UNIX-Attributen repräsentieren soll.

Abbildung 7: EIM-Registerdefinitionen für das RACF-Benutzerregister und für Benutzer von z/OS UNIX



Gruppenregisterdefinitionen

Im Folgenden wird die Erstellung einer Gruppenregisterdefinition in einer EIM-Domäne erläutert, die zur Beschreibung und Darstellung einer Gruppe von Registerdefinitionen dient.

Durch die logische Gruppierung der Registerdefinitionen kann der Arbeitsaufwand für die Konfiguration des EIM-Abgleichs reduziert werden. Sie können eine Gruppenregisterdefinition in ähnlicher Weise verwalten wie eine einzelne Registerdefinition.

Alle Mitglieder der Gruppenregisterdefinition enthalten normalerweise mindestens eine allgemeine Benutzeridentität, für die eine Ziel- oder Quellenzuordnung erstellt werden soll. Durch die Zusammenfassung von Mitgliedern zu Gruppen können Sie an Stelle mehrerer Zuordnungen lediglich eine Zuordnung erstellen, die dann für die Gruppenregisterdefinition und die Benutzeridentität gilt.

Beispiel: John Day meldet sich bei seinem Primärsystem mit der Benutzeridentität `jday` an und verwendet dann auf mehreren Systemen dieselbe Benutzeridentität (`JOHND`). Aus diesem Grund umfasst das Benutzerregister für alle Systeme die Benutzeridentität `JOHND`. Normalerweise erstellt John Day eine separate Zielzuordnung zwischen der EIM-Kennung John Day und den einzelnen Benutzerregistern, die die Benutzeridentität `JOHND` enthalten. Um den Arbeitsaufwand zur Konfiguration des EIM-Abgleichs zu reduzieren, kann er eine Gruppenregisterdefinition mit allen Benutzerregistern erstellen, in denen die Benutzeridentität `JOHND` als Gruppenmitglied definiert ist. Anschließend kann er dann eine einzige Zielzuordnung zwischen der EIM-Kennung `John Day` und der Gruppenregisterdefinition erstellen, anstatt mehrere Zielzuordnungen zwischen der EIM-Kennung John Day und den einzelnen Registerdefinitionen zu definieren. Diese einzelne Zielzuordnung zur Gruppenregisterdefinition ermöglicht der Benutzeridentität von John Day (`jday`) die Zuordnung zur Benutzeridentität `JOHND`.

Für Gruppenregisterdefinitionen gelten die folgenden Bedingungen:

- Für alle Mitglieder (einzelne Registerdefinitionen) der Gruppenregisterdefinition muss dieselbe Einstellung für die Beachtung der Groß-/Kleinschreibung gelten.
- Alle Mitglieder (einzelne Registerdefinitionen) der Gruppenregisterdefinition müssen in der EIM-Domäne definiert werden, bevor sie zu einer Gruppenregisterdefinition hinzugefügt werden können.
- Eine Registerdefinition kann Mitglied mehrerer Gruppen sein, es sollte jedoch vermieden werden, ein bestimmtes Benutzerregister als Mitglied mehrerer Gruppenregisterdefinitionen anzugeben, da es sonst

zu mehrdeutigen Ergebnissen bei Suchoperationen kommen kann. Die Gruppenregisterdefinition darf kein Mitglied einer anderen Gruppenregisterdefinition sein.

EIM-Zuordnungen

Im Folgenden wird erläutert, wie Sie zugeordnete Identitäten in unterschiedlichen Benutzerregistern verwenden können.

In EIM (EIM = Enterprise Identity Mapping) wird als *Zuordnung* ein Eintrag bezeichnet, den Sie in einer EIM-Domäne erstellen, um eine Beziehung zwischen Benutzeridentitäten in verschiedenen Benutzerregistern zu definieren. Der Typ der Zuordnung, die Sie erstellen, bestimmt, ob die definierte Beziehung direkt oder indirekt ist. Sie können einen von zwei Zuordnungstypen in EIM erstellen: Kennungszuordnungen und Richtlinienzuordnungen. Sie können Richtlinienzuordnungen an Stelle von oder in Verbindung mit Kennungszuordnungen verwenden. Die Verwendung von Zuordnungen ist von Ihrem Gesamtplan zur EIM-Implementierung abhängig.

In den folgenden Abschnitten finden Sie weitere Informationen zur Verwendung von Zuordnungen:

Suchinformationen

Im Folgenden erfahren Sie, wie Sie Suchinformationen (optionale Daten) verwenden können, um eine Zielbenutzeridentität näher zu beschreiben. Diese Zielbenutzeridentität wird von den EIM-APIs bei Abgleichsuchoperationen verwendet, um die Suche nach der gesuchten Zielbenutzeridentität weiter zu präzisieren.

Im aktuellen Release können Sie diese als Suchinformationen bezeichneten *optionalen* Daten zur näheren Bestimmung einer Zielbenutzeridentität angeben. Diese Zielbenutzeridentität kann in einer Kennungs- oder Richtlinienzuordnung angegeben werden. Die Suchinformationen werden in Form einer eindeutigen Zeichenfolge angegeben und können von der EIM-API `eimGetTargetFromSource` bzw. `eimGetTargetFromIdentifier` bei einer Abgleichsuchoperation verwendet werden, um die Suche nach der Zielbenutzeridentität, die Objekt der Operation ist, weiter einzugrenzen. Die Daten, die Sie als Suchinformationen angeben, entsprechen dem Parameter für zusätzliche Informationen über Registerbenutzer, den Sie für diese EIM-APIs verwenden.

Suchinformationen sind nur erforderlich, wenn eine Abgleichsuchoperation mehrere Zielbenutzeridentitäten zurückgeben kann. Dies ist der Fall, wenn eine oder mehrere der folgenden Bedingungen zutreffen:

- Eine EIM-Kennung besitzt mehrere einzelne Zielzuordnungen zu demselben Zielregister.
- In einer Quellenzuordnung ist für mehrere EIM-Kennungen dieselbe Benutzeridentität angegeben, und jede dieser EIM-Kennungen hat eine Zielzuordnung zu demselben Zielregister, obwohl die Benutzeridentität, die für die einzelnen Zielzuordnungen angegeben wurde, jeweils eine andere sein kann.
- Mehrere Standardrichtlinienzuordnungen für Domänen geben dasselbe Zielregister an.
- Mehrere Standardrichtlinienzuordnungen für Domänen geben dasselbe Quellen- und Zielregister an.
- Mehrere Richtlinienzuordnungen für Zertifikatfilter geben dasselbe X.509-Register, denselben Zertifikatfilter und dasselbe Zielregister an.

Anmerkung: Eine Abgleichsuchoperation, die mehrere Zielbenutzeridentitäten zurückgibt, kann bei EIM-fähigen Anwendungen einschließlich der i5/OS-Anwendungen und -Produkte, die nicht für die Verarbeitung dieser mehrdeutigen Ergebnisse konzipiert sind, Probleme verursachen. Die i5/OS-Basisanwendungen wie z. B. iSeries Access für Windows sind nicht in der Lage, anhand von Suchinformationen mehrere von einer Suchoperation zurückgegebene Zielbenutzeridentitäten zu unterscheiden. Daher sollten Sie überprüfen, ob es sinnvoll ist, die für die Domäne vorhandenen Zuordnungen erneut zu definieren. Auf diese Weise kann sichergestellt werden, dass eine Abgleichsuchoperation eine einzige Zielbenutzeridentität zurückgeben kann. So kann gewährleistet werden, dass die i5/OS-Basisanwendungen Suchoperationen ausführen und Identitäten abgleichen können.

Sie können Suchinformationen verwenden, um zu vermeiden, dass Abgleichsuchoperationen mehrere Zielbenutzeridentitäten zurückgeben. Dazu müssen Sie für jede Zielbenutzeridentität in jeder Zuordnung eindeutige Suchinformationen definieren. Diese Suchinformationen müssen für die Abgleichsuchoperation angegeben werden, um sicherzustellen, dass die Operation eine eindeutige Zielbenutzeridentität zurückgeben kann. Andernfalls sind Anwendungen, die auf EIM basieren, möglicherweise nicht in der Lage, zu bestimmen, welche Zielbenutzeridentität verwendet werden soll.

Beispiel: Sie verfügen über eine EIM-Kennung `John Day` mit zwei Benutzerprofilen auf System A. Eines dieser Benutzerprofile ist `JDUSER` auf System A, und das andere Benutzerprofil ist `JDSECADM`, das die Sonderberechtigung des Sicherheitsadministrators besitzt. Es gibt zwei Zielzuordnungen für die Kennung "John Day". Eine dieser Zielzuordnungen ist für die Benutzeridentität `JDUSER` im Zielregister `System_A` definiert. Für `JDUSER` ist die Suchinformation `Benutzerberechtigung` angegeben. Die andere Zielzuordnung ist für die Benutzeridentität `JDSECADM` im Zielregister `System_A` vorgesehen. Für `JDSECADM` wurde die Suchinformation `Sicherheitsbeauftragter` angegeben.

Wird für eine Abgleichsuchoperation keine Suchinformation angegeben, gibt die Suchoperation sowohl die Benutzeridentität `JDUSER` als auch die Benutzeridentität `JDSECADM` zurück. Wenn für eine Abgleichsuchoperation die Suchinformation `Benutzerberechtigung` angegeben wird, gibt die Suchoperation nur die Benutzeridentität `JDUSER` zurück. Und wenn für eine Abgleichsuchoperation die Suchinformation `Sicherheitsbeauftragter` angegeben wird, gibt die Suchoperation nur die Benutzeridentität `JDSECADM` zurück.

Anmerkung: Löschen Sie die letzte Zielzuordnung für eine Benutzeridentität (unabhängig davon, ob es sich um eine Kennungszuordnung oder eine Richtlinienzuordnung handelt), werden auch die Zielbenutzeridentität und alle Suchinformationen aus der Domäne gelöscht.

Da Sie viele Möglichkeiten haben, Richtlinienzuordnungen für Zertifikate und andere Zuordnungen zu verwenden und die Vorgehensweisen sich überschneiden, müssen Sie mit der Unterstützung von EIM-Abgleichrichtlinien und der Funktionsweise von Suchoperationen gut vertraut sein, bevor Sie Richtlinienzuordnungen für Zertifikatfilter erstellen und verwenden.

Kennungszuordnungen

In diesem Abschnitt wird beschrieben, wie Sie Kennungszuordnungen zur Beschreibung von Beziehungen zwischen einer EIM-Kennung (EIM = Enterprise Identity Mapping) und den Benutzeridentitäten einer Person in Benutzerregistern verwenden können. Eine Kennungszuordnung erstellt einen direkten 1:1-Abgleich zwischen einer EIM-Kennung und einer bestimmten Benutzeridentität. Sie können Kennungszuordnungen verwenden, um über die EIM-Kennung indirekt eine Beziehung zwischen Benutzeridentitäten zu definieren.

Eine EIM-Kennung steht für eine Person oder Entität in einem Unternehmen. Eine EIM-Kennungszuordnung beschreibt die Beziehung zwischen einer EIM-Kennung und einer einzelnen Benutzeridentität in einem Benutzerregister, die ebenfalls diese Person repräsentiert. Wenn Sie Zuordnungen zwischen einer EIM-Kennung und allen Benutzeridentitäten einer Person oder Entität erstellen, erzeugen Sie ein einziges, vollständiges Abbild von der Ressourcenverwendung dieser Person oder Entität innerhalb eines Unternehmens.

Benutzeridentitäten dienen zur Authentifizierung und/oder Berechtigung. Als *Authentifizierung* bezeichnet man die Überprüfung, ob eine Entität oder Person, die eine Benutzeridentität eingibt, berechtigt ist, diese Identität zu verwenden. Im Rahmen dieser Überprüfung muss die Person, die die Benutzeridentität übergibt, häufig geheime oder private Informationen über die Benutzeridentität eingeben, z. B. ein Kennwort. Als *Berechtigung* wird der Prozess bezeichnet, durch den sichergestellt wird, dass eine korrekt authentifizierte Benutzeridentität nur die Funktionen ausführen bzw. auf die Ressourcen zugreifen kann, für die sie berechtigt ist. Früher mussten fast alle Anwendungen die Identitäten in einem einzigen Benutzerregister sowohl für Authentifizierungen als auch für Berechtigungen verwenden. Über EIM-Suchoperationen stehen Anwendungen nun Benutzeridentitäten für die Authentifizierung in einem Benutzerregister und für zugeordnete Benutzeridentitäten für Berechtigungen in einem anderen Benutzerregister zur Verfügung.

Die EIM-Kennung stellt eine indirekte Zuordnung zwischen diesen Benutzeridentitäten zur Verfügung, die Anwendungen ermöglicht, basierend auf einer bekannten Benutzeridentität eine andere Benutzeridentität für eine EIM-Kennung zu ermitteln. EIM verfügt über APIs, mit deren Hilfe Anwendungen eine unbekannte Benutzeridentität in einem bestimmten Benutzerregister (Ziel) suchen. Dabei wird eine bekannte Benutzeridentität in einem beliebigen anderen Benutzerregister (Quelle) angegeben. Dieser Prozess wird als Identitätsabgleich (Identity Mapping) bezeichnet.

In EIM kann ein Administrator drei verschiedene Zuordnungstypen zwischen einer EIM-Kennung und einer Benutzeridentität definieren. Die Typen der Kennungszuordnungen sind folgende: Quellenzuordnung, Zielzuordnung, administrative Zuordnung. Der Typ der Zuordnung, die Sie erstellen, hängt davon ab, wie die Benutzeridentität verwendet wird. Beispielsweise erstellen Sie Quellen- und Zielzuordnungen für die Benutzeridentitäten, die Abgleichsuchoperationen nutzen sollen. Normalerweise wird für eine Benutzeridentität, die zur Authentifizierung verwendet wird, eine Quellenzuordnung erstellt. Dann erstellen Sie Zielzuordnungen für die Benutzeridentitäten, die zur Berechtigung verwendet werden.

Bevor Sie eine Kennungszuordnung erstellen können, müssen Sie zunächst die entsprechende EIM-Kennung und die entsprechende EIM-Registerdefinition für das Benutzerregister erstellen, das die zugeordnete Benutzeridentität enthält. Eine Zuordnung definiert die Beziehung zwischen einer EIM-Kennung und einer Benutzeridentität mit Hilfe der folgenden Informationen:

- Name der EIM-Kennung
- Name der Benutzeridentität
- Name der EIM-Registerdefinition
- Zuordnungstyp
- Optional: Suchinformationen zur weiteren Identifizierung der Zielbenutzeridentität in einer Zielzuordnung

Quellenzuordnung

Eine Quellenzuordnung ermöglicht, die Benutzeridentität in einer EIM-Suchoperation als Quelle zu nutzen und eine andere Benutzeridentität zu suchen, die der gleichen EIM-Kennung zugeordnet ist.

Benutzeridentitäten, die zur *Authentifizierung* verwendet werden, sollten über eine Quellenzuordnung mit einer EIM-Kennung verfügen. Sie können z. B. eine Quellenzuordnung für einen Kerberos-Principal erstellen, da diese Form der Benutzeridentität für die Authentifizierung verwendet wird. Soll sichergestellt werden, dass Abgleichsuchoperationen für EIM-Kennungen erfolgreich ausgeführt werden können, müssen Quellen- und Zielzuordnungen für eine einzelne EIM-Kennung zusammen verwendet werden.

Zielzuordnung

Eine Zielzuordnung ermöglicht, dass die Benutzeridentität als Ergebnis einer EIM-Suchoperation zurückgegeben wird. Benutzeridentitäten für Endbenutzer erfordern zumeist nur eine Zielzuordnung.

Benutzeridentitäten, die nicht zur Authentifizierung, sondern für *Berechtigungen* verwendet werden, sollten über eine Zielzuordnung mit einer EIM-Kennung verfügen. Sie können z. B. eine Zielzuordnung für ein i5/OS-Benutzerprofil erstellen, weil diese Form der Benutzeridentität bestimmt, welche Ressourcen und Berechtigungen der Benutzer für ein bestimmtes iSeries-System besitzt. Um sicherzustellen, dass Abgleichsuchoperationen für EIM-Kennungen erfolgreich ausgeführt werden können, müssen Quellen- und Zielzuordnungen für eine einzelne EIM-Kennung verwendet werden.

Beziehung zwischen Quellen- und Zielzuordnung

Um sicherzustellen, dass Abgleichsuchoperationen erfolgreich ausgeführt werden können, müssen Sie mindestens eine Quellen- und eine Zielzuordnung zusammen für eine einzelne EIM-Kennung erstellen.

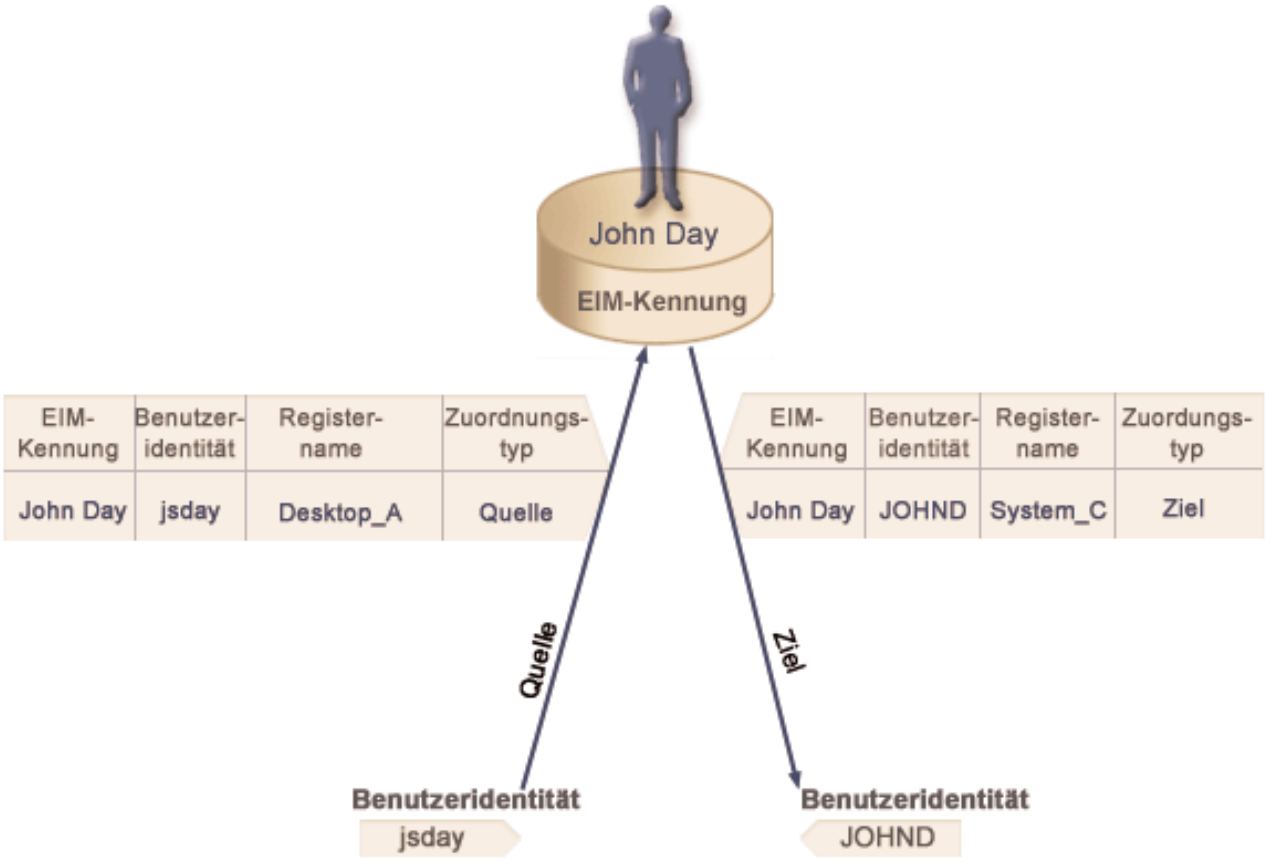
Normalerweise erstellen Sie in einem Benutzerregister für jede Benutzeridentität eine Zielzuordnung, die die Person als Berechtigung für das System oder die Anwendung, dem bzw. der das Benutzerregister entspricht, verwenden kann.

Die Benutzer Ihres Unternehmens melden sich normalerweise am Windows-Desktop an, authentifizieren sich dort und greifen dann auf einen iSeries-Server zu, um eine Reihe von Tasks auszuführen. Benutzer melden sich an ihrem Desktop mit einem Kerberos-Principal und am iSeries-Server mit einem i5/OS-Benutzerprofil an. Sie möchten eine Einzelanmeldungsumgebung erstellen, in der Benutzer sich über den Kerberos-Principal am Desktop anmelden und sich nicht mehr manuell am iSeries-Server authentifizieren müssen.

Dazu erstellen Sie für jeden Benutzer und dessen EIM-Kennung eine Quellenzuordnung für den Kerberos-Principal. Anschließend erstellen Sie für jeden Benutzer und dessen EIM-Kennung eine Zielzuordnung für das i5/OS-Benutzerprofil. Diese Konfiguration stellt sicher, dass i5/OS eine Abgleichsuchoperation ausführen kann, um das richtige Benutzerprofil für einen Benutzer, der nach der Authentifizierung am Desktop auf den iSeries-Server zugreift, zu bestimmen. Unter i5/OS kann der Benutzer dann auf der Basis des entsprechenden Benutzerprofils auf die Ressourcen des Servers zugreifen, ohne sich manuell am Server authentifizieren zu müssen.

Abbildung 6 veranschaulicht ein weiteres Beispiel, in dem ein EIM-Administrator zwei Zuordnungen, eine Quellenzuordnung und eine Zielzuordnung, für die EIM-Kennung `John Day` erstellt, um die Beziehung zwischen dieser Kennung und zwei zugeordneten Benutzeridentitäten zu definieren. Der Administrator erstellt eine Quellenzuordnung für `jsday`, einen Kerberos-Principal im Benutzerregister `Desktops`. Außerdem erstellt der Administrator im Benutzerregister `System_C` eine Zielzuordnung für das i5/OS-Benutzerprofil `JOHND`. Über diese Zuordnungen können Anwendungen im Rahmen einer EIM-Suchoperation eine unbekannte Benutzeridentität (das Ziel `JOHND`) anhand einer bekannten Benutzeridentität (der Quelle `jsday`) ermitteln.

Abbildung 6: EIM-Quellen- und -Zielzuordnungen für die EIM-Kennung `John Day`



| Gehen Sie, um das Beispiel fortzuführen, davon aus, dass der EIM-Administrator feststellt, dass John Day
| auf fünf unterschiedlichen Systemen dasselbe i5/OS-Benutzerprofil (`jsd1`) verwendet. In diesem Fall
| muss der Administrator sechs Zuordnungen für die EIM-Kennung `John Day` erstellen, um die Beziehung
| zwischen dieser Kennung und einer zugeordneten Benutzeridentität in fünf Benutzerregistern zu definie-
| ren. Hierbei werden eine Quellenzuordnung für `johnday`, ein Kerberos-Principal im Benutzerregister
| `Desktop_A` und fünf Zielzuordnungen für `jsd1` (i5/OS-Benutzerprofil) in den fünf Benutzerregistern
| `System_B`, `System_C`, `System_D`, `System_E` und `System_F` erstellt. Zur Reduzierung des Arbeitsaufwandes
| für die Konfiguration der EIM-Abgleiche erstellt der EIM-Administrator eine Gruppenregisterdefinition.
| Die Mitglieder der Gruppenregisterdefinition umfassen die Registerdefinitionsnamen `System_B`,
| `System_C`, `System_D`, `System_E` und `System_F`. Durch die Zusammenfassung von Mitgliedern zu Gruppen
| kann der Administrator eine einzige Zielzuordnung zur Gruppenregisterdefinition und zur Benutzer-
| identität erstellen, anstatt mehrere Zuordnungen zu den einzelnen Registerdefinitionsnamen angeben zu
| müssen. Die Quellen- und die Zielzuordnung bieten für Anwendungen die Möglichkeit, eine unbekannte
| Benutzeridentität (Zielidentität `jsd1`) in den fünf Benutzerregistern anzufordern, die als Mitglieder der
| Gruppenregisterdefinition dargestellt werden. Hierbei wird in einer EIM-Suchoperation eine bekannte
| Benutzeridentität (Quellenidentität `johnday`) verwendet.

Bei bestimmten Benutzern kann es erforderlich sein, für eine einzige Benutzeridentität sowohl eine Quellen- als auch eine Zielzuordnung zu erstellen. Dies ist dann der Fall, wenn ein einziges System als Client und als Server verwendet wird oder wenn es sich bei der Person um einen Administrator handelt.

Anmerkung: Benutzeridentitäten für normale Benutzer erfordern zumeist nur eine Zielzuordnung.

| Bei bestimmten Benutzern kann es erforderlich sein, für eine einzige Benutzeridentität sowohl eine Quellen- als auch eine Zielzuordnung zu erstellen. Dies ist dann der Fall, wenn ein einziges System als Client
| und als Server verwendet wird oder wenn es sich bei der Person um einen Administrator handelt.

Beispielsweise verwendet ein Administrator die Management Central-Funktion im iSeries Navigator, um ein zentrales System und verschiedene Endpunktsysteme zu verwalten. Der Administrator führt verschiedene Funktionen aus, die ihren Ursprung auf dem zentralen System oder einem Endpunktsystem haben. In dieser Situation empfiehlt es sich, für jede der Benutzeridentitäten des Administrators auf allen Systemen eine Quellen- und eine Zielzuordnung zu erstellen. Unabhängig von dem System, das der Administrator für den ersten Zugriff auf eines der anderen Systeme verwendet, wird dadurch sichergestellt, dass die Benutzeridentität, unter der der Zugriff auf das andere System erfolgt, mit der entsprechenden Benutzeridentität für das nächste System, auf das der Administrator zugreift, abgeglichen werden kann.

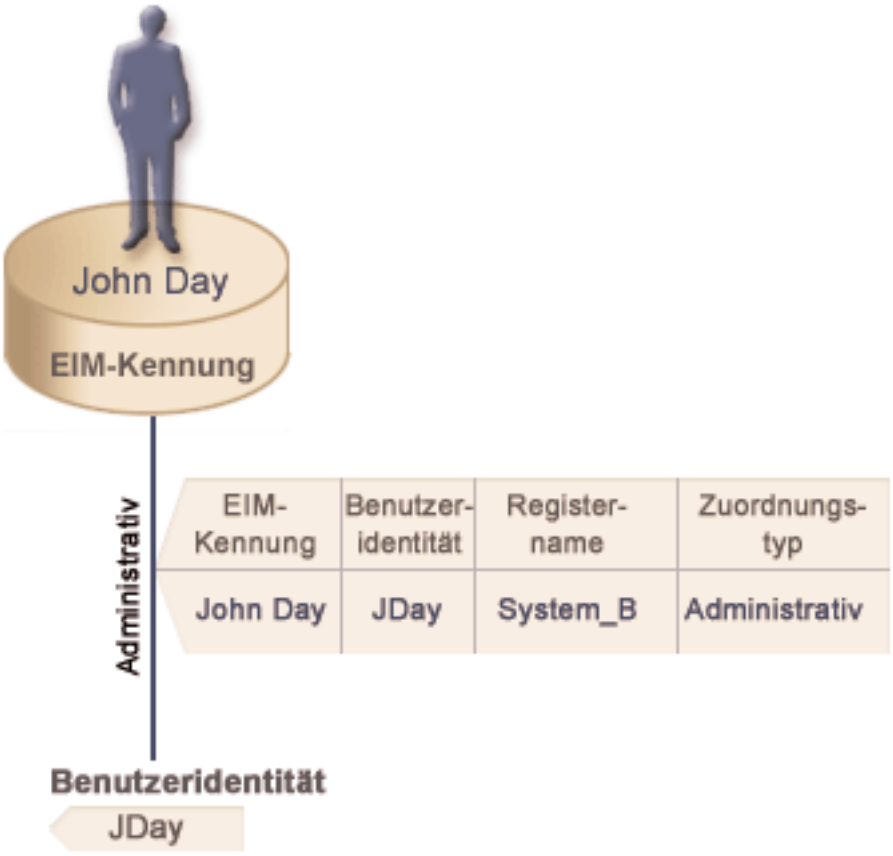
Administrative Zuordnung

Eine administrative Zuordnung für eine EIM-Kennung zeigt zumeist an, dass die mit der EIM-Kennung verknüpfte Person oder Entität eine Benutzeridentität besitzt, die für ein bestimmtes System besondere Überlegungen erfordert. Dieser Zuordnungstyp wird beispielsweise bei hochsensiblen Benutzerregistern verwendet.

Auf Grund der besonderen Beschaffenheit von administrativen Zuordnungen können für diesen Zuordnungstyp keine EIM-Abgleichsuchoperationen durchgeführt werden. Folglich gibt eine EIM-Suchoperation, bei der eine Quellenbenutzeridentität mit einer administrativen Zuordnung angegeben wird, keine Ergebnisse zurück. Ebenso wird eine Benutzeridentität mit einer administrativen Zuordnung nie als Ergebnis einer EIM-Suchoperation zurückgegeben.

In Abbildung 7 ist ein Beispiel für eine administrative Zuordnung zu sehen. In diesem Beispiel besitzt der Mitarbeiter John Day die Benutzeridentität `John_Day` auf System A und die Benutzeridentität `JDay` auf System B, welches hohe Sicherheitsanforderungen stellt. Der Systemadministrator möchte sicherstellen, dass Benutzer sich nur unter Verwendung des lokalen Benutzerregisters am System B authentifizieren können. Er verhindert somit, dass eine Anwendung den Benutzer `John Day` mit einem anderen Authentifizierungsverfahren am System authentifiziert. Die Nutzung einer administrativen Zuordnung für die Benutzeridentität `JDay` auf System B zeigt dem Administrator, dass John Day über ein Konto auf System B verfügt. EIM gibt in EIM-Suchoperationen jedoch keine Informationen über die Identität `JDay` zurück. Selbst wenn auf dem System Anwendungen vorhanden sind, die EIM-Suchoperationen verwenden, können sie keine Benutzeridentitäten mit administrativen Zuordnungen finden.

Abbildung 7: Administrative Zuordnung von EIM für die EIM-Kennung `John Day`



Richtlinienzuordnungen

In diesem Abschnitt wird beschrieben, wie Richtlinienzuordnungen zur Beschreibung einer Beziehung zwischen mehreren Benutzeridentitäten und einer einzelnen Benutzeridentität in einem Benutzerregister verwendet werden.

Die EIM-Abgleichrichtlinie ermöglicht es einem EIM-Administrator, Richtlinienzuordnungen zu erstellen und mit diesen eine Beziehung zwischen mehreren Benutzeridentitäten in einem oder mehreren Benutzerregistern und einer einzelnen Benutzeridentität in einem anderen Benutzerregister zu definieren. Richtlinienzuordnungen verwenden die Unterstützung von EIM-Abgleichrichtlinien, um n:1-Abgleiche zwischen Benutzeridentitäten ohne Einbeziehung von EIM-Kennungen zu erstellen.

Sie können Richtlinienzuordnungen an Stelle von oder in Verbindung mit Kennungszuordnungen verwenden, die 1:1-Abgleiche zwischen einer EIM-Kennung und einer einzelnen Benutzeridentität ermöglichen.

Eine Richtlinienzuordnung wirkt sich nur auf die Benutzeridentitäten aus, für die keine spezifischen einzelnen EIM-Zuordnungen vorhanden sind. Sind spezifische Kennungszuordnungen zwischen einer EIM-Kennung und Benutzeridentitäten vorhanden, wird die Zielbenutzeridentität aus der Kennungszuordnung an die Anwendung, die die Suchoperation ausführt, zurückgegeben, selbst wenn eine Richtlinienzuordnung vorhanden und die Verwendung von Richtlinienzuordnungen aktiviert ist.

Sie können drei Typen von Richtlinienzuordnungen erstellen:

Zugehörige Konzepte

„EIM-Suchoperationen” auf Seite 29
In diesem Abschnitt wird der Prozess des EIM-Abgleichs (EIM = Enterprise Identity Mapping) erläutert. Außerdem werden in diesem Abschnitt entsprechende Beispiele dargestellt.

Standardrichtlinienzuordnungen für Domänen:

Im Folgenden wird erläutert, wie eine Abgleichsbeziehung für alle Benutzeridentitäten in der Domäne eingerichtet werden kann.

Eine Standardrichtlinienzuordnung für Domänen ist eine Art der Richtlinienzuordnung, mit der Sie n:1-Abgleiche zwischen Benutzeridentitäten erstellen können. Sie können mit einer Standardrichtlinienzuordnung für Domänen eine Quellengruppe mehrerer Benutzeridentitäten (in diesem Fall alle Benutzer in der Domäne) mit einer einzelnen Zielbenutzeridentität in einem angegebenen Zielbenutzerregister abgleichen. In einer Standardrichtlinienzuordnung für Domänen stellen alle Benutzer in der Domäne die Quelle der Richtlinienzuordnung dar und werden mit einem einzelnen Zielregister und einer einzelnen Zielbenutzeridentität abgeglichen.

Wenn Sie eine Standardrichtlinienzuordnung für Domänen verwenden möchten, müssen Sie über Richtlinienzuordnungen für Domänen Abgleichsuchen aktivieren. Für das Zielbenutzerregister der Richtlinienzuordnung müssen Sie ebenfalls Abgleichsuchen aktivieren. Wenn Sie diese Aktivierung konfigurieren, können die Benutzerregister in der Richtlinienzuordnung Abgleichsuchoperationen nutzen.

Die Standardrichtlinienzuordnung für Domänen wird wirksam, wenn Kennungszuordnungen, Richtlinienzuordnungen für Zertifikatfilter oder Standardrichtlinienzuordnungen für Register des Zielregisters den Kriterien einer Abgleichsuchoperation nicht entsprechen. Daher werden alle Benutzeridentitäten in der Domäne mit einer einzelnen Zielbenutzeridentität abgeglichen, die in der Standardrichtlinienzuordnung für Domänen angegeben ist.

Beispiel: Sie erstellen eine Standardrichtlinienzuordnung für Domänen mit der Zielbenutzeridentität `John_Day` im Zielregister `Registry_xyz`, und Sie haben keine Kennungszuordnungen oder andere Richtlinienzuordnungen, die mit dieser Benutzeridentität abgeglichen werden, erstellt. Wenn `Registry_xyz` als Zielregister in Suchoperationen angegeben ist, stellt die Standardrichtlinie für Domäne sicher, dass die Zielbenutzeridentität `John_Day` für alle Benutzeridentitäten in der Domäne, für die keine anderen Zuordnungen definiert wurden, zurückgegeben wird.

Sie müssen Folgendes angeben, um eine Standardrichtlinienzuordnung für Domänen zu definieren:

- **Zielregister**. Das Zielregister, das Sie angeben, ist der Name einer EIM-Registerdefinition, die die Benutzeridentität enthält, mit der alle Benutzeridentitäten in der Domäne abgeglichen werden sollen.
- **Zielbenutzer**. Der Zielbenutzer ist der Name der Benutzeridentität, die basierend auf dieser Richtlinienzuordnung als Ziel einer EIM-Abgleichsuchoperation zurückgegeben wird.

Sie können für jedes Register in der Domäne eine Standardrichtlinienzuordnung für Domänen angeben: Wenn zwei oder mehr Richtlinienzuordnungen für Domänen auf dasselbe Zielregister verweisen, müssen Sie für jede dieser Richtlinienzuordnungen eindeutige Suchinformationen definieren, um sicherzustellen, dass sie von den Abgleichsuchoperationen unterschieden werden können. Andernfalls können Abgleichsuchoperationen mehrere Zielbenutzeridentitäten zurückgeben. Infolge dieser mehrdeutigen Ergebnisse sind Anwendungen, die auf EIM basieren, möglicherweise nicht in der Lage, zu bestimmen, welche Zielbenutzeridentität verwendet werden soll.

Da Sie viele Möglichkeiten haben, Richtlinienzuordnungen zu verwenden und die Vorgehensweisen sich überschneiden, müssen Sie mit der Unterstützung von EIM-Abgleichrichtlinien und der Funktionsweise von Suchoperationen gut vertraut sein, bevor Sie Richtlinienzuordnungen erstellen und verwenden.

Anmerkung: Sie wollen eventuell eine Standardrichtlinienzuordnung für Domänen zu einer Zielbenutzeridentität erstellen, die in einer Gruppenregisterdefinition enthalten ist. Alle Benutzer in der Domäne bilden die Quelle der Richtlinienzuordnung und werden einer Zielbenutzeridentität in einer als Ziel verwendeten Gruppenregisterdefinition zugeordnet. Die Benutzeridentität, die Sie in der Standardrichtlinienzuordnung für Domänen definieren, ist in den Mitgliedern der Gruppenregisterdefinition enthalten.

John Day verwendet z. B. auf den fünf folgenden, verschiedenen Systemen dasselbe i5/OS-Benutzerprofil (John_Day): System B, System C, System D, System E und System F. Um den Arbeitsaufwand für die Konfiguration der EIM-Abgleiche zu reduzieren, erstellt der EIM-Administrator eine Gruppenregisterdefiniton mit dem Namen Group_1. Die Mitglieder der Gruppenregisterdefinition haben die Registerdefinitionsnamen System_B, System_C, System_D, System_E und System_F. Durch die Zusammenfassung von Mitgliedern zu Gruppen kann der Administrator eine einzige Zielzuordnung zur Gruppenregisterdefinition und zur Benutzeridentität erstellen, anstatt mehrere Zuordnungen zu den einzelnen Registerdefinitionen angeben zu müssen.

Der EIM-Administrator erstellt eine Standardrichtlinienzuordnung für Domänen und verwendet hierzu die Zielbenutzeridentität John_Day im Zielregister Group_1. Im vorliegenden Fall gilt keine andere spezielle Kennungs- oder Richtlinienzuordnung. Wenn Group_1 in Suchoperationen als Zielregister angegeben wird, garantiert die Standarddomänenrichtlinie, dass die Zielbenutzeridentität John_Day für alle Benutzeridentitäten in der Domäne zurückgegeben wird, für die keine speziellen Kennungszuordnungen definiert sind.

Standardrichtlinienzuordnungen für Register:

Im Folgenden wird erläutert, wie eine Abgleichsbeziehung für alle Benutzeridentitäten in einem einzelnen Register eingerichtet werden kann.

Eine Standardrichtlinienzuordnung für Register stellt eine besondere Art einer Richtlinienzuordnung dar, mit der Sie n:1-Abgleiche zwischen Benutzeridentitäten erstellen können. Sie können mit einer Standardrichtlinienzuordnung für Register eine Quellengruppe mehrerer Benutzeridentitäten (in diesem Fall die Benutzeridentitäten in einem einzelnen Register) einer einzelnen Zielbenutzeridentität in einem angegebenen Zielbenutzerregister zuordnen. In einer Standardrichtlinienzuordnung für Register stellen alle Benutzer in einem bestimmten Register die Quelle der Richtlinienzuordnung dar und werden einem bestimmten Zielregister und einem bestimmten Zielbenutzer zugeordnet.

Wenn Sie Standardrichtlinienzuordnungen für Register verwenden möchten, müssen Sie mit Hilfe entsprechender Richtlinienzuordnungen für die Domäne Abgleichsuchen aktivieren. Außerdem müssen Sie für das Quellenregister Abgleichsuchen und für das Zielregister Abgleichsuchen sowie die Verwendung von Richtlinienzuordnungen aktivieren. Wenn Sie diese Unterstützungsfunktion konfigurieren, können die Benutzerregister in der Richtlinienzuordnung Abgleichsuchoperationen nutzen.

Die Standardrichtlinienzuordnung für Register wird wirksam, wenn für eine Abgleichsuchoperation keine passenden Kennungszuordnungen, Richtlinienzuordnungen für Zertifikatfilter oder anderen Standardrichtlinienzuordnungen für Register für das Zielregister gefunden werden können. Daher werden alle Benutzeridentitäten im Quellenregister mit einer einzelnen Zielbenutzeridentität laut Standardrichtlinienzuordnung für Register abgeglichen.

Beispiel: Sie erstellen eine Standardrichtlinienzuordnung für Register, deren Quellenregister my_realm.com ist. Damit werden Principals in einem bestimmten Kerberos-Realm bezeichnet. Für diese Richtlinienzuordnung geben Sie auch die Zielbenutzeridentität general_user1 im Zielregister i5/OS_system_reg an, bei dem es sich um ein spezielles Benutzerprofil in einem i5/OS-Benutzerregister handelt. In diesem Fall haben Sie keine Kennungszuordnungen oder Richtlinienzuordnungen, die für Benutzeridentitäten im Quellenregister gültig sind, erstellt. Wenn in Suchoperationen als Zielregister i5/OS_system_reg und als Quellenregister my_realm.com angegeben wird, kann mit der Standardrichtlinienzuordnung für Register sichergestellt werden, dass die Zielbenutzeridentität general_user1 für alle Benutzeridentitäten im Register my_realm.com zurückgegeben wird, für die keine speziellen Kennungszuordnungen oder Richtlinienzuordnungen für Zertifikatfilter definiert wurden.

Sie müssen drei Informationen angeben, um eine Standardrichtlinienzuordnung für Register zu definieren:

- **Quellenregister**. Das ist die Registerdefinition, die die Richtlinienzuordnung als Quelle der Zuordnung verwenden soll. Alle Benutzeridentitäten in diesem Quellenbenutzerregister müssen mit dem angegebenen Zielbenutzer der Richtlinienzuordnung abgeglichen werden.
- **Zielregister**. Das Zielregister, das Sie angeben, ist der Name einer EIM-Registerdefinition. Das Zielregister muss die Zielbenutzeridentität enthalten, mit der alle Benutzeridentitäten im Quellenregister abgeglichen werden sollen.
- **Zielbenutzer**. Der Zielbenutzer ist der Name der Benutzeridentität, die als Ziel einer EIM-Abgleichsuchoperation auf der Basis dieser Richtlinienzuordnung zurückgegeben wird.

Sie können mehrere Standardrichtlinienzuordnungen für Register definieren. Wenn zwei oder mehr Richtlinienzuordnungen mit demselben Quellenregister auf dasselbe Zielregister verweisen, müssen Sie für jede dieser Richtlinienzuordnungen eindeutige Suchinformationen definieren, um sicherzustellen, dass sie von den Abgleichsuchoperationen unterschieden werden können. Andernfalls besteht die Möglichkeit, dass Abgleichsuchoperationen mehrere Zielbenutzeridentitäten zurückgeben. Infolge dieser mehrdeutigen Ergebnisse sind Anwendungen, die auf EIM basieren, möglicherweise nicht in der Lage, zu bestimmen, welche Zielbenutzeridentität verwendet werden soll.

Da Sie viele Möglichkeiten haben, Richtlinienzuordnungen zu verwenden und die Vorgehensweisen sich überschneiden, müssen Sie mit der Unterstützung von EIM-Abgleichrichtlinien und der Funktionsweise von Suchoperationen gut vertraut sein, bevor Sie Richtlinienzuordnungen erstellen und verwenden.

Anmerkung: Sie wollen eventuell eine Standardrichtlinienzuordnung für Register zu einer Zielbenutzeridentität erstellen, die in einer Gruppenregisterdefinition enthalten ist. Alle Benutzer im Quellenbenutzerregister bilden die Quelle der Richtlinienzuordnung und werden einer Zielbenutzeridentität in einer als Ziel verwendeten Gruppenregisterdefinition zugeordnet. Die Benutzeridentität, die Sie in der Standardrichtlinienzuordnung für Register definieren, ist in den Mitgliedern der Gruppenregisterdefinition enthalten.

John Day verwendet z. B. auf den fünf folgenden Systemen dasselbe i5/OS-Benutzerprofil `John_Day`: System_B, System_C, System_D, System_E und System_F. Um den Arbeitsaufwand zu reduzieren, der zur Konfiguration des EIM-Abgleichs aufgewendet werden muss, erstellt der EIM-Administrator eine Gruppenregisterdefinition mit dem Namen `Group_1`. Die Mitglieder der Gruppenregisterdefinition umfassen die Registerdefinitionsnamen `System_B`, `System_C`, `System_D`, `System_E` und `System_F`. Durch die Zusammenfassung von Mitgliedern zu Gruppen kann der Administrator eine einzige Zielzuordnung zur Gruppenregisterdefinition und zur Benutzeridentität erstellen, anstatt mehrere Zuordnungen zu den einzelnen Registerdefinitionen angeben zu müssen.

Der EIM-Administrator erstellt eine Standardrichtlinienzuordnung für Register, deren Quellenregister `my_realm.com` ist. Damit werden Principals in einem bestimmten Kerberos-Realm bezeichnet. Für diese Richtlinienzuordnung gibt er außerdem die Zielbenutzeridentität `John_Day` im Zielregister `Group_1` an. Im vorliegenden Fall gelten keine anderen Kennungs- oder Richtlinienzuordnungen. Wenn in Suchoperationen als Zielregister `Group_1` und als Quellenregister `my_realm.com` angegeben wird, kann mit der Standardrichtlinienzuordnung für Register sichergestellt werden, dass die Zielbenutzeridentität `John_Day` für alle Benutzeridentitäten im Register `my_realm.com` zurückgegeben wird, für die keine speziellen Kennungszuordnungen definiert wurden.

Richtlinienzuordnungen für Zertifikatfilter:

Im Folgenden wird erläutert, wie eine Abgleichsbeziehung für eine Gruppe von Benutzeridentitäten (in Form von digitalen Zertifikaten) in einem einzelnen X.509-Register eingerichtet werden kann.

Die Richtlinienzuordnung für Zertifikatfilter können Sie verwenden, um n:1-Abgleiche zwischen Benutzeridentitäten zu erstellen. Sie können mit einer Richtlinienzuordnung für Zertifikatfilter eine Quellengruppe von Zertifikaten mit einer einzelnen Zielbenutzeridentität in einem angegebenen Zielbenutzerregister abgleichen.

In einer Richtlinienzuordnung für Zertifikatfilter müssen Sie eine Gruppe von Zertifikaten in einem einzelnen X.509-Register als Quelle der Richtlinienzuordnung angeben. Diese Zertifikate werden mit einem einzelnen Zielregister und einem einzelnen Zielbenutzer, das bzw. den Sie angeben, abgeglichen. Im Gegensatz zu einer Standardrichtlinienzuordnung für Register, in der alle Benutzer in einem einzelnen Register die Quelle der Richtlinienzuordnung darstellen, ist der Bereich einer Richtlinienzuordnung für Zertifikatfilter flexibler. Sie können eine Untergruppe von Zertifikaten im Register als Quelle angeben. Der Zertifikatfilter, den Sie für die Richtlinienzuordnung angeben, bestimmt den Umfang.

Anmerkung: Wenn Sie alle Zertifikate in einem X.509-Benutzerregister mit einer einzelnen Zielbenutzeridentität abgleichen möchten, müssen Sie eine Standardrichtlinienzuordnung für Register erstellen und verwenden.

Wenn Sie Richtlinienzuordnungen für Zertifikatfilter verwenden möchten, müssen Sie über Richtlinienzuordnungen für die Domäne Abgleichsuchen aktivieren. Außerdem müssen Sie für das Quellenregister Abgleichsuchen und für das Zielregister Abgleichsuchen sowie die Verwendung von Richtlinienzuordnungen aktivieren. Wenn Sie diese Aktivierung konfigurieren, können die Benutzerregister in der Richtlinienzuordnung Abgleichsuchoperationen nutzen.

Wenn als Quellenbenutzeridentität in einer EIM-Abgleichsuchoperation ein digitales Zertifikat definiert ist (nachdem die anfordernde Anwendung zur Formatierung des Namens der Benutzeridentität die EIM-API `eimFormatUserIdentity()` verwendet hat), prüft EIM (Enterprise Identity Mapping) zuerst, ob eine Kennungszuordnung zwischen einer EIM-Kennung und der angegebenen Benutzeridentität vorhanden ist. Ist dies nicht der Fall, vergleicht EIM die im Zertifikat angegebenen Informationen zum registrierten Namen (Distinguished Name, DN) mit den im Filter für die Richtlinienzuordnung ganz oder teilweise angegebenen Informationen zum registrierten Namen. Wenn die Informationen zum registrierten Namen im Zertifikat den Kriterien des Filters entsprechen, gibt EIM die von der Richtlinienzuordnung angegebene Zielbenutzeridentität zurück. Daher werden Zertifikate im X.509-Quellenregister, die den Kriterien des Zertifikatfilters entsprechen, mit der einzelnen Zielbenutzeridentität laut Richtlinienzuordnung für Zertifikatfilter abgeglichen.

Beispiel: Sie erstellen eine Richtlinienzuordnung für Zertifikatfilter, deren Quellenregister `certificates.x509` ist. Dieses Register enthält die Zertifikate für alle Mitarbeiter eines Unternehmens einschließlich derjenigen, die alle Manager der Personalabteilung verwenden, um bestimmte private, interne Webseiten aufzurufen und auf andere Ressourcen über einen iSeries-Server zuzugreifen. Für diese Richtlinienzuordnung können Sie auch die Zielbenutzeridentität `hr_managers` im Zielregister `system_abc`, die ein bestimmtes Benutzerprofil in einem i5/OS-Benutzerregister darstellt, angeben. Um sicherzustellen, dass nur die Zertifikate, die sich auf die Manager der Personalabteilung beziehen, von dieser Richtlinienzuordnung betroffen sind, müssen Sie einen Zertifikatfilter mit dem registrierten Namen des Zertifikatinhabers (Subject Distinguished Name, SDN) `ou=hrmgr,o=myco.com,c=us` angeben.

In diesem Fall haben Sie keine Kennungszuordnungen oder Richtlinienzuordnungen für Zertifikatfilter, die für Benutzeridentitäten im Quellenregister gültig sind, erstellt. Wenn `system_abc` als Zielregister und `certificates.x509` als Quellenregister in Suchoperationen angegeben sind, stellt die Richtlinienzuordnung für Zertifikatfilter daher sicher, dass die Zielbenutzeridentität `hr_managers` für alle Zertifikate im Register `certificates.x509`, die mit dem angegebenen Zertifikatfilter übereinstimmen und für die keine spezifischen Kennungszuordnungen definiert sind, zurückgegeben wird.

Sie müssen die folgenden Informationen angeben, um eine Richtlinienzuordnung für Zertifikatfilter zu definieren:

- **Quellenregister**. Die Quellenregisterdefinition, die Sie angeben, muss ein X.509-Benutzerregister sein. Die Richtlinie für Zertifikatfilter erstellt eine Zuordnung zwischen Benutzeridentitäten in diesem X.509-

Benutzerregister und einer einzelnen, bestimmten Zielbenutzeridentität. Die Zuordnung wird nur für die Benutzeridentitäten im Register angelegt, die mit den Kriterien des Zertifikatfilters, die Sie für diese Richtlinie angeben, übereinstimmen.

- **Zertifikatfilter**. Ein Zertifikatfilter definiert eine Gruppe ähnlicher Zertifikatattribute. Die Richtlinienzuordnung für Zertifikatfilter gleicht alle Zertifikate mit diesen definierten Attributen im X.509-Benutzerregister mit einer spezifischen Zielbenutzeridentität ab. Sie geben den Filter basierend auf einer Kombination aus registriertem Namen des Zertifikatinhabers (Subject Distinguished Name, SDN) und registriertem Namen des Zertifikatausstellers (Issuer Distinguished Name, IDN) an. Die Angaben müssen mit den Zertifikaten, die Sie als Quelle des Abgleichs verwenden möchten, übereinstimmen. Der Zertifikatfilter, den Sie für die Richtlinie angeben, muss bereits in der EIM-Domäne vorhanden sein.
- **Zielregister**. Die Zielregisterdefinition, die Sie angeben, ist das Benutzerregister, das die Benutzeridentität, mit der Sie die mit dem Zertifikatfilter übereinstimmenden Zertifikate abgleichen möchten, enthält.
- **Zielbenutzer**. Der Zielbenutzer ist der Name der Benutzeridentität, die als Ziel einer EIM-Abgleichsuchoperation auf der Basis dieser Richtlinienzuordnung zurückgegeben wird.

Da Sie viele Möglichkeiten haben, Richtlinienzuordnungen für Zertifikate und andere Zuordnungen zu verwenden und die Vorgehensweisen sich überschneiden, müssen Sie mit der Unterstützung von EIM-Abgleichrichtlinien und der Funktionsweise von Suchoperationen gut vertraut sein, bevor Sie Richtlinienzuordnungen für Zertifikatfilter erstellen und verwenden.

Anmerkung: Sie wollen eventuell eine Richtlinienzuordnung für einen Zertifikatfilter mit einer Zielbenutzeridentität erstellen, die in einer Gruppenregisterdefinition enthalten ist. Benutzer im Quellenregister, die die im Zertifikatfilter angegebenen Kriterien erfüllen, bilden die Quelle der Richtlinienzuordnung und werden einer Zielbenutzeridentität zugeordnet, die sich in einer als Ziel verwendeten Gruppenregisterdefinition befindet. Die Benutzeridentität, die Sie in der Richtlinienzuordnung für den Zertifikatfilter definieren, ist in den Mitgliedern der Gruppenregisterdefinition enthalten.

John Day verwendet z. B. auf den fünf folgenden Systemen dasselbe i5/OS-Benutzerprofil (`John_Day`): System B, System C, System D, System E und System F. Um den Arbeitsaufwand für die Konfiguration der EIM-Abgleiche zu reduzieren, erstellt der EIM-Administrator eine Gruppenregisterdefinition. Die Mitglieder der Gruppenregisterdefinition umfassen die Registerdefinitionsnamen `System_B`, `System_C`, `System_D`, `System_E` und `System_F`. Durch die Zusammenfassung von Mitgliedern zu Gruppen kann der Administrator eine einzige Zielzuordnung zur Gruppenregisterdefinition und zur Benutzeridentität erstellen, anstatt mehrere Zuordnungen zu den einzelnen Registerdefinitionen angeben zu müssen.

Der EIM-Administrator erstellt eine Richtlinienzuordnung für Zertifikatfilter, in der eine Untergruppe von Zertifikaten innerhalb eines einzelnen X.509-Registers als Quelle der Richtlinienzuordnung definiert wird. Er gibt die Zielbenutzeridentität `John_Day` im Zielregister `Group_1` an. Im vorliegenden Fall gelten keine anderen, speziellen Kennungszuordnungen oder anderen Richtlinienzuordnungen für Zertifikatfilter. Wenn `Group_1` als Zielregister für Suchoperationen angegeben wird, werden aus diesem Grund alle Zertifikate im X.509-Quellenregister, die den Zertifikatfilterkriterien entsprechen, der angegebenen Zielbenutzeridentität zugeordnet.

Zertifikatfilter:

Im Folgenden wird erläutert, wie eine Richtlinienzuordnung für einen Zertifikatfilter erstellt werden kann, mit dem alle Zertifikate mit definierten Attributen im X.509-Benutzerregister einer bestimmten Zielbenutzeridentität zugeordnet werden können.

Ein Zertifikatfilter definiert eine Gruppe ähnlicher Zertifikatattribute mit registrierten Namen für eine Gruppe von Benutzerzertifikaten in einem X.509-Quellenbenutzerregister. Sie können den Zertifikatfilter

als Basis einer Richtlinienzuordnung für Zertifikatfilter verwenden. Der Zertifikatfilter in einer Richtlinienzuordnung bestimmt, welche Zertifikate im angegebenen X.509-Register mit dem angegebenen Zielbenutzer abgeglichen werden sollen. Diese Zertifikate, die Informationen zum registrierten Namen des Zertifikatinhabers und zum registrierten Namen des Zertifikatausstellers enthalten, die mit den Kriterien des Filters übereinstimmen, werden während der Ausführung der EIM-Abgleichsuchoperationen dem angegebenen Zielbenutzer zugeordnet.

Beispiel: Sie erstellen einen Zertifikatfilter mit dem registrierten Namen des Zertifikatinhabers `o=ibm,c=us`. Alle Zertifikate mit diesen registrierten Namen, die Teil der Informationen zum registrierten Namen des Zertifikatinhabers sind, stimmen mit den Kriterien des Filters überein, z. B. ein Zertifikat mit dem registrierten Namen des Zertifikatinhabers `cn=JohnDay,ou=LegalDept,o=ibm,c=us`. Sind mehrere Zertifikatfilter vorhanden, für die das Zertifikat die Kriterien erfüllt, hat der Zertifikatfilterwert Vorrang, mit dem ein Zertifikat die größte Übereinstimmung hat. Beispiel: Sie haben einen Zertifikatfilter mit dem registrierten Namen des Zertifikatinhabers `o=ibm,c=us` und einen anderen Zertifikatfilter mit dem registrierten Namen des Zertifikatinhabers `ou=LegalDept,o=ibm,c=us`. Wenn sich im X.509-Quellenregister ein Zertifikat mit dem registrierten Namen des Zertifikatinhabers `cn=JohnDay,ou=LegalDept,o=ibm,c=us` befindet, wird der zweite bzw. spezifischere Zertifikatfilter verwendet. Wenn Sie im X.509-Quellenregister ein Zertifikat mit dem registrierten Namen des Zertifikatinhabers `cn=SharonJones,o=ibm,c=us` verwenden, wird der weniger spezifische Zertifikatfilter verwendet, da das Zertifikat mit dessen Kriterien eine größere Übereinstimmung aufweist.

Sie können eine der folgenden Informationen bzw. beide Informationen angeben, um einen Zertifikatfilter zu definieren:

- Registrierter Name des Zertifikatinhabers (Subject Distinguished Name, SDN). Der vollständige oder partielle registrierte Name, den Sie für den Filter angeben, muss dem Abschnitt des digitalen Zertifikats, der für den registrierten Namen des Zertifikatinhabers vorgesehen ist und somit den Eigner des Zertifikats angibt, entsprechen. Sie können den vollständigen registrierten Namen des Zertifikatinhabers bzw. einen oder mehrere partielle registrierte Namen, die möglicherweise den gesamten registrierten Namen des Zertifikatinhabers beinhalten, angeben.
- Registrierter Name des Zertifikatausstellers (Issuer Distinguished Name, IDN). Der vollständige oder partielle registrierte Name, den Sie für den Filter angeben, muss dem Abschnitt des digitalen Zertifikats entsprechen, der für den registrierten Namen des Zertifikatausstellers vorgesehen ist und die Zertifizierungsinstanz, die das Zertifikat ausgestellt hat, bezeichnet. Sie können den vollständigen registrierten Namen des Zertifikatausstellers bzw. einen oder mehrere partielle registrierte Namen, die möglicherweise den gesamten registrierten Namen des Zertifikatausstellers beinhalten, angeben.

Es gibt verschiedene Methoden, mit denen Sie einen Zertifikatfilter erstellen können. Dazu gehört auch die Verwendung der API eimFormatPolicyFilter() (Format EIM Policy Filter) zum Generieren von Zertifikatfiltern. Dabei wird ein Zertifikat als Schablone verwendet, um die notwendigen registrierten Namen - unter Berücksichtigung der Vorgaben zu Reihenfolge und Format für den registrierten Namen des Zertifikatinhabers und den registrierten Namen des Zertifikatausstellers - zu erstellen.

EIM-Suchoperationen

In diesem Abschnitt wird der Prozess des EIM-Abgleichs (EIM = Enterprise Identity Mapping) erläutert. Außerdem werden in diesem Abschnitt entsprechende Beispiele dargestellt.

Eine Anwendung oder ein Betriebssystem verwendet eine EIM-API, um eine *Suchoperation* auszuführen, damit die Anwendung oder das Betriebssystem eine Benutzeridentität in einem Register mit einer anderen Benutzeridentität in einem anderen Register abgleichen kann. Eine EIM-Suchoperation ist ein Prozess, durch den eine Anwendung oder ein Betriebssystem eine unbekannte zugeordnete Benutzeridentität anhand von bekannten und vertrauenswürdigen Informationen in einem bestimmten Zielregister sucht. Anwendungen, die EIM-APIs verwenden, können diese EIM-Suchoperationen nur für Informationen ausführen, die in der EIM-Domäne gespeichert sind. Eine Anwendung kann zwei Arten von EIM-Suchoperationen ausführen. Die Art der Suchoperation ist abhängig vom bereitgestellten Informationstyp: Benutzeridentität oder EIM-Kennung.

Wenn Anwendungen oder Betriebssysteme die API `eimGetTargetFromSource()` verwenden, um eine Zielbenutzeridentität für ein bestimmtes Zielregister abzurufen, müssen Sie eine *Benutzeridentität als Quelle* der Suchoperation zur Verfügung stellen. Damit eine Benutzeridentität als Quelle in einer EIM-Suchoperation benutzt werden kann, muss für sie eine Kennungsquellenzuordnung definiert oder sie muss durch eine Richtlinienzuordnung abgedeckt sein. Wenn eine Anwendung oder ein Betriebssystem diese API verwendet, muss die Anwendung oder das Betriebssystem drei Einzelinformationen angeben:

- Eine Benutzeridentität als Quelle bzw. Ausgangspunkt der Operation.
- Den Namen der EIM-Registerdefinition für die Quellenbenutzeridentität.
- Den Namen der EIM-Registerdefinition, der das Ziel der EIM-Suchoperation ist. Diese Registerdefinition beschreibt das Benutzerregister, das die von der Anwendung gesuchte Benutzeridentität enthält.

Wenn Anwendungen oder Betriebssysteme die API `eimGetTargetFromIdentifier()` verwenden, um eine Benutzeridentität für ein bestimmtes Zielregister abzurufen, müssen Sie eine *EIM-Kennung als Quelle* der EIM-Suchoperation zur Verfügung stellen. Wenn eine Anwendung oder ein Betriebssystem diese API verwendet, muss die Anwendung zwei Einzelinformationen angeben:

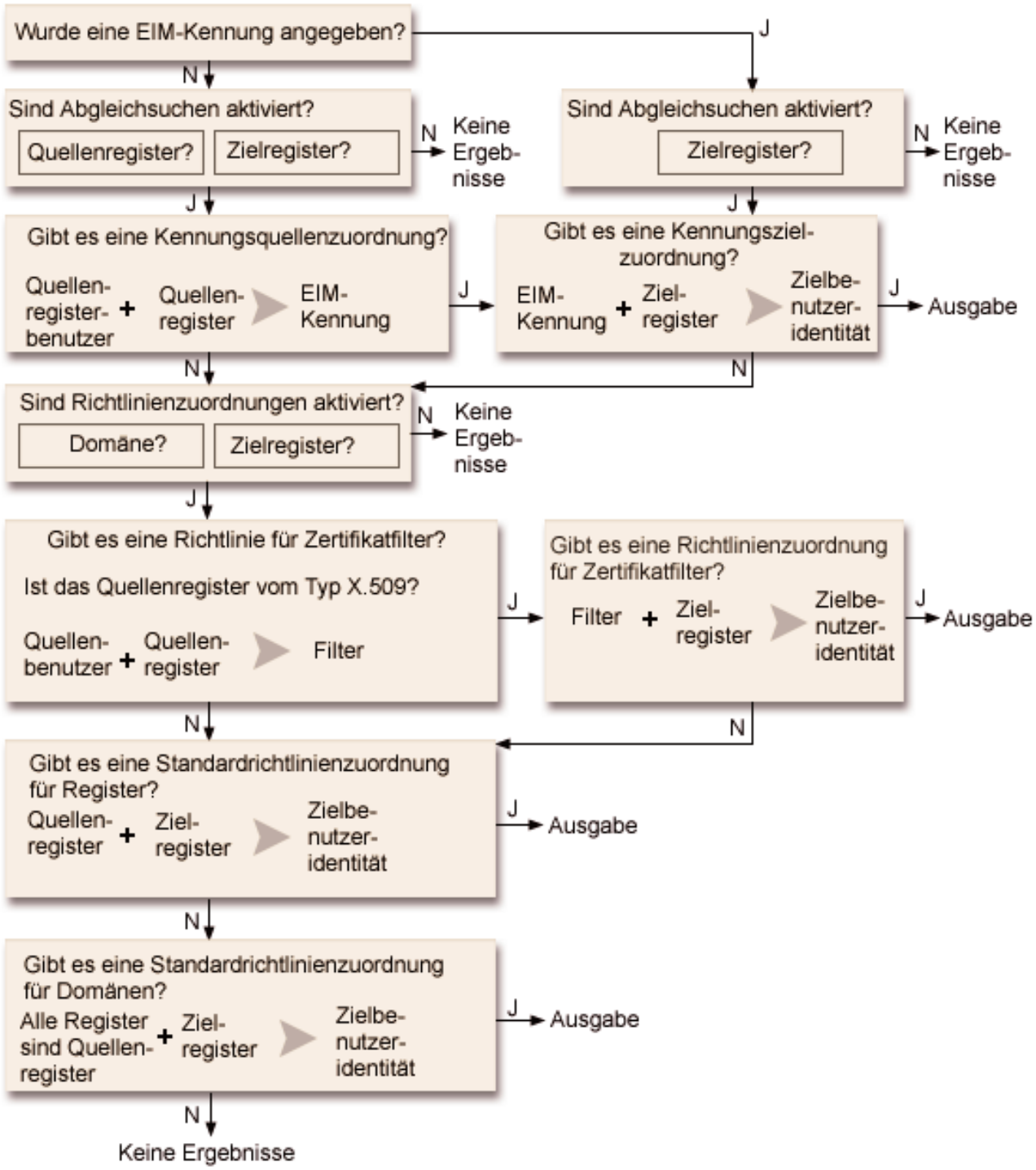
- Eine EIM-Kennung als Quelle oder Ausgangspunkt der Operation.
- Den Namen der EIM-Registerdefinition, der das Ziel der EIM-Suchoperation ist. Diese Registerdefinition beschreibt das Benutzerregister, das die von der Anwendung gesuchte Benutzeridentität enthält.

Für beide Arten der EIM-Suchoperation gilt: Damit eine Benutzeridentität als Ziel zurückgegeben werden kann, muss für die Benutzeridentität eine Zielzuordnung definiert sein. Diese Zielzuordnung kann eine Kennungszuordnung oder eine Richtlinienzuordnung sein.

Die angegebenen Informationen werden an EIM übermittelt. Die EIM-Suchoperation ermittelt anschließend alle Zielbenutzeridentitäten und gibt sie zurück. Die entsprechenden EIM-Daten werden in folgender Reihenfolge durchsucht, wie in Abbildung 10 dargestellt:

1. Kennungszielzuordnung für eine EIM-Kennung. Die EIM-Kennung kann von der API `eimGetTargetFromIdentifier()` angegeben oder anhand der von der API `eimGetTargetFromSource()` bereitgestellten Informationen bestimmt werden.
2. Richtlinienzuordnung für Zertifikatfilter.
3. Standardrichtlinienzuordnung für Register.
4. Standardrichtlinienzuordnung für Domänen.

Abbildung 10: Prozessabfolgediagramm der EIM-Suchoperation



Anmerkung: In der folgenden Prozessabfolge überprüfen die Suchoperationen zuerst die einzelnen Registerdefinitionen wie z. B. zum angegebenen Quellen- oder Zielregister. Wenn mit den Suchoperationen anhand der individuellen Registerdefinition keine Zuordnung gefunden werden kann, wird festgestellt, ob die individuelle Registerdefinition Mitglied einer Gruppenregisterdefinition ist. Ist dies der Fall, überprüft die Suchoperation die Gruppenregisterdefinition, um die Abgleichssuchanforderung auszuführen.

Die Suchoperation läuft auf folgende Weise ab:

1. Die Suchoperation überprüft, ob Abgleichsuchen aktiviert sind. Die Suchoperation bestimmt, ob Abgleichsuchen für das angegebene Quellenregister und/oder das angegebene Zielregister aktiviert sind. Wenn Abgleichsuchen nicht für ein bzw. beide Register aktiviert sind, wird die Suchoperation beendet, ohne dass eine Zielbenutzeridentität zurückgegeben wird.
2. Die Suchoperation überprüft, ob Kennungszuordnungen vorhanden sind, die mit den Suchkriterien übereinstimmen. Wurde eine EIM-Kennung zur Verfügung gestellt, verwendet die Suchoperation den angegebenen EIM-Kennungsnamen. Ist dies nicht der Fall, überprüft die Suchoperation, ob eine bestimmte Kennungsquellenzuordnung, die mit der angegebenen Quellenbenutzeridentität und dem angegebenen Quellenregister übereinstimmt, vorhanden ist. Ist eine solche Zuordnung vorhanden, wird sie von der Suchoperation zur Bestimmung des entsprechenden EIM-Kennungsnamens verwendet. Anhand dieses EIM-Kennungsnamens überprüft die Suchoperation, ob eine Kennungszielzuordnung für die EIM-Kennung, die mit dem Namen der angegebenen EIM-Zielregisterdefinition übereinstimmt, vorhanden ist. Ist dies der Fall, gibt die Suchoperation die in der Zielzuordnung definierte Zielbenutzeridentität zurück.
3. Die Suchoperation überprüft, ob die Verwendung der Richtlinienzuordnungen aktiviert ist. Außerdem überprüft die Suchoperation, ob die Domäne Abgleichsuchen mit Richtlinienzuordnungen zulässt. Darüber hinaus wird überprüft, ob das Zielregister für die Verwendung von Richtlinienzuordnungen aktiviert ist. Wenn die Domäne oder das Register nicht für Richtlinienzuordnungen aktiviert ist, wird die Suchoperation beendet, ohne dass eine Zielbenutzeridentität zurückgegeben wird.
4. Die Suchoperation überprüft, ob Richtlinienzuordnungen für Zertifikatfilter vorhanden sind. Außerdem überprüft die Suchoperation, ob die Verwendung der Richtlinienzuordnungen aktiviert ist. Handelt es sich um ein X.509-Register, wird überprüft, ob eine Richtlinienzuordnung für Zertifikatfilter, die mit dem Namen der Quellen- und Zielregisterdefinition übereinstimmt, vorhanden ist. Darüber hinaus wird überprüft, ob im X.509-Quellenregister Zertifikate, die den in der Richtlinienzuordnung für Zertifikatfilter angegebenen Kriterien entsprechen, vorhanden sind. Wenn eine übereinstimmende Richtlinienzuordnung sowie Zertifikate, die mit den Kriterien des Zertifikatfilters übereinstimmen, vorhanden sind, gibt die Suchoperation die entsprechende Zielbenutzeridentität für diese Richtlinienzuordnung zurück.
5. Die Suchoperation überprüft, ob Standardrichtlinienzuordnungen für Register vorhanden sind. Außerdem überprüft die Suchoperation, ob eine Standardrichtlinienzuordnung für Register, die mit den Namen der Quellen- und der Zielregisterdefinition übereinstimmt, vorhanden ist. Ist dies der Fall, gibt die Suchoperation die entsprechende Zielbenutzeridentität für diese Richtlinienzuordnung zurück.
6. Die Suchoperation überprüft, ob Standardrichtlinienzuordnungen für Domänen vorhanden sind. Außerdem wird überprüft, ob für die Zielregisterdefinition eine Standardrichtlinienzuordnung für Domänen definiert ist. Ist dies der Fall, gibt die Suchoperation die für diese Richtlinienzuordnung zugeordnete Zielbenutzeridentität zurück.
7. Die Suchoperation kann keine Ergebnisse zurückgeben.

Weitere Informationen zu EIM-Suchoperationen finden Sie in den folgenden Beispielen:

Zugehörige Konzepte

„EIM-Domäne" auf Seite 7
In diesem Abschnitt wird erläutert, wie eine Domäne zur Speicherung aller vorhandenen Kennungen verwendet werden kann.

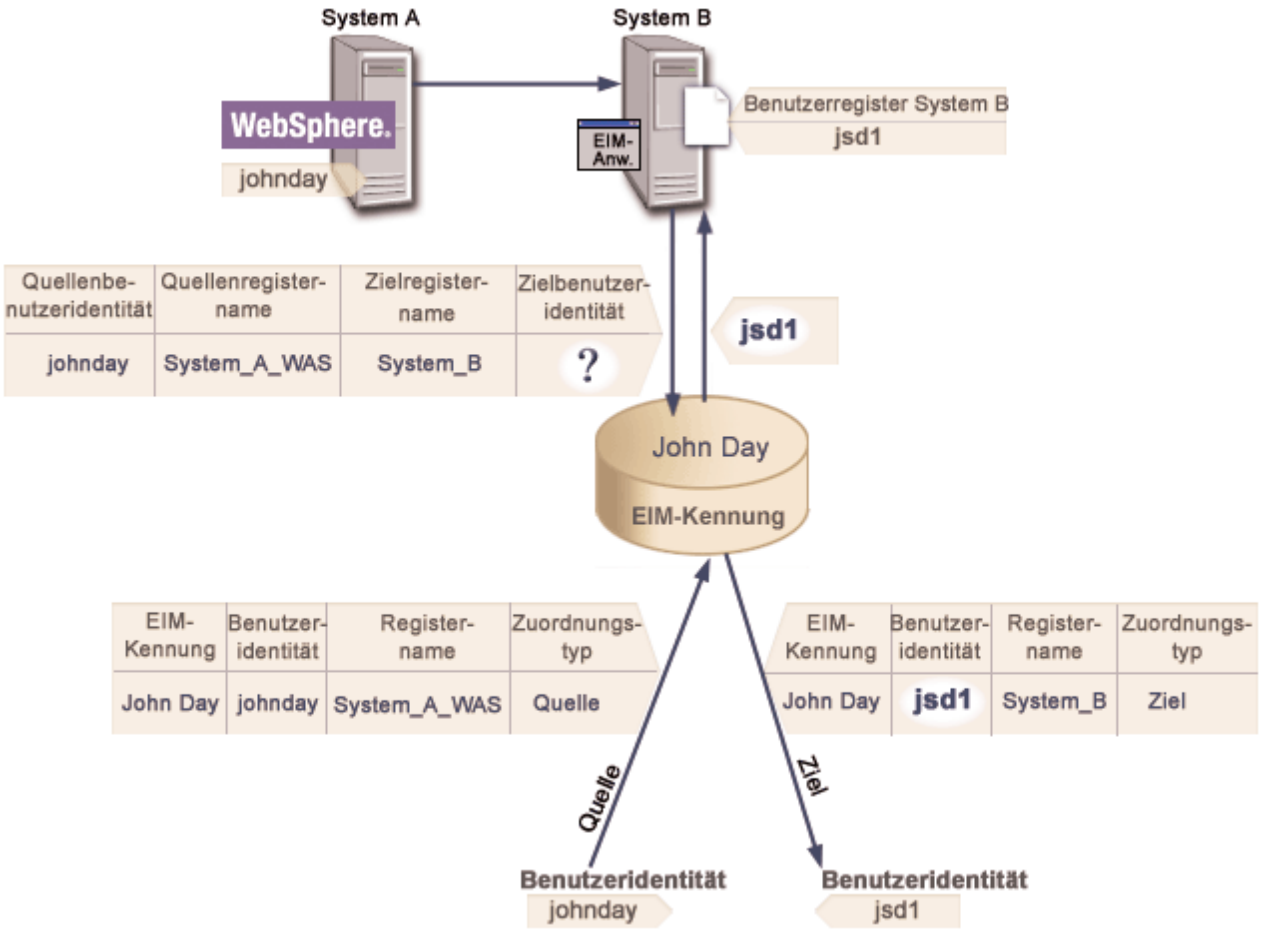
„Richtlinienzuordnungen" auf Seite 23
In diesem Abschnitt wird beschrieben, wie Richtlinienzuordnungen zur Beschreibung einer Beziehung zwischen mehreren Benutzeridentitäten und einer einzelnen Benutzeridentität in einem Benutzerregister verwendet werden.

Beispiele für Suchoperation: Beispiel 1

Im vorliegenden Beispiel erfahren Sie, wie der Suchablauf einer Suchoperation arbeitet, die eine Zielbenutzeridentität für spezielle Kennungszuordnungen auf der Basis der bekannten Benutzeridentität zurückgibt.

In Abbildung 11 wird die Benutzeridentität `johnday` mit Hilfe von LPTA (Lightweight Third-Party Authentication) auf System A beim WebSphere Application Server authentifiziert. Der WebSphere Application Server auf System A ruft ein integriertes Programm auf System B auf, um auf Daten von System B zuzugreifen. Das integrierte Programm verwendet eine EIM-API (EIM = Enterprise Identity Mapping), um eine EIM-Suchoperation auszuführen, für die die auf System A definierte Benutzeridentität als Quellenelement verwendet wird. Die Anwendung übergibt die folgenden Informationen, um die Operation auszuführen: `johnday` als Quellenbenutzeridentität, `System_A_WAS` als Name der EIM-Quellenregisterdefinition und `System_B` als Name der EIM-Zielregisterdefinition. Diese Quelleninformationen werden an EIM übergeben, und bei der EIM-Suchoperation wird eine Kennungsquellenzuordnung gesucht, die mit den Informationen übereinstimmt. Anhand des EIM-Kennungsnamens `John Day` wird bei der EIM-Suchoperation eine Zielzuordnung für diese Kennung gesucht, die mit dem Namen der EIM-Zielregisterdefinition für `System_B` übereinstimmt. Wird eine übereinstimmende Zielzuordnung gefunden, gibt die EIM-Suchoperation die Benutzeridentität `jsd1` an die Anwendung zurück.

Abbildung 11: EIM-Suchoperation gibt eine Zielbenutzeridentität von spezifischen Kennungszuordnungen basierend auf der bekannten Benutzeridentität `johnday` zurück



Beispiele für Suchoperation: Beispiel 2

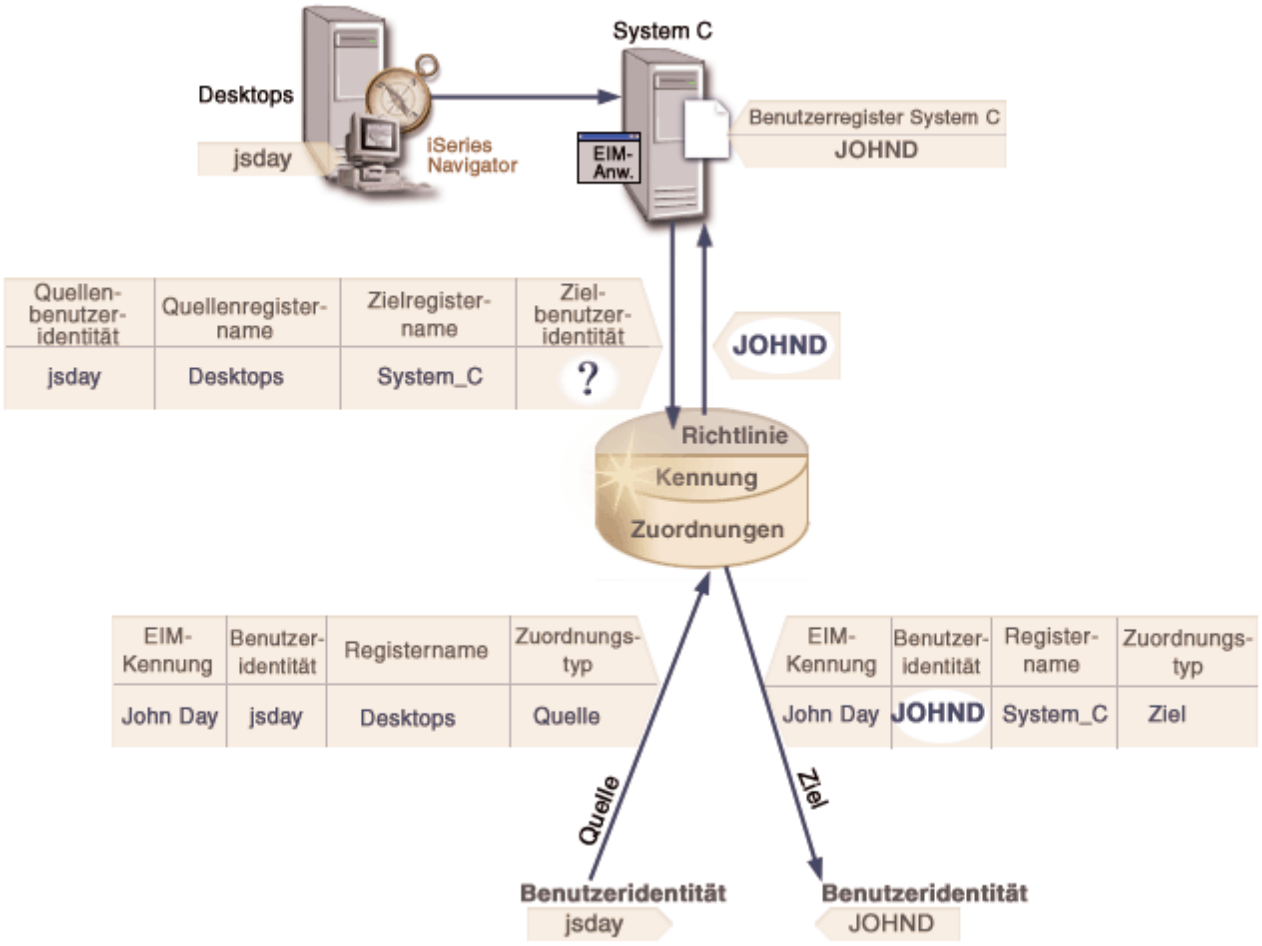
Im vorliegenden Beispiel erfahren Sie, wie der Suchablauf einer Suchoperation arbeitet, die eine Zielbenutzeridentität für spezielle Kennungszuordnungen auf der Basis des bekannten Kerberos-Principals zurückgibt.

In Abbildung 12 möchte ein Administrator einen Windows-Benutzer in einem Windows Active Directory-Register einem i5/OS-Benutzerprofil zuordnen. Als Authentifizierungsmethode wird unter Windows Kerberos verwendet. Als Name des Windows Active Directory-Registers wurde vom Administrator in EIM `Desktops` definiert. Die Benutzeridentität, die der Administrator als Basis für den Abgleich verwenden möchte, ist ein Kerberos-Principal mit dem Namen `jsday`. Als Name des i5/OS-Registers hat der Administrator in EIM `System_C` definiert. Bei der Benutzeridentität, mit der der Administrator den Abgleich durchführen möchte, handelt es sich um ein Benutzerprofil mit dem Namen `JOHND`.

Der Administrator erstellt eine EIM-Kennung mit dem Namen `John Day`. Anschließend fügt er zwei Zuordnungen zur EIM-Kennung hinzu:

- Eine Quellenzuordnung für den Kerberos-Principal mit dem Namen `jsday` im Register `Desktops`
- Eine Zielzuordnung für das i5/OS-Benutzerprofil mit dem Namen `JOHND` im Register `System_C`

Abbildung 12: EIM-Suchoperation gibt eine Zielbenutzeridentität von spezifischen Kennungszuordnungen auf der Basis des bekannten Kerberos-Principals `jsday` zurück



Diese Konfiguration ermöglicht einer Abgleichsuchoperation, einen Abgleich mit dem i5/OS-Benutzerprofil ausgehend vom Kerberos-Principal wie folgt durchzuführen:

Quellenbenutzer-identität und Quellenregister	--->	EIM-Kennung	--->	Zielbenutzeridentität
jsday im Register Desktops	--->	John Day	--->	JOHND (im Register System_C)

Die Suchoperation läuft auf folgende Weise ab:

1. Der Benutzer jsday meldet sich unter Windows mit Hilfe seines Kerberos-Principals im Windows Active Directory-Register Desktops an und authentifiziert sich.
2. Der Benutzer öffnet den iSeries Navigator, um auf Daten, die sich auf System_C befinden, zuzugreifen.
3. i5/OS verwendet eine EIM-API, um eine EIM-Suchoperation mit der Quellenbenutzeridentität jsday, dem Quellenregister Desktops und dem Zielregister System_C auszuführen.
4. Die EIM-Suchoperation überprüft, ob Abgleichsuchen für das Quellenregister Desktops und das Zielregister System_C aktiviert sind. Dies ist der Fall.
5. Die Suchoperation überprüft, ob eine bestimmte Kennungsquellenzuordnung vorhanden ist, die mit der angegebenen Benutzeridentität jsday im Quellenregister Desktops übereinstimmt.
6. Die Suchoperation verwendet die übereinstimmende Kennungsquellenzuordnung, um den entsprechenden Namen der EIM-Kennung, John Day, zu bestimmen.
7. Anhand dieses EIM-Kennungsnamens überprüft die Suchoperation, ob eine Kennungszielzuordnung für die EIM-Kennung, die mit dem Namen der angegebenen EIM-Zielregisterdefinition (System_C) übereinstimmt, vorhanden ist.
8. Eine solche Kennungszielzuordnung ist vorhanden, und die Suchoperation gibt die Zielbenutzeridentität JOHND laut Definition in der Zielzuordnung zurück.
9. Ist die Abgleichsuchoperation beendet, wird der iSeries Navigator unter dem Benutzerprofil JOHND ausgeführt. Die Benutzerberechtigung für den Zugriff auf Ressourcen und die Ausführung von Aktionen im iSeries Navigator wird von der für das Benutzerprofil JOHND und nicht von der für die Benutzeridentität jsday definierten Berechtigung bestimmt.

Beispiele für Suchoperation: Beispiel 3

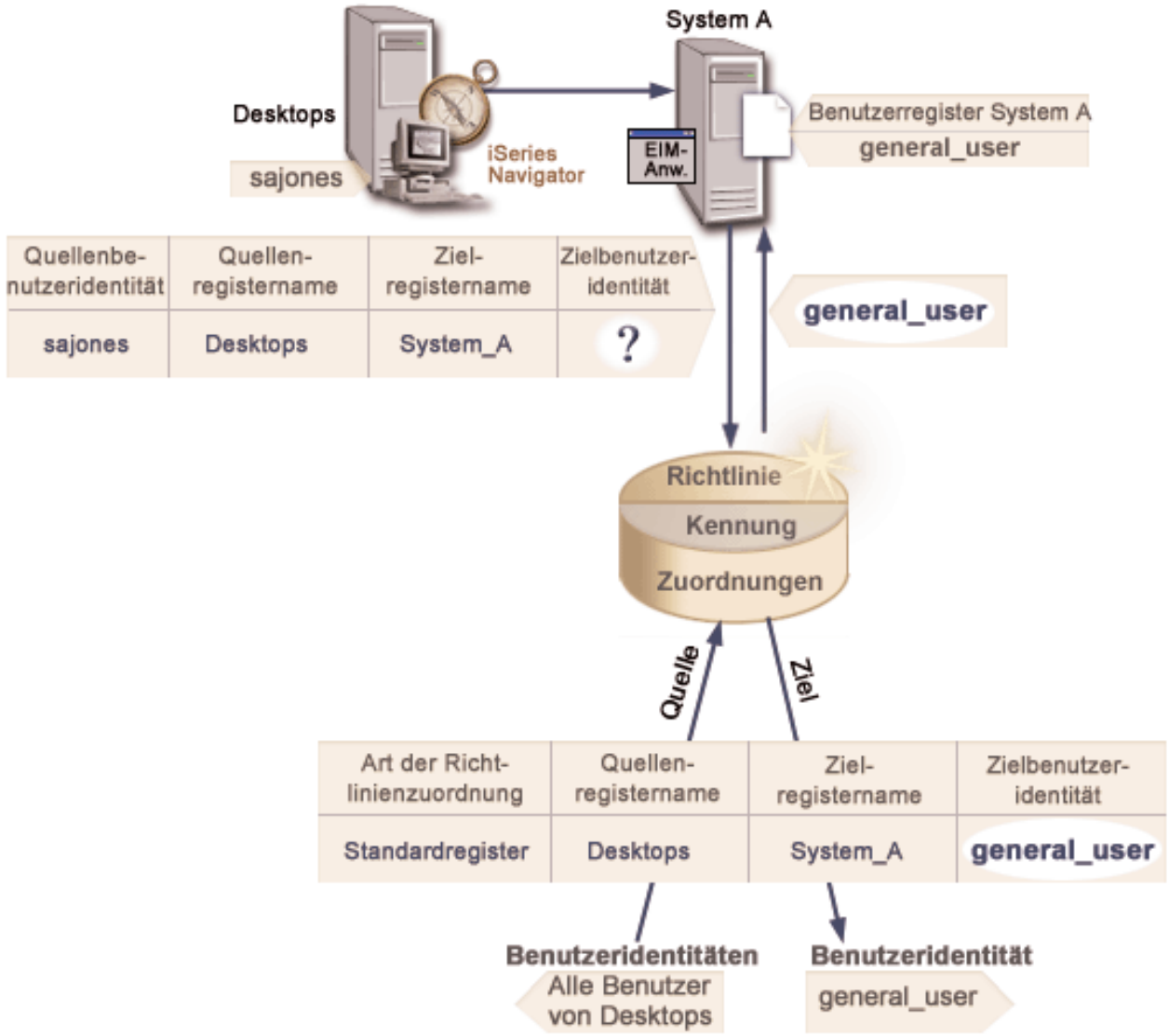
Im vorliegenden Beispiel erfahren Sie, wie der Suchablauf einer Suchoperation arbeitet, die eine Zielbenutzeridentität für eine Standardrichtlinienzuordnung für Register zurückgibt.

In Abbildung 13 möchte ein Administrator alle Desktop-Workstationbenutzer in einem Windows Active Directory-Register mit dem i5/OS-Benutzerprofil general_user im i5/OS-Register System_A in EIM (Enterprise Identity Mapping) abgleichen. Kerberos ist die Authentifizierungsmethode, die Windows verwendet. Der Name des Windows Active Directory-Registers laut Definition des Administrators in EIM ist Desktops. Eine der Benutzeridentitäten, die der Administrator als Basis für den Abgleich verwenden möchte, ist ein Kerberos-Principal mit dem Namen sajones.

Der Administrator verwendet die folgenden Angaben, um eine Standardrichtlinienzuordnung für Register zu erstellen:

- Quellenregister Desktops
- Zielregister System_A
- Zielbenutzeridentität general_user

Abbildung 13: Eine EIM-Suchoperation gibt eine Zielbenutzeridentität von einer Standardrichtlinienzuordnung für Register zurück



Diese Konfiguration ermöglicht einer Abgleichsuchoperation, alle Kerberos-Principals im Register `Desktops` einschließlich des Principals `sajones` mit dem i5/OS-Benutzerprofil `general_user` wie folgt abzugleichen:

Quellenbenutzer-identität und Quellenregister	**--->**	**Standardrichtlinien-zuordnung für Regis-ter**	**--->**	**Zielbenutzeridentität**
`sajones` im Register `Desktops`	--->	Standardrichtlinienzu-ordnung für Register	--->	`general_user` (im Register `System_A`)

Die Suchoperation läuft auf folgende Weise ab:

1. Die Benutzerin `sajones` meldet sich über ihren Kerberos-Principal im Register `Desktops` beim Windows-Desktop an und authentifiziert sich.
2. Sie öffnet den iSeries Navigator, um auf Daten zuzugreifen, die auf System A gespeichert sind.
3. i5/OS verwendet eine EIM-API, um eine EIM-Suchoperation mit der Quellenbenutzeridentität `sajones`, dem Quellenregister `Desktops` und dem Zielregister `System_A` auszuführen.

4. Die EIM-Suchoperation überprüft, ob Abgleichsuchen für das Quellenregister Desktops und das Zielregister System_A aktiviert sind. Dies ist der Fall.
5. Die Suchoperation überprüft, ob eine bestimmte Kennungsquellenzuordnung vorhanden ist, die mit der angegebenen Benutzeridentität sajones im Quellenregister Desktops übereinstimmt. Es wird keine übereinstimmende Kennungszuordnung gefunden.
6. Die Suchoperation überprüft, ob die Domäne für die Verwendung von Richtlinienzuordnungen aktiviert ist. Dies ist der Fall.
7. Die Suchoperation überprüft, ob das Zielregister (System_A) für die Verwendung von Richtlinienzuordnungen aktiviert ist. Dies ist der Fall.
8. Die Suchoperation überprüft, ob das Quellenregister (Desktops) ein X.509-Register ist. Dies ist nicht der Fall.
9. Die Suchoperation überprüft, ob eine Standardrichtlinienzuordnung für Register vorhanden ist, die mit dem Namen der Quellenregisterdefinition (Desktops) und dem Namen der Zielregisterdefinition (System_A) übereinstimmt.
10. Die Suchoperation stellt fest, dass eine Zuordnung vorhanden ist und gibt die Zielbenutzeridentität general_user zurück.

Manchmal gibt eine EIM-Suchoperation mehrdeutige Ergebnisse zurück. Das kann z. B. der Fall sein, wenn mehrere Zielbenutzeridentitäten mit den angegebenen Kriterien der Suchoperation übereinstimmen. Einige EIM-fähige Anwendungen einschließlich der i5/OS-Anwendungen und -Produkte sind nicht für die Verarbeitung dieser mehrdeutigen Ergebnisse konzipiert, so dass ihre Ausführung fehlschlagen oder unerwartete Ergebnisse zurückgegeben werden können. Möglicherweise müssen Sie eine Aktion ausführen, um dieses Problem zu beheben. Beispielsweise könnten Sie die EIM-Konfiguration ändern oder Suchinformationen für jede Zielbenutzeridentität definieren, um mehrere übereinstimmende Zielbenutzeridentitäten zu vermeiden. Außerdem können Sie einen Abgleich testen, um festzustellen, ob die Änderungen erwartungsgemäß funktionieren.

Beispiele für Suchoperationen: Beispiel 4

Im vorliegenden Beispiel erfahren Sie, wie der Suchablauf einer EIM-Suchoperation arbeitet, die eine Zielbenutzeridentität in einem Benutzerregister zurückgibt, das Mitglied einer Gruppenregisterdefinition ist.

Ein Administrator möchte eine Zuordnung zwischen einem Windows-Benutzer und einem i5/OS-Benutzerprofil herstellen. Als Authentifizierungsmethode wird unter Windows Kerberos verwendet und der Name des Kerberos-Registers, den der Administrator in EIM (EIM = Enterprise Identity Mapping) definiert hat, lautet Desktop_A. Die Benutzeridentität, die der Administrator als Zuordnungsquelle verwenden will, ist ein Kerberos-Principal mit dem Namen jday. Der Name der i5/OS-Registerdefinition, die der Administrator in EIM definiert hat, lautet Group_1 und die Benutzeridentität, zu der eine Zuordnung erstellt werden soll, ist das Benutzerprofil JOHND, das in drei unterschiedlichen Registern enthalten ist: System_B, System_C und System_D. Jedes dieser Register ist Mitglied in der Gruppenregisterdefinition Group_1.

Der Administrator erstellt eine EIM-Kennung mit dem Namen John Day. Anschließend fügt er zwei Zuordnungen zur EIM-Kennung hinzu:

- Eine Quellenzuordnung für den Kerberos-Principal mit dem Namen jday im Register Desktop_A
- Eine Zielzuordnung für das i5/OS-Benutzerprofil mit dem Namen JOHND im Register Group_1

Diese Konfiguration ermöglicht einer Abgleichsuchoperation, einen Abgleich mit dem i5/OS-Benutzerprofil ausgehend vom Kerberos-Principal wie folgt durchzuführen:

Quellenbenutzer-identität und Quellenregister	--->	EIM-Kennung	--->	Zielbenutzeridentität
jday im Register Desktop_A	--->	John Day	--->	JOHND (in der Gruppenregister-definition Group_1)

Die Suchoperation läuft auf folgende Weise ab:

1. Der Benutzer (jday) meldet sich an und authentifiziert sich unter Windows bei Desktop_A.
2. Der Benutzer öffnet den iSeries Navigator, um auf Daten, die sich auf System_B befinden, zuzugreifen.
3. i5/OS verwendet eine EIM-API, um eine EIM-Suchoperation mit der Quellenbenutzeridentität jday, dem Quellenregister Desktop_A und dem Zielregister System_B auszuführen.
4. Die EIM-Suchoperation überprüft, ob Abgleichsuchen für das Quellenregister (Desktop_A) und das Zielregister (System_B) aktiviert sind.
5. Die Suchoperation überprüft, ob eine bestimmte Quellenzuordnung vorhanden ist, die mit der angegebenen Quellenbenutzeridentität jday im Quellenregister Desktop_A übereinstimmt.
6. Die Suchoperation verwendet die übereinstimmende Quellenzuordnung, um den entsprechenden Namen der EIM-Kennung (John Day) zu bestimmen.
7. Anhand dieses EIM-Kennungsnamens überprüft die Suchoperation, ob eine einzelne Zielzuordnung für die EIM-Kennung vorhanden ist, die mit dem Namen der angegebenen EIM-Zielregisterdefinition (System_B) übereinstimmt. (Diese ist nicht vorhanden.)
8. Die Suchoperation überprüft, ob das Quellenregister (Desktop_A) Mitglied irgendeiner Gruppenregisterdefinition ist. (Dies ist nicht der Fall.)
9. Die Suchoperation überprüft, ob das Zielregister (System_B) Mitglied irgendeiner Gruppenregisterdefinition ist. Es ist Mitglied der Gruppenregisterdefinition Group_1.
10. Anhand dieses EIM-Kennungsnamens überprüft die Suchoperation, ob eine einzelne Zielzuordnung für die EIM-Kennung vorhanden ist, die mit dem Namen der angegebenen EIM-Zielregisterdefinition (Group_1) übereinstimmt.
11. Eine solche Zielzuordnung ist vorhanden, und die Suchoperation gibt die Zielbenutzeridentität JOHND zurück, die in der Zielzuordnung definiert ist.

Anmerkung: In bestimmten Fällen gibt die EIM-Suchoperation mehrdeutige Ergebnisse zurück. Dies kann geschehen, wenn mehrere Zielbenutzeridentitäten mit den angegebenen Kriterien der Suchoperation übereinstimmen. Da EIM keine einzelne Zielbenutzeridentität zurückgeben kann, schlägt die Ausführung von EIM-fähigen Anwendungen (einschließlich der i5/OS-Anwendungen und -Produkte), die die Verarbeitung dieser mehrdeutigen Ergebnisse nicht unterstützen, fehl oder es kommt zu unvorhergesehenen Ergebnissen. Möglicherweise müssen Sie geeignete Maßnahmen ergreifen, um dieses Problem zu beheben. Sie können z. B. die EIM-Konfiguration ändern oder für alle Zielbenutzeridentitäten Suchinformationen definieren, um die Ermittlung mehrerer übereinstimmender Zielbenutzeridentitäten zu verhindern. Sie können eine Zuordnung testen und auf diese Weise feststellen, ob die von Ihnen vorgenommenen Änderungen das gewünschte Ergebnis zeigen.

Beispiele für Suchoperation: Beispiel 5

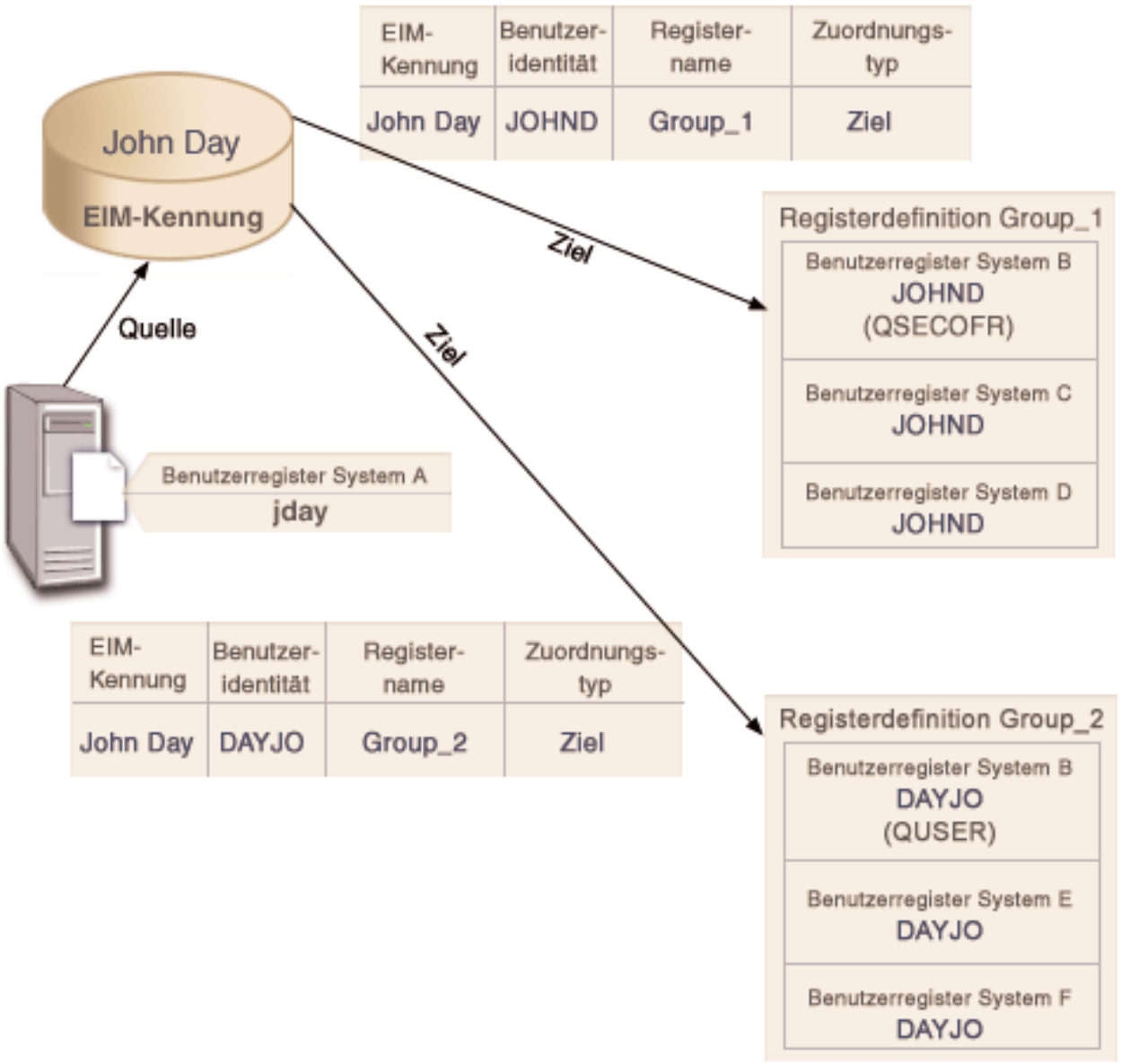
Im folgenden Beispiel werden Suchoperationen erläutert, die mehrdeutige Ergebnisse zurückgeben, in denen Gruppenregisterdefinitionen enthalten sind.

In bestimmten Fällen liefert eine Abgleichsuchoperation mehrdeutige Ergebnisse, wenn mehr als eine Zielbenutzeridentität mit den angegebenen Suchkriterien übereinstimmt. Da mehrdeutige Ergebnisse dazu

führen können, dass die Ausführung von Anwendungen, die EIM benutzen, fehlschlägt oder dass in diesen unerwartete Ergebnisse auftreten, müssen Sie entsprechende Maßnahmen einleiten, um derartige Situationen zu verhindern oder zu beseitigen.

Beachten Sie hierbei insbesondere, dass Suchoperationen mehrdeutige Ergebnisse zurückgeben können, wenn Sie eine einzelne Benutzerregisterdefinition als Mitglied mehrerer Gruppenregisterdefinitionen angeben. Wenn eine einzelne Benutzerregisterdefini- tion als Mitglied mehrerer Gruppenregisterdefinitionen angegeben wurde und Sie individuelle EIM-Kennungszuordnungen oder -richtlinienzuordnungen erstellen, die entweder als Quellen- oder als Zielregister eine Gruppenregisterdefinition verwenden, dann kann es bei der Ausführung von Suchoperationen zu mehrdeutigen Ergebnissen kommen. Sie können z. B. zwei verschiedene Benutzeridentitäten für zwei unterschiedliche Typen von Systemtasks verwenden, die Sie ausführen: Sie führen Tasks als Sicherheitsadministrator aus, für die eine Benutzeridentität mit der Berechtigung QSECOFR erforderlich ist. Außerdem führen Sie typische Benutzertasks aus, für die eine Benutzeridentität mit der Berechtigung QUSER benötigt wird. Wenn Ihre beiden Benutzeridentitäten sich in dem Benutzerregister befinden, das Mitglied zweier unterschiedlicher Gruppenregisterdefinitionen ist, und wenn Sie Zielkennungszuordnungen zu beiden Zielbenutzeridentitäten erstellen, dann ermitteln Suchoperationen beide Zielbenutzeridentitäten und geben deshalb mehrdeutige Ergebnisse aus.

Im folgenden Beispiel wird erläutert, warum dieses Problem auftreten kann, wenn Sie ein bestimmtes Benutzerregister als Mitglied von zwei Gruppenregisterdefinitionen angeben und dabei eine der Gruppenregisterdefinitionen als Zielregister in zwei unterschiedlichen EIM-Kennungszuordnungen angeben.



Beispiel:

John Day verfügt über die folgenden Benutzeridentitäten, die in einer Systemregisterdefinition enthalten sind, die als Benutzerregister für `System B` bezeichnet wird:

- JOHND
- DAYJO

Das Benutzerregister für `System B` ist Mitglied der folgenden Gruppenregisterdefinitionen:

- `Group 1`
- `Group 2`

Die EIM-Kennung John Day verfügt über zwei Zielzuordnungen mit den folgenden Angaben:

- Zielzuordnung: Das Zielregister lautet `Group 1`. Dieses Register enthält die Benutzeridentität `JOHND` im Benutzerregister für `System B`.

| • Zielzuordnung: Das Zielregister lautet Group 2. Dieses Register enthält die Benutzeridentität DAYJO im
| Benutzerregister für System B.

| In dieser Situation gibt die Abgleichsuchoperation mehrdeutige Ergebnisse zurück, weil mehr als eine
| Zielbenutzeridentität mit den angegebenen Suchkriterien übereinstimmt. Beide Benutzeridentitäten (JOHND
| und DAYOJO) stimmen mit den angegebenen Suchkriterien überein.

| Mehrdeutige Ergebnisse bei Abgleichsuchoperationen können auch auftreten, wenn Sie zwei Richtlinien-
| zuordnungen (an Stelle von einzelnen EIM-Kennungszuordnungen) erstellen, die als Zielregister
| Gruppenregisterdefinitionen verwenden.

| Um zu vermeiden, dass Suchoperationen mehrdeutige Ergebnisse zurückgeben, in denen Gruppen-
| registerdefinitionen enthalten sind, sollten Sie die folgenden Richtlinien berücksichtigen:
| • Geben Sie ein einzelnes Benutzerregister immer nur als Mitglieder einer einzigen Gruppenregister-
| definition an.
| • Überprüfen Sie die Situation sorgfältig, bevor Sie einzelne EIM-Kennungszuordnungen oder
| -Richtlinienzuordnungen erstellen, in denen als Quellen- oder Zielregister Gruppenregisterdefinitionen
| eingesetzt werden. Vergewissern Sie sich hierbei, dass die Gruppenregisterdefinition nur in einer
| Gruppenregisterdefinition als Mitglied definiert ist. Beachten Sie unbedingt, dass ein Mitglied der
| Zielgruppenregisterdefinition, das auch als Mitglied einer anderen Gruppenregisterdefinition definiert
| ist, dazu führen kann, dass bei Suchoperationen mehrdeutige Ergebnisse zurückgegeben werden.
| • Wenn es zur Ausgabe mehrdeutiger Ergebnisse gekommen ist, weil Sie eine einzelne Registerdefinition
| als Mitglied mehrerer Gruppenregisterdefinitionen angegeben haben, und wenn Sie eine einzelne
| Kennungszuordnung oder Richtlinienzuordnung erstellen, die eine dieser Gruppenregisterdefinitionen
| als Quellen- oder Zielregister verwendet, können Sie eindeutige Suchinformationen für alle Ziel-
| benutzeridentitäten in allen Zuordnungen definieren, um die Suche weiter einzugrenzen.

| Sie können im Beispiel mit John Day die folgenden Suchinformationen für alle Zielbenutzeridentitäten
| definieren:
| • Für JOHND: Definieren Sie als Suchinformationen Administrator.
| • Für DAYJO: Definieren Sie als Suchinformationen User.

| Die i5/OS-Basisanwendungen wie z. B. iSeries Access für Windows sind nicht in der Lage, anhand von
| Suchinformationen mehrere von einer Suchoperation zurückgegebene Zielbenutzeridentitäten zu unter-
| scheiden. Daher sollten Sie überprüfen, ob es sinnvoll ist, die für die Domäne vorhandenen Zuordnungen
| erneut zu definieren. Auf diese Weise kann sichergestellt werden, dass eine Abgleichsuchoperation eine
| einzige Zielbenutzeridentität zurückgeben kann. So kann gewährleistet werden, dass die i5/OS-Basisan-
| wendungen Suchoperationen ausführen und Identitäten abgleichen können.

Unterstützung und Aktivierung von EIM-Abgleichrichtlinien

In diesem Abschnitt wird erläutert, wie Richtlinienzuordnungen für Domänen aktiviert und inaktiviert werden können.

Die Unterstützung von EIM-Abgleichrichtlinien ermöglicht es Ihnen, in einer EIM-Domäne sowohl Richtlinienzuordnungen als auch spezielle Kennungszuordnungen zu verwenden. Sie können Richtlinienzuordnungen an Stelle von oder in Verbindung mit Kennungszuordnungen verwenden.

Mit der Unterstützung von EIM-Abgleichrichtlinien kann die Verwendung von Richtlinienzuordnungen für die gesamte Domäne bzw. für jedes spezifische Zielbenutzerregister aktiviert oder inaktiviert werden. Außerdem können Sie mit EIM festlegen, ob für ein Register überhaupt Abgleichsuchoperationen ausgeführt werden sollen. Daher können Sie die Unterstützung von Abgleichrichtlinien verwenden, um die Rückgabe der Ergebnisse von Abgleichsuchoperationen genauer zu steuern.

Die Standardeinstellung für eine EIM-Domäne legt fest, dass Abgleichsuchen, die Richtlinienzuordnungen verwenden, für die Domäne inaktiviert sind. Ist die Verwendung von Richtlinienzuordnungen für Domänen inaktiviert, geben alle Abgleichsuchoperationen für die Domäne nur dann Ergebnisse zurück, wenn spezielle Kennungszuordnungen zwischen Benutzeridentitäten und EIM-Kennungen verwendet werden.

Die Standardeinstellungen für die einzelnen Register sehen vor, dass die Nutzung der Abgleichsuche aktiviert und die Verwendung von Richtlinienzuordnungen inaktiviert ist. Wenn Sie die Verwendung von Richtlinienzuordnungen für ein einzelnes Zielregister aktivieren, müssen Sie sicherstellen, dass diese Einstellung auch für die Domäne aktiviert ist.

Es gibt drei Möglichkeiten, die Nutzung der Abgleichsuche und die Verwendung von Richtlinienzuordnungen für die einzelnen Register zu konfigurieren:

- Für das angegebene Register können keine Abgleichsuchoperationen verwendet werden. Mit anderen Worten, eine Anwendung, die eine Abgleichsuchoperation unter Einbeziehung dieses Registers ausführt, wird keine Ergebnisse zurückgeben.
- Abgleichsuchoperationen können nur die spezifischen Kennungszuordnungen zwischen Benutzeridentitäten und EIM-Kennungen verwenden. Abgleichsuchen werden für das Register aktiviert, Richtlinienzuordnungen werden für das Register jedoch inaktiviert.
- Abgleichsuchoperationen können spezifische Kennungszuordnungen verwenden, falls diese vorhanden sind, und können Richtlinienzuordnungen verwenden, wenn keine spezifischen Kennungszuordnungen vorhanden sind.

Zugehörige Tasks

„Richtlinienzuordnungen für eine Domäne aktivieren" auf Seite 97

„Unterstützung von Abgleichsuchen und Richtlinienzuordnungen für Zielregister aktivieren" auf Seite 105

EIM-Zugriffssteuerung

Im Folgenden wird erläutert, wie einem Benutzer der Zugriff auf eine LDAP-Benutzergruppe gewährt werden kann, um eine Domäne zu steuern.

Als EIM-Benutzer (EIM = Enterprise Identity Mapping) wird ein Benutzer bezeichnet, der auf der Basis seiner Zugehörigkeit zu einer vordefinierten LDAP-Benutzergruppe (Lightweight Directory Access Protocol) über die EIM-Zugriffssteuerung für eine bestimmte Domäne verfügt. Die Angabe der EIM-*Zugriffssteuerung* für einen Benutzer bewirkt, dass der Benutzer zu einer bestimmten LDAP-Benutzergruppe für eine bestimmte Domäne hinzugefügt wird. Jede LDAP-Gruppe hat die Berechtigung, bestimmte EIM-Verwaltungstasks für diese Domäne auszuführen. Welche Verwaltungstasks ein EIM-Benutzer ausführen kann, wird durch die Zugriffssteuerungsgruppe festgelegt, zu der der EIM-Benutzer gehört.

Anmerkung: Zum Konfigurieren von EIM müssen Sie nachweisen, dass Sie im Netzwerkkontext als vertrauenswürdig gelten. Die Anerkennung durch ein bestimmtes System reicht nicht aus. Die Berechtigung zur Konfiguration von EIM basiert nicht auf der Berechtigung des i5/OS-Benutzerprofils, sondern auf der Berechtigung für die EIM-Zugriffssteuerung. EIM ist eine Netzwerkressource und keine Ressource für ein bestimmtes System. Daher erkennt EIM i5/OS-spezifische Sonderberechtigungen wie z. B. *ALLOBJ und *SECADM für die Konfiguration nicht. Nachdem EIM konfiguriert ist, kann die Berechtigung zur Ausführung von Tasks jedoch auf einer Reihe verschiedener Typen von Benutzern einschließlich der i5/OS-Benutzerprofile basieren. IBM Directory Server for iSeries (LDAP) behandelt i5/OS-Profile mit den Sonderberechtigungen *ALLOBJ und *IOSYSCFG z. B. als Verzeichnisadministratoren.

Nur Benutzer mit EIM-Administratorberechtigung können andere Benutzer zu einer EIM-Zugriffssteuerungsgruppe hinzufügen oder die Zugriffssteuerungseinstellungen anderer Benutzer ändern. Bevor ein Benutzer Mitglied einer EIM-Zugriffssteuerungsgruppe werden kann, muss für ihn ein Eintrag im Directory-Server, der als EIM-Domänencontroller fungiert, angelegt werden. Außerdem ist zu beachten,

dass nur bestimmte Benutzertypen Mitglieder einer EIM-Zugriffssteuerungsgruppe sein können. Die Benutzeridentität kann in Form eines Kerberos-Principals, eines registrierten LDAP-Namens oder eines i5/OS-Benutzerprofils angegeben werden. Dies gilt allerdings nur, wenn die Benutzeridentität für den Directory-Server definiert ist.

Anmerkung: Der Netzwerkauthentifizierungsservice muss auf dem System konfiguriert sein, damit der Benutzertyp "Kerberos-Principal" in EIM verfügbar ist. Damit ein i5/OS-Benutzerprofil in EIM verfügbar ist, müssen Sie ein Systemobjektsuffix auf dem Directory-Server konfigurieren. Mit Hilfe dieses Suffix kann der Directory-Server auf i5/OS-Systemobjekte wie beispielsweise i5/OS-Benutzerprofile verweisen.

Im Folgenden werden die Funktionen, die die einzelnen EIM-Berechtigungsgruppen ausführen können, kurz beschrieben:

LDAP-Administrator

Der LDAP-Administrator (LDAP = Lightweight Directory Access Protocol) ist ein spezieller registrierter Name (Distinguished Name, DN) im Verzeichnis und fungiert als Administrator für das gesamte Verzeichnis. Daher hat der LDAP-Administrator Zugriff auf alle EIM-Verwaltungsfunktionen sowie das gesamte Verzeichnis. Ein Benutzer mit dieser Zugriffssteuerung kann die folgenden Funktionen ausführen:

- Domäne erstellen
- Domäne löschen
- EIM-Kennungen erstellen und entfernen
- EIM-Registerdefinitionen erstellen und entfernen
- Quellen-, Ziel- und administrative Zuordnungen erstellen und entfernen
- Richtlinienzuordnungen erstellen und entfernen
- Zertifikatfilter erstellen und entfernen
- Verwendung von Richtlinienzuordnungen für eine Domäne aktivieren und inaktivieren
- Abgleichsuchen für ein Register aktivieren und inaktivieren
- Verwendung von Richtlinienzuordnungen für ein Register aktivieren und inaktivieren
- EIM-Suchoperationen ausführen
- Kennungszuordnungen, Richtlinienzuordnungen, Zertifikatfilter, EIM-Kennungen und EIM-Registerdefinitionen abrufen
- EIM-Zugriffssteuerungsdaten hinzufügen, entfernen und auflisten
- Berechtigungsinformationen für einen Registerbenutzer ändern und entfernen

EIM-Administrator

Die Zugehörigkeit zu dieser Zugriffssteuerungsgruppe erlaubt dem Benutzer, alle EIM-Daten innerhalb dieser EIM-Domäne zu verwalten. Ein Benutzer mit dieser Zugriffssteuerung kann die folgenden Funktionen ausführen:

- Domäne löschen
- EIM-Kennungen erstellen und entfernen
- EIM-Registerdefinitionen erstellen und entfernen
- Quellen-, Ziel- und administrative Zuordnungen erstellen und entfernen
- Richtlinienzuordnungen erstellen und entfernen
- Zertifikatfilter erstellen und entfernen
- Verwendung von Richtlinienzuordnungen für eine Domäne aktivieren und inaktivieren
- Abgleichsuchen für ein Register aktivieren und inaktivieren
- Verwendung von Richtlinienzuordnungen für ein Register aktivieren und inaktivieren

- EIM-Suchoperationen ausführen
- Kennungszuordnungen, Richtlinienzuordnungen, Zertifikatfilter, EIM-Kennungen und EIM-Registerdefinitionen abrufen
- EIM-Zugriffssteuerungsdaten hinzufügen, entfernen und auflisten
- Berechtigungsinformationen für einen Registerbenutzer ändern und entfernen

Kennungsadministrator

Die Zugehörigkeit zu dieser Zugriffssteuerungsgruppe erlaubt dem Benutzer, EIM-Kennungen hinzuzufügen und zu ändern sowie Quellen- und administrative Zuordnungen zu verwalten. Ein Benutzer mit dieser Zugriffssteuerung kann die folgenden Funktionen ausführen:

- EIM-Kennungen erstellen
- Quellenzuordnungen hinzufügen und entfernen
- Administrative Zuordnungen hinzufügen und entfernen
- EIM-Suchoperationen ausführen
- Kennungszuordnungen, Richtlinienzuordnungen, Zertifikatfilter, EIM-Kennungen und EIM-Registerdefinitionen abrufen

EIM-Abgleichsoperationen

Die Zugehörigkeit zu dieser Zugriffssteuerungsgruppe erlaubt dem Benutzer, EIM-Abgleichsuchoperationen auszuführen. Ein Benutzer mit dieser Zugriffssteuerung kann die folgenden Funktionen ausführen:

- EIM-Suchoperationen ausführen
- Kennungszuordnungen, Richtlinienzuordnungen, Zertifikatfilter, EIM-Kennungen und EIM-Registerdefinitionen abrufen

Registeradministrator

Die Zugehörigkeit zu dieser Zugriffssteuerungsgruppe erlaubt dem Benutzer, alle EIM-Registerdefinitionen zu verwalten. Ein Benutzer mit dieser Zugriffssteuerung kann die folgenden Funktionen ausführen:

- Zielzuordnungen hinzufügen und entfernen
- Richtlinienzuordnungen erstellen und entfernen
- Zertifikatfilter erstellen und entfernen
- Abgleichsuchen für ein Register aktivieren und inaktivieren
- Verwendung von Richtlinienzuordnungen für ein Register aktivieren und inaktivieren
- EIM-Suchoperationen ausführen
- Kennungszuordnungen, Richtlinienzuordnungen, Zertifikatfilter, EIM-Kennungen und EIM-Registerdefinitionen abrufen

Administrator für ausgewählte Register

Die Zugehörigkeit zu dieser Zugriffssteuerungsgruppe erlaubt dem Benutzer, EIM-Informationen nur für eine angegebene Benutzerregisterdefinition (z. B. `Registry_X`) zu verwalten. Außerdem kann der Benutzer Zielzuordnungen nur für eine angegebene Benutzerregisterdefinition hinzufügen und entfernen. Ein Benutzer mit dieser Berechtigung sollte auch die Berechtigung für **EIM-Abgleichoperationen** besitzen, um Abgleichsuchoperationen und Richtlinienzuordnungen in vollem Umfang nutzen zu können. Mit dieser Berechtigung kann der Benutzer die folgenden Funktionen für bestimmte berechtigte Registerdefinitionen ausführen:

- Zielzuordnungen nur für die angegebenen EIM-Registerdefinitionen erstellen, entfernen und auflisten
- Standardrichtlinienzuordnungen für Domäne hinzufügen und entfernen
- Richtlinienzuordnungen nur für die angegebenen Registerdefinitionen hinzufügen und entfernen

- Zertifikatfilter nur für die angegebenen Registerdefinitionen hinzufügen
- Abgleichsuchen nur für die angegebenen Registerdefinitionen aktivieren und inaktivieren
- Verwendung von Richtlinienzuordnungen nur für die angegebenen Registerdefinitionen aktivieren und inaktivieren
- EIM-Kennungen abrufen
- Kennungszuordnungen und Zertifikatfilter nur für die angegebenen Registerdefinitionen abrufen
- Informationen zur EIM-Registerdefinition nur für die angegebenen Registerdefinitionen abrufen

Anmerkung: Wenn es sich bei der angegebenen Registerdefinition um eine Gruppenregisterdefinition handelt, hat ein Benutzer mit Administratorberechtigung für ausgewählte Register Administratorzugriff lediglich auf die Gruppe, nicht jedoch auf die einzelnen Gruppenmitglieder.

Ein Benutzer, der sowohl die Berechtigung **Administrator für ausgewählte Register** als auch die Berechtigung **EIM-Abgleichsuchoperationen** besitzt, kann die folgenden Funktionen ausführen:

- Richtlinienzuordnungen nur für die angegebenen Register hinzufügen und entfernen
- EIM-Suchoperationen ausführen
- Alle Kennungszuordnungen, Richtlinienzuordnungen, Zertifikatfilter, EIM-Kennungen und EIM-Registerdefinitionen abrufen.

Suchfunktion für Berechtigungsnachweis

Diese Zugriffssteuerungsgruppe ermöglicht dem Benutzer das Abrufen von Berechtigungsinformationen, z. B. von Kennwörtern.

Wenn ein Benutzer mit dieser Zugriffssteuerung eine zusätzliche EIM-Operation ausführen will, muss er Mitglied der Zugriffssteuerungsgruppe sein, die die Berechtigung zur Ausführung der gewünschten EIM-Operation bereitstellt. Wenn ein Benutzer mit dieser Zugriffssteuerung z. B. die Zielzuordnung einer bestimmten Quellenzuordnung abrufen will, muss er Mitglied einer der folgenden Zugriffssteuerungsgruppen sein:

- EIM-Administrator
- Kennungsadministrator
- EIM-Abgleichsuchoperationen
- Registeradministrator

EIM-Zugriffssteuerungsgruppe: Berechtigung für APIs

In den folgenden Tabellen finden Sie Informationen, die nach den EIM-Operationen (EIM = Enterprise Identity Mapping) gegliedert sind, die von der API ausgeführt werden.

Jede der folgenden Tabellen enthält die einzelnen EIM-APIs, die verschiedenen EIM-Zugriffssteuerungsgruppen sowie Angaben darüber, ob die Zugriffssteuerungsgruppe über die Berechtigung zur Ausführung einer bestimmten EIM-Funktion verfügt.

Tabelle 1. Mit Domänen arbeiten

EIM-API	LDAP-Administrator	EIM-Administrator	Kennungsadministrator	EIM-Abgleichsuche	Registeradministrator	Administrator für ausgewähltes Register
eimChangeDomain	X	X	-	-	-	-
eimCreateDomain	X	-	-	-	-	-
eimDeleteDomain	X	X	-	-	-	-
eimListDomains	X	X	-	-	-	-

Tabelle 2. Mit Kennungen arbeiten

EIM-API	LDAP-Administrator	EIM-Administrator	EIM-Kennungsadministrator	EIM-Abgleichsuche	EIM-Registeradministrator	Administrator für EIM-Register X
eimAddIdentifier	X	X	X	-	-	-
eimChangeIdentifier	X	X	X	-	-	-
eimListIdentifiers	X	X	X	X	X	X
eimRemoveIdentifier	X	X	-	-	-	-
eimGetAssociated Identifiers	X	X	X	X	X	X

Tabelle 3. Mit Registern arbeiten

EIM-API	LDAP-Administrator	EIM-Administrator	EIM-Kennungsadministrator	EIM-Abgleichsuche	EIM-Registeradministrator	Administrator für EIM-Register X
eimAddApplication Registry	X	X	-	-	-	-
eimAddSystemRegistry	X	X	-	-	-	-
eimChangeRegistry	X	X	-	-	X	X
eimChange RegistryUser	X	X	-	-	X	X
eimChangeRegistryAlias	X	X	-	-	X	X
eimGetRegistry NameFromAlias	X	X	X	X	X	X
eimListRegistries	X	X	X	X	X	X
eimListRegistry Associations	X	X	X	X	X	X
eimListRegistryAliases	X	X	X	X	X	X
eimListRegistry Users	X	X	X	X	X	X
eimRemoveRegistry	X	X	-	-	-	-

Tabelle 4. Mit Kennungszuordnungen arbeiten. Für die APIs `eimAddAssociation()` und `eimRemoveAssociation()` legen vier Parameter den Typ der Zuordnung fest, die hinzugefügt bzw. entfernt werden soll. Die Berechtigungen für diese APIs variieren basierend auf dem in den Parametern angegebenen Zuordnungstyp. In der folgenden Tabelle wird daher für jede API der Zuordnungstyp angegeben.

EIM-API	LDAP-Administrator	EIM-Administrator	EIM-Kennungsadministrator	EIM-Abgleichsuche	EIM-Registeradministrator	Administrator für EIM-Register X
eimAddAssociation (administrativ)	X	X	X	-	-	-
eimAddAssociation (Quelle)	X	X	X	-	-	-
eimAddAssociation (Quelle und Ziel)	X	X	X	-	X	X
eimAddAssociation (Ziel)	X	X	-	-	X	X
eimListAssociations	X	X	X	X	X	X
eimRemoveAssociation (administrativ)	X	X	X	-	-	-
eimRemoveAssociation (Quelle)	X	X	X	-	-	-
eimRemoveAssociation (Quelle und Ziel)	X	X	X	-	X	X

Tabelle 4. Mit Kennungszuordnungen arbeiten (Forts.). Für die APIs `eimAddAssociation()` und `eimRemoveAssociation()` legen vier Parameter den Typ der Zuordnung fest, die hinzugefügt bzw. entfernt werden soll. Die Berechtigungen für diese APIs variieren basierend auf dem in den Parametern angegebenen Zuordnungstyp. In der folgenden Tabelle wird daher für jede API der Zuordnungstyp angegeben.

EIM-API	LDAP-Administrator	EIM-Administrator	EIM-Kennungsadministrator	EIM-Abgleichsuche	EIM-Registeradministrator	Administrator für EIM-Register X
eimRemoveAssociation (Ziel)	X	X	-	-	X	X

Tabelle 5. Mit Richtlinienzuordnungen arbeiten

EIM-API	LDAP-Administrator	EIM-Administrator	EIM-Kennungsadministrator	EIM-Abgleichsuche	EIM-Registeradministrator	Administrator für EIM-Register X
eimAddPolicyAssociation	X	X	-	-	X	X
eimAddPolicyFilter	X	X	-	-	X	X
eimListPolicyFilters	X	X	X	X	X	X
eimRemove PolicyAssociation	X	X			X	X
eimRemovePolicyFilter	-	-	-	-	-	

Tabelle 6. Mit Abgleichen arbeiten

EIM-API	LDAP-Administrator	EIM-Administrator	EIM-Kennungsadministrator	EIM-Abgleichsuche	EIM-Registeradministrator	Administrator für EIM-Register X
eimGetAssociatedIdentifier	X	X	X	X	X	X
eimGetTargetFromIdentifier	X	X	X	X	X	X
eimGetTargetFromSource	X	X	X	X	X	X

Tabelle 7. Mit Zugriff arbeiten

EIM-API	LDAP-Administrator	EIM-Administrator	EIM-Kennungsadministrator	EIM-Abgleichsuche	EIM-Registeradministrator	Administrator für EIM-Register X
eimAddAccess	X	X	-	-	-	-
eimListAccess	X	X	-	-	-	-
eimListUserAccess	X	X	-	-	-	-
eimQueryAccess	X	X	-	-	-	-
eimRemoveAccess	X	X	-	-	-	-

EIM-Zugriffssteuerungsgruppe: Berechtigung für EIM-Tasks

Im Folgenden finden Sie eine Tabelle, in der die Beziehungen zwischen den verschiedenen EIM-Zugriffssteuerungsgruppen (EIM = Enterprise Identity Mapping) und den EIM-Tasks aufgelistet sind, die diese ausführen können.

Der LDAP-Administrator ist zwar nicht in der Tabelle aufgelistet, diese Stufe der Zugriffssteuerung ist jedoch für die Erstellung einer neuen EIM-Domäne erforderlich. Außerdem besitzt der LDAP-Administrator dieselbe Berechtigung wie der EIM-Administrator, der EIM-Administrator hat jedoch nicht automatisch die Berechtigung des LDAP-Administrators.

Tabelle 8. Tabelle 1: EIM-Zugriffssteuerungsgruppen

EIM-Task	EIM-Administrator	Kennungsadministrator	EIM-Abgleichsuchoperationen	Registeradministrator	Administrator für ausgewähltes Register	Suchfunktion für Berechtigungsnachweis
Domäne erstellen	-	-	-	-	-	
Domäne löschen	X	-	-	-	-	
Domäne ändern	X	-	-	-	-	
Richtlinienzuordnungen für Domäne aktivieren /inaktivieren	X	-	-	-	-	
Domänen suchen	X	-	-	-	-	
Systemregister hinzufügen	X	-	-	-	-	
Anwendungsregister hinzufügen	X	-	-	-	-	
Register entfernen	X	-	-	-	-	
Register ändern	X	-	-	X	X	
Abgleichsuchen für Register aktivieren /inaktivieren	X	-	-	X	X	
Richtlinienzuordnungen für Register aktivieren /inaktivieren	X	-	-	X	X	
Register suchen	X	X	X	X	X	
Kennung hinzufügen	X	X	-	-	-	
Kennung entfernen	X	-	-	-	-	
Kennung ändern	X	X	-	-	-	
Kennungen suchen	X	X	X	X	X	

Tabelle 8. Tabelle 1: EIM-Zugriffssteuerungsgruppen (Forts.)

EIM-Task	EIM-Administrator	Kennungsadministrator	EIM-Abgleichsuchoperationen	Registeradministrator	Administrator für ausgewähltes Register	Suchfunktion für Berechtigungsnachweis
Zugeordnete Kennungen abrufen	X	X	X	X	X	
Administrative Zuordnung hinzufügen /entfernen	X	X	-	-	-	
Quellenzuordnung hinzufügen /entfernen	X	X	-	-	-	
Zielzuordnung hinzufügen /entfernen	X	-	-	X	X	
Richtlinienzuordnung hinzufügen /entfernen	X	-	-	X	X	
Zertifikatfilter hinzufügen /entfernen	X	-	-	X	X	
Zertifikatfilter suchen	X	X	X	X	X	
Zuordnungen suchen	X	X	X	X	X	
Richtlinienzuordnungen suchen	X	X	X	X	X	
Zielzuordnung aus Quellenzuordnung abrufen	X	X	X	X	-	
Zielzuordnung aus Kennung abrufen	X	X	X	X	X	
Registerbenutzer ändern	X	-	-	X	X	
Registerbenutzer suchen	X	X	X	X	X	
Aliasnamen des Registers ändern	X	-	-	X	X	

Tabelle 8. Tabelle 1: EIM-Zugriffssteuerungsgruppen (Forts.)

EIM-Task	EIM-Administrator	Kennungsadministrator	EIM-Abgleichsuchoperationen	Registeradministrator	Administrator für ausgewähltes Register	Suchfunktion für Berechtigungsnachweis
Aliasnamen des Registers suchen	X	X	X	X	X	
Register aus Aliasnamen abrufen	X	X	X	X	X	
EIM-Zugriffssteuerung hinzufügen /entfernen	X	-	-	-	-	
Mitglieder der Zugriffssteuerungsgruppe anzeigen	X	-	-	-	-	
EIM-Zugriffssteuerung für angegebenen Benutzer anzeigen	X	-	-	-	-	
EIM-Zugriffssteuerung abfragen	X	-	-	-	-	
Berechtigungsnachweis ändern	X	-	-	-	-	-
Berechtigungsnachweis abrufen	X	-	-	-	-	X
1 - Wenn es sich bei der angegebenen Registerdefinition um eine Gruppenregisterdefinition handelt, hat ein Administrator für ausgewählte Register nur für die entsprechende Gruppe Administratorberechtigung, nicht jedoch für die einzelnen Gruppenmitglieder.						

LDAP-Konzepte für EIM

In diesem Abschnitt wird erläutert, wie Sie LDAP (Lightweight Directory Access Protocol) zusammen mit EIM (EIM = Enterprise Identity Mapping) verwenden können.

EIM verwendet als Domänencontroller einen LDAP-Server. Dieser LDAP-Server dient zur Speicherung der EIM-Daten. Daher sollten Sie mit einigen LDAP-Konzepten, die sich auf die Konfiguration und Verwendung von EIM in Ihrem Unternehmen beziehen, vertraut sein.

Beispielsweise können Sie einen registrierten LDAP-Namen als Benutzeridentität zur Konfiguration von EIM und zur Authentifizierung am EIM-Domänencontroller verwenden.

Um die Konfiguration und Verwendung von EIM besser zu verstehen, sollten Sie die folgenden LDAP-Konzepten kennen:

Zugehörige Konzepte

„Enterprise Identity Mapping - Konzepte" auf Seite 5
In diesem Abschnitt werden wichtige EIM-Konzepte erläutert, die Sie für eine erfolgreiche Implementierung von EIM benötigen.

Registrierter Name

Im Folgenden erfahren Sie, wie registrierte Namen (DN = Distinguished Names) im Lightweight Directory Access Protocol (LDAP) verwendet werden können.

Ein registrierter Name ist ein LDAP-Eintrag, der einen Eintrag auf einem Directory-Server (LDAP-Server) eindeutig angibt und beschreibt. Sie verwenden den EIM-Konfigurationsassistenten (EIM = Enterprise Identity Mapping), um den Directory-Server zum Speichern von EIM-Domänendaten zu konfigurieren. Da EIM den Directory-Server zum Speichern von EIM-Daten verwendet, können Sie registrierte Namen zur Authentifizierung am EIM-Domänencontroller angeben.

Registrierte Namen bestehen aus dem Namen des Eintrags sowie den Namen (sortiert von unten nach oben) der Objekte, die dem Eintrag im LDAP-Verzeichnis übergeordnet sind. Ein Beispiel für einen vollständigen registrierten Namen ist `cn=Tim Jones, o=IBM, c=US`. Jeder Eintrag besitzt mindestens ein Attribut, das zur Benennung des Eintrags verwendet wird. Dieses Benennungsattribut wird als relativer registrierter Name (Relative Distinguished Name, RDN) des Eintrags bezeichnet. Der Eintrag, der einem bestimmten relativen registrierten Namen (RDN) übergeordnet ist, wird als sein übergeordneter registrierter Name (siehe „Übergeordneter registrierter Name") bezeichnet. In diesem Beispiel ist `cn=Tim Jones` der Name des Eintrags und somit der relative registrierte Name (RDN). `o=IBM, c=US` ist der übergeordnete registrierte Name für `cn=Tim Jones`.

Da EIM den Directory-Server zum Speichern von EIM-Daten verwendet, können Sie registrierte Namen zur Authentifizierung am EIM-Domänencontroller angeben. Sie können auch einen registrierten Namen für die Benutzeridentität verwenden, die EIM für Ihren iSeries-Server konfiguriert. Beispielsweise können Sie einen registrierten Namen verwenden, wenn Sie folgende Aktionen ausführen:

- Den Directory-Server als EIM-Domänencontroller konfigurieren. Dazu müssen Sie den registrierten Namen, der den LDAP-Administrator für den Directory-Server angibt, erstellen und verwenden. Sie können den Directory-Server, falls noch nicht geschehen, konfigurieren, wenn Sie mit dem EIM-Konfigurationsassistenten eine neue Domäne erstellen und ein System zu dieser Domäne hinzufügen.
- Den EIM-Konfigurationsassistenten verwenden, um den Typ der Benutzeridentität auszuwählen, mit dem der Assistent die Verbindung zum EIM-Domänencontroller herstellen soll. "Registrierter Name" ist einer der auswählbaren Benutzertypen. Der registrierte Name muss einen Benutzer darstellen, der die Berechtigung besitzt, Objekte im lokalen Namespace des Directory-Servers zu erstellen.
- Den EIM-Konfigurationsassistenten verwenden, um den Benutzertyp auszuwählen, mit dem EIM-Operationen für Betriebssystemfunktionen ausgeführt werden sollen. Zu diesen Operationen gehören Abgleichsuchoperationen und das Löschen von Zuordnungen, wenn ein lokales i5/OS-Benutzerprofil gelöscht wird. "Registrierter Name" ist einer der auswählbaren Benutzertypen.
- Eine Verbindung zum Domänencontroller herstellen, um EIM zu verwalten, z. B., um Register und Kennungen zu verwalten und Abgleichsuchoperationen auszuführen.
- Zertifikatfilter erstellen, um den Geltungsbereich einer Richtlinienzuordnung für Zertifikatfilter zu bestimmen. Wenn Sie einen Zertifikatfilter erstellen, müssen Sie die Informationen zum registrierten Namen des Zertifikatinhabers bzw. des Zertifikatausstellers oder zum Zertifikat angeben. Ziel ist die Angabe der Kriterien, die der Filter verwendet, um zu bestimmen, welche Zertifikate von der Richtlinienzuordnung betroffen sind.

Zugehörige Informationen

Directory Server Concepts

Übergeordneter registrierter Name

Im Folgenden wird die Hierarchie der registrierten Namen (DN = Distinguished Name) erläutert.

Ein übergeordneter registrierter Name (Distinguished Name, DN) ist ein Eintrag im Namespace des LDAP-Directory-Servers (Lightweight Directory Access Protocol). Einträge des LDAP-Servers sind in einer hierarchischen Struktur angeordnet, die politische, geografische, organisatorische oder Domänengrenzen widerspiegeln kann. Ein registrierter Name wird als übergeordneter registrierter Name bezeichnet, wenn der registrierte Name der Verzeichniseintrag ist, der einem vorhandenen registrierten Namen direkt übergeordnet ist.

Ein Beispiel für einen vollständigen registrierten Namen ist `cn=Tim Jones, o=IBM, c=US`. Jeder Eintrag besitzt mindestens ein Attribut, das zur Benennung des Eintrags verwendet wird. Dieses Benennungsattribut wird als relativer registrierter Name (Relative Distinguished Name, RDN) des Eintrags bezeichnet. Der Eintrag, der einem bestimmten relativen registrierten Namen (RDN) übergeordnet ist, wird als sein übergeordneter registrierter Name bezeichnet. In diesem Beispiel ist `cn=Tim Jones` der Name des Eintrags und somit der relative registrierte Name (RDN). `o=IBM, c=US` ist der übergeordnete registrierte Name für `cn=Tim Jones`.

EIM (Enterprise Identity Mapping) verwendet als Domänencontroller einen Directory-Server, der zum Speichern von EIM-Domänendaten dient. Der übergeordnete registrierte Name in Kombination mit dem EIM-Domänennamen bestimmt die Position der EIM-Domänendaten im Namespace des Directory-Servers. Wenn Sie mit dem EIM-Konfigurationsassistenten eine neue Domäne erstellen und ein System zu dieser Domäne hinzufügen möchten, können Sie einen übergeordneten registrierten Namen für die zu erstellende Domäne angeben. Mit einem übergeordneten registrierten Namen können Sie angeben, an welcher Position im LDAP-Namespace diese EIM-Daten für die Domäne gespeichert werden sollen. Wenn Sie keinen übergeordneten registrierten Namen angeben, werden EIM-Daten unter dem eigenen Suffix im Namespace gespeichert, und die Standardposition der EIM-Domänendaten ist `ibm-eimDomainName=EIM`.

Zugehörige Informationen

Directory Server Concepts

LDAP-Schema und weitere Hinweise für EIM

In diesen Informationen wird erläutert, welche Voraussetzungen erforderlich sind, damit der Directory-Server mit EIM (Enterprise Identity Mapping) eingesetzt werden kann.

Zur Ausführung von EIM muss der Domänencontroller auf einem Directory-Server implementiert sein, der LDAP (Lightweight Directory Access Protocol) Version 3 unterstützt. Darüber hinaus muss der Directory-Server das EIM-Schema akzeptieren und die folgenden Attribute und Objektklassen identifizieren können:

- Das Attribut ibm-entryUUID
- Die IBM Attributtypen (ibmattributetypes):
  - acIEntry
  - acIPropagate
  - acISource
  - entryOwner
  - ownerPropagate
  - ownerSource
- EIM-Attribute einschließlich drei neuer Attribute für die Unterstützung von Richtlinienzuordnungen:
  - ibm-eimAdditionalInformation
  - ibm-eimAdminUserAssoc
  - ibm-eimDomainName, ibm-eimDomainVersion
  - ibm-eimRegistryAliases
  - ibm-eimRegistryEntryName
  - ibm-eimRegistryName
  - ibm-eimRegistryType

  - ibm-eimSourceUserAssoc
  - ibm-eimTargetIdAssoc
  - ibm-eimTargetUserName
  - ibm-eimUserAssoc
  - ibm-eimFilterType
  - ibm-eimFilterValue
  - ibm-eimPolicyStatus
- EIM-Objektklassen einschließlich drei neuer Klassen für die Unterstützung von Richtlinienzuordnungen:
  - ibm-eimApplicationRegistry
  - ibm-eimDomain
  - ibm-eimIdentifier
  - ibm-eimRegistry
  - ibm-eimRegistryUser
  - ibm-eimSourceRelationship
  - ibm-eimSystemRegsitry
  - ibm-eimTargetRelationship
  - ibm-eimFilterPolicy
  - ibm-eimDefaultPolicy
  - ibm-eimPolicyListAux

Diese Funktion wird von IBM Directory Server for iSeries ab V5R3 unterstützt. Weitere Informationen zu den IBM Directory Server-Produkten, die EIM unterstützen, sowie weitere Hinweise zu EIM-Domänencontrollern finden Sie im Abschnitt EIM-Domänencontroller planen.

Wenn Sie den Directory-Server gegenwärtig auf einem iSeries-System V5R2 als EIM-Domänencontroller einsetzen, müssen Sie das LDAP-Schema und die EIM-Unterstützung für diesen Directory-Server aktualisieren, damit Sie diesen auch zur Verwaltung von EIM-Domänendaten verwenden können, die unter V5R3 oder einer späteren Version erstellt wurden.

Zugehörige Informationen

iSeries LDAP

iSeries-Konzepte für EIM

In diesem Abschnitt werden alle Anwendungen für Enterprise Identity Mapping (EIM) aufgelistet.

Sie können EIM auf jeder IBM @server -Plattform implementieren. Wenn Sie EIM auf dem iSeries-Server implementieren, müssen Sie einige Punkte beachten, die ausschließlich für die Implementierung des iSeries-Servers gelten. Die folgenden Abschnitte enthalten Informationen zu EIM-fähigen i5/OS-Anwendungen, Hinweise zu Benutzerprofilen und andere Themen, die Ihnen helfen, EIM auf einem iSeries-System effizient zu nutzen:

Zugehörige Konzepte

„Enterprise Identity Mapping - Konzepte” auf Seite 5
In diesem Abschnitt werden wichtige EIM-Konzepte erläutert, die Sie für eine erfolgreiche Implementierung von EIM benötigen.

Hinweise zu i5/OS-Benutzerprofilen für EIM

Die Berechtigung zur Ausführung von Tasks in Enterprise Identity Mapping (EIM) basiert nicht auf der Berechtigung des i5/OS-Benutzerprofils, sondern auf der Berechtigung für die EIM-Zugriffssteuerung

(siehe „EIM-Zugriffssteuerung” auf Seite 42). Um i5/OS für EIM zu konfigurieren, müssen jedoch einige zusätzliche Tasks ausgeführt werden. Für diese zusätzlichen Tasks ist ein i5/OS-Benutzerprofil mit den entsprechenden Sonderberechtigungen erforderlich.

Um i5/OS über den iSeries Navigator für die Verwendung von EIM zu konfigurieren, muss Ihr Benutzerprofil über die folgenden Sonderberechtigungen verfügen:

- Sicherheitsadministrator (*SECADM)
- Berechtigung für alle Objekte (*ALLOBJ)
- Systemkonfiguration (*IOSYSCFG)

Befehlserweiterung des i5/OS-Benutzerprofils für EIM-Kennungen

Wenn Sie EIM für das System konfigurieren, können Sie für den Befehl CRTUSRPRF (Benutzerprofil erstellen; siehe hierzu Create user profile) und den Befehl CHGUSRPRF (Benutzerprofil ändern) den neuen Parameter EIMASSOC verwenden. Sie können mit diesem Parameter EIM-Kennungszuordnungen für das angegebene Benutzerprofil für das lokale Register definieren.

Wenn Sie diesen Parameter verwenden, können Sie die folgenden Informationen angeben:

- EIM-Kennungsname, d. h. ein neuer oder ein vorhandener Kennungsname.
- Eine Aktionsoption für die Zuordnung, die darin besteht, die angegebene Zuordnung hinzuzufügen (*ADD), zu ersetzen (*REPLACE) oder zu entfernen (*REMOVE).

  Anmerkung: Verwenden Sie *ADD, um neue Zuordnungen zu konfigurieren. Verwenden Sie die Option *REPLACE, wenn Sie z. B. zuvor Zuordnungen für die falsche Kennung definiert haben. Die Option *REPLACE entfernt für das lokale Register alle vorhandenen Zuordnungen des angegebenen Typs zu anderen Kennungen und fügt dann die Zuordnung, die für den Parameter angegeben wurde, hinzu. Mit der Option *REMOVE können Sie alle angegebenen Zuordnungen aus der angegebenen Kennung entfernen.
- Den Typ der Kennungszuordnung, d. h. eine Ziel- und/oder eine Quellenzuordnung bzw. eine administrative Zuordnung.
- Ob die angegebene EIM-Kennung, falls noch nicht vorhanden, erstellt werden soll.

Normalerweise erstellen Sie eine Zielzuordnung für ein i5/OS-Profil. Dies gilt insbesondere in einer Einzelanmeldungsumgebung. Nachdem Sie mit dem Befehl zur Erstellung die erforderliche Zielzuordnung für das Benutzerprofil (und die EIM-Kennung, falls erforderlich) erstellt haben, müssen Sie möglicherweise eine entsprechende Quellenzuordnung erstellen. Sie können mit dem iSeries Navigator eine Quellenzuordnung für eine andere Benutzeridentität, z. B. den Kerberos-Principal, mit dem sich der Benutzer am Netzwerk anmeldet, erstellen.

Wenn Sie EIM für das System konfiguriert haben, haben Sie eine Kombination aus Benutzeridentität und Kennwort für das System angegeben, die bei der Ausführung von EIM-Operationen für das Betriebssystem verwendet werden soll. Diese Benutzeridentität muss eine Berechtigung für die EIM-Zugriffssteuerung besitzen, die für das Erstellen von Kennungen und das Hinzufügen von Zuordnungen ausreichend ist.

Kennwörter des i5/OS-Benutzerprofils und EIM

Wenn der Administrator EIM als Teil einer Einzelanmeldungsumgebung konfiguriert, besteht seine primäre Aufgabe darin, den Umfang für die Verwaltung von Benutzerkennwörtern, der für die typischen Endbenutzer in Ihrem Unternehmen entsteht, zu reduzieren. Wenn Sie den Identitätsabgleich von EIM in Kombination mit der Kerberos-Authentifizierung verwenden, müssen die Benutzer weniger Anmeldevorgänge ausführen und sich weniger Kennwörter merken und verwalten. Sie profitieren davon, da durch den Abgleich von Benutzeridentitäten seltener Fehler bei der Kennworteingabe auftreten. Ein Beispiel

hierfür ist das Zurücksetzen von Kennwörtern, die von Benutzern vergessen wurden. Die Kennwortregeln Ihrer Sicherheitsrichtlinie sind jedoch weiterhin wirksam, d. h., Sie müssen die Benutzerprofile bearbeiten, wenn das Kennwort abläuft.

Wenn Sie noch mehr von der Einzelanmeldungsumgebung profitieren möchten, sollten Sie in Erwägung ziehen, die Kennworteinstellung für die Benutzerprofile zu ändern, die das Ziel von Identitätsabgleichen sind. Als Ziel eines Identitätsabgleichs muss der Benutzer nicht mehr das Kennwort des Benutzerprofils angeben, wenn er auf ein iSeries-System oder eine EIM-fähige i5/OS-Ressource zugreift. Für normale Benutzer können Sie die Kennworteinstellung auf *NONE setzen, damit kein Kennwort mit dem Benutzerprofil verwendet werden kann. Der Eigner des Benutzerprofils benötigt wegen des Identitätsabgleichs und der Einzelanmeldung kein Kennwort mehr. Wenn Sie als Kennworteinstellung *NONE angeben, bietet dies weitere Vorteile, da Sie und Ihre Benutzer kein Verfallsdatum von Kennwörtern mehr berücksichtigen müssen. Darüber hinaus kann niemand das Profil verwenden, um sich direkt an der iSeries anzumelden oder auf EIM-fähige i5/OS-Ressourcen zuzugreifen. Administratoren sollten aber weiterhin einen Kennwortwert für ihre Benutzerprofile besitzen, falls sie sich direkt am iSeries-System anmelden müssen. Wenn Ihr EIM-Domänencontroller z. B. ausfällt und kein Identitätsabgleich durchgeführt werden kann, muss ein Administrator sich möglicherweise direkt am iSeries-System anmelden, bis das Problem mit dem Domänencontroller gelöst ist.

i5/OS-Überwachung für EIM

Ihr Überwachungskonzept stellt einen wichtigen Bestandteil des Gesamtsicherheitsplans dar. Wenn Sie Enterprise Identity Mapping (EIM) konfigurieren und verwenden, sollten Sie die Überwachungsunterstützung für den Directory-Server konfigurieren, um zu gewährleisten, dass die Berechtigungsstufen, die Ihre Sicherheitsrichtlinie erfordert, zur Verfügung stehen. Beispielsweise kann die Überwachungsunterstützung hilfreich sein, wenn Sie feststellen möchten, welche der Benutzer, die von einer Richtlinienzuordnung abgeglichen wurden, eine Aktion im System ausgeführt oder ein Objekt geändert haben.

Weitere Informationen zur Überwachungsunterstützung für IBM Directory Server for iSeries (LDAP) enthält der Abschnitt Auditing unter dem Thema zu IBM Directory Server for iSeries (LDAP) im Information Center. Dieses Thema enthält auch die entsprechenden Verweise auf Hinweise zur i5/OS-Überwachung sowie zu den Einstellungen, die Sie aktivieren müssen, um sicherzustellen, dass die Directory-Server-Überwachung korrekt konfiguriert wird.

EIM-fähige Anwendungen für i5/OS

Die folgenden i5/OS-Anwendungen können zur Verwendung von Enterprise Identity Mapping (EIM) konfiguriert werden:

- i5/OS Host-Server (gegenwärtig von iSeries Access für Windows und iSeries Navigator verwendet)
- Telnet Server (gegenwärtig von PC5250 und IBM WebSphere Host On-Demand verwendet)
- QFileSrv.400 ODBC (ermöglicht die Verwendung der Einzelanmeldung über SQL)
- JDBC (ermöglicht die Verwendung von EIM über SQL)
- Distributed Relational Database Architecture (DRDA) (ermöglicht die Verwendung von EIM über SQL)
- IBM WebSphere Host On-Demand Version 8 (das Feature Web Express Logon)
- NetServer
- QFileSvr.400

Enterprise Identity Mapping - Szenarios

Im Folgenden wird erläutert, wie Sie Benutzeridentitäten in einer Einzelanmeldungsumgebung auf mehreren Systemen verwalten können.

Enterprise Identity Mapping (EIM) ist eine IBM Infrastrukturtechnologie, mit der Sie Benutzeridentitäten in einem Unternehmen zurückverfolgen und verwalten können. Normalerweise verwenden Sie EIM mit einem Authentifizierungsverfahren (z. B. dem Netzwerkauthentifizierungsservice), um eine Einzelanmeldungsumgebung zu implementieren.

Wenn Sie an dieser weitergehenden Verwendung von EIM interessiert sind, finden Sie weitere Informationen unter Szenarios im Thema "Einzelanmeldung" des Information Centers.

Enterprise Identity Mapping planen

Im Folgenden wird erläutert, wie Sie einen EIM-Implementierungsplan (EIM = Enterprise Identity Mapping) entwickeln können, um sicherzustellen, dass EIM für iSeries oder in einer Umgebung mit mehreren Plattformen richtig konfiguriert wird.

Für die erfolgreiche Konfiguration und Verwendung von Enterprise Identity Mapping (EIM) in Ihrem Unternehmen ist ein Implementierungsplan erforderlich. Zur Entwicklung eines solchen Plans müssen Sie Daten über die Systeme, Anwendungen und Benutzer erfassen, die EIM verwenden werden. Anhand der erfassten Informationen legen Sie die für Ihr Unternehmen am besten geeignete EIM-Konfiguration fest.

Da es sich bei EIM um eine IBM @server -Infrastrukturtechnologie handelt, die für alle IBM Plattformen zur Verfügung steht, hängt die Implementierungsplanung davon ab, welche Plattformen Sie in Ihrem Unternehmen verwenden. Obwohl es verschiedene Planungsaktivitäten gibt, die nur für einzelne Plattformen gelten, sind viele Aktivitäten für alle IBM Plattformen gültig. Sie sollten sich einen Überblick über die allgemeinen EIM-Planungsaktivitäten verschaffen, um Ihren Gesamtplan für die Implementierung zu erstellen. Folgende Seiten enthalten weitere Informationen zur Planung der EIM-Implementierung:

EIM für eServer planen

Für die erfolgreiche Konfiguration und Verwendung von Enterprise Identity Mapping (EIM) in einem Unternehmen mit mehreren Plattformen ist ein Implementierungsplan erforderlich. Zur Entwicklung dieses Plans müssen Sie Daten über die Systeme, Anwendungen und Benutzer erfassen, die EIM verwenden sollen. Anhand der erfassten Informationen legen Sie die für eine Umgebung mit mehreren Plattformen am besten geeignete EIM-Konfiguration fest.

Die folgende Liste dient als Übersicht über die Planungsaufgaben, die Sie ausführen sollten, bevor Sie EIM in einer Umgebung mit mehreren Plattformen konfigurieren und verwenden. Lesen Sie die Informationen auf den folgenden Seiten sorgfältig durch, damit Sie Ihre EIM-Konfigurationsanforderungen entsprechend planen können. Zudem werden die vom Implementierungsteam benötigten Kenntnisse, die zu erfassenden Informationen und die erforderlichen Konfigurationsentscheidungen erläutert. Sie können bei Bedarf die Planungsarbeitsblätter für EIM (Nummer 8 in der folgenden Liste) drucken und diese während des Planungsprozesses ausfüllen.

EIM-Installationsvoraussetzungen für eServer

Wenn Sie EIM (Enterprise Identity Mapping) in Ihrem Unternehmen erfolgreich implementieren möchten, müssen in den drei folgenden Bereichen bestimmte Voraussetzungen erfüllt sein:

1. Voraussetzungen auf Unternehmens- oder Netzwerkebene
2. Systemvoraussetzungen
3. Anwendungsvoraussetzungen

Voraussetzungen auf Unternehmens- oder Netzwerkebene

Sie müssen ein System in Ihrem Unternehmen oder Netzwerk als EIM-Domänencontroller konfigurieren. Dieser Controller muss ein speziell konfigurierter LDAP-Server (Lightweight Directory Access Protocol) sein, auf dem EIM-Domänendaten gespeichert und zur Verfügung gestellt werden. Bei der Auswahl eines Verzeichnisservice-Produkts als Domänencontroller müssen gewisse Aspekte berücksichtigt werden, z. B. die Tatsache, dass nicht alle LDAP-Server-Produkte EIM-Domänencontroller unterstützen.

Ein weiterer Aspekt ist die Verfügbarkeit von Verwaltungstools. Eine Option ist, die EIM-APIs in Ihre eigenen Anwendungen zur Ausführung von Verwaltungsfunktionen zu integrieren. Wenn Sie Directory Server for iSeries (LDAP) als EIM-Domänencontroller einsetzen möchten, können Sie zur Verwaltung von

EIM den iSeries Navigator benutzen. Möchten Sie mit IBM Directory arbeiten, können Sie auf das Dienstprogramm eimadmin, das Bestandteil von V1R4 LDAP SPE ist, zurückgreifen.

In den folgenden Abschnitten finden Sie Informationen darüber, welche IBM Plattformen ein Directory-Server-Produkt besitzen, das EIM unterstützt. Ausführliche Informationen zur Auswahl eines Directory-Servers, um Unterstützung für einen EIM-Domänencontroller zur Verfügung zu stellen, finden Sie unter EIM-Domänencontroller planen.

System- und Anwendungsvoraussetzungen

Alle Systeme, die zur EIM-Domäne gehören, müssen die folgenden Voraussetzungen erfüllen:

- Die LDAP-Client-Software muss installiert sein.
- Die EIM-APIs müssen implementiert sein.

Alle Anwendungen, die zur EIM-Domäne gehören, müssen in der Lage sein, für die Abgleichsuche und andere Operationen die EIM-APIs zu verwenden.

Anmerkung: Bei verteilten Anwendungen ist es möglicherweise nicht erforderlich, dass sowohl die Server- als auch die Clientseite die EIM-APIs nutzen können. Zumeist muss lediglich die Serverseite der Anwendung in der Lage sein, die EIM-APIs zu nutzen.

Die folgende Tabelle enthält Informationen zu der von den @server -Plattformen zur Verfügung gestellten EIM-Unterstützung. Die Informationen werden nach Plattform geordnet in Spalten aufgelistet, die folgende Angaben enthalten:

- Den EIM-Client, der für die Plattform zur Unterstützung der EIM-APIs erforderlich ist.
- Die Art der EIM-Konfiguration und die Verwaltungstools, die für die Plattform verfügbar sind.
- Das Directory-Server-Produkt, das für die Plattform als EIM-Domänencontroller installiert werden kann.

Eine Plattform muss nicht als EIM-Domänencontroller fungieren können, um zu einer EIM-Domäne zu gehören.

Tabelle 9. eServer-EIM-Unterstützung

Plattform	EIM-Client (API-Unterstützung)	Domänencontroller	EIM-Verwaltungstools
AIX auf pSeries	AIX R5.2	IBM Directory V5.1	Nicht verfügbar
Linux • SLES8 auf PPC64 • Red Hat 7.3 auf i386 • SLES7 auf zSeries	Download von: • IBM Directory V4.1-Client • IBM Directory V5.1-Client • Open LDAP v2.0.23-Client	IBM Directory V5.1	Nicht verfügbar
i5/OS auf iSeries	OS/400 V5R2 und i5/OS ab V5R3	OS/400 V5R2 und i5/OS ab V5R3 oder ein Directory-Server einer späteren Version	iSeries Navigator V5R2 und V5R3 oder eine spätere Version dieses Produkts

Tabelle 9. eServer-EIM-Unterstützung (Forts.)

Plattform	EIM-Client (API-Unterstützung)	Domänencontroller	EIM-Verwaltungstools
Windows 2000 auf xSeries	Download von: • IBM Directory V4.1-Client • IBM Directory V5.1-Client	IBM Directory V5.1-Client	Nicht verfügbar
z/OS auf zSeries	z/OS V1R4 LDAP SPE OW57137	z/OS V1R4 LDAP	V1R4 LDAP SPE OW57137

Anmerkung: Weitere Informationen zum Produkt IBM Directory Server enthält die Website der IBM für Webprodukte http://www-3.ibm.com/software/network/help-directory/

Sofern eine Plattform EIM-Clientunterstützung (API-Unterstützung) zur Verfügung stellt, kann das System einer EIM-Domäne hinzugefügt werden. Die Plattform muss EIM-Domänencontroller nur dann unterstützen, wenn diese bestimmte Plattform als EIM-Domänencontroller für das Unternehmen verwendet werden soll.

Nachdem Sie sich vergewissert haben, dass alle EIM-Voraussetzungen erfüllt sind, fahren Sie mit der Erfassung von Kenntnissen, Aufgabenbereichen und Berechtigungen für die EIM-Konfiguration fort.

Erforderliche Kenntnisse und Aufgabenbereiche

Enterprise Identity Mapping (EIM) wurde so konzipiert, dass in einem kleineren Unternehmen alle Konfigurations- und Verwaltungsaufgaben von einer einzigen Person bewältigt werden können. In einem größeren Unternehmen können diese Zuständigkeiten auch auf mehrere Personen verteilt werden. Die Anzahl der Teammitglieder ist vom Kenntnisstand jedes einzelnen Teammitglieds, den von der EIM-Implementierung betroffenen Plattformtypen und der Aufteilung von Sicherheitsbereichen und -zuständigkeiten in Ihrem Unternehmen abhängig.

Eine erfolgreiche EIM-Implementierung setzt die Konfiguration und Interaktion zahlreicher Softwareprodukte voraus. Da jedes dieser Produkte spezifische Kenntnisse und Aufgabenbereiche erfordert, besteht das EIM-Implementierungsteam vor allem in großen Unternehmen zumeist aus Personen mit einer Vielzahl unterschiedlicher Aufgabenbereiche.

Im Folgenden wird erläutert, welche Kenntnisse und Berechtigungen (siehe „EIM-Zugriffssteuerung" auf Seite 42) für die EIM-Implementierung erforderlich sind. Diese Kenntnisse werden in Form von Tätigkeitsbezeichnungen für Personen, die sich auf diese Kenntnisse spezialisiert haben, dargestellt. Beispielsweise wird eine Task, für die LDAP-Kenntnisse (Lightweight Directory Access Protocol) erforderlich sind, als Task für einen Directory-Server-Administrator beschrieben.

Teammitglieder und deren Aufgabenbereiche

Im Folgenden werden die Zuständigkeiten und Berechtigungen der Aufgabenbereiche beschrieben, die für die Verwaltung von EIM benötigt werden. Sie können anhand dieser Liste festlegen, welche Teammitglieder für die Installation und Konfiguration vorausgesetzter Produkte sowie für die Konfiguration von EIM und mindestens einer EIM-Domäne erforderlich sind.

Zu den ersten Aufgabenbereichen, die definiert werden müssen, gehören die Anzahl und Art der Administratoren für die EIM-Domäne. Alle Mitarbeiter mit EIM-Verwaltungsaufgaben und -berechtigungen sollten in die EIM-Planung einbezogen werden und dem EIM-Implementierungsteam angehören.

Anmerkung: EIM-Administratoren spielen in Ihrem Unternehmen eine wichtige Rolle. Sie sind ebenso wichtig wie Personen, die auf Ihren Systemen Benutzeridentitäten erstellen können. Wenn

Sie EIM-Zuordnungen für Benutzeridentitäten erstellen, legen sie fest, wer auf Ihre Computersysteme zugreifen kann und welche Berechtigung diese Person beim Zugriff besitzt. IBM empfiehlt, diese Berechtigung nur vertrauenswürdigen Personen unter Berücksichtigung der Sicherheitsrichtlinien Ihres Unternehmens zu erteilen.

Die folgende Tabelle enthält eine Liste der Aufgabenbereiche von potenziellen Teammitgliedern sowie der erforderlichen Aufgaben und Kenntnisse für die Konfiguration und Verwaltung von EIM. Ausführliche Informationen zu den EIM-Verwaltungsaufgaben, die von jedem Aufgabenbereich ausgeführt werden können, enthält der Abschnitt „EIM-Zugriffssteuerung" auf Seite 42.

Anmerkung: Wenn in Ihrem Unternehmen nur eine Person für alle EIM-Konfigurationsaufgaben und -Verwaltungsaufgaben zuständig ist, sollte diese den Aufgabenbereich des EIM-Administrators mit den entsprechenden Berechtigungen übernehmen.

Tabelle 10. Aufgabenbereiche, Aufgaben und Kenntnisse für die Konfiguration von EIM

Aufgabenbereich	**Aufgabenberechtigung**	**Erforderliche Kenntnisse**
EIM-Administrator	• Koordination von Domänenoperationen • Hinzufügen, Entfernen und Ändern von Registerdefinitionen, EIM-Kennungen und Zuordnungen für Benutzeridentitäten • Controllerberechtigung für die Daten in einer EIM-Domäne	Kenntnis der EIM-Verwaltungstools
EIM-Kennungsadministrator	• Erstellen und Ändern von EIM-Kennungen • Hinzufügen und Entfernen von administrativen und Quellenzuordnungen (Zielzuordnungen können nicht hinzugefügt oder entfernt werden)	Kenntnis der EIM-Verwaltungstools
EIM-Registeradministrator	Verwalten aller EIM-Registerdefinitionen: • Hinzufügen und Entfernen von Zielzuordnungen (administrative und Quellenzuordnungen können nicht hinzugefügt oder entfernt werden) • Aktualisieren von EIM-Registerdefinitionen	Kenntnisse in folgenden Bereichen: • Alle in der EIM-Domäne definierten Benutzerregister (z. B. Informationen über Benutzeridentitäten) • EIM-Verwaltungstools
Administrator für EIM-Register X	Verwalten einer bestimmten EIM-Registerdefinition: • Hinzufügen und Entfernen von Zielzuordnungen für ein bestimmtes Benutzerregister (z. B. Register X) • Aktualisieren einer bestimmten EIM-Registerdefinition	Kenntnisse in folgenden Bereichen: • Bestimmtes, in der EIM-Domäne definiertes Benutzerregister (z. B. Informationen über Benutzeridentitäten) • EIM-Verwaltungstools

Tabelle 10. Aufgabenbereiche, Aufgaben und Kenntnisse für die Konfiguration von EIM (Forts.)

Aufgabenbereich	Aufgabenberechtigung	Erforderliche Kenntnisse
Directory-Server-Administrator (LDAP)	• Installieren und Konfigurieren eines Directory-Servers (falls erforderlich) • Anpassen der Verzeichnisservicekonfiguration für EIM • Erstellen einer EIM-Domäne (siehe Anmerkung) • Definieren von Benutzern, die berechtigt sind, auf den EIM-Domänencontroller zuzugreifen • Optional: Definieren des ersten EIM-Administrators **Anmerkung:** Der Directory-Server-Administrator besitzt alle Berechtigungen eines EIM-Administrators.	Kenntnisse in folgenden Bereichen: • Installation, Konfiguration und Anpassung des Directory-Servers • EIM-Verwaltungstools
Benutzerregisteradministrator	• Einrichten von Benutzerprofilen oder Benutzeridentitäten für ein bestimmtes Benutzerregister • Optional: Übernahme der Aufgaben des EIM-Registeradministrators für ein bestimmtes Benutzerregister	Kenntnisse in folgenden Bereichen: • Tools zur Verwaltung des Benutzerregisters • EIM-Verwaltungstools
Systemprogrammierer oder Systemadministrator	Installation der benötigten Softwareprodukte (ggf. inklusive Installation von EIM)	Kenntnisse in folgenden Bereichen: • Systemprogrammierung oder -verwaltung • Installationsverfahren für die Plattform
Anwendungsprogrammierer	Schreiben von Anwendungen, die die EIM-APIs verwenden	Kenntnisse in folgenden Bereichen: • Plattform • Programmierkenntnisse • Programmkompilierung

Nachdem Sie die Aufgabenbereiche identifiziert haben, die Sie für die Konfiguration und Verwaltung von EIM in Ihren Unternehmen verwenden möchten, fahren Sie mit dem Abschnitt ″EIM-Domäne planen″ fort.

EIM-Domäne planen

Der Planungsprozess für die erstmalige EIM-Implementierung (Enterprise Identity Mapping) erfordert die Definition einer EIM-Domäne. Wenn Sie den größtmöglichen Nutzen aus einem zentralen Repository für den Informationsabgleich ziehen möchten, müssen Sie in Ihrem Plan festlegen, dass die Domäne von vielen Anwendungen und Systemen gemeinsam benutzt wird.

Bei der EIM-Planung erfassen Sie die Informationen, die Sie zur Definition der Domäne benötigen und notieren diese auf den Planungsarbeitsblättern. Die Beispiele in den Arbeitsblättern unterstützen Sie bei der Erfassung der Informationen in den einzelnen Planungsphasen.

In der folgenden Tabelle sind die Informationen zur Planung der Domäne enthalten. Darüber hinaus wird die Aufteilung der Aufgabenbereiche im EIM-Implementierungsteam für die einzelnen Planungsschritte empfohlen.

Anmerkung: In der Tabelle sind zwar die spezifischen, für die Erfassung der genannten Informationen zuständigen Aufgabenbereiche aufgelistet, sie gelten jedoch nur als Empfehlung. Sie sollten die Aufgabenbereiche basierend auf den Anforderungen und Sicherheitsrichtlinien Ihres Unternehmens zuweisen. In einem kleineren Unternehmen können Sie beispielsweise eine einzelne Person zum EIM-Administrator ernennen, der für alle Aspekte der Planung, Konfiguration und Verwaltung von EIM zuständig sein soll.

Tabelle 11. Für die Planung der EIM-Domänen erforderliche Informationen

Erforderliche Informationen	Aufgabenbereich
1. Existiert bereits eine Domäne, die Ihren Anforderungen entspricht, oder müssen Sie eine neue Domäne erstellen?	EIM-Administrator
2. Welcher Directory-Server wird als EIM-Domänencontroller verwendet? (Weitere Informationen zur Auswahl eines Domänencontrollers finden Sie unter EIM-Domänencontroller planen.)	LDAP-Administrator (Directory-Server) oder EIM-Administrator
3. Name der Domäne. (Sie können zudem eine optionale Beschreibung eingeben.)	EIM-Administrator
4. In welchem Bereich des Verzeichnisses werden EIM-Domänendaten gespeichert? **Anmerkung:** Es müssen bestimmte Konfigurationsaufgaben für Verzeichnisservices ausgeführt werden, bevor die Domäne erstellt werden kann. Die Art der Aufgaben ist davon abhängig, auf welchem System sich der Directory-Server befindet und welches Verzeichnis für die Speicherung von EIM-Daten ausgewählt wird.	Administrator des Directory-Servers (LDAP) oder EIM-Administrator
5. Anwendungen und Betriebssysteme innerhalb der Domäne. Bei der Konfiguration der ersten Domäne kann diese auch nur aus einem System bestehen. (Weitere Informationen finden Sie unter Benennungsplan für EIM-Registerdefinitionen entwickeln.)	EIM-Team
6. Personen und Entitäten innerhalb der Domäne. **Anmerkung:** Um die Anfangstests zu vereinfachen, können Sie die Anzahl auf ein oder zwei Teilnehmer beschränken.	EIM-Team

Nachdem Sie wissen, welche Informationen Sie zur Definition der EIM-Domäne benötigen, können Sie nun einen EIM-Domänencontroller planen, um EIM-Domänendaten zu speichern.

EIM-Domänencontroller planen

Bei der Erfassung von Informationen für die Definition der EIM-Domäne (Enterprise Identity Mapping) müssen Sie festlegen, welches Directory-Server-Produkt als EIM-Domänencontroller dienen soll. EIM setzt voraus, dass sich der Domänencontroller auf einem Directory-Server befindet, der Lightweight Directory Access Protocol (LDAP) Version 3 unterstützt. Darüber hinaus muss das Directory-Server-Produkt das LDAP-Schema akzeptieren und in der Lage sein, bestimmte Attribute und Objektklassen zu erkennen (LDAP-Schema und weitere Hinweise für EIM).

Wenn in Ihrem Unternehmen mehrere Directory-Server als Host für einen EIM-Domänencontroller in Frage kommen, sollten Sie in Betracht ziehen, sekundäre replizierte Domänencontroller zu verwenden. Wird beispielsweise von einer großen Anzahl von EIM-Abgleichsuchoperationen ausgegangen, verbessern Replikate die Leistung der Suchoperationen.

Darüber hinaus müssen Sie entscheiden, ob der Domänencontroller in Bezug auf das System, auf dem voraussichtlich die meisten Abgleichsuchoperationen ausgeführt werden, *lokal* oder *fern* ausgeführt werden soll. Wenn der Domänencontroller für das am meisten genutzte System lokal ausgeführt wird, erzie-

len Sie eine bessere Leistung der Suchoperationen im lokalen System. Halten Sie diese Planungsentscheidungen sowie die Entscheidungen bzgl. der Domäne und anderer Verzeichnisinformationen auf den Planungsarbeitsblättern fest.

Nachdem Sie festgelegt haben, welcher Directory-Server im Unternehmen als Host für den EIM-Domänencontroller fungieren soll, sind gewisse Entscheidungen über den Zugriff auf den Domänencontroller zu treffen.

Zugriff auf den Domänencontroller planen

Sie müssen einen Plan erstellen, der festlegt, wie EIM-fähige Anwendungen und Betriebssysteme und auch Sie selbst auf den Directory-Server, auf dem sich der EIM-Domänencontroller befindet, zugreifen sollen. Voraussetzungen für den Zugriff auf eine EIM-Domäne:

1. Es muss eine Bindung zum EIM-Domänencontroller hergestellt werden können.
2. Vergewissern Sie sich, dass das Bindesubjekt Mitglied einer EIM-Zugriffssteuerungsgruppe oder LDAP-Administrator ist. Weitere Informationen finden Sie unter EIM-Zugriffssteuerung verwalten.

EIM-Bindungstyp auswählen

Die EIM-APIs unterstützen zahlreiche Mechanismen zur Herstellung einer Verbindung mit dem EIM-Domänencontroller (dieser Vorgang wird auch als Binden bezeichnet). Jeder Bindemechanismus stellt eine andere Authentifizierungs- und Verschlüsselungsebene für die Verbindung zur Verfügung. Mögliche Auswahl:

- **Einfache Bindungen.** Eine einfache Bindung ist eine LDAP-Verbindung, bei der ein LDAP-Client einen registrierten Namen (Distinguished Name, DN) für Bindevorgänge und ein Bindekennwort zur Authentifizierung an den LDAP-Server übergibt. Der registrierte Name und das Kennwort für Bindevorgänge werden vom LDAP-Administrator im LDAP-Verzeichnis definiert. Dies ist die einfachste und unsicherste Authentifizierungsart, da der registrierte Name und das Kennwort für Bindevorgänge unverschlüsselt übertragen und somit abgefangen werden können. Verwenden Sie CRAM-MD5 (Challenge-Response-Authentifizierungsverfahren), um zusätzliche Schutzmaßnahmen für das Bindekennwort zu implementieren. Bei Verwendung des CRAM-MD5-Protokolls sendet der Client an Stelle des unverschlüsselten Kennworttextes einen Hashwert zur Authentifizierung an den Server.
- **Serverauthentifizierung mit Secure Sockets Layer (SSL) - serverseitige Authentifizierung.** Ein LDAP-Server kann für SSL- oder TLS-Verbindungen (Transport Layer Security) konfiguriert werden. Der LDAP-Server verwendet für seine eigene Authentifizierung am LDAP-Client ein digitales Zertifikat und baut eine verschlüsselte Kommunikationssitzung mit diesem auf. Nur der LDAP-Server wird durch das Zertifikat authentifiziert. Die Authentifizierung des Endbenutzers erfolgt über einen registrierten Namen und ein Kennwort für Bindevorgänge. Die Authentifizierungsebene entspricht somit einer einfachen Bindung, es werden jedoch alle Daten verschlüsselt (einschließlich des registrierten Namens und des Kennworts für Bindevorgänge).
- **Clientauthentifizierung mit SSL.** Ein LDAP-Server kann so konfiguriert werden, dass der Endbenutzer über ein digitales Zertifikat an Stelle eines registrierten Namens für Bindevorgänge und eines Kennworts authentifiziert werden muss, um eine sichere SSL- oder TLS-Verbindung zum LDAP-Server herzustellen. Sowohl der Client als auch der Server werden in diesem Fall authentifiziert, und die Sitzung wird verschlüsselt. Diese Option bietet eine striktere Benutzerauthentifizierung und gewährleistet den Schutz aller übertragenen Daten.
- **Kerberos-Authentifizierung.** Ein LDAP-Client kann mit einem Kerberos-Ticket am Server authentifiziert werden, welches an Stelle eines registrierten Namens für Bindevorgänge und eines Kennworts verwendet wird. Kerberos, ein anerkanntes Netzwerkauthentifizierungssystem eines Fremdanbieters, ermöglicht einem Principal (einem Benutzer oder Service), seine Identität innerhalb eines nicht gesicherten Netzwerks gegenüber einem anderen Service zu belegen. Die Authentifizierung von Principals erfolgt über einen zentralen Server, der als Key Distribution Center (KDC) bezeichnet wird. Das KDC authentifiziert einen Benutzer mit einem Kerberos-Ticket. Diese Tickets belegen die Identität des Principals gegenüber anderen Services in einem Netzwerk. Nachdem ein Principal mittels dieser Tickets

authentifiziert wurde, können der Principal und Service verschlüsselte Daten mit einem Zielservice austauschen. Diese Option bietet eine striktere Benutzerauthentifizierung und gewährleistet den Schutz der Authentifizierungsdaten.

Die Auswahl eines Bindemechanismus basiert auf der von der EIM-fähigen Anwendung benötigten Sicherheitsebene sowie auf den vom LDAP-Server (auf dem sich die EIM-Domäne befindet) unterstützten Authentifizierungsverfahren.

Sie müssen ggf. weitere Konfigurationsaufgaben für den LDAP-Server ausführen, um das ausgewählte Authentifizierungsverfahren zu aktivieren. Prüfen Sie anhand der Dokumentation des LDAP-Servers, auf dem sich der Domänencontroller befindet, welche zusätzlichen Konfigurationsaufgaben erforderlich sind.

Beispiel für ein Planungsarbeitsblatt: Domänencontrollerdaten

Nachdem Sie die Entscheidungen über den EIM-Domänencontroller getroffen haben, können Sie die vom EIM-fähigen Betriebssystem und von den Anwendungen benötigten Informationen zum EIM-Domänencontroller auf den Planungsarbeitsblättern festhalten. Anhand der in diesem Prozess erfassten Informationen kann der LDAP-Administrator die Bindeidentität der Anwendung bzw. des Betriebssystems auf dem LDAP-Directory-Server, auf dem sich der EIM-Domänencontroller befindet, definieren.

Der folgende Beispielabschnitt aus den Planungsarbeitsblättern zeigt die Informationen, die erfasst werden müssen. Darüber hinaus enthält er Beispielwerte, die Sie bei der Konfiguration des EIM-Domänencontrollers verwenden können.

Tabelle 12. Domänen- und Domänencontrollerdaten für das EIM-Planungsarbeitsblatt

Zur Konfiguration einer EIM-Domäne und eines EIM-Domänencontrollers erforderliche Informationen	**Beispielantworten**
Aussagefähiger Name für die Domäne. Dies kann der Name eines Unternehmens, einer Abteilung oder einer Anwendung sein, das/die die Domäne verwendet.	`MyDomain`
Optional: Wenn Sie eine EIM-Domäne in einem bereits vorhandenen LDAP-Verzeichnis konfigurieren, können Sie einen übergeordneten registrierten Namen für die Domäne angeben. Dieser registrierte Name ist ein Eintrag, der in der Hierarchie der Verzeichnisinformationen dem Domänennameneintrag direkt übergeordnet ist, z. B. `o=ibm,c=us`.	`o=ibm,c=us`
Resultierender vollständig qualifizierter DN (registrierter Name) der EIM-Domäne. Dies ist der vollständig definierte Name der EIM-Domäne, der das Verzeichnis für EIM-Domänendaten angibt. Der vollständig qualifizierte DN der Domäne beinhaltet mindestens den registrierten Namen für die Domäne (`ibm-eimDomainName=`) sowie den von Ihnen angegebenen Domänennamen.Wenn Sie einen übergeordneten DN für die Domäne festgelegt haben, beinhaltet der vollständig qualifizierte DN für die Domäne den relativen DN der Domäne (`ibm-eimDomainName=`), den Domänennamen (MyDomain) und den übergeordneten DN (`o=ibm,c=us`).	Eine der beiden folgenden Antworten (abhängig von der Auswahl eines übergeordneten registrierten Namens): • `ibm-eimDomainName=MyDomain` • `ibm-eimDomainName=MyDomain,o=ibm,c=us`
Verbindungsadresse für den Domänencontroller. Diese setzt sich aus der Art der Verbindung (Basis-LDAP oder sicheres LDAP, z. B. `ldap://` oder `ldaps://`) sowie den folgenden Informationen zusammen:	`ldap://`
• Optional: Hostname oder IP-Adresse • Optional: Portnummer	• `some.ldap.host` • `389`

Tabelle 12. Domänen- und Domänencontrollerdaten für das EIM-Planungsarbeitsblatt (Forts.)

Zur Konfiguration einer EIM-Domäne und eines EIM-Domänencontrollers erforderliche Informationen	**Beispielantworten**
Resultierende vollständige Verbindungsadresse für den Domänencontroller.	`ldap://some.ldap.host:389`
Von Anwendungen oder Systemen vorausgesetzter Bindemechanismus. Mögliche Auswahl: • Einfache Bindung • CRAM MD5 • Serverauthentifizierung • Clientauthentifizierung • Kerberos	Kerberos

Wenn das EIM-Konfigurations- und -Administrationsteam aus mehreren Teammitgliedern besteht, müssen Sie für jedes einzelne Teammitglied eine Bindeidentität einschließlich Bindemechanismus festlegen, die für den Zugriff auf die EIM-Domäne abhängig vom Aufgabenbereich verwendet werden. Darüber hinaus müssen Sie die Bindeidentität und den Bindemechanismus auch für die Endbenutzer der EIM-Anwendung definieren. Das folgende Beispielarbeitsblatt unterstützt Sie bei der Erfassung dieser Informationen.

Tabelle 13. Beispiel für ein Arbeitsblatt zur Planung von Bindeidentitäten

EIM-Berechtigung oder -Aufgabenbereich	**Bindeidentität**	**Bindemechanismus**	**Grund**
EIM-Administrator	eimadmin@krbrealm1.com	Kerberos	Konfigurieren und Verwalten von EIM
LDAP-Administrator	cn=administrator	Einfache Bindung	Konfigurieren des EIM-Domänencontrollers
Administrator für EIM-Register X	cn=admin2	CRAM MD5	Verwalten bestimmter Registerdefinitionen
EIM-Abgleichsuche	cn=MyApp,c=US	Einfache Bindung	Durchführen von Anwendungsableich-Suchoperationen

Nachdem Sie die zum Konfigurieren eines Domänencontrollers erforderlichen Informationen erfasst haben, können Sie einen Plan für den Identitätsabgleich entwickeln.

Benennungsplan für EIM-Registerdefinitionen aufstellen

Wenn Sie mit EIM eine Benutzeridentität in einem Benutzerregister mit der entsprechenden Benutzeridentität in einem anderen Benutzerregister abgleichen möchten, müssen beide Benutzerregister in EIM definiert sein. Sie müssen für jedes Benutzerregister der Anwendungen oder Betriebssysteme, das zur EIM-Domäne gehören soll, eine EIM-Registerdefinition erstellen. Benutzerregister können z. B. Betriebssystemregister wie RACF- (Resource Access Control Facility) oder i5/OS-Register, verteilte Register wie Kerberos-Register oder Untergruppen von Systemregistern darstellen, die nur von bestimmten Anwendungen benutzt werden.

Eine EIM-Domäne kann Registerdefinitionen für Benutzerregister auf einer beliebigen Plattform enthalten. Eine Domäne, die von einem Domänencontroller unter i5/OS verwaltet wird, kann beispielsweise Registerdefinitionen für Nicht-i5/OS-Plattformen (z. B. für ein AIX-Register) beinhalten. Sie können zwar alle Benutzerregister in einer EIM-Domäne definieren, es müssen jedoch Benutzerregister für die EIM-fähigen Anwendungen und Betriebssysteme definiert werden.

Für die EIM-Registerdefinition können Sie einen beliebigen Namen verwenden, vorausgesetzt, dieser ist in der EIM-Domäne eindeutig. Beispielsweise können Sie den Namen der EIM-Registerdefinition basierend auf dem Namen des Systems, auf dem sich das Benutzerregister befindet, festlegen. Sollte dies nicht ausreichen, um die Registerdefinition von ähnlichen Definitionen zu unterscheiden, können Sie den zu definierenden Benutzerregistertyp, getrennt durch einen Punkt (.) oder ein Unterstreichungszeichen (_), anhängen. Sie sollten jedoch unabhängig von den verwendeten Kriterien die Entwicklung einer Namenskonvention für die EIM-Registerdefinitionen in Betracht ziehen. Auf diese Weise gewährleisten Sie, dass innerhalb der Domäne einheitliche Definitionsnamen verwendet werden, die den Typ und die Instanz des definierten Benutzerregisters sowie dessen Verwendung angemessen beschreiben. Beispielsweise können Sie für die Namen der einzelnen Registerdefinitionen eine Kombination aus dem Namen der Anwendung bzw. des Betriebssystems, die/das das Register verwendet, und dem physischen Standort des Benutzerregisters im Unternehmen verwenden.

Eine für die Verwendung von EIM geschriebene Anwendung kann beispielsweise einen Aliasnamen für das Quellenregister und/oder einen Aliasnamen für das Zielregister angeben. Prüfen Sie bei der Erstellung von EIM-Registerdefinitionen in der Dokumentation für die Anwendungen, ob Sie einen oder mehrere Aliasnamen für die Registerdefinitionen festlegen müssen. Wenn Sie diese Aliasnamen den entsprechenden Registerdefinitionen zuordnen, kann die Anwendung eine Aliasnamensuche durchführen, um die EIM-Registerdefinition(en) zu ermitteln, die mit den Aliasnamen in der Anwendung übereinstimmen.

Der folgende Beispielsabschnitt des Planungsarbeitsblatts unterstützt Sie bei der Erfassung von Informationen über teilnehmende Benutzerregister. Verwenden Sie das eigentliche Arbeitsblatt, um einen Registerdefinitionsnamen für jedes Benutzerregister und gegebenenfalls Aliasnamen anzugeben. Sie können im Arbeitsblatt auch den Standort und die Verwendung des Benutzerregisters beschreiben. Die Installations- und Konfigurationsdokumentation der Anwendung enthält einen Teil der auf dem Arbeitsblatt benötigten Daten.

Tabelle 14. Beispiel für ein Planungsarbeitsblatt für EIM-Registerdefinitionsdaten

Name der Registerdefinition	**Typ des Benutzerregisters**	**Aliasname der Registerdefinition**	**Registerbeschreibung**
System_C	i5/OS-Systembenutzerregister	Siehe Anwendungsdokumentation	Hauptsystembenutzerregister für i5/OS auf System C
System_A_WAS	WebSphere LTPA	app_23_alias_source	Benutzerregister für WebSphere LTPA auf System A
System_B	Linux	Siehe Anwendungsdokumentation	Benutzerregister für Linux auf System B
System_A	i5/OS-Systembenutzerregister	app_23_alias_target app_xx_alias_target	Hauptsystembenutzerregister für i5/OS auf System A
System_D	Kerberos-Benutzerregister	app_xx_alias_source	Kerberos-Realm legal.mydomain.com
System_4	Windows 2000-Benutzerregister	Siehe Anwendungsdokumentation	Benutzerregister der Anwendung für Personalwesen auf System 4

Anmerkung: Zuordnungstypen für die einzelnen Register werden zu einem späteren Zeitpunkt im Planungsprozess festgelegt.

Nachdem Sie diesen Abschnitt des Planungsarbeitsblatts ausgefüllt haben, sollten Sie den Plan für den Identitätsabgleich entwickeln, um festzulegen, ob Kennungszuordnungen und/oder Richtlinienzuordnungen zur Erstellung der Abgleiche, die Sie für die Benutzeridentitäten in jedem definierten Benutzerregister benötigen, verwendet werden sollen.

Plan für Identitätsabgleich entwickeln

Ein wichtiger Bestandteil des Planungsprozesses für die EIM-Implementierung (Enterprise Identity Mapping) besteht darin, dass Sie festlegen, wie Sie den Identitätsabgleich in Ihrem Unternehmen durchführen möchten. Es gibt zwei Methoden für den Identitätsabgleich in EIM:

- **Kennungszuordnungen** beschreiben Beziehungen zwischen einer EIM-Kennung und den Benutzeridentitäten in Benutzerregistern, die diese Person repräsentieren. Eine Kennungszuordnung erstellt einen direkten 1:1-Abgleich zwischen einer EIM-Kennung und einer bestimmten Benutzeridentität. Sie können Kennungszuordnungen verwenden, um über die EIM-Kennung indirekt eine Beziehung zwischen Benutzeridentitäten zu definieren.

  Wenn die Sicherheitsrichtlinie genau spezifizierte Berechtigungen vorschreibt, müssen Sie für die Implementierung des Identitätsabgleichs fast ausschließlich Kennungszuordnungen verwenden. Da Sie zur Erstellung von 1:1-Abgleichen für die Benutzeridentitäten der Benutzer Identitätszuordnungen verwenden, können Sie immer genau nachvollziehen, wer eine Aktion für ein Objekt oder das System ausgeführt hat.
- **Richtlinienzuordnungen** beschreiben eine Beziehung zwischen mehreren Benutzeridentitäten und einer einzelnen Benutzeridentität in einem Benutzerregister. Richtlinienzuordnungen verwenden die Unterstützung von EIM-Abgleichrichtlinien, um n:1-Abgleiche zwischen Benutzeridentitäten ohne Einbeziehung von EIM-Kennungen zu erstellen.

  Richtlinienzuordnungen sind dann hilfreich, wenn eine oder mehrere große Benutzergruppen auf Systeme oder Anwendungen in Ihrem Unternehmen zugreifen müssen, Sie Sie aber den einzelnen Benutzern für die Zugriffsberechtigung keine spezifischen Benutzeridentitäten zuordnen möchten. Beispiel: Sie verwalten eine Webanwendung, die auf eine bestimmte interne Anwendung zugreift. Sie möchten nicht Hunderte oder Tausende von Benutzeridentitäten erstellen, um Benutzer für diese interne Anwendung zu authentifizieren. In dieser Situation können Sie den Identitätsabgleich so konfigurieren, dass alle Benutzer die Webanwendung mit einer einzigen Benutzeridentität auf der zur Ausführung der Anwendung niedrigstmöglichen Berechtigungsstufe abgeglichen werden. Diese Art von Identitätsabgleich können Sie mit Richtlinienzuordnungen durchführen.

Sie könnten der Meinung sein, dass Kennungszuordnungen für Ihr Unternehmen die beste Methode zur Steuerung der Benutzeridentitäten und für die optimale Kennwortverwaltung sind. Alternativ dazu können Sie zur Optimierung der Einzelanmeldung Richtlinienzuordnungen und Kennungszuordnungen kombinieren und für Administratoren spezifische Benutzeridentitäten anlegen. Unabhängig davon, welche Art des Identitätsabgleichs am besten Ihren Geschäftsanforderungen entspricht und zu Ihrer Sicherheitsrichtlinie passt, müssen Sie einen Plan für den Identitätsabgleich erstellen, um sicherzustellen, dass Sie den Identitätsabgleich entsprechend implementieren.

Führen Sie folgende Tasks aus, um einen Plan für den Identitätsabgleich zu erstellen:

Zugehörige Konzepte

„Zuordnungen erstellen" auf Seite 112

EIM-Zuordnungen planen: Bei Zuordnungen handelt es sich um Einträge, die Sie in einer EIM-Domäne erstellen, um eine Beziehung zwischen Benutzeridentitäten in verschiedenen Benutzerregistern zu definieren. Sie können zwei Zuordnungstypen in EIM erstellen: Kennungszuordnungen zur Definition von 1:1-Abgleichen und Richtlinienzuordnungen zur Definition von n:1-Abgleichen. Sie können Richtlinienzuordnungen an Stelle von oder in Verbindung mit Kennungszuordnungen verwenden.

Für welche Zuordnungstypen Sie sich entscheiden, hängt von der Verwendung einer bestimmten Benutzeridentität durch einen Benutzer sowie von Ihrem Plan für den Identitätsabgleich ab.

Sie können folgende Typen von Kennungszuordnungen erstellen:

- **Zielzuordnungen**

  Sie definieren Zielzuordnungen für Benutzer, die normalerweise nur von einem anderen Clientsystem auf dieses System zugreifen, um es als Server zu nutzen. Dieser Zuordnungstyp wird verwendet, wenn eine Anwendung Abgleichsuchoperationen ausführt.

- **Quellenzuordnungen**

  Sie definieren Quellenzuordnungen, wenn die Benutzeridentität die erste Identität ist, mit der sich ein Benutzer am System oder am Netzwerk anmeldet. Dieser Zuordnungstyp wird verwendet, wenn eine Anwendung Abgleichsuchoperationen ausführt.
- **Administrative Zuordnungen**

  Sie definieren administrative Zuordnungen, wenn protokolliert werden soll, dass die Benutzeridentität mit einem bestimmten Benutzer verknüpft ist, aber nicht für Abgleichsuchoperationen zur Verfügung steht. Sie können diesen Zuordnungstyp verwenden, um alle Benutzeridentitäten, die eine Person im Unternehmen verwendet, zu überwachen.

Eine **Richtlinienzuordnung** definiert immer eine Zielzuordnung.

Eine einzige Registerdefinition kann je nach Verwendung des Benutzerregisters, auf das sie verweist, mehrere Zuordnungstypen besitzen. Es bestehen zwar keine Begrenzungen hinsichtlich der Anzahl oder der Kombination der Zuordnungen, die Sie definieren können, Sie sollten die Anzahl jedoch auf ein Minimum beschränken, um die Verwaltung der EIM-Domäne zu vereinfachen.

Normalerweise zeigt eine Anwendung an, welche Registerdefinitionen sie für Quellen- und Zielregister erwartet. Die Zuordnungstypen sind jedoch nicht angegeben. Jeder Endbenutzer der Anwendung muss mit der Anwendung über mindestens eine Zuordnung abgeglichen werden. Diese Zuordnung kann ein 1:1-Abgleich zwischen der eindeutigen EIM-Kennung und einer Benutzeridentität im erforderlichen Zielregister oder ein n:1-Abgleich zwischen einem Quellenregister, zu dem die Benutzeridentität gehört, und dem erforderlichen Zielregister sein. Welchen Zuordnungstyp Sie verwenden, hängt von den Voraussetzungen für den Identitätsabgleich und den von der Anwendung zur Verfügung gestellten Kriterien ab.

Im Rahmen des Planungsprozesses haben Sie bereits zwei Planungsarbeitsblätter für die Benutzeridentitäten in Ihrem Unternehmen mit Informationen über die benötigten EIM-Kennungen und EIM-Registerdefinitionen ausgefüllt. Nun müssen Sie diese Informationen kombinieren, indem Sie die Zuordnungstypen festlegen, die Sie zum Abgleichen der Benutzeridentitäten in Ihrem Unternehmen verwenden möchten. Sie müssen festlegen, ob eine Richtlinienzuordnung für eine bestimmte Anwendung und deren Benutzerregister bzw. bestimmte Kennungszuordnungen (Quellen-, Ziel- oder administrative Zuordnung) für jede Benutzeridentität im System- oder Anwendungsregister definiert werden sollen. Zu diesem Zweck können Sie Informationen zu den erforderlichen Zuordnungstypen sowohl im Planungsarbeitsblatt für die Registerdefinition als auch in den entsprechenden Zeilen der Arbeitsblätter für die einzelnen Zuordnungen festhalten.

Bei der Erstellung Ihres Plans für den Identitätsabgleich können Sie die folgenden Beispielarbeitsblätter als Leitfaden benutzen, um die dazu erforderlichen Zuordnungsinformationen aufzuzeichnen.

Tabelle 15. Beispiel für ein Planungsarbeitsblatt für EIM-Registerdefinitionsdaten

Name der Registerdefinition	Typ des Benutzerregisters	Aliasname der Registerdefinition	Registerbeschreibung	Zuordnungstypen
System_C	i5/OS-Systembenutzerregister	Siehe Anwendungsdokumentation	Hauptsystembenutzerregister für i5/OS auf System C	Ziel
System_A_WAS	WebSphere LTPA	app_23_alias_source	Benutzerregister für WebSphere LTPA auf System A	Bevorzugt Quelle
System_B	Linux	Siehe Anwendungsdokumentation	Benutzerregister für Linux auf System B	Quelle und Ziel
System_A	i5/OS-Systembenutzerregister	app_23_alias_target app_xx_alias_target	Hauptsystembenutzerregister für i5/OS auf System A	Ziel

Tabelle 15. Beispiel für ein Planungsarbeitsblatt für EIM-Registerdefinitionsdaten (Forts.)

Name der Register-definition	Typ des Benutzer-registers	Aliasname der Registerdefinition	Registerbeschreibung	Zuordnungstypen
System_D	Kerberos-Benutzer-register	app_xx_alias_source	Kerberos-Realm legal.mydomain.com	Quelle
System_4	Windows 2000-Benutzerregister	Siehe Anwendungs-dokumentation	Benutzerregister der Anwendung für Personalwesen auf System 4	Administrativ
order.mydomain.com	Windows 2000-Benutzerregister		Hauptanmelderegister für Mitarbeiter der Auftragsannahme	Standardrichtlinie für Register (Quellen-register)
System_A_order_app	Anwendung der Auftragsannahme		Anwendungs-spezifisches Register für Auftrags-aktualisierungen	Standardrichtlinie für Register (Zielregister)
System_C_order_app	Anwendung der Auftragsannahme		Anwendungs-spezifisches Register für Auftrags-aktualisierungen	Standardrichtlinie für Register (Zielregister)

Tabelle 16. Planungsarbeitsblatt für EIM-Kennungen (Beispiel)

Eindeutiger Kennungsname	Beschreibung der Kennung oder der Benutzeridentität	Aliasname der Kennung
John S Day	Manager der Personalabteilung	app_23_admin
John J Day	Rechtsabteilung	app_xx_admin
Sharon A. Jones	Administrator der Auftragsannahme	

Tabelle 17. Planungsarbeitsblatt für Kennungszuordnung (Beispiel)

Eindeutiger Kennungsname: _____John S Day_____		
Benutzerregister	**Benutzeridentität**	**Zuordnungstypen**
System A WAS auf System A	johnday	Quelle
Linux auf System B	jsd1	Quelle und Ziel
i5/OS auf System C	JOHND	Ziel
Register 4 auf Windows 2000-System für Personalwesen	JDAY	Administrativ

Tabelle 18. Planungsarbeitsblatt für Richtlinienzuordnungen (Beispiel)

Typ der Richtlinien-zuordnung	Benutzerregister (Quelle)	Benutzerregister (Ziel)	Benutzeridentität	Beschreibung
Standardregister	order.mydomain.com	System_A_order_app	SYSUSERA	Gleicht einen authen-tifizierten Benutzer der Auftragsannahme (Windows) mit der entsprechenden Anwendungs-benutzeridentität ab.

Tabelle 18. Planungsarbeitsblatt für Richtlinienzuordnungen (Beispiel) (Forts.)

Typ der Richtlinien-zuordnung	Benutzerregister (Quelle)	Benutzerregister (Ziel)	Benutzeridentität	Beschreibung
Standardregister	order.mydomain.com	System_C_order_app	SYSUSERB	Gleicht einen authentifizierten Benutzer der Auftragsannahme (Windows) mit der entsprechenden Anwendungs-benutzeridentität ab.

Benennungsplan für EIM-Kennungen entwickeln: Bei der Planung der Anforderungen für Ihren EIM-Identitätsabgleich können Sie eindeutige EIM-Kennungen für die Benutzer von EIM-fähigen Anwendungen und Betriebssystemen in Ihrem Unternehmen erstellen, um für einen Benutzer 1:1-Zuordnungen zwischen Benutzeridentitäten herzustellen. Indem Sie Kennungszuordnungen zur Erstellung von 1:1-Abgleichen verwenden, können Sie die Vorteile der von EIM zur Verfügung gestellten Kennwortverwaltung besser nutzen.

Der von Ihnen entwickelte Benennungsplan ist abhängig von Ihren Geschäftsanforderungen und Vorgaben; die einzige Voraussetzung für EIM-Kennungsnamen besteht darin, dass die Namen eindeutig sein müssen. Manche Unternehmen verwenden den vollständigen, rechtsgültigen Namen einer Person; andere verwenden einen anderen Datentyp wie z. B. die Personalnummer der betreffenden Person. Wenn Sie EIM-Kennungsnamen auf der Basis des vollständigen Namens einer Person erstellen möchten, laufen Sie Gefahr, dass Namen doppelt vorhanden sind. Die Frage, wie Sie potenziell doppelte Kennungsnamen handhaben, hängt von Ihren persönlichen Präferenzen ab. Sie können jeden Fall manuell bearbeiten, indem Sie jedem Kennungsnamen eine vordefinierte Zeichenfolge hinzufügen, um Eindeutigkeit zu gewährleisten. Beispielsweise können Sie die Abteilungsnummer der entsprechenden Person hinzufügen.

Im Rahmen der Entwicklung eines Benennungsplans müssen Sie Entscheidungen für Ihren allgemeinen Plan für den Identitätsabgleich treffen. Sie müssen entscheiden, wann Sie Kennungen und Kennungszuordnungen bzw. Richtlinienzuordnungen für den Identitätsabgleich in Ihrem Unternehmen verwenden müssen. Für den Benennungsplan für EIM-Kennungen können Sie das Arbeitsblatt unten verwenden. Dieses Arbeitsblatt vereinfacht die Erfassung von Informationen zu den Benutzeridentitäten in Ihrem Unternehmen sowie die Planung von EIM-Kennungen für diese Benutzeridentitäten. Das Arbeitsblatt beinhaltet Informationen, die der EIM-Administrator benötigt, wenn er EIM-Kennungen oder Richtlinienzuordnungen für die Benutzer einer Anwendung erstellt.

Tabelle 19. Planungsarbeitsblatt für EIM-Kennungen (Beispiel)

Eindeutiger Kennungsname	Beschreibung der Kennung oder der Benutzeridentität	Aliasname der Kennung
John S Day	Manager der Personalabteilung	app_23_admin
John J Day	Rechtsabteilung	app_xx_admin
Sharon A. Jones	Administrator der Auftragsannahme	

Eine für die Verwendung von EIM geschriebene Anwendung kann einen Aliasnamen angeben, um die entsprechende EIM-Kennung für die Anwendung zu suchen. Die Anwendung wiederum stellt anhand dieses Aliasnamens die zu verwendende Benutzeridentität fest. Lesen Sie in der Dokumentation für die Anwendungen nach, ob Sie einen oder mehrere Aliasnamen für die Kennung festlegen müssen. Die Felder für die Beschreibung der EIM-Kennung oder der Benutzeridentität sind unformatiert, d. h., Sie können eine Beschreibung des Benutzers eingeben.

Sie müssen nicht für alle Mitarbeiter gleichzeitig EIM-Kennungen erstellen. Nachdem Sie die erste EIM-Kennung erstellt und mit dieser die EIM-Konfiguration getestet haben, können Sie weitere EIM-Kennun-

gen basierend auf den Unternehmenszielen im Hinblick auf die EIM-Nutzung erstellen. Sie haben beispielsweise die Möglichkeit, auf der Ebene von Abteilungen oder Unternehmensbereichen EIM-Kennungen hinzuzufügen. Sie können EIM-Kennungen jedoch auch bei der Einrichtung zusätzlicher EIM-Anwendungen hinzufügen.

Nachdem Sie die Informationen zum Erstellen eines Benennungsplans für EIM-Kennungen erfasst haben, können Sie für die Benutzeridentitäten Zuordnungen planen.

Planungsarbeitsblätter für EIM-Implementierung

Die folgenden Arbeitsblätter unterstützen Sie während des EIM-Planungsprozesses bei der Erfassung von Informationen, die Sie für die Konfiguration und Verwendung von EIM in Ihrem Unternehmen benötigen. Auf den Planungsseiten werden bei Bedarf ausgefüllte Beispielabschnitte der Arbeitsblätter abgebildet.

Diese Arbeitsblätter dienen als Beispiel für die Art von Arbeitsblättern, die Sie zur Erstellung eines eigenen EIM-Implementierungsplans benötigen. Die Anzahl der dargestellten Einträge ist geringer als die vermutlich für Ihre EIM-Daten benötigte Eintragszahl. Bearbeiten Sie die Arbeitsblätter, um sie an Ihre Situation anzupassen.

Tabelle 20. Arbeitsblatt für die Domänen- und Domänencontrollerdaten

Zur Konfiguration einer EIM-Domäne und eines EIM-Domänencontrollers erforderliche Informationen	**Antworten**
Aussagefähiger Name für die Domäne. Dies kann der Name eines Unternehmens, einer Abteilung oder einer Anwendung sein, das/die die Domäne verwendet.	
Optional: Ein übergeordneter registrierter Name (DN) für die Domäne. Dieser registrierte Name ist ein Eintrag, der in der Hierarchie der Verzeichnisinformationen dem Domänennameneintrag direkt übergeordnet ist, z. B. `o=ibm,c=us`.	
Resultierender, vollständig qualifizierter und registrierter Name (DN) der EIM-Domäne. Dies ist der vollständig definierte EIM-Domänenname, der das Verzeichnis für EIM-Domänendaten angibt. Der vollständig qualifizierte registrierte Name der Domäne beinhaltet mindestens den registrierten Namen für die Domäne (`ibm-eimDomainName=`) sowie den von Ihnen angegebenen Domänennamen. Wenn Sie einen übergeordneten registrierten Namen für die Domäne festgelegt haben, beinhaltet der vollständig qualifizierte registrierte Name der Domäne den relativen registrierten Namen der Domäne (`ibm-eimDomainName=`), den Domänennamen (MyDomain) und den übergeordneten registrierten Namen (`o=ibm,c=us`).	
Verbindungsadresse für den Domänencontroller. Diese setzt sich aus der Art der Verbindung (Basis-LDAP oder sicheres LDAP, z. B. `ldap://` oder `ldaps://`) sowie den folgenden Informationen zusammen:	
• Optional: Hostname oder IP-Adresse • Optional: Portnummer	
Resultierende vollständige Verbindungsadresse für den Domänencontroller.	

Tabelle 20. Arbeitsblatt für die Domänen- und Domänencontrollerdaten (Forts.)

Von Anwendungen oder Systemen vorausgesetzter Bindemechanismus. Mögliche Auswahl: • Einfache Bindung • CRAM MD5 • Serverauthentifizierung • Clientauthentifizierung • Kerberos	

Ein Beispiel für die Verwendung dieses Arbeitsblatts finden Sie unter EIM-Domänencontroller planen.

Tabelle 21. Planungsarbeitsblatt für Bindeidentitäten

EIM-Berechtigung oder -Aufgabenbereich	**Bindeidentität**	**Bindemechanismus**	**Grund**

Ein Beispiel für die Verwendung dieses Arbeitsblatts finden Sie unter EIM-Domänencontroller planen.

Tabelle 22. Planungsarbeitsblatt für EIM-Registerdefinitionsdaten

Name der Registerdefinition	**Typ des Benutzerregisters**	**Aliasname der Registerdefinition**	**Registerbeschreibung**	**Zuordnungstypen**

Ein Beispiel für die Verwendung dieses Arbeitsblatts finden Sie unter Benennungsplan für EIM-Registerdefinitionen entwickeln.

Tabelle 23. Planungsarbeitsblatt für EIM-Kennungen

Eindeutiger Kennungsname	**Beschreibung der Kennung oder der Benutzeridentität**	**Aliasname der Kennung**

Ein Beispiel für die Verwendung dieses Arbeitsblatts finden Sie unter Benennungsplan für EIM-Registerdefinitionen entwickeln.

Tabelle 24. Planungsarbeitsblatt für Kennungszuordnungen

Eindeutiger Kennungsname: _____John S Day_____		
Benutzerregister	Benutzeridentität	Zuordnungstypen

Ein Beispiel für die Verwendung dieses Arbeitsblatts finden Sie unter EIM-Zuordnungen planen.

Tabelle 25. Planungsarbeitsblatt für Richtlinienzuordnungen

Typ der Richtlinien-zuordnung	Benutzerregister (Quelle)	Benutzerregister (Ziel)	Benutzeridentität	Beschreibung

Ein Beispiel für die Verwendung dieses Arbeitsblatts finden Sie unter EIM-Zuordnungen planen.

EIM-Anwendungsentwicklung planen

Damit eine Anwendung EIM nutzen und einer Domäne hinzugefügt werden kann, muss diese Anwendung in der Lage sein, die EIM-APIs zu verwenden. Prüfen Sie in der Dokumentation zu den EIM-APIs sowie in der plattformspezifischen EIM-Dokumentation, ob Sie beim Schreiben oder Anpassen von Anwendungen für die Verwendung von EIM-APIs spezielle Planungsaspekte berücksichtigen müssen. Beispiel: Bei C- oder C++-Anwendungen, die die EIM-APIs aufrufen, müssen gegebenenfalls Kompilie-

rungsaspekte oder andere Aspekte berücksichtigt werden. Abhängig von der Anwendungsplattform kann es erforderlich sein, die Herstellung von Programmverbindungen oder Ähnliches zu berücksichtigen.

EIM für i5/OS planen

Es gibt mehrere Technologien und Services, die Enterprise Identity Mapping (EIM) auf dem iSeries-Server bereitstellt. Vor der EIM-Konfiguration auf dem Server müssen Sie festlegen, welche Leistungsmerkmale mit EIM und Einzelanmeldungsfunktionen implementiert werden sollen.

Vor der Implementierung von EIM müssen Sie grundlegende Sicherheitsmaßnahmen für Ihr Netzwerk festlegen und implementieren. EIM ermöglicht Administratoren und Benutzern eine einfachere Identitätsverwaltung im Unternehmen. Beim gemeinsamen Einsatz mit dem Netzwerkauthentifizierungsservice stellt EIM Einzelanmeldungsfunktionen für Ihr Unternehmen zur Verfügung.

Wenn Sie planen, Benutzer im Rahmen einer Einzelanmeldungsimplementierung zu authentifizieren, müssen Sie auch den Netzwerkauthentifizierungsservice konfigurieren. Informationen zur Planung des Netzwerkauthentifizierungsservice enthält der Abschnitt Netzwerkauthentifizierungsservice planen, Informationen zur Planung einer Einzelanmeldungsumgebung enthält der Abschnitt Planung.

In den folgenden Abschnitten finden Sie weitere Informationen zur Planung Ihrer EIM-Konfiguration auf der iSeries:

EIM-Installationsvoraussetzungen für iSeries

Im folgenden Planungsarbeitsblatt sind die Services aufgelistet, die Sie vor der Konfiguration von EIM installieren müssen.

Tabelle 26. Planungsarbeitsblatt für EIM-Installation

Planungsarbeitsblatt für EIM-Voraussetzungen	**Antworten**
Arbeiten Sie mit der Betriebssystemversion V5R4 (5722-SS1)?	
Sind die folgenden Optionen und Lizenzprogramme auf der iSeries™ installiert? • i5/OS Host-Server (5722-SS1 Option 12) • iSeries Access für Windows® (5722-XE1) • Qshell Interpreter (5722-SS1 Option 30) - Erforderlich zur Konfiguration von Netzwerkauthentifizierungsservice und EIM	
Ist der iSeries Navigator einschließlich der folgenden Unterkomponenten auf dem Administrator-PC installiert? • Sicherheit - Erforderlich, wenn Sie den Netzwerkauthentifizierungsservice und EIM konfigurieren möchten. • Netzwerk	
Ist das aktuellste Service-Pack für iSeries Access für Windows installiert? Sie können das aktuellste Service-Pack über die Website von iSeries Access  abrufen.	
Wenn ein Directory-Server, z. B. der IBM Directory Server for iSeries (LDAP), gegenwärtig konfiguriert ist und als EIM-Domänencontroller verwendet werden soll: Sind der registrierte Name (DN) und das Kennwort des LDAP-Administrators bekannt?	
Kann ein konfigurierter Directory-Server vorübergehend gestoppt werden? (Dies ist erforderlich, um die EIM-Konfiguration durchzuführen.)	
Besitzen Sie die Sonderberechtigungen *SECADM, *ALLOBJ und *IOSYSCFG?	
Wurden die aktuellsten vorläufigen Programmkorrekturen (PTFs) angelegt?	

Erforderliche iSeries Navigator-Optionen installieren

Wenn Sie eine Einzelanmeldungsumgebung mit EIM (Enterprise Identity Mapping) und dem Netzwerkauthentifizierungsservice aktivieren möchten, müssen Sie die Option **Netzwerk** und die Option **Sicherheit** des iSeries Navigator installieren. EIM gehört zur Option **Netzwerk**, der Netzwerkauthentifizierungsservice zur Option **Sicherheit**. Wenn der Netzwerkauthentifizierungsservice in Ihrem Netzwerk nicht verwendet werden soll, ist es nicht erforderlich, die Option **Sicherheit** des iSeries Navigator zu installieren.

Wenn Sie die Option "Netzwerk" des iSeries Navigator installieren bzw. überprüfen möchten, ob diese Option installiert ist, vergewissern Sie sich, dass iSeries Access für Windows auf dem PC installiert ist, den Sie für die Verwaltung des iSeries-Servers verwenden.

Gehen Sie wie folgt vor, um die Option **Netzwerk** zu installieren:

1. Klicken Sie auf **Start > Programme > IBM iSeries Access für Windows > Selektive Installation**.
2. Folgen Sie den Anweisungen im Dialogfenster. Erweitern Sie im Dialogfenster **Komponentenauswahl** den Eintrag **iSeries Navigator**, und wählen Sie dann die Option **Netzwerk** aus. Wenn Sie planen, den Netzwerkauthentifizierungsservice zu verwenden, müssen Sie auch die Option **Sicherheit** auswählen.
3. Führen Sie die restlichen Schritte der **selektiven Installation** durch.

Hinweise zur Sicherung und Wiederherstellung für EIM

Sie müssen einen Sicherungs- und Wiederherstellungsplan für Ihre EIM-Daten (Enterprise Identity Mapping) entwickeln, um sicherzustellen, dass die Daten geschützt sind und wiederhergestellt werden können, wenn ein Problem mit dem Directory-Server, auf dem der EIM-Domänencontroller sich befindet, auftritt. Außerdem müssen Sie in der Lage sein, wichtige EIM-Konfigurationsdaten wiederherzustellen.

Sicherung und Wiederherstellung von EIM-Domänendaten:

Wie Sie die EIM-Daten sichern, hängt davon ab, wie der Bereich des Directory-Servers, der als Domänencontroller für Ihre EIM-Daten fungiert, verwaltet werden soll.

Eine Methode der Datensicherung, insbesondere im Hinblick auf die Wiederherstellung nach einem Katastrophenfall, besteht im Sicher der Datenbankbibliothek. Die Standardbibliothek ist `QUSRDIRDB`. Wenn `changelog` aktiviert ist, müssen Sie auch die Bibliothek `QUSRDIRCL` sichern. Der Directory-Server auf dem System, auf dem Sie die Bibliothek wiederherstellen möchten, muss dasselbe LDAP-Schema und dieselbe Konfiguration besitzen wie der ursprüngliche Directory-Server. Die Dateien, in denen diese Daten gespeichert sind, befinden sich im Verzeichnis `/QIBM/UserData/OS400/DirSrv`. Weitere Konfigurationsdaten sind in den Verzeichnissen `QUSRSYS/QGLDCFG` (Objekt `*USRSPC`) und `QUSRSYS/QGLDVLDL` (Objekt `*VLDL`) gespeichert. Wenn Sie eine komplette Sicherung des gesamten Inhalts Ihres Directory-Servers durchführen möchten, müssen Sie beide Bibliotheken, die Dateien des Integrated File System sowie die `QUSRSYS`-Objekte sichern.

Weitere Informationen zur Sicherung und Wiederherstellung der wichtigsten Directory-Server-Daten finden Sie unter Save and restore Directory Server information im Abschnitt IBM Directory Server for iSeries (LDAP) des Information Center.

Sie können beispielsweise eine LDIF-Datei verwenden, um den Directory-Server-Inhalt ganz oder teilweise zu sichern. Wenn Sie die Domänendaten für einen IBM Directory Server for iSeries-Domänencontroller sichern möchten, müssen Sie die folgenden Schritte durchführen:

1. Erweitern Sie im iSeries Navigator den Eintrag **Netzwerk > Server > TCP/IP**.
2. Klicken Sie mit der rechten Maustaste auf **IBM Directory Server**, wählen Sie **Tools** und anschließend **Datei exportieren** aus, um eine Seite anzuzeigen, auf der Sie angeben können, welche Teile des Directory-Server-Inhalts in eine Datei exportiert werden sollen.

3. Übertragen Sie die Exportdatei auf den iSeries-Server, den Sie als Backup-Directory-Server verwenden möchten.
4. Erweitern Sie im iSeries Navigator auf dem Sicherungsserver den Eintrag **Netzwerk > Server > TCP/IP**.
5. Klicken Sie mit der rechten Maustaste auf **IBM Directory Server**, wählen Sie **Tools** und anschließend **Importieren** aus, um den Inhalt der übertragenen Datei auf dem neuen Directory-Server abzulegen.

Eine weitere Methode zur Sicherung der EIM-Domänendaten bietet ein Replikations-Directory-Server. Alle Änderungen an EIM-Domänendaten werden automatisch an den Replikations-Directory-Server weitergeleitet. Wenn der Directory-Server, auf dem sich der Domänencontroller befindet, ausfällt oder EIM-Daten verliert, können Sie die Daten vom Replikationsserver abrufen.

Konfiguration und Verwendung eines Replikations-Directory-Servers sind vom Typ des verwendeten Replikationsmodells abhängig. Weitere Informationen zur Replikation sowie zur Konfiguration des Replikations-Directory-Servers enthalten die Abschnitte Replication und Manage replication im Thema IBM Directory Server for iSeries (LDAP) des Information Centers.

Sicherung und Wiederherstellung von EIM-Konfigurationsdaten:

Sollte Ihr System ausfallen, müssen Sie die EIM-Konfigurationsdaten für dieses System wiederherstellen. Die systemübergreifende Sicherung und Wiederherstellung dieser Daten ist ein komplexer Vorgang.

Für die Sicherung und Wiederherstellung der EIM-Konfiguration sind die folgenden Optionen verfügbar:

- Führen Sie auf jedem System Befehl SAVSECDTA (Sicherheitsdaten sichern) aus, um EIM-Daten und andere wichtige Konfigurationsdaten zu sichern. Stellen Sie dann auf jedem System das Benutzerprofil QSYS wieder her.

  Anmerkung: Auf jedem System mit einer EIM-Konfiguration müssen Sie einzeln den Befehl SASECDTA ausführen und das Benutzerprofilobjekt QSYS wiederherstellen. Möglicherweise treten Probleme auf, wenn Sie versuchen, das Benutzerprofilobjekt auf einem System wiederherzustellen, auf dem es nicht gespeichert wurde.
- Führen Sie den EIM-Konfigurationsassistenten erneut aus, oder aktualisieren Sie die Eigenschaften des EIM-Konfigurationsordners manuell. Zur Vereinfachung dieses Vorgangs empfiehlt es sich, die Planungsarbeitsblätter für die EIM-Implementierung zu speichern oder die EIM-Konfigurationsdaten der einzelnen Systeme aufzuzeichnen.

Darüber hinaus müssen Sie berücksichtigen und planen, wie Sie die Daten des Netzwerkauthentifizierungsservice sichern und wiederherstellen möchten, wenn Sie den Netzwerkauthentifizierungsservice als Bestandteil einer Einzelanmeldungsumgebung konfiguriert haben.

Enterprise Identity Mapping konfigurieren

Im Folgenden wird erläutert, wie Sie den EIM-Konfigurationsassistenten (EIM = Enterprise Identity Mapping) zum Konfigurieren von EIM für Ihre iSeries-Server verwenden können.

Der EIM-Konfigurationsassistent ermöglicht Ihnen die schnelle und einfache Durchführung der EIM-Basiskonfiguration für Ihre iSeries. Der Assistent stellt Ihnen drei Optionen für die EIM-Systemkonfiguration zur Verfügung. Wie Sie den Assistenten einsetzen, um EIM auf einem bestimmten System zu konfigurieren, richtet sich danach, wie Sie generell den Einsatz von EIM in Ihrem Unternehmen geplant haben und welche Ansprüche Ihre EIM-Konfiguration erfüllen soll. So möchten beispielsweise viele Administratoren EIM in Verbindung mit dem Netzwerkauthentifizierungsservice verwenden, um eine Umgebung für die Einzelanmeldung für mehrere Systeme und Plattformen zu erstellen, ohne die zugrunde liegenden Sicherheitsrichtlinien ändern zu müssen. Der EIM-Konfigurationsassistent bietet Ihnen daher die Möglichkeit, den Netzwerkauthentifizierungsservice als Bestandteil Ihrer EIM-Konfigura-

tion zu konfigurieren. Konfiguration und Verwendung des Netzwerkauthentifizierungsservice sind jedoch für die Konfiguration und Verwendung von EIM nicht erforderlich.

Bevor Sie mit der Konfiguration von EIM für ein oder mehrere Systeme beginnen, planen Sie Ihre EIM-Implementierung, um alle erforderlichen Informationen zusammenzustellen. Sie müssen beispielsweise folgende Entscheidungen treffen:

- Welcher iSeries-Server soll als EIM-Domänencontroller für die EIM-Domäne konfiguriert werden? Erstellen Sie mit dem EIM-Konfigurationsassistenten zuerst eine neue Domäne auf diesem System und konfigurieren Sie anschließend alle weiteren iSeries-Server, um sie dieser Domäne hinzuzufügen.
- Soll der Netzwerkauthentifizierungsservice auf jedem System konfiguriert werden, das für EIM konfiguriert wird? Wenn dies der Fall ist, können Sie mit dem EIM-Konfigurationsassistenten auf jedem iSeries-Server eine Basiskonfiguration des Netzwerkauthentifizierungsservice erstellen. Sie müssen jedoch noch weitere Tasks ausführen, um die Konfiguration des Netzwerkauthentifizierungsservice abzuschließen.

Nachdem Sie mit dem EIM-Konfigurationsassistenten für jeden iSeries-Server eine Basiskonfiguration erstellt haben, müssen Sie noch eine Reihe weiterer EIM-Konfigurations-Tasks ausführen. Das Szenario: Einzelanmeldung für i5/OS aktivieren enthält ein Beispiel, das verdeutlicht, wie ein fiktives Unternehmen eine Einzelanmeldungsumgebung unter Verwendung des Netzwerkauthentifizierungsservice und EIM konfiguriert hat.

Um EIM konfigurieren zu können, benötigen Sie die folgenden Sonderberechtigungen:

- Sicherheitsadministrator (*SECADM)
- Berechtigung für alle Objekte (*ALLOBJ)
- Systemkonfiguration (*IOSYSCFG)

Bevor Sie den EIM-Konfigurationsassistenten starten, sollten Sie alle Schritte unter „Enterprise Identity Mapping planen" auf Seite 56 ausgeführt haben, damit genau festgelegt ist, wie EIM eingesetzt werden soll. Wenn Sie EIM bei der Erstellung einer Einzelanmeldungsumgebung konfigurieren, sollten Sie außerdem alle Schritte zur Planung der Einzelanmeldung durchführen.

Führen Sie die folgenden Schritte durch, um auf den EIM-Konfigurationsassistenten zuzugreifen:

1. Starten Sie den iSeries Navigator.
2. Melden Sie sich bei dem iSeries-Server an, für den EIM konfiguriert werden soll. Wenn Sie EIM für mehrere iSeries-Server konfigurieren möchten, fangen Sie mit dem Server an, auf dem der EIM-Domänencontroller konfiguriert werden soll.
3. Erweitern Sie **Netzwerk → Enterprise Identity Mapping**.
4. Klicken Sie mit der rechten Maustaste auf **Konfiguration**, und wählen Sie **Konfigurieren...** aus, um den EIM-Konfigurationsassistenten zu starten.
5. Wählen Sie eine EIM-Konfigurationsoption aus und folgen Sie den Anweisungen des Assistenten.
6. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen benötigen.

Nach Abschluss der Planung können Sie mit dem EIM-Konfigurationsassistenten eine von drei EIM-Basiskonfigurationen erstellen. Sie können den Assistenten verwenden, um das System einer vorhandenen Domäne hinzuzufügen oder um eine neue Domäne zu erstellen und das System hinzuzufügen. Wenn Sie eine neue Domäne erstellen und das System hinzufügen, können Sie angeben, ob Sie einen EIM-Domänencontroller auf einem lokalen oder einem fernen System konfigurieren möchten. Die folgenden Tasks enthalten Anweisungen zur Konfiguration von EIM, je nachdem welche EIM-Basiskonfiguration Sie benötigen:

Neue lokale Domäne erstellen und System hinzufügen

Im Folgenden wird erläutert, wie eine neue EIM-Domäne (EIM = Enterprise Identity Mapping) für Ihr Unternehmen erstellt und wie der lokale Directory-Server als EIM-Domänencontroller für die neue Domäne konfiguriert werden kann.

Wenn Sie mit dem EIM-Konfigurationsassistenten eine neue Domäne erstellen und das System hinzufügen, können Sie im Rahmen Ihrer EIM-Konfiguration den EIM-Domänencontroller auf dem lokalen System konfigurieren. Falls erforderlich, stellt der EIM-Konfigurationsassistent sicher, dass Sie die wichtigsten Konfigurationsdaten für den Directory-Server angeben. Wenn Kerberos auf dem iSeries-Server momentan nicht konfiguriert ist, werden Sie vom Assistenten außerdem aufgefordert, den Assistenten für den Netzwerkauthentifizierungsservice zu starten.

Wenn Sie den EIM-Konfigurationsassistenten beendet haben, können Sie die folgenden Tasks ausführen:

- Neue EIM-Domäne erstellen.
- Lokalen Directory-Server als EIM-Domänencontroller konfigurieren.
- Netzwerkauthentifizierungsservice für das System konfigurieren.
- EIM-Registerdefinitionen für das lokale i5/OS-Register und das Kerberos-Register erstellen.
- System für die Nutzung der neuen EIM-Domäne konfigurieren.

Um eine neue EIM-Domäne zu erstellen und das System hinzuzufügen, benötigen Sie die folgenden Sonderberechtigungen:

- Sicherheitsadministrator (*SECADM)
- Berechtigung für alle Objekte (*ALLOBJ)
- Systemkonfiguration (*IOSYSCFG)

Führen Sie die folgenden Schritte durch, um mit dem EIM-Konfigurationsassistenten eine neue lokale Domäne zu erstellen und das System hinzuzufügen:

1. Wählen Sie im iSeries Navigator das System aus, für das EIM konfiguriert werden soll, und erweitern Sie **Netzwerk > Enterprise Identity Mapping**.
2. Klicken Sie mit der rechten Maustaste auf **Konfiguration**, und wählen Sie **Konfigurieren...** aus, um den EIM-Konfigurationsassistenten zu starten.

   Anmerkung: Diese Option lautet **Rekonfigurieren...**, wenn EIM bereits zuvor auf dem System konfiguriert wurde.
3. Wählen Sie auf der **Begrüßungsseite** des Assistenten **Neue Domäne erstellen und System hinzufügen** aus, und klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Position der EIM-Domäne angeben** die Option **Auf dem lokalen Directory-Server** aus, und klicken Sie auf **Weiter**.

   Anmerkung: Mit dieser Option wird der lokale Directory-Server als EIM-Domänencontroller konfiguriert. Da auf diesem Directory-Server alle EIM-Daten für die Domäne gespeichert werden, muss er aktiv sein und bleiben, damit EIM-Abgleichsuchen und andere Operationen ausgeführt werden können.

   Wenn der Netzwerkauthentifizierungsservice derzeit nicht auf dem iSeries-Server konfiguriert ist oder weitere Informationen für den Netzwerkauthentifizierungsservice benötigt werden, um eine Einzelanmeldungsumgebung zu konfigurieren, wird die Seite **Konfiguration des Netzwerkauthentifizierungsservice** angezeigt. Mit Hilfe dieser Seite kann der Assistent für den Netzwerkauthentifizierungsservice gestartet werden, so dass Sie den Netzwerkauthentifizierungsservice konfigurieren können. Sie können die Konfiguration des Netzwerkauthentifizierungsservice aber auch zu einem späteren Zeitpunkt durchführen, indem Sie den Konfigurationsassistenten für diesen Service über den iSeries Navigator aufrufen. Wenn Sie die Konfiguration des Netzwerkauthentifizierungsservice abgeschlossen haben, wird der EIM-Konfigurationsassistent fortgesetzt.

5. Führen Sie die folgenden Schritte durch, um den Netzwerkauthentifizierungsservice zu konfigurieren:
   a. Wählen Sie auf der Seite **Netzwerkauthentifizierungsservice konfigurieren** die Option **Ja** aus, um den Assistenten für den Netzwerkauthentifizierungsservice zu starten. Mit diesem Assistenten können Sie mehrere i5/OS-Schnittstellen und -Services für die Nutzung eines Kerberos-Realms sowie eine Einzelanmeldungsumgebung konfigurieren, in der sowohl EIM als auch der Netzwerkauthentifizierungsservice verwendet werden.
   b. Geben Sie auf der Seite **Realm-Informationen angeben** den Namen des Standard-Realms im Feld **Standard-Realm** ein. Wenn Sie Microsoft Active Directory für die Kerberos-Authentifizierung verwenden, wählen Sie **Microsoft Active Directory wird für Kerberos-Authentifizierung verwendet** aus, und klicken Sie auf **Weiter**.
   c. Geben Sie auf der Seite **KDC-Informationen angeben** den vollständig qualifizierten Namen des Kerberos-Servers für diesen Realm im Feld **KDC** und 88 im Feld **Port** ein, und klicken Sie auf **Weiter**.
   d. Wählen Sie auf der Seite **Kennwortserverinformationen angeben** entweder **Ja** oder **Nein** für die Definition eines Kennwortservers aus. Mit dem Kennwortserver können Principals Kennwörter auf dem Kerberos-Server ändern. Wenn Sie **Ja** auswählen, geben Sie den Namen des Kennwortservers im Feld **Kennwortserver** ein. Übernehmen Sie den Standardwert 464 im Feld **Port**, und klicken Sie auf Weiter.
   e. Wählen Sie auf der Seite **Chiffrierschlüsseleinträge auswählen** die **i5/OS Kerberos-Authentifizierung** aus, und klicken Sie dann auf **Weiter**.

      Anmerkung: Sie können außerdem Chiffrierschlüsseleinträge für IBM Directory Server for iSeries (LDAP), iSeries NetServer und für IBM HTTP-Server für iSeries erstellen, wenn diese Services mit der Kerberos-Authentifizierung arbeiten sollen. Möglicherweise müssen zusätzliche Konfigurationsschritte für diese Services durchgeführt werden, bevor Sie die Kerberos-Authentifizierung verwenden können.
   f. Geben Sie auf der Seite **i5/OS-Chiffrierschlüsseleintrag erstellen** ein Kennwort ein, und bestätigen Sie es. Klicken Sie anschließend auf **Weiter**. Dieses Kennwort verwenden Sie auch, wenn Sie die i5/OS-Principals zum Kerberos-Server hinzufügen.
   g. Optional: Wählen Sie **Ja** auf der Seite **Stapeldatei erstellen** aus, geben Sie die folgenden Informationen an, und klicken Sie auf **Weiter**:
      - Aktualisieren Sie im Feld **Stapeldatei** den Verzeichnispfad. Klicken Sie auf **Durchsuchen**, um den entsprechenden Verzeichnispfad zu lokalisieren, oder editieren Sie den Pfad im Feld **Stapeldatei**.
      - Wählen Sie **Ja** im Feld **Kennwort einfügen** aus. Dies garantiert, dass alle Kennwörter, die dem i5/OS-Service-Principal zugeordnet sind, in die Stapeldatei eingefügt werden. Beachten Sie, dass Kennwörter in Klartext angezeigt werden und von jedem gelesen werden können, der über den Lesezugriff für die Stapeldatei verfügt. Daher ist es außerordentlich wichtig, dass Sie die Stapeldatei sofort nach Gebrauch wieder vom Kerberos-Server und dem PC löschen. Wenn Sie das Kennwort nicht einfügen, werden Sie bei der Ausführung der Stapeldatei zur Eingabe des Kennworts aufgefordert.

        Anmerkung: Sie können dem Microsoft Active Directory auch manuell die vom Assistenten generierten Service-Principals hinzufügen. Anweisungen hierzu finden Sie unter i5/OS-Principals zum Kerberos-Server hinzufügen.
      - Überprüfen Sie die Konfigurationsdetails für den Netzwerkauthentifizierungsservice auf der Seite **Zusammenfassung**, und klicken Sie auf **Fertig stellen**, um zum EIM-Konfigurationsassistenten zurückzukehren.
6. Wenn der lokale Directory-Server derzeit nicht konfiguriert ist, wird bei der Rückkehr zum EIM-Konfigurationsassistenten die Seite **Directory-Server konfigurieren** angezeigt. Geben Sie die folgenden Informationen ein, um den lokalen Directory-Server zu konfigurieren:

Anmerkung: Wenn Sie den lokalen Directory-Server konfigurieren, bevor Sie den EIM-Konfigurationsassistenten verwenden, wird stattdessen die Seite **Benutzer für Verbindung angeben** angezeigt. Geben Sie auf dieser Seite den registrierten Namen und das Kennwort des LDAP-Administrators ein, um sicherzustellen, dass der Assistent ausreichend berechtigt ist, um die EIM-Domäne und die darin enthaltenen Objekte zu verwalten; fahren Sie dann mit dem nächsten Schritt fort. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen benötigen.

a. Übernehmen Sie den Standardwert 389 im Feld **Port**, oder geben Sie eine andere Portnummer für die ungesicherte EIM-Kommunikation mit dem Directory-Server an.
b. Geben Sie im Feld **Registrierter Name** den registrierten LDAP-Namen (DN) ein, der den LDAP-Administrator für den Directory-Server identifiziert. Dieser registrierte Name wird vom EIM-Konfigurationsassistenten erstellt und verwendet, um den Directory-Server als Domänencontroller für die neue Domäne zu konfigurieren, die momentan erstellt wird.
c. Geben Sie im Feld **Kennwort** das Kennwort für den LDAP-Administrator ein.
d. Geben Sie im Feld **Kennwort bestätigen** das Kennwort zur Überprüfung ein zweites Mal ein.
e. Klicken Sie auf **Weiter**.

7. Geben Sie auf der Seite **Domäne angeben** die folgenden Informationen ein:
   a. Geben Sie im Feld **Domäne** den Namen der zu erstellenden EIM-Domäne ein. Übernehmen Sie den Standardnamen EIM, oder geben Sie eine beliebige Zeichenfolge ein, die Ihnen sinnvoll erscheint. Die Sonderzeichen = + < > , # ; \ und * können Sie jedoch nicht verwenden.
   b. Geben Sie im Feld **Beschreibung** eine Beschreibung der Domäne ein.
   c. Klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite **Übergeordneten registrierten Namen für Domäne angeben** die Option **Ja** aus, um einen übergeordneten registrierten Namen für die zu erstellende Domäne anzugeben. Wählen Sie **Nein** aus, wenn EIM-Daten an einer Verzeichnisposition mit einem Suffix gespeichert werden sollen, das vom EIM-Domänennamen abgeleitet wird.

   Anmerkung: Wenn Sie eine Domäne auf einem lokalen Directory-Server erstellen, ist die Angabe eines übergeordneten registrierten Namens optional. Mit der Angabe eines übergeordneten registrierten Namens können Sie festlegen, an welcher Stelle im lokalen LDAP-Namespace EIM-Daten für die Domäne gespeichert werden sollen. Wenn Sie keinen übergeordneten registrierten Namen angeben, werden die EIM-Daten unter dem eigenen Suffix im Namespace gespeichert. Verwenden Sie bei Angabe von **Ja** das Listenfeld, um das lokale LDAP-Suffix auszuwählen, das als übergeordneter registrierter Name dienen soll, oder geben Sie Text ein, um einen neuen übergeordneten registrierten Namen zu erstellen und zu benennen. Die Angabe eines übergeordneten registrierten Namens für die neue Domäne ist nicht erforderlich. Klicken Sie auf **Hilfe**, wenn Sie weitere Informationen über die Verwendung eines übergeordneten registrierten Namens benötigen.
9. Geben Sie auf der Seite **Registerinformationen** an, ob die lokalen Benutzerregister der EIM-Domäne als Registerdefinitionen hinzugefügt werden sollen. Wählen Sie eine oder beide der folgenden Registertypen aus:

   Anmerkung: Sie müssen die Registerdefinitionen nicht zum jetzigen Zeitpunkt erstellen. Wenn Sie sie später erstellen möchten, müssen Sie die Systemregisterdefinitionen hinzufügen und die EIM-Konfigurationseigenschaften aktualisieren.

   a. Wählen Sie **Lokales i5/OS** aus, um eine Registerdefinition für das lokale Register hinzuzufügen. Übernehmen Sie den im Feld enthaltenen Standardwert für den Namen der Registerdefinition oder geben Sie einen anderen Namen ein. Der EIM-Registername ist eine beliebige Zeichenfolge, die für den Registertyp und eine bestimmte Instanz dieses Registers steht.
   b. Wählen Sie **Kerberos** aus, um eine Registerdefinition für ein Kerberos-Register hinzuzufügen. Übernehmen Sie den im Feld enthaltenen Standardwert für den Namen der Registerdefinition oder geben Sie einen anderen Namen ein. Der Standardname für die Registerdefinition entspricht

dem Realm-Namen. Wenn Sie den Standardnamen übernehmen (sprich für den Kerberos-Registernamen denselben Namen verwenden wie für den Realm), können Sie die Leistung beim Abrufen von Informationen aus dem Register erhöhen. Wählen Sie ggf. **Bei Kerberos-Benutzeridentitäten muss die Groß-/Kleinschreibung beachtet werden** aus.

c. Klicken Sie auf **Weiter**.

10. Wählen Sie auf der Seite **EIM-Systembenutzer angeben** einen **Benutzerstatus** aus, den das System verwenden soll, wenn es EIM-Operationen für Betriebssystemfunktionen ausführt. Diese Operationen umfassen Abgleichsuchoperationen sowie Löschoperationen für Zuordnungen, die ausgeführt werden, wenn ein lokales i5/OS-Benutzerprofil gelöscht wird. Sie können eine der folgenden Benutzerstatusarten auswählen: **Registrierter Name und Kennwort**, **Kerberos-Chiffrierschlüsseldatei und Principal** oder **Kerberos-Principal und Kennwort**. Welche Benutzerstatusarten im Einzelnen ausgewählt werden können, hängt von der aktuellen Systemkonfiguration ab. Wenn der Netzwerkauthentifizierungsservice für das System z. B. nicht konfiguriert ist, können Benutzer mit dem Status "Kerberos" möglicherweise nicht ausgewählt werden. Der von Ihnen ausgewählte Benutzerstatus bestimmt die übrigen Informationen, die Sie noch auf der Seite eingeben müssen, folgendermaßen:

    Anmerkung: Sie müssen einen Benutzer angeben, der momentan auf dem Directory-Server definiert ist, auf dem sich der EIM-Domänencontroller befindet. Der Benutzer muss mindestens über die erforderlichen Privilegien verfügen, um die Abgleichsuchfunktion und die Registerverwaltung für das lokale Benutzerregister ausführen zu können. Ist dies nicht der Fall, können bestimmte Betriebssystemfunktionen im Zusammenhang mit der Einzelanmeldung und dem Löschen von Benutzerprofilen fehlschlagen.

    Wenn Sie den Directory-Server vor Ausführung dieses Assistenten nicht konfiguriert haben, können Sie lediglich den Benutzerstatus **Registrierter Namen und Kennwort** auswählen und als registrierten Namen nur den des LDAP-Administrators angeben.

    - Wenn Sie **Registrierter Name und Kennwort** auswählen, müssen Sie die folgenden Informationen angeben:
      - Geben Sie im Feld **Registrierter Name** den registrierten LDAP-Namen ein, der den Benutzer identifiziert, den das System zur Ausführung von EIM-Operationen verwenden soll.
      - Geben Sie im Feld **Kennwort** das Kennwort für den registrierten Namen ein.
      - Geben Sie im Feld **Kennwort bestätigen** das Kennwort zur Überprüfung ein zweites Mal ein.
    - Wenn Sie **Kerberos-Principal und Kennwort** auswählen, müssen Sie die folgenden Informationen angeben:
      - Geben Sie im Feld **Principal** den Kerberos-Principal-Namen an, den das System zur Ausführung von EIM-Operationen verwenden soll.
      - Geben Sie im Feld **Realm** den vollständig qualifizierten Kerberos-Realm-Namen ein, zu dem der Principal gehört. Der Name des Principals und des Realms identifizieren die Kerberos-Benutzer in der Chiffrierschlüsseltabelle eindeutig. Beispiel: Der Principal `jsmith` im Realm `ordept.myco.com` wird in der Chiffrierschlüsseltabelle als `jsmith@ordept.myco.com` geführt.
      - Geben Sie im Feld **Kennwort** das Kennwort für den Benutzer ein.
      - Geben Sie im Feld **Kennwort bestätigen** das Kennwort zur Überprüfung ein zweites Mal ein.
    - Wenn Sie **Kerberos-Chiffrierschlüsseldatei und -Principal** auswählen, müssen Sie die folgenden Informationen angeben:
      - Geben Sie im Feld **Chiffrierschlüsseldatei** den vollständig qualifizierten Namen des Pfads und der Chiffrierschlüsseldatei ein, die den Kerberos-Principal enthält, den das System zur Ausführung vom EIM-Operationen verwenden soll. Sie können auch auf **Durchsuchen...** klicken, um eine Chiffrierschlüsseldatei aus den Verzeichnissen des integrierten Dateisystems der iSeries auszuwählen.
      - Geben Sie im Feld **Principal** den Kerberos-Principal-Namen an, den das System zur Ausführung von EIM-Operationen verwenden soll.

– Geben Sie im Feld **Realm** den vollständig qualifizierten Kerberos-Realm-Namen ein, zu dem der Principal gehört. Der Name des Principals und des Realms identifizieren die Kerberos-Benutzer in der Chiffrierschlüsseltabelle eindeutig. Beispiel: Der Principal `jsmith` im Realm `ordept.myco.com` wird in der Chiffrierschlüsseltabelle als `jsmith@ordept.myco.com` geführt.

- Klicken Sie auf **Verbindung prüfen**, um sicherzustellen, dass der Assistent die angegebenen Benutzerinformationen verwenden kann, um erfolgreich eine Verbindung zum EIM-Domänencontroller herzustellen.
- Klicken Sie auf **Weiter**.

11. Überprüfen Sie in der Anzeige **Zusammenfassung** die von Ihnen angegebenen Konfigurationsdaten. Wenn alle Informationen richtig sind, klicken Sie auf **Fertig stellen**.

EIM-Konfiguration der Domäne abschließen

Wenn der Assistent beendet wird, fügt er die neue Domäne zum Ordner **Domänenverwaltung** hinzu, womit Sie dann eine EIM-Basiskonfiguration für diesen Server erstellt haben. Um die EIM-Konfiguration für diese Domäne endgültig abzuschließen, müssen Sie jedoch noch folgende Tasks ausführen:

1. Verwenden Sie den EIM-Konfigurationsassistenten auf jedem weiteren Server, den Sie der Domäne hinzufügen möchten.
2. Fügen Sie der EIM-Domäne bei Bedarf EIM-Registerdefinitionen für andere Nicht-iSeries-Server und Anwendungen hinzu, die Sie zur EIM-Domäne hinzufügen möchten. Diese Registerdefinitionen beziehen sich auf die tatsächlichen Benutzerregister, die zur Domäne gehören müssen. Sie können abhängig von Ihren Anforderungen in Bezug auf die EIM-Implementierung entweder Systemregisterdefinitionen hinzufügen oder Anwendungsregisterdefinitionen hinzufügen.
3. Legen Sie abhängig von diesen Anforderungen fest, ob Sie folgende Schritte durchführen müssen:
   - EIM-Kennungen für jeden einzelnen Benutzer oder jede einzelne Entität der Domäne und Kennungszuordnungen für diese Benutzer oder Entitäten erstellen.
   - Richtlinienzuordnungen erstellen, um eine Gruppe von Benutzern mit einer einzigen Zielbenutzeridentität abzugleichen.
   - Eine Kombination aus beiden Möglichkeiten erstellen.
4. Testen Sie die Identitätsabgleiche für Ihre EIM-Konfiguration mit Hilfe der EIM-Funktion Ableich testen.
5. Wenn der einzige EIM-Benutzer, den Sie definiert haben, der registrierte Name für den LDAP-Administrator ist, dann verfügt Ihr EIM-Benutzer über eine übergeordnete Berechtigung für alle Daten auf dem Directory-Server. Daher könnten Sie erwägen, einen oder mehrere registrierte Namen als zusätzliche Benutzer zu erstellen, die über eine besser geeignete EIM-Zugriffssteuerung mit eingeschränkten Rechten für EIM-Daten verfügen. Weitere Informationen zum Erstellen von registrierten Namen für den Directory-Server finden Sie im Abschnitt Distinguished names unter dem Thema zum IBM Directory Server for iSeries (LDAP). Wie viele EIM-Benutzer Sie zusätzlich definieren, hängt davon ab, welche Rolle die Trennung von Sicherheitsaufgaben und Zuständigkeiten bei Ihrer Sicherheitsrichtlinie spielt. Normalerweise können Sie mindestens die beiden folgenden Arten von registrierten Namen erstellen:
   - **Benutzer mit EIM-Administratorzugriffssteuerung**

     Dieser registrierte Name stellt die geeignete Berechtigungsstufe für einen Administrator zur Verfügung, der für die Verwaltung der EIM-Domäne verantwortlich ist. Dieser registrierte Name könnte verwendet werden, um eine Verbindung zum Domänencontroller herzustellen, wenn die Verwaltung der EIM-Domäne über den iSeries Navigator erfolgt.
   - **Mindestens ein Benutzer mit allen folgenden Zugriffssteuerungen**:
     – Kennungsadministrator
     – Registeradministrator
     – EIM-Abgleichsoperationen

Dieser Benutzer stellt die erforderliche Zugriffssteuerungsstufe für den Systembenutzer zur Verfügung, der EIM-Operationen für das Betriebssystem ausführt.

Anmerkung: Um diesen neuen registrierten Namen für den Systembenutzer an Stelle des registrierten Namens für den LDAP-Administrator benutzen zu können, müssen die EIM-Konfigurationseigenschaften für den iSeries-Server geändert werden. Unter EIM-Konfigurationseigenschaften verwalten wird erläutert, wie Sie den registrierten Namen des Systembenutzers ändern können.

Zusätzlich können Sie noch SSL (Secure Sockets Layer) oder TLS (Transport Layer Security) verwenden, um eine sichere Verbindung zum EIM-Domänencontroller zu konfigurieren und so die Übertragung von EIM-Daten zu schützen. Wenn Sie SSL für den Directory-Server aktivieren, müssen Sie die EIM-Konfigurationseigenschaften aktualisieren, indem Sie angeben, dass der iSeries-Server eine sichere SSL-Verbindung verwendet. Außerdem müssen Sie die Eigenschaften der Domäne aktualisieren, indem Sie angeben, dass EIM SSL-Verbindungen verwendet, um die Domäne über iSeries Navigator zu verwalten.

Anmerkung: Möglicherweise sind weitere Tasks erforderlich, wenn Sie eine Basiskonfiguration des Netzwerkauthentifizierungsservice erstellt haben; dies gilt insbesondere, wenn Sie eine Einzelanmeldungsumgebung implementieren. Informationen zu diesen zusätzlichen Arbeitsschritten erhalten Sie, wenn Sie alle Konfigurationsschritte im Szenario: Einzelanmeldung für i5/OS aktivieren durcharbeiten.

Neue ferne Domäne erstellen und System hinzufügen

Im Folgenden wird erläutert, wie eine neue EIM-Domäne (EIM = Enterprise Identity Mapping) für Ihr Unternehmen erstellt und wie der ferne Directory-Server als EIM-Domänencontroller für die neue Domäne konfiguriert werden kann.

Wenn Sie mit dem EIM-Konfigurationsassistenten eine neue Domäne erstellen und das System hinzufügen, können Sie im Rahmen der EIM-Konfiguration einen Directory-Server auf einem fernen System als EIM-Domänencontroller konfigurieren. Sie müssen die entsprechenden Informationen für die Verbindung zu dem fernen Directory-Server angeben, damit Sie EIM konfigurieren können. Wenn Kerberos derzeit nicht auf dem iSeries-Server konfiguriert ist, werden Sie vom Assistenten aufgefordert, den Assistenten für den Netzwerkauthentifizierungsservice zu starten.

Anmerkung: Der Directory-Server auf dem fernen System muss EIM-Unterstützung bieten. EIM setzt voraus, dass sich der Domänencontroller auf einem Directory-Server befindet, der Lightweight Directory Access Protocol (LDAP) Version 3 unterstützt. Darüber hinaus muss auf dem Directory-Server-Produkt das EIM-Schema konfiguriert sein. Der IBM Directory Server V5.1 stellt diese Unterstützung beispielsweise zur Verfügung. Weitere Informationen über die Voraussetzungen für den EIM-Domänencontroller finden Sie unter EIM-Domänencontroller planen.

Wenn Sie den EIM-Konfigurationsassistenten beendet haben, können Sie die folgenden Tasks ausführen:

- Neue EIM-Domäne erstellen.
- Fernen Directory-Server als EIM-Domänencontroller konfigurieren.
- Netzwerkauthentifizierungsservice für das System konfigurieren.
- EIM-Registerdefinitionen für das lokale i5/OS-Register und das Kerberos-Register erstellen.
- System für die Nutzung der neuen EIM-Domäne konfigurieren.

Um eine neue EIM-Domäne zu erstellen und das System hinzuzufügen, benötigen Sie die folgenden Sonderberechtigungen:

- Sicherheitsadministrator (*SECADM)
- Berechtigung für alle Objekte (*ALLOBJ)

- Systemkonfiguration (*IOSYSCFG)

Führen Sie die folgenden Schritte durch, um mit dem EIM-Konfigurationsassistenten eine Domäne auf einem fernen System zu erstellen und das System hinzuzufügen:

1. Vergewissern Sie sich, dass der Directory-Server auf dem fernen System aktiv ist.
2. Wählen Sie im iSeries Navigator das System aus, für das EIM konfiguriert werden soll, und erweitern Sie **Netzwerk > Enterprise Identity Mapping**.
3. Klicken Sie mit der rechten Maustaste auf **Konfiguration**, und wählen Sie **Konfigurieren...** aus, um den EIM-Konfigurationsassistenten zu starten.

   Anmerkung: Diese Option lautet **Rekonfigurieren...**, wenn EIM bereits zuvor auf dem System konfiguriert wurde.
4. Wählen Sie auf der **Begrüßungsseite** des Assistenten **Neue Domäne erstellen und System hinzufügen** aus, und klicken Sie auf **Weiter**.
5. Wählen Sie auf der Seite **Position der EIM-Domäne angeben** die Option **Auf dem lokalen Directory-Server** aus, und klicken Sie auf **Weiter**.

   Anmerkung: Mit dieser Option wird der lokale Directory-Server als EIM-Domänencontroller konfiguriert. Da auf diesem Directory-Server alle EIM-Daten für die Domäne gespeichert werden, muss er aktiv sein und bleiben, damit EIM-Abgleichsuchen und andere Operationen ausgeführt werden können.

   Wenn der Netzwerkauthentifizierungsservice derzeit nicht auf dem iSeries-Server konfiguriert ist oder weitere Informationen für den Netzwerkauthentifizierungsservice benötigt werden, um eine Einzelanmeldungsumgebung zu konfigurieren, wird die Seite **Konfiguration des Netzwerkauthentifizierungsservice** angezeigt. Mit Hilfe dieser Seite kann der Assistent für den Netzwerkauthentifizierungsservice gestartet werden, so dass Sie den Netzwerkauthentifizierungsservice konfigurieren können. Sie können die Konfiguration des Netzwerkauthentifizierungsservice aber auch zu einem späteren Zeitpunkt durchführen, indem Sie den Konfigurationsassistenten für diesen Service über den iSeries Navigator aufrufen. Wenn Sie die Konfiguration des Netzwerkauthentifizierungsservice abgeschlossen haben, wird der EIM-Konfigurationsassistent fortgesetzt.
6. Führen Sie die folgenden Schritte durch, um den Netzwerkauthentifizierungsservice zu konfigurieren:
   a. Wählen Sie auf der Seite **Netzwerkauthentifizierungsservice konfigurieren** die Option **Ja** aus, um den Assistenten für den Netzwerkauthentifizierungsservice zu starten. Mit diesem Assistenten können Sie mehrere i5/OS-Schnittstellen und -Services für die Nutzung eines Kerberos-Realms sowie eine Einzelanmeldungsumgebung konfigurieren, in der sowohl EIM als auch der Netzwerkauthentifizierungsservice verwendet werden.
   b. Geben Sie auf der Seite **Realm-Informationen angeben** den Namen des Standard-Realms im Feld **Standard-Realm** ein. Wenn Sie Microsoft Active Directory für die Kerberos-Authentifizierung verwenden, wählen Sie **Microsoft Active Directory wird für Kerberos-Authentifizierung verwendet** aus, und klicken Sie auf **Weiter**.
   c. Geben Sie auf der Seite **KDC-Informationen angeben** den vollständig qualifizierten Namen des Kerberos-Servers für diesen Realm im Feld **KDC** und 88 im Feld **Port** ein, und klicken Sie auf **Weiter**.
   d. Wählen Sie auf der Seite **Kennwortserverinformationen angeben** entweder **Ja** oder **Nein** für die Definition eines Kennwortservers aus. Mit dem Kennwortserver können Principals Kennwörter auf dem Kerberos-Server ändern. Wenn Sie **Ja** auswählen, geben Sie den Namen des Kennwortservers im Feld **Kennwortserver** ein. Übernehmen Sie den Standardwert 464 im Feld **Port**, und klicken Sie auf Weiter.
   e. Wählen Sie auf der Seite **Chiffrierschlüsseleinträge auswählen** die **i5/OS Kerberos-Authentifizierung** aus, und klicken Sie dann auf **Weiter**.

Anmerkung: Sie können außerdem Chiffrierschlüsseleinträge für IBM Directory Server for iSeries (LDAP), iSeries NetServer und für IBM HTTP-Server für iSeries erstellen, wenn diese Services mit der Kerberos-Authentifizierung arbeiten sollen. Möglicherweise müssen zusätzliche Konfigurationsschritte für diese Services ausgeführt werden, bevor Sie die Kerberos-Authentifizierung verwenden können.

f. Geben Sie auf der Seite **i5/OS-Chiffrierschlüsseleintrag erstellen** ein Kennwort ein, und bestätigen Sie es. Klicken Sie anschließend auf **Weiter**. Dieses Kennwort verwenden Sie auch, wenn Sie die i5/OS-Principals zum Kerberos-Server hinzufügen.

g. Optional: Wählen Sie **Ja** auf der Seite **Stapeldatei erstellen** aus, geben Sie die folgenden Informationen an, und klicken Sie auf **Weiter**:

- Aktualisieren Sie im Feld **Stapeldatei** den Verzeichnispfad. Klicken Sie auf **Durchsuchen**, um den entsprechenden Verzeichnispfad zu lokalisieren, oder editieren Sie den Pfad im Feld **Stapeldatei**.
- Wählen Sie **Ja** im Feld **Kennwort einfügen** aus. Dies garantiert, dass alle Kennwörter, die dem i5/OS-Service-Principal zugeordnet sind, in die Stapeldatei eingefügt werden. Beachten Sie, dass Kennwörter in Klartext angezeigt werden und von jedem gelesen werden können, der über den Lesezugriff für die Stapeldatei verfügt. Daher ist es außerordentlich wichtig, dass Sie die Stapeldatei sofort nach Gebrauch wieder vom Kerberos-Server und dem PC löschen. Wenn Sie das Kennwort nicht einfügen, werden Sie bei der Ausführung der Stapeldatei zur Eingabe des Kennworts aufgefordert.

  Anmerkung: Sie können die vom Assistenten generierten Service-Principals auch manuell zum Microsoft Active Directory hinzufügen. Anweisungen hierzu finden Sie unter i5/OS-Principals zum Kerberos-Server hinzufügen.
- Überprüfen Sie die Konfigurationsdetails für den Netzwerkauthentifizierungsservice auf der Seite **Zusammenfassung**, und klicken Sie auf **Fertig stellen**, um zum EIM-Konfigurationsassistenten zurückzukehren.

7. Geben Sie auf der Seite **EIM-Domänencontroller angeben** die folgenden Verbindungsinformationen für den zu konfigurierenden fernen EIM-Domänencontroller an:
   a. Geben Sie im Feld **Name des Domänencontrollers** den Namen des fernen Directory-Servers an, der als EIM-Domänencontroller für die Domäne fungieren soll, die erstellt wird. Bei dem Namen des EIM-Domänencontrollers kann es sich um den TCP/IP-Host- und Domänennamen oder um die Adresse des Directory-Servers handeln.
   b. Geben Sie die folgenden Informationen für die Verbindung zum Domänencontroller ein:
      - Wählen Sie **Sichere Verbindung (SSL oder TLS) verwenden** aus, um eine sichere Verbindung zum EIM-Domänencontroller herzustellen. Daraufhin wird entweder mit SSL (Secure Sockets Layer) oder mit TLS (Transport Layer Security) eine sichere Verbindung hergestellt, um die Übertragung von EIM-Daten über ein ungesichertes Netzwerk, wie beispielsweise das Internet, zu schützen.

        Anmerkung: Sie müssen sicherstellen, dass der EIM-Domänencontroller für die Verwendung einer sicheren Verbindung konfiguriert ist. Andernfalls kann die Verbindung zum Domänencontroller möglicherweise nicht hergestellt werden.
      - Geben Sie im Feld **Port** den TCP/IP-Port ein, auf dem der Directory-Server empfangsbereit ist. Wenn **Sichere Verbindung verwenden** ausgewählt ist, lautet der Standardport 636; andernfalls ist 389 der Standardport.
   c. Klicken Sie auf **Verbindung prüfen**, um sicherzustellen, dass der Assistent die angegebenen Informationen verwenden kann, um erfolgreich eine Verbindung zum fernen EIM-Domänencontroller herzustellen.
   d. Klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite **Benutzer für Verbindung angeben** einen **Benutzerstatus** für die Verbindung aus. Sie können eine der folgenden Benutzerstatusarten auswählen: **Registrierter Name und Kennwort**, **Kerberos-Chiffrierschlüsseldatei und Principal**, **Kerberos-Principal und Kennwort** oder

Benutzerprofil und Kennwort. Die beiden Kerberos-Benutzerstatusarten sind nur verfügbar, wenn der Netzwerkauthentifizierungsservice für das lokale iSeries-System konfiguriert ist. Der von Ihnen ausgewählte Benutzertyp bestimmt die anderen Daten, die Sie im Dialog noch angeben müssen, wie folgt:

Anmerkung: Wenn Sie sicherstellen möchten, dass der Assistent über ausreichende Berechtigungen verfügt, um die erforderlichen EIM-Objekte im Verzeichnis zu erstellen, wählen Sie als Benutzerstatus **Registrierter Name und Kennwort** aus, und geben Sie den registrierten Namen und das Kennwort des LDAP-Administrators als Benutzer an.

Sie können einen anderen Benutzer für die Verbindung angeben; dieser muss jedoch über die entsprechende LDAP-Administratorberechtigung für den fernen Directory-Server verfügen.

a. Wenn Sie **Registrierter Name und Kennwort** auswählen, müssen Sie die folgenden Informationen angeben:
   - Geben Sie im Feld **Registrierter Name** den registrierten Namen (DN) und das Kennwort des LDAP-Administrators ein, um sicherzustellen, dass der Assistent ausreichend berechtigt ist, die EIM-Domäne und die darin enthaltenen Objekte zu verwalten.
   - Geben Sie im Feld **Kennwort** das Kennwort für den registrierten Namen ein.
   - Geben Sie im Feld **Kennwort bestätigen** das Kennwort zur Überprüfung ein zweites Mal ein.

b. Wenn Sie **Kerberos-Chiffrierschlüsseldatei und -Principal** auswählen, müssen Sie die folgenden Informationen angeben:
   - Geben Sie im Feld **Chiffrierschlüsseldatei** den vollständig qualifizierten Namen des Pfads und der Chiffrierschlüsseldatei ein, die den Kerberos-Principal enthält, den der Assistent beim Verbindungsaufbau zur EIM-Domäne verwenden soll. Sie können auch auf **Durchsuchen...** klicken, um eine Chiffrierschlüsseldatei aus den Verzeichnissen des integrierten Dateisystems der iSeries auszuwählen.
   - Geben Sie im Feld **Principal** den Namen des Kerberos-Principals ein, mit dem der Benutzer identifiziert werden soll.
   - Geben Sie im Feld **Realm** den vollständig qualifizierten Kerberos-Realm-Namen ein, zu dem der Principal gehört. Der Name des Principals und des Realms identifizieren die Kerberos-Benutzer in der Chiffrierschlüsseltabelle eindeutig. Beispiel: Der Principal `jsmith` im Realm `ordept.myco.com` wird in der Chiffrierschlüsseltabelle als `jsmith@ordept.myco.com` geführt.

c. Wenn Sie **Kerberos-Principal und Kennwort** auswählen, müssen Sie die folgenden Informationen angeben:
   - Geben Sie im Feld **Principal** den Namen des Kerberos-Principals ein, den der Assistent beim Verbindungsaufbau zur EIM-Domäne verwenden soll.
   - Geben Sie im Feld **Realm** den vollständig qualifizierten Kerberos-Realm-Namen ein, zu dem der Principal gehört. Der Name des Principals und des Realms identifizieren die Kerberos-Benutzer in der Chiffrierschlüsseltabelle eindeutig. Beispiel: Der Principal `jsmith` im Realm `ordept.myco.com` wird in der Chiffrierschlüsseltabelle als `jsmith@ordept.myco.com` geführt.
   - Geben Sie im Feld **Kennwort** das Kennwort für den Kerberos-Principal ein.
   - Geben Sie im Feld **Kennwort bestätigen** das Kennwort zur Überprüfung ein zweites Mal ein.

d. Wenn Sie **Benutzerprofil und Kennwort** auswählen, müssen Sie die folgenden Informationen angeben:
   - Geben Sie im Feld **Benutzerprofil** den Namen des Benutzerprofils ein, den der Assistent beim Verbindungsaufbau zur EIM-Domäne verwenden soll.
   - Geben Sie im Feld **Kennwort** das Kennwort für das Benutzerprofil ein.
   - Geben Sie im Feld **Kennwort bestätigen** das Kennwort zur Überprüfung ein zweites Mal ein.

e. Klicken Sie auf **Verbindung prüfen**, um sicherzustellen, dass der Assistent die angegebenen Benutzerinformationen verwenden kann, um erfolgreich eine Verbindung zum EIM-Domänencontroller herzustellen.

f. Klicken Sie auf **Weiter**.

9. Geben Sie auf der Seite **Domäne angeben** die folgenden Informationen ein:
   a. Geben Sie im Feld **Domäne** den Namen der zu erstellenden EIM-Domäne ein. Übernehmen Sie den Standardnamen `EIM`, oder geben Sie eine beliebige Zeichenfolge ein, die Ihnen sinnvoll erscheint. Die Sonderzeichen `= + < > , # ; \` und `*` können Sie jedoch nicht verwenden.
   b. Geben Sie im Feld **Beschreibung** eine Beschreibung der Domäne ein.
   c. Klicken Sie auf **Weiter**.
10. Wählen Sie im Dialog **Übergeordneten registrierten Namen für Domäne angeben** die Option **Ja** aus, um den übergeordneten registrierten Namen anzugeben, den der Assistent für die Adresse der EIM-Domäne verwenden soll, die erstellt wird. Dieser registrierte Name ist ein Eintrag, der in der Hierarchie der Verzeichnisinformationen dem Domänennameneintrag direkt übergeordnet ist. Wählen Sie **Nein** aus, wenn EIM-Daten an einer Verzeichnisposition mit einem Suffix gespeichert werden sollen, das vom EIM-Domänennamen abgeleitet wird.

    Anmerkung: Wenn Sie mit dem Assistenten eine Domäne auf einem fernen Domänencontroller konfigurieren, sollten Sie einen entsprechenden übergeordneten registrierten Namen für die Domäne angeben. Da alle erforderlichen Konfigurationsobjekte für den übergeordneten registrierten Namen bereits vorhanden sein müssen, damit die EIM-Konfiguration gelingt, sollten Sie mit der Anzeigefunktion nach dem entsprechenden übergeordneten registrierten Namen suchen, statt ihn manuell einzugeben. Klicken Sie auf **Hilfe**, wenn Sie weitere Informationen über die Verwendung eines übergeordneten registrierten Namens benötigen.
11. Geben Sie auf der Seite **Registerinformationen** an, ob lokale Benutzerregister der EIM-Domäne als Registerdefinitionen hinzugefügt werden sollen. Wählen Sie eine oder beide der folgenden Registertypen aus:

    Anmerkung: Sie müssen die Registerdefinitionen nicht zum jetzigen Zeitpunkt erstellen. Wenn Sie sie später erstellen möchten, müssen Sie die Systemregisterdefinitionen hinzufügen und die EIM-Konfigurationsmerkmale aktualisieren.
    a. Wählen Sie **Lokales i5/OS** aus, um eine Registerdefinition für das lokale Register hinzuzufügen. Übernehmen Sie den im Feld enthaltenen Standardwert für den Namen der Registerdefinition oder geben Sie einen anderen Namen ein. Der EIM-Registername ist eine beliebige Zeichenfolge, die für den Registertyp und eine bestimmte Instanz dieses Registers steht.
    b. Wählen Sie **Kerberos** aus, um eine Registerdefinition für ein Kerberos-Register hinzuzufügen. Übernehmen Sie den im Feld enthaltenen Standardwert für den Namen der Registerdefinition oder geben Sie einen anderen Namen ein. Der Standardname für die Registerdefinition entspricht dem Realm-Namen. Wenn Sie den Standardnamen übernehmen (sprich für den Kerberos-Registernamen denselben Namen verwenden wie für den Realm), können Sie die Leistung beim Abrufen von Informationen aus dem Register erhöhen. Wählen Sie ggf. **Bei Kerberos-Benutzeridentitäten muss die Groß-/Kleinschreibung beachtet werden** aus.
    c. Klicken Sie auf **Weiter**.
12. Wählen Sie auf der Seite **EIM-Systembenutzer angeben** einen **Benutzerstatus** aus, den das System verwenden soll, wenn es EIM-Operationen für Betriebssystemfunktionen ausführt. Diese Operationen umfassen Abgleichsuchoperationen sowie Löschoperationen für Zuordnungen, die ausgeführt werden, wenn ein lokales i5/OS-Benutzerprofil gelöscht wird. Sie können eine der folgenden Benutzerstatusarten auswählen: **Registrierter Name und Kennwort**, **Kerberos-Chiffrierschlüsseldatei und Principal** oder **Kerberos-Principal und Kennwort**. Welchen Benutzerstatus Sie im Einzelnen auswählen können, hängt von der aktuellen Systemkonfiguration ab. Wenn beispielsweise der Netzwerkauthentifizierungsservice nicht für das System konfiguriert ist, stehen möglicherweise keine Benut-

zer mit dem Status ″Kerberos″ zur Verfügung. Der von Ihnen ausgewählte Benutzerstatus bestimmt die übrigen Informationen, die Sie auf der Seite eingeben müssen, folgendermaßen:

Anmerkung: Sie müssen einen Benutzer angeben, der momentan in dem Directory-Server definiert ist, auf dem sich der EIM-Domänencontroller befindet. Der Benutzer muss mindestens über die erforderlichen Privilegien verfügen, um die Abgleichsuchfunktion und die Registerverwaltung für das lokale Benutzerregister ausführen zu können. Ist dies nicht der Fall, können bestimmte Betriebssystemfunktionen im Zusammenhang mit der Einzelanmeldung und dem Löschen von Benutzerprofilen fehlschlagen.

Wenn Sie den Directory-Server vor Ausführung dieses Assistenten nicht konfiguriert haben, können Sie lediglich den Benutzerstatus **Registrierter Namen und Kennwort** auswählen und als registrierten Namen nur den des LDAP-Administrators angeben.

a. Wenn Sie **Registrierter Name und Kennwort** auswählen, müssen Sie die folgenden Informationen angeben:
   - Geben Sie im Feld **Registrierter Name** den registrierten LDAP-Namen ein, der den Benutzer identifiziert, den das System zur Ausführung von EIM-Operationen verwenden soll.
   - Geben Sie im Feld **Kennwort** das Kennwort für den registrierten Namen ein.
   - Geben Sie im Feld **Kennwort bestätigen** das Kennwort zur Überprüfung ein zweites Mal ein.

b. Wenn Sie **Kerberos-Principal und Kennwort** auswählen, müssen Sie die folgenden Informationen angeben:
   - Geben Sie im Feld **Principal** den Kerberos-Principal-Namen an, den das System zur Ausführung von EIM-Operationen verwenden soll.
   - Geben Sie im Feld **Realm** den vollständig qualifizierten Kerberos-Realm-Namen ein, zu dem der Principal gehört. Der Name des Principals und des Realms identifizieren die Kerberos-Benutzer in der Chiffrierschlüsseltabelle eindeutig. Beispiel: Der Principal `jsmith` im Realm `ordept.myco.com` wird in der Chiffrierschlüsseltabelle als `jsmith@ordept.myco.com` geführt.
   - Geben Sie im Feld **Kennwort** das Kennwort für den Benutzer ein.
   - Geben Sie im Feld **Kennwort bestätigen** das Kennwort zur Überprüfung ein zweites Mal ein.

c. Wenn Sie **Kerberos-Chiffrierschlüsseldatei und -Principal** auswählen, müssen Sie die folgenden Informationen angeben:
   - Geben Sie im Feld **Chiffrierschlüsseldatei** den vollständig qualifizierten Namen des Pfads und der Chiffrierschlüsseldatei ein, die den Kerberos-Principal enthält, den das System zur Ausführung vom EIM-Operationen verwenden soll. Sie können auch auf **Durchsuchen...** klicken, um eine Chiffrierschlüsseldatei aus den Verzeichnissen des integrierten Dateisystems der iSeries auszuwählen.
   - Geben Sie im Feld **Principal** den Kerberos-Principal-Namen an, den das System zur Ausführung von EIM-Operationen verwenden soll.
   - Geben Sie im Feld **Realm** den vollständig qualifizierten Kerberos-Realm-Namen ein, zu dem der Principal gehört. Der Name des Principals und des Realms identifizieren die Kerberos-Benutzer in der Chiffrierschlüsseltabelle eindeutig. Beispiel: Der Principal `jsmith` im Realm `ordept.myco.com` wird in der Chiffrierschlüsseltabelle als `jsmith@ordept.myco.com` geführt.

d. Klicken Sie auf **Verbindung prüfen**, um sicherzustellen, dass der Assistent die angegebenen Benutzerinformationen verwenden kann, um erfolgreich eine Verbindung zum EIM-Domänencontroller herzustellen.

e. Klicken Sie auf **Weiter**.

13. Überprüfen Sie in der Anzeige **Zusammenfassung** die von Ihnen angegebenen Konfigurationsdaten. Wenn alle Informationen richtig sind, klicken Sie auf **Fertig stellen**.

EIM-Konfiguration der Domäne abschließen

Wenn der Assistent beendet wird, fügt er die neue Domäne zum Ordner **Domänenverwaltung** hinzu, womit Sie dann eine EIM-Basiskonfiguration für diesen Server erstellt haben. Um die EIM-Konfiguration für diese Domäne endgültig abzuschließen, müssen Sie jedoch noch folgende Tasks ausführen:

1. Verwenden Sie den EIM-Konfigurationsassistenten auf jedem weiteren Server, den Sie der neuen Domäne hinzufügen möchten.
2. Fügen Sie der EIM-Domäne bei Bedarf EIM-Registerdefinitionen für andere Nicht-iSeries-Server und Anwendungen hinzu, die Sie zur EIM-Domäne hinzufügen möchten. Diese Registerdefinitionen beziehen sich auf die tatsächlichen Benutzerregister, die zur Domäne gehören müssen. Sie können abhängig von Ihren Anforderungen für die EIM-Implementierung entweder Systemregisterdefinitionen hinzufügen oder Anwendungsregisterdefinitionen hinzufügen.
3. Legen Sie abhängig von diesen Anforderungen fest, ob Sie folgende Schritte durchführen müssen:
   a. EIM-Kennungen für jeden einzelnen Benutzer oder jede einzelne Entität der Domäne und Kennungszuordnungen für diese Benutzer oder Entitäten erstellen.
   b. Richtlinienzuordnungen erstellen, um eine Gruppe von Benutzern mit einer einzigen Zielbenutzeridentität abzugleichen.
   c. Eine Kombination dieser Zuordnungen erstellen.
4. Testen Sie die Identitätsabgleiche für Ihre EIM-Konfiguration mit Hilfe der EIM-Funktion Ableich testen.
5. Wenn der einzig definierte EIM-Benutzer der registrierte Name für den LDAP-Administrator ist, dann verfügt Ihr EIM-Benutzer über eine übergeordnete Berechtigung für alle Daten auf dem Directory-Server. Daher können Sie überprüfen, ob es sinnvoll ist, einen oder mehrere registrierte Namen als zusätzliche Benutzer zu erstellen, die über eine besser geeignete EIM-Zugriffssteuerung mit eingeschränkten Rechten für EIM-Daten verfügen. Weitere Informationen zum Erstellen von registrierten Namen für den Directory-Server finden Sie im Abschnitt Distinguished names unter dem Thema zum IBM Directory Server for iSeries (LDAP). Wie viele EIM-Benutzer Sie zusätzlich definieren, hängt davon ab, welche Rolle die Trennung von Sicherheitsaufgaben und Zuständigkeiten bei Ihrer Sicherheitsrichtlinie spielt. Normalerweise können Sie mindestens die beiden folgenden Arten von registrierten Namen erstellen:
   - **Benutzer mit EIM-Administratorzugriffssteuerung**

     Dieser registrierte Name stellt die geeignete Berechtigungsstufe für einen Administrator zur Verfügung, der für die Verwaltung der EIM-Domäne verantwortlich ist. Dieser registrierte Name könnte verwendet werden, um eine Verbindung zum Domänencontroller herzustellen, wenn die Verwaltung der EIM-Domäne über den iSeries Navigator erfolgt.
   - **Mindestens ein Benutzer mit allen folgenden Zugriffssteuerungen**:
     – Kennungsadministrator
     – Registeradministrator
     – EIM-Abgleichsoperationen

     Dieser Benutzer stellt die erforderliche Zugriffssteuerungsstufe für den Systembenutzer zur Verfügung, der EIM-Operationen für das Betriebssystem ausführt.

   Anmerkung: Um diesen neuen registrierten Namen für den Systembenutzer an Stelle des registrierten Namens für den LDAP-Administrator benutzen zu können, müssen die EIM-Konfigurationseigenschaften für den iSeries-Server geändert werden. Unter EIM-Konfigurationseigenschaften verwalten wird erläutert, wie Sie den registrierten Namen des Systembenutzers ändern können.

Möglicherweise sind weitere Tasks erforderlich, wenn Sie eine Basiskonfiguration des Netzwerkauthentifizierungsservice erstellt haben; dies gilt insbesondere, wenn Sie eine Einzelanmeldungsumgebung implementieren. Informationen zu diesen zusätzlichen Arbeitsschritten erhalten Sie, wenn Sie alle Konfigurationsschritte im Szenario: Einzelanmeldung für i5/OS aktivieren durcharbeiten.

System zu einer vorhandenen Domäne hinzufügen

Im Folgenden wird erläutert, wie Sie den EIM-Konfigurationsassistenten (EIM = Enterprise Identity Mapping) auf einem iSeries-System zum Konfigurieren eines Domänencontrollers und zur Erstellung einer EIM-Domäne einsetzen und anschließend mit diesem Assistenten andere iSeries-Server für die Nutzung der Domäne konfigurieren können.

Nachdem Sie eine EIM-Domäne erstellt und auf einem System einen Directory-Server als Domänencontroller konfiguriert haben, können Sie die weiteren iSeries-Server (V5R2 oder später) konfigurieren, um sie der vorhandenen EIM-Domäne hinzuzufügen. Während der Arbeit mit dem Assistenten müssen Sie Informationen über die Domäne angeben, zu denen auch Informationen über die Verbindung zum EIM-Domänencontroller gehören. Wenn Sie ein System mit Hilfe des EIM-Konfigurationsassistenten zu einer vorhandenen Domäne hinzufügen und Sie sich entschieden haben, Kerberos als Bestandteil der EIM-Konfiguration zu konfigurieren, bietet Ihnen der Assistent noch die Option zum Starten des Assistenten für den Netzwerkauthentifizierungsservice an.

Wenn Sie den EIM-Konfigurationsassistenten ausführen, um eine Aufnahme in eine bestimmte Domäne durchzuführen, können Sie die folgenden Tasks ausführen:

- Netzwerkauthentifizierungsservice für das System konfigurieren.
- EIM-Registerdefinitionen für das lokale i5/OS-Register und das Kerberos-Register erstellen.
- System für die Nutzung einer vorhandenen EIM-Domäne konfigurieren.

Um das System einer vorhandenen EIM-Domäne hinzufügen zu können, benötigen Sie die folgenden Sonderberechtigungen:

- Sicherheitsadministrator (*SECADM)
- Berechtigung für alle Objekte (*ALLOBJ)

Führen Sie die folgenden Schritte durch, um den EIM-Konfigurationsassistenten zu starten und ein System zu einer vorhandenen EIM-Domäne hinzuzufügen:

1. Vergewissern Sie sich, dass der Directory-Server auf dem fernen System aktiv ist.
2. Wählen Sie im iSeries Navigator das System aus, für das EIM konfiguriert werden soll, und erweitern Sie **Netzwerk > Enterprise Identity Mapping**.
3. Klicken Sie mit der rechten Maustaste auf **Konfiguration**, und wählen Sie **Konfigurieren...** aus, um den EIM-Konfigurationsassistenten zu starten.

   Anmerkung: Diese Option lautet **Rekonfigurieren...**, wenn EIM bereits zuvor auf dem System konfiguriert wurde.
4. Wählen Sie auf der **Begrüßungsseite** des Assistenten **Einer vorhandenen Domäne hinzufügen** aus, und klicken Sie auf **Weiter**.

   Anmerkung: Wenn der Netzwerkauthentifizierungsservice derzeit nicht auf dem iSeries-Server konfiguriert ist oder weitere Informationen für den Netzwerkauthentifizierungsservice benötigt werden, um eine Einzelanmeldungsumgebung zu konfigurieren, wird die Seite **Konfiguration des Netzwerkauthentifizierungsservice** angezeigt. Mit Hilfe dieser Seite kann der Assistent für den Netzwerkauthentifizierungsservice gestartet werden, so dass Sie den Netzwerkauthentifizierungsservice konfigurieren können. Sie können die Konfiguration des Netzwerkauthentifizierungsservice aber auch zu einem späteren Zeitpunkt durchführen, indem Sie den Konfigurationsassistenten für diesen Service über den iSeries Navigator aufrufen. Wenn Sie die Konfiguration des Netzwerkauthentifizierungsservice abgeschlossen haben, wird der EIM-Konfigurationsassistent fortgesetzt.
5. Führen Sie die folgenden Schritte durch, um den Netzwerkauthentifizierungsservice zu konfigurieren:

a. Wählen Sie auf der Seite **Netzwerkauthentifizierungsservice konfigurieren** die Option **Ja** aus, um den Assistenten für den Netzwerkauthentifizierungsservice zu starten. Mit diesem Assistenten können Sie mehrere i5/OS-Schnittstellen und -Services für die Nutzung eines Kerberos-Realms sowie eine Einzelanmeldungsumgebung konfigurieren, in der sowohl EIM als auch der Netzwerkauthentifizierungsservice verwendet werden.

b. Geben Sie auf der Seite **Realm-Informationen angeben** im Feld **Standard-Realm** den Namen des Standard-Realms ein. Wenn Sie Microsoft Active Directory für die Kerberos-Authentifizierung verwenden, wählen Sie **Microsoft Active Directory wird für Kerberos-Authentifizierung verwendet** aus, und klicken Sie auf **Weiter**.

c. Geben Sie auf der Seite **KDC-Informationen angeben** den vollständig qualifizierten Namen des Kerberos-Servers für diesen Realm im Feld **KDC** und 88 im Feld **Port** ein, und klicken Sie auf **Weiter**.

d. Wählen Sie auf der Seite **Kennwortserverinformationen angeben** entweder **Ja** oder **Nein** für die Definition eines Kennwortservers aus. Mit dem Kennwortserver können Principals Kennwörter auf dem Kerberos-Server ändern. Wenn Sie **Ja** auswählen, geben Sie den Namen des Kennwortservers im Feld **Kennwortserver** ein. Übernehmen Sie den Standardwert 464 im Feld **Port**, und klicken Sie auf Weiter.

e. Wählen Sie auf der Seite **Chiffrierschlüsseleinträge auswählen** die **i5/OS Kerberos-Authentifizierung** aus, und klicken Sie dann auf **Weiter**.

   Anmerkung: Sie können außerdem Chiffrierschlüsseleinträge für IBM Directory Server for iSeries (LDAP), iSeries NetServer und für IBM HTTP-Server für iSeries erstellen, wenn diese Services mit der Kerberos-Authentifizierung arbeiten sollen. Möglicherweise müssen zusätzliche Konfigurationsschritte für diese Services ausgeführt werden, bevor Sie die Kerberos-Authentifizierung verwenden können.

f. Geben Sie auf der Seite **i5/OS-Chiffrierschlüsseleintrag erstellen** ein Kennwort ein, und bestätigen Sie es. Klicken Sie anschließend auf **Weiter**. Dieses Kennwort verwenden Sie auch, wenn Sie die i5/OS-Principals zum Kerberos-Server hinzufügen.

g. Optional: Wählen Sie **Ja** auf der Seite **Stapeldatei erstellen** aus, geben Sie die folgenden Informationen an, und klicken Sie auf **Weiter**:

   - Aktualisieren Sie im Feld **Stapeldatei** den Verzeichnispfad. Klicken Sie auf **Durchsuchen**, um den entsprechenden Verzeichnispfad zu lokalisieren, oder editieren Sie den Pfad im Feld **Stapeldatei**.
   - Wählen Sie **Ja** im Feld **Kennwort einfügen** aus. Dies garantiert, dass alle Kennwörter, die dem i5/OS-Service-Principal zugeordnet sind, in die Stapeldatei eingefügt werden. Beachten Sie, dass Kennwörter in Klartext angezeigt werden und von jedem gelesen werden können, der über den Lesezugriff für die Stapeldatei verfügt. Daher ist es außerordentlich wichtig, dass Sie die Stapeldatei sofort nach Gebrauch wieder vom Kerberos-Server und dem PC löschen. Wenn Sie das Kennwort nicht einfügen, werden Sie bei der Ausführung der Stapeldatei zur Eingabe des Kennworts aufgefordert.

     Anmerkung: Sie können die vom Assistenten generierten Service-Principals auch manuell zum Microsoft Active Directory hinzufügen. Anweisungen hierzu finden Sie unter i5/OS-Principals zum Kerberos-Server hinzufügen.
   - Überprüfen Sie die Konfigurationsdetails für den Netzwerkauthentifizierungsservice auf der Seite **Zusammenfassung**, und klicken Sie auf **Fertig stellen**, um zum EIM-Konfigurationsassistenten zurückzukehren.

6. Geben Sie auf der Seite **Domänencontroller angeben** die folgenden Informationen ein:

   Anmerkung: Der als Domänencontroller fungierende Directory-Server muss aktiv sein, damit diese EIM-Konfiguration erfolgreich abgeschlossen werden kann.

a. Geben Sie im Feld **Name des Domänencontrollers** den Namen des Systems ein, das als Domänencontroller für die EIM-Domäne fungiert, dem der iSeries-Server hinzugefügt werden soll.

b. Klicken Sie auf **Sichere Verbindung (SSL oder TLS) verwenden**, um eine sichere Verbindung zum EIM-Domänencontroller herzustellen. Daraufhin wird dann entweder mit SSL (Secure Sockets Layer) oder mit TLS (Transport Layer Security) eine sichere Verbindung hergestellt, um die Übertragung von EIM-Daten über ein ungesichertes Netzwerk, wie beispielsweise das Internet, zu schützen.

   Anmerkung: Sie müssen sicherstellen, dass der EIM-Domänencontroller für die Verwendung einer sicheren Verbindung konfiguriert ist. Andernfalls kann die Verbindung zum Domänencontroller möglicherweise nicht hergestellt werden.

c. Geben Sie im Feld **Port** den TCP/IP-Port ein, auf dem der Directory-Server empfangsbereit ist. Wenn **Sichere Verbindung verwenden** ausgewählt ist, lautet der Standardport 636; andernfalls ist 389 der Standardport.

d. Klicken Sie auf **Verbindung prüfen**, um sicherzustellen, dass der Assistent die angegebenen Informationen verwenden kann, um erfolgreich eine Verbindung zum EIM-Domänencontroller herzustellen.

e. Klicken Sie auf **Weiter**.

7. Wählen Sie auf der Seite **Benutzer für Verbindung angeben** einen **Benutzerstatus** für die Verbindung aus. Sie können einen der folgenden Benutzertypen auswählen: **Registrierter Name und Kennwort**, **Kerberos-Chiffrierschlüsseldatei und Principal**, **Kerberos-Principal und Kennwort** oder **Benutzerprofil und Kennwort**. Die beiden Kerberos-Benutzerstatusarten sind nur verfügbar, wenn der Netzwerkauthentifizierungsservice für das lokale iSeries-System konfiguriert ist. Der von Ihnen ausgewählte Benutzerstatus bestimmt die übrigen Informationen, die Sie noch auf der Seite eingeben müssen, folgendermaßen:

   Anmerkung: Wenn Sie sicherzustellen möchten, dass der Assistent über ausreichende Berechtigungen verfügt, um die erforderlichen EIM-Objekte im Verzeichnis zu erstellen, wählen Sie als Benutzerstatus **Registrierter Name und Kennwort** aus, und geben Sie den registrierten Namen und das Kennwort des LDAP-Administrators als Benutzer an.

   Sie können einen anderen Benutzer für die Verbindung angeben; dieser muss jedoch über die entsprechende LDAP-Administratorberechtigung für den fernen Directory-Server verfügen.

   - Wenn Sie **Registrierter Name und Kennwort** auswählen, müssen Sie die folgenden Informationen angeben:
     - Geben Sie im Feld **Registrierter Name** den registrierten LDAP-Namen (DN) ein, der den Benutzer identifiziert, der berechtigt ist, Objekte im lokalen Namespace des LDAP-Servers zu erstellen. Wenn Sie diesen Assistenten bereits in einem früheren Schritt für die Konfiguration des LDAP-Servers verwendet haben, geben Sie den registrierten Namen des LDAP-Administrators ein, den Sie in diesem Schritt erstellt haben.
     - Geben Sie im Feld **Kennwort** das Kennwort für den registrierten Namen ein.
     - Geben Sie im Feld **Kennwort bestätigen** das Kennwort zur Überprüfung ein zweites Mal ein.
   - Wenn Sie **Kerberos-Chiffrierschlüsseldatei und -Principal** auswählen, müssen Sie die folgenden Informationen angeben:
     - Geben Sie im Feld **Chiffrierschlüsseldatei** den vollständig qualifizierten Namen des Pfads und der Chiffrierschlüsseldatei ein, die den Kerberos-Principal enthält, den der Assistent beim Verbindungsaufbau zur EIM-Domäne verwenden soll. Sie können auch auf **Durchsuchen...** klicken, um eine Chiffrierschlüsseldatei aus den Verzeichnissen des integrierten Dateisystems der iSeries auszuwählen.
     - Geben Sie im Feld **Principal** den Namen des Kerberos-Principals ein, mit dem der Benutzer identifiziert werden soll.

– Geben Sie im Feld **Realm** den vollständig qualifizierten Kerberos-Realm-Namen ein, zu dem der Principal gehört. Der Name des Principals und des Realms identifizieren die Kerberos-Benutzer in der Chiffrierschlüsseltabelle eindeutig. Beispiel: Der Principal `jsmith` im Realm `ordept.myco.com` wird in der Chiffrierschlüsseltabelle als `jsmith@ordept.myco.com` geführt.

- Wenn Sie **Kerberos-Principal und Kennwort** auswählen, müssen Sie die folgenden Informationen angeben:
  – Geben Sie im Feld **Principal** den Namen des Kerberos-Principals ein, den der Assistent beim Verbindungsaufbau zur EIM-Domäne verwenden soll.
  – Geben Sie im Feld **Realm** den vollständig qualifizierten Kerberos-Realm-Namen ein, zu dem der Principal gehört. Der Name des Principals und des Realms identifizieren die Kerberos-Benutzer in der Chiffrierschlüsseltabelle eindeutig. Beispiel: Der Principal `jsmith` im Realm `ordept.myco.com` wird in der Chiffrierschlüsseltabelle als `jsmith@ordept.myco.com` geführt.
  – Geben Sie im Feld **Kennwort** das Kennwort für den Kerberos-Principal ein.
  – Geben Sie im Feld **Kennwort bestätigen** das Kennwort zur Überprüfung ein zweites Mal ein.
- Wenn Sie **Benutzerprofil und Kennwort** auswählen, müssen Sie die folgenden Informationen angeben:
  – Geben Sie im Feld **Benutzerprofil** den Namen des Benutzerprofils ein, den der Assistent beim Verbindungsaufbau zur EIM-Domäne verwenden soll.
  – Geben Sie im Feld **Kennwort** das Kennwort für das Benutzerprofil ein.
  – Geben Sie im Feld **Kennwort bestätigen** das Kennwort zur Überprüfung ein zweites Mal ein.
- Klicken Sie auf **Verbindung prüfen**, um sicherzustellen, dass der Assistent die angegebenen Benutzerinformationen verwenden kann, um erfolgreich eine Verbindung zum EIM-Domänencontroller herzustellen.
- Klicken Sie auf **Weiter**.

8. Wählen Sie auf der Seite **Domäne angeben** den Namen der Domäne aus, zu dem das System hinzugefügt werden soll, und klicken Sie auf **Weiter**.
9. Geben Sie auf der Seite **Registerinformationen** an, ob lokale Benutzerregister der EIM-Domäne als Registerdefinitionen hinzugefügt werden sollen. Wählen Sie eine oder beide der folgenden Registertypen aus:
   - Wählen Sie **Lokales i5/OS** aus, um eine Registerdefinition für das lokale Register hinzuzufügen. Übernehmen Sie den im Feld enthaltenen Standardwert für den Namen der Registerdefinition oder geben Sie einen anderen Namen ein. Der EIM-Registername ist eine beliebige Zeichenfolge, die für den Registertyp und eine bestimmte Instanz dieses Registers steht.

     Anmerkung: Sie müssen die lokale i5/OS-Registerdefinition nicht zum jetzigen Zeitpunkt erstellen. Wenn Sie die i5/OS-Registerdefinition später erstellen möchten, müssen Sie die Systemregisterdefinition hinzufügen und die EIM-Konfigurationsmerkmale aktualisieren.
   - Wählen Sie **Kerberos** aus, um eine Registerdefinition für ein Kerberos-Register hinzuzufügen. Übernehmen Sie den im Feld enthaltenen Standardwert für den Namen der Registerdefinition oder geben Sie einen anderen Namen ein. Der Standardname für die Registerdefinition entspricht dem Realm-Namen. Wenn Sie den Standardnamen übernehmen (sprich für den Kerberos-Registernamen denselben Namen verwenden wie für den Realm), können Sie die Leistung beim Abrufen von Informationen aus dem Register erhöhen. Wählen Sie ggf. **Bei Kerberos-Benutzeridentitäten muss die Groß-/Kleinschreibung beachtet werden** aus.

     Anmerkung: Wenn Sie den EIM-Konfigurationsassistenten auf einem anderen System verwendet haben, um eine Registerdefinition für das Kerberos-Register hinzuzufügen, für das dieses iSeries-System über einen Service-Principal verfügt, müssen Sie keine Kerberos-Registerdefinition als Bestandteil dieser Konfiguration hinzufügen. Sie müssen jedoch den Namen dieses Kerberos-Registers in den Konfigurationsmerkmalen für dieses System angeben, nachdem Sie den Assistenten beendet haben.

- Klicken Sie auf **Weiter**.

10. Wählen Sie auf der Seite **EIM-Systembenutzer angeben** einen **Benutzerstatus** aus, den das System verwenden soll, wenn es EIM-Operationen für Betriebssystemfunktionen ausführt. Diese Operationen umfassen Abgleichsuchoperationen sowie Löschoperationen für Zuordnungen, die ausgeführt werden, wenn ein lokales i5/OS-Benutzerprofil gelöscht wird. Sie können eine der folgenden Benutzerstatusarten auswählen: **Registrierter Name und Kennwort**, **Kerberos-Chiffrierschlüsseldatei und Principal** oder **Kerberos-Principal und Kennwort**. Welchen Benutzerstatus Sie im Einzelnen auswählen können, hängt von der aktuellen Systemkonfiguration ab. Wenn beispielsweise der Netzwerkauthentifizierungsservice nicht für das System konfiguriert ist, stehen möglicherweise keine Benutzer mit dem Status ″Kerberos″ zur Verfügung. Der von Ihnen ausgewählte Benutzerstatus bestimmt die übrigen Informationen, die Sie noch auf der Seite eingeben müssen, folgendermaßen:

    Anmerkung: Sie müssen einen Benutzer angeben, der momentan in dem Directory-Server definiert ist, auf dem sich der EIM-Domänencontroller befindet. Der Benutzer muss mindestens über die erforderlichen Privilegien verfügen, um die Abgleichsuchfunktion und die Registerverwaltung für das lokale Benutzerregister ausführen zu können. Ist dies nicht der Fall, können bestimmte Betriebssystemfunktionen im Zusammenhang mit der Einzelanmeldung und dem Löschen von Benutzerprofilen fehlschlagen.

    - Wenn Sie **Registrierter Name und Kennwort** auswählen, müssen Sie die folgenden Informationen angeben:
      - Geben Sie im Feld **Registrierter Name** den registrierten LDAP-Namen ein, der den Benutzer identifiziert, den das System zur Ausführung von EIM-Operationen verwenden soll.
      - Geben Sie im Feld **Kennwort** das Kennwort für den registrierten Namen ein.
      - Geben Sie im Feld **Kennwort bestätigen** das Kennwort zur Überprüfung ein zweites Mal ein.
    - Wenn Sie **Kerberos-Principal und Kennwort** auswählen, müssen Sie die folgenden Informationen angeben:
      - Geben Sie im Feld **Principal** den Kerberos-Principal-Namen an, den das System zur Ausführung von EIM-Operationen verwenden soll.
      - Geben Sie im Feld **Realm** den vollständig qualifizierten Kerberos-Realm-Namen ein, zu dem der Principal gehört. Der Name des Principals und des Realms identifizieren die Kerberos-Benutzer in der Chiffrierschlüsseltabelle eindeutig. Beispiel: Der Principal `jsmith` im Realm `ordept.myco.com` wird in der Chiffrierschlüsseltabelle als `jsmith@ordept.myco.com` geführt.
      - Geben Sie im Feld **Kennwort** das Kennwort für den Benutzer ein.
      - Geben Sie im Feld **Kennwort bestätigen** das Kennwort zur Überprüfung ein zweites Mal ein.
    - Wenn Sie **Kerberos-Chiffrierschlüsseldatei und -Principal** auswählen, müssen Sie die folgenden Informationen angeben:
      - Geben Sie im Feld **Chiffrierschlüsseldatei** den vollständig qualifizierten Namen des Pfads und der Chiffrierschlüsseldatei ein, die den Kerberos-Principal enthält, den das System zur Ausführung vom EIM-Operationen verwenden soll. Sie können auch auf **Durchsuchen...** klicken, um eine Chiffrierschlüsseldatei aus den Verzeichnissen des integrierten Dateisystems der iSeries auszuwählen.
      - Geben Sie im Feld **Principal** den Kerberos-Principal-Namen an, den das System zur Ausführung von EIM-Operationen verwenden soll.
      - Geben Sie im Feld **Realm** den vollständig qualifizierten Kerberos-Realm-Namen ein, zu dem der Principal gehört. Der Name des Principals und des Realms identifizieren die Kerberos-Benutzer in der Chiffrierschlüsseltabelle eindeutig. Beispiel: Der Principal `jsmith` im Realm `ordept.myco.com` wird in der Chiffrierschlüsseltabelle als `jsmith@ordept.myco.com` geführt.
    - Klicken Sie auf **Verbindung prüfen**, um sicherzustellen, dass der Assistent die angegebenen Benutzerinformationen verwenden kann, um erfolgreich eine Verbindung zum EIM-Domänencontroller herzustellen.
    - Klicken Sie auf **Weiter**.

11. Überprüfen Sie auf der Seite **Zusammenfassung** die von Ihnen angegebenen Konfigurationsdaten. Wenn alle Informationen richtig sind, klicken Sie auf **Fertig stellen**.

EIM-Konfiguration der Domäne abschließen

Wenn der Assistent beendet wird, fügt er die Domäne zum Ordner **Domänenverwaltung** hinzu, womit Sie dann eine EIM-Basiskonfiguration für diesen Server erstellt haben. Um die EIM-Konfiguration für diese Domäne endgültig abzuschließen, müssen Sie jedoch möglicherweise noch folgende Tasks ausführen:

1. Fügen Sie der EIM-Domäne bei Bedarf EIM-Registerdefinitionen für andere Nicht-iSeries-Server und Anwendungen hinzu, die Sie zur EIM-Domäne hinzufügen möchten. Diese Registerdefinitionen beziehen sich auf die tatsächlichen Benutzerregister, die zur Domäne gehören müssen. Sie können abhängig von Ihren Anforderungen für die EIM-Implementierung entweder Systemregisterdefinitionen hinzufügen oder Anwendungsregisterdefinitionen hinzufügen.
2. Legen Sie abhängig von diesen Anforderungen fest, ob Sie folgende Schritte durchführen müssen:
   - EIM-Kennungen für jeden einzelnen Benutzer oder jede einzelne Entität der Domäne und Kennungszuordnungen für diese Benutzer oder Entitäten erstellen.
   - Richtlinienzuordnungen erstellen, um eine Gruppe von Benutzern mit einer einzigen Zielbenutzeridentität abzugleichen.
   - Eine Kombination aus beiden Möglichkeiten erstellen.
3. Testen Sie die Identitätsabgleiche für Ihre EIM-Konfiguration mit Hilfe der EIM-Funktion Ableich testen.
4. Wenn der einzig definierte EIM-Benutzer der registrierte Name für den LDAP-Administrator ist, dann verfügt Ihr EIM-Benutzer über eine übergeordnete Berechtigung für alle Daten auf dem Directory-Server. Daher könnten Sie erwägen, einen oder mehrere registrierten Namen als zusätzliche Benutzer zu erstellen, die über eine besser geeignete EIM-Zugriffssteuerung mit eingeschränkten Rechten für EIM-Daten verfügen. Weitere Informationen zum Erstellen von registrierten Namen für den Directory-Server finden Sie im Abschnitt Distinguished names unter dem Thema zum IBM Directory Server for iSeries (LDAP). Wie viele EIM-Benutzer Sie zusätzlich definieren, hängt davon ab, welche Rolle die Trennung von Sicherheitsaufgaben und Zuständigkeiten bei Ihrer Sicherheitsrichtlinie spielt. Normalerweise können Sie mindestens die beiden folgenden Arten von registrierten Namen erstellen:
   - **Benutzer mit EIM-Administratorzugriffssteuerung**

     Dieser registrierte Name stellt die geeignete Berechtigungsstufe für einen Administrator zur Verfügung, der für die Verwaltung der EIM-Domäne verantwortlich ist. Dieser registrierte Name könnte verwendet werden, um eine Verbindung zum Domänencontroller herzustellen, wenn die Verwaltung der EIM-Domäne über den iSeries Navigator erfolgt.
   - **Mindestens ein Benutzer mit allen folgenden Zugriffssteuerungen**:
     – Kennungsadministrator
     – Registeradministrator
     – EIM-Abgleichsoperationen

     Dieser Benutzer stellt die erforderliche Zugriffssteuerungsstufe für den Systembenutzer zur Verfügung, der EIM-Operationen für das Betriebssystem ausführt.

   Anmerkung: Um diesen neuen registrierten Namen für den Systembenutzer an Stelle des registrierten Namens für den LDAP-Administrator benutzen zu können, müssen die EIM-Konfigurationseigenschaften für den iSeries-Server geändert werden. Unter EIM-Konfigurationseigenschaften verwalten wird erläutert, wie Sie den registrierten Namen des Systembenutzers ändern können.

Möglicherweise sind weitere Tasks erforderlich, wenn Sie eine Basiskonfiguration des Netzwerkauthentifizierungsservice erstellt haben; dies gilt insbesondere, wenn Sie eine Einzelanmeldungsumgebung imple-

mentieren. Informationen zu diesen zusätzlichen Arbeitsschritten erhalten Sie, wenn Sie alle Konfigurationsschritte im Szenario: Einzelanmeldung für i5/OS aktivieren durcharbeiten.

Sichere Verbindung zum EIM-Domänencontroller konfigurieren

Im Folgenden wird erläutert, wie Sie über SSL oder TLS eine sichere Verbindung zu einem Domänencontroller aufbauen können.

Sie können mit Hilfe von SSL (Secure Sockets Layer) oder TLS (Transport Layer Security Protocol) eine sichere Verbindung zum EIM-Domänencontroller (EIM = Enterprise Identity Mapping) herstellen, um die Übertragung von EIM-Daten zu schützen.

Führen Sie folgende Tasks aus, um SSL oder TLS für EIM zu konfigurieren:

1. Verwenden Sie ggf. Digital Certificate Manager (DCM), um für den Directory-Server ein Zertifikat für SSL zu erstellen (siehe hierzu Zertifikate erstmals definieren).
2. Aktivieren Sie SSL für den lokalen Directory-Server, auf dem sich der EIM-Domänencontroller befindet (siehe hierzu Enable SSL for the local directory server).
3. Aktualisieren Sie die EIM-Konfigurationseigenschaften, indem Sie angeben, dass der iSeries-Server eine sichere SSL-Verbindung verwendet. Führen Sie die folgenden Schritte durch, um die EIM-Konfigurationseigenschaften zu aktualisieren:
   a. Wählen Sie im iSeries Navigator das System aus, auf dem Sie EIM konfiguriert haben, und erweitern Sie **Netzwerk → Enterprise Identity Mapping**.
   b. Klicken Sie mit der rechten Maustaste auf **Konfiguration**, und wählen Sie **Eigenschaften** aus.
   c. Wählen Sie auf der Seite **Domäne** die Option **Sichere Verbindung (SSL oder TLS) verwenden** aus, geben Sie den gesicherten Port an, auf dem Ihr Directory-Server empfangsbereit ist, oder übernehmen Sie den Standardwert `636` im Feld **Port**, und klicken Sie auf **OK**.
4. Aktualisieren Sie die Eigenschaften für jede EIM-Domäne, indem Sie angeben, dass EIM eine SSL-Verbindung verwendet, wenn die Domäne über den iSeries Navigator verwaltet wird. Führen Sie die folgenden Schritte durch, um die EIM-Domäneneigenschaften zu aktualisieren:
   a. Wählen Sie im iSeries Navigator das System aus, auf dem Sie EIM konfiguriert haben, und erweitern Sie **Netzwerk → Enterprise Identity Mapping → Domänenverwaltung**.
   b. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
      - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter EIM-Domäne zu Domänenverwaltung hinzufügen nach.
      - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
   c. Klicken Sie mit der rechten Maustaste auf die EIM-Domäne, mit der Sie momentan verbunden sind, und wählen Sie **Eigenschaften** aus.
   d. Wählen Sie auf der Seite **Domäne** die Option **Sichere Verbindung (SSL oder TLS) verwenden** aus, geben Sie den gesicherten Port an, auf dem Ihr Directory-Server empfangsbereit ist, oder übernehmen Sie den Standardwert `636` im Feld **Port**, und klicken Sie auf **OK**.

Enterprise Identity Mapping verwalten

In diesem Abschnitt wird beschrieben, wie Sie Ihre EIM-Domäne und die EIM-Domänendaten verwalten können. Dies umfasst die Verwaltung von EIM-Domänen, Kennungen, Zuordnungen, Registerdefinitionen, EIM-Zugriffssteuerung usw.

Nachdem Sie Enterprise Identity Mapping (EIM) auf Ihrem iSeries-Server konfiguriert haben, müssen Sie zahlreiche administrative Tasks zur Verwaltung Ihrer EIM-Domäne und der Daten für diese Domäne ausführen. Die folgenden Abschnitte enthalten Informationen, die die Verwaltung von EIM in Ihrem Unternehmen betreffen.

EIM-Domänen verwalten

Im Folgenden wird erläutert, wie die EIM-Domänen (EIM = Enterprise Identity Mapping) und die EIM-Domäneneigenschaften verwaltet werden.

Alle EIM-Domänen können mit Hilfe des iSeries Navigator verwaltet werden. Damit eine EIM-Domäne verwaltet werden kann, muss sie im Ordner **Domänenverwaltung** unter dem Ordner **Netzwerk** im iSeries Navigator aufgelistet sein oder von Ihnen hinzugefügt werden. Wenn Sie mit dem EIM-Konfigurationsassistenten eine neue EIM-Domäne erstellen und konfigurieren, wird diese automatisch dem Ordner **Domänenverwaltung** hinzugefügt, so dass Sie die Domäne und die darin enthaltenen Informationen verwalten können.

Für die Verwaltung einer EIM-Domäne kann eine beliebige iSeries-Verbindung an einem beliebigen Standort im selben Netzwerk genutzt werden, wobei die verwendete iSeries nicht einmal zur Domäne gehören muss.

Für eine Domäne können die folgenden Verwaltungstasks ausgeführt werden:

EIM-Domäne zum Ordner Domänenverwaltung hinzufügen

Für diese Task benötigen Sie die Sonderberechtigung *SECADM; außerdem muss die Domäne, die dem Ordner **Domänenverwaltung** hinzugefügt werden soll, bereits vorhanden sein.

Führen Sie die folgenden Schritte durch, um dem Ordner **Domänenverwaltung** eine EIM-Domäne hinzuzufügen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping**.
2. Klicken Sie mit der rechten Maustaste auf **Domänenverwaltung**, und wählen Sie **Domäne hinzufügen...** aus.
3. Geben Sie im Dialog **Domäne hinzufügen** die erforderlichen Domänen- und Verbindungsinformationen an. Sie können auch auf **Durchsuchen...** klicken, um eine Liste der Domänen anzuzeigen, die vom angegebenen Domänencontroller verwaltet werden.

   Anmerkung: Wenn Sie auf **Durchsuchen...** klicken, wird der Dialog **Verbindung zu EIM-Domänencontroller** angezeigt. Um die Liste der Domänen anzuzeigen, müssen Sie mit der Zugriffssteuerung des LDAP-Administrators oder des EIM-Administrators eine Verbindung zum Domänencontroller herstellen. Der Inhalt der Domänenliste richtet sich danach, welche EIM-Zugriffssteuerung Sie besitzen. Wenn Sie über den LDAP-Administratorzugriff verfügen, können Sie eine Liste aller Domänen anzeigen, die vom Domänencontroller verwaltet werden. Andernfalls enthält die Liste nur diejenigen Domänen, für die Sie den EIM-Administratorzugriff besitzen.
4. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen benötigen.
5. Klicken Sie auf **OK**, um die Domäne hinzuzufügen.

Verbindung zu einer EIM-Domäne herstellen

Bevor Sie mit einer EIM-Domäne arbeiten können, müssen Sie zunächst eine Verbindung zum entsprechenden EIM-Domänencontroller herstellen. Sie können selbst dann eine Verbindung zu einer EIM-Domäne herstellen, wenn Ihr iSeries-Server derzeit nicht für die Nutzung dieser Domäne konfiguriert ist.

Um eine Verbindung zum EIM-Domänencontroller herstellen zu können, muss der jeweilige Benutzer Mitglied einer Zugriffssteuerungsgruppe sein (siehe „EIM-Zugriffssteuerung" auf Seite 42). Die Mitgliedschaft in einer EIM-Zugriffssteuerungsgruppe bestimmt, welche Tasks ein Benutzer in der Domäne ausführen und welche EIM-Daten er anzeigen oder ändern kann.

Führen Sie die folgenden Schritte durch, um eine Verbindung zu einer EIM-Domäne herzustellen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Klicken Sie mit der rechten Maustaste auf die Domäne, zu der Sie eine Verbindung herstellen möchten.

   Anmerkung: Wird die Domäne, mit der Sie arbeiten möchten, nicht unter **Domänenverwaltung** aufgelistet, müssen Sie sie hinzufügen (siehe „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96).
3. Klicken Sie mit der rechten Maustaste auf die EIM-Domäne, zu der Sie eine Verbindung herstellen möchten, und wählen Sie **Verbindung herstellen...** aus.
4. Geben Sie im Dialog **Verbindung zu EIM-Domänencontroller** den **Benutzerstatus** sowie die erforderlichen Identifikationsdaten für den Benutzer an, und wählen Sie eine Kennwortoption für die Verbindung zum Domänencontroller aus.
5. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen benötigen.
6. Klicken Sie auf **OK**, um die Verbindung zum Domänencontroller herzustellen.

Richtlinienzuordnungen für eine Domäne aktivieren

Eine Richtlinienzuordnung bietet eine Möglichkeit, n:1-Abgleiche für die Fälle zu erstellen, in denen keine Zuordnungen zwischen Benutzeridentitäten und EIM-Kennungen vorhanden sind. Mit Hilfe einer Richtlinienzuordnung kann eine Quellengruppe aus mehreren Benutzeridentitäten (keine einzelne Benutzeridentität) mit einer einzigen Zielbenutzeridentität in einem angegebenen Zielbenutzerregister abgeglichen werden. Bevor Sie jedoch Richtlinienzuordnungen verwenden können, müssen Sie sich vergewissern, dass Sie die Domäne dafür aktiviert haben, Richtlinienzuordnungen für Abgleichsuchoperationen zu verwenden.

Um die Aktivierung durchführen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die Zugriffssteuerung des EIM-Administrators verfügen.

Führen Sie die folgenden Schritte durch, um Abgleichsuchen mit Hilfe von Richtlinienzuordnungen für eine Domäne zu aktivieren:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Klicken Sie mit der rechten Maustaste auf die EIM-Domäne, in der Sie arbeiten möchten, und wählen Sie **Abgleichrichtlinie...** aus.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach. (Die Option **Abgleichrichtlinie...** ist erst verfügbar, wenn die Verbindung zur Domäne hergestellt ist.)
3. Wählen Sie auf der Seite **Allgemein** die Option **Abgleichsuchen mit Hilfe von Richtlinienzuordnungen für Domäne aktivieren** aus.
4. Klicken Sie auf **OK**.

Anmerkung: Sie müssen Abgleichsuchen und die Verwendung von Richtlinienzuordnungen für jede Zielregisterdefinition aktivieren, für die Richtlinienzuordnungen definiert sind. Wenn Sie keine Abgleichsuchen für eine Zielregisterdefinition aktivieren, kann dieses Register keine EIM-Abgleichsuchoperationen nutzen. Wenn Sie nicht angeben, dass das Zielregister Richtlinienzuordnungen verwenden kann, werden alle definierten Richtlinienzuordnungen für dieses Register von den EIM-Abgleichsuchoperationen ignoriert.

Zugehörige Konzepte

„Unterstützung und Aktivierung von EIM-Abgleichrichtlinien" auf Seite 41
In diesem Abschnitt wird erläutert, wie Richtlinienzuordnungen für Domänen aktiviert und inaktiviert werden können.

EIM-Abgleiche testen

Die EIM-Unterstützungsfunktion für das Testen von Abgleichen ermöglicht es Ihnen, EIM-Abgleichsuchoperationen für Ihre EIM-Konfiguration durchzuführen. Mit Hilfe des Tests können Sie überprüfen, ob die Zuordnung einer bestimmten Quellenbenutzeridentität zur entsprechenden Zielbenutzeridentität richtig ist. Auf diese Weise wird sichergestellt, dass EIM-Abgleichsuchoperationen anhand der angegebenen Informationen die richtige Zielbenutzeridentität zurückgeben können.

Zur Durchführung eines Abgleichstests müssen Sie mit der EIM-Domäne verbunden sein, in der Sie arbeiten möchten, und über die EIM-Zugriffssteuerung für einen der folgenden Aufgabenbereiche verfügen:

- EIM-Administrator
- Kennungsadministrator
- Registeradministrator
- EIM-Abgleichsuchoperationen

Führen Sie die folgenden Schritte durch, um Ihre EIM-Konfiguration mit Hilfe der Abgleichtestunterstützung zu testen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter EIM-Domäne zu Domänenverwaltung hinzufügen nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Klicken Sie mit der rechten Maustaste auf die EIM-Domäne, mit der Sie verbunden sind, und wählen Sie **Abgleich testen...** aus.
4. Geben Sie im Dialog **Abgleich testen** die folgenden Informationen ein:
   a. Geben Sie im Feld **Quellenregister** den Namen der Registerdefinition ein, die sich auf das Benutzerregister bezieht, das als Quelle der Abgleichsuchoperation für den Test dienen soll.
   b. Geben Sie im Feld **Quellenbenutzer** den Namen der Benutzeridentität ein, die als Quelle der Abgleichsuchoperation für den Test dienen soll.
   c. Geben Sie im Feld **Zielregister** den Namen der Registerdefinition ein, die sich auf das Benutzerregister bezieht, das als Ziel der Abgleichsuchoperation für den Test dienen soll.
   d. Optional: Geben Sie im Feld **Suchinformationen** alle für den Zielbenutzer definierten Suchinformationen ein.
5. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen benötigen.
6. Klicken Sie auf **Test**, und prüfen Sie die angezeigten Ergebnisse der Abgleichsuchoperation.

   Anmerkung: Wenn die Abgleichsuchoperation mehrdeutige Ergebnisse zurückgibt, wird der Dialog "Abgleich testen - Ergebnisse" aufgerufen, in dem eine Fehlernachricht und eine Liste der Zielbenutzer aufgeführt ist, die von der Suchoperation gefunden wurden.

   a. Um das Problem mehrdeutiger Ergebnisse zu beheben, müssen Sie einen Zielbenutzer auswählen und dann auf **Details** klicken.
   b. Daraufhin wird der Dialog "Abgleich testen - Details" aufgerufen, in dem Informationen zu den Ergebnissen der Abgleichsuchoperation für den angegebenen Zielbenutzer aufgelistet sind. Klicken Sie auf "Hilfe", wenn Sie weiterführende Informationen zu den Ergebnissen der Abgleichsuchoperation benötigen.
   c. Klicken Sie auf **Schließen**, um den Dialog **Abgleich testen - Ergebnisse** zu verlassen.
7. Fahren Sie mit dem Testen Ihrer Konfiguration fort oder klicken Sie auf **Schließen**, um den Test zu verlassen.

Mit Testergebnissen arbeiten und Probleme beheben:

Während des Testlaufs wird eine Zielbenutzeridentität zurückgegeben, wenn eine Zuordnung zwischen der Quellenbenutzeridentität und dem Zielbenutzerregister gefunden wird, das der Administrator angegeben hat. Der Test gibt auch Auskunft über den Typ der Zuordnung zwischen den beiden Benutzeridentitäten. Wenn der Testprozess keine Zuordnung anhand der angegebenen Informationen finden kann, gibt er die Zielbenutzeridentität `Keine` zurück.

Genau wie jede EIM-Abgleichsuchoperation gibt auch der Test die erste passende Zielbenutzeridentität zurück; für die Suche und Rückgabe gilt die folgende Reihenfolge:

1. Bestimmte Kennungszuordnung
2. Richtlinienzuordnung für Zertifikatfilter
3. Standardrichtlinienzuordnung für Register
4. Standardrichtlinienzuordnung für Domänen

Sollte der Test keine Zielbenutzeridentitäten zurückgeben, obwohl für die Domäne Zuordnungen konfiguriert sind, überprüfen Sie, ob Sie die richtigen Informationen für den Test angegeben haben. Ist dies der Fall, könnte das Problem eine der folgenden Ursachen haben:

- Die Unterstützung von Richtlinienzuordnungen ist nicht auf Domänenebene aktiviert. Sie müssten dann Richtlinienzuordnungen für eine Domäne aktivieren.
- Die Unterstützung von Abgleichsuchfunktionen oder Richtlinienzuordnungen ist nicht auf der individuellen Registerebene aktiviert. Sie müssten dann die Unterstützung von Abgleichsuchfunktionen und die Verwendung von Richtlinienzuordnungen für das Zielregister aktivieren.
- Eine Ziel- oder Quellenzuordnung für eine EIM-Kennung ist nicht richtig konfiguriert. Beispiel: Es ist keine oder eine falsche Quellenzuordnung für den Kerberos-Principal (oder Windows-Benutzer) vorhanden, oder die Zielzuordnung enthält eine falsche Benutzeridentität. Zeigen Sie alle Kennungszuordnungen für eine EIM-Kennung an, um die Zuordnungen für eine bestimmte Kennung überprüfen zu können.
- Eine Richtlinienzuordnung ist falsch konfiguriert. Zeigen Sie alle Richtlinienzuordnungen für eine Domäne an, um die Quellen- und Zielinformationen für alle in der Domäne definierten Richtlinienzuordnungen überprüfen zu können.
- Registerdefinition und Benutzeridentitäten stimmen auf Grund unterschiedlicher Groß-/Kleinschreibung nicht überein. Sie können das Register löschen und erneut erstellen oder die Zuordnung löschen und in der richtigen Schreibweise unter Beachtung der Groß-/Kleinschreibung erneut erstellen.

In anderen Fällen liefert der Test möglicherweise mehrdeutige Ergebnisse. Eine Fehlernachricht macht dann auf diese Situation aufmerksam. Der Test liefert mehrdeutige Ergebnisse, wenn mehrere Zielbenutzeridentitäten den angegebenen Testkriterien entsprechen. Eine Abgleichsuchoperation kann mehrere Zielbenutzeridentitäten zurückgeben, wenn eine oder mehrere der folgenden Situationen zutreffen:

- Eine EIM-Kennung verfügt über mehrere individuelle Zielzuordnungen zum gleichen Zielregister.
- Für mehrere EIM-Kennungen wurde ein und dieselbe Benutzeridentität in einer Quellenzuordnung angegeben, und jede dieser EIM-Kennungen verfügt über eine Zielzuordnung zu demselben Zielregister, obwohl die für jede Zielzuordnung angegebene Benutzeridentität unterschiedlich sein kann.
- In mehreren Standardrichtlinienzuordnungen für Domäne wurde dasselbe Zielregister angegeben.
- In mehreren Standardrichtlinienzuordnungen für Register wurde dasselbe Quellenregister und dasselbe Zielregister angegeben.
- In mehreren Richtlinienzuordnungen für Zertifikatfilter wurde dasselbe X.509-Quellenregister, derselbe Zertifikatfilter und dasselbe Zielregister angegeben.

Eine Abgleichsuchoperation, die mehrere Zielbenutzeridentitäten zurückgibt, kann zu Problemen bei EIM-fähigen Anwendungen wie z. B. i5/OS-Anwendungen und -Produkten führen. Folglich müssen Sie

die Ursache für die mehrdeutigen Ergebnisse herausfinden und festlegen, welche Maßnahmen zur Lösung des Problems erforderlich sind. Je nach Ursache können Sie eine oder mehrere der folgenden Maßnahmen ergreifen:

- Der Test gibt mehrere unerwünschte Zielidentitäten zurück. Dies weist darauf hin, dass die Zuordnungskonfiguration für die Domäne aus einem der folgenden Gründe fehlerhaft ist:
  - Eine Ziel- oder Quellenzuordnung für eine EIM-Kennung ist nicht richtig konfiguriert. Beispiel: Es ist keine oder eine falsche Quellenzuordnung für den Kerberos-Principal (oder Windows-Benutzer) vorhanden, oder die Zielzuordnung enthält eine falsche Benutzeridentität. Zeigen Sie alle Kennungszuordnungen für eine EIM-Kennung an, um die Zuordnungen für eine bestimmte Kennung überprüfen zu können.
  - Eine Richtlinienzuordnung ist falsch konfiguriert. Zeigen Sie alle Richtlinienzuordnungen für eine Domäne an, um die Quellen- und Zielinformationen für alle in der Domäne definierten Richtlinienzuordnungen überprüfen zu können.
- Der Test gibt mehrere Zielbenutzeridentitäten zurück, und diese Ergebnisse entsprechen auch der Art und Weise, wie Sie Zuordnungen konfiguriert haben; in diesem Fall müssen Sie Suchinformationen für jede Zielbenutzeridentität angeben. Sie müssen für alle Zielbenutzeridentitäten, die über dieselbe Quelle verfügen, eindeutige Suchinformationen angeben (entweder eine EIM-Kennung für Kennungszuordnungen oder ein Quellenbenutzerregister für Richtlinienzuordnungen). Auf diese Weise stellen Sie sicher, dass eine Suchoperation statt aller möglichen Zielbenutzeridentitäten nur eine einzige zurückgibt. Siehe Suchinformationen einer Zielbenutzeridentität hinzufügen. Diese Suchinformationen müssen Sie zur Abgleichsuchoperation angeben.

  Anmerkung: Diese Vorgehensweise ist nur möglich, wenn die Anwendung die Benutzung von Suchinformationen unterstützt. Die i5/OS-Basisanwendungen wie z. B. iSeries Access für Windows sind nicht in der Lage, anhand von Suchinformationen mehrere von einer Suchoperation zurückgegebene Zielbenutzeridentitäten zu unterscheiden. Daher sollten Sie überprüfen, ob es sinnvoll ist, die für die Domäne vorhandenen Zuordnungen erneut zu definieren. Auf diese Weise kann sichergestellt werden, dass eine Abgleichsuchoperation eine einzige Zielbenutzeridentität zurückgeben kann. So kann gewährleistet werden, dass die i5/OS-Basisanwendungen Suchoperationen ausführen und Identitäten abgleichen können.

Weitere Informationen über potenzielle Abgleichprobleme und entsprechende Lösungen, die hier nicht beschrieben wurden, finden Sie unter „Fehlerbehebung beim EIM-Abgleich" auf Seite 134.

EIM-Domäne aus Ordner Domänenverwaltung entfernen

Sie können eine EIM-Domäne, die Sie nicht mehr verwalten möchten, aus dem Ordner **Domänenverwaltung** entfernen. Beachten Sie jedoch, dass das Entfernen einer Domäne aus dem Ordner **Domänenverwaltung nicht** dasselbe ist, wie das Löschen der Domäne; auch werden beim Entfernen keine Domänendaten vom Domänencontroller gelöscht. Lesen Sie Domäne löschen, wenn Sie die Domäne mitsamt den Domänendaten wirklich löschen möchten.

Zum Entfernen einer Domäne benötigen Sie keine Zugriffssteuerung (siehe „EIM-Zugriffssteuerung" auf Seite 42).

Führen Sie die folgenden Schritte durch, um eine EIM-Domäne, die Sie nicht mehr verwalten möchten, aus dem Ordner **Domänenverwaltung** zu entfernen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping**.
2. Klicken Sie mit der rechten Maustaste auf **Domänenverwaltung**, und wählen Sie **Domäne entfernen...** aus.
3. Wählen Sie die zu entfernende EIM-Domäne aus der Liste **Domänenverwaltung** aus.
4. Klicken Sie auf **OK**, um die Domäne zu entfernen.

EIM-Domäne und alle Konfigurationsobjekte löschen

Bevor Sie eine EIM-Domäne löschen können, müssen Sie sämtliche Registerdefinitionen und EIM-Kennungen aus der Domäne löschen. Wenn Sie die Domäne und die darin enthaltenen Daten zwar nicht löschen aber die Domäne dennoch nicht mehr verwalten möchten, können Sie die Domäne entfernen.

Um eine EIM-Domäne löschen zu können, müssen Sie über die im Abschnitt „EIM-Zugriffssteuerung" auf Seite 42 beschriebene Zugriffssteuerung für einen der folgenden Aufgabenbereiche verfügen:

- LDAP-Administrator
- EIM-Administrator

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wenn nötig, löschen Sie alle Registerdefinitionen aus der EIM-Domäne.
3. Wenn nötig, löschen Sie alle EIM-Kennungen aus der EIM-Domäne.
4. Klicken Sie mit der rechten Maustaste auf die Domäne, die Sie löschen möchten, und wählen Sie **Löschen...** aus.
5. Klicken Sie im Dialog **Löschen bestätigen** auf **Ja**.

Anmerkung: Daraufhin wird der Dialog "Löschen von ... läuft" aufgerufen, in dem der Status des Domänenlöschvorgangs bis zum Abschluss des Prozesses angezeigt wird.

EIM-Registerdefinitionen verwalten

In diesem Abschnitt wird erläutert, wie die EIM-Registerdefinitionen (EIM = Enterprise Identity Mapping) für die Benutzerregister in Ihrem Unternehmen, die EIM nutzen, erstellt und verwaltet werden können.

Damit Benutzerregister und die darin enthaltenen Benutzeridentitäten eine EIM-Domäne nutzen können, müssen Sie EIM-Registerdefinitionen für sie erstellen. Über die Verwaltung dieser EIM-Registerdefinitionen können Sie dann festlegen, wie die Benutzerregister und ihre Benutzeridentitäten in EIM integriert werden sollen.

Für Registerdefinitionen können die folgenden Verwaltungstasks ausgeführt werden:

Zugehörige Konzepte

„Richtlinienzuordnung erstellen" auf Seite 114

Zugehörige Tasks

„Richtlinienzuordnung löschen" auf Seite 127

Systemregisterdefinition hinzufügen

Um eine Systemregisterdefinition zu erstellen, müssen Sie mit der EIM-Domäne verbunden sein, in der gearbeitet werden soll. Darüber hinaus müssen Sie über die Zugriffssteuerung des EIM-Administrators verfügen.

Führen Sie die folgenden Schritte durch, um einer EIM-Domäne eine Systemregisterdefinition hinzuzufügen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter Domänenverwaltung aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter „Verbindung zu einer EIM-Domäne herstellen" auf Seite 96 nach.
3. Erweitern Sie die EIM-Domäne, mit der Sie jetzt verbunden sind.

4. Klicken Sie mit der rechten Maustaste auf **Benutzerregister**, wählen Sie **Register hinzufügen** und anschließend **System...** aus.
5. Geben Sie im Dialogfenster **Systemregister hinzufügen** folgende Informationen über die Systemregisterdefinition ein:
   a. Einen Namen für die Systemregisterdefinition.
   b. Den Typ der Registerdefinition.
   c. Eine Beschreibung der Systemregisterdefinition.
   d. (Optional) Die URL-Adresse des Benutzerregisters.
   e. Wenn nötig, einen oder mehrere Aliasnamen für die Systemregisterdefinition.
6. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen benötigen.
7. Klicken Sie auf **OK**, um die Informationen zu speichern und die Registerdefinition zur EIM-Domäne hinzuzufügen.

Anwendungsregisterdefinition hinzufügen

Um eine Anwendungsregisterdefinition zu erstellen, müssen Sie mit der EIM-Domäne verbunden sein, in der gearbeitet werden soll. Darüber hinaus müssen Sie über die Zugriffssteuerung des EIM-Administrators verfügen.

Führen Sie die folgenden Schritte durch, um einer EIM-Domäne eine Anwendungsregisterdefinition hinzuzufügen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter Domänenverwaltung aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter „Verbindung zu einer EIM-Domäne herstellen" auf Seite 96 nach.
3. Erweitern Sie die EIM-Domäne, mit der Sie jetzt verbunden sind.
4. Klicken Sie mit der rechten Maustaste auf **Benutzerregister**, wählen Sie **Register hinzufügen** und anschließend **Anwendung...** aus.
5. Geben Sie im Dialogfenster **Anwendungsregister hinzufügen** folgende Informationen über die Anwendungsregisterdefinition ein:
   a. Einen Namen für die Anwendungsregisterdefinition.
   b. Den Namen der Systemregisterdefinition, zu der das hier definierte Anwendungsbenutzerregister als Teilauflistung gehört. Die hier angegebene Systemregisterdefinition muss bereits in EIM vorhanden sein, sonst kann die Anwendungsregisterdefinition nicht erstellt werden.
   c. Den Typ der Registerdefinition.
   d. Eine Beschreibung der Anwendungsregisterdefinition.
   e. Wenn nötig, einen oder mehrere Aliasnamen für die Anwendungsregisterdefinition.
6. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen benötigen.
7. Klicken Sie auf **OK**, um die Informationen zu speichern und die Registerdefinition zur EIM-Domäne hinzuzufügen.

Gruppenregisterdefinition hinzufügen

Um eine Gruppenregisterdefinition zu erstellen, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die Zugriffssteuerung für den EIM-Administrator verfügen.

Führen Sie die folgenden Schritte durch, um einer EIM-Domäne eine Gruppenregisterdefinition hinzuzufügen:

1. Erweitern Sie die Einträge **Netzwerk → Enterprise Identity Mapping → Domänenverwaltung**.

2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   a. Wird die gewünschte EIM-Domäne in der Domänenverwaltung nicht aufgelistet, sollten Sie die Informationen unter EIM-Domäne zur Domänenverwaltung hinzufügen lesen.
   b. Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie die Informationen im Abschnitt Verbindung zum EIM-Domänencontroller herstellen.
3. Erweitern Sie die EIM-Domäne, mit der Sie verbunden sind.
4. Klicken Sie mit der rechten Maustaste auf **Benutzerregister**, wählen Sie **Register hinzufügen** und anschließend **Gruppe....** aus.
5. Geben Sie im Dialog ″Gruppenregister hinzufügen″ folgende Informationen zur Gruppenregisterdefinition an:
   a. Name der Gruppenregisterdefinition.
   b. Wählen Sie **Bei Gruppenregistermitgliedern muss die Groß-/Kleinschreibung beachtet werden** aus, wenn bei allen Mitgliedern der Gruppenregisterdefinition die Groß-/Kleinschreibung beachtet werden muss.
   c. Beschreibung der Gruppenregisterdefinition.
   d. Wenn nötig, einen oder mehrere Aliasnamen für die Gruppenregisterdefinition.
6. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen benötigen.
7. Klicken Sie auf **OK**, um die Informationen zu speichern und die Registerdefinition zur EIM-Domäne hinzuzufügen.

Aliasnamen zu Registerdefinition hinzufügen

Wenn Sie oder Ihr Anwendungsentwickler einer Registerdefinition ein weiteres Unterscheidungsmerkmal hinzufügen möchten, können Sie einen Aliasnamen für die Registerdefinition erstellen. Der Aliasname kann dann von Ihnen oder anderen Personen zur besseren Unterscheidung zwischen einzelnen Benutzerregistern verwendet werden.

Durch diese Aliasnamenunterstützung können Programmierer Anwendungen schreiben, ohne im Voraus den EIM-Registerdefinitionsnamen zu kennen, der von dem Administrator, der die Anwendung implementiert, frei gewählt werden kann. Den von der Anwendung verwendeten Aliasnamen findet der EIM-Administrator zumeist in der Anwendungsdokumentation. Anhand dieser Informationen kann der EIM-Administrator der EIM-Registerdefinition, die das Benutzerregister repräsentiert, welches die Anwendung verwenden soll, den gleichen Namen zuordnen.

Um einer Registerdefinition einen Aliasnamen hinzufügen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die Zugriffssteuerung (siehe „EIM-Zugriffssteuerung" auf Seite 42) für einen der folgenden Aufgabenbereiche verfügen:

- Registeradministrator
- Administrator für ausgewählte Register (für das Register, das geändert wird)
- EIM-Administrator

Führen Sie die folgenden Schritte durch, um einer EIM-Registerdefinition einen Aliasnamen hinzuzufügen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter Domänenverwaltung aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter „Verbindung zu einer EIM-Domäne herstellen" auf Seite 96 nach.
3. Erweitern Sie die EIM-Domäne, mit der Sie jetzt verbunden sind.

4. Klicken Sie auf **Benutzerregister**, um die Liste der in der Domäne enthaltenen Registerdefinitionen anzuzeigen.

   Anmerkung: Wenn Sie über die Zugriffssteuerung eines Administrators für ausgewählte Register verfügen, enthält die Liste nur diejenigen Registerdefinitionen, für die Sie speziell berechtigt sind.
5. Klicken Sie mit der rechten Maustaste auf die Registerdefinition, der Sie einen Aliasnamen hinzufügen möchten, und wählen Sie **Eigenschaften...** aus.
6. Wählen Sie die Seite **Aliasnamen** aus und geben Sie den Aliasnamen und -typ an, den Sie hinzufügen möchten.

   Anmerkung: Sie können auch einen Aliasnamentyp angeben, der nicht in der Typenliste enthalten ist.
7. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen benötigen.
8. Klicken Sie auf **Hinzufügen**.
9. Klicken Sie auf **OK**, um Ihre Änderungen an der Registerdefinition zu speichern.

Eigenen Benutzerregistertyp in EIM definieren

Wenn Sie eine EIM-Registerdefinition erstellen, können Sie einen von mehreren vordefinierten Benutzerregistertypen angeben, der ein Benutzerregister repräsentiert, das auf einem System innerhalb des Unternehmens vorhanden ist. Obwohl die vordefinierten Registerdefinitionstypen für die meisten Betriebs- systembenutzerregister geeignet sind, müssen Sie möglicherweise eine Registerdefinition erstellen, für die es in EIM keinen vordefinierten Typ gibt. Sie haben in diesem Fall zwei Möglichkeiten. Sie können entweder eine vorhandene Registerdefinition verwenden, die über ähnliche Merkmale verfügt wie Ihr Benutzerregister, oder Sie können ein eigenes Benutzerregister definieren.

Um ein Benutzerregister zu definieren, das nicht in EIM vordefiniert ist, müssen Sie den Registertyp mit Hilfe einer Objektkennung (OID) im Format **Objektkennung-Normalisierung** angeben, wobei **Objektkennung** für eine Objektkennung in der Schreibweise mit Trennzeichen (z. B. 1.2.3.4.5.6.7) und **Normalisierung** entweder für den Wert **caseExact** oder **caseIgnore** steht. Die Objektkennung (OID) für iSeries ist beispielsweise `1.3.18.0.2.33.2-caseIgnore`.

Sie sollten alle benötigten OIDs von anerkannten OID-Registrierungsinstanzen abrufen, um sicherzustellen, dass Sie eindeutige OIDs erstellen und verwenden. Durch Verwendung eindeutiger OIDs können Sie potenzielle Konflikte mit OIDs vermeiden, die von anderen Unternehmen oder Anwendungen erstellt werden.

Es gibt zwei Möglichkeiten, OIDs abzurufen.

- **Registrieren Sie die Objekte bei einer Instanz**. Diese Methode bietet sich an, wenn Sie nur wenige feststehende OIDs benötigen, um Informationen darzustellen. Diese OIDs könnten beispielsweise Zertifikatrichtlinien für Benutzer in Ihrem Unternehmen repräsentieren.
- **Lassen Sie sich von einer Registrierungsinstanz eine OID-Basisfolge zuteilen (arc assignment) und ordnen Sie Ihre eigenen OIDs dann nach Bedarf zu**. Diese Methode, bei der Ihnen ein Bereich von Objektkennungen (in Schreibweise mit Trennzeichen) zugeordnet wird, bietet sich an, wenn Sie zahlreiche OIDs benötigen oder Ihre OID-Zuordnungen geändert werden müssen. Die OID-Basisfolge besteht aus den Anfangsziffern (in Schreibweise mit Trennzeichen), auf deren Basis Sie dann Ihre **Objektkennungen** erstellen müssen. Die OID-Basisfolge könnte beispielsweise `1.2.3.4.5.` lauten. Durch Hinzufügen können Sie aus dieser Basisfolge dann OIDs erstellen (beispielsweise im Format `1.2.3.4.5.x.x.x`)).

Folgende Internetressourcen bieten weitere Informationen über die Registrierung von OIDs bei einer Registrierungsinstanz:

- Das American National Standards Institute (ANSI) ist die US-Registrierungsinstanz für Organisationsnamen unter dem weltweiten Registrierungsprozess, der von der International Standards Organization (ISO) und der International Telecommunication Union (ITU) eingerichtet wurde. Auf der Website der

allgemein zugänglichen ANSI-Dokumentbibliothek http://public.ansi.org/ansionline/Documents/ finden Sie ein Datenblatt im Microsoft Word-Format, mit dem Sie einen Registered Application Provider Identifier (RID) beantragen können. Zu dem Datenblatt gelangen Sie durch Auswahl von **Other Services > Registration Programs**. Die ANSI OID-Folge für Organisationen ist `2.16.840.1`. ANSI berechnet eine Gebühr für die Zuordnung von OID-Folgen. Die zugeordnete OID-Folge geht Ihnen etwa zwei Wochen nach Antragstellung zu. ANSI weist jeder neuen OID-Folge eine Nummer zu (NEWNUM), beispielsweise `2.16.840.1.NEWNUM`.

- Die nationale Normeninstitution unterhält in den meisten Ländern oder Regionen ein OID-Register, das normalerweise ebenfalls Folgen enthält, die unter der OID `2.16` zugeordnet sind. Es kann sein, dass umfangreichere Recherchen notwendig sind, um die zuständige OID-Instanz für ein bestimmtes Land oder eine bestimmte Region herauszufinden. Die Adressen der nationalen ISO-Mitglieder finden Sie unter http://www.iso.ch/addresse/membodies.html . Neben der postalischen und der E-Mail-Adresse ist vielfach auch ein Verweis auf eine Website enthalten.
- Die Internet Assigned Numbers Authority (IANA) ordnet private Unternehmensnummern, bei denen es sich um OIDs handelt, in der Folge `1.3.6.1.4.1` zu. Bis dato hat die IANA Folgen für mehr als 7500 Unternehmen zugeordnet. Die Anwendungsseite finden Sie unter http://www.iana.org/cgi-bin/enterprise.pl unter Private Enterprise Numbers. Die IANA benötigt normalerweise etwa eine Woche für die Zuteilung. Eine OID von der IANA ist kostenlos. Die IANA weist eine Nummer (NEWNUM) zu, so dass die neue OID-Folge `1.3.6.1.4.1.NEWNUM` lautet.
- Die US-Bundesregierung unterhält das Computer Security Objects Registry (CSOR). Das CSOR ist die Benennungsinstanz für die Folge `2.16.840.1.101.3` und registriert derzeit Objekte für Sicherheitslabels, Verschlüsselungsalgorithmen und Zertifikatrichtlinien. Die OIDs für Zertifikatrichtlinien sind in der Folge `2.16.840.1.101.3.2.1` definiert. Das CSOR stellt Richtlinien-OIDs für Behörden der US-Bundesregierung zur Verfügung. Weitere Informationen über das CSOR finden Sie unter http://csrc.nist.gov/csor/ .

  Zugehörige Informationen

  http://csrc.nist.gov/csor/pkireg.htm

Unterstützung von Abgleichsuchen und Richtlinienzuordnungen für Zielregister aktivieren

Die EIM-Unterstützung von Abgleichrichtlinien bietet die Möglichkeit, Richtlinienzuordnungen zu verwenden, um n:1-Abgleiche für den Fall zu erstellen, dass keine Zuordnungen zwischen Benutzeridentitäten und einer EIM-Kennung vorhanden sind. Mit Hilfe einer Richtlinienzuordnung kann eine Quellengruppe aus mehreren Benutzeridentitäten (keine einzelne Benutzeridentität) mit einer einzigen Zielbenutzeridentität in einem angegebenen Zielbenutzerregister abgeglichen werden.

Bevor Sie jedoch Richtlinienzuordnungen verwenden können, müssen Sie zunächst sicherstellen, dass Sie Abgleichsuchen mit Hilfe von Richtlinienzuordnungen für die Domäne aktivieren. Sie müssen außerdem eine oder zwei Einstellungen für jedes Register aktivieren:

- **Abgleichsuchen für Register aktivieren**. Wählen Sie diese Option aus, um sicherzustellen, dass das Register EIM-Abgleichsuchoperationen nutzen kann, und zwar unabhängig davon, ob Richtlinienzuordnungen für das Register definiert sind.
- **Richtlinienzuordnungen verwenden**. Wählen Sie diese Option aus, um dieses Register als Zielregister einer Richtlinienzuordnung zuzulassen und sicherzustellen, dass es EIM-Abgleichsuchoperationen nutzen kann.

Wenn Sie keine Abgleichsuchen für das Register aktivieren, kann dieses Register überhaupt keine EIM-Abgleichsuchoperationen nutzen. Wenn Sie nicht angeben, dass das Register Richtlinienzuordnungen verwenden kann, werden alle Richtlinienzuordnungen für dieses Register von den EIM-Abgleichsuchoperationen ignoriert, wenn das Register Ziel der Operation ist.

Um Abgleichsuchen mit Hilfe von Richtlinienzuordnungen für ein Zielregister aktivieren zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die Zugriffssteuerung (siehe „EIM-Zugriffssteuerung" auf Seite 42) für einen der folgenden Aufgabenbereiche verfügen:

- EIM-Administrator
- Registeradministrator
- Administrator für ausgewählte Register (für das Register, das aktiviert werden soll)

Führen Sie die folgenden Schritte durch, um die Unterstützung von Abgleichsuchen im Allgemeinen zu aktivieren und die Verwendung von Richtlinienzuordnungen im Speziellen zu erlauben:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Wählen Sie **Benutzerregister** aus, um die Liste der Registerdefinitionen für die Domäne anzuzeigen.

   Anmerkung: Wenn Sie über die Zugriffssteuerung eines Administrators für ausgewählte Register verfügen, enthält die Liste nur diejenigen Registerdefinitionen, für die Sie speziell berechtigt sind.
4. Klicken Sie mit der rechten Maustaste auf die Registerdefinition, für die Sie die Unterstützung von Abgleichrichtlinien aktivieren möchten, und wählen Sie **Abgleichrichtlinie...** aus.
5. Wählen Sie auf der Seite **Allgemein** die Option **Abgleichsuchen mit Hilfe von Richtlinienzuordnungen für Domäne aktivieren** aus. Die Auswahl dieser Option ermöglicht dem Register die Nutzung von EIM-Abgleichsuchoperationen. Wird diese Option nicht ausgewählt, kann eine Suchoperation keine Daten für das Register zurückgeben, und zwar unabhängig davon, ob das Register das Quellen- oder das Zielregister in einer Suchoperation darstellt.
6. Wählen Sie **Richtlinienzuordnungen verwenden** aus. Die Auswahl dieser Option ermöglicht Suchoperationen die Verwendung von Richtlinienzuordnungen als Basis für die Rückgabe von Daten, wenn das Register das Ziel der Suchoperation ist.
7. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Anmerkung: Bevor ein Register Richtlinienzuordnungen verwenden kann, müssen Sie außerdem sicherstellen, dass Sie Richtlinienzuordnungen für eine Domäne aktivieren.

Zugehörige Konzepte

„Unterstützung und Aktivierung von EIM-Abgleichrichtlinien" auf Seite 41
In diesem Abschnitt wird erläutert, wie Richtlinienzuordnungen für Domänen aktiviert und inaktiviert werden können.

Registerdefinition löschen

Wenn Sie eine Registerdefinition aus einer EIM-Domäne löschen, hat dies keine Auswirkungen auf das Benutzerregister, auf das die Registerdefinition verweist, dieses Benutzerregister dann die EIM-Domäne jedoch nicht mehr nutzen. Beim Löschen einer Registerdefinition ist dennoch Folgendes zu beachten:

- Wenn eine Registerdefinition gelöscht wird, gehen alle Zuordnungen für das betreffende Benutzerregister verloren. Wenn Sie das Register erneut für die Domäne definieren, müssen Sie alle erforderlichen Zuordnungen ebenfalls erneut erstellen.
- Wenn eine X.509-Registerdefinition gelöscht wird, gehen auch alle für dieses Register definierten Zertifikatfilter verloren. Wenn Sie das X.509-Register erneut für die Domäne definieren, müssen Sie alle erforderlichen Zertifikatfilter ebenfalls erneut erstellen.

- Eine Systemregisterdefinition kann nicht gelöscht werden, wenn Anwendungsregisterdefinitionen vorhanden sind, in denen die Systemregisterdefinition als übergeordnetes Register angegeben ist.

Um eine Registerdefinition löschen zu können, müssen Sie mit der EIM-Domäne verbunden sein, in der Sie arbeiten möchten, und über die Zugriffssteuerung des EIM-Administrators verfügen.

Führen Sie die folgenden Schritte durch, um eine EIM-Registerdefinition zu löschen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Erweitern Sie die EIM-Domäne, mit der Sie verbunden sind.
4. Klicken Sie auf **Benutzerregister**, um die Liste der Registerdefinitionen für die Domäne anzuzeigen.

   Anmerkung: Wenn Sie über die Zugriffssteuerung eines Administrators für ausgewählte Register verfügen, enthält die Liste nur diejenigen Registerdefinitionen, für die Sie speziell berechtigt sind.
5. Klicken Sie mit der rechten Maustaste auf das Benutzerregister, das Sie löschen möchten, und wählen Sie **Löschen...** aus.
6. Klicken Sie im **Bestätigungsdialog** auf **Ja**, um die Registerdefinition zu löschen.

Aliasnamen aus Registerdefinition entfernen

Um einen Aliasnamen aus einer Registerdefinition für EIM (EIM = Enterprise Identity Mapping) entfernen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die Zugriffssteuerung (siehe hierzu „EIM-Zugriffssteuerung" auf Seite 42) für einen der folgenden Aufgabenbereiche verfügen:

- Registeradministrator
- Administrator für ausgewählte Register (für die Registerdefinition, mit der Sie arbeiten möchten)
- EIM-Administrator

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Erweitern Sie die EIM-Domäne, mit der Sie verbunden sind.
4. Klicken Sie auf **Benutzerregister**, um die Liste der Registerdefinitionen für die Domäne anzuzeigen.

   Anmerkung: Wenn Sie über die Zugriffssteuerung eines Administrators für ausgewählte Register verfügen, enthält die Liste nur diejenigen Registerdefinitionen, für die Sie speziell berechtigt sind.
5. Klicken Sie mit der rechten Maustaste auf eine Registerdefinition, und wählen Sie **Eigenschaften...** aus.
6. Wählen Sie die Seite **Aliasname** aus.
7. Wählen Sie den Aliasnamen aus, der entfernt werden soll, und klicken Sie auf **Entfernen**.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Mitglied zu einer Gruppenregisterdefinition hinzufügen

Um einer Gruppenregisterdefinition ein Mitglied hinzufügen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die EIM-Zugriffssteuerung für einen der folgenden Aufgabenbereiche verfügen:

- EIM-Administrator
- Registeradministrator
- Administrator für ausgewählte Register (für die Gruppenregisterdefinition, zu der ein Mitglied hinzugefügt werden soll, und für das einzelne Mitglied, das hinzugefügt werden soll)

Führen Sie die folgenden Schritte durch, um ein Mitglied zu einer Gruppenregisterdefinition hinzuzufügen:

1. Erweitern Sie die Einträge **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   a. Wird die gewünschte EIM-Domäne in der Domänenverwaltung nicht aufgelistet, sollten Sie die Informationen unter EIM-Domäne zur Domänenverwaltung hinzufügen lesen.
   b. Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie die Informationen im Abschnitt Verbindung zum EIM-Domänencontroller herstellen.
3. Erweitern Sie die EIM-Domäne, mit der Sie verbunden sind.
4. Klicken Sie auf **Benutzerregister**, um die Liste der in der Domäne enthaltenen Registerdefinitionen anzuzeigen.
5. Klicken Sie mit der rechten Maustaste auf die Gruppenregisterdefinition, zu der ein Mitglied hinzugefügt werden soll, und wählen Sie dann **Eigenschaften...** aus.
6. Wählen Sie die Seite **Mitglieder** aus, und klicken Sie dann auf **Hinzufügen**.
7. Wählen Sie im Dialog **EIM-Gruppenregistermitglied hinzufügen** mindestens eine Registerdefinition aus, und klicken Sie dann auf **OK**. Der Inhalt der Liste ist von Ihrer EIM-Zugriffssteuerung abhängig und beschränkt sich auf Registerdefinitionen mit derselben Einstellung für die Beachtung der Groß-/Kleinschreibung, die auch für andere Mitglieder der Gruppe definiert ist.
8. Klicken Sie auf **OK**, um den Dialog zu verlassen.

EIM-Kennungen verwalten

Im Folgenden wird erläutert, wie EIM-Kennungen (EIM = Enterprise Identity Mapping) für eine Domäne erstellt und verwaltet werden können.

Das Erstellen und Verwenden von EIM-Kennungen, die die Benutzer in Ihrem Netzwerk repräsentieren, kann sich als äußerst hilfreich erweisen, wenn es darum geht, herauszufinden, welche Person eine bestimmte Benutzeridentität besitzt. Die Benutzer innerhalb eines Unternehmens ändern sich ständig: einige kommen hinzu, andere gehen und wieder andere wechseln den Arbeitsbereich. Diese Veränderungen können für Probleme in der Verwaltung sorgen, denn ständig müssen Benutzeridentitäten und Kennwörter für Systeme und Anwendungen innerhalb des Netzwerks im Auge behalten werden. Außerdem nimmt die Kennwortverwaltung in einem Unternehmen enorm viel Zeit in Anspruch. Sie können sich das Protokollieren der Benutzeridentitäten erheblich leichter machen, wenn Sie EIM-Kennungen erstellen und diese den Benutzeridentitäten der einzelnen Benutzer zuordnen. Auf diese Weise können Sie auch die Kennwortverwaltung vereinfachen.

Die Implementierung einer Umgebung für die Einzelanmeldung erleichtert auch die Verwaltung von Benutzeridentitäten, insbesondere, wenn die entsprechenden Benutzer in eine andere Abteilung oder einen anderen Arbeitsbereich innerhalb des Unternehmens wechseln. Die Aktivierung der Einzelanmeldung kann es diesen Benutzern ersparen, sich neue Benutzernamen und Kennwörter für neue Systeme merken zu müssen.

Anmerkung: Wie EIM-Kennungen erstellt und verwendet werden, hängt von den Erfordernissen des jeweiligen Unternehmens ab. Weitere Informationen finden Sie unter „Benennungsplan für EIM-Kennungen entwickeln" auf Seite 69.

EIM-Kennungen können für alle EIM-Domänen verwaltet werden, die unter dem Ordner **Domänenverwaltung** verfügbar sind. Sie können die folgenden Verwaltungstasks für die EIM-Kennungen in einer EIM-Domäne ausführen:

EIM-Kennung erstellen

Um eine EIM-Kennung erstellen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die Zugriffssteuerung (siehe „EIM-Zugriffssteuerung" auf Seite 42) für einen der folgenden Aufgabenbereiche verfügen:

- Kennungsadministrator
- EIM-Administrator

Führen Sie die folgenden Schritte durch, um eine EIM-Kennung für eine Person oder eine Entität in Ihrem Unternehmen zu erstellen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Erweitern Sie die EIM-Domäne, mit der Sie verbunden sind.
4. Klicken Sie mit der rechten Maustaste auf **Kennungen**, und wählen Sie **Neue Kennung...** aus.
5. Geben Sie im Dialog **Neue EIM-Kennung** folgende Informationen ein:
   a. Name für die Kennung.
   b. Ob das System einen eindeutigen Namen generieren soll.
   c. Beschreibung der Kennung.
   d. Ggf. einen oder mehrere Aliasnamen für die Kennung.
6. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen benötigen.
7. Klicken Sie nach Eingabe aller erforderlichen Informationen auf **OK**, um die EIM-Kennung zu erstellen.

Anmerkung: Wenn Sie eine große Anzahl von EIM-Kennungen erstellen, dauert es nach dem Erweitern des Ordners **Kennungen** möglicherweise einige Zeit, bis die Liste der Kennungen angezeigt wird. Um die Leistung in einem solchen Fall zu erhöhen, können Sie die „Sicht der EIM-Kennungen anpassen" auf Seite 111.

Aliasnamen zu EIM-Kennung hinzufügen

Sie können einen Aliasnamen erstellen, um ein zusätzliches Unterscheidungsmerkmal für eine EIM-Kennung zur Verfügung zu stellen (siehe „EIM-Kennung" auf Seite 9). Aliasnamen können Ihnen bei der Suche nach einer bestimmten EIM-Kennung im Rahmen einer EIM-Suchoperation helfen. Aliasnamen sind beispielsweise hilfreich, wenn sich der rechtsgültige Name einer Person von dem verwendeten Namen unterscheidet.

Die Namen von EIM-Kennungen müssen innerhalb der EIM-Domäne eindeutig sein. Aliasnamen sind daher in Situationen hilfreich, in denen die Verwendung eindeutiger Kennungsnamen problematisch ist. Gibt es in einem Unternehmen beispielsweise mehrere Mitarbeiter mit dem gleichen Namen, kann die Nutzung von Eigennamen als EIM-Kennung zu Verwechslungen führen. Wenn beispielsweise zwei Benutzer mit dem Namen John J. Johnson vorhanden sind, könnten Sie den Aliasnamen John Joseph

Johnson für den einen und John Jeffrey Johnson für den anderen Benutzer erstellen, um die einzelnen Identitäten besser unterscheiden zu können. Die zusätzlichen Aliasnamen könnten beispielsweise die Personalnummer, die Abteilungsnummer, die Positionsbezeichnung oder ein anderes Attribut enthalten.

Um einer EIM-Kennung einen Aliasnamen hinzufügen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die Zugriffssteuerung (siehe „EIM-Zugriffssteuerung" auf Seite 42) für einen der folgenden Aufgabenbereiche verfügen:

- EIM-Administrator
- Kennungsadministrator

Führen Sie die folgenden Schritte durch, um einer EIM-Kennung einen Aliasnamen hinzuzufügen.

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Erweitern Sie die EIM-Domäne, mit der Sie verbunden sind.
4. Klicken Sie auf **Kennungen**, um im rechten Teilfenster eine Liste der in der Domäne verfügbaren EIM-Kennungen anzuzeigen.

   Anmerkung: Gelegentlich kann es beim Erweitern des Ordners **Kennungen** einige Zeit dauern, bis die Liste der Kennungen angezeigt wird. Um die Leistung in diesem Fall zu erhöhen, können Sie die Sicht anpassen (siehe „Sicht der EIM-Kennungen anpassen" auf Seite 111).
5. Klicken Sie mit der rechten Maustaste auf die EIM-Kennung, der Sie einen Aliasnamen hinzufügen möchten, und wählen Sie **Eigenschaften...** aus.
6. Geben Sie im Feld **Aliasname** den Aliasnamen ein, der dieser EIM-Kennung hinzugefügt werden soll, und klicken Sie auf **Hinzufügen**.
7. Klicken Sie auf **OK**, um Ihre Änderungen an der EIM-Kennung zu speichern.

Aliasnamen aus EIM-Kennung entfernen

Um einen Aliasnamen aus einer EIM-Kennung entfernen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die Zugriffssteuerung (siehe „EIM-Zugriffssteuerung" auf Seite 42) für einen der folgenden Aufgabenbereiche verfügen:

- Kennungsadministrator
- EIM-Administrator

Führen Sie die folgenden Schritte durch, um einen Aliasnamen aus einer EIM-Kennung zu entfernen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Erweitern Sie die EIM-Domäne, mit der Sie verbunden sind.
4. Klicken Sie auf **Kennungen**, um im rechten Teilfenster eine Liste der in der Domäne verfügbaren EIM-Kennungen anzuzeigen.

Anmerkung: Gelegentlich kann es beim Erweitern des Ordners **Kennungen** einige Zeit dauern, bis die Liste der Kennungen angezeigt wird. Um die Leistung zu verbessern, wenn in der Domäne eine große Anzahl von EIM-Kennungen vorhanden ist, sollten Sie die „Sicht der EIM-Kennungen anpassen".

5. Klicken Sie mit der rechten Maustaste auf die EIM-Kennung, für die Sie einen Aliasnamen entfernen möchten, und wählen Sie **Eigenschaften...** aus.
6. Wählen Sie den Aliasnamen aus, der entfernt werden soll, und klicken Sie auf **Entfernen**.
7. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

EIM-Kennung löschen

Um eine EIM-Kennung löschen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die Zugriffssteuerung des EIM-Administrators verfügen.

Führen Sie die folgenden Schritte durch, um eine EIM-Kennung zu löschen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Erweitern Sie die EIM-Domäne, mit der Sie jetzt verbunden sind.
4. Klicken Sie auf **Kennungen**.

   Anmerkung: Gelegentlich kann es beim Erweitern des Ordners **Kennungen** einige Zeit dauern, bis die Liste der Kennungen angezeigt wird. Um die Leistung zu verbessern, wenn in der Domäne eine große Anzahl von EIM-Kennungen vorhanden ist, sollten Sie die „Sicht der EIM-Kennungen anpassen".
5. Wählen Sie die EIM-Kennung aus, die Sie löschen möchten. Um mehrere Kennungen zu löschen, halten Sie während der Auswahl die Taste **Strg** gedrückt.
6. Klicken Sie mit der rechten Maustaste auf die gewünschten EIM-Kennungen, und wählen Sie **Löschen** aus.
7. Klicken Sie im Dialog **Löschen bestätigen** auf **Ja**, um die ausgewählten EIM-Kennungen endgültig zu löschen.

Sicht der EIM-Kennungen anpassen

Gelegentlich kann es beim Erweitern des Ordners **Kennungen** einige Zeit dauern, bis die Liste der Kennungen angezeigt wird. Um die Leistung in einem solchen Fall zu erhöhen, können Sie die Sicht des Ordners **Kennungen** anpassen.

Führen Sie dazu die folgenden Schritte durch:

1. Erweitern Sie **Netzwerk —> Enterprise Identity Mapping —> Domain Management**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Klicken Sie mit der rechten Maustaste auf den Ordner **Kennungen**, und wählen Sie **Diese Ansicht anpassen** aus.
4. Geben Sie die Bedingungen für die Anzeige der EIM-Kennungen in der Domäne an. Um die Anzahl der angezeigten EIM-Kennungen zu beschränken, geben Sie die Zeichen an, nach denen die Kennun-

gen sortiert werden sollen. Sie können ein oder mehrere Platzhalterzeichen (*) verwenden. Als Sortierbedingung könnten Sie beispielsweise *JOHNSON* im Feld **Kennungen** eingeben. Als Ergebnis erhalten Sie dann alle EIM-Kennungen, in denen die Zeichenfolge JOHNSON als Bestandteil des Namens enthalten ist, sowie die EIM-Kennungen, in denen die Zeichenfolge JOHNSON als Bestandteil des Aliasnamens enthalten ist.

5. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Zuordnungen verwalten

In diesen Informationen wird erläutert, welche Zuordnungstypen mit EIM (Enterprise Identity Mapping) verwaltet werden können.

In EIM können zwei Typen von Zuordnungen erstellt und verwaltet werden, die direkte oder indirekte Beziehungen zwischen Benutzeridentitäten definieren: Kennungszuordnungen und Richtlinienzuordnungen. Kennungszuordnungen können zwischen EIM-Kennungen und deren Benutzeridentitäten erstellt und verwaltet werden; auf diese Weise können indirekte, jedoch spezielle individuelle Beziehungen zwischen Benutzeridentitäten definiert werden. Richtlinienzuordnungen können erstellt werden, um eine Beziehung zwischen mehreren Benutzeridentitäten in einem oder mehreren Registern und einer bestimmten Zielbenutzeridentität in einem anderen Register zu beschreiben. Richtlinienzuordnungen verwenden die EIM-Unterstützung von Abgleichrichtlinien, um n:1-Abgleiche zwischen Benutzeridentitäten ohne Einbeziehung einer EIM-Kennung durchzuführen. Da beide Zuordnungstypen Beziehungen zwischen Benutzeridentitäten in einem Unternehmen definieren, ist die Verwaltung von Zuordnungen ein wichtiges Element innerhalb der EIM-Verwaltung.

Die Verwaltung der Zuordnungen innerhalb einer Domäne spielt eine maßgebliche Rolle bei der Vereinfachung der Verwaltungstasks, die erforderlich sind, um nachzuvollziehen, welche Benutzer über Konten auf den verschiedenen Systemen im Netzwerk verfügen. Bei der Implementierung eines sicheren Einzelanmeldungsnetzwerks müssen Sie darauf achten, Kennungs- und Richtlinienzuordnungen immer auf dem neuesten Stand zu halten.

Für Zuordnungen können die folgenden Verwaltungstasks ausgeführt werden:

Zuordnungen erstellen

Es gibt zwei Möglichkeiten, um Zuordnungen zu erstellen:

- Sie können eine Kennungszuordnung erstellen, um indirekt eine Beziehung zwischen zwei Benutzeridentitäten zu definieren, die von einer einzigen Person verwendet werden. Eine Kennungszuordnung beschreibt eine Beziehung zwischen einer EIM-Kennung und einer Benutzeridentität in einem Benutzerregister. Kennungszuordnungen ermöglichen 1:1-Abgleiche zwischen einer EIM-Kennung und jeder der verschiedenen Benutzeridentitäten für den Benutzer, der durch die EIM-Kennung dargestellt wird.
- Sie können eine Richtlinienzuordnung erstellen, um direkt eine Beziehung zwischen mehreren Benutzeridentitäten in einem oder mehreren Registern und einer bestimmten Zielbenutzeridentität in einem anderen Register zu definieren. Richtlinienzuordnungen verwenden die EIM-Unterstützung von Abgleichrichtlinien, um n:1-Abgleiche zwischen Benutzeridentitäten ohne Einbeziehung einer EIM-Kennung durchzuführen. Mit Hilfe von Richtlinienzuordnungen können Sie schnell eine Vielzahl von Abgleichen zwischen zusammengehörigen Benutzeridentitäten in unterschiedlichen Benutzerregistern durchführen.

Ob Sie sich für Kennungszuordnungen, Richtlinienzuordnungen oder eine Kombination aus beiden Methoden entscheiden, hängt von den Erfordernissen Ihrer EIM-Implementierung ab.

Zugehörige Konzepte

„Plan für Identitätsabgleich entwickeln” auf Seite 66

Kennungszuordnung erstellen:

Kennungszuordnungen definieren eine Beziehung zwischen einer EIM-Kennung und einer Benutzeridentität in Ihrem Unternehmen, die der Person oder Entität zugeordnet ist, auf die die EIM-Kennung verweist. Sie können drei Typen von Kennungszuordnungen erstellen: Ziel-, Quellen- und administrative Zuordnungen. Zur Vermeidung potenzieller Probleme mit Zuordnungen und der Art und Weise wie diese Identitäten abgleichen, müssen Sie einen Gesamtplan für den Identitätsabgleich in Ihrem Unternehmen erstellen, bevor Sie mit der Definition von Zuordnungen beginnen können.

Um eine Kennungszuordnung erstellen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein, und über die Zugriffssteuerung (siehe „EIM-Zugriffssteuerung" auf Seite 42) verfügen, die zum Erstellen des gewünschten Zuordnungstyps erforderlich ist.

Um eine Quellen- oder eine administrative Zuordnung erstellen zu können, müssen Sie über die EIM-Zugriffssteuerung für einen der folgenden Aufgabenbereiche verfügen:

- Kennungsadministrator
- EIM-Administrator

Um eine Zielzuordnung erstellen zu können, müssen Sie über die EIM-Zugriffssteuerung für einen der folgenden Aufgabenbereiche verfügen:

- Registeradministrator
- Administrator für ausgewählte Register (für die Registerdefinition, die sich auf das Benutzerregister bezieht, in dem die Zielbenutzeridentität enthalten ist)
- EIM-Administrator

Führen Sie die folgenden Schritte durch, um eine Kennungszuordnung zu erstellen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Erweitern Sie die EIM-Domäne, mit der Sie jetzt verbunden sind.
4. Klicken Sie auf **Kennungen**, um die Liste der EIM-Kennungen für die Domäne anzuzeigen.

   Anmerkung: Gelegentlich kann es beim Erweitern des Ordners **Kennungen** einige Zeit dauern, bis die Liste der Kennungen angezeigt wird. Um die Leistung in diesem Fall zu erhöhen, können Sie die Sicht anpassen (siehe „Sicht der EIM-Kennungen anpassen" auf Seite 111).
5. Klicken Sie mit der rechten Maustaste auf die EIM-Kennung, für die Sie eine Zuordnung erstellen möchten, und wählen Sie **Eigenschaften...** aus.
6. Wählen Sie die Seite **Zuordnungen** aus, und klicken Sie auf **Hinzufügen...**.
7. Geben Sie im Dialog **Zuordnung hinzufügen** folgende Informationen zur Definition der Zuordnung ein:
   - Name des Registers, das die Benutzeridentität enthält, die Sie der EIM-Kennung zuordnen möchten. Geben Sie den präzisen Namen einer vorhandenen Registerdefinition an, oder blättern Sie in den Definitionen, um die gewünschte Definition auszuwählen.
   - Name der Benutzeridentität, die Sie der EIM-Kennung zuordnen möchten.
   - Typ der Zuordnung. Sie können einen der folgenden drei Zuordnungstypen erstellen:
     - Administrativ
     - Quelle
     - Ziel
8. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen benötigen.

9. Optional. Um eine Zielzuordnung zu erstellen, klicken Sie auf **Erweitert...**, um den Dialog **Zuordnung hinzufügen - Erweitert** anzuzeigen. Geben Sie Suchinformationen für die Zielbenutzeridentität an, und klicken Sie auf **OK**, um zum Dialog **Zuordnung hinzufügen** zurückzukehren.
10. Klicken Sie nach Eingabe aller erforderlichen Informationen auf **OK**, um die Zuordnung zu erstellen.

Richtlinienzuordnung erstellen: Eine Richtlinienzuordnung stellt eine Möglichkeit dar, um auf direktem Weg eine Beziehung zwischen mehreren Benutzeridentitäten in einem oder mehreren Registern und einer bestimmten Zielbenutzeridentität in einem anderen Register zu definieren. Richtlinienzuordnungen verwenden die Unterstützungsfunktion für EIM-Abgleichrichtlinien, um n:1-Abgleiche zwischen Benutzeridentitäten herzustellen, ohne dass hierzu die EIM-Kennung herangezogen wird. Da sich die zahlreichen Verwendungsmöglichkeiten von Richtlinienzuordnungen überlappen, werden genaue Kenntnisse der EIM-Unterstützung von Abgleichrichtlinien vorausgesetzt, um Richtlinienzuordnungen erstellen und verwenden zu können. Zur Vermeidung potenzieller Probleme mit Zuordnungen und der Art und Weise, wie diese den Identitätsabgleich durchführen, müssen Sie außerdem einen Gesamtplan für den Identitätsabgleich in Ihrem Unternehmen erstellen, bevor Sie mit der Definition von Zuordnungen beginnen können.

Ob Sie sich für Kennungszuordnungen, Richtlinienzuordnungen oder eine Kombination aus beiden Methoden entscheiden, hängt von den Erfordernissen Ihrer EIM-Implementierung ab.

Die Vorgehensweise beim Erstellen einer Richtlinienzuordnung richtet sich nach dem Typ der Richtlinienzuordnung. Weitere Informationen über das Erstellen von Richtlinienzuordnungen finden Sie in folgenden Abschnitten:

Zugehörige Konzepte

„EIM-Registerdefinitionen verwalten" auf Seite 101
In diesem Abschnitt wird erläutert, wie die EIM-Registerdefinitionen (EIM = Enterprise Identity Mapping) für die Benutzerregister in Ihrem Unternehmen, die EIM nutzen, erstellt und verwaltet werden können.

Standardrichtlinienzuordnung für Domänen erstellen:

Um eine Standardrichtlinienzuordnung für Domänen erstellen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die „EIM-Zugriffssteuerung" auf Seite 42 für einen der folgenden Aufgabenbereiche verfügen:

- EIM-Administrator
- Registeradministrator

Anmerkung: Eine Richtlinienzuordnung beschreibt eine Beziehung zwischen mehreren Benutzeridentitäten und einer einzelnen Benutzeridentität in einem Zielbenutzerregister. Mit Hilfe einer Richtlinienzuordnung kann eine Beziehung zwischen einer Quellengruppe aus mehreren Benutzeridentitäten und einer einzigen Zielbenutzeridentität in einem angegebenen Zielbenutzerregister beschrieben werden. Richtlinienzuordnungen verwenden die EIM-Unterstützung von Abgleichrichtlinien, um n:1-Abgleiche zwischen Benutzeridentitäten ohne Einbeziehung einer EIM-Kennung durchzuführen.

Da sich die zahlreichen Verwendungsmöglichkeiten von Richtlinienzuordnungen überlappen, werden genaue Kenntnisse der EIM-Unterstützung von Abgleichrichtlinien vorausgesetzt, um Richtlinienzuordnungen erstellen und verwenden zu können. Zur Vermeidung potenzieller Probleme mit Zuordnungen und der Art und Weise, wie diese den Identitätsabgleich durchführen, müssen Sie außerdem einen Gesamtplan für den Identitätsabgleich in Ihrem Unternehmen erstellen, bevor Sie mit der Definition von Zuordnungen beginnen können.

In der Standardrichtlinienzuordnung für Domänen stellen alle Benutzer in der Domäne die Quelle der Richtlinienzuordnung dar und werden mit einem einzelnen Zielbenutzerregister und Zielbenutzer abge-

glichen. Für jedes Register in der Domäne kann eine Standardrichtlinienzuordnung für Domänen definiert werden. Wenn sich mindestens zwei Domänenrichtlinienzuordnungen auf dasselbe Zielregister beziehen, können für jede dieser Richtlinienzuordnungen eindeutige Suchinformationen definiert werden, um sicherzustellen, dass Abgleichsuchoperationen die Zuordnungen voneinander unterscheiden können. Andernfalls könnten Abgleichsuchoperationen mehrere Zielbenutzeridentitäten zurückgeben. Die Folge mehrdeutiger Ergebnisse könnte sein, dass Anwendungen, die EIM benutzen, nicht mehr in der Lage sind, die richtige Zielidentität festzustellen.

Führen Sie die folgenden Schritte durch, um eine Standardrichtlinienzuordnung für Domänen zu erstellen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Klicken Sie mit der rechten Maustaste auf die EIM-Domäne, in der Sie arbeiten möchten, und wählen Sie **Abgleichrichtlinie...** aus.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Wählen Sie auf der Seite `Allgemein` die Option **Abgleichsuchen mit Hilfe von Richtlinienzuordnungen für Domäne aktivieren** aus.
4. Wählen Sie die Seite **Domäne** aus, und klicken Sie auf **Hinzufügen...**.
5. Geben Sie im Dialog **Standardrichtlinienzuordnung für Domäne hinzufügen** die folgenden erforderlichen Informationen ein:
   - Name der Registerdefinition des **Zielregisters** für die Richtlinienzuordnung.
   - Name der Benutzeridentität des **Zielbenutzers** für die Richtlinienzuordnung.
6. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen in diesem und in nachfolgenden Dialogen benötigen.
7. Optional. Klicken Sie auf **Erweitert...**, um den Dialog **Zuordnung hinzufügen - Erweitert** anzuzeigen. Geben Sie **Suchinformationen** für die Richtlinienzuordnung an, und klicken Sie auf **OK**, um zum Dialog **Standardrichtlinienzuordnung für Domäne hinzufügen** zurückzukehren.

   Anmerkung: Wenn sich mindestens zwei Standardrichtlinienzuordnungen für Domänen auf dasselbe Zielregister beziehen, müssen Sie eindeutige Suchinformationen für jede der Zielbenutzeridentitäten in diesen Richtlinienzuordnungen definieren. Dadurch, dass Sie in dieser Situation Suchinformationen für jede Zielbenutzeridentität definieren, stellen Sie sicher, dass Abgleichsuchoperationen die Identitäten voneinander unterscheiden können. Andernfalls könnten Abgleichsuchoperationen mehrere Zielbenutzeridentitäten zurückgeben. Die Folge solch mehrdeutiger Ergebnisse könnte sein, dass Anwendungen, die EIM benutzen, nicht mehr in der Lage sind, die richtige Zielidentität festzustellen.
8. Klicken Sie auf **OK**, um die neue Richtlinienzuordnung zu erstellen und zur Seite **Domäne** zurückzukehren. Die neue Richtlinienzuordnung wird jetzt in der Tabelle **Standardrichtlinienzuordnungen** angezeigt.
9. Prüfen Sie, ob die neue Richtlinienzuordnung für das Zielregister aktiviert ist.
10. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und den Dialog **Abgleichrichtlinie** zu verlassen.

Anmerkung: Prüfen Sie, ob die Unterstützung von Abgleichrichtlinien und die Verwendung von Richtlinienzuordnungen für Zielbenutzerregister richtig aktiviert ist. Wenn nicht, kann die Richtlinienzuordnung nicht in Kraft treten.

Standardrichtlinienzuordnung für Register erstellen:

Um eine Standardrichtlinienzuordnung für Register erstellen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die „EIM-Zugriffssteuerung" auf Seite 42 für einen der folgenden Aufgabenbereiche verfügen:

- EIM-Administrator
- Registeradministrator

Anmerkung: Eine Richtlinienzuordnung beschreibt eine Beziehung zwischen mehreren Benutzeridentitäten und einer einzelnen Benutzeridentität in einem Zielbenutzerregister. Mit Hilfe einer Richtlinienzuordnung kann eine Beziehung zwischen einer Quellengruppe aus mehreren Benutzeridentitäten und einer einzigen Zielbenutzeridentität in einem angegebenen Zielbenutzerregister beschrieben werden. Richtlinienzuordnungen verwenden die EIM-Unterstützung von Abgleichrichtlinien, um n:1-Abgleiche zwischen Benutzeridentitäten ohne Einbeziehung einer EIM-Kennung durchzuführen.

Da sich die zahlreichen Verwendungsmöglichkeiten von Richtlinienzuordnungen überlappen, werden genaue Kenntnisse der EIM-Unterstützung von Abgleichrichtlinien vorausgesetzt, um Richtlinienzuordnungen erstellen und verwenden zu können. Zur Vermeidung potenzieller Probleme mit Zuordnungen und der Art und Weise, wie diese den Identitätsabgleich durchführen, müssen Sie außerdem einen Gesamtplan für den Identitätsabgleich in Ihrem Unternehmen erstellen, bevor Sie mit der Definition von Zuordnungen beginnen können.

In einer Standardrichtlinienzuordnung für Register stellen alle Benutzer in einem einzelnen Register die Quelle der Richtlinienzuordnung dar und werden mit einem einzelnen Zielbenutzerregister und Zielbenutzer abgeglichen. Wenn Sie die Standardrichtlinienzuordnung für Register für das Zielregister aktivieren, stellt die Richtlinienzuordnung sicher, dass diese Quellenbenutzeridentitäten alle mit einem einzigen bestimmten Zielregister und Zielbenutzer abgeglichen werden können.

Führen Sie die folgenden Schritte durch, um eine Standardrichtlinienzuordnung für Register zu erstellen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Wählen Sie auf der Seite `Allgemein` die Option **Abgleichsuchen mit Hilfe von Richtlinienzuordnungen für Domäne aktivieren** aus.
4. Wählen Sie auf der Seite `Allgemein` die Option **Abgleichsuchen mit Hilfe von Richtlinienzuordnungen für Domäne aktivieren** aus.
5. Geben Sie im Dialog **Standardrichtlinienzuordnung für Register hinzufügen** die folgenden erforderlichen Informationen ein:
   - Name der Registerdefinition des **Quellenregisters** für die Richtlinienzuordnung.
   - Name der Registerdefinition des **Zielregisters** für die Richtlinienzuordnung.
   - Name der Benutzeridentität des **Zielbenutzers** für die Richtlinienzuordnung.
6. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen in diesem und in nachfolgenden Dialogen benötigen.
7. Optional. Klicken Sie auf **Erweitert...**, um den Dialog **Zuordnung hinzufügen - Erweitert** anzuzeigen. Geben Sie **Suchinformationen** für die Richtlinienzuordnung an, und klicken Sie auf **OK**, um zum Dialog **Standardrichtlinienzuordnung für Register hinzufügen** zurückzukehren. Wenn sich mindestens zwei Richtlinienzuordnungen mit demselben Quellenregister auf dasselbe Zielregister beziehen, müssen Sie eindeutige Suchinformationen für jede der Zielbenutzeridentitäten in diesen Richtlinienzuordnungen definieren. Dadurch, dass Sie in dieser Situation Suchinformationen für jede

Zielbenutzeridentität definieren, stellen Sie sicher, dass Abgleichsuchoperationen die Identitäten voneinander unterscheiden können. Andernfalls könnten Abgleichsuchoperationen mehrere Zielbenutzeridentitäten zurückgeben. Die Folge solch mehrdeutiger Ergebnisse könnte sein, dass Anwendungen, die EIM benutzen, nicht mehr in der Lage sind, die richtige Zielidentität festzustellen.

8. Klicken Sie auf **OK**, um die neue Richtlinienzuordnung zu erstellen und zur Seite **Register** zurückzukehren. Die neue Standardrichtlinienzuordnung für Register wird jetzt in der Tabelle **Standardrichtlinienzuordnungen** angezeigt.
9. Prüfen Sie, ob die neue Richtlinienzuordnung für das Zielregister aktiviert ist.
10. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und den Dialog **Abgleichrichtlinie** zu verlassen.

Anmerkung: Prüfen Sie, ob die Unterstützung von Abgleichrichtlinien und die Verwendung von Richtlinienzuordnungen für Zielbenutzerregister richtig aktiviert ist. Wenn nicht, kann die Richtlinienzuordnung nicht in Kraft treten.

Richtlinienzuordnung für Zertifikatfilter erstellen:

Um eine Richtlinienzuordnung für Zertifikatfilter erstellen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die „EIM-Zugriffssteuerung" auf Seite 42 für einen der folgenden Aufgabenbereiche verfügen:

- EIM-Administrator
- Registeradministrator

Anmerkung: Eine Richtlinienzuordnung beschreibt eine Beziehung zwischen einer Quellengruppe aus mehreren Benutzeridentitäten und einer einzelnen Zielbenutzeridentität in einem angegebenen Zielbenutzerregister. Richtlinienzuordnungen verwenden die EIM-Unterstützung von Abgleichrichtlinien, um n:1-Abgleiche zwischen Benutzeridentitäten ohne Einbeziehung einer EIM-Kennung durchzuführen.

Da sich die zahlreichen Verwendungsmöglichkeiten von Richtlinienzuordnungen überlappen, werden genaue Kenntnisse der EIM-Unterstützung von Abgleichrichtlinien vorausgesetzt, um Richtlinienzuordnungen erstellen und verwenden zu können. Zur Vermeidung potenzieller Probleme mit Zuordnungen und der Art und Weise, wie diese den Identitätsabgleich durchführen, müssen Sie außerdem einen Gesamtplan für den Identitätsabgleich in Ihrem Unternehmen erstellen, bevor Sie mit der Definition von Zuordnungen beginnen können.

In einer Richtlinienzuordnung für Zertifikatfilter wird eine Gruppe von Zertifikaten in einem einzelnen X.509-Register als Quelle der Richtlinienzuordnung angegeben. Diese Zertifikate werden mit einem von Ihnen angegebenen einzelnen Zielregister und Zielbenutzer abgeglichen. Im Unterschied zu einer Standardrichtlinienzuordnung für Register, bei der alle Benutzer in einem einzelnen Register die Quelle der Richtlinienzuordnung bilden, ist der Geltungsbereich einer Richtlinienzuordnung für Zertifikatfilter flexibler. Als Quelle kann eine Untergruppe von Zertifikaten in dem Register angegeben werden. Der Zertifikatfilter, den Sie für die Richtlinienzuordnung angeben, bestimmt deren Geltungsbereich.

Anmerkung: Erstellen und verwenden Sie eine Standardrichtlinienzuordnung für Register, wenn Sie alle Zertifikate in einem X.509-Benutzerregister mit einer einzigen Zielbenutzeridentität abgleichen möchten.

Der Zertifikatfilter steuert, wie eine Richtlinienzuordnung für Zertifikatfilter eine Quellengruppe aus Benutzeridentitäten - in diesem Fall digitale Zertifikate - mit einer bestimmten Zielbenutzeridentität abgleicht. Daher muss der zu verwendende Zertifikatfilter vorhanden sein, bevor Sie eine Richtlinienzuordnung für Zertifikatfilter erstellen können.

Bevor Sie eine Richtlinienzuordnung für Zertifikatfilter erstellen können, müssen Sie zunächst einen Zertifikatfilter erstellen, der als Basis der Richtlinienzuordnung verwendet werden soll.

Führen Sie die folgenden Schritte durch, um eine Richtlinienzuordnung für Zertifikatfilter zu erstellen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Klicken Sie mit der rechten Maustaste auf die EIM-Domäne, in der Sie arbeiten möchten, und wählen Sie **Abgleichrichtlinie...** aus.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Wählen Sie auf der Seite `Allgemein` die Option **Abgleichsuchen mit Hilfe von Richtlinienzuordnungen für Domäne aktivieren** aus.
4. Wählen Sie die Seite **Zertifikatfilter** aus, und klicken Sie auf **Hinzufügen...**, um den Dialog **Richtlinienzuordnung für Zertifikatfilter** anzuzeigen.
5. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen in diesem und in nachfolgenden Dialogen benötigen.
6. Geben Sie die folgenden erforderlichen Informationen ein, um die Richtlinienzuordnung zu definieren:
   a. Geben Sie den Namen der Registerdefinition des X.509-Benutzerregisters ein, das als **X.509-Quellenregister** für die Richtlinienzuordnung verwendet werden soll. Sie können auch auf **Durchsuchen...** klicken, um die Liste der Registerdefinitionen für die Domäne anzuzeigen und eine Definition auszuwählen.
   b. Klicken Sie auf **Auswählen**, um den Dialog **Zertifikatfilter auswählen** anzuzeigen und einen vorhandenen Zertifikatfilter auszuwählen, der als Basis für die neue Richtlinienzuordnung für Zertifikatfilter dienen soll.

      Anmerkung: Sie **müssen** einen bereits vorhandenen Zertifikatfilter verwenden. Wenn der gewünschte Zertifikatfilter nicht in der Liste enthalten ist, klicken Sie auf **Hinzufügen...**, um einen neuen Zertifikatfilter zu erstellen.
   c. Geben Sie den Namen der Registerdefinition des **Zielregisters** ein, oder klicken Sie auf **Durchsuchen**, um die Liste der Registerdefinitionen für die Domäne anzuzeigen und eine Definition auszuwählen.
   d. Geben Sie den Namen des **Zielbenutzers** an, mit dem alle Zertifikate im **X.509-Quellenregister** abgeglichen werden sollen, die dem Zertifikatfilter entsprechen. Sie können auch auf **Durchsuchen...** klicken, um die Liste der Benutzer für die Domäne anzuzeigen und einen Benutzer auszuwählen.
   e. Optional. Klicken Sie auf **Erweitert...**, um den Dialog **Zuordnung hinzufügen - Erweitert** anzuzeigen. Geben Sie **Suchinformationen** für die Zielbenutzeridentität an, und klicken Sie auf **OK**, um zum Dialog **Richtlinienzuordnung für Zertifikatfilter hinzufügen** zurückzukehren.

      Anmerkung: Wenn sich mindestens zwei Richtlinienzuordnungen mit demselben X.509-Quellenregister und denselben Zertifikatfilterkriterien auf dasselbe Zielregister beziehen, müssen Sie eindeutige Suchinformationen für die Zielbenutzeridentitäten in jeder dieser Richtlinienzuordnungen definieren. Dadurch, dass Sie in dieser Situation Suchinformationen für jede Zielbenutzeridentität definieren, stellen Sie sicher, dass Abgleichsuchoperationen die Identitäten voneinander unterscheiden können. Andernfalls könnten Abgleichsuchoperationen mehrere Zielbenutzeridentitäten zurückgeben. Die Folge solch mehrdeutiger Ergebnisse könnte sein, dass Anwendungen, die EIM benutzen, nicht mehr in der Lage sind, die richtige Zielidentität festzustellen.

7. Klicken Sie auf **OK**, um die neue Richtlinienzuordnung für Zertifikatfilter zu erstellen und zur Seite **Zertifikatfilter** zurückzukehren. Die neue Richtlinienzuordnung wird in der Liste angezeigt.
8. Prüfen Sie, ob die neue Richtlinienzuordnung für das Zielregister aktiviert ist.
9. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und den Dialog **Abgleichrichtlinie** zu verlassen.

Anmerkung: Prüfen Sie, ob die Unterstützung von Abgleichrichtlinien und die Verwendung von Richtlinienzuordnungen für Zielbenutzerregister richtig aktiviert ist. Wenn nicht, kann die Richtlinienzuordnung nicht in Kraft treten.

Zertifikatfilter erstellen:

Ein Zertifikatfilter definiert eine Gruppe gleichartiger DN-Zertifikat-Attribute (DN = registrierte Name) für Benutzer-Zertifikate in einem X.509-Quellenbenutzerregister. Der Zertifikatfilter kann als Basis einer Richtlinienzuordnung für Zertifikatfilter benutzt werden. Der Zertifikatfilter in einer Richt- linienzuordnung bestimmt, welche Zertifikate in dem angegebenen X.509-Quellenregister mit dem angegebenen Zielbenutzer abgeglichen werden. Diese Zertifikate, die Informationen zum registrierten Namen des Zertifikatinhabers und zum registrierten Namen des Zertifikatausstellers enthalten, die mit den Kriterien des Filters übereinstimmen, werden während der Ausführung der EIM-Abgleichsuchoperationen dem angegebenen Zielbenutzer zugeordnet.

Um einen Zertifikatfilter erstellen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die Zugriffssteuerung (siehe „EIM-Zugriffssteuerung” auf Seite 42) für einen der folgenden Aufgabenbereiche verfügen:

- EIM-Administrator
- Registeradministrator
- Administrator für ausgewählte Register (für die Registerdefinition, die sich auf das X.509-Benutzerregister bezieht, für das der Zertifikatfilter erstellt werden soll)

Ein Zertifikatfilter wird auf der Basis bestimmter DN-Informationen aus einem digitalen Zertifikat erstellt. Als DN-Informationen können Sie entweder den registrierten Namen des Zertifikatinhabers oder den registrierten Namen des Zertifikatausstellers angeben. Der registrierte Name für einen Zertifikatfilter kann vollständig oder teilweise angegeben werden.

Wenn Sie den Zertifikatfilter einer Richtlinienzuordnung für Zertifikatfilter hinzufügen, bestimmt der Filter, welche Zertifikate in einem X.509-Register mit der Zielbenutzeridentität abgeglichen werden, die von der Richtlinienzuordnung angeben wird. Wenn ein digitales Zertifikat die Quellenbenutzeridentität in einer EIM-Abgleichsuchoperation ist (nachdem die anfordernde Anwendung den Namen der Benutzeridentität mit der EIM-API `eimFormatUserIdentity()` formatiert hat), und die Richtlinienzuordnung für Zertifikatfilter zutrifft, vergleicht EIM die DN-Informationen im Zertifikat mit denen im Filter. Wenn beide übereinstimmen, gibt EIM die Zielbenutzeridentität zurück, die von der Richtlinienzuordnung für Zertifikatfilter angegeben wird.

Wenn Sie den Zertifikatfilter erstellen, haben Sie drei Möglichkeiten, um den erforderlichen registrierten Namen anzugeben:

- Sie können den registrierten Namen eines bestimmten Zertifikats vollständig oder teilweise als **Registrierten Namen des Zertifikatinhabers** und/oder als **Registrierten Namen des Zertifikatausstellers** eingeben.
- Sie können Informationen aus einem bestimmten Zertifikat in die Zwischenablage kopieren und damit eine Liste von Zertifikatfilterkandidaten generieren, die auf den Informationen für den registrierten Namen im Zertifikat basiert. Sie können dann die registrierten Namens für den Zertifikatfilter auswählen.

Anmerkung: Wenn Sie die erforderlichen Informationen für den registrieren Namen generieren möchten, um einen Zertifikatfilter zu erstellen, müssen Sie zuerst die Informationen des Zertifikats in die Zwischenablage kopieren, bevor Sie diese Task ausführen können. Das Zertifikat muss außerdem in einem Base64-verschlüsselten Format vorliegen. Weitere Informationen über Methoden zum Erhalt von Zertifikaten im richtigen Format, finden Sie unter Zertifikatfilter.

- Sie können eine Liste von Zertifikatfilterkandidaten generieren, die auf den Informationen für den registrierten Namen in einem digitalen Zertifikat basiert, für das eine Quellenzuordnung zu einer EIM-Kennung vorhanden ist. Sie können dann die registrierten Namens für den Zertifikatfilter auswählen.

Führen Sie die folgenden Schritte durch, um einen Zertifikatfilter zu erstellen, der als Basis für eine Richtlinienzuordnung für Zertifikatfilter dienen soll:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Klicken Sie mit der rechten Maustaste auf die EIM-Domäne, in der Sie arbeiten möchten, und wählen Sie **Abgleichrichtlinie...** aus.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Wählen Sie die Seite **Zertifikatfilter** aus, und klicken Sie auf **Zertifikatfilter...**, um den Dialog **Zertifikatfilter** anzuzeigen.

   Anmerkung: Wenn Sie auf **Zertifikatfilter...** klicken, ohne eine Richtlinienzuordnung auszuwählen, wird der Dialog **EIM-Register durchsuchen** angezeigt. In diesem Dialog können Sie ein X.509-Register aus einer Liste von X.509-Registerdefinitionen in der Domäne auswählen, für das Zertifikatfilter angezeigt werden sollen. Der Inhalt der Liste richtet sich danach, welche EIM-Zugriffssteuerung Sie besitzen.
4. Klicken Sie auf **Hinzufügen...**, um den Dialog **Zertifikatfilter hinzufügen** anzuzeigen.
5. Im Dialog **Zertifikatfilter hinzufügen** müssen Sie auswählen, ob ein einzelner Zertifikatfilter hinzugefügt oder ein Zertifikatfilter auf der Basis eines bestimmten digitalen Zertifikats generiert werden soll. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen in diesem und in nachfolgenden Dialogen benötigen.
   a. Wenn Sie **Einzelnen Zertifikatfilter hinzufügen** auswählen, können Sie den **registrierten Namen des Zertifikatinhabers**, den **registrierten Namen des Zertifikatausstellers** oder beide vollständig oder teilweise angeben. Klicken Sie auf **OK**, um den Zertifikatfilter zu erstellen und zum Dialog **Zertifikatfilter** zurückzukehren. Die Filter wird jetzt in der Liste angezeigt.
   b. Wenn Sie **Zertifikatfilter aus einem digitalen Zertifikat generieren** auswählen, klicken Sie auf **OK**, um den Dialog **Zertifikatfilter generieren** anzuzeigen.
      1) Fügen Sie die verschlüsselte Base64-Version der Zertifikatinformationen, die Sie zuvor in Ihre Zwischenablage kopiert haben, in das Feld **Zertifikatinformationen** ein.
      2) Klicken Sie auf **OK**, um eine Liste potenzieller Zertifikatfilter auf der Basis des **registrierten Namens des Zertifikatinhabers** und des **registrierten Namens des Zertifikatausstellers** zu generieren.
      3) Wählen Sie im Dialog **Zertifikatfilter durchsuchen** einen oder mehrere dieser Zertifikatfilter aus. Klicken Sie auf **OK**, um zum Dialog **Zertifikatfilter auswählen** zurückzukehren, in dem jetzt die ausgewählten Zertifikatfilter angezeigt werden.
   c. Wenn Sie **Zertifikatfilter aus einer Quellenzuordnung für einen X.509-Benutzer generieren** auswählen, müssen Sie auf **OK** klicken, um den Dialog **Zertifikatfilter generieren** anzuzeigen. Dieser Dialog enthält eine Liste der X.509-Benutzeridentitäten, die Quellenzuordnungen zu einer EIM-Kennung in der Domäne besitzen.
      1) Wählen Sie die X.509-Benutzeridentität aus, deren digitales Zertifikat Sie verwenden möchten, um einen oder mehrere Zertifikatfilterkandidaten zu generieren, und klicken Sie auf **OK**.

2) Klicken Sie auf **OK**, um eine Liste potenzieller Zertifikatfilter auf der Basis des **registrierten Namens des Zertifikatinhabers** und des **registrierten Namens des Zertifikatausstellers** zu generieren.
3) Wählen Sie im Dialog **Zertifikatfilter durchsuchen** einen oder mehrere dieser potenziellen Zertifikatfilter aus. Klicken Sie auf **OK**, um zum Dialog **Zertifikatfilter auswählen** zurückzukehren, in dem jetzt die ausgewählten Zertifikatfilter angezeigt werden.

Sie können den neuen Zertifikatfilter jetzt als Basis für die Erstellung einer Richtlinienzuordnung für Zertifikatfilter verwenden.

Suchinformationen einer Zielbenutzeridentität hinzufügen

Suchinformationen sind optionale eindeutige Kennzeichnungsdaten für die Zielbenutzeridentität in einer Zuordnung. Bei dieser Zuordnung kann es sich entweder um eine Kennungsziel- oder eine Richtlinienzuordnung handeln. Suchinformationen sind nur erforderlich, wenn eine Abgleichsuchoperation mehrere Zielbenutzeridentitäten zurückgibt. Diese Situation kann bei EIM-fähigen Anwendungen (einschließlich i5/OS-Anwendungen und -Produkten), die die Verarbeitung solch mehrdeutiger Ergebnisse nicht unterstützen, zu Problemen führen.

Wenn nötig, können Sie jeder Zielbenutzeridentität eindeutige Suchinformationen hinzufügen, um sie detaillierter zu beschreiben. Diese Suchinformationen für eine Zielbenutzeridentität müssen der Abgleichsuchoperation zur Verfügung gestellt werden, um sicherzustellen, dass die Operation eine eindeutige Zielbenutzeridentität zurückgibt. Andernfalls sind Anwendungen, die sich auf EIM stützen, möglicherweise nicht in der Lage, die zu verwendende Zielidentität genau zu bestimmen.

Anmerkung: Wenn EIM-Suchoperationen nicht mehrere Zielbenutzeridentitäten zurückgeben sollen, müssen Sie Ihre EIM-Zuordnungskonfiguration korrigieren, statt das Problem mit Hilfe von Suchinformationen zu beheben. Weitere Informationen hierzu finden Sie unter „Fehlerbehebung beim EIM-Abgleich" auf Seite 134.

Die Vorgehensweise beim Hinzufügen von Suchinformationen zur detaillierten Beschreibung einer Zielbenutzeridentität variiert, je nachdem, ob die Zielbenutzeridentität in einer Kennungs- oder einer Zielzuordnung definiert ist. Doch unabhängig davon, wie die Suchinformationen hinzugefügt werden - sie werden auf jeden Fall mit der Zielbenutzeridentität und nicht mit der jeweiligen Kennungs- oder der Richtlinienzuordnung verknüpft.

Suchinformationen einer Zielbenutzeridentität in einer Kennungszuordnung hinzufügen:

Um der Zielbenutzeridentität in einer Kennungszuordnung Suchinformationen hinzufügen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die Zugriffssteuerung (siehe „EIM-Zugriffssteuerung" auf Seite 42) für einen der folgenden Aufgabenbereiche verfügen:

- Registeradministrator
- Administrator für ausgewählte Register (für die Registerdefinition, die sich auf das Benutzerregister bezieht, in dem die Zielbenutzeridentität enthalten ist)
- EIM-Administrator

Führen Sie die folgenden Schritte durch, um der Zielbenutzeridentität in einer Kennungszuordnung Suchinformationen hinzufügen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.

- Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.

3. Erweitern Sie die EIM-Domäne, mit der Sie verbunden sind.
4. Klicken Sie auf **Kennungen**, um die Liste der EIM-Kennungen für die Domäne anzuzeigen.

   Anmerkung: Gelegentlich kann es beim Erweitern des Ordners **Kennungen** einige Zeit dauern, bis die Liste der Kennungen angezeigt wird. Um die Leistung zu verbessern, wenn in der Domäne eine große Anzahl von EIM-Kennungen definiert ist, können Sie die Sicht des Ordners **Kennungen** anpassen, indem Sie den Suchwert einschränken, der bei der Anzeige von Kennungen verwendet wird. Klicken Sie mit der rechten Maustaste auf **Kennungen**, wählen Sie **Diese Ansicht anpassen... > Anzeigeoptionen** aus, und geben Sie die Anzeigekriterien für die Liste der EIM-Kennungen an, die in die Sicht aufgenommen werden sollen.
5. Klicken Sie mit der rechten Maustaste auf eine EIM-Kennung, und wählen Sie **Eigenschaften...** aus.
6. Wählen Sie die Seite **Zuordnungen** aus, wählen Sie die Zielzuordnung aus, zu der Sie Suchinformationen hinzufügen möchten, und klicken Sie auf **Details...**. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen benötigen.
7. Geben Sie im Dialog **Zuordnung - Details** die **Suchinformationen** an, mit denen Sie die Zielbenutzeridentität in dieser Zuordnung genauer beschreiben möchten, und klicken Sie auf **Hinzufügen**.
8. Wiederholen Sie diesen Schritt für alle Suchinformationen, die Sie der Zuordnung hinzufügen möchten.
9. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Dialog **Zuordnung - Details** zurückzukehren.
10. Klicken Sie auf **OK**, um den Dialog zu verlassen.

Suchinformationen einer Zielbenutzeridentität in einer Richtlinienzuordnung hinzufügen:

Um der Zielbenutzeridentität in einer Richtlinienzuordnung Suchinformationen hinzufügen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die Zugriffssteuerung (siehe „EIM-Zugriffssteuerung" auf Seite 42) für einen der folgenden Aufgabenbereiche verfügen:

- Registeradministrator
- Administrator für ausgewählte Register (für die Registerdefinition, die sich auf das Benutzerregister bezieht, in dem die Zielbenutzeridentität enthalten ist)
- EIM-Administrator

Führen Sie die folgenden Schritte durch, um der Zielbenutzeridentität in einer Richtlinienzuordnung Suchinformationen hinzufügen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Verwenden Sie im Dialog **Abgleichrichtlinie** die Seiten, auf denen die Richtlinienzuordnungen für die Domäne angezeigt werden.
4. Wählen Sie die Richtlinienzuordnung für das Zielregister aus, das die Zielbenutzeridentität enthält, der Sie Suchinformationen hinzufügen möchten.
5. Klicken Sie auf **Details...**, um den entsprechenden Dialog **Richtlinienzuordnung - Details** für den Typ der Richtlinie anzuzeigen, den Sie ausgewählt haben. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen benötigen.

6. Geben Sie die **Suchinformationen** an, mit denen Sie die Zielbenutzeridentität in dieser Richtlinienzuordnung genauer beschreiben möchten, und klicken Sie auf **Hinzufügen**. Wiederholen Sie diesen Schritt für alle Suchinformationen, die Sie der Zuordnung hinzufügen möchten.
7. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Ausgangsdialog **Richtlinienzuordnung - Details** zurückzukehren.
8. Klicken Sie auf **OK**, um den Dialog zu verlassen.

Suchinformationen für Zielbenutzeridentität entfernen

Suchinformationen sind optionale eindeutige Kennzeichnungsdaten für die Zielbenutzeridentität in einer Zuordnung. Bei dieser Zuordnung kann es sich entweder um eine Kennungsziel- oder eine Richtlinienzuordnung handeln. Suchinformationen sind nur erforderlich, wenn eine Abgleichsuchoperation mehrere ZielBenutzeridentitäten zurückgeben kann. Diese Situation kann bei EIM-fähigen Anwendungen (einschließlich i5/OS-Anwendungen und -Produkten), die die Verarbeitung solch mehrdeutiger Ergebnisse nicht unterstützen, zu Problemen führen.

Diese Suchinformationen müssen der Abgleichsuchoperation zur Verfügung gestellt werden, um sicherzustellen, dass die Operation eine eindeutige ZielBenutzeridentität zurückgibt. Wenn zuvor definierte Suchinformationen jedoch nicht mehr benötigt werden, können Sie diese entfernen, damit sie nicht mehr für Suchoperationen zur Verfügung gestellt werden müssen.

Die Vorgehensweise beim Entfernen von Suchinformationen für eine Zielbenutzeridentität variiert, je nachdem, ob die Zielbenutzeridentität in einer Kennungs- oder einer Zielzuordnung definiert ist. Suchinformationen werden auf jeden Fall mit der Zielbenutzeridentität und nicht mit der jeweiligen Kennungs- oder der Richtlinienzuordnung verknüpft. Folglich werden sowohl die Benutzeridentität als auch die Suchinformationen aus der EIM-Domäne gelöscht, wenn Sie die letzte Kennungs- oder Richtlinienzuordnung löschen, die diese Zielbenutzeridentität definieren.

Suchinformationen für Zielbenutzeridentität in einer Kennungszuordnung entfernen:

Um Suchinformationen für die Zielbenutzeridentität in einer Kennungszuordnung entfernen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die Zugriffssteuerung (siehe „EIM-Zugriffssteuerung" auf Seite 42) für einen der folgenden Aufgabenbereiche verfügen:

- Registeradministrator
- Administrator für ausgewählte Register (für die Registerdefinition, die sich auf das Benutzerregister bezieht, in dem die Zielbenutzeridentität enthalten ist)
- EIM-Administrator

Führen Sie die folgenden Schritte durch, um Suchinformationen für die Zielbenutzeridentität in einer Kennungszuordnung zu entfernen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Erweitern Sie die EIM-Domäne, mit der Sie verbunden sind.
4. Klicken Sie auf **Kennungen**, um die Liste der EIM-Kennungen für die Domäne anzuzeigen.

   Anmerkung: Gelegentlich kann es beim Erweitern des Ordners **Kennungen** einige Zeit dauern, bis die Liste der Kennungen angezeigt wird. Um die Leistung zu verbessern, wenn in der Domäne eine große Anzahl von EIM-Kennungen definiert ist, können Sie die Sicht des Ordners **Kennungen** anpassen, indem Sie den Suchwert einschränken, der bei der

Anzeige von Kennungen verwendet wird. Klicken Sie mit der rechten Maustaste auf **Kennungen**, wählen Sie **Diese Ansicht anpassen... > Anzeigeoptionen** aus, und geben Sie die Anzeigekriterien für die Liste der EIM-Kennungen an, die in die Sicht aufgenommen werden sollen.

5. Klicken Sie mit der rechten Maustaste auf eine EIM-Kennung, und wählen Sie **Eigenschaften...** aus.
6. Wählen Sie die Seite **Zuordnungen** aus, wählen Sie die Zielzuordnung für die Benutzeridentität aus, für die Sie Suchinformationen entfernen möchten, und klicken Sie auf **Details...**.
7. Wählen Sie im Dialog **Zuordnung - Details** die Suchinformationen aus, die Sie für die Zielbenutzeridentität entfernen möchten, und klicken Sie auf **Entfernen**.

   Anmerkung: Wenn Sie auf **Entfernen** klicken, wird keine Bestätigungsaufforderung angezeigt.
8. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Dialog **Zuordnung - Details** zurückzukehren.
9. Klicken Sie auf **OK**, um den Dialog zu verlassen.

Suchinformationen für Zielbenutzeridentität in einer Richtlinienzuordnung entfernen:

Um Suchinformationen für die Zielbenutzeridentität in einer Richtlinienzuordnung entfernen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die Zugriffssteuerung (siehe „EIM-Zugriffssteuerung" auf Seite 42) für einen der folgenden Aufgabenbereiche verfügen:

- Registeradministrator
- Administrator für ausgewählte Register (für die Registerdefinition, die sich auf das Benutzerregister bezieht, in dem die Zielbenutzeridentität enthalten ist)
- EIM-Administrator

Führen Sie die folgenden Schritte durch, um Suchinformationen für die Zielbenutzeridentität in einer Richtlinienzuordnung zu entfernen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Verwenden Sie im Dialog **Abgleichrichtlinie** die Seiten, auf denen die Richtlinienzuordnungen für die Domäne angezeigt werden.
4. Wählen Sie die Richtlinienzuordnung für das Zielregister aus, das die Zielbenutzeridentität enthält, für die Sie Suchinformationen entfernen möchten.
5. Klicken Sie auf **Details...**, um den entsprechenden Dialog **Richtlinienzuordnung - Details** für den Typ der Richtlinie anzuzeigen, den Sie ausgewählt haben.
6. Wählen Sie die Suchinformationen aus, die Sie für die Zielbenutzeridentität entfernen möchten, und klicken Sie auf **Entfernen**.

   Anmerkung: Wenn Sie auf **Entfernen** klicken, wird keine Bestätigungsaufforderung angezeigt.
7. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Ausgangsdialog **Richtlinienzuordnung - Details** zurückzukehren.
8. Klicken Sie auf **OK**, um den Dialog zu verlassen.

Alle Kennungszuordnungen für eine EIM-Kennung anzeigen

Um alle Zuordnungen für eine EIM-Kennung anzeigen zu können, müssen Sie mit der EIM-Domäne verbunden sein, in der Sie arbeiten möchten, und über die zur Ausführung dieser Task erforderliche

„EIM-Zugriffssteuerung" auf Seite 42 verfügen. Sie können alle Zuordnungen mit allen Zugriffssteuerungsebenen außer "Administrator für ausgewählte Register" anzeigen. Diese Zugriffssteuerungsebene gestattet Ihnen nur die Auflistung und Anzeige derjenigen Zuordnungen zu Registern, für die Sie explizit berechtigt sind, es sei denn, Sie verfügen außerdem über die Zugriffssteuerung für EIM-Abgleichsuchoperationen.

Führen Sie die folgenden Schritte durch, um alle Zuordnungen zwischen einer EIM-Kennung und den Benutzeridentitäten (IDs) anzuzeigen, für die Kennungszuordnungen definiert sind:

Führen Sie die folgenden Schritte durch, um die Zuordnungen für eine Kennung anzuzeigen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Erweitern Sie die EIM-Domäne, mit der Sie verbunden sind.
4. Klicken Sie auf **Kennungen**, um die Liste der EIM-Kennungen für die Domäne anzuzeigen.

   Anmerkung: Gelegentlich kann es beim Erweitern des Ordners **Kennungen** einige Zeit dauern, bis die Liste der Kennungen angezeigt wird. Um die Leistung zu verbessern, wenn in der Domäne eine große Anzahl von EIM-Kennungen definiert ist, können Sie die Sicht des Ordners **Kennungen** anpassen, indem Sie den Suchwert einschränken, der bei der Anzeige von Kennungen verwendet wird. Klicken Sie mit der rechten Maustaste auf **Kennungen**, wählen Sie **Diese Ansicht anpassen... > Anzeigeoptionen** aus, und geben Sie die Anzeigekriterien für die Liste der EIM-Kennungen an, die in die Sicht aufgenommen werden sollen.
5. Wählen Sie eine EIM-Kennung aus, klicken Sie mit der rechten Maustaste auf die EIM-Kennung, und wählen Sie **Eigenschaften** aus.
6. Wählen Sie die Seite **Zuordnungen** aus, um eine Liste der zugeordneten Benutzeridentitäten für die ausgewählte EIM-Kennung anzuzeigen.
7. Klicken Sie auf **OK**, um den Vorgang zu beenden.

Alle Richtlinienzuordnungen einer Domäne anzeigen

Um alle Richtlinienzuordnungen einer Domäne anzeigen zu können, müssen Sie mit der EIM-Domäne verbunden sein, in der Sie arbeiten möchten, und über die zur Ausführung dieser Task erforderliche „EIM-Zugriffssteuerung" auf Seite 42 verfügen. Sie können alle Richtlinienzuordnungen mit allen Zugriffssteuerungsebenen außer "Administrator für ausgewählte Register" anzeigen. Diese Zugriffssteuerungsebene gestattet Ihnen nur die Auflistung und Anzeige derjenigen Zuordnungen zu Registern, für die Sie explizit berechtigt sind. Folglich können Sie mit dieser Zugriffssteuerung keine Standardrichtlinienzuordnungen für Domänen auflisten oder anzeigen, es sei denn, Sie verfügen außerdem über die Zugriffssteuerung für EIM-Abgleichsuchoperationen.

Führen Sie die folgenden Schritte durch, um alle Richtlinienzuordnungen für eine Domäne anzuzeigen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Klicken Sie mit der rechten Maustaste auf die EIM-Domäne, in der Sie arbeiten möchten, und wählen Sie **Abgleichrichtlinie...** aus.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Wählen Sie eine Seite aus, um die für die Domäne definierten Richtlinienzuordnungen anzuzeigen:

a. Wählen Sie die Seite **Domäne** aus, um die für die Domäne definierten Standardrichtlinienzuordnungen für Domänen anzuzeigen und um festzustellen, ob eine Richtlinienzuordnung auf Registerebene aktiviert ist.
b. Wählen Sie die Seite **Register** aus, um die für die Domäne definierten Standardrichtlinienzuordnungen für Register anzuzeigen. Sie können außerdem anzeigen, welchen Quellen- und Zielregister von den Richtlinienzuordnungen betroffen sind.
c. Wählen Sie die Seite **Zertifikatfilter** aus, um die auf Registerebene definierten und aktivierten Richtlinienzuordnungen für Zertifikatfilter anzuzeigen.

4. Klicken Sie auf **OK**, um den Vorgang zu beenden.

Alle Richtlinienzuordnungen für eine Registerdefinition anzeigen

Um alle Richtlinienzuordnungen für ein bestimmtes Register anzeigen zu können, müssen Sie mit der EIM-Domäne verbunden sein, in der Sie arbeiten möchten, und über die zur Ausführung dieser Task erforderliche „EIM-Zugriffssteuerung" auf Seite 42 verfügen. Sie können alle Richtlinienzuordnungen mit allen Zugriffssteuerungsebenen außer "Administrator für ausgewählte Register" anzeigen. Diese Zugriffssteuerungsebene gestattet Ihnen nur die Auflistung und Anzeige derjenigen Zuordnungen zu Registern, für die Sie explizit berechtigt sind. Folglich können Sie mit dieser Zugriffssteuerung keine Standardrichtlinienzuordnungen für Domäne auflisten oder anzeigen, es sei denn, Sie verfügen außerdem über die Zugriffssteuerung für EIM-Abgleichsuchoperationen.

Führen Sie die folgenden Schritte durch, um alle Richtlinienzuordnungen für eine Registerdefinition anzuzeigen.

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Klicken Sie mit der rechten Maustaste auf die Registerdefinition, mit der Sie arbeiten möchten, und wählen Sie **Abgleichrichtlinie...** aus.
4. Wählen Sie eine Seite aus, um die für die angegebene Registerdefinition definierten Richtlinienzuordnungen anzuzeigen:
   - Wählen Sie die Seite **Domäne** aus, um die für das Register definierten Standardrichtlinienzuordnungen für Domänen anzuzeigen.
   - Wählen Sie die Seite **Register** aus, um die für das Register definierten und aktivierten Standardrichtlinienzuordnungen für Register anzuzeigen.
   - Wählen Sie die Seite **Zertifikatfilter** aus, um die für das Register definierten und aktivierten Richtlinienzuordnungen für Zertifikatfilter anzuzeigen.
5. Klicken Sie auf **OK**, um den Vorgang zu beenden.

Kennungszuordnung löschen

Um eine Kennungszuordnung löschen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die Zugriffssteuerung (siehe „EIM-Zugriffssteuerung" auf Seite 42) verfügen, die zum Löschen des gewünschten Zuordnungstyps erforderlich ist.

Um eine Quellen- oder eine administrative Zuordnung löschen zu können, müssen Sie über die EIM-Zugriffssteuerung für einen der folgenden Aufgabenbereiche verfügen:

- Kennungsadministrator
- EIM-Administrator

Um eine Zielzuordnung löschen zu können, müssen Sie über die EIM-Zugriffssteuerung für einen der folgenden Aufgabenbereiche verfügen:

- Registeradministrator
- Administrator für ausgewählte Register (für die Registerdefinition, die sich auf das Benutzerregister bezieht, in dem die Zielbenutzeridentität enthalten ist)
- EIM-Administrator

Führen Sie die folgenden Schritte durch, um eine Kennungszuordnung zu löschen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Erweitern Sie die EIM-Domäne, mit der Sie verbunden sind.
4. Klicken Sie auf **Kennungen**, um die Liste der EIM-Kennungen für die Domäne anzuzeigen.

   Anmerkung: Gelegentlich kann es beim Erweitern des Ordners **Kennungen** einige Zeit dauern, bis die Liste der Kennungen angezeigt wird. Um die Leistung in einem solchen Fall zu erhöhen, können Sie die Sicht des Ordners **Kennungen** anpassen, indem Sie die Suchkriterien für die Anzeige der Kennungen eingrenzen. Klicken Sie mit der rechten Maustaste auf **Kennungen**, wählen Sie **Diese Ansicht anpassen... > Anzeigeoptionen** aus, und geben Sie die Anzeigekriterien für die Liste der EIM-Kennungen an, die in die Sicht aufgenommen werden sollen.
5. Wählen Sie eine EIM-Kennung aus, klicken Sie mit der rechten Maustaste auf die EIM-Kennung, und wählen Sie **Eigenschaften** aus.
6. Wählen Sie die Seite **Zuordnungen** aus, um eine Liste der zugeordneten Benutzeridentitäten für die ausgewählte EIM-Kennung anzuzeigen.
7. Wählen Sie die Zuordnung aus, die Sie löschen möchten, und klicken Sie auf **Entfernen**.

   Anmerkung: Wenn Sie auf **Entfernen** klicken, wird keine Bestätigungsaufforderung angezeigt.
8. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Anmerkung: Wenn Sie eine Zielzuordnung entfernen, kann es zu Fehlern bei Abgleichsuchoperationen für das Zielregister kommen, die sich auf die gelöschte Zuordnung stützen, sofern es keine anderen Zuordnungen (Richtlinienzuordnungen oder Kennungszuordnungen) für das betroffene Zielregister gibt.

Die einzige Möglichkeit, eine Benutzeridentität für EIM zu definieren, besteht darin, diese Identität während der Erstellung einer Kennungs- oder einer Richtlinienzuordnung anzugeben. Folglich ist diese Benutzeridentität nicht mehr in EIM definiert, wenn Sie die letzte Zielzuordnung für die Benutzeridentität löschen (entweder durch Entfernen einer bestimmten Zielzuordnung oder durch Entfernen einer Richtlinienzuordnung). In diesem Fall gehen dann auch der Name der Benutzeridentität und alle Suchinformationen verloren.

Richtlinienzuordnung löschen

Um eine Richtlinienzuordnung löschen zu können, müssen Sie mit der EIM-Domäne, in der gearbeitet werden soll, verbunden sein und über die „EIM-Zugriffssteuerung" auf Seite 42 für einen der folgenden Aufgabenbereiche verfügen:

- Registeradministrator
- EIM-Administrator

Führen Sie die folgenden Schritte durch, um eine Richtlinienzuordnung zu löschen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Wählen Sie die entsprechende Seite für den Typ der Richtlinienzuordnung aus, den Sie löschen möchten.
4. Wählen Sie auf dieser Seite dann die entsprechende Richtlinienzuordnung aus, und klicken Sie auf **Entfernen**.

   Anmerkung: Wenn Sie auf **Entfernen** klicken, wird keine Bestätigungsaufforderung angezeigt.
5. Klicken Sie auf **OK**, um den Dialog **Abgleichrichtlinie** zu verlassen und Ihre Änderungen zu speichern.

Anmerkung: Wenn Sie eine Zielrichtlinienzuordnung entfernen, kann es zu Fehlern bei Abgleichsuchoperationen für das Zielregister kommen, die sich auf die gelöschte Richtlinienzuordnung stützen, sofern es keine anderen Zuordnungen (Richtlinienzuordnungen oder Kennungszuordnungen) für das betroffene Zielregister gibt.

Die einzige Möglichkeit, eine Benutzeridentität für EIM zu definieren, besteht darin, diese Identität während der Erstellung einer Kennungs- oder einer Richtlinienzuordnung anzugeben. Folglich ist diese Benutzeridentität nicht mehr in EIM definiert, wenn Sie die letzte Zielzuordnung für die Benutzeridentität löschen (entweder durch Entfernen einer bestimmten Zielzuordnung oder durch Entfernen einer Richtlinienzuordnung). In diesem Fall gehen dann auch der Name der Benutzeridentität und alle Suchinformationen verloren.

Zugehörige Konzepte

„EIM-Registerdefinitionen verwalten" auf Seite 101
In diesem Abschnitt wird erläutert, wie die EIM-Registerdefinitionen (EIM = Enterprise Identity Mapping) für die Benutzerregister in Ihrem Unternehmen, die EIM nutzen, erstellt und verwaltet werden können.

EIM-Benutzerzugriffssteuerung verwalten

Im Folgenden wird erläutert, wie der Benutzerzugriff mit LDAP verwaltet werden kann.

Ein EIM-Benutzer (EIM = Enterprise Identity Mapping) ist ein Benutzer, der über die „EIM-Zugriffssteuerung" auf Seite 42 verfügt. Diese wird auf der Basis seiner Zugehörigkeit zu einer vordefinierten LDAP-Benutzergruppe (LDAP = Lightweight Directory Access Protocol) gewährt. Mit Erteilung der EIM-Zugriffssteuerung wird der entsprechende Benutzer einer bestimmten LDAP-Benutzergruppe hinzugefügt. Jede LDAP-Gruppe ist berechtigt, diverse EIM-Verwaltungstasks in der Domäne auszuführen. Art und Umfang der Verwaltungstasks, einschließlich Suchoperationen, die ein Benutzer ausführen darf, richten sich danach, welcher Zugriffssteuerungsgruppe der EIM-Benutzer angehört.

Nur Benutzer mit der Zugriffssteuerung LDAP-Administrator oder EIM-Administrator können andere Benutzer zu einer EIM-Zugriffssteuerungsgruppe hinzufügen oder Zugriffssteuerungseinstellungen für andere Benutzer ändern. Bevor ein Benutzer Mitglied einer EIM-Zugriffssteuerungsgruppe werden kann, muss für diesen Benutzer ein Eintrag in dem Directory-Server vorhanden sein, der als EIM-Domänencontroller dient. Außerdem können nur bestimmte Benutzertypen Mitglied einer EIM-Zugriffssteuerungsgruppe werden, nämlich Kerberos-Principals, registrierte Namen und i5/OS-Benutzerprofile.

Anmerkung: Damit ein Kerberos-Principal in EIM verfügbar ist, muss der Netzwerkauthentifizierungsservice auf dem System konfiguriert sein. Damit ein i5/OS-Benutzerprofil in EIM verfügbar

ist, müssen Sie ein Systemobjektsuffix auf dem Directory-Server konfigurieren. Mit Hilfe dieses Suffix kann der Directory-Server auf i5/OS-Systemobjekte wie beispielsweise i5/OS-Benutzerprofile verweisen.

Führen Sie die folgenden Schritte durch, um die Zugriffssteuerung für einen vorhandenen Directory-Server-Benutzer zu verwalten oder einen vorhandenen Directory-Server-Benutzer zu einer EIM-Zugriffssteuerungsgruppe hinzuzufügen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.
2. Wählen Sie die EIM-Domäne aus, in der Sie arbeiten möchten.
   - Wird die gewünschte EIM-Domäne nicht unter **Domänenverwaltung** aufgelistet, lesen Sie unter „EIM-Domäne zum Ordner Domänenverwaltung hinzufügen" auf Seite 96 nach.
   - Wenn momentan keine Verbindung zu der EIM-Domäne besteht, in der Sie arbeiten möchten, lesen Sie unter Verbindung zum EIM-Domänencontroller herstellen nach.
3. Klicken Sie mit der rechten Maustaste auf die EIM-Domäne, mit der Sie verbunden sind, und wählen Sie **Zugriffssteuerung...** aus.
4. Wählen Sie im Dialog **EIM-Zugriffssteuerung bearbeiten** den **Benutzerstatus** aus, um die Felder für die Angabe der Benutzerkenndaten anzuzeigen.
5. Geben Sie die erforderlichen Informationen für den Benutzer ein, der die EIM-Zugriffssteuerung verwalten soll, und klicken Sie auf **OK**, um die Anzeige **EIM-Zugriffssteuerung bearbeiten** aufzurufen. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen benötigen.
6. Wählen Sie eine oder mehrere **Zugriffssteuerungsgruppen** für den Benutzer aus, und klicken Sie auf **OK**, um den Benutzer zu den ausgewählten Gruppen hinzuzufügen. Klicken Sie auf **Hilfe**, wenn Sie weitere Informationen über die Berechtigungen der einzelnen Gruppen sowie über besondere Voraussetzungen wünschen.
7. Klicken Sie nach Eingabe aller erforderlichen Informationen auf **OK**, um Ihre Änderungen zu speichern.

EIM-Konfigurationseigenschaften verwalten

Im Folgenden wird erläutert, wie Sie verschiedene Eigenschaften von EIM (Enterprise Identity Mapping) konfigurieren können. Hierzu gehören z. B. Domänen, Benutzeridentitäten und Registerdefinitionen.

Sie können eine Reihe unterschiedlicher EIM-Konfigurationseigenschaften für Ihren Server verwalten. Normalerweise wird dies nicht häufig vorkommen, doch es gibt Situationen, in denen eine Änderung der Konfigurationseigenschaften erforderlich wird. Wenn beispielsweise Ihr System ausfällt und Sie Ihre EIM-Konfigurationseigenschaften erneut erstellen müssen, können Sie entweder den EIM-Konfigurationsassistenten erneut ausführen oder die Eigenschaften wie hier beschrieben ändern. Eine weiteres Beispiel: Wenn Sie bei Ausführung des EIM-Konfigurationsassistenten entschieden haben, keine Registerdefini- tionen für die lokalen Register zu erstellen, können Sie die Registerdefinition wie hier beschrieben aktualisieren.

Sie können folgende Eigenschaften ändern:

- Die EIM-Domäne, zu der der Server gehört.
- Die Verbindungsinformationen für den EIM-Domänencontroller.
- Die Benutzeridentität, mit der das System EIM-Operationen für Betriebssystemfunktionen ausführt.
- Die Namen der Registerdefinitionen, die die Benutzerregister bezeichnen, die das System bei der Ausführung von EIM-Operationen für Betriebssystemfunktionen verwenden kann. Diese Registerdefi- nitionsnamen beziehen sich auf die lokalen Benutzerregister, die Sie bei Ausführung des EIM-Konfigurationsassistenten erstellt haben.

  Anmerkung: Wenn Sie sich bei Ausführung des EIM-Konfigurationsassistenten dafür entschieden haben, keine lokalen Registerdefinitionsnamen zu erstellen - entweder, weil die Register bereits in der EIM-Domäne definiert waren oder weil Sie sie zu einem späteren Zeitpunkt

definieren wollten - müssen Sie die Eigenschaften der Systemkonfiguration an dieser Stelle mit diesen Registerdefinitionsnamen aktualisieren. Das System benötigt die Registerdefinitionsinformationen, um EIM-Operationen für Betriebssystemfunktionen ausführen zu können.

Um EIM-Konfigurationseigenschaften ändern zu können, benötigen Sie die folgenden Sonderberechtigungen:

- Sicherheitsadministrator (*SECADM)
- Berechtigung für alle Objekte (*ALLOBJ)

Führen Sie die folgenden Schritte durch, um EIM-Konfigurationseigenschaften für Ihren iSeries-Server zu ändern:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping**.
2. Klicken Sie mit der rechten Maustaste auf **Konfiguration**, und wählen Sie **Eigenschaften** aus.
3. Nehmen Sie die entsprechenden Änderungen an den EIM-Konfigurationsdaten vor.
4. Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen benötigen.
5. Klicken Sie auf **Konfiguration prüfen**, um sicherzustellen, dass das System anhand der angegebenen Informationen in der Lage ist, erfolgreich eine Verbindung zum EIM-Domänencontroller herzustellen.
6. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Anmerkung: Wenn Sie den EIM-Konfigurationsassistenten nicht verwendet haben, um eine Domäne zu erstellen oder ein System zu einer Domäne hinzuzufügen, erstellen Sie keine EIM-Konfiguration, indem Sie die Konfigurationseigenschaften manuell eingeben. Wenn Sie den Assistenten verwenden, um Ihre EIM-Basiskonfiguration zu erstellen, können Sie potenzielle Konfigurationsprobleme vermeiden, denn der Assistent übernimmt noch weitere Aufgaben neben der Konfiguration dieser Eigenschaften.

Fehlerbehebung bei Enterprise Identity Mapping

In diesem Abschnitt sind allgemeine Probleme und Fehler aufgeführt, die bei der Konfiguration und Verwendung von EIM auftreten können. Außerdem werden entsprechende Lösungen vorgeschlagen.

Enterprise Identity Mapping (EIM) ist ein Zusammenschluss mehrerer Technologien sowie zahlreicher Anwendungen und Funktionen. Folglich kann es in vielen Bereichen zu Problemen kommen. Im Folgenden werden einige der Probleme und Fehler beschrieben, die bei der Arbeit mit EIM auftreten können, und es werden Vorschläge zur Fehlerbehebung angeboten.

Zugehörige Informationen

Fehlerbehebung

Fehlerbehebung bei Problemen mit dem Domänencontroller

Zahlreiche Faktoren können dazu führen, dass es beim Versuch, eine Verbindung zum Domänencontroller herzustellen, zu Problemen kommt. Informieren Sie sich anhand der folgenden Tabelle darüber, wie Sie potenzielle Probleme lösen können, die beim Aufbau der Verbindung zum Domänencontroller auftreten können.

Tabelle 27. Verbindung zum Domänencontroller - Probleme und Lösungen

Problem	Lösungen
Sie können keine Verbindung zum Domänencontroller herstellen, wenn Sie zur Verwaltung von EIM den iSeries Navigator benutzen.	Möglicherweise wurden die Verbindungsinformationen für die zu verwaltende Domäne nicht richtig angegeben. Führen Sie die folgenden Schritte durch, um die Verbindungsinformationen zu überprüfen: • Erweitern Sie **Netzwerk-->Enterprise Identity Mapping-->Netzwerk->Domänenverwaltung**. Klicken Sie mit der rechten Maustaste auf die Domäne, die Sie verwalten möchten, und wählen Sie **Eigenschaften** aus. • Überprüfen Sie, ob der Name des **Domänencontrollers** und (falls angegeben) der **Übergeordnete registrierte Name** richtig angegeben sind. • Überprüfen Sie, ob die **Verbindungsinformationen** für den Domänencontroller richtig sind. Vergewissern Sie sich, dass die **Portnummer** richtig ist. Wenn **Sichere Verbindung (SSL oder TLS) verwenden** ausgewählt ist, muss der Directory-Server für die Verwendung von SSL konfiguriert sein. Klicken Sie auf **Verbindung prüfen**, um zu prüfen, ob Sie anhand der angegebenen Informationen eine Verbindung zum Domänencontroller erfolgreich herstellen können. • Überprüfen Sie, ob die Benutzerinformationen in der Anzeige **Verbindung zu Domänencontroller** richtig sind.

Tabelle 27. Verbindung zum Domänencontroller - Probleme und Lösungen (Forts.)

Problem	Lösungen
Das Betriebssystem oder Anwendungen können keine Verbindung zum Domänencontroller herstellen, um auf EIM-Daten zuzugreifen. Beispielsweise schlagen EIM-Abgleichsuchoperationen fehl, die für das System ausgeführt werden. Dies kann durch eine falsche EIM-Konfiguration auf dem System oder den Systemen verursacht werden.	Überprüfen Sie Ihre EIM-Konfiguration. Erweitern Sie **Netzwerk-->Enterprise Identity Mapping-->Konfiguration** auf dem System an dem Sie sich authentifizieren möchten. Klicken Sie mit der rechten Maustaste auf den Ordner **Konfiguration**, wählen Sie **Eigenschaften** aus, und überprüfen Sie Folgendes: • Seite **Domäne**: – Sind der Name des Domänencontrollers und die Portnummern richtig? – Klicken Sie auf **Konfiguration prüfen**, um zu prüfen, ob der Domänencontroller aktiv ist. – Ist der Name des lokalen Registers richtig angegeben? – Ist der Name des Kerberos-Registers richtig angegeben? – Überprüfen Sie, ob **EIM-Operationen für dieses System aktivieren** ausgewählt ist. • Seite **Systembenutzer**: – Reicht die EIM-Zugriffssteuerung des angegebenen Benutzers aus, um Abgleichsuchen auszuführen, und verfügt er über ein gültiges Kennwort? Informationen über die unterschiedlichen Benutzerberechtigungen finden Sie in der Onlinehilfefunktion. **Anmerkung:** Wenn Sie das Kennwort für den angegebenen Systembenutzer im Directory-Server geändert haben, müssen Sie das Kennwort auch an dieser Stelle ändern. Wenn die beiden Kennwörter nicht übereinstimmen, kann der Systembenutzer keine EIM-Funktionen für das Betriebssystem ausführen und Abgleichsuchoperationen schlagen fehl. – Klicken Sie auf **Verbindung prüfen**, um die Richtigkeit der Benutzerinformationen zu bestätigen.
Die Konfigurationsdaten scheinen richtig zu sein, aber es kann keine Verbindung zum Domänencontroller hergestellt werden.	• Vergewissern Sie sich, dass der als EIM-Domänencontroller fungierende Directory-Server aktiv ist. Handelt es sich bei dem Domänencontroller um einen iSeries-Server, können Sie den iSeries Navigator verwenden und folgende Schritte durchführen: 1. Erweitern Sie **Netzwerk > Server > TCP/IP**. 2. Überprüfen Sie, ob sich der Directory-Server im Status **Gestartet** befindet. Wenn der Server gestoppt ist, klicken Sie mit der rechten Maustaste auf **Directory-Server**, und wählen Sie **Starten...** aus.

Nachdem Sie die Verbindungsinformationen überprüft und sich vergewissert haben, dass der Directory-Server aktiv ist, führen Sie die folgenden Schritte durch, um eine Verbindung zum Domänencontroller herzustellen:

1. Erweitern Sie **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**.

2. Klicken Sie mit der rechten Maustaste auf die EIM-Domäne, zu der Sie eine Verbindung herstellen möchten, und wählen Sie **Verbindung herstellen...** aus.
3. Geben Sie den Benutzerstatus und die erforderlichen Benutzerinformationen an, die für die Verbindung zum EIM-Domänencontroller verwendet werden sollen.
4. Klicken Sie auf **OK**.

Fehlerbehebung bei allgemeinen Problemen mit der EIM-Konfiguration und Domänen

Sowohl bei der Konfiguration von EIM für Ihr System als auch beim Zugriff auf eine EIM-Domäne können Sie auf zahlreiche Probleme stoßen. Informieren Sie sich anhand der folgenden Tabelle über häufig auftretende Probleme und entsprechende Lösungsvorschläge.

Tabelle 28. EIM-Konfiguration und EIM-Domänen - Probleme und Lösungen

Problem	Lösungen
EIM-Konfigurationsassistent hat sich während der **Endverarbeitung** ″aufgehängt″.	Möglicherweise wartet der Assistent darauf, dass der Domänencontroller gestartet wird. Vergewissern Sie sich, dass beim Systemstart des Directory-Servers keine Fehler aufgetreten sind. Überprüfen Sie bei iSeries-Servern das Jobprotokoll für `QDIRSRV` im Subsystem `QSYSWRK`. Führen Sie dazu die folgenden Schritte durch: 1. Erweitern Sie im iSeries Navigator **Work Management > Subsysteme > Qsyswrk**. 2. Klicken Sie mit der rechten Maustaste auf **Qdirsrv**, und wählen Sie **Jobprotokoll** aus.
Als Sie mit Hilfe des EIM-Konfigurationsassistenten auf einem fernen System eine Domäne erstellt haben, erhielten Sie die folgende Fehlernachricht: ″Der eingegebene übergeordnete registrierte Name (DN) ist ungültig. Der registrierte Name muss auf dem fernen Directory-Server vorhanden sein. Einen neuen oder vorhandenen übergeordneten registrierten Namen angeben oder auswählen.″	Der für die ferne Domäne angegebene übergeordnete registrierte Name ist nicht vorhanden. „Neue ferne Domäne erstellen und System hinzufügen” auf Seite 82 enthält weitere Informationen über die Verwendungsweise des EIM-Konfigurationsassistenten. Außerdem enthält die Onlinehilfefunktion detaillierte Informationen darüber, wie ein übergeordneter registrierter Name beim Erstellen einer Domäne angegeben wird.
Sie erhalten eine Nachricht darüber, dass die EIM-Domäne nicht vorhanden ist.	Wenn Sie keine EIM-Domäne erstellt haben, verwenden Sie den EIM-Konfigurationsassistenten. Dieser erstellt Ihnen eine EIM-Domäne oder ermöglicht Ihnen die Konfiguration einer bereits vorhandenen EIM-Domäne. Wenn Sie eine EIM-Domäne erstellt haben, vergewissern Sie sich, dass der angegebene Benutzer zu einer Zugriffssteuerungsgruppe (siehe „EIM-Zugriffssteuerung” auf Seite 42) mit ausreichender Zugriffsberechtigung für die Domäne gehört.
Sie erhalten eine Nachricht darüber, dass ein EIM-Objekt (Kennung, Register, Zuordnung, Richtlinienzuordnung oder Zertifikatfilter) nicht gefunden wurde, oder dass Sie keine Berechtigung für EIM-Daten haben.	Überprüfen Sie, ob das EIM-Objekt vorhanden ist und der angegebene Benutzer zu einer Zugriffssteuerungsgruppe (siehe „EIM-Zugriffssteuerung” auf Seite 42) mit ausreichender Zugriffsberechtigung für dieses Objekt gehört.

Tabelle 28. EIM-Konfiguration und EIM-Domänen - Probleme und Lösungen (Forts.)

Problem	Lösungen
Beim Erweitern des Ordners **Kennungen** dauert es eine ganze Weile, bis die Liste der Kennungen angezeigt wird.	Dies kann vorkommen, wenn die Domäne zahlreiche EIM-Kennungen enthält. Sie können dieses Problem dadurch beheben, dass Sie die Sicht des Ordners **Kennungen** anpassen, indem Sie die Suchkriterien für die Anzeige der Kennungen einschränken. Führen Sie dazu die folgenden Schritte durch: 1. Erweitern Sie im iSeries Navigator **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**. 2. Erweitern Sie die Domäne, deren EIM-Kennungen angezeigt werden sollen. 3. Klicken Sie mit der rechten Maustaste auf **Kennungen**, und wählen Sie **Diese Ansicht anpassen > Anzeigeoptionen...** aus. 4. Geben Sie die Anzeigekriterien zum Erstellen der Liste der EIM-Kennungen für diese Sicht an. **Anmerkung:** Der Stern (*) kann dabei als Platzhalterzeichen verwendet werden. 5. Klicken Sie auf **OK**. Wenn Sie das nächste Mal auf **Kennungen** klicken, werden nur die EIM-Kennungen angezeigt, die mit den angegebenen Kriterien übereinstimmen.
Bei der Verwaltung von EIM mit dem iSeries Navigator erhalten Sie die Fehlernachricht, dass das EIM-Handle nicht mehr gültig ist.	Die Verbindung zum Domänencontroller ist unterbrochen. Führen Sie die folgenden Schritte durch, um die Verbindung zum Domänencontroller wiederherzustellen: 1. Erweitern Sie im iSeries Navigator **Netzwerk > Enterprise Identity Mapping > Domänenverwaltung**. 2. Klicken Sie mit der rechten Maustaste auf die Domäne, mit der Sie arbeiten möchten, und wählen Sie **Verbindung wiederherstellen** aus. 3. Geben Sie die Verbindungsinformationen an. 4. Klicken Sie auf **OK**.
Bei Verwendung des Kerberos-Protokolls für die Authentifizierung in EIM wird Diagnosenachricht `CPD3E3F` ins Jobprotokoll geschrieben.	Diese Nachricht wird immer generiert, wenn Operationen zur Authentifizierung oder zum Identitätsabgleich fehlschlagen. Die Diagnosenachricht enthält sowohl über- als auch untergeordnete Statuscodes, die angeben, wo das Problem aufgetreten ist. Die häufigsten Fehler und deren Behebung werden in der Nachricht dokumentiert. Informationen zur Fehlerbehebung finden Sie im Hilfetext für die Diagnosenachricht. Weitere Informationen finden Sie außerdem unter Fehlerbehebung bei Einzelanmeldungskonfigurationen.

Fehlerbehebung beim EIM-Abgleich

Zahlreiche häufig auftretende Probleme können dazu führen, dass EIM-Abgleiche vollständig fehlschlagen oder einen unerwarteten Verlauf nehmen. In der folgenden Tabelle finden Sie Informationen darüber, welche Probleme zu einem Fehlschlagen eines EIM-Abgleichs führen können, sowie darüber, wie das

jeweilige Problem gelöst werden könnte. Wenn EIM-Abgleiche fehlschlagen, müssen Sie möglicherweise alle genannten Lösungsvorschläge durchgehen, um sicherzustellen, dass Sie das oder die ursächlichen Probleme auch tatsächlich finden und lösen.

Tabelle 29. Allgemeine EIM-Abgleichsfehler und zugehörige Lösungen

Problem	Lösungen
Verbindungsinformationen für den Domänencontroller sind möglicherweise falsch oder Domänencontroller ist nicht aktiv.	Siehe Fehlerbehebung bei Problemen mit dem Domänencontroller; dort wird erläutert, wie Verbindungsinformationen des Domänencontrollers geprüft werden und wie geprüft wird, ob der Domänencontroller aktiv ist.
EIM-Abgleichsuchoperationen für das System schlagen fehl. Dies kann durch eine falsche EIM-Konfiguration auf dem System oder den Systemen verursacht werden.	Überprüfen Sie Ihre EIM-Konfiguration. Erweitern Sie **Netzwerk-->Enterprise Identity Mapping-->Konfiguration** auf dem System, an dem Sie sich authentifizieren möchten. Klicken Sie mit der rechten Maustaste auf den Ordner **Konfiguration**, wählen Sie **Eigenschaften** aus, und überprüfen Sie Folgendes: • Seite **Domäne**: – Sind der Name des Domänencontrollers und die Portnummern richtig? – Klicken Sie auf **Konfiguration prüfen**, um zu prüfen, ob der Domänencontroller aktiv ist. – Ist der Name des lokalen Registers richtig angegeben? – Ist der Name des Kerberos-Registers richtig angegeben? – Überprüfen Sie, ob **EIM-Operationen für dieses System aktivieren** ausgewählt ist. • Seite **Systembenutzer**: – Reicht die EIM-Zugriffssteuerung des angegebenen Benutzers aus, um Abgleichsuchen auszuführen, und verfügt er über ein gültiges Kennwort? Informationen über die unterschiedlichen Benutzerberechtigungen finden Sie in der Onlinehilfefunktion. **Anmerkung:** Wenn Sie das Kennwort für den angegebenen Systembenutzer im Directory-Server geändert haben, müssen Sie das Kennwort auch an dieser Stelle ändern. Wenn die beiden Kennwörter nicht übereinstimmen, kann der Systembenutzer keine EIM-Funktionen für das Betriebssystem ausführen und Abgleichsuchoperationen schlagen fehl. – Klicken Sie auf **Verbindung prüfen**, um die Richtigkeit der Benutzerinformationen zu bestätigen.

Tabelle 29. Allgemeine EIM-Abgleichsfehler und zugehörige Lösungen (Forts.)

Problem	Lösungen
Eine Abgleichsuchoperation gibt mehrere Zielbenutzeridentitäten zurück. Dies kann vorkommen, wenn eine oder mehrere der folgenden Situationen zutreffen: • Eine EIM-Kennung verfügt über mehrere individuelle Zielzuordnungen zu ein und demselben Zielregister. • Für mehrere EIM-Kennungen wurde in einer Quellenzuordnung ein und dieselbe Benutzeridentität angegeben, und jede dieser EIM-Kennungen verfügt über eine Zielzuordnung zu ein und demselben Zielregister, obwohl die für jede Zielzuordnung angegebene Benutzeridentität unterschiedlich sein kann. • In mehreren Standardrichtlinienzuordnungen für Domänen wurde dasselbe Zielregister angeben. • In mehreren Standardrichtlinienzuordnungen für Register wurde dasselbe Quellenregister und dasselbe Zielregister angeben. • In mehreren Richtlinienzuordnungen für Zertifikatfilter wurde dasselbe X.509-Quellenregister, derselbe Zertifikatfilter und dasselbe Zielregister angegeben.	Überprüfen Sie mit Hilfe der Funktion EIM-Abgleich testen, ob die Zuordnung einer bestimmten Quellenbenutzeridentität zur entsprechenden Zielbenutzeridentität korrekt ausgeführt wird. Die Vorgehensweise bei der Fehlerbehebung hängt von den Testergebnissen ab: • Der Test gibt wegen einem der folgenden Gründe mehrere unerwünschte Zielidentitäten zurück: – Dies kann darauf hinweisen, dass die Zuordnungskonfiguration für die Domäne aus einem der folgenden Gründe fehlerhaft ist: - Eine Ziel- oder Quellenzuordnung für eine EIM-Kennung ist nicht richtig konfiguriert. Beispiel: Es ist keine oder eine falsche Quellenzuordnung für den Kerberos-Principal (oder Windows-Benutzer) vorhanden, oder die Zielzuordnung enthält eine falsche Benutzeridentität. Zeigen Sie alle Kennungszuordnungen für eine EIM-Kennung an, um die Zuordnungen für eine bestimmte Identifikation überprüfen zu können. - Eine Richtlinienzuordnung ist falsch konfiguriert. Zeigen Sie alle Richtlinienzuordnungen für Domänen an, um die Quellen- und Zielinformationen für alle in der Domäne definierten Richtlinienzuordnungen überprüfen zu können. – Dies kann darauf hinweisen, dass Gruppenregisterdefinitionen, die mehrere allgemeine Mitglieder enthalten, als Quellen- oder Zielregister für EIM-Kennungszuordnungen oder entsprechende Richtlinienzuordnungen definiert sind. Verwenden Sie die detaillierten Informationen, die durch die Testabgleichsuchoperation generiert wurden, um festzustellen, ob es sich bei den Quellen- oder Zielregistern um Gruppenregisterdefinitionen handelt. Ist dies der Fall, müssen Sie die Eigenschaften der Gruppenregisterdefinition überprüfen, um festzustellen, ob die Gruppenregisterdefinitionen allgemeine Mitglieder enthalten. – Der Test gibt mehrere Zielbenutzeridentitäten zurück, und diese Ergebnisse entsprechen auch der Art und Weise, wie Sie Zuordnungen konfiguriert haben. In diesem Fall müssen Sie für jede Zielbenutzeridentität Suchinformationen angeben, um sicherzustellen, dass eine Suchoperation eine einzelne Zielbenutzeridentität und nicht alle möglichen Zielbenutzeridentitäten zurückgibt. Siehe Suchinformationen zu Zielbenutzeridentität hinzufügen.

Tabelle 29. Allgemeine EIM-Abgleichsfehler und zugehörige Lösungen (Forts.)

Problem	Lösungen
(Fortsetzung)	**Anmerkung:** Diese Vorgehensweise funktioniert nur, wenn die Anwendung für die Verwendung der Suchinformationen auch aktiviert ist. Die i5/OS-Basisanwendungen wie z. B. iSeries Access für Windows sind nicht in der Lage, anhand von Suchinformationen mehrere von einer Suchoperation zurückgegebene Zielbenutzeridentitäten zu unterscheiden. Daher sollten Sie überprüfen, ob es sinnvoll ist, die für die Domäne vorhandenen Zuordnungen erneut zu definieren. Auf diese Weise kann sichergestellt werden, dass eine Abgleichsuchoperation eine einzige Zielbenutzeridentität zurückgeben kann. So kann gewährleistet werden, dass die i5/OS-Basisanwendungen Suchoperationen ausführen und Identitäten abgleichen können.
EIM-Suchoperationen geben keine Ergebnisse zurück, aber es sind Zuordnungen für die Domäne konfiguriert.	Überprüfen Sie mit Hilfe der Funktion EIM-Abgleich testen, ob die Zuordnung einer bestimmten Quellenbenutzeridentität zur entsprechenden Zielbenutzeridentität korrekt ausgeführt wird. Prüfen Sie, ob Sie die richtigen Informationen für den Test angegeben haben. Ist dies der Fall, könnte das Problem eine der folgenden Ursachen haben: • Die Zuordnungskonfiguration ist falsch. Prüfen Sie Ihre Zuordnungskonfiguration mit Hilfe der Informationen zur Fehlerbehebung im vorherigen Eintrag. • Die Unterstützung von Richtlinienzuordnungen ist nicht auf Domänenebene aktiviert. Sie müssten dann Richtlinienzuordnungen für eine Domäne aktivieren. • Die Unterstützung von Abgleichsuchfunktionen oder Richtlinienzuordnungen ist nicht auf der individuellen Registerebene aktiviert. Sie müssten dann die Unterstützung von Abgleichsuchfunktionen und die Verwendung von Richtlinienzuordnungen für das Zielregister aktivieren. • Registerdefinition und Benutzeridentitäten stimmen auf Grund unterschiedlicher Groß-/Kleinschreibung nicht überein. Sie können das Register löschen und erneut erstellen oder die Zuordnung löschen und mit der richtigen Schreibweise unter Beachtung der Groß-/Kleinschreibung erneut erstellen.

APIs für Enterprise Identity Mapping

Im Folgenden werden die EIM-APIs und deren Benutzung in Anwendungen und im Netzwerk beschrieben.

Enterprise Identity Mapping (EIM) ermöglicht eine plattformübergreifende Verwaltung der Benutzeridentitäten. EIM verfügt über zahlreiche Anwendungsprogrammierschnittstellen (APIs), mit denen Anwendungen EIM-Operationen für eine Anwendung oder einen Anwendungsbenutzer ausführen können. Sie können diese APIs zur Durchführung von Identitätsabgleichsuchoperationen, diversen EIM-Verwaltungs- und Konfigurationsfunktionen sowie für Informationsänderungen und Abfragefunktionen verwenden. Diese APIs werden von allen IBM Plattformen unterstützt.

EIM-APIs lassen sich in die folgenden Kategorien unterteilen:
- EIM-Handhabungs- und Verbindungsoperationen
- EIM-Domänenverwaltung
- Registeroperationen
- EIM-Kennungsoperationen
- EIM-Zuordnungsverwaltung
- EIM-Abgleichsuchoperationen
- EIM-Berechtigungsverwaltung

Anwendungen, die die EIM-Informationen in einer EIM-Domäne mit diesen APIs verwalten oder benutzen, verwenden normalerweise das folgende Programmiermodell:
1. EIM-Kennung abrufen.
2. Verbindung zu einer EIM-Domäne herstellen.
3. Normale Anwendungsverarbeitung.
4. API für EIM-Verwaltung oder API für EIM-Abgleichsuchoperationen verwenden.
5. Normale Anwendungsverarbeitung.
6. Vor Beendigung des Vorgangs Löschung der EIM-Handle.

Zugehörige Informationen

Enterprise Identity Mapping (EIM) APIs

Referenzinformationen für Enterprise Identity Mapping

Im Folgenden finden Sie Angaben zu weiteren Informationsquellen, die Sie bei der Verwendung von EIM benutzen können.

Wenn Sie weitere Informationen über Technologien im Zusammenhang mit Enterprise Identity Mapping wünschen, lesen Sie die folgenden Themen im Information Center:
- **Einzelanmeldung** Dieses Thema enthält Informationen über die Konfiguration und Verwaltung einer Einzelanmeldungsumgebung für Ihr Unternehmen; dort finden Sie auch zahlreiche Szenarien, mit deren Hilfe Sie sich ein Bild davon machen können, welchen Nutzen die Einzelanmeldung Ihrem Unternehmen bringt.
- **Netzwerkauthentifizierungsservice** Dieses Thema enthält Informationen über die Konfiguration und die Handhabung des Netzwerkauthentifizierungsservice, der iSeries-Implementierung des Kerberos-Protokolls. Wenn Sie den Netzwerkauthentifizierungsservice in Verbindung mit EIM konfigurieren, können Sie eine Einzelanmeldungsumgebung für Ihr Unternehmen erstellen.
- **IBM Directory Server for iSeries (LDAP)** Dieses Thema enthält Informationen über die Konfiguration und zum Konzept des IBM Directory Server for iSeries (LDAP). In EIM kann der Directory-Server als Host für den EIM-Domänencontroller und zum Speichern von EIM-Domänendaten verwendet werden.

Bedingungen

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

Persönliche Nutzung: Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM weder weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Kommerzielle Nutzung: Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und

anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Abgesehen von den hier gewährten Berechtigungen erhalten Sie keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum.

IBM behält sich das Recht vor, die in diesem Dokument gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Verordnungen, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Informationen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf ″as-is″-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit oder die Freiheit der Rechte Dritter zur Verfügung gestellt.

Anhang. Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. An Stelle der IBM Produkte, Programme oder Services können auch andere ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Europe
IBM Director of Licensing
92066 Paris La Defense Cedex
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt; die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete, der IBM Lizenzvereinbarung für Maschinencode oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht der IBM dar, unterliegen Änderungen oder können zurückgenommen werden, und repräsentieren nur die Ziele der IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Diese Veröffentlichung dient nur zu Planungszwecken. Die in dieser Veröffentlichung enthaltenen Informationen können geändert werden, bevor die beschriebenen Produkte verfügbar sind.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogrammes illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Musteranwendungsprogramme, die in Quellensprache geschrieben sind. Sie dürfen diese Musterprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, verwenden, vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Musterprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. IBM kann deshalb die Zuverlässigkeit, Wartungsfreundlichkeit und Funktion dieser Programme nicht gewährleisten.

Kopien oder Teile der Musterprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

© (Name Ihrer Firma) (Jahr). Teile des vorliegenden Codes wurden aus Musterprogrammen der IBM Corp. abgeleitet. © Copyright IBM Corp. _Jahr/Jahre angeben_. Alle Rechte vorbehalten.

Marken

Folgende Namen sind in gewissen Ländern Marken der International Business Machines Corporation:

AIXDistributed Relational Database Architecture
Domino
DRDA
eServer
i5/OS
IBM
iSeries
Lotus Notes
NetServer
OS/400

pSeries
RACF

RDN
Tivoli
WebSphere
xSeries
z/OS

zSeries

Lotus, Lotus Notes, Freelance und WordPro sind in gewissen Ländern Marken der International Business Machines Corporation und der Lotus Development Corporation.

Microsoft, Windows, Windows NT und das Windows-Logo sind in gewissen Ländern Marken der Microsoft Corporation.

| Linux ist in gewissen Ländern eine Marke von Linus Torvalds.

UNIX ist in gewissen Ländern eine eingetragene Marke von The Open Group.

Andere Namen von Unternehmen, Produkten oder Services können Marken oder Servicemarken anderer Unternehmen sein.

Bedingungen

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

Persönliche Nutzung: Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM weder weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Kommerzielle Nutzung: Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Abgesehen von den hier gewährten Berechtigungen erhalten Sie keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum.

IBM behält sich das Recht vor, die in diesem Dokument gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Verordnungen, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Informationen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf ″as-is″-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit oder die Freiheit der Rechte Dritter zur Verfügung gestellt.