System i

Sicherheit Einzelanmeldung

Version 6 Release 1

System i

Sicherheit Einzelanmeldung

Version 6 Release 1

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen", auf Seite 97 gelesen werden.

Diese Ausgabe bezieht sich auf Version 6, Release 1, Modifikation 0 von IBM i5/OS (Produktnummer 5761-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 System i Security Single sign-on, Version 6 Release 1,
herausgegeben von International Business Machines Corporation, USA

Herausgegeben von:
SW TSC Germany
Kst. 2877
Februar 2008

Inhaltsverzeichnis

Einzelanmeldung 1
Neuerungen in V6R1 1
PDF-Datei für die Einzelanmeldung 2
Einzelanmeldungskonzepte 2
Übersicht zur Einzelanmeldung 2
Authentifizierung 4
Berechtigung 5
Domänen 6
Identitätsabgleich 7
i5/OS-Unterstützung 9
ISV-Unterstützung 10
Szenarios: Einzelanmeldung 11
Szenario: Einzelanmeldungstestumgebung erstellen 12
Planungsarbeitsblätter ausfüllen 15
Basiskonfiguration für die Einzelanmeldung für System A erstellen 19
Service-Principal von System A zum Kerberos-Server hinzufügen 21
Ausgangsverzeichnis für John Day auf System A erstellen 22
Konfiguration des Netzwerkauthentifizierungsservice auf System A testen 22
EIM-Kennung für John Day erstellen 23
EIM-Identitätsabgleiche testen 23
System i Access für Windows-Anwendungen für die Verwendung der Kerberos-Authentifizierung konfigurieren 24
Konfiguration des Netzwerkauthentifizierungsservice und von EIM überprüfen . . . 25
(Optional) Hinweise für die Konfigurationsnachbereitung 25
Szenario: Einzelanmeldung für i5/OS aktivieren 26
Planungsarbeitsblätter ausfüllen 31
Basiskonfiguration für die Einzelanmeldung für System A erstellen 37
System B zur Nutzung der EIM-Domäne und für den Netzwerkauthentifizierungsservice konfigurieren 40
Beide i5/OS-Service-Principals zum Kerberos-Server hinzufügen 41
Benutzerprofile auf System A und System B erstellen 43
Ausgangsverzeichnisse auf System A und System B erstellen 43
Netzwerkauthentifizierungsservice auf System A und System B testen 43
EIM-Kennungen für die beiden Administratoren John Day und Sharon Jones erstellen . . 44
Kennungszuordnungen für John Day erstellen 45
Kennungszuordnungen für Sharon Jones erstellen 46
Standardrichtlinienzuordnungen für Register erstellen 47
Register für die Nutzung von Suchoperationen und Richtlinienzuordnungen aktivieren . . . 48
EIM-Identitätsabgleiche testen 49
System i Access für Windows-Anwendungen für die Verwendung der Kerberos-Authentifizierung konfigurieren 52
Konfiguration des Netzwerkauthentifizierungsservice und von EIM überprüfen . . . 53
(Optional) Hinweise für die Konfigurationsnachbereitung 53
Szenario: Netzwerkauthentifizierungsservice und EIM an mehrere Systeme weitergeben 54
Planungsarbeitsblätter ausfüllen 58
Systemverwaltungsgruppe erstellen 60
Systemeinstellungen vom Modellsystem (System A) an System B und System C weitergeben 61
Konfiguration für den Netzwerkauthentifizierungsservice und EIM auf System B und System C ausführen. 62
Netzwerkauthentifizierungsservice und EIM auf System D (ab V5R2) konfigurieren . . . 62
Szenario: Management Central-Server für Einzelanmeldung konfigurieren. 63
Anzeige der Domäne in der Domänenverwaltung überprüfen 67
EIM-Kennungen erstellen. 68
Kennungszuordnungen erstellen 68
Management Central-Server zur Nutzung des Netzwerkauthentifizierungsservice konfigurieren 69
Management Central-Server zur Nutzung von EIM konfigurieren 69
Szenario: Einzelanmeldung für ISV-Anwendungen aktivieren 71
Planungsarbeitsblatt für Systemvoraussetzungen ausfüllen 72
Neue Anwendung schreiben oder vorhandene Anwendung ändern 73
Einzelanmeldungstestumgebung erstellen . . 73
Anwendung testen 74
Beispiel: ISV-Code 74
Einzelanmeldung planen 83
Voraussetzungen zur Konfiguration einer Einzelanmeldungsumgebung 83
Planungsarbeitsblätter für die Einzelanmeldung 84
Einzelanmeldung konfigurieren. 87
Einzelanmeldung verwalten 89
Fehler bei der Einzelanmeldung beheben 90
Referenzinformationen für die Einzelanmeldung . . 94

Anhang. Bemerkungen 97
Informationen zu Programmierschnittstellen . . . 98
Marken. 98
Bedingungen 99

Einzelanmeldung

Wenn Sie eine Möglichkeit suchen, um die Anzahl der Kennwörter zu reduzieren, die von Ihren Benutzern verwendet und von Ihren Administratoren verwaltet werden müssen, dann sollten Sie die Implementierung einer Einzelanmeldungsumgebung in Erwägung ziehen.

Im Folgenden wird eine Einzelanmeldungslösung für i5/OS vorgestellt, die mit dem Netzwerkauthentifizierungsservice (IBM Implementierung des Kerberos V5-Standards des MIT) sowie mit Enterprise Identity Mapping (EIM) arbeitet. Durch eine Einzelanmeldungslösung kann die Anzahl der Anmeldevorgänge und Kennwörter reduziert werden, die ein Benutzer für den Zugriff auf mehrere Anwendungen und Server durchführen muss bzw. benötigt.

Anmerkung: Beachten Sie bitte die wichtigen rechtlichen Informationen, die in „Haftungsausschluss für Programmcode" auf Seite 94 aufgeführt sind.

Neuerungen in V6R1

Lesen Sie die neuen oder erheblich geänderten Informationen in der Themensammlung zur Einzelanmeldung.

Neue oder erweiterte Funktionen für die Einzelanmeldung

- In den Vorgängerreleases von i5/OS unterstützte die Einzelanmeldung die Zuordnung zu einer lokalen Benutzeridentität in EIM (Enterprise Identity Mapping) pro System. In i5/OS V6R1 unterstützt die Einzelanmeldung die Auswahl aus mehreren lokalen Benutzeridentitätszuordnungen für dasselbe System. Hierbei wird die IP-Adresse des Zielsystems verwendet, um die korrekte lokale Benutzeridentitätszuordnung auf diesem System auszuwählen.
- Erweiterungen bei EIM und beim Netzwerkauthentifizierungsservice

  Viele der neuen oder erweiterten Funktionen der Einzelanmeldung resultieren aus neuen oder erweiterten Funktionen, die für EIM oder den Netzwerkauthentifizierungsservice implementiert wurden. Hierbei handelt es sich um die beiden Technologien, auf denen die i5/OS-Einzelanmeldungslösung basiert. Weitere Informationen zu den einzelnen Erweiterungen finden Sie in den folgenden Themen:
  - Neuerungen in V6R1 (Informationen für EIM)
  - Neuerungen in V6R1 (Informationen für Netzwerkauthentifizierungsservice)

Neue oder ergänzte Informationen zu diesem Thema

In den vorherigen Ausgaben dieser Veröffentlichung wurden die Informationen zur Einzelanmeldungsfunktion in den Themen zum Netzwerkauthentifizierungsservice und zu EIM bereitgestellt, weil die Einzelanmeldungsumgebung auf diesen beiden Technologien basiert. Dieses neue Thema enthält nun gebündelte Informationen zur Konfiguration und Verwendung der Einzelanmeldung. Es enthält darüber hinaus erweiterte und ergänzte Informationen sowie wichtige Konzepte, detaillierte Informationen zur Planung sowie verschiedene Szenarios, in denen Sie darüber informiert werden, wann und wie die Funktionen der Einzelanwendung genutzt werden können.

Neuerungen und Änderungen anzeigen

Um technische Änderungen zu markieren, werden im Information Center die folgenden Symbole verwendet:

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

In PDF-Dateien werden am linken Rand möglicherweise Änderungsmarkierungen (|) angezeigt, mit denen neue oder geänderte Informationen gekennzeichnet sind.

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

PDF-Datei für die Einzelanmeldung

Die vorliegenden Informationen können als PDF-Datei angezeigt und gedruckt werden.

Zum Anzeigen oder Herunterladen der PDF-Version dieses Dokuments wählen Sie Einzelanmeldung (ca. 600 KB) aus.

Sie können die folgenden zugehörigen Themen anzeigen oder herunterladen:

- Enterprise Identity Mapping (EIM) (ca. 700 KB). Bei EIM (Enterprise Identity Mapping) handelt es sich um einen Mechanismus für den Abgleich einer Person oder Entität (z. B. eines Service) mit den entsprechenden Benutzeridentitäten in den verschiedenen Benutzerregistern des Unternehmens.
- Netzwerkauthentifizierungsservice (ca. 990 KB). Der Netzwerkauthentifizierungsservice ermöglicht einem System die Nutzung eines vorhandenen Kerberos-Netzwerks.

PDF-Dateien speichern

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

1. Klicken Sie mit der rechten Maustaste auf den PDF-Link in Ihrem Browser.
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.

Einzelanmeldungskonzepte

Bei der Einzelanmeldung werden mehrere Services und Verfahren eingesetzt, um eine Lösung zu implementieren, die sich durch eine vereinfachte Identitäts- und Berechtigungsverwaltung auszeichnet.

In den folgenden Themen werden die Vorteile der Einzelanmeldung erläutert und es wird beschrieben, wie die verschiedenen Services zum Aufbau dieser Lösung eingesetzt werden. Bevor Sie die Einzelanmeldung verwenden, sollten Sie sich mit diesen Konzepten vertraut machen:

Übersicht zur Einzelanmeldung

Eine Einzelanmeldungslösung vereinfacht die Benutzung der Systeme innerhalb Ihres Unternehmens, wenn dort mehrere Benutzernamen und Kennwörter definiert sind. Die Implementierung einer Einzelanmeldungslösung bietet Vorteile für Benutzer, Administratoren und Anwendungsentwickler.

In traditionellen Netzwerkumgebungen führt ein Benutzer die Authentifizierung gegenüber einem System oder einer Anwendung durch, indem er die in oder von diesem System bzw. dieser Anwendung definierten Benutzerberechtigungen angibt. Normalerweise wurde sowohl für die Authentifizierung als auch für die Berechtigung dasselbe Benutzerregister verwendet, wenn ein Benutzer versuchte, auf eine Ressource zuzugreifen, die von dem betreffenden System bzw. der betreffenden Anwendung verwaltet wurde. In

einer Einzelanmeldungsumgebung muss für die Authentifizierung und die Berechtigung nicht unbedingt dasselbe Benutzerregister verwendet werden, um einem Benutzer den Zugriff auf eine Ressource zu erteilen, die von dem System bzw. der Anwendung verwaltet wird. In Einzelanmeldungsumgebungen wird zur Authentifizierung der Netzwerkauthentifizierungsservice (Kerberos-Authentifizierung) eingesetzt. Dort muss das für die Authentifizierung verwendete Benutzerregister nicht unbedingt mit dem Register übereinstimmen, das vom System oder der Anwendung definiert wurde. In einer traditionellen Netzwerkumgebung ergibt sich hierdurch ein Problem bei der Berechtigung.

In einer Netzwerkumgebung mit Einzelanmeldung verwenden Anwendungen Enterprise Identity Mapping (EIM), um dieses Problem zu beheben. Bei EIM handelt es sich um einen Mechanismus für den Abgleich bzw. die Zuordnung einer Person oder Entität mit bzw. zu den entsprechenden Benutzeridentitäten in den verschiedenen Registern des Unternehmens. Anwendungsentwickler für i5/OS verwenden EIM zur Erstellung von Anwendungen, die ein Benutzerregister zur Authentifizierung und ein anderes für die Berechtigung verwenden, wobei der Benutzer nicht zweimal seine Berechtigungsnachweise eingeben muss. Der Einsatz einer Einzelanmeldungsumgebung hat zahlreiche Vorteile. Diese betreffen nicht ausschließlich die Benutzer. Auch Administratoren und Anwendungsentwickler profitieren von einer solchen Einzelanmeldungslösung.

Vorteile für den Benutzer

Durch eine Einzelanmeldungslösung kann die Anzahl der Anmeldevorgänge reduziert werden, die ein Benutzer für den Zugriff auf mehrere Anwendungen und Server ausführen muss. Wird die Einzelanmeldung verwendet, muss die Authentifizierung nur einmal durchgeführt werden, wenn sich der Benutzer beim Netzwerk anmeldet. Durch die Verwendung von EIM kann der Benutzer mit weniger Benutzernamen und Kennwörtern arbeiten, um auf andere Systeme innerhalb des Netzwerks zuzugreifen. Nachdem sich der Benutzer einmal im Netzwerk authentifiziert hat, kann er unternehmensweit auf Services und Anwendungen zugreifen, ohne dass hierzu auf den verschiedenen Systemen mehrere Kennwörter benötigt werden.

Vorteile für den Administrator

Für den Administrator bietet die Einzelanmeldung den Vorteil, dass die Sicherheitsverwaltungsaufgaben eines Unternehmens erheblich vereinfacht werden können. Ohne die Einzelanmeldung werden die Kennwörter des Benutzers möglicherweise auf unterschiedlichen Systemen zwischengespeichert, wodurch sich Sicherheitslücken für das gesamte Netzwerk ergeben können. Administratoren verwenden viel Zeit und beträchtliche Mittel auf die Entwicklung von Lösungen, die dieses Sicherheitsrisiko reduzieren. Durch die Einzelanmeldung kann der Verwaltungsaufwand für die Authentifizierung reduziert und gleichzeitig die Sicherheit des gesamten Netzwerks gewährleistet werden. Darüber hinaus können durch die Einzelanmeldung die Verwaltungskosten gesenkt werden, die durch das Zurücksetzen vergessener Kennwörter entstehen. Administratoren können eine Einzelanmeldungsumgebung einrichten, in der der Benutzer über eine einmalige Anmeldung bei einem Microsoft Windows-Betriebssystem Zugriff auf das gesamte Netzwerk erhält. Auf diese Weise kann der Aufwand für die Authentifizierung und die Verwaltung der Identifikationsdaten auf ein Minimum reduziert werden.

Vorteile für den Anwendungsentwickler

Für Entwickler, die Anwendungen für den Einsatz in heterogenen Netzwerken entwickeln, besteht eines der zentralen Probleme darin, Anwendungen für mehrere Ebenen zu erstellen, wobei die einzelnen Ebenen auf unterschiedlichen Plattformen implementiert sein können. Durch den Einsatz von EIM können Anwendungsentwickler Anwendungen schreiben, die für die Authentifizierung das am besten geeignete Benutzerregister verwenden, während für die Berechtigung ein anderes Benutzerregister verwendet werden kann. Da es nicht erforderlich ist, anwendungsspezifische Benutzerregister, die zugehörige Sicherheitssemantik und spezielle Sicherheitseinrichtungen auf Anwendungsebene zu implementieren, können die Kosten für die Implementierung von plattformübergreifenden Anwendungen mit mehreren Ebenen erheblich gesenkt werden.

Zugehörige Konzepte

„Authentifizierung"
Die Authentifizierung ist Bestandteil einer Einzelanmeldungslösung. Sie dient dazu, einen Benutzer zu identifizieren und diese Identität dann anhand bestimmter Daten (normalerweise anhand eines Benutzernamens und des zugehörigen Kennworts) zu überprüfen.

„Berechtigung" auf Seite 5
Als Berechtigung wird der Prozess bezeichnet, bei dem einem Benutzer der Zugriff auf eine Netzwerk- oder Systemressource gewährt wird.

Zugehörige Informationen

Enterprise Identity Mapping

Authentifizierung

Die Authentifizierung ist Bestandteil einer Einzelanmeldungslösung. Sie dient dazu, einen Benutzer zu identifizieren und diese Identität dann anhand bestimmter Daten (normalerweise anhand eines Benutzernamens und des zugehörigen Kennworts) zu überprüfen.

Der Authentifizierungsprozess unterscheidet sich vom Prozess der Berechtigungserteilung, bei dem einer Entität oder Person der Zugriff auf eine Netzwerk- oder Systemressource gewährt oder verweigert wird.

In einer Einzelanmeldungsumgebung wird der Prozess und die Verwaltung der Authentifizierung für Benutzer und Administratoren optimiert. Auf Grund der Implementierungsweise der Einzelanmeldung auf Ihrem System müssen die Benutzer nicht nur weniger oft Ihre Benutzer-IDs und Kennwörter eingeben, sondern benötigen (wenn Sie das System entsprechend konfigurieren) überhaupt keine i5/OS-Kennwörter. Administratoren müssen weniger häufig ID- und Kennwortprobleme beheben, weil Benutzer sich weniger IDs und Kennwörter merken müssen, um auf die verwendeten Systeme zuzugreifen.

Schnittstellen, die die Einzelanmeldung unterstützen, müssen zur Authentifizierung Kerberos verwenden. Der Netzwerkauthentifizierungsservice stellt die i5/OS-Implementierung der Kerberos-Authentifizierungsfunktion dar. Er bietet einen verteilten Authentifizierungsmechanismus und verwendet hierzu einen Kerberos-Server, der auch als Key Distribution Center (KDC) bezeichnet wird. Mit Hilfe des KDC werden Service-Tickets erstellt, die zur Authentifizierung des Benutzers (in Kerberos als **Principal** bezeichnet) gegenüber einem Netzwerkservice verwendet werden. Das Ticket dient zur Belegung der Identität des Principals gegenüber anderen Services, die vom Principal innerhalb des Netzwerks angefordert werden.

Anmerkung: Wenn Sie als Anwendungsentwickler arbeiten, können Sie weitere Authentifizierungsmethoden verwenden, wenn Sie Ihre Anwendungen für den Einsatz in einer Einzelanmeldungsumgebung einrichten. Sie können z. B. Anwendungen erstellen, die mit einer Authentifizierungsmethode (z. B. mit digitalen Zertifikaten) und mit EIM-APIs arbeiten, um Ihrer Anwendung die Nutzung einer Einzelanmeldungsumgebung zu ermöglichen.

Zugehörige Konzepte

„Übersicht zur Einzelanmeldung" auf Seite 2
Eine Einzelanmeldungslösung vereinfacht die Benutzung der Systeme innerhalb Ihres Unternehmens, wenn dort mehrere Benutzernamen und Kennwörter definiert sind. Die Implementierung einer Einzelanmeldungslösung bietet Vorteile für Benutzer, Administratoren und Anwendungsentwickler.

„Berechtigung" auf Seite 5
Als Berechtigung wird der Prozess bezeichnet, bei dem einem Benutzer der Zugriff auf eine Netzwerk- oder Systemressource gewährt wird.

Zugehörige Informationen

Netzwerkauthentifizierungsservice

Berechtigung

Als Berechtigung wird der Prozess bezeichnet, bei dem einem Benutzer der Zugriff auf eine Netzwerk- oder Systemressource gewährt wird.

In den meisten Unternehmen wird ein zweistufiger Prozess eingesetzt, mit dem Benutzern der Zugriff auf die Netzwerkressourcen gewährt wird. Die erste Phase dieses Prozesses wird als Authentifizierung bezeichnet. Bei der Authentifizierung handelt es sich um einen Prozess, bei dem der Benutzer sich gegenüber dem Unternehmen identifiziert. Normalerweise muss der Benutzer hierzu bei der Sicherheitskomponente des Unternehmens eine ID und ein Kennwort eingeben. Anschließend überprüft die Sicherheitskomponente dann die empfangenen Daten. Nach dem erfolgreichen Abschluss der Authentifizierung erhält der Benutzer Anweisungen zur Ausführung eines bestimmten Prozesses, einen Berechtigungsnachweis oder ein Ticket, mit dessen Hilfe er nachweisen kann, dass er sich bei dem betreffenden Unternehmen bereits erfolgreich authentifiziert hat. Als Beispiel einer Benutzerauthentifizierung kann die Kombination aus ID und Kennwortprüffrage aufgeführt werden, die für die Herstellung einer System i Navigator-Verbindung eingegeben werden muss. Nach erfolgreicher Authentifizierung wird dem Benutzer ein Job zugeordnet, der unter seiner Benutzer-ID ausgeführt wird. In der zweiten Phase erhält der Benutzer die Berechtigung. Es ist wichtig, den Unterschied zwischen der Authentifizierung und der Berechtigung zu kennen.

Als Berechtigung wird der Prozess bezeichnet, mit dem festgestellt wird, ob eine Entität oder Person berechtigt ist, auf eine Unternehmensressource zuzugreifen. Die Berechtigungsprüfung wird durchgeführt, nachdem der Benutzer sich beim Unternehmen authentifiziert hat, weil es zur Berechtigung erforderlich ist, dass das Unternehmen feststellen kann, wer versucht, auf seine Ressourcen zuzugreifen. Die Berechtigungsprüfung ist verbindlich und ein fester Bestandteil der Systemabläufe. Die zur Berechtigungsprüfung ausgeführten Verarbeitungsoperationen finden normalerweise im Hintergrund statt und werden vom Benutzer meist nur dann registriert, wenn ihm der Zugriff auf die gewünschten Ressourcen verweigert wird. Als Beispiel für einen Berechtigungsprozess kann der Benutzer den Befehl `CRTSRCPF QGPL/MYFILE` eingeben. Daraufhin führt das System eine Berechtigungsprüfung für den Befehl `CRTSRCPF` und die Bibliothek `QGPL` durch. Wenn der Benutzer nicht über die erforderliche Berechtigung für die Benutzung des Befehls und den Zugriff auf die Bibliothek verfügt, schlägt die Benutzeranforderung fehl.

Ein Unternehmen, das die i5/OS-Einzelanmeldungslösung implementiert hat, verwendet zur Verwaltung des Benutzerzugriffs auf die Unternehmensressourcen Enterprise Identity Mapping (EIM). EIM führt keine Berechtigungsprüfung durch, die Funktion für den Identitätsabgleich richtet jedoch die lokalen IDs für Benutzer ein, die sich beim Unternehmen erfolgreich authentifiziert haben. Die Quelleneinheit (bzw. der Benutzer) erhält über die lokale ID Zugriff auf das Zielsystem sowie die für den Zugriff erforderlichen Berechtigungen. Beispiel: Sie arbeiten in der folgenden, einfachen Unternehmensumgebung:

Mitarbeitername (EIM-Identität)	Quellenbenutzer (EIM-Quelleneinheit)	Zielbenutzer für System A (EIM-Zieleinheit)	Zuständigkeit des Mitarbeiters	Benutzerkommentare - System A
Susan Doe	SusanD	SecOfficer	IT-Sicherheitsbeauftragte	Alle Sonderberechtigungen. Hat Zugriff auf alle Dateien und Informationen.
Fred Ray	FredR	PrimeAcnt	Leitender Buchhalter	Keine Sonderberechtigungen. Hat Zugriff auf alle Lohnbuchhaltungsdaten.
Nancy Me	NancyM	PrimePGM	Teamleiterin IT-Anwendungen	Keine Sonderberechtigungen. Hat Zugriff auf alle Anwendungsquellendateien des Unternehmens.
Brian Fa	BrianF	GenAcnt1	Buchhalter	Keine Sonderberechtigungen. Hat Zugriff auf einen Teil der Lohnbuchhaltungsdaten.

Mitarbeitername (EIM-Identität)	Quellenbenutzer (EIM-Quelleneinheit)	Zielbenutzer für System A (EIM-Zieleinheit)	Zuständigkeit des Mitarbeiters	Benutzerkommentare - System A
Tracy So	TracyS	ITPgm2	IT-Programmiererin	Keine Sonderberechtigungen. Hat Zugriff auf einen Teil der Anwendungsquellendateien des Unternehmens.
Daryl La	DarylL	ITPgm3	IT-Programmiererin	Keine Sonderberechtigungen. Hat Zugriff auf einen Teil der Anwendungsquellendateien des Unternehmens.
Sherry Te	SherryT	PrimeMKT	Vertriebsbeauftragte	Keine Sonderberechtigungen. Hat Zugriff auf alle Marketingdaten.

Es ist wichtig, dass alle Zuordnungen zwischen Benutzern und Ressourcen korrekt definiert sind. Sind die Zuordnungen falsch, dann haben Benutzer Zugriff auf Daten außerhalb Ihres Zuständigkeitsbereichs, was in den meisten Unternehmen aus Gründen der Sicherheit nicht erwünscht ist. Systemadministratoren müssen bei der Erstellung der EIM-Abgleiche mit größter Sorgfalt vorgehen und sicherstellen, dass die Benutzer den richtigen lokalen Register-IDs zugeordnet sind. Wenn Sie z. B. der IT-Programmiererin Daryl La die ID der Sicherheitsbeauftragten Susan Doe zugeordnet haben, könnte sich dadurch für Ihr System ein Sicherheitsrisiko ergeben. Auch dieses Beispiel veranschaulicht nochmals, wie wichtig es ist, dass der Sicherheitsadministrator geeignete Vorkehrungen zur Sicherung der Zielsysteme eines Unternehmens trifft.

Zugehörige Konzepte

„Übersicht zur Einzelanmeldung" auf Seite 2
Eine Einzelanmeldungslösung vereinfacht die Benutzung der Systeme innerhalb Ihres Unternehmens, wenn dort mehrere Benutzernamen und Kennwörter definiert sind. Die Implementierung einer Einzelanmeldungslösung bietet Vorteile für Benutzer, Administratoren und Anwendungsentwickler.

„Authentifizierung" auf Seite 4
Die Authentifizierung ist Bestandteil einer Einzelanmeldungslösung. Sie dient dazu, einen Benutzer zu identifizieren und diese Identität dann anhand bestimmter Daten (normalerweise anhand eines Benutzernamens und des zugehörigen Kennworts) zu überprüfen.

Zugehörige Informationen

Enterprise Identity Mapping

Domänen

Zur Implementierung einer Einzelanmeldungsumgebung werden EIM- und Windows-Domänen verwendet.

Obwohl sowohl die EIM- als auch die Windows-Domäne mit dem Wort "Domäne" bezeichnet werden, weisen sie sehr unterschiedliche Definitionen auf. Im Folgenden werden die Unterschiede beschrieben, die zwischen diesen beiden Domänentypen bestehen.

EIM-Domäne

Bei einer EIM-Domäne handelt es sich um eine Datensammlung, in der die EIM-Kennungen, -Zuordnungen und -Benutzerregisterdefinitionen enthalten sind, die in dieser Domäne definiert sind. Diese Daten werden auf einem LDAP-Server (LDAP = Lightweight Directory Access Protocol) wie z. B. IBM Tivoli Directory Server for i5/OS gespeichert, der auf jedem System des Netzwerks ausgeführt werden kann, das in dieser Domäne definiert ist. Administratoren können Systeme (EIM-Clients) wie z. B. i5/OS-Systeme so konfigurieren, dass diese die Domäne nutzen können. Auf diese Weise können die Systeme und Anwendungen die Domänendaten für die Ausführung von EIM-Suchoperationen und für den Identitätsabgleich verwenden.

Windows 2000-Domäne

Bei der Einzelanmeldung wird als Windows 2000-Domäne ein Windows-Netzwerk bezeichnet, das mehrere Systeme, die als Clients und Server arbeiten, und außerdem eine Vielzahl von Services und Anwendungen umfasst, die von diesen Systemen benutzt werden. Im Folgenden sind einige der Komponenten aufgeführt, die bei der Einzelanmeldung eingesetzt werden und in einer Windows 2000-Domäne enthalten sein können:

Realm Ein Realm stellt einen Verbund aus mehreren Systemen und Services dar. Hauptzweck eines Realms ist die Authentifizierung von Clients und Services. Jeder Realm verwendet einen bestimmten Kerberos-Server, um die zum Realm gehörenden Principals zu verwalten.

Kerberos-Server

Ein Kerberos-Server, der auch als Key Distribution Center (KDC) bezeichnet wird, stellt einen Netzwerkservice dar, der auf einem Windows 2000-Server implementiert ist und zur Bereitstellung von Tickets und temporären Sitzungsschlüsseln für den Netzwerkauthentifizierungsservice dient. Auf dem Kerberos-Server wird eine Datenbank geführt, die Principals (Benutzer und Services) mit ihren zugeordneten geheimen Schlüsseln enthält. Der Kerberos-Server setzt sich aus dem Authentifizierungsserver und dem Ticket-granting Server zusammen. Ein Kerberos-Server verwendet Microsoft Windows Active Directory, um die Daten im Kerberos-Benutzerregister zu speichern und zu verwalten.

Microsoft Windows Active Directory

Bei Microsoft Windows Active Directory handelt es sich um einen LDAP-Server, der zusammen mit dem Kerberos-Server auf dem Windows 2000-Server implementiert ist. Active Directory wird zum Speichern und Verwalten der Informationen in einem Kerberos-Benutzerregister verwendet. Microsoft Windows Active Directory verwendet als Standardsicherheitsmechanismus die Kerberos-Authentifizierung. Aus diesem Grund setzen Sie die Kerberos-Technologie bereits ein, wenn Sie zur Verwaltung Ihrer Benutzer Microsoft Active Directory verwenden.

Zugehörige Konzepte

„Identitätsabgleich"
Als Identitätsabgleich wird der Prozess bezeichnet, bei dem definierte Beziehungen zwischen Benutzeridentitäten innerhalb eines Unternehmens verwendet werden, um Anwendungen und Betriebssystemen eine Zuordnung zwischen einer Benutzeridentität und einer anderen, zugehörigen Benutzeridentität zu ermöglichen.

Zugehörige Informationen

Enterprise Identity Mapping

Enterprise Identity Mapping - Konzepte

Identitätsabgleich

Als Identitätsabgleich wird der Prozess bezeichnet, bei dem definierte Beziehungen zwischen Benutzeridentitäten innerhalb eines Unternehmens verwendet werden, um Anwendungen und Betriebssystemen eine Zuordnung zwischen einer Benutzeridentität und einer anderen, zugehörigen Benutzeridentität zu ermöglichen.

Die Möglichkeit zur Herstellung einer solchen Zuordnung zwischen verschiedenen Identitäten ist für die Aktivierung der Einzelanmeldung von zentraler Bedeutung, da es hierdurch möglich wird, den Prozess der Authentifizierung vom Prozess der Berechtigung zu trennen. Der Identitätsabgleich erlaubt einem Benutzer die Anmeldung bei einem System und seine Authentifizierung auf der Basis der Berechtigungsnachweise einer bestimmten Benutzeridentität und den anschließenden Zugriff auf ein weiteres System oder eine weitere Ressource, ohne dass hierzu wieder entsprechende Berechtigungsnachweise eingegeben werden müssen. Stattdessen wird die authentifizierte Identität mit der Identität für das angeforderte System bzw. die angeforderte Ressource abgeglichen. Hierdurch wird die Benutzung der verfügbaren Systeme und Ressourcen erheblich vereinfacht, da der Benutzer bei der Anmeldung am zweiten System nicht

nochmals seine Berechtigungsnachweise eingeben muss. Außerdem werden seine Berechtigungen für das zweite System über die entsprechende Identität verarbeitet.

Zur Implementierung der Einzelanmeldung müssen Sie bestimmte EIM-Daten innerhalb der EIM-Domäne erstellen, um die Beziehungen zu definieren, die für die korrekte Zuordnung von Identitäten innerhalb der Einzelanmeldungsumgebung erforderlich sind. Hierdurch kann sichergestellt werden, dass EIM diese Daten zur Ausführung von Abgleichsuchoperationen für die Einzelanmeldung verwenden kann. Sie verwenden EIM zum Erstellen von Zuordnungen, mit denen die Beziehungen zwischen Benutzeridentitäten innerhalb Ihres Unternehmens definiert werden können. Sie können sowohl Kennungs- als auch Richtlinienzuordnungen erstellen, um diese Beziehungen zu definieren. Die Auswahl der zu verwendenden Methode hängt davon ab, welche Funktionsweise Sie beim Identitätsabgleich implementieren möchten.

Kennungszuordnungen

Kennungszuordnungen ermöglichen Ihnen das Definieren einer Eins-zu-eins-Beziehung zwischen Benutzeridentitäten. Hierbei wird eine EIM-Kennung benutzt, die für eine Einzelperson festgelegt ist. Kennungszuordnungen ermöglichen Ihnen die gezielte Steuerung des Identitätsabgleichs bei Benutzeridentitäten und sind besonders nützlich, wenn Einzelpersonen Benutzeridentitäten mit Sonderberechtigungen und anderen Berechtigungen besitzen. Diese Zuordnungen legen fest, wie die Benutzeridentitäten miteinander abgeglichen werden. In einem typischen Identitätsabgleichsszenario erstellen Sie Quellenzuordnungen für die Authentifizierung von Benutzeridentitäten und Zielzuordnungen für den Abgleich der zu authentifizierenden Benutzeridentität mit den zugehörigen Benutzeridentitäten, um die Berechtigung für den Zugriff auf andere Systeme und Ressourcen zu genehmigen. Beispiel: Sie erstellen die folgenden Kennungszuordnungen zwischen einer EIM-Kennung und den entsprechenden Benutzeridentitäten eines Benutzers:

- Eine Quellenzuordnung für den Kerberos-Principal des Benutzers, bei dem es sich um die Identität handelt, mit der sich der Benutzer beim Netzwerk anmeldet und in diesem authentifiziert wird.
- Zielzuordnungen für alle Benutzeridentitäten in den verschiedenen Benutzerregistern, die vom Benutzer verwendet werden. Hierzu gehören z. B. die Windows 2000-Benutzerprofile.

Im folgenden Beispiel wird dargestellt, wie der Identitätsabgleichsprozess bei der Kennungszuordnung eingesetzt wird. Der Sicherheitsadministrator von MyCo, Inc. erstellt eine EIM-Kennung (John Day) für einen Mitarbeiter. Diese EIM-Kennung dient zur eindeutigen Identifikation von John Day innerhalb des Unternehmens. Der Administrator erstellt anschließend Kennungszuordnungen zwischen der Kennung für John Day und den beiden Benutzeridentitäten, die dieser normalerweise im Unternehmen verwendet. Diese Zuordnungen legen fest, wie die Benutzeridentitäten abgeglichen werden. Der Administrator erstellt eine Quellenzuordnung für die Windows-Identität, bei der es sich um einen Kerberos-Principal handelt, und eine Zielzuordnung für ein Windows 2000-Benutzerprofil. Diese Zuordnungen ermöglichen der Windows-Identität des Benutzers den Abgleich mit seinem Windows 2000-Benutzerprofil.

John Day verwendet den zugehörigen Benutzernamen und das Kennwort jeden Morgen für die Anmeldung bei seiner Windows 2000-Workstation. Nach der Anmeldung startet er System i Access für Windows, um dann über Windows 2000 auf das Windows 2000-System zuzugreifen. Da die Einzelanmeldung aktiviert ist, verwendet der Identitätsabgleichsprozess seine authentifizierte Windows-Identität, um nach dem zugehörigen Windows 2000-Benutzerprofil zu suchen, und führt dann für den Benutzer transparent seine Authentifizierung und Berechtigung für Windows 2000 durch.

| In den Vorgängerreleases von i5/OS unterstützte die Einzelanmeldung die Zuordnung zu einer lokalen
| Benutzeridentität in EIM (Enterprise Identity Mapping) pro System. Nun unterstützt die Einzelan-
| meldung die Auswahl aus mehreren lokalen Benutzeridentitätszuordnungen für dasselbe System. Hierbei
| wird die IP-Adresse des Zielsystems verwendet, um die korrekte lokale Benutzeridentitätszuordnung auf
| diesem System auszuwählen.

Richtlinienzuordnungen

Richtlinienzuordnungen ermöglichen Ihnen das Definieren einer Viele-zu-eins-Beziehung zwischen einer Gruppe von Benutzeridentitäten in einem oder auch in mehreren Benutzerregistern und einer bestimmten Zielbenutzeridentität in einem anderen Benutzerregister. Normalerweise verwenden Sie Richtlinienzuordnungen, um eine Gruppe von Benutzern, die alle dieselbe Berechtigungsstufe für eine Anwendung benötigen, und eine einzelne Benutzeridentität abzugleichen, die über die gewünschte Berechtigung verfügt.

Im folgenden Beispiel wird dargestellt, wie der Identitätsabgleich bei der Definition von Richtlinienzuordnungen eingesetzt wird. Eine bestimmte Anzahl von Mitarbeitern der Auftragsannahmeabteilung von MyCo, Inc. benötigen alle dieselbe Berechtigung, um auf eine webbasierte Anwendung zuzugreifen, die auf dem Server unter Windows 2000 ausgeführt wird. Diese Benutzer verfügen momentan über Benutzeridentitäten für diesen Zweck, die in einem einzigen Benutzerregister mit dem Namen Order_app definiert sind. Der Administrator erstellt eine Standardrichtlinienzuordnung für Register, um alle Benutzer im Benutzerregister Order_app mit einem einzigen Windows 2000-Benutzerprofil abzugleichen. Dieses Windows 2000-Benutzerprofil mit dem Namen SYSUSER stellt die Mindestberechtigung bereit, die für diese Gruppe von Benutzern benötigt wird. Durch Ausführung dieses Konfigurationsschrittes kann der Administrator sicherstellen, dass alle Benutzer der webbasierten Anwendung über die Zugriffsberechtigungen mit den korrekten Berechtigungsstufen verfügen, die sie benötigen. Allerdings hat diese Lösung auch Vorteile für den Administrator, da es für ihn nicht mehr erforderlich ist, für jeden Benutzer einzelne Windows 2000-Benutzerprofile zu erstellen und zu verwalten.

Zugehörige Konzepte

„Domänen" auf Seite 6
Zur Implementierung einer Einzelanmeldungsumgebung werden EIM- und Windows-Domänen verwendet.

Zugehörige Informationen

EIM-Kennung

EIM-Registerdefinitionen

EIM-Zuordnungen

EIM-Abgleichsuchoperationen

EIM-Domäne

i5/OS-Unterstützung

Die i5/OS-Implementierung von Enterprise Identity Mapping (EIM) und Kerberos (im Folgenden als Netzwerkauthentifizierungsservice bezeichnet) stellt dem Benutzer eine echte Einzelanmeldungsumgebung mit mehreren Ebenen zur Verfügung.

Der Netzwerkauthentifizierungsservice ist die IBM Implementierung von Kerberos und für die GSS-APIs (GSS = Generic Security Service). Sie können EIM zum Definieren von Zuordnungen verwenden, die einen Abgleich zwischen einem Kerberos-Principal und einem i5/OS-Benutzerprofil ermöglichen. Anschließend kann diese Zuordnung verwendet werden, um festzustellen, welche EIM-Kennung einem lokalen i5/OS-Benutzerprofil bzw. dem entsprechenden Kerberos-Principal entspricht. Diese Funktionsweise stellt einen der Vorteile dar, die die Aktivierung der Einzelanmeldung auf dem Server unter i5/OS bietet.

i5/OS-Aktivierung für die Einzelanmeldung

Zur Aktivierung einer Einzelanmeldungsumgebung nutzt IBM zwei Technologien, die zusammen eingesetzt werden. Hierbei handelt es sich um EIM und den Netzwerkauthentifizierungsservice, der die IBM Implementierung von Kerberos und der GSS-APIs ist. Durch die Konfiguration dieser beiden Technologien kann der Administrator ein System so einrichten, dass eine Einzelanmeldungsumgebung unterstützt wird. Windows 2000, Windows XP, Windows Vista, AIX und z/OS verwenden zur Benutzerauthentifizie-

rung im Netzwerk das Kerberos-Protokoll. Kerberos benutzt ein netzwerkbasiertes, sicheres Key Distribution Center (KDC), mit dem Principals (Kerberos-Benutzer) im Netzwerk authentifiziert werden können. Die erfolgreiche Authentifizierung eines Benutzers im KDC wird durch ein Kerberos-Ticket belegt. Dieses Ticket kann von einem Benutzer an einen Service übergeben werden, der zur Annahme von Tickets konfiguriert wurde. Der Service, durch den das Ticket angenommen wurde, verwendet dieses zur Feststellung der Benutzeridentität (innerhalb des Kerberos-Benutzerregisters und des zugehörigen Realms) und zur Überprüfung der Richtigkeit dieser Benutzeridentität.

Während der Netzwerkauthentifizierungsservice einem Server die Nutzung eines Kerberos-Realms ermöglicht, bietet EIM ein Verfahren zur Zuordnung dieser Kerberos-Principals zu einer einzigen EIM-Kennung, die diesen Benutzer unternehmensweit darstellt. Andere Benutzeridentitäten wie z. B. i5/OS-Benutzernamen können dieser EIM-Kennung ebenfalls zugeordnet werden. Auf der Basis dieser Zuordnungen stellt EIM ein Verfahren für i5/OS und für Anwendungen zur Verfügung, mit dem festgestellt werden kann, welches i5/OS-Benutzerprofil der Person oder Entität zugeordnet ist, die durch den Kerberos-Principal dargestellt wird. Die in EIM gespeicherten Daten sind in einer Baumstruktur gespeichert, deren Stammelement eine EIM-Kennung bildet. Die Liste der Benutzeridentitäten, die dieser EIM-Kennung zugeordnet sind, stellen hingegen die Zweige dieser Baumstruktur dar.

Die Aktivierung der Einzelanmeldung auf Ihrem Server vereinfacht die Verwaltung von i5/OS-Benutzerprofilen und reduziert die Anzahl der Anmeldevorgänge, die ein Benutzer für den Zugriff auf mehrere i5/OS-Anwendungen und -Server ausführen muss. Darüber hinaus kann auf diese Weise der Zeitaufwand reduziert werden, der für die Kennwortverwaltung der einzelnen Benutzer anfällt. Durch die Einzelanmeldung ist es für jeden Benutzer möglich, beim Zugriff auf die benötigten Anwendungen und Server mit weniger Kennwörtern zu arbeiten. Hierdurch wird die System i-Benutzung erheblich vereinfacht.

Momentan für die Einzelanmeldung aktivierte i5/OS-Client- und -Serveranwendungen

- i5/OS Host-Server wird momentan von System i Access für Windows und System i Navigator verwendet.
- Telnet-Server: Momentan verwendet von PC5250 und IBM WebSphere Host On-Demand Version 8: Funktion Web Express Logon.
- Open DataBase Connectivity (ODBC): Ermöglicht die Einzelanmeldung bei i5/OS-Datenbanken über ODBC.
- Java Database Connectivity (JDBC): Ermöglicht die Einzelanmeldung bei i5/OS-Datenbanken über ODBC.
- Distributed Relational Database Architecture (DRDA): Ermöglicht die Einzelanmeldung bei i5/OS-Datenbanken über ODBC.
- QFileSrv.400.

ISV-Unterstützung

Ein unabhängiger Softwareanbieter (ISV = Independent Software Vendor) kann Anwendungen und Programme erstellen, die eine Einzelanmeldungsumgebung nutzen können.

Als unabhängiger Softwareanbieter ist Ihnen bekannt, dass viele Ihrer Kunden Einzelanmeldungsumgebungen implementieren wollen, um die Kosten- und Zeitvorteile zu nutzen, die sich durch den Einsatz einer solchen Umgebung ergeben. Sie wollen sicherstellen, dass Ihre Anwendungsprodukte so entworfen sind, dass eine Nutzung von Einzelanmeldungsumgebungen möglich ist, so dass Sie auch weiterhin in der Lage sind, die Anforderungen Ihrer Kunden zu erfüllen.

Um Ihre Anwendungen für die Nutzung einer i5/OS-Einzelanmeldungsumgebung zu aktivieren, müssen Sie die folgenden Tasks ausführen:

Aktivieren Ihrer i5/OS-Serveranwendungen für EIM

Eine der Grundlagen für die Implementierung einer Einzelanmeldungsumgebung ist Enterprise Identity Mapping (EIM). Bei Enterprise Identity Mapping (EIM) handelt es sich um einen Mechanismus für den Abgleich bzw. die Zuordnung einer Person oder Entität mit bzw. zu den entsprechenden Benutzeridentitäten in den verschiedenen Registern des Unternehmens. Anwendungsentwickler für i5/OS verwenden EIM zur Erstellung von Anwendungen, die ein Benutzerregister zur Authentifizierung und ein anderes für die Berechtigung verwenden, wobei der Benutzer nicht zweimal seine Berechtigungsnachweise eingeben muss. EIM stellt APIs zur Erstellung und Verwaltung dieser Identitätsabgleichbeziehungen zur Verfügung. Darüber hinaus werden von dem Produkt APIs bereitgestellt, die von den Anwendungen zur Abfrage dieser Informationen verwendet werden können. Sie können Anwendungen schreiben, die die EIM-APIs zur Ausführung von Suchoperationen nach Benutzeridentitäten innerhalb eines Unternehmens einsetzen.

Aktivieren Ihrer i5/OS-Server- und -Clientanwendungen zur Verwendung eines allgemeinen Authentifizierungsverfahrens

Sie können jedes allgemein verfügbare Authentifizierungsverfahren für die Einzelanmeldungsumgebung Ihrer Anwendung einsetzen, die Einzelanmeldungsumgebung von i5/OS basiert aber auf dem Netzwerkauthentifizierungsservice (Kerberos), der eine integrierte Einzelanmeldungsumgebung mit Windows 2000- und 2003-Domänen bereitstellt. Wenn Sie möchten, dass Ihre Anwendungen die gleiche integrierte Einzelanmeldungsumgebung mit derselben Sicherheitsstufe nutzen können wie i5/OS, sollten Sie als Authentifizierungsverfahren für Ihre Anwendungen ebenfalls den Netzwerkauthentifizierungsservice verwenden. Im Folgenden sind Beispiele zu den verschiedenen Authentifizierungsmethoden aufgeführt, die Sie für Ihre Anwendungen auswählen können:

Netzwerkauthentifizierungsservice

Im Szenario: Einzelanmeldung für ISV-Anwendungen aktivieren erfahren Sie, wie Sie EIM-Anwendungsprogrammierschnittstellen (APIs) zusammen mit dem Netzwerkauthentifizierungsservice zur Erstellung von Anwendungen einsetzen können, die den vollen Funktionsumfang einer Einzelanmeldungsumgebung nutzen können. Dieses Szenario enthält verschiedene ISV-Codebeispiele einschließlich einiger Pseudocodebeispiele, z. B. Pseudocodeelemente und Codefragmente, die Sie zur Fertigstellung Ihres Programms verwenden können.

Digitale Zertifikate

Sie können Anwendungen für eine Einzelanmeldungsumgebung entwickeln, die zur Authentifizierung digitale Zertifikate verwenden. Um den Code in Ihr Programm einzufügen, der zur Authentifizierung mit Hilfe digitaler Zertifikate benötigt wird, müssen Sie die Digital Certificate Management APIs verwenden.

Lightweight Directory Access Protocol (LDAP)

Sie können Anwendungen für eine Einzelanmeldungsumgebung entwickeln, die zur Authentifizierung den Directory-Server verwenden. Um den Code in Ihr Programm einzufügen, der zur Authentifizierung mit Hilfe des Directory-Servers benötigt wird, müssen Sie die Lightweight Directory Access APIs verwenden.

Zugehörige Informationen

Enterprise Identity Mapping

EIM APIs

Szenarios: Einzelanmeldung

Diese Szenarios enthalten Beispiele aus dem realen Geschäftsleben, die für die Planung, Konfiguration und den Einsatz der Einzelanmeldung in einem Unternehmen verwendet werden können.

Obwohl alle Szenarios Modelle für Netzwerkadministratoren bereitstellen, gibt es auch ein Szenario für Anwendungsentwickler, in dem die Aufgaben dargestellt werden, die vom Entwickler ausgeführt werden müssen, um Anwendungen zu erstellen, die eine Einzelanmeldungsumgebung nutzen können.

Szenario: Einzelanmeldungstestumgebung erstellen

In diesem Szenario wird dargestellt, wie der Netzwerkauthentifizierungsservice und EIM konfiguriert werden müssen, um eine Basistestumgebung für die Einzelanmeldung zu erstellen. Verwenden Sie dieses Szenario, um sich vorab in einer isolierten Testumgebung einen grundlegenden Überblick über die Arbeitsschritte zu verschaffen, die zur Konfiguration einer Einzelanmeldungsumgebung auszuführen sind, bevor Sie die Einzelanmeldung unternehmensweit implementieren.

Situation

Sie sind der Netzwerkadministrator John Day, der bei einem Großhandelsunternehmen mit zahlreichen Mitarbeitern angestellt ist. Momentan verwenden Sie viel Zeit darauf, Fehler bei der Verwendung der in Ihrem Unternehmen definierten Benutzer-IDs und Kennwörter (z. B. Fehler durch vergessene Kennwörter) zu beheben. Ihr Netzwerk besteht aus mehreren System i-Modellen und einem Windows 2000-Server, auf dem Ihre Benutzer in Microsoft Windows Active Directory registriert sind. Wie Sie wissen, verwendet Microsoft Active Directory zur Authentifizierung von Windows-Benutzern das Kerberos-Protokoll. Sie wissen auch, dass die System i-Plattform eine Einzelanmeldungslösung unterstützt, die auf einer Implementierung der Kerberos-Authentifizierung basiert. Diese Implementierung wird als Netzwerkauthentifizierungsservice bezeichnet und zusammen mit EIM (Enterprise Identity Mapping) eingesetzt.

Sie sind sehr interessiert daran, welche Vorteile die Einzelanmeldung für Ihr Unternehmen bieten würde. Allerdings möchten Sie sich fundierte Kenntnisse zur Konfiguration und zu den Verwendungsmöglichkeiten einer Einzelanmeldungslösung aneignen, bevor Sie diese unternehmensweit einführen. Aus diesem Grund wollen Sie zuerst eine Testumgebung konfigurieren.

Nachdem Sie die verschiedenen Benutzergruppen Ihres Unternehmens geprüft haben, wählen Sie die Auftragsannahmeabteilung aus, um die Testumgebung zu implementieren. Die Mitarbeiter dieser Abteilung verwenden mehrere Anwendungen, die auf einem bestimmten System i-Modell installiert sind, um eingehende Kundenbestellungen zu bearbeiten. Aus diesem Grund bietet die Auftragsannahmeabteilung hervorragende Möglichkeiten, um eine Einzelanmeldungstestumgebung einzurichten, mit deren Hilfe Sie sich mit der Funktionsweise der Einzelanmeldung vertraut machen und feststellen können, welche Faktoren bei der Planung einer unternehmensweiten Einzelanmeldungsimplementierung berücksichtigt werden müssen.

Vorteile des Szenarios

- Darstellung der Vorteile der Einzelanmeldung in einer isolierten Testumgebung zum besseren Verständnis der Nutzungsmöglichkeiten vor der Einrichtung einer unternehmensweiten Einzelanmeldungsumgebung.
- Erarbeitung detaillierter Daten zum Planungsprozess, die zur schnellen und erfolgreichen Implementierung der Einzelanmeldung im gesamten Unternehmen erforderlich sind.
- Reduzierung des Einarbeitungsaufwands für die Nutzung einer unternehmensweiten Implementierung der Einzelanmeldung.

Ziele

Als Netzwerkadministrator von MyCo, Inc. wollen Sie eine isolierte Einzelanmeldungsumgebung für Testzwecke einrichten, in der eine begrenzte Anzahl von Benutzern mit einem einzigen System i-Modell arbeitet. Sie möchten umfangreiche Tests durchführen, um sicherzustellen, dass die definierten Benutzeridentitäten innerhalb der Testumgebung korrekt zugeordnet werden. Auf der Basis dieser Konfiguration wollen Sie die Testumgebung schrittweise erweitern und weitere Systeme und Benutzer Ihres Unternehmens aufnehmen.

Dieses Szenario hat die folgenden Ziele:

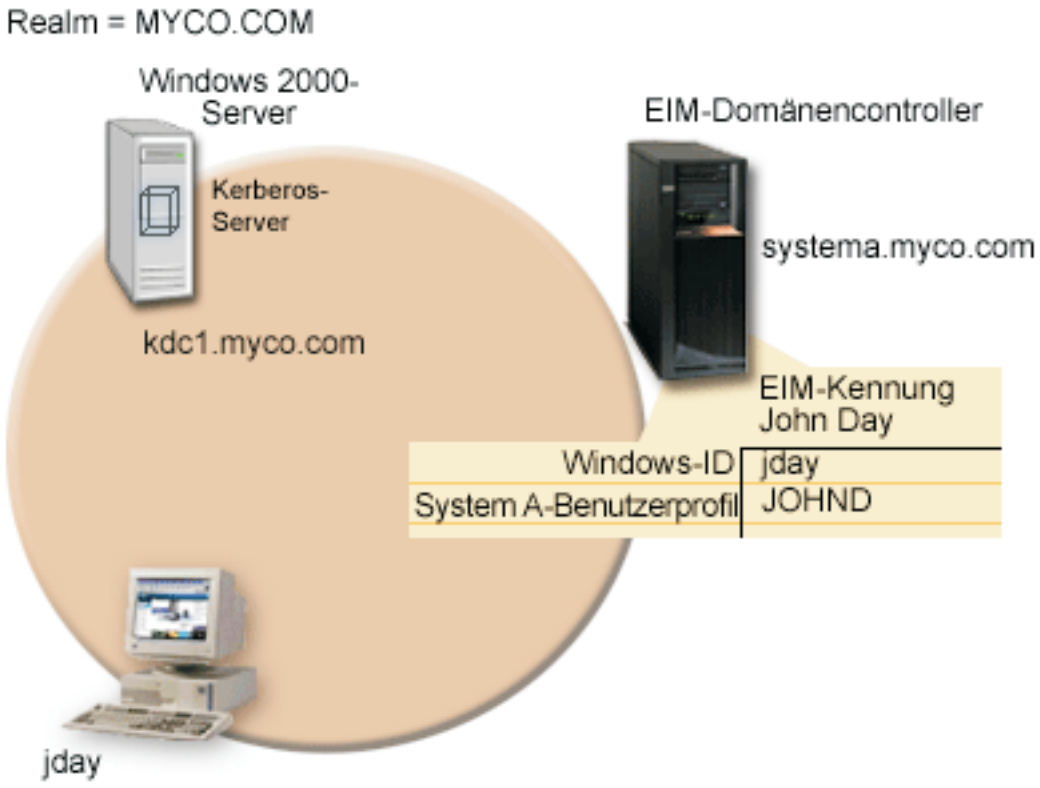
- Das System i-Modell mit der Bezeichnung System A muss innerhalb des Realms MYCO.COM Kerberos einsetzen können, um die Benutzer und Services zu authentifizieren, die diese Einzelanmeldungstest-

umgebung nutzen. Um das System für die Verwendung von Kerberos zu aktivieren, muss System A für den Einsatz des Netzwerkauthentifizierungsservice konfiguriert werden.
- Der Directory-Server auf System A muss als Domänencontroller für die neue EIM-Domäne fungieren.

  Anmerkung: Unter „Domänen" auf Seite 6 wird beschrieben, wie eine EIM-Domäne und eine Windows 2000-Domäne in eine Einzelanmeldungsumgebung integriert werden können.
- Ein Benutzerprofil auf System A und ein Kerberos-Principal müssen jeweils einer einzigen EIM-Kennung zugeordnet sein.
- Ein Kerberos-Service-Principal muss verwendet werden, um den Benutzer bei den System i Access für Windows-Anwendungen zu authentifizieren.

Details

Die folgende Abbildung veranschaulicht die Netzwerkumgebung für dieses Szenario.



Die Abbildung veranschaulicht die folgenden Punkte, die für dieses Szenario relevant sind.

Für das Unternehmen definierte EIM-Domänendaten
- Eine EIM-Registerdefinition für System A mit dem Namen SYSTEMA.MYCO.COM.
- Eine EIM-Registerdefinition für das Kerberos-Register mit dem Namen MYCO.COM.
- Eine EIM-Kennung mit dem Namen John Day. Diese Kennung dient zur eindeutigen Identifikation von John Day, dem Administrator von MyCo.
- Eine Quellenzuordnung für den Kerberos-Principal jday auf dem Windows 2000-Server.
- Eine Zielzuordnung für das Benutzerprofil JOHND auf System A.

Windows 2000-Server

- Fungiert als Kerberos-Server (kdc1.myco.com) für das Netzwerk, wird auch als KDC (Key Distribution Center) bezeichnet.
- Der Standard-Realm für den Kerberos-Server ist `MYCO.COM`.
- Der Kerberos-Principal jday ist beim Kerberos-Server auf dem Windows 2000-Server registriert. Dieser Principal wird zur Erstellung einer Quellenzuordnung zur EIM-Kennung John Day verwendet.

System A

- Verwendet i5/OS ab Version 5 Release 4 (V5R4) mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS Host-Server (5761-SS1 Option 12)
  - Qshell Interpreter (5761-SS1 Option 30)
  - System i Access für Windows (5761-XE1)

  Anmerkung: Sie können dieses Szenario mit einem Server implementieren, der unter i5/OS ab V5R3 arbeitet. Allerdings können einige der Konfigurationsschritte auf Grund der Erweiterungen in i5/OS V5R4 leicht abweichen. 5722 ist der Produktcode für i5/OS-Optionen und -Produkte mit einer Version vor V6R1.
- IBM Directory Server for System i (LDAP) auf System A wird als EIM-Domänencontroller für die neue EIM-Domäne MyCoEimDomain konfiguriert.
- System A nutzt die EIM-Domäne MyCoEimDomain.
- Der Principal-Name für System A lautet `krbsvr400/systema.myco.com@MYCO.COM`.
- Das Benutzerprofil JOHND ist auf System A vorhanden. Sie erstellen eine Zielzuordnung zwischen diesem Benutzerprofil und der EIM-Kennung John Day.
- Das Ausgangsverzeichnis für das i5/OS-Benutzerprofil JOHND (/home/JOHND) ist auf System A definiert.

Für die Verwaltung der Einzelanmeldung verwendeter Client-PC

- Wird unter dem Betriebssystem Microsoft Windows 2000 ausgeführt.
- Verwendet System i Access für Windows (5761-XE1).
- Verwendet den System i Navigator mit den folgenden installierten Unterkomponenten:
  - Netzwerk
  - Sicherheit
- Fungiert als primäres Anmeldesystem für den Administrator John Day.
- Konfiguriert als Bestandteil des Realms MYCO.COM (Windows-Domäne).

Voraussetzungen und Annahmen

Zur erfolgreichen Implementierung dieses Szenarios müssen die folgenden Voraussetzungen und Annahmen zutreffen:

1. Alle Systemvoraussetzungen einschließlich der Installation der Software und des Betriebssystems wurden überprüft.

   Führen Sie folgende Schritte durch, um festzustellen, ob die erforderlichen Lizenzprogramme installiert wurden:

   a. Erweitern Sie im System i Navigator die Einträge für **Ihr System** → **Konfiguration und Service** → **Software** → **Installierte Produkte**.
   b. Vergewissern Sie sich, dass alle erforderlichen Lizenzprogramme installiert sind.
2. Die gesamte erforderliche Hardwareplanung und -konfiguration wurde durchgeführt.
3. TCP/IP und die Basissystemsicherheit wurden auf jedem System konfiguriert und getestet.

4. Der Directory-Server und EIM sollten zuvor noch nicht auf System A konfiguriert worden sein.

   Anmerkung: Die Anweisungen in diesem Szenario basieren auf der Annahme, dass der Directory-Server zuvor noch nicht auf System A konfiguriert wurde. Wurde dieses Produkt bereits konfiguriert, können Sie diese Anweisungen trotzdem mit geringen Änderungen anwenden. Diese Änderungen sind an den entsprechenden Stellen in den Konfigurationsschritten vermerkt.
5. Für die Auflösung der Hostnamen im Netzwerk wird ein einziger DNS-Server verwendet. Es werden keine Hosttabellen für die Auflösung der Hostnamen verwendet.

   Anmerkung: Die Verwendung von Hosttabellen kann bei der Kerberos-Authentifizierung zu Fehlern bei der Namensauflösung oder zu anderen Problemen führen.

Konfigurationsschritte

Anmerkung: Sie sollten sich mit den im Zusammenhang mit der Einzelanmeldung verwendeten Konzepten, z. B. mit dem Netzwerkauthentifizierungsservice und EIM (Enterprise Identity Mapping), eingehend vertraut machen, bevor Sie dieses Szenario implementieren. Wenn Sie bereit sind, mit diesem Szenario fortzufahren, sollten Sie die folgenden Schritte durchführen:

Zugehörige Tasks

„Anwendung testen" auf Seite 74
Sie haben die Entwicklung der client- und der serverspezifischen Aktualisierungen für Ihre Anwendung **Kalender** abgeschlossen, so dass diese Anwendung nun in einer Einzelanmeldungsumgebung unter i5/OS ausgeführt werden kann. Jetzt können Sie die Anwendung testen.

„Einzelanmeldung konfigurieren" auf Seite 87
Zum Konfigurieren einer Einzelanmeldungsumgebung müssen Sie eine kompatible Authentifizierungsmethode verwenden und EIM zum Erstellen und Verwalten der Benutzerprofile und Identitätsabgleiche benutzen.

Zugehörige Informationen

Hinweise zur Auflösung von Hostnamen

Enterprise Identity Mapping - Konzepte

Planungsarbeitsblätter ausfüllen

Die folgenden Planungsarbeitsblätter wurden auf der Basis der allgemeinen Planungsarbeitsblätter für die Einzelanmeldung an dieses Szenario angepasst.

Diese Planungsarbeitsblätter veranschaulichen die Informationen, die Sie zusammenstellen, sowie die Entscheidungen, die Sie treffen müssen, um die Einzelanmeldungsimplementierung vorzubereiten, die im vorliegenden Szenario beschrieben wird. Um eine erfolgreiche Implementierung sicherzustellen, sollten Sie für alle vorausgesetzten Elemente im Arbeitsblatt die Antwort "Ja" geben können. Außerdem sollten Sie alle Informationen, die zur Fertigstellung der Arbeitsblätter erforderlich sind, aufzeichnen, bevor Sie Konfigurationsaufgaben ausführen.

Anmerkung: Sie sollten sich mit den im Zusammenhang mit der Einzelanmeldung verwendeten Konzepten, z. B. mit dem Netzwerkauthentifizierungsservice und EIM (Enterprise Identity Mapping), eingehend vertraut machen, bevor Sie dieses Szenario implementieren.

Tabelle 1. Arbeitsblatt für die Einzelanmeldungsvoraussetzungen

Arbeitsblatt für Voraussetzungen	Antworten
Arbeitet Ihr System mit i5/OS ab V5R4?	Ja

Tabelle 1. Arbeitsblatt für die Einzelanmeldungsvoraussetzungen (Forts.)

Arbeitsblatt für Voraussetzungen	Antworten
Sind die folgenden Optionen und Lizenzprogramme auf System A installiert? • i5/OS Host-Server (5761-SS1 Option 12) • Qshell Interpreter (5761-SS1 Option 30) • System i Access für Windows (5761-XE1) **Anmerkung:** 5722 ist der Produktcode für i5/OS-Optionen und -Produkte mit einer Version vor V6R1.	Ja
Ist eine Anwendung installiert, die auf allen PCs, die sich in der Einzelanmeldungsumgebung befinden, für die Einzelanmeldung aktiviert ist? **Anmerkung:** In diesem Szenario wurde auf allen teilnehmenden PCs System i Access für Windows (5761-XE1) installiert.	Ja
Ist der System i Navigator auf dem Administrator-PC installiert? • Ist die Unterkomponente ″Sicherheit″ des System i Navigator auf dem PC des Administrators installiert? • Ist die Unterkomponente ″Netzwerk″ des System i Navigator auf dem PC des Administrators installiert?	Ja
Ist das neueste System i Access für Windows-Service-Pack installiert? Informationen zum neuesten Service-Pack finden Sie auf der Webseite für System i Access .	Ja
Verfügt der Administrator über die Sonderberechtigungen *SECADM, *ALLOBJ und *IOSYSCFG?	Ja
Fungiert eines der folgenden Systeme als Kerberos-Server (auch als KDC bezeichnet)? Wenn ja, geben Sie an, um welches System es sich handelt. 1. Windows (R) 2000-Server **Anmerkung:** Microsoft Windows 2000 Server verwendet als Standardsicherheitsmechanismus die Kerberos-Authentifizierung. 2. Windows (R) Server 2003 3. i5/OS PASE ab V5R3 4. AIX-Server 5. z/OS	Ja, Windows 2000-Server
Sind alle PCs Ihres Netzwerks in einer Windows 2000-Domäne konfiguriert?	Ja
Wurden die neuesten PTFs (vorläufigen Programmkorrekturen) angelegt?	Ja
Beträgt die Abweichung zwischen der Systemzeit des System i-Modells und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung größer, lesen Sie die Informationen in Systemzeiten synchronisieren.	Ja
Arbeiten Sie beim Kerberos-Server mit i5/OS PASE?	Auf dem System muss IBM Network Authentication Enablement for i5/OS (5761-NAE) installiert sein.

Sie benötigen diese Informationen, um EIM und den Netzwerkauthentifizierungsservice so zu konfigurieren, dass eine Einzelanmeldungstestumgebung erstellt werden kann.

Tabelle 2. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung für System A

Planungsarbeitsblatt für die Konfiguration von System A	**Antworten**
Verwenden Sie die folgenden Informationen, um den EIM-Konfigurationsassistenten auszuführen. Die Informationen in diesem Arbeitsblatt korrelieren mit den Informationen, die Sie zur Angabe auf den einzelnen Seiten im Assistenten benötigen:	
Wie möchten Sie EIM auf Ihrem System konfigurieren? • System zu einer vorhandenen Domäne hinzufügen • Neue Domäne erstellen und System hinzufügen	Neue Domäne erstellen und System hinzufügen.
Wo möchten Sie die EIM-Domäne konfigurieren?	Auf dem lokalen Directory-Server **Anmerkung:** Bei dieser Auswahl wird der Directory-Server auf demselben System konfiguriert, auf dem Sie gegenwärtig EIM konfigurieren.
Möchten Sie den Netzwerkauthentifizierungsservice konfigurieren? **Anmerkung:** Sie müssen den Netzwerkauthentifizierungsservice konfigurieren, um die Einzelanmeldung konfigurieren zu können.	Ja
Der Assistent für den Netzwerkauthentifizierungsservice wird über den EIM-Konfigurationsassistenten gestartet. Verwenden Sie die folgenden Informationen, um den Assistenten für den Netzwerkauthentifizierungsservice auszuführen: **Anmerkung:** Der Assistent für den Netzwerkauthentifizierungsservice kann unabhängig vom EIM-Konfigurationsassistenten gestartet werden.	
Wie lautet der Name des Kerberos-Standard-Realms, zu dem Ihr System i-Modell gehören soll? **Anmerkung:** Eine Windows 2000-Domäne ist mit einem Kerberos-Realm vergleichbar. Microsoft Windows Active Directory verwendet als Standardsicherheitsmechanismus die Kerberos-Authentifizierung.	`MYCO.COM`
Verwenden Sie Microsoft Active Directory?	Ja
Wie heißt der Kerberos-Server, der auch als KDC (Key Distribution Center) bezeichnet wird, für diesen Kerberos-Standard-Realm? An welchem Port ist der Kerberos-Server empfangsbereit?	**KDC**: `kdc1.myco.com` **Port**: `88` **Anmerkung:** Dies ist der Standardport für den Kerberos-Server.
Möchten Sie einen Kennwortserver für diesen Standard-Realm konfigurieren? Wenn ja, beantworten Sie die folgenden Fragen: Wie lautet der Name des Kennwortservers für diesen Kerberos-Server? An welchem Port ist der Kennwortserver empfangsbereit?	Ja **Kennwortserver**: `kdc1.myco.com` **Port**: `464` **Anmerkung:** Dies ist der Standardport für den Kennwortserver.
Für welche Services sollen Chiffrierschlüsseleinträge erstellt werden? • i5/OS-Kerberos-Authentifizierung • LDAP • IBM HTTP-Server für i5/OS • i5/OS NetServer • NFS-Server (Network File System)	i5/OS-Kerberos-Authentifizierung
Wie lautet das Kennwort für Ihre(n) Service-Principal(s)?	`systema123` **Anmerkung:** Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.

Tabelle 2. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung für System A (Forts.)

Planungsarbeitsblatt für die Konfiguration von System A	**Antworten**
Möchten Sie eine Stapeldatei erstellen, um das Hinzufügen der Service-Principals für System A zum Kerberos-Register zu automatisieren?	Ja
Möchten Sie für die i5/OS-Service-Principals in der Stapeldatei Kennwörter hinzufügen?	Ja
Wenn Sie den Assistenten für den Netzwerkauthentifizierungsservice verlassen, gelangen Sie in den EIM-Konfigurationsassistenten zurück. Verwenden Sie die folgenden Informationen, um den EIM-Konfigurationsassistenten auszuführen:	
Geben Sie Benutzerinformationen an, die der Assistent bei der Konfiguration des Directory-Servers verwenden soll. Dies ist der Benutzer der Verbindung. Sie müssen die Portnummer, den registrierten Namen (Distinguished Name, DN) des Administrators und ein Kennwort für den Administrator angeben. **Anmerkung:** Geben Sie den registrierten Namen und das Kennwort des LDAP-Administrators an, um sicherzustellen, dass der Assistent eine ausreichende Berechtigung zur Verwaltung der EIM-Domäne und der darin enthaltenen Objekte besitzt.	**Port**: `389` **Registrierter Name**: `cn=administrator` **Kennwort**: `mycopwd` **Anmerkung:** Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.
Wie lautet der Name der EIM-Domäne, die Sie erstellen möchten?	`MyCoEimDomain`
Möchten Sie einen übergeordneten registrierten Namen für die EIM-Domäne angeben?	Nein
Welche Benutzerregister möchten Sie zur EIM-Domäne hinzufügen?	Lokales i5/OS--SYSTEMA.MYCO.COM Kerberos--MYCO.COM **Anmerkung:** Bei den Kerberos-Principals, die auf dem Windows 2000-Server gespeichert sind, muss die Groß-/Kleinschreibung nicht beachtet werden. Aus diesen Grund sollte **Bei Kerberos-Benutzeridentitäten muss die Groß-/Kleinschreibung beachtet werden** nicht ausgewählt werden.
Welchen EIM-Benutzer soll System A bei der Ausführung von EIM-Operationen verwenden? Dies ist der Systembenutzer. **Anmerkung:** Wenn Sie den Directory-Server nicht vor der Konfiguration der Einzelanmeldung konfiguriert haben, können Sie als registrierten Namen für den Systembenutzer nur die Kombination aus dem registrierten Namen und dem Kennwort des LDAP-Administrators bereitstellen.	**Benutzerart**: `Registrierter Name und Kennwort` **Benutzer**: `cn=administrator` **Kennwort**: `mycopwd` **Anmerkung:** Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.
Nach Abschluss des EIM-Konfigurationsassistenten müssen Sie die folgenden Informationen verwenden, um die restlichen Arbeitsschritte auszuführen, die zur Konfiguration der Einzelanmeldung erforderlich sind:	
Wie lautet der Name des i5/OS-Benutzerprofils des Benutzers?	`JOHND`
Wie lautet der Name der EIM-Kennung, die Sie erstellen möchten?	`John Day`
Welche Zuordnungen sollen erstellt werden?	Quellenzuordnung: Kerberos-Principal `jday` Zielzuordnung: i5/OS-Benutzerprofil `JOHND`
Wie lautet der Name des Benutzerregisters, das den Kerberos-Principal enthält, für den die Quellenzuordnung erstellt werden soll?	`MYCO.COM`
Wie lautet der Name des Benutzerregisters, das das i5/OS-Benutzerprofil enthält, für das die Zielzuordnung erstellt werden soll?	`SYSTEMA.MYCO.COM`

Tabelle 2. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung für System A (Forts.)

Planungsarbeitsblatt für die Konfiguration von System A	Antworten
Welche Informationen müssen Sie angeben, um den EIM-Identitätsabgleich zu testen?	**Quellenregister**: `MYCO.COM` **Quellenbenutzer**: `jday` **Zielregister**: `SYSTEMA.MYCO.COM`

Zugehörige Informationen

Enterprise Identity Mapping - Konzepte

Basiskonfiguration für die Einzelanmeldung für System A erstellen

Der EIM-Konfigurationsassistent hilft Ihnen bei der Erstellung einer EIM-Basiskonfiguration und ruft außerdem den Assistenten für den Netzwerkauthentifizierungsservice auf, damit Sie eine Basiskonfiguration des Netzwerkauthentifizierungsservice erstellen können.

Anmerkung: Die Anweisungen in diesem Szenario basieren auf der Annahme, dass IBM Tivoli Directory Server for i5/OS zuvor noch nicht auf System A konfiguriert wurde. Wurde dieses Produkt bereits konfiguriert, können Sie diese Anweisungen trotzdem mit geringen Änderungen anwenden. Diese Änderungen sind an den entsprechenden Stellen in den Konfigurationsschritten vermerkt.

Nach Ausführung dieses Arbeitsschrittes sind die folgenden Tasks abgeschlossen:

- Erstellen einer neuen EIM-Domäne.
- Konfigurieren des Directory-Servers als EIM-Domänencontroller auf System A.
- Konfigurieren des Netzwerkauthentifizierungsservice.
- Erstellen der EIM-Registerdefinitionen des i5/OS-Registers und des Kerberos-Registers für System A in der neu erstellten EIM-Domäne.
- Konfigurieren von System A zur Nutzung der EIM-Domäne.

1. Erweitern Sie im System i Navigator die Einträge für **System A** → **Netzwerk** → **Enterprise Identity Mapping**.
2. Klicken Sie mit der rechten Maustaste auf **Konfiguration**, und wählen Sie **Konfigurieren** aus, um den EIM-Konfigurationsassistenten zu starten.
3. Wählen Sie auf der **Begrüßungsseite** die Auswahl **Neue Domäne erstellen und System hinzufügen**. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Position der EIM-Domäne angeben** die Auswahl **Auf dem lokalen Directory-Server** aus. Klicken Sie auf **Weiter**. Daraufhin wird der Assistent für den Netzwerkauthentifizierungsservice angezeigt.

   Anmerkung: Der Assistent für den Netzwerkauthentifizierungsservice wird nur angezeigt, wenn das System feststellt, dass zusätzliche Informationen eingegeben werden müssen, um den Netzwerkauthentifizierungsservice für die Einzelanmeldungsimplementierung zu konfigurieren.
5. Führen Sie die folgenden Schritte durch, um den Netzwerkauthentifizierungsservice zu konfigurieren:
   a. Wählen Sie auf der Seite **Netzwerkauthentifizierungsservice konfigurieren** die Auswahl **Ja** aus.

      Anmerkung: Daraufhin wird der Assistent für den Netzwerkauthentifizierungsservice gestartet. Mit diesem Assistenten können Sie verschiedene i5/OS-Schnittstellen und -Services zur Nutzung eines Kerberos-Realms konfigurieren.
   b. Geben Sie auf der Seite **Realm-Informationen angeben** im Feld **Standard-Realm** den Wert `MYCO.COM` ein, und wählen Sie **Microsoft Active Directory wird für Kerberos-Authentifizierung verwendet** aus. Klicken Sie auf **Weiter**.

c. Geben Sie auf der Seite **KDC-Informationen angeben** im Feld **KDC** den Wert `kdc1.myco.com` und im Feld **Port** den Wert 88 ein. Klicken Sie auf **Weiter**.

d. Wählen Sie auf der Seite **Kennwortserverinformationen angeben** die Auswahl **Ja** aus. Geben Sie im Feld **Kennwortserver** den Wert `kdc1.myco.com` und im Feld **Port** den Wert 464 ein. Klicken Sie auf **Weiter**.

e. Wählen Sie auf der Seite **Chiffrierschlüsseleinträge auswählen** die Auswahl **i5/OS-Kerberos-Authentifizierung** aus. Klicken Sie auf **Weiter**.

f. Geben Sie auf der Seite **i5/OS-Chiffrierschlüsseleintrag erstellen** ein Kennwort ein und bestätigen Sie es. Klicken Sie anschließend auf **Weiter**. Beispiel: `systema123`. Dieses Kennwort wird verwendet, wenn System A zum Kerberos-Server hinzugefügt wird.

   Anmerkung: Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.

g. Optional: Wählen Sie auf der Seite **Stapeldatei erstellen** die Auswahl **Ja** aus, machen Sie die folgenden Angaben, und klicken Sie auf **Weiter**:

   - **Stapeldatei:** Fügen Sie am Ende des standardmäßig verwendeten Stapeldateinamens die Zeichenfolge `systema` an. Beispiel: `C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystema.bat`.
   - Wählen Sie **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 jeder Person mit Lesezugriffsberechtigung für die Stapeldatei gelesen werden können. Daher wird empfohlen, dass Sie die Stapeldatei nach dem Gebrauch unverzüglich vom Kerberos-Server und von Ihrem PC löschen.

     Anmerkung: Wenn Sie das Kennwort nicht einfügen, werden Sie bei der Ausführung der Stapeldatei zur Eingabe des Kennworts aufgefordert.

h. Überprüfen Sie die Konfigurationsdetails für den Netzwerkauthentifizierungsservice auf der Seite **Zusammenfassung**, und klicken Sie auf **Fertig stellen**, um den Assistenten für den Netzwerkauthentifizierungsservice zu beenden und zum EIM-Konfigurationsassistenten zurückzukehren.

6. Geben Sie auf der Seite **Directory-Server konfigurieren** die folgenden Informationen ein, und klicken Sie auf **Weiter**:

   Anmerkung: Wenn Sie den Directory-Server vor dem Beginn dieses Szenarios konfiguriert haben, erscheint die Seite **Benutzer für Verbindung angeben** an Stelle der Seite **Directory-Server konfigurieren**. In diesem Fall müssen Sie den registrierten Namen und das Kennwort für den LDAP-Administrator angeben.

   - **Port**: `389`
   - **Registrierter Name**: `cn=Administrator`
   - **Kennwort**: `mycopwd`

     Anmerkung: Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.

7. Geben Sie auf der Seite **Domäne angeben** im Feld **Domäne** den Namen der Domäne ein, und klicken Sie dann auf **Weiter**. Beispiel: `MyCoEimDomain`.

8. Wählen Sie auf der Seite **Übergeordneten registrierten Namen für Domäne angeben** die Auswahl **Nein** aus, und klicken Sie dann auf **Weiter**.

   Anmerkung: Wenn der Directory-Server aktiv ist, wird die Nachricht angezeigt, dass Sie den Directory-Server beenden und erneut starten müssen, damit die Änderungen wirksam werden. Klicken Sie auf **Ja**, um den Directory-Server erneut zu starten.

9. Wählen Sie auf der Seite **Registerinformationen Lokales i5/OS** und **Kerberos** aus, und klicken Sie dann auf **Weiter**. Notieren Sie die Registernamen. Sie benötigen diese Registernamen, wenn Sie Zuordnungen zu EIM-Kennungen erstellen.

   Anmerkung:

   - Registernamen müssen in der Domäne eindeutig sein.
   - Sie können für das Benutzerregister einen speziellen Registerdefinitionsnamen eingeben, wenn Sie einen speziellen Benennungsplan für Registerdefinitionen (siehe hierzu Benennungsplan für EIM-Registerdefinitionen aufstellen) verwenden möchten. Für dieses Szenario können Sie jedoch die Standardwerte akzeptieren.

10. Wählen Sie auf der Seite **EIM-Systembenutzer angeben** den Benutzer aus, den das Betriebssystem bei der Ausführung von EIM-Operationen für Betriebssystemfunktionen verwendet. Klicken Sie anschließend auf **Weiter**.

    Anmerkung: Da Sie den Directory-Server nicht konfiguriert haben, bevor Sie die Schritte in diesem Szenario durchgeführt haben, können Sie nur den registrierten Namen des LDAP-Administrators als registrierten Namen auswählen.

    - **Benutzerart**: `Registrierter Name und Kennwort`
    - **Registrierter Name**: `cn=Administrator`
    - **Kennwort**: `mycopwd`

      Anmerkung: Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.

11. Bestätigen Sie die EIM-Konfigurationsdaten auf der Seite **Zusammenfassung**. Klicken Sie auf **Fertig stellen**.

Nach Abschluss der Basiskonfiguration für EIM und den Netzwerkauthentifizierungsservice auf System A können Sie nun den Service-Principal für System A zum Kerberos-Server hinzufügen.

Service-Principal von System A zum Kerberos-Server hinzufügen

Sie können zwischen zwei Methoden wählen, um den erforderlichen i5/OS-Service-Principal zum Kerberos-Server hinzuzufügen.

Sie können den Service-Principal wie im vorliegenden Szenario dargestellt manuell hinzufügen oder zur Ausführung dieses Arbeitsschrittes eine Stapeldatei verwenden. Sie haben diese Stapeldatei in Schritt 2 erstellt. Wenn Sie diese Datei verwenden möchten, können Sie sie mit FTP (File Transfer Protocol) auf den Kerberos-Server kopieren und dann ausführen.

Führen Sie die folgenden Schritte durch, um Principals anhand der Stapeldatei zum Kerberos-Server hinzuzufügen:

Vom Assistenten erstellte FTP-Stapeldatei

1. Öffnen Sie auf der Windows 2000-Workstation, die Sie zur Konfiguration des Netzwerkauthentifizierungsservice verwendet haben, eine Bedienerführung, und geben Sie `ftp kdc1.myco.com` ein, um eine FTP-Sitzung auf Ihrem PC zu starten. Sie werden aufgefordert, den Benutzernamen und das Kennwort des Administrators einzugeben.
2. Geben Sie an der FTP-Bedienerführung `lcd "C:\Documents and Settings\All Users\Documents\IBM\Client Access"` ein. Drücken Sie die Eingabetaste. Daraufhin sollte die Nachricht `Lokales Verzeichnis jetzt C:\Documents and Settings\All Users\Documents\IBM\Client Access` angezeigt werden.
3. Geben Sie an der FTP-Bedienerführung `cd \mein_verzeichnis` ein. Hierbei steht *mein_verzeichnis* für ein auf kdc1.myco.com befindliches Verzeichnis.

4. Geben Sie an der FTP-Bedienerführung `put NASConfigsystema.bat` ein. Daraufhin sollte die Nachricht: `226 Übertragung abgeschlossen` (oder ähnlicher Wortlaut) angezeigt werden.
5. Geben Sie `quit` ein, um die FTP-Sitzung zu verlassen.

Stapeldatei auf kdc1.myco.com ausführen

1. Öffnen Sie auf dem Windows 2000-Server das Verzeichnis, in das die Stapeldatei übertragen wurde.
2. Lokalisieren Sie die Datei `NASConfigsystema.bat`, und führen Sie sie durch Doppelklicken aus.
3. Vergewissern Sie sich nach der Ausführung der Datei, dass der i5/OS-Principal zum Kerberos-Server hinzugefügt wurde. Führen Sie dazu die folgenden Schritte durch:
   a. Erweitern Sie auf dem Windows 2000-Server die Einträge **Verwaltungstools** → **Active Directory-Benutzer und -Computer** → **Benutzer**.
   b. Vergewissern Sie sich, dass das System i-Modell über ein Benutzerkonto verfügt, indem Sie die entsprechende Windows 2000-Domäne auswählen.

      Anmerkung: Diese Windows 2000-Domäne muss mit dem Namen des Standard-Realms übereinstimmen, den Sie bei der Konfiguration des Netzwerkauthentifizierungsservice angegeben haben.
   c. Suchen Sie in der angezeigten Benutzerliste **systema_1_krbsvr400**. Hierbei handelt es sich um das Benutzerkonto, das für den i5/OS-Principal-Namen generiert wurde.
   d. (Optional) Rufen Sie die Eigenschaften des Active Directory-Benutzers auf. Wählen Sie auf der Registerkarte **Konto** den Eintrag **Konto wird für Delegierungszwecke vertraut** aus.

      Anmerkung: Dieser optionale Schritt ermöglicht es Ihrem System, die Berechtigungsnachweise eines Benutzers an andere Systeme zu delegieren oder weiterzuleiten. Folglich kann der i5/OS-Service-Principal im Namen des Benutzers auf Services zuzugreifen, die sich auf mehreren Systemen befinden. Dies ist besonders in einem Netzwerk mit mehreren Ebenen von Vorteil.

Nachdem Sie den Service-Principal für System A zum Kerberos-Server hinzugefügt haben, können Sie nun ein Ausgangsverzeichnis für John Day erstellen.

Ausgangsverzeichnis für John Day auf System A erstellen

Sie müssen im Ausgangsverzeichnis (/home) ein Unterverzeichnis erstellen, in dem der Kerberos-Cache für Berechtigungsnachweise gespeichert werden kann.

Führen Sie folgende Schritte durch, um ein Ausgangsverzeichnis zu erstellen:

Geben Sie an der Bedienerführung Folgendes ein: `CRTDIR '/home/benutzerprofil'`. Hierbei steht `benutzerprofil` für den Namen Ihres i5/OS-Benutzerprofils. Beispiel: `CRTDIR '/home/JOHND'`.

Nachdem Sie nun das Ausgangsverzeichnis erstellt haben, können Sie die Konfiguration des Netzwerkauthentifizierungsservice überprüfen.

Konfiguration des Netzwerkauthentifizierungsservice auf System A testen

Nachdem Sie nun die Tasks zur Konfiguration des Netzwerkauthentifizierungsservice auf System A durchgeführt haben, müssen Sie überprüfen, ob Ihre Konfiguration fehlerfrei funktioniert. Hierzu können Sie ein Ticket-granting Ticket für den Principal-Namen von System A anfordern.

Führen Sie die folgenden Schritte durch, um die Konfiguration des Netzwerkauthentifizierungsservice zu testen:

Anmerkung: Vergewissern Sie sich, dass Sie ein Ausgangsverzeichnis für Ihr i5/OS-Benutzerprofil erstellt haben, bevor Sie diese Prozedur ausführen.

1. Geben Sie an einer Bedienerführung `QSH` ein, um den Qshell Interpreter zu starten.

2. Geben Sie `keytab list` ein, um eine Liste der Principals anzuzeigen, die in der Chiffrierschlüsseldatei registriert sind. In diesem Szenario sollte als Principal-Name für System A "krbsvr400/systema.myco.com@MYCO.COM" angezeigt werden.
3. Geben Sie `kinit -k krbsvr400/systema.myco.com@MYCO.COM` ein. Wenn dieser Befehl erfolgreich ausgeführt wird, werden vom Befehl kinit keine Fehler ausgegeben.
4. Geben Sie `klist` ein, um sicherzustellen, dass als Standard-Principal "krbsvr400/systema.myco.com@MYCO.COM" definiert ist.

Nachdem Sie die Konfiguration des Netzwerkauthentifizierungsservice getestet haben, können Sie nun eine EIM-Kennung für John Day erstellen.

EIM-Kennung für John Day erstellen

Nachdem Sie nun die einführenden Schritte zur Erstellung einer Basiskonfiguration für die Einzelanmeldung durchgeführt haben, können Sie damit beginnen, Daten zu dieser Konfiguration hinzuzufügen, um Ihre Einzelanmeldungstestumgebung zu vervollständigen.

Sie müssen die EIM-Kennung erstellen, die Sie im Planungsarbeitsblatt angegeben haben. In diesem Szenario steht die EIM-Kennung für einen Namen, der Sie (d. h. John Day) innerhalb Ihres Unternehmens eindeutig identifiziert.

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

1. Erweitern Sie im System i Navigator die Einträge für **System A** → **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung** → **MyCoEimDomain**.

   Anmerkung: Möglicherweise werden Sie aufgefordert, eine Verbindung zum Domänencontroller herzustellen. In diesem Fall wird das Dialogfenster **Verbindung zu EIM-Domänencontroller** angezeigt. Sie müssen eine Verbindung zur Domäne herstellen, um Aktionen in der Domäne ausführen zu können. Um eine Verbindung zum Domänencontroller herzustellen, müssen Sie die folgenden Informationen angeben und dann auf **OK** klicken:

   - **Benutzerart:** `Registrierter Name`
   - **Registrierter Name**: `cn=Administrator`
   - **Kennwort**: `mycopwd`

     Anmerkung: Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.
2. Klicken Sie mit der rechten Maustaste auf **Kennungen**, und wählen Sie **Neue Kennung** aus.
3. Geben Sie im Dialogfenster **Neue EIM-Kennung** im Feld **Kennung** einen Namen für die neue Kennung ein, und klicken Sie dann auf **OK**. Verwenden Sie z. B. den Namen John Day.

Nachdem Sie Ihre Kennung erstellt haben, können Sie Zuordnungen zur Kennung hinzufügen, um die Beziehung zwischen der Kennung und dem zugehörigen Kerberos-Principal und dem i5/OS-Benutzerprofil zu definieren.

EIM-Identitätsabgleiche testen

Sie müssen sicherstellen, dass die EIM-Abgleichsuchoperationen auf der Basis der konfigurierten Zuordnungen die richtigen Ergebnisse zurückgeben.

Um zu testen, ob die EIM-Abgleichoperationen fehlerfrei funktionieren, müssen Sie die folgenden Arbeitsschritte ausführen:

1. Erweitern Sie im System i Navigator die Einträge für **System A** → **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung** → **MyCoEimDomain**.

Anmerkung: Möglicherweise werden Sie aufgefordert, eine Verbindung zum Domänencontroller herzustellen. In diesem Fall wird das Dialogfenster **Verbindung zu EIM-Domänencontroller** angezeigt. Sie müssen eine Verbindung zur Domäne herstellen, um Aktionen in der Domäne ausführen zu können. Um eine Verbindung zum Domänencontroller herzustellen, müssen Sie die folgenden Informationen angeben und dann auf **OK** klicken:

- **Benutzerart:** `Registrierter Name`
- **Registrierter Name**: `cn=Administrator`
- **Kennwort**: `mycopwd`

Anmerkung: Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.

2. Klicken Sie mit der rechten Maustaste auf **MyCoEimDomain**, und wählen Sie **Abgleich testen** aus.
3. Geben Sie im Dialogfenster **Abgleich testen** die erforderlichen Informationen an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen:
   - **Quellenregister**: `MYCO.COM`
   - **Quellenbenutzer**: `jday`
   - **Zielregister**: `SYSTEMA.MYCO.COM`

   Anmerkung: Klicken Sie auf **Hilfe**, wenn Sie Hilfe für die Eingabe der erforderlichen Informationen in den einzelnen Feldern benötigen.

   Klicken Sie auf **Test** und dann auf **Schließen**.

Wenn Ihre EIM-Abgleiche korrekt konfiguriert sind, werden im Bereich **Gefundener Abgleich** der Seite die folgenden Ergebnisse angezeigt:

Für diese Felder	Siehe diese Resultate
Zielbenutzer	JOHND
Ursprung	EIM-Kennung: John Day

Wenn Sie Nachrichten bzw. Fehlernachrichten empfangen, die auf Probleme mit den Abgleichen oder der Übertragung hinweisen, lesen Sie Fehlerbehebung bei Enterprise Identity Mapping, um Lösungen für diese Probleme zu finden.

Nachdem Sie die EIM-Identitätsabgleiche getestet haben, können Sie nun System i Access für Windows-Anwendungen für die Benutzung der Kerberos-Authentifizierung konfigurieren.

System i Access für Windows-Anwendungen für die Verwendung der Kerberos-Authentifizierung konfigurieren

Bevor Sie den System i Navigator für den Zugriff auf Ihr System einsetzen können, müssen Sie eine Kerberos-Authentifizierung durchführen. Aus diesem Grund müssen Sie System i Access für Windows auf Ihrem PC so konfigurieren, dass die Kerberos-Authentifizierung verwendet werden kann.

Zur Konfiguration von System i Access für Windows-Anwendungen für die Kerberos-Authentifizierung müssen Sie die folgenden Arbeitsschritte ausführen:

Anmerkung: Jeder Ihrer Benutzer muss alle diese Schritte auf seinem eigenen PC durchführen.

1. Melden Sie sich bei der Windows 2000-Domäne an, indem Sie an Ihrem PC eine Anmeldung durchführen.
2. Klicken Sie im System i Navigator auf Ihrem PC mit der rechten Maustaste auf den Eintrag für **System A**, und wählen Sie dann **Eigenschaften** aus.

3. Wählen Sie auf der Seite **Verbindung** die Auswahl **Kerberos-Principal-Namen verwenden, keine Anforderung** aus. Daraufhin können System i Access für Windows-Verbindungen für die Authentifizierung den Namen des Kerberos-Principals und das zugehörige Kennwort verwenden.
4. Es erscheint eine Nachricht, die anzeigt, dass Sie alle Anwendungen, die gegenwärtig ausgeführt werden, schließen und erneut starten müssen, damit die Änderungen der Verbindungseinstellungen wirksam werden. Klicken Sie auf **OK**. Beenden Sie anschließend den System i Navigator, und starten Sie ihn dann erneut.

Nachdem die System i Access für Windows-Anwendungen nun so konfiguriert sind, dass die Kerberos-Authentifizierung verwendet wird, können Sie die Einzelanmeldungsumgebung überprüfen.

Konfiguration des Netzwerkauthentifizierungsservice und von EIM überprüfen

Sie haben die einzelnen Abschnitte der Konfiguration der Einzelanmeldung überprüft und sichergestellt, dass die gesamte Konfiguration vollständig ist. Jetzt müssen Sie überprüfen, ob EIM und der Netzwerkauthentifizierungsservice ordnungsgemäß konfiguriert wurden und die Einzelanmeldung erwartungsgemäß funktioniert.

Lassen Sie den Benutzer John Day die folgenden Schritte durchführen, um zu überprüfen, ob die Umgebung für die Einzelanmeldung ordnungsgemäß funktioniert:

1. Erweitern Sie im System i Navigator den Eintrag für **System A**, um eine Verbindung zu System A zu öffnen.
2. Drücken Sie F5, um die Anzeige zu aktualisieren.
3. Suchen Sie im rechten Fensterbereich in der Spalte **Name** nach `System A`, und überprüfen Sie, ob das i5/OS-Benutzerprofil von John Day (`JOHND`) als zugehöriger Eintrag in der Spalte **Angemeldeter Benutzer** angezeigt wird.

Der System i Navigator konnte mit Hilfe von EIM eine Zuordnung zwischen dem Kerberos-Principal jday und dem Benutzerprofil JOHND von System A herstellen, weil für die EIM-Kennung John Day entsprechende Zuordnungen definiert sind. Die Verbindung der System i Navigator-Sitzung für System A wird nun unter dem Namen JOHND hergestellt.

(Optional) Hinweise für die Konfigurationsnachbereitung

Nach Durchführung des Szenarios ist der registrierte Name (DN) für den LDAP-Administrator der einzige EIM-Benutzer, den Sie definiert haben und der von EIM verwendet werden kann.

Der registrierte Name des LDAP-Administrators, den Sie für den Systembenutzer auf System A angegeben haben, besitzt eine hohe Berechtigungsstufe für alle Daten auf dem Directory-Server. Daher möchten Sie möglicherweise einen oder mehrere registrierte Namen als zusätzliche Benutzer erstellen, deren EIM-Zugriffssteuerung für EIM-Daten besser an die geltenden Anforderungen angepasst und eingeschränkt ist. Wie viele EIM-Benutzer Sie zusätzlich definieren, hängt davon ab, welche Rolle in Ihren Sicherheitsrichtlinien die Trennung von Sicherheitsaufgaben und Sicherheitszuständigkeiten spielt. Normalerweise werden mindestens die beiden folgenden Arten von registrierten Namen erstellt:

- **Ein Benutzer mit EIM-Administratorrechten**

  Der registrierte Name des EIM-Administrators stellt die richtige Berechtigungsstufe für einen Administrator bereit, der für die Verwaltung der EIM-Domäne verantwortlich ist. Dieser registrierte Name für den EIM-Administrator kann verwendet werden, um eine Verbindung zum Domänencontroller herzustellen, wenn die Verwaltung der EIM-Domäne vollständig über den System i Navigator erfolgt.
- **Mindestens ein Benutzer, der die Zugriffssteuerung für alle folgenden Bereiche und Operationen besitzt**:
  - Kennungsadministrator
  - Registeradministrator
  - EIM-Abgleichoperation

Dieser Benutzer besitzt die richtige Zugriffssteuerungsstufe, die der Systembenutzer benötigt, der EIM-Operationen für das Betriebssystem ausführt.

Anmerkung: Wenn Sie diesen neuen registrierten Namen des Systembenutzers an Stelle des registrierten Namens des LDAP-Administrators verwenden wollen, müssen Sie die EIM-Konfigurationseigenschaften für jedes System ändern. In diesem Szenario müssen Sie die Eigenschaften der EIM-Konfiguration bei allen System i-Modellen ändern, die Sie einrichten.

Zugehörige Informationen

EIM-Konfigurationseigenschaften verwalten

Szenario: Einzelanmeldung für i5/OS aktivieren

In diesem Szenario wird dargestellt, wie der Netzwerkauthentifizierungsservice und EIM konfiguriert werden müssen, um in einem Unternehmen eine systemübergreifende Einzelanmeldungsumgebung zu erstellen. Dieses Szenario baut auf den Konzepten und Tasks auf, die im vorherigen Szenario dargestellt wurden, in dem die Erstellung einer einfachen Einzelanmeldungstestumgebung erläutert wurde.

Situation

Sie sind als Netzwerkadministrator für ein Unternehmen tätig. Ihre Aufgabe besteht darin, das Unternehmensnetzwerk sowie die Netzwerksicherheit für Ihr Unternehmen einschließlich der Auftragsannahmeabteilung zu verwalten. Sie überwachen die IT-Operationen für viele Mitarbeiter, die Kundenaufträge per Telefon entgegennehmen. Sie überwachen auch zwei andere Netzwerkadministratoren, die Ihnen bei der Verwaltung des Netzwerks helfen.

Die Mitarbeiter der Auftragsannahmeabteilung verwenden Windows 2000 und i5/OS. Sie benötigen mehrere Kennwörter, um auf die täglich benutzten Anwendungen zuzugreifen. Folglich verbringen Sie viel Zeit mit der Verwaltung und Behebung von Problemen im Zusammenhang mit Kennwörtern und Benutzeridentitäten. Sie setzen beispielsweise vergessene Kennwörter zurück.

Als Netzwerkadministrator des Unternehmens suchen Sie ständig nach Wegen, den Geschäftsablauf zu verbessern, angefangen bei der Auftragsannahmeabteilung. Sie wissen, dass die meisten Mitarbeiter dieselbe Art von Berechtigung benötigen, um auf die Anwendung zur Abfrage des Inventarstatus zugreifen zu können. Es erscheint Ihnen überflüssig und zeitaufwändig, einzelne Benutzerprofile und zahlreiche Kennwörter, die in dieser Situation erforderlich sind, zu verwalten. Darüber hinaus wissen Sie, dass es für alle Mitarbeiter von Vorteil wäre, wenn sie weniger Benutzer-IDs und Kennwörter verwenden müssten. Gehen Sie wie folgt vor:

- Vereinfachen Sie die Kennwortverwaltung für die Auftragsannahmeabteilung. Insbesondere geht es darum, den Benutzerzugriff auf die Anwendung, die von Ihren Mitarbeitern routinemäßig für Kundenaufträge verwendet wird, effizient zu verwalten.
- Reduzieren Sie die Verwendung mehrerer Benutzer-IDs und Kennwörter für die Mitarbeiter der Abteilung und die Netzwerkadministratoren. Sie möchten allerdings nicht, dass auf Ihrem System die gleichen Windows 2000-IDs und i5/OS-Benutzerprofile verwendet werden. Außerdem möchten Sie kein Kennwortcaching und keine Kennwortsynchronisation durchführen.

Sie wissen, dass i5/OS die Einzelanmeldung unterstützt. Diese Lösung bietet Ihren Benutzern die Möglichkeit, sich nur einmal anzumelden, um auf mehrere Anwendungen und Services, für die normalerweise verschiedene Benutzer-IDs und Kennwörter erforderlich sind, zugreifen zu können. Da die Benutzer zur Ausführung ihrer Arbeit weniger Benutzer-IDs und Kennwörter benötigen, müssen Sie auch weniger Kennwortprobleme lösen. Die Einzelanmeldung scheint eine ideale Lösung zu sein, da sie die Kennwortverwaltung auf folgende Weise vereinfacht:

- Für typische Benutzer, die dieselbe Berechtigung für eine Anwendung benötigen, können Sie Richtlinienzuordnungen erstellen. Beispiel: Die Mitarbeiter der Auftragsannahmeabteilung sollen in der Lage sein, sich einmal mit ihrem Windows-Benutzernamen und -Kennwort anzumelden und dann auf eine neue Anwendung für Inventarabfrage in der Produktionsabteilung zuzugreifen, ohne sich erneut

authentifizieren zu müssen. Dennoch möchten Sie sicherstellen, dass die Benutzer mit der richtigen Berechtigungsstufe auf die Anwendungen zugreifen können. Zur Erreichung dieses Ziels erstellen Sie eine Richtlinienzuordnung, mit der die Windows 2000-Benutzeridentitäten für diese Benutzergruppe einem einzigen i5/OS-Benutzerprofil zugeordnet werden, das über die erforderliche Berechtigungsstufe zur Ausführung der Anwendung für die Inventarabfrage verfügt. Da diese Anwendung nur Abfragen zulässt, in denen die Benutzer keine Daten ändern können, besteht für Sie keine Notwendigkeit einer detaillierten Prüfung. Daher können Sie sicher sein, dass die Verwendung einer Richtlinienzuordnung in dieser Situation Ihren Sicherheitsrichtlinien entspricht.

Sie erstellen eine Richtlinienzuordnung, um die Gruppe der Mitarbeiter der Auftragsannahmeabteilung, die ähnliche Berechtigungen benötigen, einem einzigen i5/OS-Benutzerprofil mit der erforderlichen Berechtigungsstufe für die Anwendung für die Inventarabfrage zuzuordnen. Die Benutzer profitieren davon, da sie sich ein Kennwort weniger merken und eine Anmeldung weniger durchführen müssen. Als Administrator profitieren Sie, da Sie für den Benutzerzugriff auf die Anwendung nur ein Benutzerprofil statt mehrerer Benutzerprofile für jedes Mitglied der Gruppe verwalten müssen.

- Für jeden Ihrer Netzwerkadministratoren, die Benutzerprofile mit Sonderberechtigungen, wie z. B. *ALLOBJ und *SECADM, verwenden, können Sie Kennungszuordnungen erstellen. Beispielsweise sollten alle Benutzeridentitäten eines Netzwerkadministrators untereinander genau und einzeln zugeordnet werden, da der Administrator eine hohe Berechtigungsstufe besitzt.

  Auf der Basis der Sicherheitsrichtlinien des Unternehmens erstellen Sie Kennungszuordnungen, um die Windows-Identität jedes Netzwerkadministrators ausdrücklich seinem i5/OS-Benutzerprofil zuzuordnen. Sie können die Aktivität des Administrators auf Grund des Eins-zu-eins-Abgleichs, der von den Kennungszuordnungen bereitgestellt wird, einfacher überwachen und protokollieren. Beispielsweise können Sie die Jobs und Objekte, die auf dem System ausgeführt werden, für eine bestimmte Benutzeridentität überwachen. Ihr Netzwerkadministrator profitiert davon, da er sich ein Kennwort weniger merken und eine Anmeldung weniger durchführen muss. Als Netzwerkadministrator profitieren Sie davon, weil Sie in der Lage sind, die Beziehungen zwischen den Benutzeridentitäten der Administratoren genau zu steuern.

Dieses Szenario hat folgende Vorteile:

- Vereinfachung des Authentifizierungsprozesses für Benutzer.
- Vereinfachung der Verwaltung des Zugriffs auf Anwendungen.
- Reduzierung des Systemaufwands für die Verwaltung des Zugriffs auf Server im Netzwerk.
- Reduzierung des Sicherheitsrisikos hinsichtlich des Kennwortdiebstahls.
- Vermeidung von Mehrfachanmeldungen.
- Vereinfachung der Verwaltung von Benutzeridentitäten im Netzwerk.

Ziele

In diesem Szenario sind Sie der Administrator von MyCo, Inc., der die Einzelanmeldung für die Benutzer in der Auftragsannahmeabteilung aktivieren möchte.

Dieses Szenario hat die folgenden Ziele:

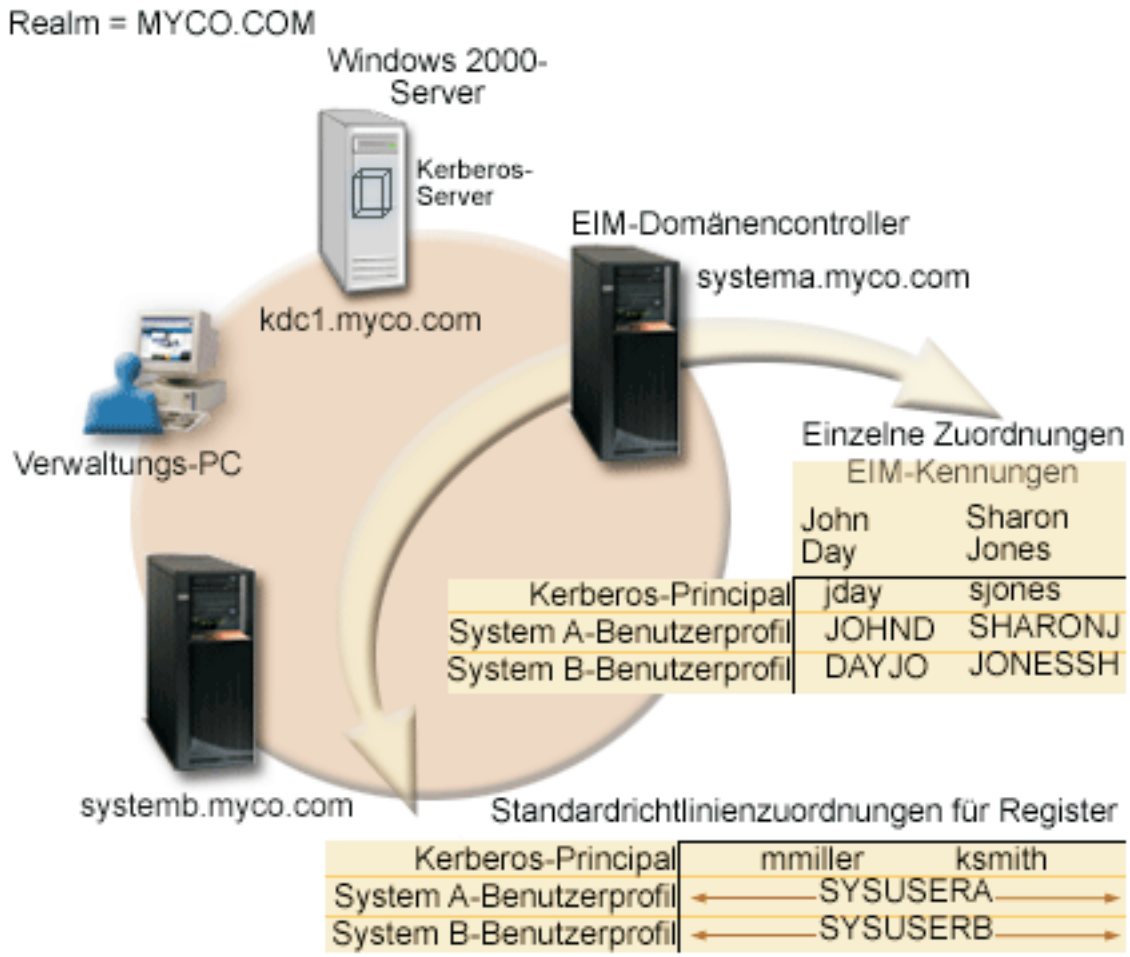
- System A und System B müssen zum Realm MYCO.COM gehören, um die Benutzer und Services, die zur Einzelanmeldungsumgebung gehören, authentifizieren zu können. Wenn Sie die Systeme für die Verwendung von Ker-
  beros aktivieren möchten, müssen System A und System B für den Netzwerkauthentifizierungsservice konfiguriert werden.
- IBM Directory Server for System i (LDAP) auf System A muss als Domänencontroller für die neue EIM-Domäne fungieren.

  Anmerkung: Unter Domänen wird beschrieben, wie zwei verschiedene Domänentypen, eine EIM-Domäne und eine Windows 2000-Domäne, in der Einzelanmeldungsumgebung verwendet werden können.

- Alle Benutzeridentitäten im Kerberos-Register müssen einem einzigen i5/OS-Benutzerprofil zugeordnet werden können. Das Benutzerprofil muss die erforderliche Berechtigung für den Benutzerzugriff auf die Anwendung für die Inventarabfrage besitzen.
- Entsprechend den Sicherheitsrichtlinien müssen zwei Administratoren (John Day und Sharon Jones), die auch über Benutzeridentitäten im Kerberos-Register verfügen, Kennungszuordnungen besitzen, um diese Identitäten ihren i5/OS-Benutzerprofilen mit der Sonderberechtigung *SECADM zuzuordnen. Diese Eins-zu-eins-Abgleiche ermöglichen Ihnen, die Jobs und Objekte, die auf dem System ausgeführt werden, für diese Benutzeridentitäten genau zu überwachen.
- Ein Kerberos-Service-Principal muss verwendet werden, um die Benutzer bei den System i Access für Windows-Anwendungen (einschließlich System i Navigator) zu authentifizieren.

Details

Die folgende Abbildung veranschaulicht die Netzwerkumgebung für dieses Szenario.



Die Abbildung veranschaulicht die folgenden Punkte, die für dieses Szenario relevant sind.

EIM-Domänendaten, die für das Unternehmen definiert sind

- Drei Registerdefinitionsnamen:
  - Der Registerdefinitionsname MYCO.COM für das Register des Windows 2000-Servers. Sie definieren diesen Namen, wenn Sie den EIM-Konfigurationsassistenten auf System A ausführen.

  - Der Registerdefinitionsname SYSTEMA.MYCO.COM für das i5/OS-Register auf System A. Sie definieren diesen Namen, wenn Sie den EIM-Konfigurationsassistenten auf System A ausführen.
  - Der Registerdefinitionsname SYSTEMB.MYCO.COM für das i5/OS-Register auf System B. Sie definieren diesen Namen, wenn Sie den EIM-Konfigurationsassistenten auf System B ausführen.
- Zwei Standardrichtlinienzuordnungen für Register:

  Anmerkung: EIM-Suchoperationen bewirken, dass Kennungszuordnungen die höchste Priorität zugeordnet wird. Wenn eine Benutzeridentität als Quelle in einer Richtlinienzuordnung und in einer Kennungszuordnung definiert ist, wird die Benutzeridentität nur über die Kennungszuordnung zugeordnet. In diesem Szenario verfügen zwei Netzwerkadministratoren, John Day und Sharon Jones, über Benutzeridentitäten im Register MYCO.COM, das die Quelle der Standardrichtlinienzuordnungen für Register ist. Diese Administratoren besitzen jedoch, wie unten dargestellt, auch Kennungszuordnungen für ihre Benutzeridentitäten im Register MYCO.COM. Die Kennungszuordnungen stellen sicher, dass die Benutzeridentitäten im Register MYCO.COM nicht über die Richtlinienzuordnungen abgeglichen werden. Die Kennungszuordnungen stellen hingegen sicher, dass ihre Benutzeridentitäten im Register MYCO.COM einzeln anderen spezifischen einzelnen Benutzeridentitäten zugeordnet werden.

  - Eine Standardrichtlinienzuordnung für Register ordnet alle Benutzeridentitäten im Register MYCO-.COM des Windows 2000-Servers einem einzigen i5/OS-Benutzerprofil mit dem Namen SYSUSERA im Register SYSTEMA.MYCO.COM auf System A zu. Im vorliegenden Szenario stellen mmiller und ksmith zwei dieser Benutzeridentitäten dar.
  - Eine Standardrichtlinienzuordnung für Register ordnet alle Benutzeridentitäten im Register MYCO-.COM des Windows 2000-Servers einem einzigen i5/OS-Benutzerprofil mit dem Namen SYSUSERB im Register SYSTEMB.MYCO.COM auf System B zu. Im vorliegenden Szenario stellen mmiller und ksmith zwei dieser Benutzeridentitäten dar.
- Zwei EIM-Kennungen mit den Namen John Day und Sharon Jones zur Bezeichnung der zwei Netzwerkadministratoren im Unternehmen, die diese Namen haben.
- Für die EIM-Kennung John Day sind die folgenden Kennungszuordnungen definiert:
  - Eine Quellenzuordnung für die Benutzeridentität jday, bei der es sich um einen Kerberos-Principal im Register des Windows 2000-Servers handelt.
  - Eine Zielzuordnung für die Benutzeridentität JOHND, bei der es sich um ein Benutzerprofil im i5/OS-Register auf System A handelt.
  - Eine Zielzuordnung für die Benutzeridentität DAYJO, bei der es sich um ein Benutzerprofil im i5/OS-Register auf System B handelt.
- Für die EIM-Kennung Sharon Jones sind die folgenden Kennungszuordnungen definiert:
  - Eine Quellenzuordnung für die Benutzeridentität sjones, bei der es sich um einen Kerberos-Principal im Register des Windows 2000-Servers handelt.
  - Eine Zielzuordnung für die Benutzeridentität SHARONJ, bei der es sich um ein Benutzerprofil im i5/OS-Register auf System A handelt.
  - Eine Zielzuordnung für die Benutzeridentität JONESSH, bei der es sich um ein Benutzerprofil im i5/OS-Register auf System B handelt.

Windows 2000-Server

- Fungiert als Kerberos-Server (`kdc1.myco.com`) für das Netzwerk und wird auch als KDC (Key Distribution Center) bezeichnet.
- Der Standard-Realm für den Kerberos-Server ist `MYCO.COM`.
- Alle Microsoft Windows Active Directory-Benutzer, die keine Kennungszuordnungen besitzen, werden auf allen System i-Modellen einem einzigen i5/OS-Benutzerprofil zugeordnet.

System A

- Verwendet i5/OS ab Version 5 Release 4 (V5R4) mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS Host-Server (5761-SS1 Option 12)
  - Qshell Interpreter (5761-SS1 Option 30)
  - System i Access für Windows (5761-XE1)

Anmerkung: Sie können dieses Szenario mit einem Server implementieren, der unter i5/OS V5R3 arbeitet. Allerdings können einige der Konfigurationsschritte auf Grund der Erweiterungen in i5/OS ab V5R4 leicht abweichen. 5722 ist der Produktcode für i5/OS-Optionen und -Produkte mit einer Version vor V6R1.

- Der Directory-Server auf System A wird als EIM-Domänencontroller für die neue EIM-Domäne MyCoEimDomain konfiguriert.
- Nutzt die EIM-Domäne MyCoEIMDomain.
- Der Name des Service-Principals lautet `krbsvr400/systema.myco.com@MYCO.COM`.
- Der vollständig qualifizierte Hostname lautet `systema.myco.com`. Dieser Name ist in einem einzigen Domain Name System (DNS) registriert, auf das alle PCs und Server im Netzwerk zeigen.
- In Ausgangsverzeichnissen auf System A sind die Caches für Kerberos-Berechtigungsnachweise für i5/OS-Benutzerprofile gespeichert.

System B

- Verwendet i5/OS ab Version 5 Release 4 (V5R4) mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS Host-Server (5761-SS1 Option 12)
  - Qshell Interpreter (5761-SS1 Option 30)
  - System i Access für Windows (5761-XE1)
- Hat den vollständig qualifizierten Hostnamen `systemb.myco.com`. Dieser Name ist in einem einzigen Domain Name System (DNS) registriert, auf das alle PCs und Server im Netzwerk zeigen.
- Der Principal-Name für System B lautet `krbsvr400/systemb.myco.com@MYCO.COM`.
- Nutzt die EIM-Domäne MyCoEIMDomain.
- In Ausgangsverzeichnissen auf System B sind die Caches für Kerberos-Berechtigungsnachweise für i5/OS-Benutzerprofile gespeichert.

Verwaltungs-PC

- Wird unter dem Betriebssystem Microsoft Windows 2000 ausgeführt.
- Verwendet i5/OS ab V5R4 System i Access für Windows (5761-XE1).
- Verwendet den System i Navigator mit den folgenden installierten Unterkomponenten:
  - Netzwerk
  - Sicherheit
  - Benutzer und Gruppen
- Fungiert als primäres Anmeldesystem für den Administrator.
- Konfiguriert als Bestandteil des Realms MYCO.COM (Windows-Domäne).

Voraussetzungen und Annahmen

Zur erfolgreichen Durchführung der in diesem Szenario beschriebenen Schritte müssen die folgenden Voraussetzungen und Annahmen erfüllt sein:

1. Alle Systemvoraussetzungen einschließlich der Installation der Software und des Betriebssystems wurden überprüft.

Führen Sie folgende Schritte durch, um festzustellen, ob die erforderlichen Lizenzprogramme installiert wurden:

a. Erweitern Sie im System i Navigator die Einträge für **Ihr System** → **Konfiguration und Service** → **Software** → **Installierte Produkte**.
b. Vergewissern Sie sich, dass alle erforderlichen Lizenzprogramme installiert sind.

2. Die erforderliche Hardwareplanung und -konfiguration wurde durchgeführt.
3. TCP/IP und die Basissystemsicherheit wurden auf jedem System konfiguriert und getestet.
4. Der Directory-Server und EIM sollten zuvor noch nicht auf System A konfiguriert worden sein.

   Anmerkung: Die Anweisungen in diesem Szenario basieren auf der Annahme, dass der Directory-Server zuvor noch nicht auf System A konfiguriert wurde. Wurde dieses Produkt bereits konfiguriert, können Sie diese Anweisungen trotzdem mit geringen Änderungen anwenden. Diese Änderungen sind an den entsprechenden Stellen in den Konfigurationsschritten vermerkt.
5. Für die Auflösung der Hostnamen im Netzwerk wird ein einziger DNS-Server verwendet. Es werden keine Hosttabellen für die Auflösung der Hostnamen verwendet.

   Anmerkung: Die Verwendung von Hosttabellen kann bei der Kerberos-Authentifizierung zu Fehlern bei der Namensauflösung oder zu anderen Problemen führen.

Konfigurationsschritte

Anmerkung: Sie sollten sich mit den im Zusammenhang mit der Einzelanmeldung verwendeten Konzepten, d. h. mit dem Netzwerkauthentifizierungsservice und EIM (Enterprise Identity Mapping), eingehend vertraut machen, bevor Sie dieses Szenario durcharbeiten. Wenn Sie bereit sind, mit diesem Szenario fortzufahren, sollten Sie die folgenden Schritte durchführen:

Zugehörige Tasks

„Einzelanmeldung konfigurieren" auf Seite 87
Zum Konfigurieren einer Einzelanmeldungsumgebung müssen Sie eine kompatible Authentifizierungsmethode verwenden und EIM zum Erstellen und Verwalten der Benutzerprofile und Identitätsabgleiche benutzen.

Zugehörige Informationen

Hinweise zur Auflösung von Hostnamen

Enterprise Identity Mapping - Konzepte

EIM-Zuordnungen

Hinweise zur Auflösung von Hostnamen

Planungsarbeitsblätter ausfüllen

Die folgenden Planungsarbeitsblätter wurden auf der Basis der allgemeinen Planungsarbeitsblätter für die Einzelanmeldung an dieses Szenario angepasst.

Diese Planungsarbeitsblätter veranschaulichen die Informationen, die Sie zusammenstellen, sowie die Entscheidungen, die Sie treffen müssen, um die Einzelanmeldungsimplementierung vorzubereiten, die im vorliegenden Szenario beschrieben wird. Um eine erfolgreiche Implementierung sicherzustellen, sollten Sie für alle vorausgesetzten Elemente im Arbeitsblatt die Antwort "Ja" geben können. Außerdem sollten Sie alle Informationen, die zur Fertigstellung der Arbeitsblätter erforderlich sind, aufzeichnen, bevor Sie Konfigurationsaufgaben ausführen.

Anmerkung: Sie müssen mit den Konzepten im Zusammenhang mit der Einzelanmeldung, wie z. B. dem Netzwerkauthentifizierungsservice und EIM (Enterprise Identity Mapping), vertraut sein,

um dieses Szenario implementieren zu können.

Tabelle 3. Arbeitsblatt für die Einzelanmeldungsvoraussetzungen

Arbeitsblatt für Voraussetzungen	**Antworten**
Arbeitet Ihr System mit i5/OS ab V5R4?	Ja
Sind die folgenden Optionen und Lizenzprogramme auf System A und System B installiert? • i5/OS Host-Server (5761-SS1 Option 12) • Qshell Interpreter (5761-SS1 Option 30) • System i Access für Windows (5761-XE1) **Anmerkung:** 5722 ist der Produktcode für i5/OS-Optionen und -Produkte mit einer Version vor V6R1.	Ja
Ist eine Anwendung installiert, die auf allen PCs, die sich in der Einzelanmeldungsumgebung befinden werden, für die Einzelanmeldung aktiviert ist? **Anmerkung:** In diesem Szenario wurde auf allen teilnehmenden PCs System i Access für Windows (5761-XE1) installiert.	Ja
Ist der System i Navigator auf dem Administrator-PC installiert? • Ist die Unterkomponente ″Netzwerk″ des System i Navigator auf dem PC, der für die Verwaltung der Einzelanmeldung verwendet wird, installiert? • Ist die Unterkomponente ″Sicherheit″ des System i Navigator auf dem PC, der für die Verwaltung der Einzelanmeldung verwendet wird, installiert? • Ist die Unterkomponente ″Benutzer und Gruppen″ des System i Navigator auf dem PC, der für die Verwaltung der Einzelanmeldung verwendet wird, installiert?	Ja
Ist das neueste IBM System i Access für Windows-Service-Pack installiert? Informationen zum neuesten Service-Pack finden Sie auf der Webseite für System i Access .	Ja
Besitzt der Administrator für die Einzelanmeldung die Sonderberechtigungen *SECADM, *ALLOBJ und *IOSYSCFG?	Ja
Fungiert eines der folgenden Systeme als Kerberos-Server (auch als KDC bezeichnet)? Wenn ja, geben Sie an, um welches System es sich handelt. 1. Microsoft Windows 2000-Server **Anmerkung:** Microsoft Windows 2000-Server verwendet als Standardsicherheitsmechanismus die Kerberos-Authentifizierung. 2. Windows (R) Server 2003 3. i5/OS PASE (ab V5R3) 4. AIX-Server 5. z/OS	Ja, Windows 2000-Server
Sind alle PCs Ihres Netzwerks in einer Windows 2000-Domäne konfiguriert?	Ja
Wurden die neuesten PTFs (vorläufigen Programmkorrekturen) angelegt?	Ja
Beträgt die Abweichung zwischen der Systemzeit des System i-Modells und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung größer, lesen Sie die Informationen in Systemzeiten synchronisieren.	Ja

Tabelle 3. Arbeitsblatt für die Einzelanmeldungsvoraussetzungen (Forts.)

Arbeitsblatt für Voraussetzungen	Antworten
Arbeiten Sie beim Kerberos-Server mit i5/OS PASE?	Auf dem System muss IBM Network Authentication Enablement for i5/OS (5761-NAE) installiert sein.

Sie benötigen diese Informationen, um EIM und den Netzwerkauthentifizierungsservice auf System A zu konfigurieren.

Tabelle 4. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung für System i A

Planungsarbeitsblatt für die Konfiguration von System A	Antworten
Verwenden Sie die folgenden Informationen, um den EIM-Konfigurationsassistenten auszuführen. Die Informationen in diesem Arbeitsblatt korrelieren mit den Informationen, die Sie zur Angabe auf den einzelnen Seiten im Assistenten benötigen:	
Wie möchten Sie EIM auf Ihrem System konfigurieren? • System zu einer vorhandenen Domäne hinzufügen • Neue Domäne erstellen und System hinzufügen	Neue Domäne erstellen und System hinzufügen.
Wo möchten Sie die EIM-Domäne konfigurieren?	Auf dem lokalen Directory-Server **Anmerkung:** Bei dieser Auswahl wird der Directory-Server auf demselben System konfiguriert, auf dem Sie gegenwärtig EIM konfigurieren.
Möchten Sie den Netzwerkauthentifizierungsservice konfigurieren? **Anmerkung:** Sie müssen den Netzwerkauthentifizierungsservice konfigurieren, um die Einzelanmeldung konfigurieren zu können.	Ja
Der Assistent für den Netzwerkauthentifizierungsservice wird über den EIM-Konfigurationsassistenten gestartet. Verwenden Sie die folgenden Informationen, um den Assistenten für den Netzwerkauthentifizierungsservice auszuführen.	
Wie lautet der Name des Kerberos-Standard-Realms, zu dem Ihr System i-Modell gehören soll? **Anmerkung:** Eine Windows 2000-Domäne ist mit einem Kerberos-Realm vergleichbar. Microsoft Windows Active Directory verwendet die Kerberos-Authentifizierung als Standardsicherheitsmechanismus.	`MYCO.COM`
Verwenden Sie Microsoft Active Directory?	Ja
Wie heißt der Kerberos-Server, der auch als KDC (Key Distribution Center) bezeichnet wird, für diesen Kerberos-Standard-Realm? An welchem Port ist der Kerberos-Server empfangsbereit?	**KDC:** `kdc1.myco.com` **Port:** `88` **Anmerkung:** Dies ist der Standardport für den Kerberos-Server.
Möchten Sie einen Kennwortserver für diesen Standard-Realm konfigurieren? Wenn ja, beantworten Sie die folgenden Fragen: Wie lautet der Name des Kennwortservers für diesen Kerberos-Server? An welchem Port ist der Kennwortserver empfangsbereit?	Ja **Kennwortserver:** `kdc1.myco.com` **Port:** `464` **Anmerkung:** Dies ist der Standardport für den Kennwortserver.

Tabelle 4. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung für System i A (Forts.)

Planungsarbeitsblatt für die Konfiguration von System A	**Antworten**
Für welche Services sollen Chiffrierschlüsseleinträge erstellt werden? • i5/OS-Kerberos-Authentifizierung • LDAP • IBM HTTP-Server für i5/OS • i5/OS NetServer • NFS-Server (Network File System)	i5/OS-Kerberos-Authentifizierung
Wie lautet das Kennwort für Ihre(n) Service-Principal(s)?	`systema123` **Anmerkung:** Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.
Möchten Sie eine Stapeldatei erstellen, um das Hinzufügen der Service-Principals für System A zum Kerberos-Register zu automatisieren?	Ja
Möchten Sie für die i5/OS-Service-Principals in der Stapeldatei Kennwörter hinzufügen?	Ja
Wenn Sie den Assistenten für den Netzwerkauthentifizierungsservice verlassen, gelangen Sie in den EIM-Konfigurationsassistenten zurück. Verwenden Sie die folgenden Informationen, um den EIM-Konfigurationsassistenten auszuführen:	
Geben Sie Benutzerinformationen an, die der Assistent bei der Konfiguration des Directory-Servers verwenden soll. Dies ist der Benutzer der Verbindung. Sie müssen die Portnummer, den registrierten Namen (Distinguished Name, DN) des Administrators und ein Kennwort für den Administrator angeben. **Anmerkung:** Geben Sie den registrierten Namen und das Kennwort des LDAP-Administrators an, um sicherzustellen, dass der Assistent eine ausreichende Berechtigung zur Verwaltung der EIM-Domäne und der darin enthaltenen Objekte besitzt.	**Port:** `389` **Registrierter Name:** `cn=Administrator` **Kennwort:** `mycopwd` **Anmerkung:** Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.
Wie lautet der Name der EIM-Domäne, die Sie erstellen möchten?	`MyCoEimDomain`
Möchten Sie einen übergeordneten registrierten Namen für die EIM-Domäne angeben?	Nein
Welche Benutzerregister möchten Sie zur EIM-Domäne hinzufügen?	Lokales i5/OS--SYSTEMA.MYCO.COM Kerberos--KDC1.MYCO.COM **Anmerkung:** Sie dürfen **Bei Kerberos-Benutzeridentitäten muss die Groß-/Kleinschreibung beachtet werden** nicht auswählen, wenn sie vom Assistenten angeboten wird.
Welchen EIM-Benutzer soll System A bei der Ausführung von EIM-Operationen verwenden? Dies ist der Systembenutzer. **Anmerkung:** Wenn Sie den Directory-Server nicht vor der Konfiguration der Einzelanmeldung konfiguriert haben, können Sie als registrierten Namen für den Systembenutzer nur die Kombination aus dem registrierten Namen und dem Kennwort des LDAP-Administrators bereitstellen.	**Benutzerart:** `Registrierter Name` **Registrierter Name:** `cn=Administrator` **Kennwort:** `mycopwd` **Anmerkung:** Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.

Sie benötigen diese Informationen, damit System B die EIM-Domäne nutzen kann und Sie den Netzwerkauthentifizierungsservice auf System B konfigurieren können.

Tabelle 5. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung für System B

Planungsarbeitsblatt für die Konfiguration von System B	**Antworten**
Verwenden Sie die folgenden Informationen, um den EIM-Konfigurationsassistenten für System B auszuführen:	
Wie möchten Sie EIM auf Ihrem System konfigurieren?	System zu einer vorhandenen Domäne hinzufügen
Möchten Sie den Netzwerkauthentifizierungsservice konfigurieren? **Anmerkung:** Sie müssen den Netzwerkauthentifizierungsservice konfigurieren, um die Einzelanmeldung konfigurieren zu können.	Ja
Der Assistent für den Netzwerkauthentifizierungsservice wird über den EIM-Konfigurationsassistenten gestartet. Verwenden Sie die folgenden Informationen, um den Assistenten für den Netzwerkauthentifizierungsservice auszuführen: **Anmerkung:** Der Assistent für den Netzwerkauthentifizierungsservice kann unabhängig vom EIM-Konfigurationsassistenten gestartet werden.	
Wie lautet der Name des Kerberos-Standard-Realms, zu dem Ihr System i-Modell gehören soll? **Anmerkung:** Eine Windows 2000-Domäne ist mit einem Kerberos-Realm vergleichbar. Microsoft Active Directory verwendet als Sicherheitsmechanismus die Kerberos-Authentifizierung.	`MYCO.COM`
Verwenden Sie Microsoft Active Directory?	Ja
Welcher Kerberos-Server wird für diesen Kerberos-Standard-Realm verwendet? An welchem Port ist der Kerberos-Server empfangsbereit?	**KDC:** `kdc1.myco.com` **Port:** `88` **Anmerkung:** Dies ist der Standardport für den Kerberos-Server.
Möchten Sie einen Kennwortserver für diesen Standard-Realm konfigurieren? Wenn ja, beantworten Sie die folgenden Fragen: Wie lautet der Name des Kennwortservers für diesen Kerberos-Server? An welchem Port ist der Kennwortserver empfangsbereit?	Ja **Kennwortserver:** `kdc1.myco.com` **Port:** `464` **Anmerkung:** Dies ist der Standardport für den Kennwortserver.
Für welche Services sollen Chiffrierschlüsseleinträge erstellt werden? • i5/OS-Kerberos-Authentifizierung • LDAP • IBM HTTP-Server für i5/OS • i5/OS NetServer	i5/OS-Kerberos-Authentifizierung
Wie lautet das Kennwort für Ihre i5/OS-Service-Principals?	systemb123 **Anmerkung:** Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.
Möchten Sie eine Stapeldatei erstellen, um das Hinzufügen der Service-Principals für System B zum Kerberos-Register zu automatisieren?	Ja
Möchten Sie für die i5/OS-Service-Principals in der Stapeldatei Kennwörter hinzufügen?	Ja
Wenn Sie den Assistenten für den Netzwerkauthentifizierungsservice verlassen, gelangen Sie in den EIM-Konfigurationsassistenten zurück. Verwenden Sie die folgenden Informationen, um den EIM-Konfigurationsassistenten für System B auszuführen:	

Tabelle 5. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung für System B (Forts.)

Planungsarbeitsblatt für die Konfiguration von System B	**Antworten**
Wie lautet der Name des EIM-Domänencontrollers für die EIM-Domäne, die Sie dem System hinzufügen möchten?	systema.myco.com
Möchten Sie die Verbindung mit SSL oder TLS sichern?	Nein
An welchem Port ist der EIM-Domänencontroller empfangsbereit?	389
Über welchen Benutzer möchten Sie eine Verbindung zum Domänencontroller herstellen? Dies ist der Benutzer der Verbindung. **Anmerkung:** Geben Sie den registrierten Namen und das Kennwort des LDAP-Administrators an, um sicherzustellen, dass der Assistent eine ausreichende Berechtigung zur Verwaltung der EIM-Domäne und der darin enthaltenen Objekte besitzt.	**Benutzerart:** `Registrierter Name und Kennwort` **Registrierter Name:** `cn=Administrator` **Kennwort:** `mycopwd` **Anmerkung:** Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.
Wie lautet der Name der EIM-Domäne, die Sie dem System hinzufügen möchten?	`MyCoEimDomain`
Möchten Sie einen übergeordneten registrierten Namen für die EIM-Domäne angeben?	Nein
Wie lautet der Name des Benutzerregisters, das Sie zur EIM-Domäne hinzufügen möchten?	Lokales i5/OS--SYSTEMB.MYCO.COM
Welchen EIM-Benutzer soll System B bei der Ausführung von EIM-Operationen verwenden? Dies ist der Systembenutzer. **Anmerkung:** In einer früheren Phase dieses Szenarios haben Sie den EIM-Konfigurationsassistenten verwendet, um den Directory-Server auf System A zu konfigurieren. Auf diese Weise haben Sie einen registrierten Namen und ein Kennwort für den LDAP-Administrator erstellt. Dies ist der einzige registrierte Name, der für den Directory-Server definiert ist. Daher müssen Sie diesen registrierten Namen und das Kennwort hier angeben.	**Benutzerart:** `Registrierter Name und Kennwort` **Registrierter Name:** `cn=Administrator` **Kennwort:** `mycopwd` **Anmerkung:** Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.

Tabelle 6. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung - Benutzerprofile

Name des i5/OS-Benutzerprofils	**Kennwort ist angegeben**	**Sonderberechtigung (Berechtigungsklasse)**	**System**
SYSUSERA	Nein	Benutzer	System A
SYSUSERB	Nein	Benutzer	System B

Tabelle 7. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung - EIM-Domänendaten

Name der Kennung	**Benutzerregister**	**Benutzeridentität**	**Zuordnungsart**	**Beschreibung der Kennung**
John Day	MYCO.COM	jday	Quelle	Benutzeridentität für Kerberos-Anmeldung (Windows 2000)
John Day	SYSTEMA.MYCO.COM	JOHND	Ziel	i5/OS-Benutzerprofil auf System A
John Day	SYSTEMB.MYCO.COM	DAYJO	Ziel	i5/OS-Benutzerprofil auf System B

Tabelle 7. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung - EIM-Domänendaten (Forts.)

Name der Kennung	Benutzerregister	Benutzeridentität	Zuordnungsart	Beschreibung der Kennung
Sharon Jones	MYCO.COM	sjones	Quelle	Benutzeridentität für Kerberos-Anmeldung (Windows 2000)
Sharon Jones	SYSTEMA.MYCO.COM	SHARONJ	Ziel	i5/OS-Benutzerprofil auf System A
Sharon Jones	SYSTEMB.MYCO.COM	JONESSH	Ziel	i5/OS-Benutzerprofil auf System B

Tabelle 8. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung - EIM-Domänendaten - Richtlinienzuordnungen

Art der Richtlinienzuordnung	Benutzerregister (Quelle)	Benutzerregister (Ziel)	Benutzeridentität	Beschreibung
Standardregister	MYCO.COM	SYSTEMA.MYCO.COM	SYSUSERA	Ordnet authentifizierte Kerberos-Benutzer dem entsprechenden i5/OS-Benutzerprofil zu.
Standardregister	MYCO.COM	SYSTEMB.MYCO.COM	SYSUSERB	Ordnet authentifizierte Kerberos-Benutzer dem entsprechenden i5/OS-Benutzerprofil zu.

Zugehörige Informationen

Enterprise Identity Mapping - Konzepte

Basiskonfiguration für die Einzelanmeldung für System A erstellen

Der EIM-Konfigurationsassistent hilft Ihnen bei der Erstellung einer EIM-Basiskonfiguration und ruft außerdem den Assistenten für den Netzwerkauthentifizierungsservice auf, damit Sie eine Basiskonfiguration des Netzwerkauthentifizierungsservice erstellen können.

Anmerkung: Die Anweisungen in diesem Szenario basieren auf der Annahme, dass IBM Tivoli Directory Server for i5/OS zuvor noch nicht auf System A konfiguriert wurde. Wurde dieses Produkt bereits konfiguriert, können Sie diese Anweisungen trotzdem mit geringen Änderungen anwenden. Diese Änderungen sind an den entsprechenden Stellen in den Konfigurationsschritten vermerkt.

Verwenden Sie die Informationen in den Arbeitsblättern, um EIM und den Netzwerkauthentifizierungsservice auf System A zu konfigurieren. Nach Ausführung dieses Arbeitsschrittes sind die folgenden Tasks abgeschlossen:

- Erstellen einer neuen EIM-Domäne.
- Konfigurieren des Directory-Servers als EIM-Domänencontroller auf System A.
- Konfigurieren des Netzwerkauthentifizierungsservice.
- Erstellen von EIM-Registerdefinitionen für das i5/OS- und das Kerberos-Register auf System A.

- Konfigurieren von System A zur Nutzung der EIM-Domäne.
  1. Erweitern Sie im System i Navigator die Einträge für **System A → Netzwerk → Enterprise Identity Mapping**.
  2. Klicken Sie mit der rechten Maustaste auf **Konfiguration**, und wählen Sie **Konfigurieren** aus, um den EIM-Konfigurationsassistenten zu starten.
  3. Wählen Sie auf der **Begrüßungsseite** die Auswahl **Neue Domäne erstellen und System hinzufügen**. Klicken Sie auf **Weiter**.
  4. Wählen Sie auf der Seite **Position der EIM-Domäne angeben** die Auswahl **Auf dem lokalen Directory-Server** aus. Klicken Sie auf **Weiter**.
  5. Führen Sie die folgenden Schritte durch, um den Netzwerkauthentifizierungsservice zu konfigurieren:
     a. Wählen Sie auf der Seite **Netzwerkauthentifizierungsservice konfigurieren** die Auswahl **Ja** aus.

        Anmerkung: Daraufhin wird der Assistent für den Netzwerkauthentifizierungsservice gestartet. Mit diesem Assistenten können Sie verschiedene i5/OS-Schnittstellen und -Services zur Nutzung des Kerberos-Realms konfigurieren.

     b. Geben Sie auf der Seite **Realm-Informationen angeben** im Feld **Standard-Realm** den Wert `MYCO.COM` ein, und wählen Sie **Microsoft Active Directory wird für Kerberos-Authentifizierung verwendet** aus. Klicken Sie auf **Weiter**.
     c. Geben Sie auf der Seite **KDC-Informationen angeben** im Feld **KDC** den Wert `kdc1.myco.com` als Namen des Kerberos-Servers und im Feld **Port** den Wert 88 ein. Klicken Sie auf **Weiter**.
     d. Wählen Sie auf der Seite **Kennwortserverinformationen angeben** die Auswahl **Ja** aus. Geben Sie im Feld **Kennwortserver** den Wert `kdc1.myco.com` und im Feld **Port** den Wert `464` ein. Klicken Sie auf **Weiter**.
     e. Wählen Sie auf der Seite **Chiffrierschlüsseleinträge auswählen** die Auswahl **i5/OS-Kerberos-Authentifizierung** aus. Klicken Sie auf **Weiter**.
     f. Geben Sie auf der Seite **i5/OS-Chiffrierschlüsseleintrag erstellen** ein Kennwort ein und bestätigen Sie es. Klicken Sie anschließend auf **Weiter**. Beispiel: `systema123`. Dieses Kennwort wird verwendet, wenn der Service-Principal von System A zum Kerberos-Server hinzugefügt wird.

        Anmerkung: Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.

     g. Wählen Sie auf der Seite **Stapeldatei erstellen** die Auswahl **Ja** aus, machen Sie die folgenden Angaben, und klicken Sie auf **Weiter**:
        - **Stapeldatei:** Fügen Sie am Ende des standardmäßig verwendeten Stapeldateinamens die Zeichenfolge `systema` an. Beispiel: `C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystema.bat`.
        - Wählen Sie **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 jeder Person mit Lesezugriffsberechtigung für die Stapeldatei gelesen werden können. Daher wird empfohlen, dass Sie die Stapeldatei nach dem Gebrauch unverzüglich vom Kerberos-Server und von Ihrem PC löschen.

          Anmerkung: Wenn Sie das Kennwort nicht einfügen, werden Sie bei der Ausführung der Stapeldatei zur Eingabe des Kennworts aufgefordert.

     h. Auf der Seite **Zusammenfassung** können Sie die Details zur Konfiguration des Netzwerkauthentifizierungsservice überprüfen. Klicken Sie auf **Fertig stellen**.
  6. Geben Sie auf der Seite **Directory-Server konfigurieren** die folgenden Informationen ein, und klicken Sie auf **Weiter**.

Anmerkung: Wenn Sie den Directory-Server vor dem Beginn dieses Szenarios konfiguriert haben, erscheint die Seite **Benutzer für Verbindung angeben** an Stelle der Seite **Directory-Server konfigurieren**. In diesem Fall müssen Sie den registrierten Namen und das Kennwort für den LDAP-Administrator angeben.

- **Port**: `389`
- **Registrierter Name**: `cn=Administrator`
- **Kennwort:** `mycopwd`

Anmerkung: Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.

7. Geben Sie auf der Seite **Domäne angeben** den Namen der Domäne im Feld **Domäne** ein. Beispiel: `MyCoEimDomain`.
8. Wählen Sie auf der Seite **Übergeordneten registrierten Namen für Domäne angeben** die Auswahl **Nein** aus. Klicken Sie auf **Weiter**.

   Anmerkung: Wenn der Directory-Server aktiv ist, wird die Nachricht angezeigt, dass Sie den Directory-Server beenden und erneut starten müssen, damit die Änderungen wirksam werden. Klicken Sie auf **Ja**, um den Directory-Server erneut zu starten.
9. Wählen Sie auf der Seite **Registerinformationen Lokales i5/OS** und **Kerberos** aus. Klicken Sie auf **Weiter**. Notieren Sie die Registernamen. Sie benötigen diese Registernamen, wenn Sie Zuordnungen zu EIM-Kennungen erstellen.

   Anmerkung:
   - Registernamen müssen in der Domäne eindeutig sein.
   - Sie können für das Benutzerregister einen speziellen Registerdefinitionsnamen eingeben, wenn Sie einen speziellen Benennungsplan für Registerdefinitionen (siehe hierzu Benennungsplan für EIM-Registerdefinitionen aufstellen) verwenden möchten. Für dieses Szenario können Sie jedoch die Standardwerte akzeptieren.
10. Wählen Sie auf der Seite **EIM-Systembenutzer angeben** den Benutzer aus, den das Betriebssystem bei der Ausführung von EIM-Operationen für Betriebssystemfunktionen verwendet. Klicken Sie anschließend auf **Weiter**.

    Anmerkung: Da Sie den Directory-Server nicht konfiguriert haben, bevor Sie die Schritte in diesem Szenario durchgeführt haben, können Sie nur den registrierten Namen des LDAP-Administrators als registrierten Namen auswählen.
    - **Benutzerart**: `Registrierter Name und Kennwort`
    - **Registrierter Name**: `cn=Administrator`
    - **Kennwort**: `mycopwd`

    Anmerkung: Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.
11. Bestätigen Sie die EIM-Konfigurationsdaten auf der Seite **Zusammenfassung**. Klicken Sie auf **Fertig stellen**.

Sie haben nun eine Basiskonfiguration für EIM und für den Netzwerkauthentifizierungsservice auf System A erstellt. Als Nächstes werden Sie System B für die Nutzung der EIM-Domäne konfigurieren, die Sie soeben erstellt haben.

System B zur Nutzung der EIM-Domäne und für den Netzwerkauthentifizierungsservice konfigurieren

Nachdem Sie eine neue Domäne erstellt und den Netzwerkauthentifizierungsservice auf System A konfiguriert haben, müssen Sie nun System B zur Nutzung der EIM-Domäne konfigurieren. Außerdem müssen Sie auf System B den Netzwerkauthentifizierungsservice konfigurieren.

Verwenden Sie die Informationen aus Ihren Arbeitsblättern, um diesen Schritt durchzuführen.

1. Erweitern Sie im System i Navigator die Einträge für **System B → Netzwerk → Enterprise Identity Mapping**.
2. Klicken Sie mit der rechten Maustaste auf **Konfiguration**, und wählen Sie **Konfigurieren** aus, um den Konfigurationsassistenten zu starten.
3. Wählen Sie auf der **Begrüßungsseite** die Auswahl **Neue Domäne erstellen und System hinzufügen**. Klicken Sie auf **Weiter**.
4. Führen Sie die folgenden Schritte durch, um den Netzwerkauthentifizierungsservice zu konfigurieren:
   a. Wählen Sie auf der Seite **Netzwerkauthentifizierungsservice konfigurieren** die Auswahl **Ja** aus.

      Anmerkung: Daraufhin wird der Assistent für den Netzwerkauthentifizierungsservice gestartet. Mit diesem Assistenten können Sie verschiedene i5/OS-Schnittstellen und -Services zur Nutzung eines Kerberos-Realms konfigurieren.

   b. Geben Sie auf der Seite **Realm-Informationen angeben** im Feld **Standard-Realm** den Wert `MYCO.COM` ein, und wählen Sie **Microsoft Active Directory wird für Kerberos-Authentifizierung verwendet** aus. Klicken Sie auf **Weiter**.
   c. Geben Sie auf der Seite **KDC-Informationen angeben** im Feld **KDC** den Wert `kdc1.myco.com` als Namen des Kerberos-Servers und im Feld **Port** den Wert `88` ein. Klicken Sie auf **Weiter**.
   d. Wählen Sie auf der Seite **Kennwortserverinformationen angeben** die Auswahl **Ja** aus. Geben Sie im Feld **Kennwortserver** den Wert `kdc1.myco.com` und im Feld **Port** den Wert `464` ein. Klicken Sie auf **Weiter**.
   e. Wählen Sie auf der Seite **Chiffrierschlüsseleinträge auswählen** die Auswahl **i5/OS-Kerberos-Authentifizierung** aus. Klicken Sie auf **Weiter**.
   f. Geben Sie auf der Seite **i5/OS-Chiffrierschlüsseleintrag erstellen** ein Kennwort ein und bestätigen Sie es. Klicken Sie anschließend auf **Weiter**. Beispiel: `systema123`. Dieses Kennwort wird verwendet, wenn der Service-Principal von System A zum Kerberos-Server hinzugefügt wird.

      Anmerkung: Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.

   g. Wählen Sie auf der Seite **Stapeldatei erstellen** die Auswahl **Ja** aus, machen Sie die folgenden Angaben, und klicken Sie auf **Weiter**.
      - **Stapeldatei:** Fügen Sie am Ende des standardmäßig verwendeten Stapeldateinamens die Zeichenfolge `systemb` an. Beispiel: `C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystemb.bat`.
      - Wählen Sie **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 jeder Person mit Lesezugriffsberechtigung für die Stapeldatei gelesen werden können. Daher wird empfohlen, dass Sie die Stapeldatei nach dem Gebrauch unverzüglich vom Kerberos-Server und von Ihrem PC löschen.

        Anmerkung: Wenn Sie das Kennwort nicht einfügen, werden Sie bei der Ausführung der Stapeldatei zur Eingabe des Kennworts aufgefordert.

   h. Auf der Seite **Zusammenfassung** können Sie die Details zur Konfiguration des Netzwerkauthentifizierungsservice überprüfen. Klicken Sie auf **Fertig stellen**.

5. Geben Sie auf der Seite **Domänencontroller angeben** die folgenden Informationen ein, und klicken Sie auf **Weiter**.
   - **Domänencontrollername**: `systema.myco.com`
   - **Port**: `389`
6. Geben Sie auf der Seite **Benutzer für Verbindung angeben** die folgenden Informationen an, und klicken Sie auf **Weiter**:

   Anmerkung: Geben Sie den registrierten Namen des LDAP-Administrators sowie dessen Kennwort an, die Sie zuvor in diesem Szenario auf System A erstellt haben.
   - **Benutzerart**: `Registrierter Name und Kennwort`
   - **Registrierter Name**: `cn=Administrator`
   - **Kennwort**: `mycopwd`

     Anmerkung: Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.
7. Geben Sie auf der Seite **Domäne angeben** den Namen der Domäne an, die Sie dem System hinzufügen möchten. Klicken Sie auf **Weiter**. Beispiel: `MyCoEimDomain`.
8. Wählen Sie auf der Seite **Registerinformationen** die Auswahl **Lokales i5/OS** aus und heben Sie die Auswahl **Kerberos-Register** auf. (Das Kerberos-Register wurde beim Erstellen der Domäne MyCoEimDomain erstellt.) Klicken Sie auf **Weiter**. Notieren Sie die Registernamen. Sie benötigen diese Registernamen, wenn Sie Zuordnungen zu EIM-Kennungen erstellen.

   Anmerkung:
   - Registernamen müssen in der Domäne eindeutig sein.
   - Sie können für das Benutzerregister einen speziellen Registerdefinitionsnamen eingeben, wenn Sie einen speziellen Benennungsplan für Registerdefinitionen (siehe hierzu Benennungsplan für EIM-Registerdefinitionen aufstellen) verwenden möchten. Für dieses Szenario können Sie jedoch die Standardwerte akzeptieren.
9. Wählen Sie auf der Seite **EIM-Systembenutzer angeben** den Benutzer aus, den das Betriebssystem bei der Ausführung von EIM-Operationen für Betriebssystemfunktionen verwendet. Klicken Sie anschließend auf **Weiter**.

   Anmerkung: Geben Sie den registrierten Namen des LDAP-Administrators sowie dessen Kennwort an, die Sie zuvor in diesem Szenario auf System A erstellt haben.
   - **Benutzerart**: `Registrierter Name und Kennwort`
   - **Registrierter Name**: `cn=Administrator`
   - **Kennwort**: `mycopwd`

     Anmerkung: Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.
10. Bestätigen Sie auf der Seite **Zusammenfassung** die EIM-Konfiguration. Klicken Sie auf **Fertig stellen**.

Sie haben nun System B für die Nutzung der Domäne und des Netzwerkauthentifizierungsservice konfiguriert.

Beide i5/OS-Service-Principals zum Kerberos-Server hinzufügen

Sie können zwischen zwei Methoden wählen, um die erforderlichen i5/OS-Service-Principals zum Kerberos-Server hinzuzufügen.

Sie können die Principals manuell, wie im Szenario dargestellt, oder anhand einer Stapeldatei hinzufügen. Sie haben diese Stapeldatei in Schritt 2 erstellt. Wenn Sie diese Datei verwenden möchten, können Sie sie mit FTP (File Transfer Protocol) auf den Kerberos-Server kopieren und dann ausführen.

Führen Sie die folgenden Schritte durch, um Namen von Principals anhand der Stapeldatei zum Kerberos-Server hinzuzufügen:

Vom Assistenten erstellte FTP-Stapeldateien

1. Öffnen Sie auf der Windows 2000-Workstation, die der Administrator zur Konfiguration des Netzwerkauthentifizierungsservice verwendet hat, ein Befehlsfenster, und geben Sie dort `ftp kdc1.myco.com` ein. Mit diesem Befehl wird eine FTP-Sitzung auf Ihrem PC gestartet. Sie werden aufgefordert, den Benutzernamen und das Kennwort des Administrators einzugeben.
2. Geben Sie an der FTP-Bedienerführung `lcd "C:\Documents and Settings\All Users\Documents\IBM\Client Access"` ein. Drücken Sie die Eingabetaste. Daraufhin sollte die Nachricht `Lokales Verzeichnis jetzt C:\Documents and Settings\All Users\Documents\IBM\Client Access` angezeigt werden.
3. Geben Sie an der FTP-Bedienerführung `cd \mein_verzeichnis` ein. Hierbei steht *mein_verzeichnis* für ein auf kdc1.myco.com befindliches Verzeichnis.
4. Geben Sie an der FTP-Bedienerführung `put NASConfigsystema.bat` ein. Daraufhin sollte die Nachricht: `226 Übertragung abgeschlossen` (oder ähnlicher Wortlaut) angezeigt werden.
5. Geben Sie `quit` ein, um die FTP-Sitzung zu verlassen.

   Anmerkung: Wiederholen Sie diese Schritte, um die Datei NASConfigsystemb.bat auf den Windows 2000-Server zu übertragen.

Beide Stapeldateien auf kdc1.myco.com ausführen

1. Öffnen Sie auf dem Windows 2000-Server das Verzeichnis, in das die Stapeldateien übertragen wurden.
2. Lokalisieren Sie die Datei `NASConfigsystema.bat`, und führen Sie sie durch Doppelklicken aus.
3. Wiederholen Sie diese Schritte für `NASConfigsystemb.bat`.
4. Vergewissern Sie sich nach der Ausführung der einzelnen Dateien, dass der i5/OS-Principal zum Kerberos-Server hinzugefügt wurde. Führen Sie dazu die folgenden Schritte durch:
   a. Erweitern Sie auf dem Windows 2000-Server die Einträge **Verwaltungstools → Active Directory-Benutzer und -Computer → Benutzer**.
   b. Vergewissern Sie sich, dass das System i-Modell über ein Benutzerkonto verfügt, indem Sie die entsprechende Windows 2000-Domäne auswählen.

      Anmerkung: Diese Windows 2000-Domäne muss mit dem Namen des Standard-Realms übereinstimmen, den Sie bei der Konfiguration des Netzwerkauthentifizierungsservice angegeben haben.

   c. Suchen Sie in der angezeigten Benutzerliste die Einträge **systema_1_krbsvr400** und **systemb_1_krbsvr400**. Hierbei handelt es sich um die Benutzerkonten, die für den i5/OS-Principal-Namen generiert wurden.
   d. (Optional) Rufen Sie die Eigenschaften der Active Directory-Benutzer auf. Wählen Sie auf der Registerkarte **Konto** den Eintrag **Konto wird für Delegierungszwecke vertraut** aus.

      Anmerkung: Dieser optionale Schritt ermöglicht es Ihrem System, die Berechtigungsnachweise eines Benutzers an andere Systeme zu delegieren oder weiterzuleiten. Folglich kann der i5/OS-Service-Principal im Namen des Benutzers auf Services zuzugreifen, die sich auf mehreren Systemen befinden. Dies ist besonders in einem Netzwerk mit mehreren Ebenen von Vorteil.

Nachdem Sie die i5/OS-Service-Principals zum Kerberos-Server hinzugefügt haben, können Sie auf dem System i-Modell Benutzerprofile erstellen.

Benutzerprofile auf System A und System B erstellen

Die Benutzer im Kerberos-Register MYCO.COM sollen alle einem einzigen i5/OS-Benutzerprofil auf den verschiedenen System i-Modellen zugeordnet werden.

Aus diesem Grund müssen Sie ein i5/OS-Benutzerprofil auf System A und System B erstellen. Verwenden Sie die Informationen aus Ihren Arbeitsblättern, um ein Benutzerprofil für diese Benutzer zu erstellen:

1. Erweitern Sie im System i Navigator die Einträge für **System A → Benutzer und Gruppen**.
2. Klicken Sie mit der rechten Maustaste auf **Alle Benutzer**, und wählen Sie **Neuer Benutzer** aus.
3. Geben Sie im Dialogfenster **Neuer Benutzer** im Feld **Benutzername** den Wert `SYSUSERA` ein.
4. Wählen Sie im Feld **Kennwort** die Auswahl **Kein Kennwort (Anmeldung nicht zulässig)** aus.
5. Klicken Sie auf **Funktionsspektrum**.
6. Wählen Sie auf der Seite **Berechtigungen** im Feld **Berechtigungsklasse** die Auswahl **Benutzer** aus. Klicken Sie auf **OK** und dann auf **Hinzufügen**.

Wiederholen Sie diese Schritte auf System B, geben Sie dabei jedoch im Feld **Benutzername** den Wert `SYSUSERB` ein.

Nachdem Sie die Benutzerprofile auf System A und System B erstellt haben, können Sie nun die Ausgangsverzeichnisse für alle i5/OS-Benutzerprofile erstellen.

Ausgangsverzeichnisse auf System A und System B erstellen

Jeder Benutzer, der eine Verbindung zu einem System i-Modell und den entsprechenden Anwendungen herstellen möchte, benötigt ein Verzeichnis im Ausgangsverzeichnis (/home). In diesem Verzeichnis wird der dem Benutzer zugeordnete Kerberos-Cache für Berechtigungsnachweise gespeichert.

Führen Sie folgende Schritte durch, um ein Ausgangsverzeichnis für einen Benutzer zu erstellen:

Geben Sie in der Befehlszeile von System A Folgendes ein: `CRTDIR '/home/benutzerprofil'`. Hierbei steht `benutzerprofil` für den Namen des System i-Benutzerprofils des Benutzers. Beispiel: `CRTDIR '/home/SYSUSERA'`. Mit diesem Befehl wird ein Ausgangsverzeichnis für das Benutzerprofil auf System A erstellt, das für alle Active Directory-Benutzer gilt.

Wiederholen Sie diesen Befehl auf System B, geben Sie dabei jedoch SYSUSERB an, um ein Ausgangsverzeichnis für das Benutzerprofil auf System B zu erstellen.

Nachdem Sie nun die Ausgangsverzeichnisse erstellt haben, können Sie die Konfiguration des Netzwerkauthentifizierungsservice auf den Systemen testen.

Netzwerkauthentifizierungsservice auf System A und System B testen

Nachdem Sie die Tasks zur Konfiguration des Netzwerkauthentifizierungsservice für beide Systeme ausgeführt haben, müssen Sie überprüfen, ob Ihre Konfigurationen für System A und System B ordnungsgemäß funktionieren.

Zum Testen der Funktionsfähigkeit dieser Konfigurationen können Sie die folgenden Schritte durchführen, um ein Ticket-granting Ticket für die Principals von System A und System B anzufordern:

Anmerkung: Vergewissern Sie sich, dass Sie ein Ausgangsverzeichnis für Ihr iSeries-Benutzerprofil erstellt haben, bevor Sie diese Prozedur ausführen.

1. Geben Sie an einer Bedienerführung `QSH` ein, um den Qshell Interpreter zu starten.
2. Geben Sie `keytab list` ein, um eine Liste der Principals anzuzeigen, die in der Chiffrierschlüsseldatei registriert sind. In diesem Szenario sollte als Principal-Name für System A "krbsvr400/systema.myco.com@MYCO.COM" angezeigt werden.

3. Geben Sie `kinit -k krbsvr400/systema.myco.com@MYCO.COM` ein, um ein Ticket-granting Ticket vom Kerberos-Server anzufordern. Mit diesem Befehl wird geprüft, ob Ihr System i-Modell ordnungsgemäß konfiguriert wurde und ob das Kennwort in der Chiffrierschlüsseldatei mit dem auf dem Kerberos-Server gespeicherten Kennwort übereinstimmt. Ist dies der Fall, kann der Befehl kinit ohne Fehler angezeigt werden.
4. Geben Sie `klist` ein, um sicherzustellen, dass der Standard-Principal krbsvr400/iseriesa.myco.com@MYCO.COM lautet. Mit diesem Befehl wird der Inhalt eines Kerberos-Caches für Berechtigungsnachweise angezeigt und geprüft, ob ein gültiges Ticket für den Service-Principal des System i-Modells erstellt und in den Cache für Berechtigungsnachweise auf dem System aufgenommen wurde.

```
 Ticket cache: FILE:/QIBM/USERDATA/OS400/NETWORKAUTHENTICATION/creds/krbcred

 Default principal: krbsvr400/systema.myco.com@MYCO.COM

Server: krbtgt/MYCO.COM@MYCO.COM
  Valid 200X/06/09-12:08:45 to 20XX/11/05-03:08:45
$
```

Wiederholen Sie diese Arbeitsschritte mit dem Namen des Service-Principals für System B: krbsvr400/systemb.myco.com@MYCO.COM

Nachdem Sie die Konfiguration des Netzwerkauthentifizierungsservice auf System A und System B getestet haben, können Sie eine EIM-Kennung für jeden der Administratoren erstellen.

EIM-Kennungen für die beiden Administratoren John Day und Sharon Jones erstellen

In diesem Szenario erstellen Sie zwei EIM-Kennungen, John Day und Sharon Jones.

Bei der Konfiguration der Einzelanmeldungstestumgebung müssen Sie EIM-Kennungen für zwei Ihrer Administratoren erstellen, damit sich beide mit ihren Windows-Benutzeridentitäten bei System i-Umgebungen anmelden können.

Führen Sie die folgenden Schritte durch, um die EIM-Kennungen zu erstellen:

1. Erweitern Sie im System i Navigator die Einträge für **System A** → **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung** → **MyCoEimDomain**.

   Anmerkung: Möglicherweise werden Sie aufgefordert, eine Verbindung zum Domänencontroller herzustellen. In diesem Fall wird das Dialogfenster **Verbindung zu EIM-Domänencontroller** angezeigt. Sie müssen eine Verbindung zur Domäne herstellen, um Aktionen in der Domäne ausführen zu können. Um eine Verbindung zum Domänencontroller herzustellen, müssen Sie die folgenden Informationen angeben und dann auf **OK** klicken:

   - **Benutzerart:** `Registrierter Name`
   - **Registrierter Name**: `cn=Administrator`
   - **Kennwort**: `mycopwd`

     Anmerkung: Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.
2. Klicken Sie mit der rechten Maustaste auf **Kennungen**, und wählen Sie **Neue Kennung** aus.
3. Geben Sie im Dialogfenster **Neue EIM-Kennung** im Feld **Kennung** den Namen `John Day` ein.
4. Klicken Sie auf **OK**.

Wiederholen Sie die Schritte 2 bis 4, geben Sie jedoch im Feld **Kennung** den Namen `Sharon Jones` ein.

Nachdem Sie nun eine EIM-Kennung für alle Administratoren erstellt haben, müssen Sie als Nächstes Kennungszuordnungen erstellen, mit den die Benutzeridentitäten den Kennungen zugeordnet werden. Erstellen Sie als Erstes die Kennungszuordnungen für John Day.

Kennungszuordnungen für John Day erstellen

Sie müssen die entsprechenden Zuordnungen zwischen der EIM-Kennung, John Day, und den Benutzeridentitäten, die von der durch die Kennung angegebenen Person verwendet werden, erstellen. Die Kennungszuordnungen ermöglichen dem Benutzer, richtige Konfiguration vorausgesetzt, die Nutzung einer Einzelanmeldungsumgebung.

In diesem Szenario müssen Sie eine Quellenzuordnung und zwei Zielzuordnungen für die Kennung "John Day" erstellen:

- Eine Quellenzuordnung für den Kerberos-Principal "jday", die Benutzeridentität, die die Person John Day zur Anmeldung bei Windows und im Netzwerk verwendet. Die Quellenzuordnung bietet die Möglichkeit, den Kerberos-Principal einer anderen Benutzeridentität zuzuordnen als derjenigen, die in einer entsprechenden Zielzuordnung definiert ist.
- Eine Zielzuordnung für das System i-Benutzerprofil JOHND. Hierbei handelt es sich um die Benutzeridentität, die der Benutzer John Day zur Anmeldung beim System i-Modell und bei anderen System i-Anwendungen auf System A verwendet. Die Zielzuordnung gibt an, dass eine Abgleichsuchoperation eine Zuordnung zwischen dieser und einer anderen Benutzeridentität herstellen kann. Die Zuordnung erfolgt hierbei auf der Basis einer Quellenzuordnung für dieselbe Kennung.
- Eine Zielzuordnung für das System i-Benutzerprofil DAYJO. Hierbei handelt es sich um die Benutzeridentität, die der Benutzer John Day für die Anmeldung beim System i Navigator und bei anderen System i-Anwendungen auf System B benutzt. Die Zielzuordnung gibt an, dass eine Abgleichsuchoperation dieser Benutzeridentität zugeordnet werden kann, und zwar von einer anderen Benutzeridentität als der, die in einer Quellenzuordnung für dieselbe Kennung definiert wurde.

Verwenden Sie die Informationen aus Ihren Arbeitsblättern, um die Zuordnungen zu erstellen:

Führen Sie die folgenden Schritte durch, um die Quellenzuordnung für den Kerberos-Principal von John Day zu erstellen:

1. Erweitern Sie auf System A die Einträge für **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung** → **MyCoEimDomain** → **Kennungen**.
2. Klicken Sie mit der rechten Maustaste auf **John Day**, und wählen Sie **Eigenschaften** aus.
3. Klicken Sie auf der Seite **Zuordnungen** auf **Hinzufügen**.
4. Geben Sie im Dialogfenster **Zuordnung hinzufügen** die gewünschten Daten an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **OK**.
   - **Register**: `MYCO.COM`
   - **Benutzer**: `jday`
   - **Zuordnungsart**: `Quelle`
5. Klicken Sie auf **OK**, um das Dialogfenster **Zuordnung hinzufügen** zu schließen.

Führen Sie die folgenden Schritte durch, um eine Zielzuordnung für das System i-Benutzerprofil von John Day auf System A zu erstellen:

1. Klicken Sie auf der Seite **Zuordnungen** auf **Hinzufügen**.
2. Geben Sie im Dialogfenster **Zuordnung hinzufügen** die gewünschten Daten an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **OK**:
   - **Register**: `SYSTEMA.MYCO.COM`
   - **Benutzer**: `JOHND`
   - **Zuordnungsart**: `Ziel`
3. Klicken Sie auf **OK**, um das Dialogfenster **Zuordnung hinzufügen** zu schließen.

Führen Sie die folgenden Schritte durch, um eine Zielzuordnung für das System i-Benutzerprofil von John Day auf System B zu erstellen:

1. Klicken Sie auf der Seite **Zuordnungen** auf **Hinzufügen**.
2. Geben Sie im Dialogfenster **Zuordnung hinzufügen** die gewünschten Daten an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **OK**:
   - **Register**: `SYSTEMB.MYCO.COM`
   - **Benutzer**: `DAYJO`
   - **Zuordnungsart**: `Ziel`
3. Klicken Sie auf **OK**, um das Dialogfenster **Zuordnung hinzufügen** zu schließen.
4. Klicken Sie auf **OK**, um das Dialogfenster **Eigenschaften** zu schließen.

Nachdem Sie die Kennungszuordnungen erstellt haben, die eine Zuordnung zwischen den Benutzeridentitäten von John Day und seiner EIM-Kennung herstellen, können Sie die gleichen Zuordnungen für Sharon Jones erstellen.

Kennungszuordnungen für Sharon Jones erstellen

Sie müssen die entsprechenden Zuordnungen zwischen der EIM-Kennung, Sharon Jones, und den Benutzeridentitäten, die von der durch die Kennung angegebenen Person verwendet werden, erstellen. Diese Zuordnungen ermöglichen dem Benutzer, richtige Konfiguration vorausgesetzt, die Nutzung einer Einzelanmeldungsumgebung.

In diesem Szenario müssen Sie eine Quellenzuordnung und zwei Zielzuordnungen für die Kennung ″Sharon Jones″ erstellen:

- Eine Quellenzuordnung für den Kerberos-Principal ″sjones″, die Benutzeridentität, die die Person Sharon Jones zur Anmeldung bei Windows und im Netzwerk verwendet. Die Quellenzuordnung bietet die Möglichkeit, den Kerberos-Principal einer anderen Benutzeridentität zuzuordnen als derjenigen, die in einer entsprechenden Zielzuordnung definiert ist.
- Eine Zielzuordnung für das i5/OS-Benutzerprofil SHARONJ. Hierbei handelt es sich um die Benutzeridentität, die die Benutzerin Sharon Jones für die Anmeldung beim System i Navigator und bei anderen i5/OS-Anwendungen auf System A benutzt. Die Zielzuordnung gibt an, dass eine Abgleichsuchoperation dieser Benutzeridentität zugeordnet werden kann, und zwar von einer anderen Benutzeridentität als der, die in einer Quellenzuordnung für dieselbe Kennung definiert wurde.
- Eine Zielzuordnung für das i5/OS-Benutzerprofil JONESSH. Hierbei handelt es sich um die Benutzeridentität, die die Benutzerin Sharon Jones für die Anmeldung beim System i Navigator und bei anderen i5/OS-Anwendungen auf System B benutzt. Die Zielzuordnung gibt an, dass eine Abgleichsuchoperation dieser Benutzeridentität zugeordnet werden kann, und zwar von einer anderen Benutzeridentität als der, die in einer Quellenzuordnung für dieselbe Kennung definiert wurde.

Verwenden Sie die Informationen aus Ihren Arbeitsblättern, um die Zuordnungen zu erstellen:

Führen Sie die folgenden Schritte durch, um die Quellenzuordnung für den Kerberos-Principal von Sharon Jones zu erstellen:

1. Erweitern Sie auf System A die Einträge für **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung** → **MyCoEimDomain** → **Kennungen**.
2. Klicken Sie mit der rechten Maustaste auf **Sharon Jones**, und wählen Sie **Eigenschaften** aus.
3. Klicken Sie auf der Seite **Zuordnungen** auf **Hinzufügen**.
4. Geben Sie im Dialogfenster **Zuordnung hinzufügen** die gewünschten Daten an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **OK**.
   - **Register**: `MYCO.COM`
   - **Benutzer**: `sjones`
   - **Zuordnungsart**: `Quelle`
5. Klicken Sie auf **OK**, um das Dialogfenster **Zuordnung hinzufügen** zu schließen.

Führen Sie die folgenden Schritte durch, um eine Zielzuordnung für das i5/OS-Benutzerprofil von Sharon Jones auf System A zu erstellen:

1. Klicken Sie auf der Seite **Zuordnungen** auf **Hinzufügen**.
2. Geben Sie im Dialogfenster **Zuordnung hinzufügen** die gewünschten Daten an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **OK**:
   - **Register**: SYSTEMA.MYCO.COM
   - **Benutzer**: SHARONJ
   - **Zuordnungsart**: Ziel
3. Klicken Sie auf **OK**, um das Dialogfenster **Zuordnung hinzufügen** zu schließen.

   Führen Sie die folgenden Schritte durch, um eine Zielzuordnung für das i5/OS-Benutzerprofil von Sharon Jones auf System B zu erstellen:
4. Klicken Sie auf der Seite **Zuordnungen** auf **Hinzufügen**.
5. Geben Sie im Dialogfenster **Zuordnung hinzufügen** die gewünschten Daten an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **OK**:
   - **Register**: SYSTEMB.MYCO.COM
   - **Benutzer**: JONESSH
   - **Zuordnungsart**: Ziel
6. Klicken Sie auf **OK**, um das Dialogfenster **Zuordnung hinzufügen** zu schließen.
7. Klicken Sie auf **OK**, um das Dialogfenster **Eigenschaften** zu schließen.

Nachdem Sie die Kennungszuordnungen erstellt haben, die eine Zuordnung zwischen den Benutzeridentitäten von Sharon Jones und ihrer EIM-Kennung herstellen, können Sie die Standardrichtlinienzuordnungen für Register erstellen, mit denen eine Zuordnung zwischen allen Kerberos-Registerbenutzern und einem bestimmten Benutzerprofil in jedem der Benutzerregister des System i-Modells hergestellt werden kann.

Standardrichtlinienzuordnungen für Register erstellen

Sie möchten alle Microsoft Active Directory-Benutzer auf dem Windows 2000-Server dem Benutzerprofil SYSUSERA auf System A und dem Benutzerprofil SYSUSERB auf System B zuordnen.

Sie können Richtlinienzuordnungen verwenden, um Abgleiche direkt zwischen einer Gruppe von Benutzern und einer einzelnen Zielbenutzeridentität zu erstellen. In diesem Fall können Sie eine Standardrichtlinienzuordnung für Register erstellen, mit der alle Benutzeridentitäten (für die keine Kennungszuordnungen vorhanden sind) im Kerberos-Register MYCO.COM einem einzigen i5/OS-Benutzerprofil auf System A zuordnet werden.

Sie benötigen zwei Richtlinienzuordnungen, um dieses Ziel zu erreichen. Jede Richtlinienzuordnung verwendet die Definition des Benutzerregisters MYCO.COM als Quelle der Zuordnung. Jede Richtlinienzuordnung ordnet jedoch abhängig davon, auf welches System i-Modell der Kerberos-Benutzer zugreift, Benutzeridentitäten in diesem Register verschiedenen Zielbenutzeridentitäten zu.

- Eine Richtlinienzuordnung ordnet die Kerberos-Principals im Benutzerregister MYCO.COM dem Zielbenutzer SYSUSERA im Zielregister SYSTEMA.MYCO.COM zu.
- Die andere Richtlinienzuordnung ordnet die Kerberos-Principals im Benutzerregister MYCO.COM dem Zielbenutzer SYSUSERB im Zielregister SYSTEMB.MYCO.COM zu.

Verwenden Sie die Informationen aus Ihren Arbeitsblättern, um zwei Standardrichtlinienzuordnungen für Register zu erstellen:

Anmerkung: Bevor Sie jedoch Richtlinienzuordnungen verwenden können, müssen Sie sich vergewissern, dass Sie die Domäne dafür aktiviert haben, Richtlinienzuordnungen für Abgleichsuchoperationen zu verwenden. Sie haben die Möglichkeit, diese Aktivierung bei der Erstellung Ihrer Richtlinienzuordnung durchzuführen. Gehen Sie dazu wie folgt vor:

1. Erweitern Sie im System i Navigator die Einträge für **System A** → **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung**.
2. Klicken Sie mit der rechten Maustaste auf **MyCoEimDomain**, und wählen Sie **Abgleichrichtlinie** aus.
3. Wählen Sie auf der Seite **Allgemein** die Auswahl **Abgleichsuchen mit Hilfe von Richtlinienzuordnungen für Domäne MyCoEimDomain aktivieren** aus.

Führen Sie die folgenden Schritte durch, um die Standardrichtlinienzuordnung für Register für die Benutzer, die dem Benutzerprofil SYSUSERA auf System A zugeordnet werden sollen, zu erstellen:

1. Klicken Sie auf der Seite **Register** auf **Hinzufügen**.
2. Geben Sie im Dialogfenster **Standardrichtlinienzuordnung für Register hinzufügen** die gewünschten Daten an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **OK**:
   - **Quellenregister**: `MYCO.COM`
   - **Zielregister**: `SYSTEMA.MYCO.COM`
   - **Zielbenutzer**: `SYSUSERA`
3. Klicken Sie auf **OK**, um das Dialogfenster **Abgleichrichtlinie** zu schließen.

   Führen Sie die folgenden Schritte durch, um die Standardrichtlinienzuordnung für Register für die Benutzer, die dem Benutzerprofil SYSUSERB auf System B zugeordnet werden sollen, zu erstellen:
4. Klicken Sie auf der Seite **Register** auf **Hinzufügen**.
5. Geben Sie im Dialogfenster **Standardrichtlinienzuordnung für Register hinzufügen** die gewünschten Daten an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **OK**:
   - **Quellenregister**: `MYCO.COM`
   - **Zielregister**: `SYSTEMB.MYCO.COM`
   - **Zielbenutzer**: `SYSUSERB`
6. Klicken Sie auf **OK**, um das Dialogfenster **Abgleichrichtlinie** zu schließen.

Nachdem Sie nun die Standardrichtlinienzuordnungen für Register erstellt haben, können Sie die Register für die Nutzung von Suchoperationen und Richtlinienzuordnungen aktivieren.

Register für die Nutzung von Suchoperationen und Richtlinienzuordnungen aktivieren

Mit EIM können Sie steuern, wie dieses Produkt von den einzelnen Registern genutzt wird. Da eine Richtlinienzuordnung weitreichende Auswirkungen in einem Unternehmen haben kann, können Sie festlegen, ob sich Richtlinienzuordnungen auf ein Register auswirken können.

Außerdem können Sie festlegen, ob ein Register überhaupt Abgleichsuchoperationen nutzen soll. Wenn Sie Richtlinienzuordnungen für ein Register verwenden möchten, müssen Sie deren Verwendung für das gegebene Register aktivieren und das Register für die Nutzung von Suchoperationen aktivieren. Führen Sie die folgenden Schritte durch, um Register für die Verwendung von Richtlinienzuordnungen und die Nutzung von Suchoperationen zu aktivieren:

Führen Sie die folgenden Schritte durch, um das Register MYCO.COM für die Nutzung von Abgleichsuchoperationen zu aktivieren:

1. Erweitern Sie im System i Navigator die Einträge für **System A** → **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung** → **MyCoEimDomain** → **Benutzerregister**.
2. Klicken Sie mit der rechten Maustaste auf **MYCO.COM**, und wählen Sie **Abgleichrichtlinie** aus.
3. Wählen Sie auf der Seite **Allgemein** die Auswahl **Abgleichsuchen mit Hilfe von Richtlinienzuordnungen für Register MYCO aktivieren** aus. Klicken Sie auf **OK**.

Führen Sie die folgenden Schritte durch, um das Register SYSTEMA.MYCO.COM für die Nutzung von Abgleichsuchoperationen und Richtlinienzuordnungen zu aktivieren:

1. Erweitern Sie im System i Navigator die Einträge für **System A** → **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung** → **MyCoEimDomain** → **Benutzerregister**.
2. Klicken Sie mit der rechten Maustaste auf **SYSTEMA.MYCO.COM**, und wählen Sie **Abgleichrichtlinie** aus.
3. Wählen Sie auf der Seite **Allgemein** die Auswahl **Abgleichsuchen für Register SYSTEMA.MYCO-.COM aktivieren** und dann **Richtlinienzuordnungen verwenden** aus. Klicken Sie auf **OK**.

Wiederholen Sie diese Schritte, um das Register SYSTEMB.MYCO.COM für die Nutzung von Abgleichsuchoperationen und Richtlinienzuordnungen zu aktivieren, wählen Sie jedoch auf der Seite **Allgemein** die Auswahl **Abgleichsuchen für Register SYSTEMB.MYCO.COM aktivieren** und dann **Richtlinienzuordnungen verwenden** aus. Klicken Sie auf **OK**.

Nachdem Sie die EIM-Konfiguration für Ihre Register und Benutzer abgeschlossen haben, können Sie die resultierenden Zuordnungen testen, um sicherzustellen, dass diese wie gewünscht arbeiten.

EIM-Identitätsabgleiche testen

Sie haben alle benötigten Zuordnungen erstellt und müssen jetzt sicherstellen, dass die EIM-Abgleichsuchoperationen basierend auf den konfigurierten Zuordnungen die richtigen Ergebnisse zurückgeben.

Bei diesem Szenario müssen Sie die Zuordnungen, die für die Kennungszuordnungen der einzelnen Administratoren verwendet werden, sowie die Zuordnungen, die für die Standardrichtlinienzuordnungen für Register verwendet werden, testen. Führen Sie diese Schritte durch, um die EIM-Abgleiche zu testen:

Abgleiche für John Day testen

Gehen Sie wie folgt vor, um zu testen, ob die Kennungsabgleiche für John Day erwartungsgemäß funktionieren:

1. Erweitern Sie im System i Navigator die Einträge für **System A** → **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung** → **MyCoEimDomain**.

   Anmerkung: Möglicherweise werden Sie aufgefordert, eine Verbindung zum Domänencontroller herzustellen. In diesem Fall wird das Dialogfenster **Verbindung zu EIM-Domänencontroller** angezeigt. Sie müssen eine Verbindung zur Domäne herstellen, um Aktionen in der Domäne ausführen zu können. Um eine Verbindung zum Domänencontroller herzustellen, müssen Sie die folgenden Informationen angeben und dann auf **OK** klicken:
   - **Benutzerart:** `Registrierter Name`
   - **Registrierter Name**: `cn=Administrator`
   - **Kennwort**: `mycopwd`

     Anmerkung: Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.
2. Klicken Sie mit der rechten Maustaste auf **MyCoEimDomain**, und wählen Sie **Abgleich testen** aus.
3. Geben Sie im Dialogfenster **Abgleich testen** die gewünschten Daten an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **Test**.
   - **Quellenregister**: `MYCO.COM`
   - **Quellenbenutzer**: `jday`
   - **Zielregister**: `SYSTEMA.MYCO.COM`
4. Die Ergebnisse werden im Abschnitt **Gefundener Abgleich** der Seite wie folgt angezeigt:

Für diese Felder	Siehe diese Resultate
Zielbenutzer	JOHND

Für diese Felder	Siehe diese Resultate
Ursprung	EIM-Kennung: John Day

5. Klicken Sie auf **Schließen**.

   Wiederholen Sie diese Schritte, wählen Sie jedoch für das Feld **Zielregister** den Wert `SYTEMB.MYCO.COM` aus. Die Ergebnisse werden im Abschnitt **Gefundener Abgleich** der Seite wie folgt angezeigt:

Für diese Felder	Siehe diese Resultate
Zielbenutzer	DAYJO
Ursprung	EIM-Kennung: John Day

Abgleiche für Sharon Jones testen

Führen Sie die folgenden Schritte durch, um die Abgleiche, die für die einzelnen Zuordnungen für Sharon Jones verwendet werden, zu testen:

1. Erweitern Sie im System i Navigator die Einträge für **System A** → **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung** → **MyCoEimDomain**.

   Anmerkung: Möglicherweise werden Sie aufgefordert, eine Verbindung zum Domänencontroller herzustellen. In diesem Fall wird das Dialogfenster **Verbindung zu EIM-Domänencontroller** angezeigt. Sie müssen eine Verbindung zur Domäne herstellen, um Aktionen in der Domäne ausführen zu können. Um eine Verbindung zum Domänencontroller herzustellen, müssen Sie die folgenden Informationen angeben und dann auf **OK** klicken:

   - **Benutzerart:** `Registrierter Name`
   - **Registrierter Name**: `cn=Administrator`
   - **Kennwort**: `mycopwd`

     Anmerkung: Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.
2. Klicken Sie mit der rechten Maustaste auf **MyCoEimDomain**, und wählen Sie **Abgleich testen** aus.
3. Geben Sie im Dialogfenster **Abgleich testen** die gewünschten Daten an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **Test**:
   - **Quellenregister**: `MYCO.COM`
   - **Quellenbenutzer**: `sjones`
   - **Zielregister**: `SYSTEMA.MYCO.COM`
4. Die Ergebnisse werden im Abschnitt **Gefundener Abgleich** der Seite wie folgt angezeigt:

Für diese Felder	Siehe diese Resultate
Zielbenutzer	SHARONJ
Ursprung	EIM-Kennung: Sharon Jones

5. Klicken Sie auf **Schließen**.

Wiederholen Sie diese Schritte, wählen Sie jedoch für das Feld **Zielregister** den Wert `SYSTEMB.MYCO.COM` aus. Die Ergebnisse werden im Abschnitt **Gefundener Abgleich** der Seite wie folgt angezeigt:

Für diese Felder	Siehe diese Resultate
Zielbenutzer	JONESSH
Ursprung	EIM-Kennung: Sharon Jones

Für Standardrichtlinienzuordnung für Register verwendete Abgleiche testen

Führen Sie die folgenden Schritte durch, um zu testen, ob die Abgleiche für die Benutzer in der Auftragsannahmeabteilung basierend auf den von Ihnen definierten Richtlinienzuordnungen erwartungsgemäß funktionieren:

1. Erweitern Sie im System i Navigator die Einträge für **System A** → **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung** → **MyCoEimDomain**.

   Anmerkung: Möglicherweise werden Sie aufgefordert, eine Verbindung zum Domänencontroller herzustellen. In diesem Fall wird das Dialogfenster **Verbindung zu EIM-Domänencontroller** angezeigt. Sie müssen eine Verbindung zur Domäne herstellen, um Aktionen in der Domäne ausführen zu können. Um eine Verbindung zum Domänencontroller herzustellen, müssen Sie die folgenden Informationen angeben und dann auf **OK** klicken:

   - **Benutzerart:** `Registrierter Name`
   - **Registrierter Name**: `cn=Administrator`
   - **Kennwort**: `mycopwd`

     Anmerkung: Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.
2. Klicken Sie mit der rechten Maustaste auf **MyCoEimDomain**, und wählen Sie **Abgleich testen** aus.
3. Geben Sie im Dialogfenster **Abgleich testen** die gewünschten Daten an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **Test**:
   - **Quellenregister**: `MYCO.COM`
   - **Quellenbenutzer**: `mmiller`
   - **Zielregister**: `SYSTEMA.MYCO.COM`
4. Die Ergebnisse werden im Abschnitt **Gefundener Abgleich** der Seite wie folgt angezeigt:

Für diese Felder	Siehe diese Resultate
Zielbenutzer	SYSUSERA
Ursprung	Richtlinienzuordnung für Register

5. Klicken Sie auf **Schließen**.

Führen Sie die folgenden Schritte durch, um die Abgleiche zu testen, die für die Standardrichtlinienzuordnung für Register verwendet werden, mit der Ihre Benutzer dem Profil SYSUSERB auf System B zugeordnet werden:

1. Erweitern Sie im System i Navigator die Einträge für **System A** → **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung** → **MyCoEimDomain**.

   Anmerkung: Möglicherweise werden Sie aufgefordert, eine Verbindung zum Domänencontroller herzustellen. In diesem Fall wird das Dialogfenster **Verbindung zu EIM-Domänencontroller** angezeigt. Sie müssen eine Verbindung zur Domäne herstellen, um Aktionen in der Domäne ausführen zu können. Um eine Verbindung zum Domänencontroller herzustellen, müssen Sie die folgenden Informationen angeben und dann auf **OK** klicken:

   - **Benutzerart:** `Registrierter Name`
   - **Registrierter Name**: `cn=Administrator`
   - **Kennwort**: `mycopwd`

Anmerkung: Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.

2. Klicken Sie mit der rechten Maustaste auf **MyCoEimDomain**, und wählen Sie **Abgleich testen** aus.
3. Geben Sie im Dialogfenster **Abgleich testen** die gewünschten Daten an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **Test**:
   - **Quellenregister**: `MYCO.COM`
   - **Quellenbenutzer**: `ksmith`
   - **Zielregister**: `SYSTEMB.MYCO.COM`
4. Die Ergebnisse werden im Abschnitt **Gefundener Abgleich** der Seite wie folgt angezeigt:

Für diese Felder	Siehe diese Resultate
Zielbenutzer	SYSUSERB
Ursprung	Richtlinienzuordnung für Register

5. Klicken Sie auf **Schließen**.

Wenn Sie Nachrichten bzw. Fehlernachrichten empfangen, die auf Probleme mit den Abgleichen oder der Übertragung hinweisen, sollten Sie die Informationen unter Fehlerbehebung bei Enterprise Identity Mapping lesen, um diese Probleme zu lösen.

Nachdem Sie die EIM-Identitätsabgleiche getestet haben, können Sie nun System i Access für Windows-Anwendungen für die Benutzung der Kerberos-Authentifizierung konfigurieren.

System i Access für Windows-Anwendungen für die Verwendung der Kerberos-Authentifizierung konfigurieren

Bevor Sie den System i Navigator für den Zugriff auf Ihr System einsetzen können, müssen Sie eine Kerberos-Authentifizierung durchführen. Aus diesem Grund müssen Sie System i Access für Windows auf Ihrem PC so konfigurieren, dass die Kerberos-Authentifizierung verwendet werden kann.

Zur Konfiguration von System i Access für Windows-Anwendungen für die Kerberos-Authentifizierung müssen Sie die folgenden Arbeitsschritte ausführen:

Anmerkung: Jeder Ihrer Benutzer muss alle diese Schritte auf seinem eigenen PC durchführen.

1. Melden Sie sich bei der Windows 2000-Domäne an, indem Sie an Ihrem PC eine Anmeldung durchführen.
2. Klicken Sie im System i Navigator auf Ihrem PC mit der rechten Maustaste auf den Eintrag für **System A**, und wählen Sie dann **Eigenschaften** aus.
3. Wählen Sie auf der Seite **Verbindung** die Auswahl **Kerberos-Principal-Namen verwenden, keine Anforderung** aus. Daraufhin können System i Access für Windows-Verbindungen für die Authentifizierung den Namen des Kerberos-Principals und das zugehörige Kennwort verwenden.
4. Es erscheint eine Nachricht, die anzeigt, dass Sie alle Anwendungen, die gegenwärtig ausgeführt werden, schließen und erneut starten müssen, damit die Änderungen der Verbindungseinstellungen wirksam werden. Klicken Sie auf **OK**. Beenden Sie anschließend den System i Navigator, und starten Sie ihn dann erneut.

Nachdem die System i Access für Windows-Anwendungen nun so konfiguriert sind, dass die Kerberos-Authentifizierung verwendet wird, können Sie die Einzelanmeldungsumgebung überprüfen.

Konfiguration des Netzwerkauthentifizierungsservice und von EIM überprüfen

Sie haben nun die einzelnen Bestandteile der Einzelanmeldungskonfiguration überprüft und sichergestellt, dass die gesamte Konfiguration vollständig ist. Jetzt müssen Sie überprüfen, ob EIM und der Netzwerkauthentifizierungsservice ordnungsgemäß konfiguriert wurden und die Einzelanmeldung erwartungsgemäß funktioniert.

Lassen Sie den Benutzer John Day die folgenden Schritte durchführen, um zu überprüfen, ob die Umgebung für die Einzelanmeldung ordnungsgemäß funktioniert:

1. Erweitern Sie im System i Navigator den Eintrag für **System A**, um eine Verbindung zu System A zu öffnen.
2. Drücken Sie F5, um die Anzeige zu aktualisieren.
3. Suchen Sie im rechten Fensterbereich in der Spalte **Name** nach `System A`, und überprüfen Sie, ob das i5/OS-Benutzerprofil von John Day (`JOHND`) als zugehöriger Eintrag in der Spalte **Angemeldeter Benutzer** angezeigt wird.

Der System i Navigator konnte mit Hilfe von EIM eine Zuordnung zwischen dem Kerberos-Principal jday und dem Benutzerprofil JOHND von System A herstellen, weil für die EIM-Kennung John Day entsprechende Zuordnungen definiert sind. Die Verbindung der System i Navigator-Sitzung für System A wird nun unter dem Namen JOHND hergestellt.

Wiederholen Sie diese Schritte für Sharon Jones und für mindestens eine der Benutzeridentitäten, die dem Benutzerprofil SYSUSERA oder SYSUSERB zugeordnet sind.

(Optional) Hinweise für die Konfigurationsnachbereitung

Nach Durchführung des Szenarios ist der registrierte Name (DN) für den LDAP-Administrator der einzige EIM-Benutzer, den Sie definiert haben und der von EIM verwendet werden kann.

Der registrierte Name des LDAP-Administrators, den Sie für den Systembenutzer auf System A angegeben haben, besitzt eine hohe Berechtigungsstufe für alle Daten auf dem Directory-Server. Daher möchten Sie möglicherweise einen oder mehrere registrierte Namen als zusätzliche Benutzer erstellen, deren EIM-Zugriffssteuerung für EIM-Daten besser an die geltenden Anforderungen angepasst und eingeschränkt ist. Wie viele EIM-Benutzer Sie zusätzlich definieren, hängt davon ab, welche Rolle in Ihren Sicherheitsrichtlinien die Trennung von Sicherheitsaufgaben und Sicherheitszuständigkeiten spielt. Normalerweise werden mindestens die beiden folgenden Arten von registrierten Namen erstellt:

- **Ein Benutzer mit EIM-Administratorrechten**

  Der registrierte Name des EIM-Administrators stellt die richtige Berechtigungsstufe für einen Administrator bereit, der für die Verwaltung der EIM-Domäne verantwortlich ist. Dieser registrierte Name für den EIM-Administrator kann verwendet werden, um eine Verbindung zum Domänencontroller herzustellen, wenn die Verwaltung der EIM-Domäne vollständig über den System i Navigator erfolgt.
- **Mindestens ein Benutzer, der die Zugriffssteuerung für alle folgenden Bereiche und Operationen besitzt**:
  - Kennungsadministrator
  - Registeradministrator
  - EIM-Abgleichoperation

  Dieser Benutzer besitzt die richtige Zugriffssteuerungsstufe, die der Systembenutzer benötigt, der EIM-Operationen für das Betriebssystem ausführt.

Anmerkung: Wenn Sie diesen neuen registrierten Namen des Systembenutzers an Stelle des registrierten Namens des LDAP-Administrators verwenden wollen, müssen Sie die EIM-Konfigurationseigenschaften für jedes System ändern. In diesem Szenario müssen Sie die Eigenschaften der EIM-Konfiguration bei allen System i-Modellen ändern, die Sie einrichten.

Szenario: Netzwerkauthentifizierungsservice und EIM an mehrere Systeme weitergeben

Im vorliegenden Szenario wird dargestellt, wie Sie mit dem Assistenten für die Funktionssynchronisation im System i Navigator eine Einzelanmeldungskonfiguration in einer i5/OS-Umgebung mit unterschiedlichen Releases an mehrere Systeme weitergeben können. Administratoren können auf diese Weise den Zeitaufwand reduzieren, indem Sie die Einzelanmeldung nur ein einziges Mal konfigurieren und dann an alle Systeme weitergeben, anstatt jedes System einzeln zu konfigurieren.

Situation

Sie sind der Netzwerkadministrator eines großen Herstellers von Kfz-Teilen. Sie verwalten fünf Systeme dem System i Navigator. Ein System wird als zentrales System eingesetzt, auf dem Daten gespeichert und mit dem die Endpunktsysteme verwaltet werden. Sie haben sich über die Vorteile der Einzelanmeldung informiert und wollen nun eine Einzelanmeldungsumgebung in Ihrem Unternehmen konfigurieren. Sie haben soeben die Einrichtung einer Testumgebung auf einem System abgeschlossen und möchten die Einzelanmeldungsumgebung nun unternehmensweit implementieren. Sie verfügen über vier weitere Server, die konfiguriert werden müssen, und Sie möchten nun ein möglichst zeitsparendes Verfahren zur Konfiguration dieser Einheiten anwenden.

Sie wissen, dass der System i Navigator den Assistenten für die Funktionssynchronisation umfasst, mit dem Sie die Einzelanmeldungskonfiguration von einem System kopieren und auf einem anderen i5/OS-System ab V5R3 anwenden können. Auf diese Weise ist es nicht erforderlich, jedes der Systeme einzeln zu konfigurieren.

Allerdings arbeitet eines Ihrer Systeme unter OS/400 Version 5 Release 2 (V5R2). Da OS/400 V5R2 den Assistenten für die Funktionssynchronisation nicht unterstützt, müssen Sie dieses System separat konfigurieren, damit auch dort die aktuelle EIM-Konfiguration und die aktuelle Konfiguration des Netzwerkauthentifizierungsservice, die auf dem Modellsystem eingesetzt wird, definiert werden kann.

Dieses Szenario hat folgende Vorteile:

- Vereinfachung der Konfigurations-Tasks, die für den Netzwerkauthentifizierungsservice und für EIM auf den verschiedenen Systemen zur Erstellung einer Einzelanmeldungsumgebung durchgeführt werden müssen.
- Reduzierung des Aufwands für die Konfiguration mehrerer Server, da Sie nur einen Assistenten verwenden, um eine einzige, manuell ausgeführte Konfiguration auf eine Reihe anderer Server zu kopieren und dort anzulegen.

Ziele

Als Netzwerkadministrator von MyCo, Inc. wollen Sie eine Einzelanmeldungsumgebung für Ihr Unternehmen einrichten, das alle verfügbaren Server nutzen können. Außerdem wollen Sie die vorhandenen Server so schnell und einfach wie möglich konfigurieren.

Dieses Szenario hat die folgenden Ziele:

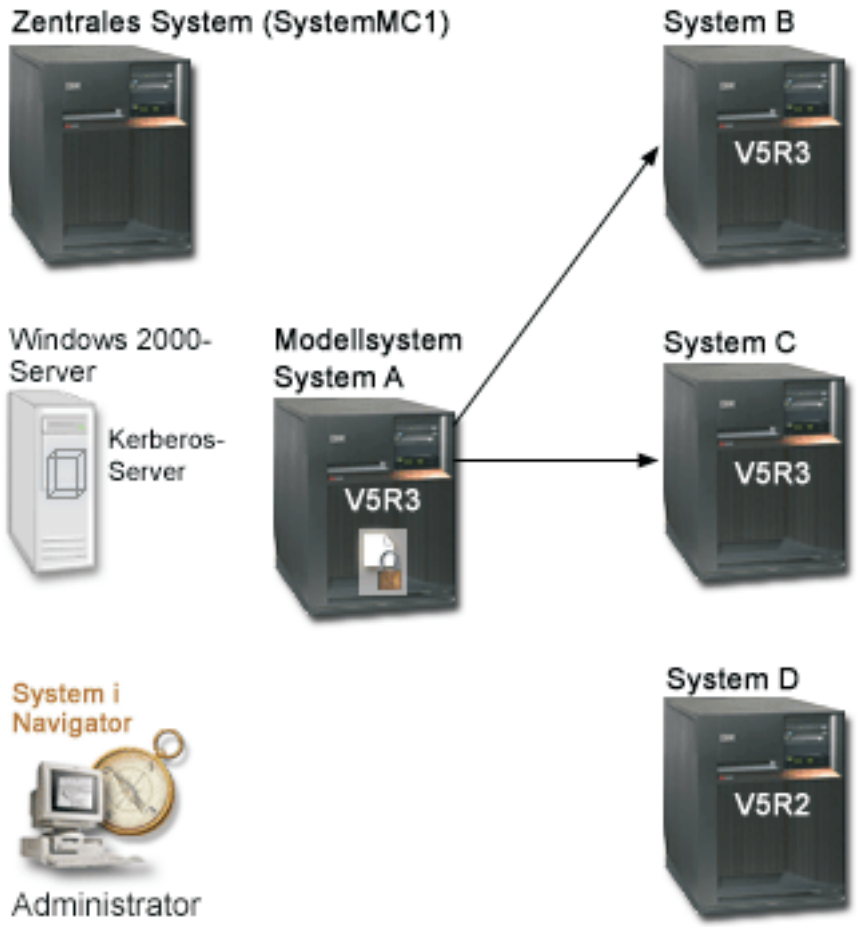
- System A verfügt über eine Konfiguration für den Netzwerkauthentifizierungsservice und eine EIM-Konfiguration, die während der Erstellung der Testumgebung definiert wurden. Aus diesem Grund muss System A als Modellsystem für die Weitergabe dieser Konfigurationen an die Endpunktsysteme System B und System C verwendet werden.
- Alle Systeme werden so konfiguriert, dass sie sich in derselben EIM-Domäne befinden. Außerdem müssen sie denselben Kerberos-Server und denselben Domänencontroller benutzen.

  Anmerkung: Unter Domänen wird beschrieben, wie zwei Domänentypen, d. h. eine EIM-Domäne und eine Windows 2000-Domäne, in der Einzelanmeldungsumgebung verwendet werden können.

- System D (das OS/400 V5R2-System) muss manuell für den Netzwerkauthentifizierungsservice und EIM konfiguriert werden.

Details

Die folgende Abbildung veranschaulicht die Netzwerkumgebung für dieses Szenario.



Die Abbildung veranschaulicht die folgenden Punkte, die für dieses Szenario relevant sind.

Windows 2000-Server

- Fungiert als Kerberos-Server für das Netzwerk und wird auch als KDC (Key Distribution Center) bezeichnet.
- Alle Benutzer sind beim Kerberos-Server auf dem Windows 2000-Server registriert.

System MC1 - Zentrales System

- Verwendet i5/OS ab Version 5 Release 3 (V5R3) mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS Host-Server
  - System i Access für Windows
- Speichert und terminiert die Synchronisationsfunktionen der verschiedenen Endpunktsysteme und führt diese Tasks aus.
- Ist für den Netzwerkauthentifizierungsservice und EIM konfiguriert.

System A - Modellsystem

Anmerkung: Das Modellsystem sollte ähnlich konfiguriert sein wie das System A im „Szenario: Einzelanmeldungstestumgebung erstellen" auf Seite 12. Verwenden Sie dieses Szenario, um sicherzustellen, dass alle Tasks für die Konfiguration der Einzelanmeldung auf dem Modellsystem ausgeführt und überprüft wurden.

- Verwendet i5/OS ab Version 5 Release 3 (V5R3) mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS Host-Server
  - System i Access für Windows
- Ist für den Netzwerkauthentifizierungsservice und EIM konfiguriert.
- Ist das Modellsystem, über das die Konfiguration des Netzwerkauthentifizierungsservice und die EIM-Konfiguration an die Zielsysteme weitergeleitet werden.

System B

- Verwendet i5/OS ab Version 5 Release 3 (V5R3) mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS Host-Server
  - System i Access für Windows
- Ist eines der Zielsysteme für die Weitergabe der Konfiguration des Netzwerkauthentifizierungsservice und der EIM-Konfiguration.

System C

- Verwendet i5/OS ab Version 5 Release 3 (V5R3) mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS Host-Server
  - System i Access für Windows
- Ist eines der Zielsysteme für die Weitergabe der Konfiguration des Netzwerkauthentifizierungsservice und der EIM-Konfiguration.

System D

- Verwendet OS/400 Version 5 Release 2 (V5R2) mit den folgenden installierten Optionen und Lizenzprogrammen:
  - OS/400 Host-Server
  - System i Access für Windows
  - Cryptographic Access Provider
- Die folgenden vorläufigen Programmkorrekturen (PTFs) für V5R2 wurden angelegt:
  - SI08977
  - SI08979
- Erfordert eine separate, manuelle Konfiguration des Netzwerkauthentifizierungsservice und von EIM mit Hilfe des entsprechenden Assistenten im System i Navigator.

Administrator-PC

- Verwendet System i Access für Windows
- Verwendet den System i Navigator ab V5R4 mit den folgenden Unterkomponenten:

  Anmerkung: Nur für den PC zur Verwaltung des Netzwerkauthentifizierungsservice erforderlich.
  - Netzwerk
  - Sicherheit

Voraussetzungen und Annahmen

Zur erfolgreichen Implementierung dieses Szenarios müssen die folgenden Voraussetzungen und Annahmen zutreffen:

System MC1 - Voraussetzungen des zentralen Systems

1. Alle Systemvoraussetzungen einschließlich der Installation der Software und des Betriebssystems wurden überprüft.

   Führen Sie folgende Schritte durch, um festzustellen, ob die erforderlichen Lizenzprogramme installiert wurden:

   a. Erweitern Sie im System i Navigator die Einträge für **Ihr System** → **Konfiguration und Service** → **Software** → **Installierte Produkte**.

   b. Vergewissern Sie sich, dass alle erforderlichen Lizenzprogramme installiert sind.
2. Die gesamte erforderliche Hardwareplanung und -konfiguration wurde durchgeführt.
3. TCP/IP und die Basissystemsicherheitsfunktion wurden konfiguriert und getestet.
4. SSL (Secure Sockets Layer) wurde konfiguriert, um die Datenübertragung zwischen diesen Servern zu schützen.

   Anmerkung: Wenn Sie die Konfiguration des Netzwerkauthentifizierungsservice an Server weitergeben, werden sensible Daten wie Kennwörter über das Netzwerk gesendet. Sie sollten SSL verwenden, um diese Informationen zu schützen, insbesondere, wenn diese beim Senden das lokale Netzwerk (Local Area Network, LAN) verlassen. Ausführliche Informationen finden Sie unter Scenario: Secure all connections to your Management Central server with SSL.

System A - Voraussetzungen des Modellsystems

Anmerkung: Bei diesem Szenario wird davon ausgegangen, dass System A korrekt für die Einzelanmeldung konfiguriert ist. Verwenden Sie das „Szenario: Einzelanmeldungstestumgebung erstellen" auf Seite 12, um sicherzustellen, dass alle Tasks für die Konfiguration der Einzelanmeldung auf dem Modellsystem ausgeführt und überprüft wurden.

1. Alle Systemvoraussetzungen einschließlich der Installation der Software und des Betriebssystems wurden überprüft.

   Führen Sie folgende Schritte durch, um festzustellen, ob die erforderlichen Lizenzprogramme installiert wurden:

   a. Erweitern Sie im System i Navigator die Einträge für **Ihr System** → **Konfiguration und Service** → **Software** → **Installierte Produkte**.

   b. Vergewissern Sie sich, dass alle erforderlichen Lizenzprogramme installiert sind.
2. Die gesamte erforderliche Hardwareplanung und -konfiguration wurde durchgeführt.
3. TCP/IP und die Basissystemsicherheitsfunktion wurden konfiguriert und getestet.
4. SSL (Secure Sockets Layer) wurde konfiguriert, um die Datenübertragung zwischen diesen Servern zu schützen.

   Anmerkung: Wenn Sie die Konfiguration des Netzwerkauthentifizierungsservice an Server weitergeben, werden sensible Daten wie Kennwörter über das Netzwerk gesendet. Sie sollten SSL verwenden, um diese Informationen zu schützen, insbesondere, wenn diese beim Senden das lokale Netzwerk (Local Area Network, LAN) verlassen. Ausführliche Informationen finden Sie unter Scenario: Secure all connections to your Management Central server with SSL.

System B, System C und System D - Voraussetzungen der Endpunktsysteme

1. Alle Systemvoraussetzungen einschließlich der Installation der Software und des Betriebssystems wurden überprüft.

   Führen Sie folgende Schritte durch, um festzustellen, ob die erforderlichen Lizenzprogramme installiert wurden:

   a. Erweitern Sie im System i Navigator die Einträge für **Ihr System** → **Konfiguration und Service** → **Software** → **Installierte Produkte**.
   b. Vergewissern Sie sich, dass alle erforderlichen Lizenzprogramme installiert sind.
2. Die gesamte erforderliche Hardwareplanung und -konfiguration wurde durchgeführt.
3. TCP/IP und die Basissystemsicherheitsfunktion wurden konfiguriert und getestet.
4. SSL (Secure Sockets Layer) wurde konfiguriert, um die Datenübertragung zwischen diesen Servern zu schützen.

   Anmerkung: Wenn Sie die Konfiguration des Netzwerkauthentifizierungsservice an Server weitergeben, werden sensible Daten wie Kennwörter über das Netzwerk gesendet. Sie sollten SSL verwenden, um diese Informationen zu schützen, insbesondere, wenn diese beim Senden das lokale Netzwerk (Local Area Network, LAN) verlassen. Ausführliche Informationen finden Sie unter Scenario: Secure all connections to your Management Central server with SSL.

Voraussetzungen des Windows 2000-Servers

1. Die gesamte erforderliche Hardwareplanung und -konfiguration wurde durchgeführt.
2. TCP/IP wurde auf dem Server konfiguriert und getestet.
3. Windows 2000-Domäne wurde konfiguriert und getestet.
4. Alle Benutzer im Netzwerk wurden zum Kerberos-Server hinzugefügt.

Konfigurationsschritte

Um die Konfiguration des Netzwerkauthentifizierungsservice und die EIM-Konfiguration vom Modellsystem System A an die Endpunktsysteme System B und System C weiterzugeben, müssen Sie die folgenden Tasks ausführen:

Anmerkung: Sie sollten sich mit den Konzepten, die im Zusammenhang mit der Einzelanmeldung verwendet werden, z. B. mit dem Netzwerkauthentifizierungsservice und EIM (Enterprise Identity Mapping), vertraut machen, bevor Sie dieses Szenario implementieren. Lesen Sie die folgenden Themen, um sich mit den Begriffen und Konzepten im Zusammenhang mit der Einzelanmeldung vertraut zu machen:

Zugehörige Informationen

Enterprise Identity Mapping - Konzepte

Planungsarbeitsblätter ausfüllen

Die folgenden Planungsarbeitsblätter wurden auf der Basis der allgemeinen Planungsarbeitsblätter für die Einzelanmeldung an dieses Szenario angepasst.

Diese Planungsarbeitsblätter veranschaulichen die Informationen, die Sie zusammenstellen, sowie die Entscheidungen, die Sie treffen müssen, um dieses Szenario vorzubereiten. Um eine erfolgreiche Implementierung sicherzustellen, sollten Sie für alle vorausgesetzten Elemente im Arbeitsblatt die Antwort ″Ja″ geben können. Außerdem sollten Sie alle Informationen, die zur Fertigstellung der Arbeitsblätter erforderlich sind, aufzeichnen, bevor Sie Konfigurationsaufgaben ausführen.

Tabelle 9. Netzwerkauthentifizierungsservice und EIM weitergeben - Arbeitsblatt für Voraussetzungen

Arbeitsblatt für Voraussetzungen	Antworten
Arbeiten Sie auf den folgenden Systemen mit i5/OS ab V5R3: • System MC1 • System A • System B • System C	Ja
Wurden die neuesten PTFs (vorläufigen Programmkorrekturen) angelegt?	Ja
Arbeiten Sie auf System D mit OS/400 ab V5R2?	Ja
Haben Sie die im Folgenden aufgeführten, aktuellsten vorläufigen Programmkorrekturen (PTFs) für System D angelegt? • SI08977 • SI08979	Ja
Sind die folgenden Optionen und Lizenzprogramme auf allen System i-Modellen installiert? • i5/OS Host-Server (5761-SS1 Option 12) • IBM System i Access für Windows (5761-XE1) • Cryptographic Access Provider für OS/400 V5R2- oder i5/OS V5R3-Systeme. Diese Option wird für Systeme, die mit i5/OS ab V5R4 arbeiten, nicht benötigt. **Anmerkung:** 5722 ist der Produktcode für i5/OS-Optionen und -Produkte mit einer Version vor V6R1.	Ja
Ist System i Access für Windows (5761-XE1) auf dem Administrator-PC installiert?	Ja
Ist der System i Navigator auf dem Administrator-PC mit den folgenden Unterkomponenten installiert: • Netzwerk • Sicherheit	Ja
Ist das neueste IBM System i Access für Windows-Service-Pack installiert? Informationen zum neuesten Service-Pack finden Sie auf der Webseite für System i Access  .	Ja
Verfügen Sie über die Sonderberechtigungen *SECADM, *ALLOBJ und *IOSYSCFG?	Ja
Fungiert eines der folgenden Systeme als Kerberos-Server? Wenn ja, geben Sie an, um welches System es sich handelt. 1. Microsoft Windows 2000-Server **Anmerkung:** Microsoft Windows 2000 Server verwendet als Standardsicherheitsmechanismus die Kerberos-Authentifizierung. 2. Windows(R) Server 2003 3. i5/OS PASE (ab V5R3) 4. AIX-Server 5. z/OS	Ja, Windows 2000-Server
Für Windows 2000 Server und Windows(R) Server 2003: Sind die Windows-Unterstützungstools (enthalten das Tool ktpass) installiert?	Ja
Beträgt die Abweichung zwischen der Systemzeit des System i-Modells und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung größer, lesen Sie die Informationen in Systemzeiten synchronisieren.	Ja

Tabelle 9. Netzwerkauthentifizierungsservice und EIM weitergeben - Arbeitsblatt für Voraussetzungen (Forts.)

Arbeitsblatt für Voraussetzungen	**Antworten**
Arbeiten Sie beim Kerberos-Server mit i5/OS PASE?	Auf dem System muss IBM Network Authentication Enablement for i5/OS (5761-NAE) installiert sein.

Tabelle 10. Netzwerkauthentifizierungsservice und EIM weitergeben - Planungsarbeitsblatt

Planungsarbeitsblatt für die Weitergabe der Konfigurationsdaten für den Netzwerkauthentifizierungsservice und EIM von System A an System B und System C	**Antworten**
Wie lautet der Name der Systemverwaltungsgruppe?	Systemverwaltungsgruppe MyCo
Welche Systeme werden in diese Systemverwaltungsgruppe aufgenommen?	System B, System C
Welches System wird als Modellsystem verwendet?	System A
Welche Funktionen sollen an diese Systemverwaltungsgruppe weitergegeben werden?	Netzwerkauthentifizierungsservice und Enterprise Identity Mapping (EIM)
Welche Chiffrierschlüsselarten sollen zur Chiffrierschlüsseldatei des Zielsystems hinzugefügt werden?	i5/OS-Kerberos-Authentifizierung
Wie lauten die Kennwörter, die jedem dieser Service-Principals für das Modell- und das Zielsystem zugeordnet sind? **Anmerkung:** Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Verwenden Sie diese Kennwörter niemals in Ihrer eigenen Konfiguration, um die System- bzw. Netzwerksicherheit nicht zu gefährden.	Kennwort der Principals für System A, B und C: `system123` Kennwort des Principals für System D: `systemd123`
Über welchen Benutzer möchten Sie eine Verbindung zum Domänencontroller herstellen?	**Benutzerart:** `Registrierter Name und Kennwort` **Registrierter Name:** `cn=Administrator` **Kennwort:** `mycopwd`

Systemverwaltungsgruppe erstellen

Bevor Sie die Konfiguration des Netzwerkauthentifizierungsservice und die EIM-Konfiguration an die Zielsysteme weitergeben können, müssen Sie eine Systemverwaltungsgruppe für alle Endpunktsysteme erstellen.

Eine Systemverwaltungsgruppe besteht aus einer Reihe von Systemen, die Sie verwalten und auf die Sie ähnliche Einstellungen und Attribute (z. B. für die Konfiguration des Netzwerkauthentifizierungsservice) anwenden können.

1. Erweitern Sie im System i Navigator den Eintrag für **Management Central (System MC1)**.
2. Klicken Sie mit der rechten Maustaste auf **Systemverwaltungsgruppen**, und wählen Sie **Neue Systemverwaltungsgruppe** aus, um eine neue Systemverwaltungsgruppe zu erstellen.
3. Geben Sie auf der Seite **Allgemein** im Namensfeld die Zeichenfolge `Systemverwaltungsgruppe MyCo` ein.
4. Geben Sie eine Beschreibung für diese Systemverwaltungsgruppe an.
5. Wählen Sie in der Liste **Verfügbare Systeme** System B und System C aus, und klicken Sie dann auf **Hinzufügen**. Daraufhin werden diese Systeme zur Liste **Ausgewählte Systeme** hinzugefügt.
6. Klicken Sie auf **OK**.
7. Erweitern Sie den Eintrag **Systemverwaltungsgruppen**, um zu überprüfen, ob Ihre Systemverwaltungsgruppe hinzugefügt wurde.

Nachdem Sie nun eine Systemverwaltungsgruppe für Ihre Endpunktsysteme erstellt haben, können Sie die Konfiguration des Netzwerkauthentifizierungsservice und die EIM-Konfiguration an diese Systeme weitergeben.

Systemeinstellungen vom Modellsystem (System A) an System B und System C weitergeben

Der Assistent für die Funktionssynchronisation im System i Navigator ermöglicht Ihnen die Weitergabe von Systemeinstellungen an mehrere Endpunktsysteme innerhalb derselben Systemverwaltungsgruppe.

Führen Sie diese Tasks aus, um die Konfiguration des Netzwerkauthentifizierungsservice und die EIM-Konfiguration an die Zielsysteme weiterzugeben:

1. Erweitern Sie im System i Navigator die Einträge für **Management Central (System MC1)** → **Systemverwaltungsgruppen**.
2. Klicken Sie mit der rechten Maustaste auf **Systemverwaltungsgruppe MyCo**, und wählen Sie **Systemwerte** → **Funktionen synchronisieren** aus. Klicken Sie dann auf **Weiter**. Daraufhin wird der **Assistent für die Funktionssynchronisation** aufgerufen.
3. Überprüfen Sie auf der **Begrüßungsseite** die Informationen zum Assistenten für die Funktionssynchronisation. Auf der **Begrüßungsseite** sind die Funktionen aufgelistet, die Sie später im Assistenten synchronisieren können.

   Anmerkung: Wenn Sie die Konfiguration des Netzwerkauthentifizierungsservice und die EIM-Konfiguration an Server weitergeben, werden sensible Daten wie z. B. Kennwörter über das Netzwerk gesendet. Sie sollten SSL verwenden, um diese Informationen zu schützen, insbesondere, wenn diese beim Senden das lokale Netzwerk (Local Area Network, LAN) verlassen. Ausführliche Informationen finden Sie unter Scenario: Secure all connections to your Management Central server with SSL.
4. Wählen Sie auf der Seite **Modellsystem System A** als Modellsystem aus, und klicken Sie dann auf **Weiter**. Dieses Modellsystem wird als Basis für die Synchronisation der Konfiguration des Netzwerkauthentifizierungsservice und der EIM-Konfiguration mit anderen Systemen verwendet.
5. Wählen Sie auf der Seite **Zielsysteme und -gruppen** die Auswahl **Systemverwaltungsgruppe MyCo** aus. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Zu aktualisierende Komponenten Netzwerkauthentifizierungsservice (Kerberos)** und **Enterprise Identity Mapping** aus. Klicken Sie auf **Konfiguration prüfen**. Klicken Sie nach der Überprüfung der Konfiguration auf **Weiter**.

   Anmerkung: Wenn die Überprüfung von EIM fehlschlägt, liegt möglicherweise ein Fehler in der EIM-Konfiguration des Modellsystems vor. Wenn die Konfiguration des Netzwerkauthentifizierungsservice fehlschlägt, liegt möglicherweise ein Fehler in der Konfiguration dieses Service auf dem Modellsystem vor.

   Um diese Fehler zu beheben, müssen Sie die EIM-Konfiguration und die Konfiguration des Netzwerkauthentifizierungsservice auf dem Modellsystem überprüfen, die gefundenen Fehler beheben und dann wieder zum Anfang des Szenarios zurückkehren und nochmals beginnen. Verwenden Sie das „Szenario: Einzelanmeldungstestumgebung erstellen" auf Seite 12, um sicherzustellen, dass alle Tasks für die Konfiguration der Einzelanmeldung auf dem Modellsystem ausgeführt und überprüft wurden.
7. Wählen Sie auf der Seite **Netzwerkauthentifizierungsservice** die Auswahl **i5/OS-Kerberos-Authentifizierung** aus, und geben Sie in den Feldern **Kennwort** und **Kennwort bestätigen** die Zeichenfolge `systema123` ein. Klicken Sie anschließend auf **Weiter**.

   Anmerkung: Dieses Kennwort wird für den Chiffrierschlüsseleintrag auf jedem Zielsystem verwendet. Wenn die Sicherheitsrichtlinie auf jedem System ein anderes Kennwort erfordert, können Sie diesen Schritt überspringen. Sie können stattdessen nach der Beendigung

dieses Assistenten die Chiffrierschlüsseleinträge manuell zu einzelnen Systemen hinzufügen und für jedes System ein anderes Kennwort eingeben.

8. Wählen Sie auf der Seite **Enterprise Identity Mapping** den Benutzer aus, den das Betriebssystem bei der Ausführung von EIM-Operationen verwendet.
   - **Benutzerart**: `Registrierter Name und Kennwort`
   - **Registrierter Name**: `cn=Administrator`
   - **Kennwort**: `mycopwd`
9. Überprüfen Sie auf der Seite **Zusammenfassung**, dass die entsprechenden Einstellungen auf dieser Seite aufgelistet sind. Klicken Sie auf **Fertig stellen**.
10. Erweitern Sie im System i Navigator die Einträge für **Management Central (System MC1)** → **Task-Aktivität** → **Systemwerte**.
11. Vergewissern Sie sich, dass die Task erfolgreich ausgeführt wurde.

Zugehörige Informationen

Chiffrierschlüsseldateien verwalten

Konfiguration für den Netzwerkauthentifizierungsservice und EIM auf System B und System C ausführen

Obwohl der Assistent für die Funktionssynchronisation die meisten Konfigurationsdaten weitergibt, die für eine Einzelanmeldungsumgebung benötigt werden, müssen Sie einige zusätzliche Arbeitsschritte ausführen, um die Einzelanmeldungskonfiguration für System B und System C mit dem System i Navigator vollständig auszuführen.

Im Folgenden sind die Tasks aufgeführt, die Sie abhängig davon, wie Sie die Einzelanmeldungsumgebung definiert haben, auf System B und System C ausführen müssen:

1. Fügen Sie i5/OS-Service-Principals zum Kerberos-Server hinzu.
2. Erstellen Sie für jeden Benutzer ein Ausgangsverzeichnis.
3. Testen Sie den Netzwerkauthentifizierungsservice.
4. Erstellen Sie EIM-Kennungen für die vorhandenen Benutzer.
5. Erstellen Sie Quellen- und Zielzuordnungen für die EIM-Kennungen.
6. Optional: Erstellen Sie Richtlinienzuordnungen.
7. Optional: Aktivieren Sie die Register für die Nutzung von Suchoperationen und die Verwendung von Richtlinienzuordnungen.
8. Testen Sie die EIM-Abgleiche.
9. Optional: Konfigurieren Sie die System i Access für Windows-Anwendungen für die Verwendung von Kerberos.
10. Überprüfen Sie die Konfiguration des Netzwerkauthentifizierungsservice und die EIM-Konfiguration.

Verwenden Sie das „Szenario: Einzelanmeldung für i5/OS aktivieren" auf Seite 26 als Richtlinie für die Ausführung der Konfiguration auf System B und System C. Dieses Szenario enthält eine Schritt-für-Schritt-Anleitung zur Ausführung aller Tasks, die für die Aktivierung der Einzelanmeldungsfunktion erforderlich sind.

Sie haben nun alle Tasks ausgeführt, die für die Weitergabe der Konfigurationsdaten für EIM und den Netzwerkauthentifizierungsservice von System A an System B und System C erforderlich sind.

Netzwerkauthentifizierungsservice und EIM auf System D (ab V5R2) konfigurieren

System D arbeitet mit OS/400 ab V5R2. Dieses Release bietet keine Unterstützung für den Assistenten für die Funktionssynchronisation.

Aus diesem Grund können die Konfigurationen auf System A nicht an System D weitergegeben werden. Stattdessen müssen Sie den EIM-Konfigurationsassistenten und den Assistenten für den Netzwerkauthentifizierungsservice verwenden, um dieses System manuell zu konfigurieren. Außerdem müssen Sie zusätzliche Schritte ausführen, um System D die Nutzung der Einzelanmeldungsumgebung zu ermöglichen.

Abhängig von der Art und Weise, wie Sie die Einzelanmeldung auf System A konfiguriert haben, müssen Sie hierzu die folgenden Arbeitsschritte ausführen:

1. Konfigurieren Sie System D zur Nutzung der EIM-Domäne und des Netzwerkauthentifizierungsservice. Verwenden Sie hierzu den EIM-Konfigurationsassistenten und den Assistenten für den Netzwerkauthentifizierungsservice.
2. Fügen Sie i5/OS-Service-Principals zum Kerberos-Server hinzu.
3. Erstellen Sie für jeden Benutzer ein Ausgangsverzeichnis.
4. Testen Sie den Netzwerkauthentifizierungsservice.
5. Erstellen Sie EIM-Kennungen für die vorhandenen Benutzer.
6. Erstellen Sie Quellen- und Zielzuordnungen für die EIM-Kennungen.
7. Optional: Erstellen Sie Richtlinienzuordnungen.
8. Optional: Aktivieren Sie die Register für die Nutzung von Suchoperationen und die Verwendung von Richtlinienzuordnungen.
9. Testen Sie die EIM-Abgleiche.
10. Optional: Konfigurieren Sie die System i Access für Windows-Anwendungen für die Verwendung von Kerberos.
11. Überprüfen Sie die Konfiguration des Netzwerkauthentifizierungsservice und die EIM-Konfiguration.

Verwenden Sie das Szenario Einzelanmeldung für i5/OS aktivieren als Richtlinie für die Ausführung der Konfiguration auf System D, so dass diese mit der Einzelanmeldungskonfiguration auf System A übereinstimmt. Dieses Szenario enthält Schritt-für-Schritt-Anleitungen zur Ausführung aller Tasks, die für die Aktivierung der Einzelanmeldungsfunktion erforderlich sind. Im Szenario für die Aktivierung der Einzelanmeldung für i5/OS sollten Sie die Anweisungen für System B befolgen, da dieses System zu einer bereits vorhandenen EIM-Domäne hinzugefügt wird, wie dies auch bei System D im vorliegenden Szenario der Fall ist.

Sie haben die Weitergabe der Konfiguration des Netzwerkauthentifizierungsservice und der EIM-Konfiguration an mehrere Systeme abgeschlossen. Wenn Sie den Management Central-Server so konfigurieren möchten, dass er eine Einzelanmeldungsumgebung nutzen kann, müssen Sie einige zusätzliche Tasks ausführen. Detaillierte Informationen hierzu finden Sie im Szenario: Management Central-Server für Einzelanmeldungsumgebung konfigurieren.

Szenario: Management Central-Server für Einzelanmeldung konfigurieren

Dieses Szenario veranschaulicht die Konfiguration Ihrer Management Central-Server für die Nutzung einer Einzelanmeldungsumgebung. Nachdem die zuständigen Administratoren das Szenario zur Weitergabe einer Einzelanmeldungskonfiguration an mehrere Systeme abgeschlossen haben, können die erforderlichen Konfigurationsschritte ausgeführt werden, um die Einbindung der Management Central-Server in die Einzelanmeldungsumgebung zu ermöglichen.

Situation

Sie sind als Systemadministrator eines mittelständischen Herstellers von Ersatzteilen tätig. Sie haben während der letzten drei Jahre einen System i Navigator-Management Central-Server verwendet, um einen zentralen Server und drei Endpunktserver zu verwalten. Ihr Zuständigkeitsbereich umfasst das Anlegen von PTFs, das Erstellen neuer Benutzerkonten im Netzwerk sowie andere Verwaltungsaufgaben. Sie fan-

| den es schon immer sinnvoll, PTFs von Ihrem zentralen Server aus an die gewünschten Zielsysteme zu
| senden, um diese dort zu installieren, da dies viel Zeit spart. Ihr Unternehmen hat gerade ein Upgrade
| auf i5/OS V5R4 oder eine spätere Version dieses Produkts durchgeführt und Ihr Sicherheitsadministrator
| hat eine neue Sicherheitsrichtlinie für Ihr Unternehmen implementiert, die vorschreibt, dass die Benutzer-
| kennwörter auf jedem System des Netzwerks unterschiedlich sein müssen. Zuvor war es bei den
| Management Central-Servern erforderlich, dass Benutzerprofile und -kennwörter netzwerkübergreifend
| einheitlich waren. Sie haben erfahren, dass es unter i5/OS ab V5R4 bei Verwendung der Einzelan-
| meldung auf den Management Central-Servern nicht mehr erforderlich ist, auf jedem Endpunktsystem
| übereinstimmende Benutzerprofile und -kennwörter zu definieren, um die Management Central-Server-
| funktionen zu verwenden. Dadurch reduziert sich der Aufwand für die Kennwortverwaltung auf Ihren
| i5/OS-Systemen.

Sie haben das Szenario zum Aktivieren der Einzelanmeldung für i5/OS für eines Ihrer neuen Systeme abgeschlossen und anschließend das Szenario für die Weitergabe des Netzwerkauthentifizierungsservice und von EIM an mehrere Systeme. Jetzt möchten Sie alle Management Central-Server so konfigurieren, dass diese die Einzelanmeldungsumgebung nutzen können.

Dieses Szenario hat folgende Vorteile:

- Reduzierung des Verwaltungsaufwandes für Benutzerprofile auf dem zentralen System sowie den Endpunktsystemen.
- Reduzierung des Verwaltungsaufwandes für die Benutzerkennwörter auf dem zentralen System sowie den Endpunktsystemen.
- Einhaltung der neuen Sicherheitsrichtlinie des Unternehmens, die vorschreibt, dass die Benutzerkennwörter auf den einzelnen Systemen eindeutig sein müssen.

Ziele

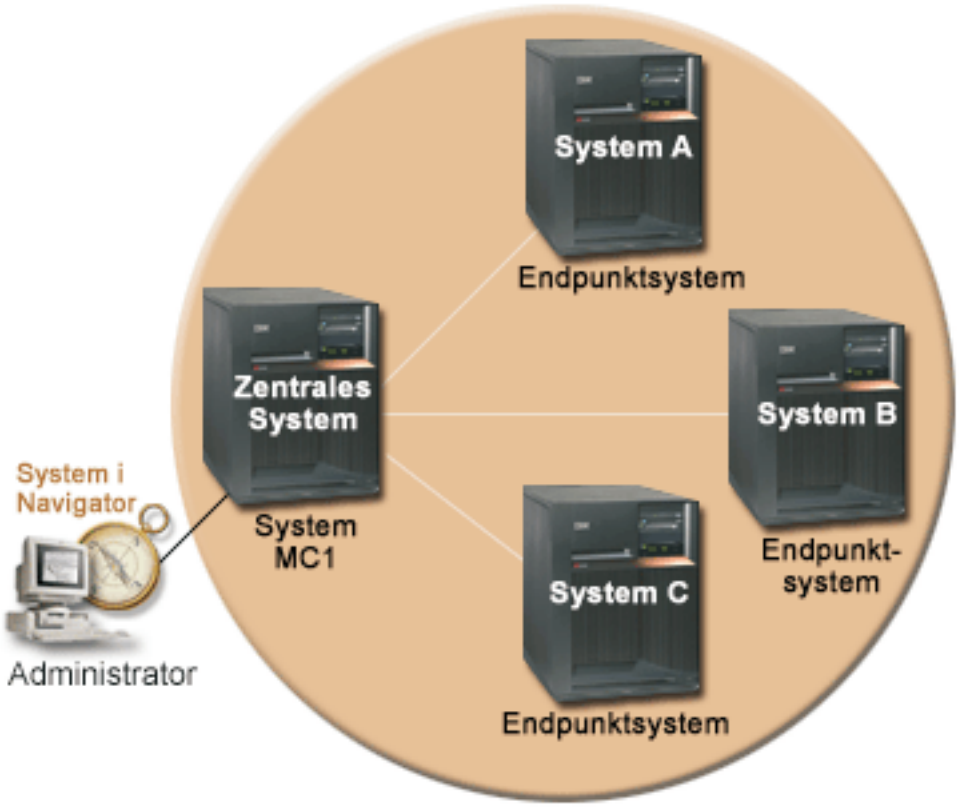
Sie sind einer der drei Systemadministratoren Ihres Unternehmens. Sie und die beiden anderen Administratoren Amanda und George wollen eine einfache Einzelanmeldungsumgebung einrichten, die den Verwaltungsaufwand reduziert und den Zugriff auf zentral verwaltete Anwendungen und Netzwerkressourcen vereinfacht.

Das Szenario hat die folgenden Zielsetzungen:

- Einhaltung der neuen Sicherheitsrichtlinie Ihres Unternehmens durch Aktivierung der Einzelanmeldungsfunktion auf den Management Central-Servern, die unter i5/OS arbeiten.
- Vereinfachung der Kennwortverwaltung durch Wegfall der Notwendigkeit, auf jedem über den Management Central-Server verwalteten Endpunktsystem mit demselben Benutzerprofil und -kennwort zu arbeiten.
- Möglichkeit zur Nutzung einer Einzelanmeldungsumgebung für alle vom Management Central-Server verwalteten Endpunktsysteme.
- Gewährleistung der Ressourcensicherheit innerhalb des Unternehmens durch Zuordnung der Benutzer zu bestimmten EIM-Kennungen an Stelle von Richtlinienzuordnungen.

Details

In der folgenden Abbildung wird die Netzwerkumgebung für dieses Szenario dargestellt:



Die Abbildung veranschaulicht die folgenden Punkte, die für dieses Szenario relevant sind.

- **Zentrales System System MC1 (Modellsystem):**
  - Verwendet i5/OS ab Version 5 Release 4 (V5R4) mit den folgenden installierten Optionen und Lizenzprogrammen:
    - i5/OS Host-Server (5761-SS1 Option 12)
    - IBM System i Access für Windows (5761-XE1)

    Anmerkung: 5722 ist der Produktcode für i5/OS-Optionen und -Produkte mit einer Version vor V6R1.
  - Speichert und terminiert die Tasks für die Synchronisationseinstellungen der verschiedenen Endpunktsysteme und führt diese Tasks aus.
  - Konfiguriert für Netzwerkauthentifizierungsservice und EIM.
  - Ausgewähltes Modellsystem, über das die Konfigurationen des Netzwerkauthentifizierungsservice und für EIM an die Zielsysteme weitergeleitet werden.

    Anmerkung: Das Modellsystem sollte ähnlich konfiguriert sein wie System A im Szenario: Einzelanmeldungstestumgebung erstellen. Verwenden Sie dieses Szenario, um sicherzustellen, dass alle Tasks für die Konfiguration der Einzelanmeldung auf dem Modellsystem ausgeführt und überprüft wurden.
- **Endpunktsysteme System A, System B und System C:**
  - Verwendet i5/OS ab Version 5 Release 4 (V5R4) mit den folgenden installierten Optionen und Lizenzprogrammen:

- i5/OS Host-Server (5761-SS1 Option 12)
- System i Access für Windows (5761-XE1)

– Konfiguriert für Netzwerkauthentifizierungsservice und EIM.

- **PC des Administrators:**
  – Verwendet System i Access für Windows (5761-XE1) ab V5R4.
  – Verwendet den System i Navigator mit den folgenden Unterkomponenten:
    - Netzwerk
    - Sicherheit

    Anmerkung: Nur für den PC zur Verwaltung des Netzwerkauthentifizierungsservice erforderlich.

Voraussetzungen und Annahmen

Zur erfolgreichen Implementierung dieses Szenarios müssen die folgenden Voraussetzungen und Annahmen zutreffen:

- **Zentrales System System MC1 (Modellsystem):**

  Anmerkung: Bei diesem Szenario wird davon ausgegangen, dass das zentrale System korrekt für die Einzelanmeldung konfiguriert ist. Verwenden Sie das Szenario: Einzelanmeldungstestumgebung erstellen, um sicherzustellen, dass alle Tasks für die Konfiguration der Einzelanmeldung auf dem zentralen System ausgeführt und überprüft wurden.

  – Alle Systemvoraussetzungen einschließlich der Installation der Software und des Betriebssystems wurden überprüft. Führen Sie folgende Schritte durch, um festzustellen, ob die erforderlichen Lizenzprogramme installiert wurden:
    - Erweitern Sie im System i Navigator die Einträge für **Ihr System** → **Konfiguration und Service** → **Software** → **Installierte Produkte**.
    - Vergewissern Sie sich, dass alle erforderlichen Lizenzprogramme installiert sind.
  – Die gesamte erforderliche Hardwareplanung und -konfiguration wurde durchgeführt.
  – TCP/IP und die Basissystemsicherheitsfunktion wurden konfiguriert und getestet.
  – SSL (Secure Sockets Layer) wurde konfiguriert, um die Datenübertragung zwischen diesen Servern zu schützen.

    Anmerkung: Wenn Sie die Konfiguration des Netzwerkauthentifizierungsservice
    tergeben, werden sensible Daten wie Kennwörter über das Netzwerk gesendet. Sie sollten SSL verwenden, um diese Informationen zu schützen, insbesondere, wenn diese beim Senden das lokale Netzwerk (Local Area Network, LAN) verlassen. Ausführliche Informationen finden Sie unter Scenario: Secure all connections to your Management Central server with SSL.

- **Endpunktsysteme System A, System B und System C:**
  – Alle Systemvoraussetzungen einschließlich der Installation der Software und des Betriebssystems wurden überprüft. Führen Sie folgende Schritte durch, um festzustellen, ob die erforderlichen Lizenzprogramme installiert wurden:
    - Erweitern Sie im System i Navigator die Einträge für **Ihr System** → **Konfiguration und Service** → **Software** → **Installierte Produkte**.
    - Vergewissern Sie sich, dass alle erforderlichen Lizenzprogramme installiert sind.
  – Die gesamte erforderliche Hardwareplanung und -konfiguration wurde durchgeführt.
  – TCP/IP und die Basissystemsicherheitsfunktion wurden konfiguriert und getestet.
  – SSL (Secure Sockets Layer) wurde konfiguriert, um die Datenübertragung zwischen diesen Servern zu schützen.

Anmerkung: Wenn Sie die Konfiguration des Netzwerkauthentifizierungsservice tergeben, werden sensible Daten wie Kennwörter über das Netzwerk gesendet. Sie sollten SSL verwenden, um diese Informationen zu schützen, insbesondere, wenn diese beim Senden das lokale Netzwerk (Local Area Network, LAN) verlassen. Ausführliche Informationen finden Sie unter Scenario: Secure all connections to your Management Central server with SSL.

- Sie haben den Netzwerkauthentifizierungsservice und EIM auf dem zentralen System und den Endpunktsystemen bereits konfiguriert. Detaillierte Informationen hierzu finden Sie im Szenario: Einzelanmeldung für i5/OS aktivieren und Szenario: Netzwerkauthentifizierungsservice und EIM an mehrere Systeme weitergeben.
- Sie verwenden als Kerberos-Server Microsoft Windows Active Directory.
- Sie haben (im Szenario: Einzelanmeldung für i5/OS aktivieren) bereits i5/OS-Service-Principal-Namen zum Kerberos-Server hinzugefügt.
- Sie haben (im Szenario: Netzwerkauthentifizierungsservice und EIM an mehrere Systeme weitergeben) die Konfiguration des Netzwerkauthentifizierungsservice bereits getestet.

Konfigurationsschritte

Gehen Sie wie folgt vor, um für die Benutzer der Management Central-Server die Einzelanmeldung zu aktivieren:

Anzeige der Domäne in der Domänenverwaltung überprüfen

Bevor Sie EIM-Kennungen erstellen können, müssen Sie sicherstellen, dass die EIM-Domäne, mit der Sie arbeiten, erfolgreich zur **Domänenverwaltung** hinzugefügt wurde.

Wenn Sie die EIM-Domäne bereits zur **Domänenverwaltung** hinzugefügt haben, können Sie die Arbeitschritte überspringen, die zum Hinzufügen der EIM-Domäne zur **Domänenverwaltung** erforderlich sind, und mit den Arbeitsschritten fortfahren, die zur Erstellung einer neuen EIM-Kennung ausgeführt werden müssen.

Gehen Sie wie folgt vor, um die EIM-Domäne zur Domänenverwaltung hinzuzufügen:

1. Erweitern Sie im System i Navigator auf dem PC unter **Meine Verbindungen** den Eintrag für das zentrale System **System MC1**, und wählen Sie dann **Netzwerk → Enterprise Identity Mapping → Domänenverwaltung** aus.
2. Klicken Sie mit der rechten Maustaste auf **Domänenverwaltung**, und wählen Sie dann **Domäne hinzufügen** aus.
3. Überprüfen Sie auf der Seite **Domäne hinzufügen**, ob das Feld **Domänencontroller** den vollständig qualifizierten Namen des Domänencontrollers für die hinzuzufügende Domäne enthält. Im vorliegenden Beispiel lautet der Name des Domänencontrollers `System MC1.myco.com` und der Name der hinzuzufügenden EIM-Domäne `MyCoEimDomain`.
4. Klicken Sie auf **OK**.
5. Erweitern Sie unter **Domänenverwaltung** den Eintrag `MyCoEimDomain`. Daraufhin wird die Anzeige **Verbindung zu EIM-Domänencontroller** aufgerufen.

   Anmerkung: Sie müssen eine Verbindung zum EIM-Domänencontroller herstellen, bevor Sie versuchen können, die Domäne zu verwalten.
6. Geben Sie auf der Seite **Verbindung zu EIM-Domänencontroller** den registrierten Namen und das Kennwort ein, die Sie während der Konfiguration des EIM-Domänencontrollers erstellt haben, und klicken Sie dann auf **OK**. Wenn Sie z. B. das Szenario zum Aktivieren der Einzelanmeldung für i5/OS durchgearbeitet haben, dann müssen Sie den registrierten Namen `cn=administrator` und das Kennwort `mycopwd` eingeben.

EIM-Kennungen erstellen

Bei der Einrichtung einer Einzelanmeldungsumgebung müssen Sie eine EIM-Kennung erstellen, um eine Person darzustellen.

Diese Task muss für jeden Benutzer ausgeführt werden, der Zugriff auf die Funktionen des Management Central-Servers erhalten soll. Führen Sie die folgenden Schritte durch, um eine neue EIM-Kennung zu erstellen:

1. Klicken Sie mit der rechten Maustaste unter `MyCoEimDomain` auf **Kennungen**, und wählen Sie dann **Neue Kennung** aus.
2. Geben Sie auf der Seite **Neue EIM-Kennung** im Feld **Kennung** einen Namen für die neue Kennung ein, und klicken Sie dann auf **OK**. Im vorliegenden Beispiel erstellen Sie eine EIM-Kennung für Ihre Kollegin, die Systemadministratorin Amanda Jones. Deswegen geben Sie im Feld **Kennung** den Namen `Amanda Jones` ein.

Wiederholen Sie die Schritte 1 bis 3 für alle Personen, die eine EIM-Kennung benötigen.

Kennungszuordnungen erstellen

Sie müssen eine Quellen- und eine Zielzuordnung zwischen jeder EIM-Kennung und den Benutzerprofilen auf allen Endpunktsystemen und auch auf dem zentralen System **System MC1** erstellen.

Dieser Schritt muss für jeden Benutzer ausgeführt werden, der über das zentrale System Zugriff auf die Ressourcen erhalten soll. Obwohl auch Richtlinienzuordnungen verwendet werden können, haben Sie sich gegen diese Lösung entschieden, um das Risiko zu beseitigen, dass nicht berechtigte Benutzer unbeabsichtigt Zugriff auf die verfügbaren Ressourcen erhalten. Nachdem Sie diesen Schritt durchgeführt haben, verfügt jeder Benutzer über eine EIM-Kennung, die jedem der entsprechenden Benutzerprofile auf den Endpunktsystemen zugeordnet ist. Diese Zuordnungen ermöglichen dem Benutzer die Nutzung Ihrer Einzelanmeldungsumgebung. Führen Sie die folgenden Schritte durch, um die erforderlichen Zuordnungen zu erstellen:

1. Erstellen Sie die Zuordnung **Quelle**:
   a. Wählen Sie auf dem PC über den System i Navigator das zentrale System **System MC1** aus, und erweitern Sie anschließend die Einträge für **Netzwerk → Enterprise Identity Mapping → Domänenverwaltung**.
   b. Erweitern Sie `MyCoEimDomain`, und wählen Sie dann **Kennungen** aus. Daraufhin wird im rechten Fensterbereich eine Liste der verfügbaren Kennungen angezeigt.
   c. Klicken Sie mit der rechten Maustaste auf `Amanda Jones`, und wählen Sie dann **Eigenschaften** aus.
   d. Klicken Sie auf der Registerkarte **Zuordnungen** auf **Hinzufügen**.
   e. Klicken Sie auf der Seite **Zuordnung hinzufügen** auf die Schaltfläche **Durchsuchen** neben dem Feld **Register**, und wählen Sie die Registerdefinition für das Register des Endpunktsystems aus, auf dem das Benutzerprofil gespeichert ist, das der Kennung von `Amanda Jones` zugeordnet werden soll. Im vorliegenden Beispiel möchten Sie eine Zuordnung zwischen der EIM-Kennung `Amanda Jones` und dem Benutzerprofil `AMJONES` auf dem Endpunktsystem **System A** erstellen.
   f. Geben Sie im Feld **Benutzer** das Benutzerprofil `AMJONES` ein.
   g. Wählen Sie im Feld **Zuordnungstyp** den Eintrag **Quelle** aus, und klicken Sie dann auf **OK**. Daraufhin wird die Zuordnung zur Liste der Zuordnungen hinzugefügt, die auf der Registerkarte **Zuordnungen** enthalten ist.
2. Erstellen Sie die Zuordnung **Ziel**:
   a. Klicken Sie auf der Registerkarte **Zuordnungen** der Seite **EIM-Kennungen** auf **Hinzufügen**.
   b. Klicken Sie auf der Seite **Zuordnung hinzufügen** auf **Durchsuchen**, und wählen Sie dann den Registernamen für **System A** aus.
   c. Geben Sie im Feld **Benutzer** das Benutzerprofil `AMJONES` ein.

Wiederholen Sie diese Schritte für alle Endpunktsysteme und EIM-Kennungen, für die Zuordnungen erstellt werden sollen. Nachdem Sie alle erforderlichen Schritte durchgeführt haben, müssen Sie im Dialogfenster **Eigenschaften für EIM-Kennungen** auf **OK** klicken.

Management Central-Server zur Nutzung des Netzwerkauthentifizierungsservice konfigurieren

Sie müssen das zentrale System und alle Endpunktsysteme zur Nutzung des Netzwerkauthentifizierungsservice (Kerberos) konfigurieren.

Führen Sie die Arbeitsschritte im Szenario: Kerberos-Authentifizierung zwischen Endpunktsystemen verwenden aus, um das zentrale System und alle Endpunktsysteme für die Nutzung von Kerberos zu konfigurieren.

Nachdem Sie dieses Szenario durchgearbeitet haben, müssen Sie im nächsten Schritt dieses Szenarios das zentrale System und alle Endpunktsysteme für die Verwendung von EIM konfigurieren.

Management Central-Server zur Nutzung von EIM konfigurieren

Zur Konfiguration des Management Central-Servers müssen Sie den System i Navigator verwenden.

Führen Sie die folgenden Schritte aus, um das zentrale System und alle Endpunktsysteme zur Nutzung von EIM zu konfigurieren:

1. Konfigurieren Sie das zentrale System zur Nutzung von EIM:
   a. Klicken Sie auf Ihrem PC im System i Navigator mit der rechten Maustaste auf das zentrale System **System MC1**, und wählen Sie dann **Eigenschaften** aus.
   b. Klicken Sie auf die Registerkarte **Sicherheit**, und vergewissern Sie sich, dass **Kerberos-Authentifizierung verwenden** ausgewählt wurde.
   c. Wählen Sie für den Identitätsabgleich die Auswahl **Verwenden, wenn Identität vorhanden ist (andernfalls Profil verwenden)** aus.

      Anmerkung: Sie können die Auswahl **Identitätsabgleich anfordern** auswählen. In diesem Fall schlägt allerdings die Ausführung von System i Navigator-Funktionen für Endpunktsysteme, die mit den Management Central-Servern arbeiten, bei EIM-Kennungen fehl, für die keine EIM-Zuordnungen erstellt wurden.
   d. Klicken Sie auf **OK**, um diesen Wert für **System MC1** zu definieren. Daraufhin wird eine Nachricht angezeigt, in der Sie auf die Voraussetzungen für die Konfiguration der Management Central-Server für die Verwendung des Netzwerkauthentifizierungsservice und von EIM hingewiesen werden.
   e. Klicken Sie auf **OK**, um anzugeben, dass Sie die Voraussetzungen zur Kenntnis genommen haben.
2. Erstellen Sie eine Systemverwaltungsgruppe:
   a. Erweitern Sie im System i Navigator den Eintrag für **System MC1**.
   b. Klicken Sie mit der rechten Maustaste auf **Systemverwaltungsgruppen**, und wählen Sie **Neue Systemverwaltungsgruppe** aus.
   c. Geben Sie auf der Seite **Allgemein** im Feld **Name** den Namen der Systemverwaltungsgruppe ein. Erstellen Sie eine Beschreibung für diese Systemverwaltungsgruppe. Im vorliegenden Beispiel geben Sie eine Systemverwaltungsgruppe mit dem Namen **group1** an und beschreiben diese als Gruppe von Endpunktsystemen, die von **System MC1** verwaltet werden.
   d. Wählen Sie in der Liste **Verfügbares System** das zentrale System **System MC1** und alle Endpunktsysteme (**System A**, **System B** und **System C**) aus, und klicken Sie dann auf **Hinzufügen**. Auf diese Weise werden diese Systeme der Liste **Ausgewählte Systeme** hinzugefügt.
   e. Klicken Sie auf **OK**.
   f. Erweitern Sie den Eintrag **Systemverwaltungsgruppen**, um zu überprüfen, ob Ihre Systemverwaltungsgruppe (**group1**) hinzugefügt wurde.
3. Erfassen Sie die Inventardaten der Systemverwaltungsgruppe:

a. Erweitern Sie im System i Navigator den Eintrag für **System MC1**, und wählen Sie dann **Systemverwaltungsgruppen** aus.
b. Klicken Sie mit der rechten Maustaste auf **group1**, und wählen Sie dann **Inventar → Erfassen** aus.
c. Wählen Sie auf der Seite **Inventar erfassen** für die Systemverwaltungsgruppe **group1** die Auswahl **Systemwerte** aus, und klicken Sie dann auf **OK**.

   Anmerkung: Standardmäßig wird daraufhin ein Dialogfenster angezeigt, in dem Sie darüber informiert werden, dass die Task **Inventar erfassen** gestartet wurde. Wenn Sie die Standardeinstellung geändert haben, wird dieses Dialogfenster allerdings nicht angezeigt.

d. Klicken Sie auf **OK**.
e. Lesen Sie auf der Seite **Inventarstatus erfassen** alle angezeigten Statuswerte, und beheben Sie alle möglicherweise auftretenden Fehler. Details zu verschiedenen Statuswerten, die sich auf die Inventarerfassung beziehen und die auf dieser Seite erscheinen, erhalten Sie, wenn Sie **Hilfe → Hilfe für Task-Status** auswählen.
f. Wählen Sie auf der Hilfeseite **Task-Status** die Auswahl **Inventar** aus. Auf dieser Seite werden alle möglichen Statuswerte mit detaillierten Beschreibungen sowie Informationen zur Fehlerbehebung angezeigt.
g. Nach dem erfolgreichen Abschluss der Inventarerfassung können Sie das Statusfenster schließen.

4. Vergleichen und aktualisieren Sie die EIM-Einstellungen:
   a. Erweitern Sie im System i Navigator den Eintrag für das zentrale System **System MC1**, und wählen Sie dann **Systemverwaltungsgruppen** aus.
   b. Klicken Sie mit der rechten Maustaste auf die Systemverwaltungsgruppe **group1**, und wählen Sie dann **Systemwerte → Vergleichen und aktualisieren** aus.
   c. Füllen Sie die Felder im Dialogfenster **Vergleichen und aktualisieren** der Systemverwaltungsgruppe aus:
      1) Wählen Sie im Feld **Modellsystem** das zentrale System **System MC1** aus.
      2) Wählen Sie **Management Central** für das Feld **Kategorie** aus.
      3) Wählen Sie in der Liste der zu vergleichenden Einträge **EIM für Benutzerabgleich verwenden** und **Identitätsabgleich anfordern** aus.
   d. Überprüfen Sie, ob die Zielsysteme in der Systemverwaltungsgruppe enthalten sind, und klicken Sie dann auf **OK**, um die Aktualisierung zu starten. Auf diese Weise wird jedes Zielsystem in der Systemverwaltungsgruppe mit den EIM-Einstellungen, die auf dem Modellsystem ausgewählt wurden, aktualisiert.

      Anmerkung: Standardmäßig wird ein Dialogfenster angezeigt, in dem Sie darüber informiert werden, dass die Task **Vergleichen und aktualisieren** gestartet wurde. Wenn Sie die Standardeinstellung geändert haben, wird dieses Dialogfenster allerdings nicht angezeigt.

   e. Klicken Sie auf **OK**.
   f. Vergewissern Sie sich im Statusdialogfenster **Werte aktualisieren**, dass die Aktualisierung auf allen Systemen ausgeführt wird, und schließen Sie das Dialogfenster anschließend.

5. Starten Sie den Management Central-Server auf dem zentralen System und allen Endpunktsystemen erneut:
   a. Erweitern Sie im System i Navigator den Eintrag für **Meine Verbindungen**.
   b. Erweitern Sie die Sicht des System i Navigator-Systems, für das ein Neustart durchgeführt werden soll.
   c. Erweitern Sie **Netzwerk → Server**, und wählen Sie **TCP/IP** aus.
   d. Klicken Sie mit der rechten Maustaste auf **Management Central**, und wählen Sie **Stoppen** aus. Die Serversicht wird ausgeblendet und es wird eine Nachricht angezeigt, in der Sie darüber informiert werden, dass keine Serververbindung mehr besteht.

e. Nachdem der Management Central-Server gestoppt wurde, müssen Sie auf **Starten** klicken, um einen Neustart dieser Einheit durchzuführen.

6. Wiederholen Sie diese Schritte für alle Endpunktsysteme (System A, System B und System C).

Szenario: Einzelanmeldung für ISV-Anwendungen aktivieren

In den folgenden Szenarios werden typische Situationen in Einzelanmeldungsimplementierungen dargestellt, die Sie bei der Planung eigener Zertifikatsimplementierungen im Rahmen Ihrer Serversicherheitsrichtlinien unterstützen.

Situation

Sie sind der leitende Anwendungsentwickler eines unabhängigen Softwareanbieters (ISV = Independent Software Vendor) und verantwortlich für die Überprüfung der Anwendungen, die von Ihrem Unternehmen entwickelt und an seine System i Navigator-Kunden geliefert werden. Sie wissen, dass der System i Navigator Ihren Kunden die Möglichkeit zum Erstellen und zur Nutzung einer Einzelanmeldungsumgebung bietet. Sie möchten, dass Ihre Anwendungen diese Einzelanmeldungsfunktionen nutzen, weil Sie überzeugt sind, dass sich dadurch die Absatzchancen Ihres Produkts verbessern. Sie wollen eine Anwendung mit dem Namen **Kalender** für System i Navigator-Kunden auf den Markt bringen, deren Einzelanmeldungsumgebung auf dem Netzwerkauthentifizierungsservice und EIM (Enterprise Identity Mapping) basiert. Die Anwendung **Kalender** ermöglicht Benutzern das Anzeigen und Verwalten ihres täglichen Terminplans. Um die Anwendung **Kalender** für die Einzelanmeldung zu aktivieren, müssen Sie speziellen Server-Code in die Anwendung integrieren, mit dessen Hilfe diese die Einzelanmeldungsumgebung nutzen kann. Sie verfügen bereits über Erfahrungen mit dem Erstellen von Anwendungen, die mit EIM-API-Aufrufen arbeiten, im vorliegenden Fall werden Sie aber zum ersten Mal eine Anwendung benutzen, die auch mit API-Aufrufen für den Netzwerkauthentifizierungsservice arbeitet.

Anmerkung: Es besteht auch die Möglichkeit, Anwendungen für Einzelanmeldungsumgebungen zu entwickeln, die mit einer anderen Authentifizierungsmethode arbeiten. Sie können z. B. an Stelle des Codes für die Authentifizierung über den Netzwerkauthentifizierungsservice auch Code in die Anwendung integrieren, der für die Durchführung der Authentifizierung mit digitalen Zertifikaten oder zur Herstellung einer Bindung zum Directory-Server benötigt wird.

Ziele

Sie möchten Ihre Anwendung **Kalender** System i Navigator-Kunden anbieten, die nach einer Anwendung suchen, mit der sie eine Einzelanmeldungsumgebung nutzen können. Sie möchten die Anwendung **Kalender** serverseitig für die Nutzung einer Einzelanmeldungsumgebung aktivieren. Bei der Ausführung des vorliegenden Szenarios haben Sie die folgenden Zielsetzungen:

- Sie wollen die Serverkomponente einer vorhandenen Anwendung **Kalender** ändern oder eine neue Anwendung **Kalender** entwickeln, die eine Einzelanmeldungsumgebung nutzt, die mit EIM und dem Netzwerkauthentifizierungsservice arbeitet.
- Sie wollen eine Einzelanmeldungsumgebung erstellen, in der die Anwendung getestet werden kann.
- Sie wollen Ihre Anwendung **Kalender** testen und auf diese Weise sicherstellen, dass diese eine Einzelanmeldungsumgebung erfolgreich nutzen kann.

Voraussetzungen und Annahmen

Die Implementierung dieses Szenarios hängt von den folgenden Voraussetzungen und Vorbedingungen ab:

- Sie möchten die Anwendung **Kalender** so konfigurieren, dass diese eine Einzelanmeldungsumgebung nutzen kann, die für den Einsatz von Kerberos und EIM konfiguriert ist.
- Sie verfügen bereits über Erfahrungen mit der Erstellung von Anwendungen für die System i Navigator-Plattform.

- Sie verwenden den System i Navigator mit den folgenden installierten Optionen und Lizenzprogrammen:
  - System i Navigator Host-Server (5761-SS1 Option 12)
  - IBM System i Access für Windows (5761-XE1)

  Anmerkung: 5722 ist der Produktcode für i5/OS-Optionen und -Produkte mit einer Version vor V6R1.
- Das i5/OS-System wurde für die Nutzung eines Kerberos-Realms konfiguriert.
- Zum Schreiben von Anwendungen benutzen Sie eine der folgenden Sprachen:
  - Sie benutzen zum Schreiben Ihrer Anwendungen eine ILE-Programmiersprache wie z. B. C und Sie verfügen über Kenntnisse zur GSS-API-Gruppe.
  - Sie benutzen zum Schreiben Ihrer Anwendungen Java und Sie verfügen über Kenntnisse zur JGSS-API-Gruppe.

    Anmerkung: Abhängig von den verwendeten JGSS-APIs benötigen Sie möglicherweise auch die Java Toolbox.
- Sie haben die Clientkomponente Ihrer Anwendung bereits fertiggestellt und diese für die Verwendung der Kerberos-Authentifizierung aktiviert.

Konfigurationsschritte

Zugehörige Informationen

Programmierung

Generic Security Service API

IBM® Java Generic Security Service (JGSS)

Planungsarbeitsblatt für Systemvoraussetzungen ausfüllen

Füllen Sie das folgende Planungsarbeitsblatt aus, um sicherzustellen, dass alle Systemvoraussetzungen für die erfolgreiche Einrichtung einer Einzelanmeldungsumgebung erfüllt sind, in der Sie Ihre Anwendung testen können.

Planungsarbeitsblatt für Systemvoraussetzungen	Antworten
Arbeitet Ihr System mit i5/OS ab V5R4?	Ja
Ist System i Access für Windows auf dem PC installiert, auf dem die Administratoraufgaben ausgeführt werden?	Ja
Ist die Unterkomponente "Sicherheit" des System i Navigator auf dem PC installiert, auf dem die Administratoraufgaben ausgeführt werden?	Ja
Ist die Unterkomponente "Netzwerk" des System i Navigator auf dem PC installiert, auf dem die Administratoraufgaben ausgeführt werden?	Ja
Verfügen Sie über die Sonderberechtigungen *SECADM, *ALLOBJ und *IOSYSCFG?	Ja
Fungiert eines der folgenden Systeme als Kerberos-Server? Wenn ja, geben Sie an, um welches System es sich handelt. 1. Microsoft Windows 2000-Server **Anmerkung:** Microsoft Windows 2000 Server verwendet als Standardsicherheitsmechanismus die Kerberos-Authentifizierung. 2. Windows® Server 2003 3. i5/OS PASE (ab V5R3) 4. AIX-Server 5. z/OS	Ja
Für Windows 2000-Server: Sind die Windows-Unterstützungstools (enthalten das Tool ktpass) installiert?	Ja

Planungsarbeitsblatt für Systemvoraussetzungen	Antworten
Sind alle PCs, die in Ihrem Netzwerk die Einzelanmeldungsumgebung nutzen sollen, in einer i5/OS-Domäne konfiguriert?	Ja
Wurden die neuesten PTFs (vorläufigen Programmkorrekturen) angelegt?	Ja
Sind die neuesten System i Access für Windows-Service-Packs installiert? Informationen zum neuesten Service-Pack finden Sie auf der Webseite für System i Access for Windows  .	Ja
Beträgt die Abweichung zwischen der Systemzeit des System i-Modells und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung größer, lesen Sie die Informationen in Systemzeiten synchronisieren.	Ja

Neue Anwendung schreiben oder vorhandene Anwendung ändern

Sie können nun den serverspezifischen Code, mit dem die Anwendung **Kalender** aktiviert wird, in Ihr System integrieren, um der Anwendung die Nutzung einer Einzelanmeldungsumgebung zu ermöglichen.

Anhand Ihrer vorhandenen Programmierungserfahrung mit EIM-APIs erstellen Sie nun den folgenden Programmablauf:

- Anwendungsinitialisierung
  - EIM-Handle Get
  - EIM-Verbindung
- Verarbeitungsschleife
  - Warten auf Benutzeranforderung
  - Authentifizieren des Benutzers mit Kerberos
  - Aufrufen von EIM zum Abgleich des Benutzers des Netzwerkauthentifizierungsservice mit dem lokalen Benutzer
  - Umschalten zum lokalen Benutzer
  - Ausführen der Task
  - Zurückschalten zum ursprünglichen Benutzer
  - Wechseln in den Status "Warten auf Benutzeranforderung"

    Anmerkung: Bei diesem Szenario wird davon ausgegangen, dass der Client-Code zur Aktivierung ihrer Anwendung für eine i5/OS-Einzelanmeldungsumgebung bereits erstellt oder geändert wurde. Deswegen werden nur die Arbeitsschritte angegeben, die zur Erstellung der serverspezifischen Komponenten des Programms erforderlich sind.
- Anwendungsbeendigung
  - EIM-Handle Destroy

Beispiele für Pseudocodeelemente und Codefragmente, die Sie zur Fertigstellung der Serverkomponente Ihres Programms verwenden können, finden Sie unter ISV-Codebeispiele. Wenn Sie den erforderlichen Client- und Server-Code zu Ihrer Anwendung **Kalender** hinzugefügt haben, können Sie eine Einzelanmeldungstestumgebung erstellen, um die erforderlichen Tests durchzuführen.

Einzelanmeldungstestumgebung erstellen

Zum Erstellen einer Testumgebung für die Einzelanmeldung müssen Sie vor der Ausführung des hier erläuterten Szenarios noch ein anderes Szenario ausführen.

Führen Sie die Anweisungen im Szenario: Einzelanmeldungstestumgebung erstellen aus. In diesem Szenario wird dargestellt, wie der Netzwerkauthentifizierungsservice und EIM konfiguriert werden müssen,

um eine Basistestumgebung für die Einzelanmeldung zu erstellen. Dieses Szenario führt Sie durch die folgenden Schritte, die zum Konfigurieren einer einfachen Einzelanmeldungsumgebung und zum Arbeiten mit dieser Umgebung erforderlich sind:

1. Füllen Sie die benötigten Planungsarbeitsblätter aus.
2. Erstellen Sie eine Basiskonfiguration für die Einzelanmeldung für das iSeries-System.
3. Fügen Sie den iSeries-Service-Principal zum Kerberos-Server hinzu.
4. Erstellen Sie auf dem iSeries-System ein Ausgangsverzeichnis für einen Testbenutzer mit dem Namen John Day.
5. Testen Sie die Konfiguration des Netzwerkauthentifizierungsservice auf dem iSeries-System.
6. Erstellen Sie eine EIM-Kennung für John Day.
7. Erstellen Sie eine Quellen- und eine Zielzuordnung für die neue EIM-Kennung.
8. Testen Sie die EIM-Identitätsabgleiche.
9. Konfigurieren Sie die System i Access für Windows-Anwendungen für die Verwendung von Kerberos.
10. Überprüfen Sie die Konfiguration des Netzwerkauthentifizierungsservice und die EIM-Konfiguration.

Nachdem Sie die im Szenario beschriebene Einzelanmeldungstestumgebung erstellt haben, können Sie die Anwendung **Kalender** testen, um zu überprüfen, ob diese fehlerfrei arbeitet.

Anwendung testen

Sie haben die Entwicklung der client- und der serverspezifischen Aktualisierungen für Ihre Anwendung **Kalender** abgeschlossen, so dass diese Anwendung nun in einer Einzelanmeldungsumgebung unter i5/OS ausgeführt werden kann. Jetzt können Sie die Anwendung testen.

Führen Sie die folgenden Arbeitsschritte aus, um zu überprüfen, ob die von Ihnen erstellte Anwendung in einer Einzelanmeldungsumgebung fehlerfrei funktioniert.

1. Melden Sie den (im Szenario zur Erstellung einer Einzelanmeldungstestumgebung erstellten) Testbenutzer `jday` bei der Windows 2000-Domäne an, indem Sie für diesen Benutzer eine Anmeldung an einem PC durchführen.
2. Veranlassen Sie den Testbenutzer, sich bei der Anwendung **Kalender**, die sich auf dem PC befindet, anzumelden. Wenn der Kalender geöffnet wird, bedeutet dies, dass EIM verwendet wurde, um den Kerberos-Principal `jday` mit dem i5/OS-Benutzerprofil `JOHND` abzugleichen. Dieser Abgleich wird ausgeführt, weil eine Zuordnung für die EIM-Kennung `John Day` vorhanden ist. Die **Kalender**-Anwendungssitzung für das System i-Modell verfügt nun über eine Verbindung, die über `JOHND` hergestellt wurde. Die ISV-Anwendung wurde erfolgreich für eine i5/OS-Einzelanmeldungsumgebung aktiviert.

Zugehörige Konzepte

„Szenario: Einzelanmeldungstestumgebung erstellen" auf Seite 12
In diesem Szenario wird dargestellt, wie der Netzwerkauthentifizierungsservice und EIM konfiguriert werden müssen, um eine Basistestumgebung für die Einzelanmeldung zu erstellen. Verwenden Sie dieses Szenario, um sich vorab in einer isolierten Testumgebung einen grundlegenden Überblick über die Arbeitsschritte zu verschaffen, die zur Konfiguration einer Einzelanmeldungsumgebung auszuführen sind, bevor Sie die Einzelanmeldung unternehmensweit implementieren.

Beispiel: ISV-Code

Im Folgenden wird ein Mustercode für das Schreiben eines Kerberos-Servers sowie zum Aufrufen von EIM-APIs dargestellt, über die eine Zuordnung zwischen einem Kerberos-Principal und einem i5/OS-Benutzerprofil hergestellt werden kann.

IBM erteilt Ihnen eine nicht ausschließliche Copyrightlizenz für die Nutzung aller Programmcodebeispiele, aus denen Sie ähnliche Funktionen generieren können, die an Ihre spezifischen Anforderungen angepasst sind.

Der gesamte Mustercode wird von IBM nur zur Veranschaulichung bereitgestellt. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. IBM kann deshalb die Zuverlässigkeit, Wartungsfreundlichkeit und Funktion dieser Programme nicht gewährleisten.

Alle enthaltenen Programme werden ohne jede Wartung (auf "as-is"-Basis) und ohne jede Gewährleistung zur Verfügung gestellt. IBM übernimmt ausdrücklich keine Gewährleistung für die Handelsüblichkeit und Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter.

Anmerkung: Wenn Sie die Codebeispiele verwenden, stimmen Sie den im „Haftungsausschluss für Programmcode" auf Seite 94 genannten Bedingungen zu.

```
/***   START OF SPECIFICATIONS   ***********************************/
/*                                                                   */
/*  MODULE NAME: Kerberos/EIM server sample                          */
/*                                                                   */
/*  DESCRIPTION:  Below is sample code for writing a Kerberos server */
/*                along with calling EIM APIs to map from a Kerberos */
/*                principal to an i5/OS user profile.                */
/*                                                                   */
/*                NOTE: Error checking has been removed.             */
/*********************************************************************/


/* #include files removed here                                      */

//-------------------------------------------------------------------
//  EIM assumptions:
//     On the System i model where this program is running the EIM
//     configuration information has been set.  The information used
//     by this program is:
//     - ldapURL
//     - local registry
//     EIM ldap lookup connection
//     -  The ldap connection information needed for doing the mapping
//        lookups in this program can be stored in a validation list
//        or other user secure space.  Here we will just hard code
//        pretend values.
//     -  This connection will only be used for a lookup operation so
//        the ldap user only needs EIM mapping lookup authroity.
//     All EIM data (Identifiers and associations) has been added.
//-------------------------------------------------------------------



#define LDAP_BINDDN   "cn=mydummmy"
#define LDAP_BINDPW   "special"


//-------------------------------------------------------------------
//
//  Function:  l_eimError
//  Purpose:   EIM error has occurred.  This function will print out the
//             EIM error message.
//
//-------------------------------------------------------------------
void l_eimError(char * function, EimRC * err)
{
    char * msg = NULL;
    printf("EIM ERROR for function = %s.\n", function);
    msg = eimErr2String(err);
    printf("   %s\n",msg);
    free(msg);
}


//-------------------------------------------------------------------
```

```
//
//  Function:  l_eimConnect
//  Purpose:   Get an EIM handle and connect to the ldap server.
//
//--------------------------------------------------------------------
int l_eimConnect(EimHandle * handle)
{
    int             rc = 0;
    char eimerr[150];
    EimRC *err = (EimRC *)&eimerr;
    EimConnectInfo   con;

    /* This needs to be at least 48. */
    err->memoryProvidedByCaller = 150;

    //----------------------------------------------------------------
    // Create handle.  We will pass NULL for the URL indicating that we
    // will use the information that was configured for the system.
    //----------------------------------------------------------------
    eimCreateHandle(handle,
                    NULL,
                    err);


    //----------------------------------------------------------------
    // Connect
    //----------------------------------------------------------------
    // The ldap user id and password might be stored in a validation
    // list or other user secure space.  Here we will just hard code
    // pretend values.
    // You can also choose to use Kerberos authentication when
    // connecting to ldap. You will first need to verify your ldap
    // server is set up to accept kerberos authentication.
    //----------------------------------------------------------------
    // This connection will only be used for a lookup operation so the
    // ldap user only needs EIM mapping lookup authroity.
    //----------------------------------------------------------------
    con.type = EIM_SIMPLE;
    con.creds.simpleCreds.protect = EIM_PROTECT_NO;
    con.creds.simpleCreds.bindDn = LDAP_BINDDN;
    con.creds.simpleCreds.bindPw = LDAP_BINDPW;
    con.ssl = NULL;
    eimConnect(handle,
               con,
               err);
    return 0;
}

//--------------------------------------------------------------------
//--------------------------------------------------------------------
//
//  Function:  getOS400User
//  Purpose:   Get OS400 user associated with the kerberos user and exchange
//             to the user.
//
//--------------------------------------------------------------------
int  getOS400User(EimHandle  * handle,
                  char       * OS400User,
                     gss_buffer_desc * client_name)
{

    char * principal;
    char * realm;
    char * atsign;

    //----------------------------------------------------------------
    //
```

```
    //   Get principal and realm from the kerberos client_name.
    //
    //-------------------------------------------------------------------
    //   client_name.value contains string of principal@realm.  Get
    //   pointer to each piece.
    //-------------------------------------------------------------------
    principal = client_name->value;
    atsign = strchr(principal, '@');
    *atsign = 0x00;                   // NULL end the principal
    realm = atsign + 1;               // ASdvance pointer to the realm

    //-------------------------------------------------------------------
    //
    //   Call EIM to get the target user associated with the kerberos
    //   source user.  This sample application assumes that the
    //   kerberos realm name is also the name of the EIM registry
    //   defining this realm.
    //
    //-------------------------------------------------------------------
    listPtr = (EimList *)listBuff;
    for (i = 0; i < 2; i++)
    {
        if (0 != (rc =
                  eimGetTargetFromSource(handle,
                                         realm,
                                         principal,
                                         NULL,         // use configured
                                                       // local
                                                       // registry.
                                         NULL,
                                         listSize,
                                         listPtr,
                                         err)))
        {
            l_eimError("eimGetTargetFromSource", err);
            return -1;
        }

        if (listPtr->bytesAvailable == listPtr->bytesReturned)
            break;
        else
        {
            listSize = listPtr->bytesAvailable;
            freeStorage = malloc(listSize);
            listPtr = (EimList *)freeStorage;
        }
    }

    // Check the number of entries found, if 0 no mapping exists
    // otherwise extract user profile from buffer and cleanup
    // storage

    return 0;

}

/*********************************************************************/
/* Function Name: get_kerberos_credentials_for_server                */
/*                                                                   */
/* Descriptive Name: Basically this function finds the keytab entry */
/*                   for this server. It will use this to validate   */
/*                   the tokens received.                            */
/*                                                                   */
/* Input:     char * service_name - the service name.                */
/*            gss_buffer_t msg_buf -  the input message              */
/* Output:                                                           */
/*            gss_cred_id_t *server_creds - The output credential    */
```

```
/*                                                                  */
/* Exit Normal:  return value == 0                                  */
/* Exit Error:   -1, error was encountered,                         */
/********************************************************************/
int get_kerberos_credentials_for_server (
    char *        service_name,  /* name of service principal       */
    gss_cred_id_t * server_creds)  /* credential acquired           */
{
     gss_buffer_desc name_buf;         /* buffer for import name    */
     gss_name_t server_name;           /* gss service name          */
     OM_uint32 maj_stat,               /* GSS status code           */
               min_stat;               /* Mechanism kerberos status */

     /* Convert service name to GSS internal format                 */
     name_buf.value = service_name;
     name_buf.length = strlen((char *)name_buf.value) + 1;
     maj_stat = gss_import_name(
                      &min_stat,      /* kerberos status       */
                      &name_buf,      /* name to convert       */
         (gss_OID) gss_nt_service_name,    /* name type     */
                      &server_name);  /* GSS internal name         */

     /* Acquire credentials for the service from keytab             */
     maj_stat = gss_acquire_cred(
                      &min_stat,      /* kerberos status       */
                      server_name,        /* gss internal name     */
                      GSS_C_INDEFINITE,   /* max credential life   */
                      GSS_C_NULL_OID_SET, /* use default mechanism */
                      GSS_C_ACCEPT,       /* credential usage      */
                      server_creds,       /* output cred handle    */
                      NULL,               /* ignore actual mech    */
                      NULL);              /* ignore time remaining */

     /* Release the gss internal format name                        */
     gss_release_name(&min_stat, &server_name);

     return 0;
}

/********************************************************************/
/* Function Name: do_kerberos_authentication()                      */
/* Purpose: Any valid client request is accepted.  If a context     */
/*          is established, its handle is returned in context and   */
/*          the client name is returned.                            */
/*                                                                  */
/* Exit Normal:  return value == 0                                  */
/* Exit Error:   -1, error was encountered,                         */
/********************************************************************/
int do_kerberos_authentication (int   s,
                                /* socket connection       */
    gss_cred_id_t server_creds,   /* credentials for the server   */
    gss_ctx_id_t * context,      /* GSS context                  */
    gss_buffer_t client_name)    /* kerberos principal           */
{
    gss_buffer_desc send_tok,     /* token to send to client      */
                recv_tok;     /* token received from client   */
     gss_name_t client;            /* client principal             */
     OM_uint32 maj_stat,       /* GSS status code              */
                min_stat;     /* Mechanism (kerberos) status  */
     msgDesc_t msgSend,       /* Message buffer to send       */
                msgRecv;     /* Message buffer received      */
     gss_OID doid;

     *context = GSS_C_NO_CONTEXT;     /* initialize the context     */

     do {
          /* Receive the message from the client                    */
```

```
   memset(&msgRecv, 0x00, sizeof(msgRecv));
   if (0 != recvAmessage(s, &msgRecv))
      return -1;
   recv_tok.length = msgRecv.dataLength;
   recv_tok.value = msgRecv.buffer;

          /* Accept the secuirty context                          */
   maj_stat = gss_accept_sec_context(
                              &min_stat,    /* kerberos status      */
                context,      /* context handle       */
               server_creds, /* acquired server creds */
                &recv_tok,    /* token received       */
          GSS_C_NO_CHANNEL_BINDINGS,   /* no CB       */
                &client,      /* client requestor     */
                NULL,         /* ignore mech type     */
                &send_tok,    /* token to be sent     */
                NULL,         /* ignore ctx flags     */
                NULL,         /* ignore time_rec      */
                NULL);        /* ignore delegated cred */

                    /* release the received token    */
              gss_release_buffer(&min_stat, &recv_tok);

            /* Check to see if there is a token client wants mutual
             authentication.                                      */
   if (send_tok.length != 0)
   {

             /* Send the token message to the other side           */
             /* release the send token buffer                      */
   }
     } while (maj_stat == GSS_S_CONTINUE_NEEDED);

     /* client name is returned - extract client from ticket. This
        client name will be used to map to the OS400 user profile   */
     maj_stat = gss_display_name(&min_stat, client, client_name, &doid);

     maj_stat = gss_release_name(&min_stat, &client);

     return 0;
}

/*********************************************************************/
/*                                                                   */
/* Function Name: getTestPort()                                      */
/*                                                                   */
/* Descriptive Name: get the port on which the server is listening  */
/*                                                                   */
/* Input:     char * service - the service name.  If null, looks    */
/*               for kerb-test-server.                               */
/*                                                                   */
/* Output:   none                                                    */
/*                                                                   */
/* Exit Normal:  return value == port number                         */
/*                                                                   */
/* Exit Error:   N/A                                                 */
/*                                                                   */
/*********************************************************************/
CLINKAGE int getTestPort(char *name)
{
  struct servent service;
  struct servent_data   servdata;
  char defaultName[] = "krb-test-server", *servName;
  char tcp[] = "tcp";
  int retPort, rc;
  memset(&servdata, 0x00, sizeof(servdata));
  memset(&service, 0x00, sizeof(service));
```

```
  if (name == NULL)
    servName = defaultName;
  else
    servName = name;
  rc = getservbyname_r(servName, tcp, &service,
                       &servdata);
  if (rc != 0)
    retPort = DEFAULT_KERB_SERVER_PORT;
  else
    retPort = service.s_port;


  return ntohl(retPort);
}                               /* end getPort                  */

/*********************************************************************/
/*                                                                   */
/* Function Name: getListeningSocket()                               */
/*                                                                   */
/* Descriptive Name: get a listening socket created and return it.   */
/*                                                                   */
/* Input:     none.                                                  */
/*                                                                   */
/* Output:   listening socket created.                               */
/*                                                                   */
/* Exit Normal:  return value == listening socket.                   */
/*                                                                   */
/* Exit Error:   -1, error was encountered.                          */
/*                                                                   */
/* NOTE: Error checking removed                                      */
/*                                                                   */
/*********************************************************************/
CLINKAGE int getListeningSocket(void)
{
  int                   rc, sd, option;
  struct sockaddr_in    sin;

  sd = socket(AF_INET, SOCK_STREAM, 0)

  option = 1;

  setsockopt(sd, SOL_SOCKET, SO_REUSEADDR,
             (char *)&option, sizeof(option));

  memset(&sin, 0x00, sizeof(sin));
  sin.sin_family = AF_INET;
  sin.sin_port = htons(getTestPort(NULL));
  bind(sd, (struct sockaddr *)&sin, sizeof(sin));

  listen(sd, SOMAXCONN);

  return sd;
}                                /* end getListeningSocket()     */


/*********************************************************************/
/*                                                                   */
/* Function Name: getServerSocket()                                  */
/*                                                                   */
/* Descriptive Name: get a server socket that is connected to a      */
/*                   client.  This routine blocks waiting for        */
/*                   the client.                                     */
/*                                                                   */
/* Input:     int lsd  - listening socket.                           */
/*                                                                   */
/* Output:    server socket created.                                 */
/*                                                                   */
```

```
/* Exit Normal:  return value == server socket.                      */
/*                                                                   */
/* Exit Error:   -1, error was encountered.                          */
/*                                                                   */
/* NOTE: Error checking removed                                      */
/*                                                                   */
/*********************************************************************/
CLINKAGE int getServerSocket(int lsd)
{
  return accept(lsd, NULL, 0);
}                                /* end getServerSocket()        */

/*********************************************************************/
/*                                                                   */
/* Function Name: main                                               */
/*                                                                   */
/* Descriptive Name: Driver for the server program which performs    */
/*                   kerberos authentication and EIM mapping.        */
/*                                                                   */
/* Input:     char* service_name - name of service requested         */
/*                                                                   */
/* Exit Normal:  0 = success                                         */
/*                                                                   */
/* Exit Error:   -1, error was encountered.                          */
/*                                                                   */
/* NOTE: Error checking removed                                      */
/*                                                                   */
/*********************************************************************/
 int main(int argc, char **argv)
{
      int  ssd,                  /* server socket                */
                lsd;             /* listening socket             */
    char     *service_name;      /* name of service (input)      */
    gss_cred_id_t   server_creds; /* server credentials to acquire */
    gss_ctx_id_t     context;    /* GSS context                  */
    OM_uint32      maj_stat,     /* GSS status code              */
                     min_stat;   /* Mechanism (kerberos) status  */
    gss_buffer_desc  client_name;    /* Client principal establishing
                                        context.                  */
    char  OS400User[10];
    char  save_handle[SY_PH_MAX_PRFHDL_LEN];  // *CURRENT profile handle
    char  client_handle[SY_PH_MAX_PRFHDL_LEN];// Swap to profile handle
    EimHandle        eimHandle;

    Qus_EC_t errorcode;
    memset(errorcode, 0x00, 256);
    errorcode->Bytes_Provided = 256;
    service_name = argv[1];

    /*-------------------------------------------------------------------
    //  Kerberos setup
    //      Acquire credentials for the service
    //-------------------------------------------------------------------*/
    get_kerberos_credentials_for_server(service_name, &server_creds);

    /*-------------------------------------------------------------------
    // get a listening socket
    //-------------------------------------------------------------------*/
    lsd = getListeningSocket();

    /*-------------------------------------------------------------------
    //   EIM setup
    //   Connect to eim
    // ------------------------------------------------------------------*/
    l_eimConnect(&eimHandle);
```

```
    /*-------------------------------------------------------------
    //   Save a copy of the current user so we can swap back to it
    //   after each request
    // -------------------------------------------------------------*/
    QsyGetProfileHandleNoPwd(save_handle,
                             "*CURRENT  ",
                             "*NOPWD    ",
                              &errorcode);

    /*-------------------------------------------------------------
    //  Loop waiting for requests on the socket
    //-------------------------------------------------------------*/
          do { /* loop until the application or the system is ended     */
               /* Save the profile handle of the current user        */
           /* Accept a TCP connection             */
         ssd = getServerSocket(lsd);
         /* ------------------------------------------------------------
         //  Establish context with the client and get the client name.
         //------------------------------------------------------------
         //  The client name contains the kerberos principal and realm. In
         //  EIM these equate to the source user and source registry.
         //------------------------------------------------------------ */
         do_kerberos_authentication(ssd,
                                    server_creds,
                    &context,
                                    &client_name);

  /*-------------------------------------------------------------
         //  Perform eim mapping lookup operation to get the associated
        //  OS400 user.
         //------------------------------------------------------------ */
         getOS400User(&eimHandle,
                OS400User,
                  &client_name);
    /* ------------------------------------------------------------
                // Swap to the user returned from EIM lookup
        // ------------------------------------------------------------ */
                QsyGetProfileHandleNoPwd(client_handle,
                                         client_name,
                                         "*NOPWDCHK ",
                                          &errorcode);
                QsySetToProfileHandle(client_handle, &errorcode);
    /* ------------------------------------------------------------
         // do the real work of the application here as the application is
                // now running under an appropriate user profile
        // ------------------------------------------------------------ */
                   // Call or code application specific behavior here.

     /* ------------------------------------------------------------
                // reset the process to run under the original user profile
        // ------------------------------------------------------------ */
                QsySetToProfileHandle(save_handle, &errorcode);

     } while (1)

    eimDestroy_handle(&eimHandle);
    gss_delete_sec_context(&min_stat, &context, NULL);
    close(ssd);
    close(lsd);
    gss_release_cred(&min_stat, &server_creds);
    return 0;
}
```

Einzelanmeldung planen

Während des Planungsprozesses für die Einzelanmeldung werden die Software- und Hardwarevoraussetzungen identifiziert, die zur Implementierung der Einzelanmeldung in Ihrem Unternehmen erfüllt werden müssen.

Bei der Planung müssen Sie sorgfältig darauf achten, dass die von Ihnen erstellte Einzelanmeldungsumgebung den individuellen Anforderungen Ihres Unternehmens entspricht. Während des Planungsprozesses für Ihre i5/OS-Einzelanmeldungsumgebung müssen Sie verschiedene Entscheidungen treffen. Hierzu zählt z. B. die Frage, ob Richtlinienzuordnungen erstellt werden sollen. Bei dieser Entscheidung sind die Sicherheitsanforderungen Ihres Unternehmens von entscheidender Bedeutung.

Im Folgenden sind verschiedene Ressourcen aufgeführt, die Sie zum Abschluss der Planungsphase Ihrer Einzelanmeldungsumgebung verwenden können:

Nachdem Sie die Planung Ihrer Einzelanmeldungsumgebung erfolgreich abgeschlossen haben, können Sie nun mit der Konfiguration dieser Umgebung fortfahren.

Zugehörige Tasks

„Einzelanmeldung konfigurieren" auf Seite 87
Zum Konfigurieren einer Einzelanmeldungsumgebung müssen Sie eine kompatible Authentifizierungsmethode verwenden und EIM zum Erstellen und Verwalten der Benutzerprofile und Identitätsabgleiche benutzen.

Zugehörige Informationen

EIM für i5/OS planen

Voraussetzungen zur Konfiguration einer Einzelanmeldungsumgebung

Ihr System muss die folgenden Hardware- und Softwarevoraussetzungen erfüllen, bevor Sie eine Einzelanmeldungsumgebung implementieren können.

Voraussetzungen für i5/OS ab V5R4

Anmerkung: Die Einzelanmeldung steht auch unter OS/400 V5R2 und i5/OS V5R3 zur Verfügung. Die detaillierten Informationen zur Konfiguration, die im vorliegenden Thema enthalten sind, beziehen sich jedoch auf die neue Einzelanmeldungsfunktion, die nur unter i5/OS ab V5R4 zur Verfügung steht und z. B. die Definition von Richtlinienzuordnungen erlaubt.

Um eine Einzelanmeldungsumgebung zu erstellen, müssen die folgenden Voraussetzungen erfüllt sein:
- i5/OS ab V5R4 ist auf dem System installiert.
- Die neuesten PTFs (vorläufigen Programmkorrekturen) für i5/OS wurden angelegt.
- System i Access für Windows ab V5R4 ist auf dem System installiert.
- Das neueste Service-Pack für System i Access für Windows ist auf dem System installiert.

  Informationen zum Anfordern des neuesten Service-Packs finden Sie auf der Website für System i Access.
- i5/OS Host-Server (5761-SS1 Option 12) ist auf dem System installiert.
- Qshell Interpreter (5761-SS1 Option 30) ist auf dem System installiert.
- TCP/IP und die Basissystemsicherheitsfunktion wurden konfiguriert.

Anmerkung: 5722 ist der Produktcode für i5/OS-Optionen und -Produkte mit einer Version vor V6R1. Wenn Sie im System i Navigator den Assistenten für die Funktionssynchronisation einsetzen wollen, um eine vorhandene Einzelanmeldungskonfiguration an mehrere andere Systeme weiterzugeben, müssen Sie die beteiligten Systeme für die Verwendung von SSL (Secure Sockets Layer) konfigurieren, um die Übertragung sensibler Konfigurationsdaten (z. B. der Kennwörter) über ein gesichertes Medium durchzuführen.

Voraussetzungen für den Client-PC

Um eine Einzelanmeldungsumgebung zu erstellen, müssen die folgenden Voraussetzungen erfüllt sein:

- Auf dem System wird das Betriebssystem Microsoft Windows 2000, Microsoft Windows XP oder Microsoft Windows Vista Ultimate Business verwendet.
- System i Access für Windows ab V5R4 ist auf dem System installiert.
  - Auf dem Administrator-PC für die Einzelanmeldung ist die Unterkomponente "Netzwerk" des System i Navigator installiert.
  - Auf dem Administrator-PC für die Einzelanmeldung ist die Unterkomponente "Sicherheit" des System i Navigator installiert.
- Das neueste Service-Pack für System i Access für Windows ist auf dem System installiert.

  Informationen zum Anfordern des neuesten Service-Packs finden Sie auf der Website für System i Access.
- TCP/IP ist auf dem System konfiguriert.

Voraussetzungen für den Microsoft Windows-Server

Um eine Einzelanmeldungsumgebung zu erstellen, müssen die folgenden Voraussetzungen erfüllt sein:

- Die Hardwareplanung und die Konfiguration der entsprechenden Einheiten ist abgeschlossen.
- Auf dem System wird das Betriebssystem Windows 2000 Server, Windows Server 2003 oder Microsoft Windows Vista Ultimate Business verwendet.
- Die Windows-Unterstützungstools (beinhalten das Tool ktpass) sind installiert.
- TCP/IP ist auf dem System konfiguriert.
- Die Windows 2000-Domäne ist konfiguriert.
- Die Benutzer innerhalb des Netzwerks werden mit Hilfe von Microsoft Windows Active Directory zu einer Windows 2000-Domäne hinzugefügt.

Sie können die bereitgestellten Planungsarbeitsblätter für die Einzelanmeldung verwenden, um die benötigten Informationen zusammenzustellen. Diese Arbeitsblätter können auch als Entscheidungshilfe bei der Implementierung Ihrer Einzelanmeldungsumgebung eingesetzt werden. Jedes Arbeitsblatt enthält eine Liste der Tasks, die Sie ausführen müssen.

Planungsarbeitsblätter für die Einzelanmeldung

Füllen Sie die folgenden Arbeitsblätter aus, um zu überprüfen, ob Ihr System alle Voraussetzungen für die Einzelanmeldung erfüllt und ob Sie alle Faktoren Ihres Systems und seiner Sicherheitsanforderungen berücksichtigt haben.

Bevor Sie diese Planungsarbeitsblätter für die Konfiguration benutzen, müssen Sie die Planung der gesamten Einzelanmeldungsimplementierung durchführen. Mit den folgenden Planungsarbeitsblättern für die Konfiguration können Sie überprüfen, ob Ihr System alle Voraussetzungen erfüllt und ob Sie alle Faktoren Ihrer System i-Umgebung berücksichtigt haben.

Planungsarbeitsblatt für die Einzelanmeldungsvoraussetzungen

Das hier dargestellte, detaillierte Arbeitsblatt unterstützt Sie dabei festzustellen, ob Ihr System alle Hardware- und Softwarevoraussetzungen erfüllt, um die Implementierung der Einzelanmeldung durchzuführen. Um eine erfolgreiche Implementierung sicherzustellen, sollten Sie für alle im Arbeitsblatt aufgeführten, vorausgesetzten Elemente die Antwort **Ja** geben können. Außerdem sollten Sie alle Informationen zusammenstellen, die zum Ausfüllen der Arbeitsblätter erforderlich sind, bevor Sie die Konfigurations-Tasks ausführen.

Tabelle 11. Arbeitsblatt für die Einzelanmeldungsvoraussetzungen

Arbeitsblatt für Voraussetzungen	Antworten
Arbeitet Ihr System mit i5/OS ab V5R4?	
Sind die folgenden Optionen und Lizenzprogramme auf Ihrem Server installiert? • i5/OS Host-Server (5761-SS1 Option 12) • Qshell Interpreter (5761-SS1 Option 30) • System i Access für Windows (5761-XE1) **Anmerkung:** 5722 ist der Produktcode für i5/OS-Optionen und -Produkte mit einer Version vor V6R1.	
Ist eine Anwendung installiert, die auf allen PCs, die sich in der Einzelanmeldungsumgebung befinden werden, für die Einzelanmeldung aktiviert ist? **Anmerkung:** Für die hier aufgeführten Szenarios wurde auf allen PCs System i Access für Windows (5761-XE1) installiert.	
Ist der System i Navigator auf dem Administrator-PC installiert? • Ist die Unterkomponente "Sicherheit" des System i Navigator auf dem PC des Administrators installiert? • Ist die Unterkomponente "Netzwerk" des System i Navigator auf dem PC des Administrators installiert?	
Ist das neueste System i Access für Windows-Service-Pack installiert? Informationen zum neuesten Service-Pack finden Sie auf der Webseite für System i Access .	
Verfügt der Administrator über die Sonderberechtigungen *SECADM, *ALLOBJ und *IOSYSCFG?	
Fungiert eines der folgenden Systeme als Kerberos-Server (auch als KDC bezeichnet)? Wenn ja, geben Sie an, um welches System es sich handelt. 1. Windows 2000-Server **Anmerkung:** Microsoft Windows 2000-Server verwendet als Standardsicherheitsmechanismus die Kerberos-Authentifizierung. 2. Windows(R) Server 2003 3. i5/OS PASE (ab V5R3) 4. AIX-Server 5. z/OS	
Sind alle PCs Ihres Netzwerks in einer Windows 2000-Domäne konfiguriert?	
Wurden die neuesten PTFs (vorläufigen Programmkorrekturen) angelegt?	
Beträgt die Abweichung zwischen der Systemzeit des System i-Modells und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung größer, lesen Sie die Informationen in Systemzeiten synchronisieren.	

Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung

Anhand des folgenden Planungsarbeitsblattes für die Konfiguration können Sie überprüfen, ob Ihr System alle Hardware- und Softwarevoraussetzungen für die Einzelanmeldung erfüllt. Darüber hinaus können Sie anhand dieses Arbeitsblattes feststellen, ob Sie alle Konfigurations-Tasks für EIM (Enterprise

Identity Mapping) und den Netzwerkauthentifizierungsservice ausgeführt haben, die zur erfolgreichen Implementierung einer Einzelanmeldungsumgebung erforderlich sind.

Anmerkung: Das Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung unterstützt Sie bei der Implementierung einer Einzelanmeldungsumgebung, die auf EIM (Enterprise Identity Mapping) und dem Netzwerkauthentifizierungsservice basiert. Wenn Sie ein anderes Authentifizierungsverfahren wie z. B. IBM Tivoli Directory Server for i5/OS oder digitale Zertifikate einsetzen möchten, müssen Sie bestimmte Elemente dieses Arbeitsblattes an Ihre individuellen Gegebenheiten anpassen.

Tabelle 12. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung

Planungsarbeitsblatt für die Konfiguration	**Antworten**
Verwenden Sie die folgenden Informationen, um den EIM-Konfigurationsassistenten auszuführen:	
Wie möchten Sie EIM auf Ihrem System konfigurieren? • System zu einer vorhandenen Domäne hinzufügen • Neue Domäne erstellen und System hinzufügen	
Wo möchten Sie die EIM-Domäne konfigurieren?	
Möchten Sie den Netzwerkauthentifizierungsservice konfigurieren?	
Der Assistent für den Netzwerkauthentifizierungsservice wird über den EIM-Konfigurationsassistenten gestartet. Verwenden Sie die folgenden Informationen, um den Assistenten für den Netzwerkauthentifizierungsservice auszuführen: **Anmerkung:** Der Assistent für den Netzwerkauthentifizierungsservice kann auch unabhängig vom EIM-Konfigurationsassistenten gestartet werden.	
Wie lautet der Name des Kerberos-Standard-Realms, zu dem Ihr System gehören soll? **Anmerkung:** Eine Windows 2000-Domäne ist mit einem Kerberos-Realm vergleichbar. Microsoft Windows Active Directory verwendet als Standardsicherheitsmechanismus die Kerberos-Authentifizierung.	
Verwenden Sie Microsoft Active Directory?	
Wie heißt der Kerberos-Server, der auch als KDC (Key Distribution Center) bezeichnet wird, für diesen Kerberos-Standard-Realm? An welchem Port ist der Kerberos-Server empfangsbereit?	
Möchten Sie einen Kennwortserver für diesen Standard-Realm konfigurieren? Wenn ja, beantworten Sie die folgenden Fragen: Wie lautet der Name des Kennwortservers für diesen Kerberos-Server? An welchem Port ist der Kennwortserver empfangsbereit?	
Für welche Services sollen Chiffrierschlüsseleinträge erstellt werden? • i5/OS-Kerberos-Authentifizierung • LDAP • IBM HTTP-Server für i5/OS • i5/OS NetServer • NFS-Server (Network File System)	
Wie lautet das Kennwort für Ihre(n) Service-Principal(s)?	
Möchten Sie eine Stapeldatei erstellen, um das Hinzufügen der Service-Principals für System A zum Kerberos-Register zu automatisieren?	
Möchten Sie für die i5/OS-Service-Principals in der Stapeldatei Kennwörter hinzufügen?	

Tabelle 12. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung (Forts.)

Wenn Sie den Assistenten für den Netzwerkauthentifizierungsservice verlassen, gelangen Sie in den EIM-Konfigurationsassistenten zurück. Verwenden Sie die folgenden Informationen, um den EIM-Konfigurationsassistenten auszuführen:	
Geben Sie Benutzerinformationen an, die der Assistent bei der Konfiguration des Directory-Servers verwenden soll. Dies ist der Benutzer der Verbindung. Sie müssen die Portnummer, den registrierten Namen (Distinguished Name, DN) des Administrators und ein Kennwort für den Administrator angeben.	
Wie lautet der Name der EIM-Domäne, die Sie erstellen möchten?	
Möchten Sie einen übergeordneten registrierten Namen für die EIM-Domäne angeben?	
Welche Benutzerregister möchten Sie zur EIM-Domäne hinzufügen?	
Welchen EIM-Benutzer soll System A bei der Ausführung von EIM-Operationen verwenden? Dies ist der Systembenutzer.	
Nach Abschluss des EIM-Konfigurationsassistenten müssen Sie die folgenden Informationen verwenden, um die restlichen Arbeitsschritte auszuführen, die zur Konfiguration der Einzelanmeldung erforderlich sind:	
Wie lautet der Name des i5/OS-Benutzerprofils des Benutzers?	
Wie lautet der Name der EIM-Kennung, die Sie erstellen möchten?	
Welche Zuordnungen sollen erstellt werden?	
Wie lautet der Name des Benutzerregisters, das den Kerberos-Principal enthält, für den die Quellenzuordnung erstellt werden soll?	
Wie lautet der Name des Benutzerregisters, das das i5/OS-Benutzerprofil enthält, für das die Zielzuordnung erstellt werden soll?	
Welche Informationen müssen Sie angeben, um den EIM-Identitätsabgleich zu testen?	

Zugehörige Tasks

„Einzelanmeldung konfigurieren"
Zum Konfigurieren einer Einzelanmeldungsumgebung müssen Sie eine kompatible Authentifizierungsmethode verwenden und EIM zum Erstellen und Verwalten der Benutzerprofile und Identitätsabgleiche benutzen.

Einzelanmeldung konfigurieren

Zum Konfigurieren einer Einzelanmeldungsumgebung müssen Sie eine kompatible Authentifizierungsmethode verwenden und EIM zum Erstellen und Verwalten der Benutzerprofile und Identitätsabgleiche benutzen.

Bei den i5/OS-Einzelanmeldungslösungen wird als Authentifizierungsmethode der Netzwerkauthentifizierungsservice (Kerberos) verwendet.

Da die Konfiguration einer Einzelanmeldungsumgebung komplex sein kann, sollten Sie eventuell eine Testumgebung erstellen, bevor Sie die Einzelanmeldung unternehmensweit implementieren. Das Szenario zur Erstellung einer Einzelanmeldungstestumgebung veranschaulicht die Konfiguration einer solchen Testumgebung, so dass Sie sich mit den Planungsanforderungen zur Implementierung der Einzelanmeldung sowie der Funktionsweise und den Einsatzmöglichkeiten einer solchen Umgebung besser vertraut machen können.

Nachdem Sie die gewünschte Konfiguration in der Testumgebung überprüft haben, können Sie die hierbei gewonnenen Erkenntnisse bei der Planung der unternehmensweiten Implementierung einer Einzelanmeldungslösung anwenden. Wenn Sie mehr über die erweiterten Konfigurationsoptionen erfahren möchten, die Sie bei der Implementierung einer Einzelanmeldungsumgebung verwenden können, sollten Sie das Szenario zum Aktivieren der Einzelanmeldung für i5/OS durcharbeiten.

Nachdem Sie sich mit diesem und den anderen Einzelanmeldungsszenarios vertraut gemacht haben, können Sie mit Hilfe der Planungsarbeitsblätter für die Einzelanmeldung einen fundierten Implementierungsplan für die Einzelanmeldung erstellen, der optimal auf der Erfordernisse Ihres Unternehmens abgestimmt ist. Nachdem Sie die Daten dieser Planungsarbeitsblätter erarbeitet haben, sind Sie bereit, mit dem Konfigurationsprozess fortzufahren.

Die Konfiguration der Einzelanmeldung umfasst eine Reihe detaillierter Konfigurationsschritte. Hier werden die allgemeinen Konfigurations-Tasks für die Einzelanmeldung beschrieben und Links zu detaillierteren Konfigurationsinformationen für EIM und den Netzwerkauthentifizierungsservice bereitgestellt, die Sie bei Bedarf nutzen können.

Gehen Sie wie folgt vor, um eine Einzelanmeldungsumgebung zu konfigurieren:

1. Erstellen Sie die Windows 2000-Domäne.
   a. Konfigurieren Sie auf dem Active Directory-Server das Key Distribution Center (KDC).

      Anmerkung: Sie können die KDC unter i5/OS PASE erstellen, anstatt eine Windows-Domäne zu erstellen und die KDC auf einem Windows-Server auszuführen.
   b. Fügen Sie i5/OS-Service-Principals zum Kerberos-Server hinzu.
   c. Erstellen Sie für jeden Kerberos-Benutzer, der die Einzelanmeldungsumgebung nutzen soll, ein Ausgangsverzeichnis.
   d. Überprüfen Sie die TCP/IP-Domäneninformationen.
2. Erstellen Sie eine EIM-Domäne, indem Sie auf einem Server sowohl den Assistenten für den Netzwerkauthentifizierungsservice als auch den EIM-Konfigurationsassistenten ausführen. Nachdem Sie diese Assistenten ausgeführt haben, sind die folgenden Maßnahmen erfolgreich abgeschlossen:
   a. Konfiguration der i5/OS-Schnittstellen für die Annahme von Kerberos-Tickets.
   b. Konfiguration des Directory-Servers auf dem System i-System als EIM-Domänencontroller.
   c. Erstellung einer EIM-Domäne.
   d. Konfiguration einer Benutzeridentität, die von i5/OS und i5/OS-Anwendungen zur Ausführung von EIM-Operationen verwendet werden kann.
   e. Hinzufügung einer Registerdefinition für das lokale i5/OS-Register und das lokale Kerberos-Register (sofern konfiguriert) zu EIM.
3. Wenn Sie mit Servern arbeiten, die i5/OS ab V5R3 benutzen, sollten Sie das Szenario: Netzwerkauthentifizierungsservice und EIM an mehrere Systeme weitergeben lesen. Dort wird detailliert beschrieben, wie der Assistent für die Funktionssynchronisation im System i Navigator zur Weitergabe einer Einzelanmeldungskonfiguration an mehrere Server in einer i5/OS-Umgebung mit mehreren Releases verwendet werden kann. Administratoren können auf diese Weise den Zeitaufwand reduzieren, indem die Einzelanmeldung nur ein einziges Mal konfiguriert und dann an alle Systeme weitergegeben wird, anstatt jedes System einzeln zu konfigurieren.
4. Schließen Sie die Konfiguration des Netzwerkauthentifizierungsservice ab. Auf der Basis des Implementierungsplans für die Einzelanmeldung können Sie ein Ausgangsverzeichnis für die Benutzer Ihrer Server erstellen.
5. Führen Sie auf der Basis des Implementierungsplans eine Anpassung Ihrer EIM-Umgebung durch, indem Sie Zuordnungen für die Benutzeridentitäten Ihres Unternehmens definieren.
   a. Konfigurieren Sie weitere Server zur Nutzung der EIM-Domäne.
   b. Erstellen Sie die erforderlichen EIM-Kennungen und -Kennungszuordnungen.
   c. Fügen Sie bei Bedarf weitere Registerdefinitionen hinzu.

d. Erstellen Sie die erforderlichen Richtlinienzuordnungen.

6. Testen Sie die Einzelanmeldungskonfiguration.

   Um zu überprüfen, ob der Netzwerkauthentifizierungsservice und EIM korrekt konfiguriert wurden, müssen Sie sich mit einer Benutzer-ID beim System anmelden und anschließend den System i Navigator öffnen. Wird keine i5/OS-Anmeldeaufforderung angezeigt, konnte EIM die Zuordnung des Kerberos-Principals zu einer ID der Domäne erfolgreich ausführen.

   Anmerkung: Wenn der Test der Einzelanmeldungskonfiguration fehlschlägt, dann ist Ihnen bei der Konfiguration möglicherweise ein Fehler unterlaufen. Sie können dann eine Fehlerbehebung für die Einzelanmeldung durchführen. Lesen Sie hierzu die Informationen zur Erkennung und Behebung der gelegentlich in einer Einzelanmeldungskonfiguration auftretenden Fehler.

Zugehörige Konzepte

„Szenario: Einzelanmeldungstestumgebung erstellen" auf Seite 12
In diesem Szenario wird dargestellt, wie der Netzwerkauthentifizierungsservice und EIM konfiguriert werden müssen, um eine Basistestumgebung für die Einzelanmeldung zu erstellen. Verwenden Sie dieses Szenario, um sich vorab in einer isolierten Testumgebung einen grundlegenden Überblick über die Arbeitsschritte zu verschaffen, die zur Konfiguration einer Einzelanmeldungsumgebung auszuführen sind, bevor Sie die Einzelanmeldung unternehmensweit implementieren.

„Szenario: Einzelanmeldung für i5/OS aktivieren" auf Seite 26
In diesem Szenario wird dargestellt, wie der Netzwerkauthentifizierungsservice und EIM konfiguriert werden müssen, um in einem Unternehmen eine systemübergreifende Einzelanmeldungsumgebung zu erstellen. Dieses Szenario baut auf den Konzepten und Tasks auf, die im vorherigen Szenario dargestellt wurden, in dem die Erstellung einer einfachen Einzelanmeldungstestumgebung erläutert wurde.

„Planungsarbeitsblätter für die Einzelanmeldung" auf Seite 84
Füllen Sie die folgenden Arbeitsblätter aus, um zu überprüfen, ob Ihr System alle Voraussetzungen für die Einzelanmeldung erfüllt und ob Sie alle Faktoren Ihres Systems und seiner Sicherheitsanforderungen berücksichtigt haben.

Zugehörige Tasks

„Einzelanmeldung planen" auf Seite 83
Während des Planungsprozesses für die Einzelanmeldung werden die Software- und Hardwarevoraussetzungen identifiziert, die zur Implementierung der Einzelanmeldung in Ihrem Unternehmen erfüllt werden müssen.

„Fehler bei der Einzelanmeldung beheben" auf Seite 90
Anhand der folgenden Verfahren zur Fehlerbehebung können einige der gelegentlich auftretenden Probleme bei der Konfiguration und beim Einsatz einer Einzelanmeldungsumgebung behoben werden.

Zugehörige Informationen

Netzwerkauthentifizierungsservice konfigurieren

Enterprise Identity Mapping konfigurieren

Einzelanmeldung verwalten

Zur Verwaltung einer Einzelanmeldungsumgebung können Sie den Netzwerkauthentifizierungsservice sowie Enterprise Identity Mapping (EIM) verwenden.

Nach der Implementierung einer Einzelanmeldungsumgebung müssen Sie möglicherweise verschiedene Verwaltungsaufgaben ausführen, um die Übereinstimmung dieser Umgebung mit den geltenden Sicherheitsrichtlinien zu gewährleisten, so wie dies auch bei allen anderen Komponenten Ihres Netzwerks erforderlich wäre.

Weitere Informationen zur Verwaltung dieser Funktionen für die Pflege Ihrer Einzelanmeldungsumgebung finden Sie in den folgenden Abschnitten:

- Netzwerkauthentifizierungsservice verwalten

  Hier finden Sie Informationen zu allgemeinen Verwaltungsaufgaben für den Netzwerkauthentifizierungsservice, z. B. zum Synchronisieren der Systemzeiten, zum Hinzufügen und Löschen von Realms sowie zum Hinzufügen eines Kerberos-Servers etc.
- Enterprise Identity Mapping verwalten

  Dieser Abschnitt enthält Informationen zu allgemeinen EIM-Verwaltungsaufgaben wie z. B. zur Verwaltung von Zuordnungen, zu Kennungen und Registerdefinitionen usw.

Wenn beim Arbeiten in der Einzelanmeldungsumgebung Probleme auftreten, können Sie für die Einzelanmeldung eine Fehlerbehebung durchführen.

Zugehörige Tasks

„Fehler bei der Einzelanmeldung beheben"
Anhand der folgenden Verfahren zur Fehlerbehebung können einige der gelegentlich auftretenden Probleme bei der Konfiguration und beim Einsatz einer Einzelanmeldungsumgebung behoben werden.

Fehler bei der Einzelanmeldung beheben

Anhand der folgenden Verfahren zur Fehlerbehebung können einige der gelegentlich auftretenden Probleme bei der Konfiguration und beim Einsatz einer Einzelanmeldungsumgebung behoben werden.

Sie können verschiedene Maßnahmen ergreifen, um Probleme zu vermeiden, die in einer i5/OS-Einzelanmeldungskonfiguration auftreten können:

1. Sie können überprüfen, ob Ihr Netzwerkauthentifizierungsservice korrekt arbeitet, indem Sie den qshell-Befehl `kinit` ausführen. Hierzu müssen Sie die qshell-Umgebung aufrufen und dort den Befehl `kinit -k <servicename>` eingeben. Dieser Befehl arbeitet mit dem Chiffrierschlüsseleintrag, der vom Assistenten für den Netzwerkauthentifizierungsservice erstellt wurde. Dieser Befehl überprüft, ob das verschlüsselte Kennwort des Service mit dem Kennwort übereinstimmt, das im KDC (Key Distribution Center) gespeichert ist. Wenn die Ausführung dieses Befehls fehlschlägt, sollten Sie nochmals die Informationen zur Konfiguration des Netzwerkauthentifizierungsservice aufrufen.
2. Überprüfen Sie die Konfigurationen für die Auflösung von Hostnamen einschließlich der DNS-Server.
3. Überprüfen Sie die Daten zur EIM-Systemkonfiguration auf allen i5/OS-Systemen, auf denen Abgleichsuchoperationen ausgeführt werden.
   a. Öffnen Sie den System i Navigator.
   b. Wählen Sie das System aus, und erweitern Sie die Einträge für **Netzwerk → Enterprise Identity Mapping → Konfiguration**.
   c. Klicken Sie mit der rechten Maustaste auf den Ordner **Konfiguration**, und wählen Sie dann **Eigenschaften** aus.
   d. Überprüfen Sie auf der Seite **Domäne** die Einstellungen für die Domänenverbindung, und klicken Sie dann auf **Konfiguration prüfen**. Daraufhin wird überprüft, ob der Domänencontroller aktiv ist und ob die Einstellungen des Domänencontrollers korrekt sind.
   e. Klicken Sie auf der Seite **Systembenutzer** auf **Verbindung prüfen**, um festzustellen, ob der Systembenutzer korrekt angegeben wurde.
4. Überprüfen Sie die definierten EIM-Zuordnungen, indem Sie die Funktion zum Testen der EIM-Abgleiche verwenden, um festzustellen, ob die von Ihnen definierten Zuordnungen zur Durchführung der gewünschten Abgleichsoperationen führen.
5. Wenn Ihre Einzelanmeldungskonfiguration ein Netzwerk mit mehreren Ebenen umfasst, müssen Sie überprüfen, ob die Ticketdelegierung für den Server der mittleren Ebene aktiviert wurde. Dies ist erforderlich, damit der Server der mittleren Ebene die Benutzerberechtigungen an den nächsten Server weiterleiten kann. Sie können die Ticketdelegierung auf dem Active Directory- oder auf dem Kerb-

eros-Server aktivieren. Als Beispiel für ein Netzwerk mit mehreren Ebenen kann ein PC aufgeführt werden, der bei einem bestimmten Server authentifiziert wird und dann eine Verbindung zu einem anderen Server herstellt.

Wenn nach Überprüfung der oben aufgeführten Schritte weiterhin Probleme mit der Einzelanmeldung auftreten, sollten Sie anhand der folgenden Tabelle feststellen, ob es eventuell bereits Lösungen für die in Ihrer Konfiguration aufgetretenen Fehler gibt:

Tabelle 13. Tabelle zur Fehlerbehebung

Symptome	Lösungen
Probleme bei der Auflösung von Hostnamen	
Sie können in Ihrer Einzelanmeldungsumgebung keine Verbindung zu i5/OS-Systemen herstellen.	• Dieser Fehler kann auf ein Problem bei der Auflösung von Hostnamen zurückzuführen sein. Überprüfen Sie, ob bei der Auflösung am PC und auf dem System i-Modell derselbe Hostname ermittelt wird. Überprüfen Sie die Konfigurationen für die Auflösung von Hostnamen einschließlich des DNS-Servers. Weitere Informationen hierzu finden Sie unter Hinweise zur Auflösung von Hostnamen. • Dieser Fehler kann auf ein Problem bei der Konfiguration des Netzwerkauthentifizierungsservice zurückzuführen sein. Weitere Informationen hierzu finden Sie unter Fehlerbehebung im i5/OS Information Center.
Das Dienstprogramm NSLOOKUP kann die Hostnamenauflösung nicht durchführen, wenn eine IP-Adresse angegeben wird, während Sie überprüfen, ob die Hostnamenauflösung auf dem System i-System das gleiche Ergebnis ermittelt wie die Hostnamenauflösung auf einem Client-PC.	Das Dienstprogramm NSLOOKUP verwendet den momentan konfigurierten DNS, um IP-Adressen auf der Basis von Hostnamen bzw. Hostnamen auf der Basis von IP-Adressen aufzulösen. Wenn die Auflösung eines Hostnamens auf der Basis einer IP-Adresse fehlschlägt, dann ist dieser Fehler mit großer Wahrscheinlichkeit darauf zurückzuführen, dass im DNS ein PTR-Satz fehlt. Wenden Sie sich an den DNS-Administrator, und bitten Sie diesen, einen PTR-Satz für diese IP-Adresse hinzuzufügen.
EIM-Konfigurationsprobleme	
Die EIM-Zuordnungen arbeiten nicht in der gewünschten Weise. In bestimmten Fällen können Sie sich mit dem System i Navigator nicht beim System anmelden, wenn Sie mit der Kerberos-Authentifizierung arbeiten.	• Der Domänencontroller ist inaktiv. Aktivieren Sie den Domänencontroller. • Die EIM-Konfiguration auf den Systemen, auf denen Sie die Kerberos-Authentifizierung oder die Herstellung von Zuordnungen anfordern, ist nicht korrekt. Überprüfen Sie Ihre EIM-Konfiguration. Erweitern Sie auf dem System, bei dem Sie sich authentifizieren möchten, die Einträge für **Netzwerk → Enterprise Identity Mapping → Konfiguration**. Klicken Sie mit der rechten Maustaste auf den Ordner **Konfiguration**, und wählen Sie dann **Eigenschaften** aus. Wählen Sie anschließend **Netzwerk → Enterprise Identity Mapping → Konfiguration** aus.
EIM-Konfigurationsprobleme	

Tabelle 13. Tabelle zur Fehlerbehebung (Forts.)

Symptome	Lösungen
Die EIM-Zuordnungen arbeiten nicht in der gewünschten Weise. In bestimmten Fällen können Sie sich mit dem System i Navigator nicht beim System anmelden, wenn Sie mit der Kerberos-Authentifizierung arbeiten. (Fortsetzung)	• 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 Kennwörter im Directory-Server aktualisiert werden, müssen diese Änderungen immer auch in der Systemkonfiguration nachvollzogen werden. - Klicken Sie auf **Verbindung prüfen**, um die Richtigkeit der Benutzerinformationen zu bestätigen. • Die EIM-Domänenkonfiguration ist nicht korrekt: **Anmerkung:** Sie können die EIM-Abgleiche testen und auf diese Weise feststellen, ob die Zuordnungen für Ihre EIM-Domäne richtig konfiguriert sind. – 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 (siehe hierzu Alle Kennungszuordnungen für eine EIM-Kennung anzeigen) an, um die Zuordnungen für eine bestimmte Kennung zu überprüfen. – Eine Richtlinienzuordnung ist falsch konfiguriert. Zeigen Sie alle Richtlinienzuordnungen für eine Domäne (siehe hierzu Alle Richtlinienzuordnungen für eine Domäne anzeigen) an, um die Quellen- und Zielinformationen für alle in der Domäne definierten Richtlinienzuordnungen zu überprüfen. – Die ausgeführten Abgleichssuchoperationen geben mehrere Zielidentitäten zurück. Dies deutet darauf hin, dass mehrdeutige Zuordnungen konfiguriert sind. Sie müssen die EIM-Abgleiche testen, um festzustellen, welche Abgleiche nicht korrekt sind. – 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. • Die EIM-Unterstützung ist nicht aktiviert. – EIM wurde auf dem System inaktiviert. Überprüfen Sie, ob auf der Seite **Domäne** für die Eigenschaften der EIM-Konfiguration des Systems **EIM-Operationen für dieses System aktivieren** ausgewählt ist. Erweitern Sie hierzu die Einträge für **Netzwerk → Enterprise Identity Mapping → Konfiguration → Eigenschaften**. – 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 Abgleichsuchen und Richtlinienzuordnungen für Zielregister aktivieren.
Probleme bei der Konfiguration des Netzwerkauthentifizierungsservice	

Tabelle 13. Tabelle zur Fehlerbehebung (Forts.)

Symptome	Lösungen
Nachdem Sie die Erstellung einer Chiffrierschlüsselliste angefordert haben (`keytab list`), wird kein Chiffrierschlüsseleintrag (`keytab entry`) zurückgegeben.	• Dieser Fehler kann auf ein Problem bei der Auflösung von Hostnamen auf dem System i-Modell zurückzuführen sein. Wenn Sie mit einer Hosttabelle arbeiten, führen Sie den Befehl `CFGTCP` (TCP/IP konfigurieren), Auswahl 10 (Mit TCP/IP-Hosttabelleneinträgen arbeiten) aus, und überprüfen Sie, ob der Name des primären Hosts als erster Eintrag für die IP-Adresse des Servers aufgelistet ist. • Überprüfen Sie die Konfigurationen für die Auflösung von Hostnamen einschließlich des DNS-Servers. Weitere Informationen hierzu finden Sie unter Hinweise zur Auflösung von Hostnamen.
Es können keine Benutzerverbindungen zum System hergestellt werden.	Das Herstellen einer Benutzerverbindung zu einem System schlägt möglicherweise fehl, wenn die EIM-Registerdefinition für das Kerberos-Register fälschlicherweise so definiert wurde, dass die Groß-/Kleinschreibung beachtet werden muss. In diesem Fall müssen Sie das Kerberos-Register löschen und anschließend erneut erstellen. **Anmerkung:** Durch diesen Arbeitsschritt gehen alle Zuordnungen verloren, die für dieses Register definiert wurden. Diese müssen neu erstellt werden.
Der Benutzer erhält die Nachricht, dass ein falsches Kennwort verwendet wurde, wenn er die Konfiguration des Netzwerkauthentifizierungsservice überprüft.	Das im Key Distribution Center (KDC) gespeicherte Kennwort des Service stimmt nicht mit dem Kennwort überein, das für den Service im Chiffrierschlüssel definiert wurde. Aktualisieren Sie den Chiffrierschlüsseleintrag, indem Sie mit dem Befehl zum Hinzufügen eines Chiffrierschlüssels das Kennwort des Service im KDC aktualisieren.
Der Benutzer erhält die folgende Nachricht: `Name des Standardcaches für Berechtigungsnachweise kann nicht abgerufen werden.`	Überprüfen Sie, ob für den Benutzer, der den Befehl `kinit` ausführt, ein Ausgangsverzeichnis (`/home/<benutzerprofil>` vorhanden ist.
Der Benutzer erhält die folgende Nachricht: `Antwort ist für Datagramm zu groß.`	Aktualisieren Sie die Konfiguration des Netzwerkauthentifizierungsservice, so dass als Datenübertragungsprotokoll TCP verwendet wird. 1. Wählen Sie im System i Navigator das System aus, das die Nachricht ausgegeben hat. 2. Wählen Sie **Sicherheit → Eigenschaften für Netzwerkauthentifizierungsservice** aus. 3. Wählen Sie auf der Seite **Allgemein** die Auswahl **TCP verwenden** aus. Klicken Sie anschließend auf **OK**.
Gelegentlich auftretende Fehler	

Tabelle 13. Tabelle zur Fehlerbehebung (Forts.)

Symptome	Lösungen
Wenn Sie versuchen, die Einzelanmeldung zu benutzen, erhalten Sie die Fehlernachricht CWBSY10XX.	• Verwenden Sie den Hilfetext, der zur Nachricht angezeigt werden kann, um das Problem zu beheben. • Verwenden Sie die detaillierte System Access-Tracefunktion, um festzustellen, ob das korrekte Kerberos-Ticket abgerufen wurde. • Laden Sie das Microsoft-Dienstprogramm kerbtray herunter, um zu überprüfen, ob der Benutzer über die erforderlichen Kerberos-Berechtigungsnachweise verfügt. • Wenn die Einzelanmeldung fehlschlägt, sollten Sie die Jobs für QZSOSIGN im Subsystem QUSRWRK prüfen. Durchsuchen Sie die Jobs nach der Nachricht CPD3E3F. Sobald Sie die Nachricht CPD3E3F gefunden haben, können Sie die Anweisungen zur Wiederherstellung lesen, die in der Nachricht angegeben sind. 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. • Wenn PC5250 fehlschlägt, müssen Sie Folgendes überprüfen: – Durchsuchen Sie die Jobs für QTVDEVICE nach der Nachricht CPD3E3F. – Überprüfen Sie den Systemwert QRMTSIGN, und stellen Sie fest, ob für diesen die Einstellung *VERIFY oder *SAMEPRF definiert wurde.

Zugehörige Informationen

RFC 1713: Tools for DNS debugging

Fehlerbehebung bei Enterprise Identity Mapping

Netzwerkauthentifizierungsservice konfigurieren

Hinweise zur Auflösung von Hostnamen

EIM-Abgleiche testen

Referenzinformationen für die Einzelanmeldung

In den veröffentlichten IBM Redbooks und in anderen Themensammlungen des Information Centers finden Sie Informationen, die zur Themensammlung für die Einzelanmeldung gehören. Sie können alle bereitgestellten PDF-Dateien anzeigen oder drucken.

IBM Redbooks

Die IBM Redbooks-Veröffentlichung IBM System i Security Guide for IBM i5/OS Version 5 Release 4 enthält ein Kapitel zur Authentifizierung mit Hilfe der Einzelanmeldung.

Weitere Informationen

- Enterprise Identity Mapping
- Netzwerkauthentifizierungsservice
- IBM Tivoli Directory Server for i5/OS
- Digital Certificate Manager

Haftungsausschluss für Programmcode

IBM erteilt Ihnen eine nicht ausschließliche Copyrightlizenz für die Nutzung aller Programmcodebeispiele, aus denen Sie ähnliche Funktionen generieren können, die an Ihre spezifischen Anforderungen angepasst sind.

Vorbehaltlich einer gesetzlichen Gewährleistung, die nicht ausgeschlossen werden kann, geben IBM oder ihre Programmentwickler und Lieferanten keine ausdrückliche oder implizite Gewährleistung für die Marktfähigkeit, die Eignung für einen bestimmten Zweck oder die Freiheit von Rechten Dritter in Bezug auf das Programm oder die technische Unterstützung.

Auf keinen Fall sind IBM oder ihre Programmentwickler und Lieferanten in folgenden Fällen haftbar, auch wenn auf die Möglichkeit solcher Schäden hingewiesen wurde:

1. Verlust oder Beschädigung von Daten;
2. direkte, unmittelbare, mittelbare oder sonstige Folgeschäden; oder
3. entgangener Gewinn, entgangene Geschäftsabschlüsse, Umsätze, Schädigung des guten Namens oder Verlust erwarteter Einsparungen.

Einige Rechtsordnungen erlauben nicht den Ausschluss oder die Begrenzung von Folgeschäden, so dass einige oder alle der obigen Einschränkungen und Ausschlüsse möglicherweise nicht anwendbar sind.

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 zuständigen 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 andere Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter 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 Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
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 werden lediglich als Service für den Kunden bereitgestellt 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 YBWA
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 Dokument aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von 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 kontrollierten 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 davon 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 von IBM dar, unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogramms 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, zu verwenden, zu 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. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch 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.

Informationen zu Programmierschnittstellen

In der vorliegenden Veröffentlichung werden vorgesehene Programmierschnittstellen dokumentiert, mit deren Hilfe Kunden Programme für den Zugriff auf die Services von IBM i5/OS schreiben können.

Marken

Folgende Namen sind Marken der IBM Corporation in den USA und/oder anderen Ländern:

AIX
Distributed Relational Database Architecture
DRDA

i5/OS
IBM
iSeries
NetServer
System i
Tivoli
WebSphere
z/OS

Adobe, das Adobe-Logo, PostScript und das PostScript-Logo sind Marken oder eingetragene Marken der Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Java und alle auf Java basierenden Marken und Logos sind Marken von Sun Microsystems, Inc. in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Hersteller 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 Veröffentlichungen. 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.