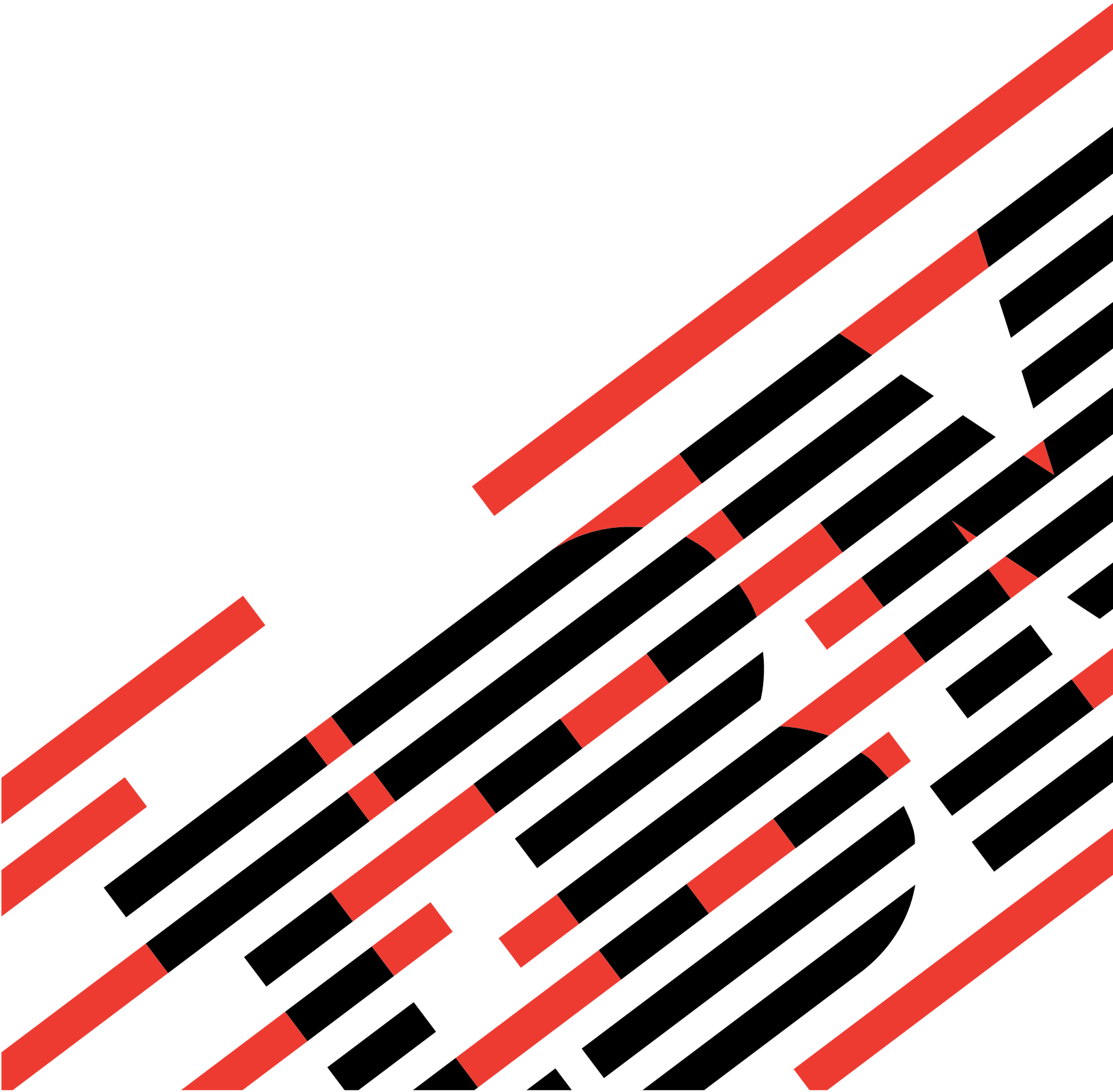
IBM

eserver

iSeries

# Netzwerkauthentifizierungsservice

*Version 5 Release 3*



IBM

@server

iSeries

# Netzwerkauthentifizierungsservice

*Version 5 Release 3*

**Anmerkung**

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen", auf Seite 157 gelesen werden.

- Die IBM Homepage finden Sie im Internet unter: **ibm.com**
- IBM und das IBM Logo sind eingetragene Marken der International Business Machines Corporation.
- Das e-business-Symbol ist eine Marke der International Business Machines Corporation.
- Infoprint ist eine eingetragene Marke der IBM.
- ActionMedia, LANDesk, MMX, Pentium und ProShare sind Marken der Intel Corporation in den USA und/oder anderen Ländern.
- C-bus ist eine Marke der Corollary, Inc. in den USA und/oder anderen Ländern.
- Java und alle auf Java basierenden Marken und Logos sind Marken der Sun Microsystems, Inc. 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.
- PC Direct ist eine Marke der Ziff Communications Company in den USA und/oder anderen Ländern.
- SET und das SET-Logo sind Marken der SET Secure Electronic Transaction LLC.
- UNIX ist eine eingetragene Marke der Open Group in den USA und/oder anderen Ländern.
- Marken anderer Unternehmen/Hersteller werden anerkannt.

**Fünfte Ausgabe (August 2005)**

| Diese Ausgabe bezieht sich auf Version 5, Release 3, Modifikation 2 des Betriebssystems IBM Operating System/400
| (Produktnummer 5722–SS1) und alle nachfolgenden Releases und Modifikationen, es sei denn, es erfolgen anders
| lautende Angaben in neuen Ausgaben. Diese Version kann nicht auf allen RISC-Modellen (Reduced Instruction Set
| Computer) ausgeführt werden. Auf CICS-Modellen ist sie nicht ausführbar.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
*IBM @server iSeries Network autentication service, Version 5 Release 3,*
herausgegeben von International Business Machines Corporation, USA



Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
August 2005

# Inhaltsverzeichnis

# Netzwerkauthentifizierungsservice

Der Netzwerkauthentifizierungsservice ermöglicht dem iSeries-Server und verschiedenen iSeries-Services, wie z. B. iSeries Access für Windows, für die Authentifizierung ein Kerberos-Ticket anstelle einer Kombination aus Benutzername und Kennwort zu verwenden. Das Kerberos-Protokoll, das vom Massachusetts Institute of Technology entwickelt wurde, erlaubt einem Principal (Benutzer oder Service) in einem unsicheren Netzwerk seine Identität gegenüber einem anderen Service nachzuweisen. Die Authentifizierung von Principals wird über einen zentralen Server, den so genannten Kerberos-Server, oder KDC (Key Distribution Center - Instanz zur Schlüsselverteilung) durchgeführt.

**Anmerkung:** In dieser Dokumentation wird durchgängig der generische Begriff „Kerberos-Server" verwendet.

Ein Benutzer authentifiziert sich mit einem Principal und einem Kennwort, das auf dem Kerberos-Server gespeichert ist. Wenn ein Principal authentifiziert ist, setzt der Kerberos-Server ein Ticket-granting Ticket (TGT) an den Benutzer ab. Wenn ein Benutzer auf eine Anwendung oder einen Service im Netzwerk zugreifen muss, sendet die Clientanwendung auf dem PC des Benutzers das TGT an den Kerberos-Server zurück, um ein Service-Ticket für den Zielservice bzw. die Zielanwendung zu erhalten. Die Kerberos-Clientanwendung sendet das Service-Ticket dann zur Authentifizierung an den Service oder die Anwendung. Wenn der Service oder die Anwendung das Ticket akzeptiert, wird ein Sicherheitskontext erstellt, und die Benutzeranwendung kann dann Daten mit einem Zielservice austauschen. Anwendungen können einen Benutzer authentifizieren und seine Identität sicher an andere Services im Netzwerk weiterleiten. Nachdem ein Benutzer bekannt ist, sind separate Funktionen erforderlich, um die Berechtigung des Benutzers zur Verwendung der Netzwerkressourcen zu überprüfen.

Der Netzwerkauthentifizierungsservice implementiert die folgenden Spezifikationen:

- Kerberos Version 5 Protocol Request for Comment (RFC) 1510
- Viele der verwendeten Kerberos-Protokoll-APIs, die in der Branche De-facto-Standard sind
- Generic Security Service (GSS)-APIs laut RFCs 1509, 1964 und 2743

Die i5/OS-Implementierung des Netzwerkauthentifizierungsservice kann mit Authentifizierungs- und Delegierungsservices sowie Services zur Sicherung und Datenvertraulichkeit verwendet werden, vorausgesetzt, diese sind mit den genannten RFCs und den APIs von Microsoft Windows 2000 Security Service Provider Interface (SSPI) kompatibel. Das Microsoft Windows Active Directory verwendet Kerberos als Standardsicherheitsmechanismus. Wenn Benutzer zum Microsoft Windows Active Directory hinzugefügt werden, entspricht deren Windows-Kennung einem Kerberos-Principal. Der Netzwerkauthentifizierungsservice gewährleistet die Interoperabilität mit dem Microsoft Windows Active Directory und dessen Implementierung des Kerberos-Protokolls.

| **Wichtig:** Einige iSeries-Schnittstellen verwenden möglicherweise immer noch „OS/400" anstelle von
| „i5/OS".

Der Abschnitt „Haftungsausschluss für Programmcode" auf Seite 2 enthält wichtige rechtliche Hinweise.

Neuerungen in V5R3
In diesem Abschnitt sind die funktionalen Erweiterungen des Netzwerkauthentifizierungsservice für dieses Release aufgelistet.

Thema drucken
In diesem Abschnitt wird beschrieben, wie Sie PDF-Versionen von diesen Informationen und entsprechenden Referenzinformationen drucken können, wie z. B. Aktivierung der Einzelanmeldung (Single Signon) und Enterprise Identity Mapping (EIM).

Szenarios
In diesem Abschnitt wird anhand von Beispielen veranschaulicht, wie Unternehmen den Netzwerkauthentifizierungsservice in ihren Netzwerken verwenden.

Konzepte
Dieser Abschnitt beschreibt Konzepte für den Netzwerkauthentifizierungsservice und Kerberos.

Netzwerkauthentifizierungsservice planen
In diesem Abschnitt ist die Hard- und Software aufgeführt, die für die Konfiguration des Netzwerkauthentifizierungsservice erforderlich ist.

Netzwerkauthentifizierungsservice konfigurieren
In diesem Abschnitt wird beschrieben, wie Sie den Assistenten für den Netzwerkauthentifizierungsservice verwenden, um einen iSeries-Server zur Teilnahme an einem Kerberos-Realm zu konfigurieren.

Netzwerkauthentifizierungsservice verwalten
In diesem Abschnitt wird beschrieben, wie Sie den Netzwerkauthentifizierungsservice und die Kerberos-Authentifizierung in Ihrem Netzwerk verwalten können.

Fehlerbehebung
In diesem Abschnitt werden Lösungen für allgemeine Probleme mit dem Netzwerkauthentifizierungsservice beschrieben.

Referenzinformationen
Hier erfahren Sie, wo Sie weitere Informationen zu Kerberos und Themen, die sich mit dem Netzwerkauthentifizierungsservice befassen, wie z. B. Aktivierung der Einzelanmeldung (Single Signon) und Enterprise Identity Mapping (EIM), finden können.

Unter Besondere Bedingungen finden Sie rechtliche Hinweise zur Verwendung des Kerberos-Protokolls.

## Haftungsausschluss für Programmcode

Dieses Dokument enthält Programmierungsbeispiele.

Vorbehaltlich einer gesetzlichen Gewährleistung, die nicht ausgeschlossen werden kann, geben IBM, die 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, die Programmentwickler und Lieferanten in folgenden Fällen haftbar, auch wenn auf die Möglichkeit solcher Schäden hingewiesen wurde:

1. Verlust oder Beschädigung von Daten;
2. unmittelbare, mittelbare oder sonstige Folgeschäden; oder
3. entgangener Gewinn, entgangene Geschäftsabschlüsse, Umsatze, 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.

## Neuerungen in V5R3

Der Netzwerkauthentifizierungsservice ermöglicht dem iSeries-Server die Teilnahme an einem Netzwerk, welches das Kerberos-Protokoll zur Benutzerauthentifizierung im Netzwerk verwendet. In den folgenden Informationen werden die neuen Funktionen für dieses Release beschrieben:

**Funktionale Erweiterungen des Netzwerkauthentifizierungsservice**

In V5R3 wurden verschiedene funktionale Erweiterungen durchgeführt, um die Verwaltung des Netzwerkauthentifizierungsservice zu vereinfachen.

Diese Erweiterungen sind:

**Konfigurationsassistent für Kerberos-Service-Principal**
Dieser neue Assistent im iSeries Navigator ermöglicht Administratoren das Hinzufügen von Service-Principals für die i5/OS-Kerberos-Authentifizierung, Directory Services (LDAP), IBM HTTP-Server für iSeries oder iSeries NetServer-Schnittstellen. Bei der EIM-Konfiguration (Enterprise Identity Mapping) prüft der EIM-Assistent, ob der Netzwerkauthentifizierungsservice konfiguriert ist. Ist dies der Fall, prüft der Assistent, ob Chiffrierschlüsseldateieinträge für eine dieser Systemschnittstellen fehlen. Der EIM-Assistent startet dann den Assistenten des Kerberos-Service-Principals, damit der Administrator diese Services zur Chiffrierschlüsseldatei hinzufügen kann. Detaillierte Anweisungen hierzu finden Sie unter „Chiffrierschlüsseldateien verwalten" auf Seite 127.

**Verbesserte Auflösung von Hostnamen**
Im Konfigurationsassistenten für den Netzwerkauthentifizierungsservice und den Kerberos-Service-Principal empfangen Administratoren Alert-Nachrichten, wenn Hostnamen von einem PC und der iSeries nicht übereinstimmen. Wenn Hostnamen nicht aufgelöst werden, haben Administratoren die Möglichkeit, mehrere Chiffrierschlüsseldateieinträge für jeden dieser Hostnamen zu erstellen. Bevor Sie den Netzwerkauthentifizierungsservice konfigurieren, sollten Sie sich unbedingt mit der Hostauflösung in Ihrem Netzwerk vertraut machen. Detaillierte Anweisungen hierzu finden Sie unter „Hinweise zur Auflösung von Hostnamen" auf Seite 95.

**Unterstützung für HTTP-Server**
HTTP-Server für iSeries unterstützt jetzt die Kerberos-Authentifizierung. Bei der Konfiguration des Netzwerkauthentifizierungsservice können Administratoren Chiffrierschlüsseldateieinträge für den HTTP-Server erstellen und die Instanzen des HTTP-Servers so konfigurieren, dass sie Kerberos-Tickets zur Benutzerauthentifizierung akzeptieren.

**Neues Interoperabilitätstool für Microsoft Windows Active Directory**
Während der Konfiguration des Netzwerkauthentifizierungsservice wird ein Tool generiert, das dem Administrator hilft, Microsoft Windows Active Directory so zu konfigurieren, dass es mit dem iSeries-Server zusammenwirken kann.

### Unterstützung für einen Kerberos-Server in i5/OS PASE

Ein Administrator kann jetzt einen Kerberos-Server in i5/OS Portable Application Solutions Environment (PASE) konfigurieren. i5/OS PASE stellt eine integrierte Laufzeitumgebung für AIX-Anwendungen zur Verfügung. Unter „Szenario: Kerberos-Server in i5/OS PASE konfigurieren" auf Seite 5 erfahren Sie, wie ein Kerberos-Server in i5/OS PASE konfiguriert wird.

### Neue iSeries Navigator-Unterstützung für den Netzwerkauthentifizierungsservice

Der neue Assistent für Funktionssynchronisation im iSeries Navigator ermöglicht Ihnen, eine Konfiguration des Netzwerkauthentifizierungsservice von einem Modellsystem an mehrere Endpunktsysteme weiterzugeben. Wenn Sie die Konfiguration des Netzwerkauthentifizierungsservice weitergegeben haben, können Sie auch die Endpunktsysteme so konfigurieren, dass sie die Kerberos-Authentifizierung verwenden.

In den folgenden Szenarios erfahren Sie, wie diese Tasks ausgeführt werden:

- „Szenario: Konfiguration des Netzwerkauthentifizierungsservice an mehrere Systeme weitergeben" auf Seite 30
- „Szenario: Kerberos-Authentifizierung zwischen Management Central-Servern verwenden" auf Seite 41

### Neues Thema "Einzelanmeldung"

Ein neues Thema, Einzelanmeldung, hilft Administratoren, über die Konfiguration und Verwendung von Netzwerkauthentifizierungsservice und Enterprise Identity Mapping (EIM) in ihrem Unternehmen eine Umgebung für die Einzelanmeldung zu erstellen.

### Neuerungen und Änderungen anzeigen

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

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

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

## Thema drucken

Zum Anzeigen oder Herunterladen der PDF-Version wählen Sie Netzwerkauthentifizierungsservice (ca. 1.398 KB) aus.

Sie können die folgenden zugehörigen Themen anzeigen oder herunterladen:

- Einzelanmeldung (600 KB) enthält die folgenden Themen:
  - Szenarios, die zeigen, wie der Netzwerkauthentifizierungsservice mit EIM (Enterprise Identity Mapping) verwendet werden kann, um die Einzelanmeldung in einem Unternehmen bereitzustellen.
  - Konzepte, die die Einzelanmeldung und ihre Vorzüge erläutern.
- Enterprise Identity Mapping (EIM) (800 KB) enthält die folgenden Themen:
  - Szenarios, die allgemeine EIM-Implementierungen zeigen.
  - Konzepte und Planungsinformationen, die das Verständnis von EIM und die Planung für EIM vereinfachen.

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

1. Öffnen Sie die PDF-Datei im Browser, indem Sie auf den o. a. Link klicken.
2. Klicken Sie im Browsermenü auf **Datei**.
3. Klicken Sie auf **Speichern unter...**
4. Navigieren Sie zu dem Verzeichnis, in dem die PDF-Datei gespeichert werden soll.
5. Klicken Sie auf **Speichern**.

Falls Sie Adobe Acrobat Reader zum Anzeigen oder Drucken der PDF benötigen, können Sie eine Kopie von der Adobe-Website (www.adobe.com/product/acrobat/readstep.html) herunterladen. 

## Szenarios

Die folgenden Szenarios enthalten Beschreibungen allgemeiner Umgebungen, in denen der Netzwerkauthentifizierungsservice verwendet werden kann, um i5/OS die Teilnahme an einem Kerberos-Netzwerk zu ermöglichen.

Überprüfen Sie die folgenden Szenarios, um sich mit den technischen und Konfigurationsdetails, die bei der Konfiguration des Netzwerkauthentifizierungsservice eine Rolle spielen, vertraut zu machen:

Szenario: Kerberos-Server in i5/OS PASE konfigurieren
Anhand dieses Szenarios können Sie einen Kerberos-Server in i5/OS PASE einfacher planen und konfigurieren.

Szenario: Netzwerkauthentifizierungsservice konfigurieren
Dieses Szenario hilft Ihnen bei der Konfiguration des Netzwerkauthentifizierungsservice.

Szenario: Cross-Realm-Vertrauensbeziehung konfigurieren
Mit diesem Szenario können Sie eine Cross-Realm-Vertrauensbeziehung zwischen Microsoft Windows Active Directory und i5/OS PASE konfigurieren.

Szenario: Konfiguration des Netzwerkauthentifizierungsservice an mehrere Systeme weitergeben
Dieses Szenario veranschaulicht, wie Sie die Konfiguration des Netzwerkauthentifizierungsservice mit dem Assistenten für Funktionssynchronisation im iSeries Navigator vereinfachen können.

Szenario: Kerberos-Authentifizierung zwischen Management Central-Servern verwenden
Dieses Szenario veranschaulicht, wie die Kerberos-Authentifizierung zwischen Management Central-Servern auf Endpunktsystemen verwendet wird.

Szenario: Einzelanmeldung für i5/OS aktivieren
Dieses Szenario veranschaulicht, wie der Netzwerkauthentifizierungsservice und EIM konfiguriert werden, um eine Einzelanmeldungsumgebung zu erstellen.

# Szenario: Kerberos-Server in i5/OS PASE konfigurieren

## Situation

Sie arbeiten in Ihrem Unternehmen als Administrator und sind für die Sicherheitsverwaltung eines mittelgroßen Netzwerks verantwortlich. Sie möchten Benutzer über einen zentralen Server authentifizieren. Sie haben sich entschlossen, einen Kerberos-Server einzurichten, der Benutzer für Ressourcen im gesamten Unternehmen authentifizieren soll. Sie haben viele Optionen für die Implementierung einer Kerberos-Lösung in Ihrem Netzwerk untersucht. Sie wissen, dass der Windows 2000-Server Kerberos verwendet, um Benutzer für eine Windows-Domäne zu authentifizieren. Dies erhöht jedoch die Kosten im Rahmen Ihres geringen IT-Budgets. Anstatt eine Windows 2000-Domäne zur Benutzerauthentifizierung zu verwenden, haben Sie beschlossen, einen Kerberos-Server auf Ihrem iSeries-Server in i5/OS PASE (Portable Application Solutions Environment) zu konfigurieren. i5/OS PASE stellt eine integrierte Laufzeitumgebung für AIX-Anwendungen zur Verfügung. Sie möchten die Flexibilität von i5/OS PASE nutzen, um Ihren eigenen Kerberos-Server zu konfigurieren. Der Kerberos-Server in i5/OS PASE soll Benutzer in Ihrem Netzwerk, die Windows 2000- und Windows XP-Workstations verwenden, authentifizieren.

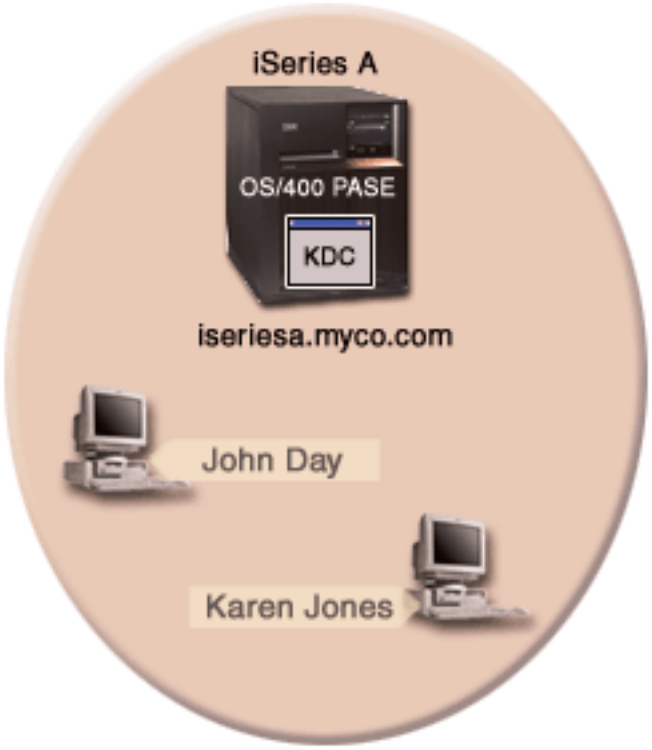
## Ziele

In diesem Szenario möchte MyCo, Inc. durch Ausführung der folgenden Tasks einen Kerberos-Server in i5/OS PASE einrichten:

- Kerberos-Server in der i5/OS PASE-Umgebung konfigurieren
- Netzwerkbenutzer zu einem Kerberos-Server hinzufügen
- Workstations, die das Betriebssystem Windows 2000 ausführen, zur Teilnahme am Kerberos-Realm, der in i5/OS PASE konfiguriert ist, konfigurieren
- Netzwerkauthentifizierungsservice auf iSeries A konfigurieren
- Authentifizierung in Ihrem Netzwerk testen

## Details

Die folgende Abbildung veranschaulicht die Netzwerkumgebung für dieses Szenario.




**iSeries A**

- Fungiert als Kerberos-Server (kdc1.myco.com) für das Netzwerk, wird auch als KDC (Key Distribution Center) bezeichnet.
- Wird unter i5/OS Version 5 Release 3 (V5R3) mit den folgenden Optionen und Lizenzprogrammen ausgeführt:
  - i5/OS Host-Server (5722-SS1 Option 12)
  - i5/OS PASE (5722-SS1 Option 33)
  - Qshell Interpreter (5722-SS1 Option 30)
  - Cryptographic Access Provider (5722-AC3)
  - iSeries Access für Windows (5722-XE1)
- Hat den vollständig qualifizierten Hostnamen iseriesa.myco.com.

**Client-PCs**

- **Für alle PCs in diesem Szenario:**
  - Verwenden die Betriebssysteme Windows 2000 und Windows XP.
  - Windows 2000-Unterstützungstools (beinhalten den Befehl ksetup) sind auf allen PCs installiert.
- **Für Administrator-PC:**
  - iSeries Access für Windows (5722-XE1) ist installiert.
  - iSeries Navigator mit den Unterkomponenten ″Sicherheit″ und ″Netzwerk″ ist installiert.

## Voraussetzungen und Annahmen

In diesem Szenario werden die folgenden Punkte als gegeben vorausgesetzt; das Szenario konzentriert sich auf die Tasks zur Konfiguration eines Kerberos-Servers in i5/OS PASE.

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 iSeries Navigator den Eintrag für Ihren **iSeries-Server → 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-Verbindungen wurden konfiguriert und in Ihrem Netzwerk getestet.
4. Ein einzelner DNS-Server wird für die Auflösung der Hostnamen im Netzwerk verwendet. Es werden keine Hosttabellen für die Auflösung der Hostnamen verwendet.

   **Anmerkung:** Die Verwendung von Hosttabellen mit Kerberos-Authentifizierung kann zu Fehlern bei der Namensauflösung oder anderen Problemen führen. Ausführliche Informationen zur Auflösung von Hostnamen mit der Kerberos-Authentifizierung finden Sie unter „Hinweise zur Auflösung von Hostnamen" auf Seite 95.

## Konfigurationsschritte

Führen Sie die folgenden Schritte durch, um einen Kerberos-Server in i5/OS PASE sowie den Netzwerkauthentifizierungsservice zu konfigurieren:

1. Planungsarbeitsblätter ausfüllen
2. Kerberos-Server in i5/OS PASE konfigurieren
3. Verschlüsselungswerte auf dem i5/OS PASE-Kerberos-Server ändern
4. Kerberos-Server in i5/OS PASE stoppen und erneut starten
5. Host-Principals für Windows 2000- und Windows XP-Workstations erstellen
6. Benutzer-Principals auf dem Kerberos-Server erstellen
7. Service-Principal von iSeries A zum Kerberos-Server hinzufügen
8. Windows 2000- und Windows XP-Workstations konfigurieren
9. Netzwerkauthentifizierungsservice konfigurieren
10. Ein Ausgangsverzeichnis für Benutzer auf iSeries A erstellen
11. Konfiguration des Netzwerkauthentifizierungsservice auf iSeries A testen

## Details zum Szenario: Kerberos-Server in i5/OS PASE konfigurieren

Die folgenden Tasks sind erforderlich, um einen Kerberos-Server in i5/OS PASE zu konfigurieren. Lesen Sie den Abschnitt Voraussetzungen und Annahmen und vergewissern Sie sich, dass Sie alle erforderlichen Tasks ausgeführt haben, bevor Sie das folgende Szenario durcharbeiten:

## Schritt 1: Planungsarbeitsblätter ausfüllen

Das folgende Planungsarbeitsblatt enthält Informationen, die Sie vervollständigen müssen, bevor Sie die Tasks des Szenarios ausführen.

*Tabelle 1. Planungsarbeitsblatt für Voraussetzungen*

| Fragen | Antworten |
|---|---|
| Arbeiten Sie mit i5/OS V5R3 (5722-SS1) oder einer späteren Version? | Ja |
| Sind die folgenden Optionen und Lizenzprogramme auf der iSeries A installiert?<br>• i5/OS Host-Server (5722-SS1 Option 12)<br>• i5/OS PASE (5722-SS1 Option 33)<br>• Qshell Interpreter (5722-SS1 Option 30)<br>• Cryptographic Access Provider (5722-AC3)<br>• iSeries Access für Windows (5722-XE1) | Ja |
| Ist auf allen PCs Windows 2000 oder Windows XP installiert? | Ja |
| Sind die Windows 2000-Unterstützungstools (beinhalten den Befehl ksetup) auf allen PCs installiert? | Ja |
| Ist iSeries Access für Windows (5722-XE1) auf dem Administrator-PC installiert? | Ja |
| Ist iSeries Navigator auf dem Administrator-PC installiert?<br>• Ist die Unterkomponente "Sicherheit" des iSeries Navigator auf dem PC des Administrators installiert?<br>• Ist die Unterkomponente "Netzwerk" des iSeries Navigator auf dem PC des Administrators installiert? | Ja<br>Ja<br>Ja |
| Ist das aktuellste Service-Pack für iSeries Access für Windows installiert? Sie können das aktuellste Service-Pack über iSeries Access abrufen. | Ja |
| Besitzen Sie die Sonderberechtigungen *SECADM, *ALLOBJ und *IOSYSCFG? Sie benötigen diese Sonderberechtigungen, um den Assistenten für den Netzwerkauthentifizierungsservice für dieses Szenario ausführen zu können. | Ja |
| Ist der DNS konfiguriert und verwenden Sie die richtigen Hostnamen für den iSeries-Server und den Kerberos-Server? | Ja |
| Unter welchem Betriebssystem möchten Sie den Kerberos-Server konfigurieren?<br>1. Windows (R) 2000-Server<br>2. Windows Server 2003<br>3. AIX Server<br>4. i5/OS PASE (ab V5R3)<br>5. zSeries | i5/OS PASE |
| Wurden die aktuellsten vorläufigen Programmkorrekturen (PTFs) angelegt? | Ja |
| Beträgt die Abweichung zwischen der Systemzeit der iSeries und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung größer, lesen Sie Systemzeiten synchronisieren. | Ja |

Für dieses Szenario müssen Sie verschiedene Kennwörter angeben. Das folgende Planungsarbeitsblatt enthält eine Liste von Kennwörtern, die Sie für dieses Szenario verwenden müssen. Verwenden Sie diese Tabelle als Referenz, wenn Sie die Konfigurationsschritte zur Konfiguration des Kerberos-Servers in i5/OS PASE durchführen.

**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 Kennwörter*

| Entität | Kennwort |
|---|---|
| i5/OS PASE-Administrator: admin/admin<br>**Anmerkung:** i5/OS PASE gibt `admin/admin` als Standardbenutzernamen für den Administrator an. | secret |
| i5/OS PASE-Datenbankmaster | pasepwd |
| Windows 2000-Workstations:<br>• pc1.myco.com (PC von John Day)<br>• pc2.myco.com (PC von Karen Jones) | secret1<br>secret2 |
| Kerberos-Benutzer-Principals:<br>• day@MYCO.COM<br>• jones@MYCO.COM | 123day<br>123jones |
| i5/OS-Service-Principal für iSeries A: krbsvr400/iseriesa.myco.com@MYCO.COM | iseriesa123 |

Das folgende Planungsarbeitsblatt veranschaulicht, welche Informationen Sie benötigen, bevor Sie mit der Konfiguration des Kerberos-Servers in i5/OS PASE und des Netzwerkauthentifizierungsservice beginnen können. Alle Fragen auf den Arbeitsblättern für Voraussetzungen und Kennwörter müssen beantwortet werden, bevor Sie mit der Konfiguration des Kerberos-Servers in i5/OS PASE fortfahren.

*Tabelle 3. Planungsarbeitsblatt für die Konfiguration eines Kerberos-Servers in i5/OS PASE und die Konfiguration des Netzwerkauthentifizierungsservice*

| Fragen | Antworten |
|---|---|
| Wie lautet der Name des Kerberos-Standard-Realm? | MYCO.COM |
| Befindet sich der Standard-Realm in Microsoft Active Directory? | Nein |
| 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<br>**Port:** 88<br>**Anmerkung:** Dies ist der Standardport für den Kerberos-Server. |
| Möchten Sie einen Kennwortserver für diesen Standard-Realm konfigurieren? | Nein<br>**Anmerkung:** Gegenwärtig werden Kennwortserver von i5/OS PASE oder AIX nicht unterstützt. |
| Für welche Services möchten Sie Chiffrierschlüsseleinträge erstellen?<br>• i5/OS-Kerberos-Authentifizierung<br>• LDAP<br>• iSeries IBM HTTP-Server<br>• iSeries NetServer | i5/OS-Kerberos-Authentifizierung |
| Möchten Sie eine Stapeldatei erstellen, um das Hinzufügen der Service-Principals zum Microsoft Active Directory zu automatisieren? | Nicht anwendbar |
| Wie lautet der Standardbenutzername für den i5/OS PASE-Administrator?<br><br>Wie lautet das Kennwort für den i5/OS PASE-Administrator?<br>**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. | Benutzername: admin/admin<br>Kennwort: secret |

*Tabelle 3. Planungsarbeitsblatt für die Konfiguration eines Kerberos-Servers in i5/OS PASE und die Konfiguration des Netzwerkauthentifizierungsservice (Forts.)*

| Fragen | Antworten |
|---|---|
| Welche Namenskonvention soll für Ihre Principals, die Benutzer in Ihrem Netzwerk bezeichnen, verwendet werden? | Principals, die Benutzer bezeichnen, werden mit dem in Kleinbuchstaben geschriebenen Familiennamen, gefolgt vom in Großbuchstaben geschriebenen Realm-Namen, angegeben. |
| Wie lauten die Principal-Namen der Kerberos-Benutzer für diese Benutzer:<br>• John Day<br>• Karen Jones | day@MYCO.COM<br>jones@MYCO.COM |
| Wie lauten die i5/OS-Benutzerprofilnamen für diese Benutzer:<br>• John Day<br>• Karen Jones | JOHND<br>KARENJ |
| Wie lauten die Windows 2000-Benutzernamen für diese Benutzer:<br>• John Day<br>• Karen Jones | johnday<br>karenjones |
| Wie lauten die Hostnamen für diese Windows 2000-Workstations:<br>• PC von John Day<br>• PC von Karen Jones | pc1.myco.com<br>pc2.myco.com |
| Wie lautet der Name des i5/OS-Service-Principals für die iSeries A? | krbsvr400/iseriesa.myco.com@MYCO.COM<br>**Anmerkung:** Der Name dieses Service-Principals dient nur als Beispiel. Geben Sie in Ihrer Konfiguration den Hostnamen und die Domäne Ihres i5/OS-Systems als Name des Service-Principals an. |

## Schritt 2: Kerberos-Server in i5/OS PASE konfigurieren

Verwenden Sie die Informationen aus Ihren Arbeitsblättern, um einen Kerberos-Server unter i5/OS PASE auf der iSeries A wie folgt zu konfigurieren:

**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.

1. Geben Sie in einer zeichenorientierten Schnittstelle `call QP2TERM` in der Befehlszeile ein. Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.
2. Geben Sie in der Befehlszeile `export PATH=$PATH:/usr/krb5/sbin` ein. Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.
3. Geben Sie in der Befehlszeile `config.krb5 -S -d myco.com -r MYCO.COM` ein. `-d` ist der DNS Ihres Netzwerks und `-r` ist der Name des Realms. (In diesem Beispiel ist myco.com der DNS-Name und MYCO.COM der Realmname.) Dieser Befehl aktualisiert die Datei krb5.config mit dem Domä- nennamen und dem Realm für den Kerberos-Server, erstellt die Kerberos-Datenbank innerhalb des integrierten Dateisystems und konfiguriert den Kerberos-Server in i5/OS PASE. Sie werden aufgefordert, die folgenden Kennwörter einzugeben:
   - Hauptkennwort für Datenbank: `pasepwd`
   - Kennwort für Principal admin/admin: `secret`
4. Drücken Sie PF3 (Verlassen), um die PASE-Umgebung zu verlassen.

Sie haben den Kerberos-Server in i5/OS PASE konfiguriert und müssen jetzt die Verschlüsselungswerte auf dem Kerberos-Server ändern.

## Schritt 3: Verschlüsselungswerte auf dem i5/OS PASE-Kerberos-Server ändern

Die Standardverschlüsselungseinstellungen des Kerberos-Servers müssen geändert werden, damit Clients am i5/OS PASE-Kerberos-Server authentifiziert werden können und ein Betrieb mit Windows-Workstations möglich ist. Zum Ändern der Standardverschlüsselungseinstellungen müssen Sie die Datei kdc.conf im Verzeichnis /etc/krb5 editieren. Gehen Sie dazu wie folgt vor:

1. Geben Sie in einer zeichenorientierten Schnittstelle `edtf '/var/krb5/krb5kdc/kdc.conf'` ein, um auf die Datei kdc.conf zuzugreifen.
2. Ändern Sie die folgenden Zeilen in der Datei kdc.conf:

```
supported_enctypes = des3-cbc-sha1:normal
des-cbc-md5:normal des-cbc-crc:normal
kdc_supported_enctypes = des3-cbc-sha1:normal
des-cbc-md5:normal des-cbc-crc:normal
```

   in

```
supported_enctypes = des-cbc-md5:normal
kdc_supported_enctypes = des-cbc-md5:normal
```

Sie haben die zum Ändern der Verschlüsselungswerte auf dem Kerberos-Server erforderlichen Schritte durchgeführt. Jetzt müssen Sie den Kerberos-Server stoppen und erneut starten, damit diese Änderungen wirksam werden.

## Schritt 4: Kerberos-Server in i5/OS PASE stoppen und erneut starten

Der Kerberos-Server muss in i5/OS PASE gestoppt und erneut gestartet werden, damit die zuvor geänderten Verschlüsselungswerte aktualisiert werden. Führen Sie die folgenden Schritte durch:

1. Geben Sie in einer zeichenorientierten Schnittstelle `call QP2TERM` in der Befehlszeile ein. Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.
2. Geben Sie in der Befehlszeile `export PATH=$PATH:/usr/krb5/sbin` ein. Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.
3. Geben Sie in der Befehlszeile stop.krb5 ein. Mit diesem Befehl wird der Kerberos-Server gestoppt.
4. Geben Sie in der Befehlszeile start.krb5 ein. Mit diesem Befehl wird der Kerberos-Server gestartet.

Sie haben die Schritte zum Neustart des Kerberos-Servers durchgeführt und müssen jetzt Host-Principals für die Windows-Workstations erstellen.

## Schritt 5: Host-Principals für Windows 2000- und Windows XP-Workstations erstellen

Sie müssen die Host-Principals, die Kerberos zur Authentifizierung der PC-Benutzer verwendet, erstellen. Wenn i5/OS PASE bereits aktiv ist, können Sie die Schritte 1 und 2 überspringen.

Führen Sie die folgenden Schritte durch, um die Host-Principals für die Workstations zu erstellen:

1. Geben Sie in einer zeichenorientierten Schnittstelle `call QP2TERM` in der Befehlszeile ein. Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.
2. Geben Sie in der Befehlszeile `export PATH=$PATH:/usr/krb5/sbin` ein. Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.
3. Geben Sie in der Befehlszeile `kadmin -p admin/admin` ein, und drücken Sie die Eingabetaste.
4. Melden Sie sich mit dem Kennwort des Administrators an. Beispiel: `secret`.

5. Geben Sie bei der kadmin-Eingabeaufforderung `addprinc -pw secret1 host/pc1.myco.com` ein. Damit wird ein Host-Principal für den PC von John Day erstellt.
6. Geben Sie bei der kadmin-Eingabeaufforderung `addprinc -pw secret2 host/pc2.myco.com` ein. Damit wird ein Host-Principal für den PC von Karen Jones erstellt.
7. Geben Sie `quit` ein, um die kadmin-Schnittstelle zu verlassen.

Sie haben die Host-Principals für die Windows-Workstations erstellt und müssen jetzt Benutzer-Principals für die Benutzer John Day und Karen Jones erstellen.

## Schritt 6: Benutzer-Principals auf dem Kerberos-Server erstellen

Damit Benutzer für Services im Netzwerk authentifiziert werden können, müssen Sie sie als Principals zum Kerberos-Server hinzufügen. Principal ist der Kerberos-Begriff für die Kombination aus einem Benutzernamen und einem Kennwort. Diese Principals werden auf dem Kerberos-Server gespeichert und zur Validierung von Benutzern im Netzwerk verwendet.

1. Geben Sie in einer zeichenorientierten Schnittstelle `call QP2TERM` in der Befehlszeile ein. Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.
2. Geben Sie in der Befehlszeile `export PATH=$PATH:/usr/krb5/sbin` ein. Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.
3. Geben Sie in der Befehlszeile `kadmin -p admin/admin` ein, und drücken Sie die Eingabetaste.
4. Melden Sie sich mit dem Kennwort des Administrators an. Beispiel: `secret`.
5. Geben Sie bei einer kadmin-Eingabeaufforderung `addprinc -pw 123day day` ein.
6. Sie empfangen eine Nachricht wie folgende:

   ```
   Principal "day@MYCO.COM" created.
   ```

   Auf diese Weise wird der Benutzer-Principal für John Day erstellt.

Wiederholen Sie diese Schritte für Karen Jones, geben Sie jedoch `jones` als Principal-Name und `123jones` als Kennwort ein.

Sie haben die Host-Principals und Benutzer-Principals erstellt und müssen jetzt die i5/OS-Service-Principals zum Kerberos-Server hinzufügen.

## Schritt 7: Service-Principal von iSeries A zum Kerberos-Server hinzufügen

Damit i5/OS-Schnittstellen Kerberos-Tickets akzeptieren können, müssen Sie sie als Principals zum Kerberos-Server hinzufügen. Wenn Sie sich bereits in der kadmin-Umgebung befinden, können Sie die Schritte 1 bis 4 überspringen.

**Anmerkung:** Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Sie dürfen nicht in einer echten Konfiguration verwendet werden. Der Name des Principals dient nur als Beispiel.

1. Geben Sie in einer zeichenorientierten Schnittstelle `call QP2TERM` in der Befehlszeile ein. Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.
2. Geben Sie in der Befehlszeile `export PATH=$PATH:/usr/krb5/sbin` ein. Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.
3. Geben Sie in der Befehlszeile `kadmin -p admin/admin` ein, und drücken Sie die Eingabetaste.
4. Melden Sie sich mit dem Kennwort des Administrators an. Beispiel: `secret`.
5. Geben Sie bei der kadmin-Eingabeaufforderung `addprinc -pw iseriesa123 krbsvr400/iseriesa.myco.com` ein.

6. Sie empfangen eine Nachricht wie folgende:

   ```
   Principal "krbsvr400/iseriesa.myco.com@MYCO.COM" created.
   ```

7. Geben Sie `quit` ein, um die kadmin-Schnittstelle zu verlassen, und drücken Sie F3 (Verlassen), um die PASE-Umgebung zu verlassen.

Sie haben den i5/OS-Service-Principal zum Kerberos-Server hinzugefügt. Wenn Sie beabsichtigen, nach Abschluss dieses Szenarios eine Einzelanmeldungsumgebung zu erstellen, müssen Sie Ihre Workstations als Teil einer Arbeitsgruppe konfigurieren (Schritt 8). Fahren Sie andernfalls mit Schritt 9 fort (Netzwerkauthentifizierungsservice konfigurieren).

## Schritt 8: Windows 2000- und Windows XP-Workstations konfigurieren

**Anmerkung:** Dieser Schritt ist optional für die Konfiguration eines Kerberos-Servers in i5/OS PASE. Wenn Sie jedoch beabsichtigen, nach der Konfiguration des Kerberos-Servers eine Umgebung für die Einzelanmeldungen zu erstellen, müssen Sie diesen Schritt durchführen.

Konfigurieren Sie die Client-Workstations als Bestandteil einer Arbeitsgruppe, indem Sie den Kerberos-Realm und den Kerberos-Server auf der Workstation festlegen. Sie müssen außerdem ein Kennwort festlegen, das der Workstation zugeordnet 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.

Führen Sie die folgenden Schritte durch, um die Workstations zu konfigurieren:

1. Geben Sie in einer Befehlszeile auf der Windows 2000-Workstation Folgendes ein:

   ```
   C:> ksetup /setdomain MYCO.COM
   C:> ksetup /addkdc MYCO.COM kdc1.myco.com
   ```

2. Legen Sie das Kennwort des Kontos der lokalen Maschine fest, indem Sie bei der Eingabeaufforderung der Windows 2000-Workstation Folgendes eingeben:

   ```
   C:> ksetup /setmachpassword secret1
   ```

3. Ordnen Sie den Kerberos-Benutzer-Principal von John Day (day@MYCO.COM) seinem Windows 2000-Benutzernamen (johnday) zu. Geben Sie bei der Eingabeaufforderung der Windows 2000-Workstation Folgendes ein:

   ```
   C:> ksetup /mapuser day@MYCO.COM johnday
   ```

4. Möchten Sie überprüfen, ob der Kerberos-Benutzer-Principal von John Day mit seinem Windows 2000-Benutzernamen übereinstimmt, geben Sie bei der Eingabeaufforderung der Windows 2000-Workstation Folgendes ein:

   ```
   C:> ksetup
   ```

   Überprüfen Sie anschließend das Ergebnis.

5. Starten Sie den PC erneut, damit die Änderungen wirksam werden.

Wiederholen Sie diese Schritte für die Workstation von Karen Jones, geben Sie jedoch folgende Informationen ein:

- Kennwort der lokalen Maschine: `secret2`
- Kerberos-Benutzer-Principal: `jones@MYCO.COM`

| • Windows 2000-Benutzername: `karenjones`

| Sie haben die Workstations konfiguriert und müssen jetzt den Netzwerkauthentifizierungsservice mit
| dem entsprechenden Assistenten konfigurieren.

## | Schritt 9: Netzwerkauthentifizierungsservice konfigurieren

| Führen Sie die folgenden Schritte durch, um den Netzwerkauthentifizierungsservice zu konfigurieren:

| 1. Erweitern Sie im iSeries Navigator den Eintrag **iSeries A → Sicherheit**.
| 2. Klicken Sie mit der rechten Maustaste auf **Netzwerkauthentifizierungsservice** und wählen Sie **Konfigurieren** aus, um den Konfigurationsassistenten zu starten.

| **Anmerkung:** Nach der Konfiguration des Netzwerkauthentifizierungsservice lautet diese Option **Rekonfigurieren**.

| 3. Die **Begrüßungsseite** enthält Informationen zu den vom Assistenten erstellten Objekten. Klicken Sie auf **Weiter**.
| 4. Geben Sie auf der Seite **Realm-Informationen angeben** im Feld **Standard-Realm** MYCO.COM ein. Klicken Sie auf **Weiter**.
| 5. Geben Sie auf der Seite **KDC-Informationen angeben** im Feld **KDC** den Wert `kdc1.myco.com` für den Kerberos-Server und im Feld **Port** den Wert 88 ein. Klicken Sie auf **Weiter**.
| 6. Wählen Sie auf der Seite **Kennwortserverinformationen angeben** die Option **Nein** aus. Klicken Sie auf **Weiter**.
| 7. Wählen Sie auf der Seite **Chiffrierschlüsseleinträge auswählen** die Option **i5/OS-Kerberos-Authentifizierung** aus. Klicken Sie auf **Weiter**.
| 8. Geben Sie auf der Seite **i5/OS-Chiffrierschlüsseleintrag erstellen** ein Kennwort ein und bestätigen Sie es. Klicken Sie anschließend auf **Weiter**. Beispiel: `iseriesa123`. Dieses Kennwort wird verwendet, wenn iSeries A zum Kerberos-Server hinzugefügt wird.
| 9. Auf der Seite **Zusammenfassung** können Sie die Details zur Konfiguration des Netzwerkauthentifizierungsservice überprüfen. Klicken Sie auf **Fertig stellen**.

| Sie haben den Netzwerkauthentifizierungsservice konfiguriert und müssen jetzt Ausgangsverzeichnisse
| für beide Benutzer erstellen.

## | Schritt 10: Ein Ausgangsverzeichnis für Benutzer auf der iSeries A erstellen

| Jeder Benutzer, der eine Verbindung zu i5/OS-Schnittstellen herstellen möchte, benötigt ein Verzeichnis
| im Ausgangsverzeichnis (/home). Dieses Verzeichnis enthält den Namen des Kerberos-Cache für
| Berechtigungsnachweise, der dem Benutzer zugeordnet ist. Führen Sie folgende Schritte durch, um ein
| Ausgangsverzeichnis für einen Benutzer zu erstellen:

| Geben Sie in der i5/OS-Befehlszeile Folgendes ein: `CRTDIR '/home/Benutzerprofil'`, wobei
| `Benutzerprofil` den Namen des i5/OS-Benutzerprofils für den Benutzer bezeichnet. Beispiel: `CRTDIR
| '/home/JOHND'` für den Benutzer John Day.

| Wiederholen Sie den Befehl für Karen Jones, geben Sie jedoch das entsprechende i5/OS-Benutzerprofil,
| `KARENJ`, an.

| Sie haben für Ihre Benutzer Ausgangsverzeichnisse erstellt und müssen jetzt sicherstellen, dass der Netz-
| werkauthentifizierungsservice ordnungsgemäß funktioniert.

## | Schritt 11: Netzwerkauthentifizierungsservice testen

| Sie sollten die Konfiguration des Netzwerkauthentifizierungsservice testen, indem Sie ein Ticket-granting
| Ticket für den i5/OS-Principal und andere Principals in Ihrem Netzwerk anfordern.

**Anmerkung:** Vergewissern Sie sich, dass Sie ein Ausgangsverzeichnis für Ihr i5/OS-Benutzerprofil erstellt haben, bevor Sie diesen Test durchführen.

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

1. Geben Sie in einer Befehlszeile `QSH` ein, um den Qshell Interpreter zu starten.
2. Geben Sie `keytab list` ein, um eine Liste der Principals, die in der Chiffrierschlüsseldatei registriert sind, anzuzeigen. Die folgenden Ergebnisse sollten angezeigt werden:

```
Principal: krbsvr400/iseriesa.myco.com@MYCO.COM
  Key version: 2
  Key type: 56-bit DES using key derivation
  Entry timestamp: 200X/05/29-11:02:58
```

3. Geben Sie `kinit -k krbsvr400/iseriesa.myco.com@MYCO.COM` ein, um ein Ticket-granting Ticket vom Kerberos-Server anzufordern. Mit diesem Befehl wird geprüft, ob Ihr iSeries-Server ordnungsgemäß konfiguriert wurde und das Kennwort in der Chiffrierschlüsseldatei mit dem auf dem Kerberos-Server gespeicherten Kennwort übereinstimmt.Ist dies der Fall, kann der Befehl QSH 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-Cache für Berechtigungsnachweise angezeigt und geprüft, ob ein gültiges Ticket für den i5/OS-Service-Principal erstellt und in den Cache für Berechtigungsnachweise auf dem iSeries-System aufgenommen wurde.

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

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

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

Sie haben die Schritte durchgeführt, die erforderlich sind, um den iSeries-Server als Kerberos-Server zu konfigurieren, und Sie können die Benutzer im Realm MYCO.COM mit Kerberos authentifizieren.

## Szenario: Netzwerkauthentifizierungsservice konfigurieren

### Situation

Sie sind ein Netzwerkadministrator, der das Netzwerk für die Auftragsannahme in Ihrem Unternehmen verwaltet. Sie haben kürzlich eine iSeries zum Netzwerk hinzugefügt, auf der Sie verschiedene Anwendungen, die für Ihre Abteilung erforderlich sind, installieren möchten. In Ihrem Netzwerk verwalten Sie Benutzer mit Microsoft Windows Active Directory auf einem Microsoft Windows 2000-Server. Gegenwärtig verwenden alle Ihre Benutzer Workstations, auf denen das Betriebssystem Microsoft Windows 2000 ausgeführt wird. Sie haben eigene Kerberos-fähige Anwendungen, die Generic Security Service (GSS)-APIs verwenden.

Dieses Szenario hat folgende Vorteile:

- Der Authentifizierungsprozess für Benutzer wird vereinfacht.
- Der Systemaufwand für die Zugriffsverwaltung bezüglich der Server im Netzwerk wird verringert.
- Das Sicherheitsrisiko durch Kennwortdiebstahl wird verringert.

## Ziele

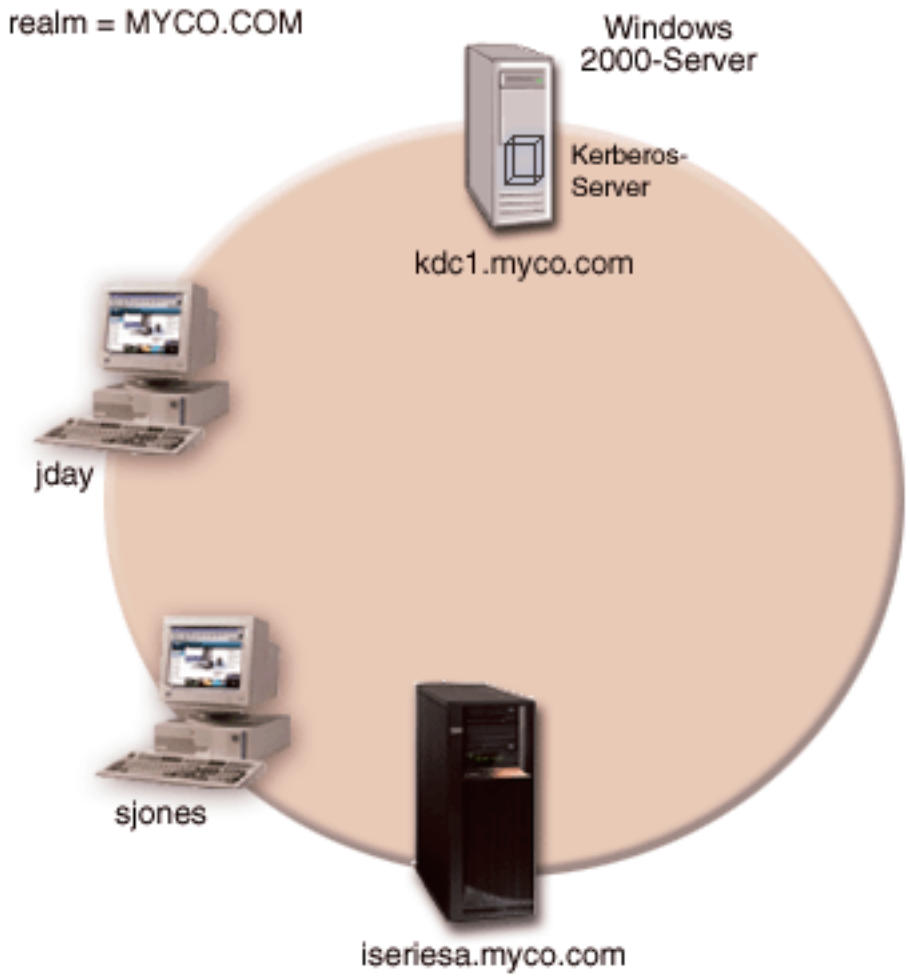
In diesem Szenario möchte MyCo, Inc. ein iSeries-System zu einem vorhandenen Realm hinzufügen, in dem ein Windows 2000-Server als Kerberos-Server fungiert. Die iSeries enthält verschiedene kritische Geschäftsanwendungen, auf die nur die richtigen Benutzer Zugriff haben sollen. Benutzer müssen vom Kerberos-Server authentifiziert werden, um die Zugriffsberechtigung für diese Anwendungen zu erhalten.

Die Ziele dieses Szenarios:

- Der iSeries soll die Teilnahme an einem vorhandenen Kerberos-Server ermöglicht werden
- Es sollen sowohl Principal- als auch auch Benutzernamen im Netzwerk zulässig sein
- Kerberos-Benutzern sollen die Möglichkeit erhalten, ihre eigenen Kennwörter auf dem Kerberos-Server zu ändern

## Details

Die folgende Abbildung veranschaulicht die Netzwerkkenndaten von MyCo.



**iSeries A**

- Wird unter i5/OS Version 5 Release 3 (V5R3) mit den folgenden Optionen und Lizenzprogrammen ausgeführt:
  - i5/OS Host-Server (5722-SS1 Option 12)
  - Qshell Interpreter (5722-SS1 Option 30)
  - iSeries Access für Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3 Option 35)
- Der Principal-Name von iSeries A ist krbsvr400/iseriesa.myco.com@MYCO.COM.

**Windows 2000-Server**

- Fungiert als Kerberos-Server für den Realm MYCO.COM.
- Der vollständig qualifizierte Hostname des Kerberos-Servers ist kdc1.myco.com.

**Client-PCs**

- Verwenden das Betriebssystem Windows (R) 2000.
- Auf dem PC zur Verwaltung des Netzwerkauthentifizierungsservice sind die folgenden Produkte installiert:
  - iSeries Access für Windows (5722-XE1)
  - iSeries Navigator und die Unterkomponenten ″Sicherheit″ und ″Netzwerk″

## Voraussetzungen und Annahmen

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

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

   a. Erweitern Sie im iSeries Navigator den Eintrag für Ihren **iSeries-Server → 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 Basissystemsicherheit wurden auf jedem dieser Server konfiguriert und getestet.
4. Ein einzelner DNS-Server wird für die Auflösung der Hostnamen im Netzwerk verwendet. Es werden keine Hosttabellen für die Auflösung der Hostnamen verwendet.

   **Anmerkung:** Die Verwendung von Hosttabellen mit Kerberos-Authentifizierung kann zu Fehlern bei der Namensauflösung oder anderen Problemen führen. Ausführliche Informationen zur Auflösung von Hostnamen mit der Kerberos-Authentifizierung finden Sie unter „Hinweise zur Auflösung von Hostnamen” auf Seite 95.

## Konfigurationsschritte

1. Die Planungsarbeitsblätter und Prüflisten für den Netzwerkauthentifizierungsservice ausfüllen.
2. Netzwerkauthentifizierungsservice auf der iSeries A konfigurieren.
3. Principal der iSeries A zum Kerberos-Server hinzufügen.
4. Ein Ausgangsverzeichnis für jeden Benutzer auf der iSeries A erstellen.
5. Konfiguration des Netzwerkauthentifizierungsservice auf der iSeries A testen.

## Details zum Szenario: Netzwerkauthentifizierungsservice konfigurieren Schritt 1: Planungsarbeitsblätter ausfüllen

Die folgenden Planungsarbeitsblätter veranschaulichen die Art der Informationen, die Sie benötigen, um mit der Konfiguration des Netzwerkauthentifizierungsservice beginnen zu können. Alle Antworten auf dem Arbeitsblatt für Voraussetzungen müssen mit Ja beantwortet werden, bevor Sie mit der Konfiguration des Netzwerkauthentifizierungsservice fortfahren.

*Tabelle 4. Arbeitsblatt für Voraussetzungen*

| Fragen | Antworten |
|---|---|
| Arbeiten Sie mit i5/OS V5R3 (5722-SS1) oder einer späteren Version? | Ja |
| Sind die folgenden Lizenzprogramme auf der iSeries A installiert?<br>• i5/OS Host Servers (5722-SS1 Option 12)<br>• Qshell Interpreter (5722-SS1 Option 30)<br>• iSeries Access für Windows (5722-XE1)<br>• Cryptographic Access Provider (5722-AC3) | Ja |
| Ist Windows 2000 auf Ihren PCs installiert? | Ja |
| Ist iSeries Access für Windows (5722-XE1) auf dem Administrator-PC installiert? | Ja |
| Ist iSeries Navigator auf dem Administrator-PC installiert?<br>• Ist die Unterkomponente ″Sicherheit″ des iSeries Navigator auf dem PC des Administrators installiert?<br>• Ist die Unterkomponente ″Netzwerk″ des iSeries Navigator auf dem PC des Administrators installiert? | Ja<br>Ja<br>Ja |
| Ist das aktuellste Service-Pack für iSeries Access für Windows installiert? Sie können das aktuellste Service-Pack über iSeries Access abrufen. | Ja |
| Besitzen Sie die Sonderberechtigungen *SECADM, *ALLOBJ und *IOSYSCFG? | Ja |
| Ist eines der folgenden Produkte auf dem sicheren System, das als Kerberos-Server fungieren soll, installiert? Wenn ja, welches?<br>1. Windows 2000-Server<br>2. Windows Server 2003<br>3. AIX Server<br>4. i5/OS PASE (ab V5R3)<br>5. zSeries | Ja, Windows 2000-Server |
| Sind alle PCs Ihres Netzwerks in einer Windows 2000-Domäne konfiguriert?<br>**Anmerkung:** Eine Windows 2000-Domäne ist mit einem Kerberos-Realm vergleichbar. Microsoft Active Directory verwendet die Kerberos-Authentifizierung als Sicherheitsmechanismus. | Ja |
| Wurden die aktuellsten vorläufigen Programmkorrekturen (PTFs) angelegt? | Ja |
| Beträgt die Abweichung zwischen der Systemzeit der iSeries und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung größer, lesen Sie Systemzeiten synchronisieren. | Ja |

*Tabelle 5. Planungsarbeitsblatt für den Netzwerkauthentifizierungsservice*

| Fragen | Antworten |
|---|---|
| Wie lautet der Name des Kerberos-Standard-Realm, zu dem Ihre iSeries gehören soll?<br>**Anmerkung:** Eine Windows 2000-Domäne ist mit einem Kerberos-Realm vergleichbar.Microsoft Active Directory verwendet die Kerberos-Authentifizierung als Sicherheitsmechanismus. | 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<br>**Port:** 88<br>**Anmerkung:** Dies ist der Standardport für den Kerberos-Server. |

*Tabelle 5. Planungsarbeitsblatt für den Netzwerkauthentifizierungsservice (Forts.)*

| Fragen | Antworten |
|---|---|
| Möchten Sie einen Kennwortserver für diesen Standard-Realm konfigurieren? Wenn ja, beantworten Sie die folgenden Fragen:<br><br>Wie lautet der Name des Kennwortservers für diesen Kerberos-Server?<br>An welchem Port ist der Kennwortserver empfangsbereit? | Ja<br><br>**Kennwortserver:**<br>kdc1.myco.com<br>**Port:** 464<br>**Anmerkung:** Dies ist der Standardport für den Kennwortserver. |
| Für welche Services sollen Chiffrierschlüsseleinträge erstellt werden?<br>• i5/OSKerberos-Authentifizierung<br>• LDAP<br>• iSeries IBM HTTP-Server<br>• iSeries NetServer | i5/OS-Kerberos-Authentifizierung |
| Welches Kennwort soll für Ihre(n) i5/OS-Service-Principal(s) verwendet werden?<br>**Anmerkung:** Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Sie dürfen nicht in einer echten Konfiguration verwendet werden. | iseriesa123 |
| Möchten Sie eine Stapeldatei erstellen, um das Hinzufügen der Service-Principals zum Microsoft Active Directory zu automatisieren? | Ja |
| Welche i5/OS-Benutzerprofilnamen werden für John Day und Sharon Jones verwendet? | JOHND<br>SHARONJ |

## Schritt 2: Netzwerkauthentifizierungsservice auf der iSeries A konfigurieren

Verwenden Sie die Informationen von Ihren Arbeitsblättern, um den Netzwerkauthentifizierungsservice auf der iSeries A wie folgt zu konfigurieren:

1. Erweitern Sie im iSeries Navigator den Eintrag **iSeries A → Sicherheit**.
2. Klicken Sie mit der rechten Maustaste auf **Netzwerkauthentifizierungsservice**, und wählen Sie **Konfigurieren** aus, um den Konfigurationsassistenten zu starten.

   **Anmerkung:** Nach der Konfiguration des Netzwerkauthentifizierungsservice lautet diese Option **Rekonfigurieren**.
3. Die **Begrüßungsseite** enthält Informationen zu den vom Assistenten erstellten Objekten. Klicken Sie auf **Weiter**.
4. 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**.
5. Geben Sie auf der Seite **KDC-Informationen angeben** im Feld **KDC** den Wert `kdc1.myco.com` für den Kerberos-Server und im Feld **Port** den Wert 88 ein. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Kennwortserverinformationen angeben** die Option **Ja** aus. Geben Sie im Feld **Kennwortserver** den Wert `kdc1.myco.com` und im Feld **Port** den Wert `464` ein. Klicken Sie auf **Weiter**.
7. Wählen Sie auf der Seite **Chiffrierschlüsseleinträge auswählen** die Option **i5/OS-Kerberos-Authentifizierung** aus. Klicken Sie auf **Weiter**.
8. Geben Sie auf der Seite **i5/OS-Chiffrierschlüsseleintrag erstellen** ein Kennwort ein und bestätigen Sie es. Beispiel: `iseriesa123`. Dieses Kennwort wird verwendet, wenn iSeries A zum Kerberos-Server hinzugefügt wird.

**Anmerkung:** Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Sie dürfen nicht in einer echten Konfiguration verwendet werden.

Klicken Sie auf **Weiter**.

9. Wählen Sie auf der Seite **Stapeldatei erstellen** die Option **Ja** aus, um diese Datei zu erstellen, und machen Sie die folgenden Angaben:
   - **Stapeldatei:** Fügen Sie am Ende des standardmäßig verwendeten Stapeldateinamens die Zeichenfolge `iseriesa` an. Beispiel: `C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigiseriesa.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:** Alternativ dazu können Sie Service-Principals, die vom Assistenten generiert wurden, manuell zum Kerberos-Server hinzufügen. Im Abschnitt „Dem Kerberos-Server i5/OS-Principals hinzufügen" auf Seite 114 wird erläutert, wie i5/OS-Service-Principals dem Kerberos-Server manuell hinzugefügt werden .
10. Auf der Seite **Zusammenfassung** können Sie die Details zur Konfiguration des Netzwerkauthentifizierungsservice überprüfen. Klicken Sie auf **Fertig stellen**.

Die Konfiguration des Netzwerkauthentifizierungsservice auf der iSeries A ist jetzt abgeschlossen. Der nächste Schritt besteht darin, den Principal zum Kerberos-Server hinzuzufügen.

## Schritt 3: Principal von iSeries 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 Principal manuell, wie im Szenario dargestellt, oder anhand einer Stapeldatei hinzufügen. Sie haben diese Stapeldatei in Schritt 2 erstellt. Wenn Sie diese Datei verwenden möchten, müssen Sie sie mit FTP (File Transfer Protocol) auf den Kerberos-Server kopieren und dann ausführen. Führen Sie die folgenden Schritte durch, um den Principal anhand der Stapeldatei zum Kerberos-Server hinzuzufügen:

**Vom Assistenten erstellte FTP-Stapeldatei**

1. Öffnen Sie auf der Windows 2000-Workstation, die der Administrator zur Konfiguration des Netzwerkauthentifizierungsservice verwendet hat, ein Befehlsfenster und geben Sie `ftp kdc1.myco.com` ein. Auf diese Weise starten Sie eine FTP-Sitzung auf Ihrem PC. Sie werden aufgefordert, den Benutzernamen und das Kennwort des Administrators einzugeben.
2. Geben Sie bei der FTP-Eingabeaufforderung `lcd "C:\Documents and Settings\All Users\Documents\IBM\Client Access"` ein. Drücken Sie die Eingabetaste. Sie sollten die Nachricht `Lokales Verzeichnis jetzt C:\Documents and Settings\All Users\Documents\IBM\Client Access` empfangen.
3. Geben Sie bei der FTP-Eingabeaufforderung `binary` ein. Damit wird angezeigt, dass die zu übertragende Datei binär ist.
4. Geben Sie bei der FTP-Eingabeaufforderung `cd \meinVerzeichnis` ein. *meinVerzeichnis* bezeichnet ein auf kdc1.myco.com befindliches Verzeichnis.
5. Geben Sie bei der FTP-Eingabeaufforderung `put NASConfigiseriesa.bat` ein. Sie sollten diese Nachricht empfangen: `226 Transfer complete`.

**Stapeldatei auf kdc1.myco.com ausführen**

1. Öffnen Sie auf dem Windows 2000-Server den Ordner, in den Sie die Stapeldateien übertragen haben.
2. Suchen Sie die Datei NASConfigiseriesa.bat, und klicken Sie doppelt auf die Datei, um sie auszuführen.

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 **Start → Programme → Verwaltungstools → Active Directory-Benutzer und -Computer → Benutzer**.
   b. Vergewissern Sie sich, dass die iSeries über ein Benutzerkonto verfügt, indem Sie die entsprechende Windows-Domäne auswählen.

      **Anmerkung:** Diese Windows-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 **iseriesa_1_krbsvr400**. Dies ist das Benutzerkonto, das für den i5/OS-Principal-Namen generiert wurde.
   d. (Optional) Rufen Sie die Eigenschaften der Active Directory-Benutzer auf. Wählen Sie auf der Indexzunge **Konto** die Option **Konto wird für Delegierungszwecke vertraut** aus.

      **Anmerkung:** Dieser optionale Schritt ermöglicht Ihrem System, die Berechtigungen 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. In einem Netzwerk mit mehreren Ebenen ist dies nützlich.

Sie haben den i5/OS-Service-Principal zum Kerberos-Server hinzugefügt und müssen jetzt für jeden Ihrer Benutzer ein Ausgangsverzeichnis erstellen.

## Schritt 4: Ein Ausgangsverzeichnis für Benutzer auf der iSeries A erstellen

Jeder Benutzer, der eine Verbindung zu i5/OS und i5/OS-Anwendungen herstellen möchte, benötigt ein Verzeichnis im Ausgangsverzeichnis (/home). Dieses Verzeichnis enthält den Namen des Kerberos-Cache für Berechtigungsnachweise, der dem Benutzer zugeordnet ist. Führen Sie folgende Schritte durch, um ein Ausgangsverzeichnis für einen Benutzer zu erstellen:

Geben Sie in der i5/OS-Befehlszeile Folgendes ein: `CRTDIR '/home/Benutzerprofil'`, wobei `Benutzerprofil` den Namen des i5/OS-Benutzerprofils für den Benutzer bezeichnet. Beispiel: `CRTDIR '/home/JOHND'` für den Benutzer John Day.

Wiederholen Sie den Befehl für Sharon Jones, geben Sie jedoch das entsprechende i5/OS-Benutzerprofil, `SHARONJ`, an.

Sie haben für alle Benutzer Ausgangsverzeichnisse erstellt und müssen jetzt sicherstellen, dass der Netzwerkauthentifizierungsservice ordnungsgemäß funktioniert.

## Schritt 5: Netzwerkauthentifizierungsservice auf der iSeries A testen

Sie müssen sicherstellen, dass der Netzwerkauthentifizierungsservice ordnungsgemäß konfiguriert wurde, indem Sie ein Ticket-granting Ticket für den Principal der iSeries A anfordern:

1. Geben Sie in einer Befehlszeile `QSH` ein, um den Qshell Interpreter zu starten.
2. Geben Sie `keytab list` ein, um eine Liste der Principals, die in der Chiffrierschlüsseldatei registriert sind, anzuzeigen. Die folgenden Ergebnisse sollten angezeigt werden:

```
Principal: krbsvr400/iseriesa.myc.com@MYCO.COM
  Key version: 2
  Key type: 56-bit DES using key derivation
  Entry timestamp: 200X/05/29-11:02:58
```

3. Geben Sie `kinit -k krbsvr400/iseriesa.myco.com@MYCO.COM` ein, um ein Ticket-granting Ticket vom Kerberos-Server anzufordern. Mit diesem Befehl wird geprüft, ob Ihr iSeries-Server ordnungsgemäß konfiguriert wurde und das Kennwort in der Chiffrierschlüsseldatei mit dem auf dem Kerberos-Server gespeicherten Kennwort übereinstimmt. Ist dies der Fall, kann der Befehl QSH 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-Cache für Berechtigungsnachweise angezeigt und geprüft, ob ein gültiges Ticket für den i5/OS-Service-Principal erstellt und in den Cache für Berechtigungsnachweise auf dem iSeries-System aufgenommen wurde.

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

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

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

Sie haben die Tasks, die zur Konfiguration des Netzwerkauthentifizierungsservice auf der iSeries A erforderlich sind, abgeschlossen.

## Szenario: Cross-Realm-Vertrauensbeziehung konfigurieren

### Situation

Sie sind Sicherheitsadministrator für ein Großhandelsunternehmen. Gegenwärtig verwalten Sie die Sicherheit für Systeme, die von Mitarbeitern der Auftragsannahme und des Versands verwendet werden. Sie haben einen Kerberos-Server für die Auftragsannahme konfiguriert. Sie haben den Netzwerkauthentifizierungsservice auf dem iSeries-System in dieser Abteilung so konfiguriert, dass er auf diesen Kerberos-Server verweist. Der Versand besteht aus einem iSeries-System, das einen in i5/OS PASE konfigurierten Kerberos-Server besitzt. Sie haben auf diesem iSeries-System einen Netzwerkauthentifizierungsservice konfiguriert, der auf den Kerberos-Server in i5/OS PASE verweist.

Da Benutzer in beiden Realms Services verwenden müssen, die auf iSeries-Systemen in jeder Abteilung gespeichert sind, sollen beide Kerberos-Server in jeder Abteilung Benutzer authentifizieren, unabhängig davon, in welchem Kerberos-Realm sie sich befinden.

### Ziele

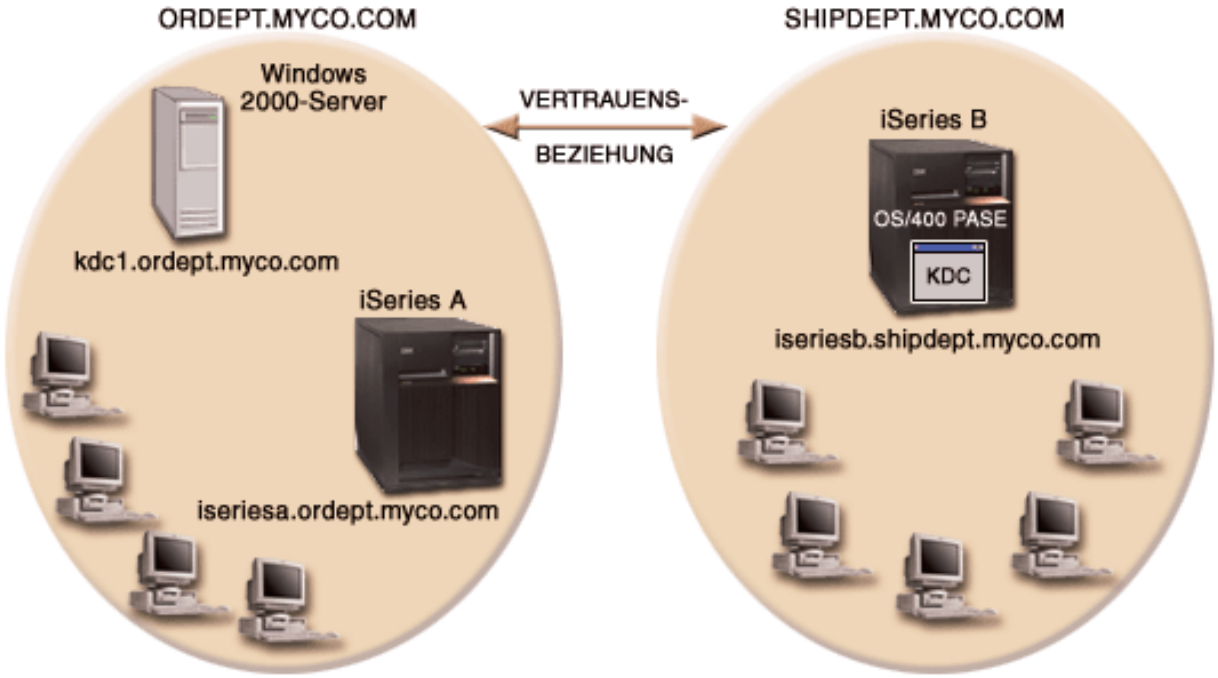
In diesem Szenario möchte MyCo, Inc. eine Vertrauensbeziehung zwischen zwei bereits bestehenden Kerberos-Realms herstellen: Ein Realm besteht aus einem Windows 2000-Server, der als Kerberos-Server für die Auftragsannahme fungiert. Dieser Server authentifiziert Benutzer, die in dieser Abteilung arbeiten, für Services, die auf einem iSeries-Server installiert sind. Der andere Realm besteht aus einem Kerberos-Server, der in i5/OS PASE auf einer iSeries konfiguriert ist, die Services für die Benutzer im Versand zur Verfügung stellt. Die Benutzer müssen für Services in beiden Abteilungen authentifiziert werden.

Die Ziele dieses Szenarios:

- Clients und Hosts soll in jedem Netzwerk die Zugriffsberechtigung für das jeweils andere Netzwerk erteilt werden
- Die Authentifizierung in Netzwerken soll vereinfacht werden
- Die Ticket-Delegierung für Benutzer und Services soll in beiden Netzwerken zugelassen werden

## Details

Detaillierte Beschreibung der Umgebung, die dieses Szenario verwendet, einschließlich einer Abbildung, die die Topologie und alle wichtigen Elemente dieser Umgebung sowie deren wechselseitige Beziehungen veranschaulicht.




**Auftragsannahme**

**iSeries A**

- Wird unter i5/OS Version 5 Release 3 (V5R3) mit den folgenden Optionen und Lizenzprogrammen ausgeführt:
  - i5/OS Host-Server (5722-SS1 Option 12)
  - iSeries Access für Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3)
- Der Netzwerkauthentifizierungsservice ist für die Teilnahme am Realm ORDEPT.MYCO.COM konfiguriert. Der i5/OS-Principal, krbsrv400/iseriesa.ordept.myco.com@ORDEPT.MYCO.COM, wurde zur Windows 2000-Domäne hinzugefügt.
- iSeries A hat den vollständig qualifizierten Hostnamen iseriesa.ordept.myco.com.

**Windows 2000-Server**

- Fungiert als Kerberos-Server für den Realm ORDEPT.MYCO.COM.
- Hat den DNS-Hostnamen kdc1.ordept.myco.com.
- Jeder Benutzer, der in der Auftragsannahme arbeitet, wurde im Microsoft Active Directory auf dem Windows 2000-Server mit einem Principal-Namen und -Kennwort definiert.

**Client-PCs**

- Verwenden das Betriebssystem Windows 2000.
- Auf dem PC zur Verwaltung des Netzwerkauthentifizierungsservice sind die folgenden Produkte installiert:
  - iSeries Access für Windows (5722-XE1)

– iSeries Navigator und die folgenden Unterkomponenten:
  - Sicherheit
  - Netzwerk

**Versand**

**iSeries B**

- Wird unter i5/OS Version 5 Release 3 (V5R3) mit den folgenden Optionen und Lizenzprogrammen ausgeführt:
  – i5/OS PASE (5722-SS1 Option 33)
  – Cryptographic Access Provider (5722-AC3)
  – iSeries Access für Windows (5722-XE1)
- Hat einen in i5/OS PASE konfigurierten Kerberos-Server mit dem Realm SHIPDEPT.MYCO.COM.
- Der Netzwerkauthentifizierungsservice ist für die Teilnahme am Realm SHIPDEPT.MYCO.COM konfiguriert. Der i5/OS-Principal, krbsrv400/iseriesb.shipdept.myco.com@SHIPDEPT.MYCO.COM, wurde dem i5/OS PASE-Kerberos-Server hinzugefügt.
- iSeries B und der i5/OS PASE-Kerberos-Server verwenden den vollständig qualifizierten Hostnamen iseriesb.shipdept.myco.com.
- Jeder Benutzer, der in der Auftragsannahme arbeitet, wurde auf dem i5/OS PASE-Kerberos-Server mit einem Principal-Namen und -Kennwort definiert.

**Client-PCs**

- Verwenden das Betriebssystem Windows 2000.
- Auf dem PC zur Verwaltung des Netzwerkauthentifizierungsservice sind die folgenden Produkte installiert:
  – iSeries Access für Windows (5722-XE1)
  – iSeries Navigator und die folgenden Unterkomponenten:
    - Sicherheit
    - Netzwerk

## Voraussetzungen und Annahmen

In diesem Szenario werden die folgenden Punkte als gegeben vorausgesetzt; das Szenario konzentriert sich auf die Tasks zur Herstellung einer Vertrauensbeziehung zwischen zwei bereits bestehenden Kerberos-Realms.

**iSeries A - Voraussetzungen**

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 iSeries Navigator den Eintrag für Ihren **iSeries-Server → 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 Basissystemsicherheit wurden auf iSeries A konfiguriert und getestet.
4. Der Netzwerkauthentifizierungsservice wurde konfiguriert und getestet.
5. Ein einzelner DNS-Server wird für die Auflösung der Hostnamen im Netzwerk verwendet. Es werden keine Hosttabellen für die Auflösung der Hostnamen verwendet.

**Anmerkung:** Die Verwendung von Hosttabellen mit Kerberos-Authentifizierung kann zu Fehlern bei der Namensauflösung oder anderen Problemen führen. Ausführliche Informationen zur Auflösung von Hostnamen mit der Kerberos-Authentifizierung finden Sie unter „Hinweise zur Auflösung von Hostnamen" auf Seite 95.

**iSeries B - Voraussetzungen**

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 iSeries Navigator den Eintrag für Ihren **iSeries-Server → 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 Basissystemsicherheit wurden auf Ihrem iSeries-Server konfiguriert und getestet.
4. Der Netzwerkauthentifizierungsservice wurde konfiguriert und getestet.

**Windows 2000-Server - Voraussetzungen**

1. Die gesamte erforderliche Hardwareplanung und -konfiguration wurde durchgeführt.
2. TCP/IP wurde auf dem Server konfiguriert und getestet.
3. Microsoft Active Directory wurde konfiguriert und getestet.
4. Jeder Benutzer, der in der Auftragsannahme arbeitet, wurde in Microsoft Active Directory mit einem Principal-Namen und -Kennwort definiert.

## Konfigurationsschritte

Gehen Sie wie folgt vor, um eine Vertrauensbeziehung zwischen zwei Realms zu definieren:

1. Planungsarbeitsblatt ausfüllen
2. Sicherstellen, dass der Kerberos-Server in i5/OS PASE auf iSeries B gestartet wurde
3. Realm-Trust-Principal auf dem i5/OS PASE-Kerberos-Server erstellen
4. Verschlüsselungswerte auf dem i5/OS PASE-Kerberos-Server ändern
5. Windows 2000-Server so konfigurieren, dass der Realm SHIPDEPT.MYCO.COM als vertrauenswürdig akzeptiert wird
6. Den Realm SHIPDEPT.MYCO.COM der iSeries A hinzufügen

## Details zum Szenario: Cross-Realm-Vertrauensbeziehung konfigurieren

Die folgenden Tasks sind erforderlich, um eine Cross-Realm-Vertrauensbeziehung zwischen der Auftragsannahme und dem Versand von MyCo zu konfigurieren. Lesen Sie den Abschnitt Voraussetzungen und Annahmen und vergewissern Sie sich, dass Sie alle erforderlichen Tasks ausgeführt haben, bevor Sie das folgende Szenario durcharbeiten:

## Schritt 1: Planungsarbeitblatt ausfüllen

Das folgende Planungsarbeitsblatt veranschaulicht die Art der Informationen, die Sie benötigen, um mit der Konfiguration der Cross-Realm-Vertrauensbeziehung beginnen zu können.

Das folgende Planungsarbeitsblatt enthält Informationen, die Sie vervollständigen müssen, bevor Sie die Tasks des Szenarios ausführen.

*Tabelle 6. Planungsarbeitsblatt für Voraussetzungen*

| Fragen | Antworten |
|---|---|
| Arbeiten Sie mit i5/OS V5R3 (5722-SS1) oder einer späteren Version? | Ja |
| Sind die folgenden Optionen und Lizenzprogramme auf der iSeries A installiert?<br>• i5/OS Host-Server (5722-SS1 Option 12)<br>• iSeries Access für Windows (5722-XE1)<br>• Cryptographic Access Provider (5722-AC3) | Ja |
| Sind die folgenden Lizenzprogramme auf der iSeries B installiert?<br>• iSeries Access für Windows (5722-XE1)<br>• Cryptographic Access Provider (5722-AC3)<br>• i5/OS PASE (5722-SS1 Option 33) | Ja |
| Ist auf allen PCs Windows 2000 installiert? | Ja |
| Ist iSeries Access für Windows (5722-XE1) auf dem PC installiert, der zur Verwaltung des Netzwerkauthentifizierungsservice verwendet wird? | Ja |
| Sind iSeries Navigator und die folgenden Unterkomponenten auf dem PC installiert, der zur Verwaltung des Netzwerkauthentifizierungsservice verwendet wird?<br>• Sicherheit<br>• Netzwerk | Ja |
| Ist das aktuellste Service-Pack für iSeries Access für Windows installiert? Sie können das aktuellste Service-Pack über iSeries Access abrufen. | Ja |
| Besitzen Sie die Sonderberechtigung *ALLOBJ für die iSeries-Server? | Ja |
| Besitzen Sie die Administratorberechtigung für den Windows 2000-Server? | Ja |
| Ist der DNS konfiguriert und verwenden Sie die richtigen Hostnamen für den iSeries-Server und den Kerberos-Server? | Ja |
| Unter welchem Betriebssystem möchten Sie den Kerberos-Server konfigurieren?<br>1. Windows (R) 2000-Server<br>2. Windows Server 2003<br>3. AIX Server<br>4. i5/OS PASE (ab V5R3)<br>5. zSeries | i5/OS PASE |
| Wurden die aktuellsten vorläufigen Programmkorrekturen (PTFs) angelegt? | Ja |
| Beträgt die Abweichung zwischen der Systemzeit der iSeries und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung größer, lesen Sie Systemzeiten synchronisieren. | Ja |

*Tabelle 7. Planungsarbeitsblatt für Cross-Realm-Vertrauensbeziehung*

| Planungsarbeitsblatt für Cross-Realm-Vertrauensbeziehung | Antworten |
|---|---|
| Wie lauten die Namen der Realms, für die Sie eine Vertrauensbeziehung herstellen möchten?<br>• Der Kerberos-Realm, der den Windows 2000-Server als Kerberos-Server verwendet<br>• Der Kerberos-Realm, der iSeries B als Kerberos-Server (konfiguriert in i5/OS PASE) verwendet | ORDEPT.MYCO.COM<br>SHIPDEPT.MYCO.COM |

Tabelle 7. Planungsarbeitsblatt für Cross-Realm-Vertrauensbeziehung (Forts.)

| Planungsarbeitsblatt für Cross-Realm-Vertrauensbeziehung | Antworten |
|---|---|
| Wurden alle i5/OS-Service-Principals und Benutzer-Principals den entsprechenden Kerberos-Servern zugeordnet? | Ja |
| Wie lautet der Standardbenutzername für den i5/OS PASE-Administrator?<br><br>Welches Kennwort möchten Sie für den i5/OS PASE-Administrator angeben?<br>**Anmerkung:** Dieses Kennwort muss mit dem Kennwort übereinstimmen, das Sie bei der Einrichtung des Kerberos-Servers in i5/OS PASE verwendet haben. 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. | Benutzername: admin/admin<br>Kennwort: secret |
| Wie lauten die Principal-Namen, die zur Konfiguration der Cross-Realm-Vertrauensbeziehung verwendet werden?<br><br>Wie lautet das Kennwort für jeden dieser Principals?<br>**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. | Principal:<br>krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM<br><br>Kennwort: shipord1<br><br>Principal:<br>krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO<br>.COM<br><br>Kennwort: shipord2 |
| Wie lauten die vollständig qualifizierten Hostnamen für die einzelnen Kerberos-Server dieser Realms?<br>• ORDEPT.MYCO.COM<br>• SHIPDEPT.MYCO.COM | kdc1.ordept.myco.com<br>iseriesb.shipdept.myco.com |
| Weichen die Systemzeiten aller Systeme nicht mehr als fünf Minuten voneinander ab? Ist die Abweichung größer, lesen Sie Systemzeiten synchronisieren. | Ja |

## Schritt 2: Sicherstellen, dass der Kerberos-Server in i5/OS PASE auf iSeries B gestartet wurde

Vor der Konfiguration der Cross-Realm-Vertrauensbeziehung müssen Sie sicherstellen, dass der i5/OS PASE-Kerberos-Server gestartet wurde. Sie verwenden den Verarbeitungsstatistikbefehl, um zu ermitteln, ob der i5/OS PASE-Kerberos-Server gestartet wurde.

1. Geben Sie in einer zeichenorientierten Schnittstelle auf der iSeries B `call QP2TERM` ein. Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.
2. Geben Sie in der Befehlszeile `ps -ef | grep krb5` ein. Dieser Befehl zeigt an, dass Sie für jeden Prozess im System, der die Zeichenfolge krb5 enthält, alle Verarbeitungsstatistiken anzeigen möchten. Wird der Kerberos-Server ausgeführt, werden möglicherweise Ergebnisse wie die folgenden angezeigt:

```
> ps -ef | grep krb5
    qsys   113   1   0 08:54:04      -  0:00 /usr/krb5/sbin/krb5kdc
    qsys   123   1   0 08:54:13      -  0:00 /usr/krb5/sbin/kadmind
  $
```

Wurde der Kerberos-Server nicht gestartet, werden möglicherweise die folgenden Ergebnisse angezeigt:

```
> ps -ef | grep krb5
  $
```

3. Führen Sie die folgenden Schritte durch, wenn der Kerberos-Server nicht gestartet wurde:
   a. Geben Sie in der Befehlszeile `export PATH=$PATH:/usr/krb5/sbin` ein, und drücken Sie die Eingabetaste.
   b. Geben Sie `start.krb5` ein, und drücken Sie die Eingabetaste.

   Die folgenden Ergebnisse werden angezeigt:

```
> start.krb5
  Starting krb5kdc...
  krb5kdc was started successfully.
  Starting kadmind...
  kadmind was started successfully.
  The command completed successfully.
  $
```

Sie haben sichergestellt, dass der Kerberos-Server auf iSeries B gestartet wurde und müssen jetzt einen Realm-Trust-Principal auf dem Kerberos-Server erstellen.

## Schritt 3: Realm-Trust-Principal auf dem i5/OS PASE-Kerberos-Server erstellen

1. Geben Sie in einer zeichenorientierten Schnittstelle `call QP2TERM` ein. Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.
2. Geben Sie in der Befehlszeile `export PATH=$PATH:/usr/krb5/sbin` ein. Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.
3. Geben Sie in der Befehlszeile `kadmin -p admin/admin` ein, und drücken Sie die Eingabetaste.
4. Melden Sie sich mit dem Kennwort des Administrators an. Beispiel: `secret`.
5. Geben Sie bei der kadmin-Eingabeaufforderung `addprinc krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM` ein. Sie werden aufgefordert, ein Kennwort für den Principal "krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM" einzugeben. Geben Sie `shipord1` als Kennwort ein. Drücken Sie die Eingabetaste. Sie werden aufgefordert, das Kennwort erneut einzugeben. Dann empfangen Sie eine Nachricht wie folgende:

```
Principal "krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM" created.
```

   .
6. Geben Sie bei der kadmin-Eingabeaufforderung `addprinc krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO.COM` ein. Sie werden aufgefordert, ein Kennwort für den Principal "krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO.COM" einzugeben. Geben Sie `shipord2` als Kennwort ein. Drücken Sie die Eingabetaste. Sie werden aufgefordert, das Kennwort erneut einzugeben. Dann empfangen Sie eine Nachricht wie folgende:

```
Principal "krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO.COM" created.
```

7. Geben Sie `quit` ein, um die kadmin-Schnittstelle zu verlassen, und drücken Sie F3 (Verlassen), um die PASE-Umgebung zu verlassen.

Sie haben den Realm-Trust-Principal auf dem i5/OS PASE-Kerberos-Server erstellt und müssen jetzt die Verschlüsselungswerte auf dem Server ändern.

## Schritt 4: Verschlüsselungswerte auf dem i5/OS PASE-Kerberos-Server ändern

Die Standardverschlüsselungseinstellungen des Kerberos-Servers müssen geändert werden, damit Clients am i5/OS PASE-Kerberos-Server authentifiziert werden können und ein Betrieb mit Windows-Workstations möglich ist. Zum Ändern der Standardverschlüsselungseinstellungen müssen Sie die Datei kdc.conf im Verzeichnis /var/krb5/krb5kdc editieren. Gehen Sie dazu wie folgt vor:

1. Geben Sie in einer zeichenorientierten Schnittstelle `edtf '/var/krb5/krb5kdc/kdc.conf'` ein, um auf die Datei kdc.conf zuzugreifen.
2. Ändern Sie die folgenden Zeilen in der Datei kdc.conf:

```
supported_enctypes = des3-cbc-sha1:normal
des-cbc-md5:normal des-cbc-crc:normal
kdc_supported_enctypes = des3-cbc-sha1:normal
des-cbc-md5:normal des-cbc-crc:normal
```

   in

```
supported_enctypes = des-cbc-md5:normal
kdc_supported_enctypes = des-cbc-md5:normal
```

Sie haben die Verschlüsselungswerte auf dem Kerberos-Server geändert und müssen jetzt den Windows 2000-Server so konfigurieren, dass er den Realm SHIPDEPT.MYCO.COM als vertrauenswürdig akzeptiert.

## Schritt 5: Windows 2000-Server so konfigurieren, dass SHIPDEPT.MYCO.COM als vertrauenswürdig akzeptiert wird

Sie haben die iSeries B so konfiguriert, dass sie den Realm ORDEPT.MYCO.COM (wird manchmal als eine Windows-Domäne innerhalb der Windows-Schnittstelle bezeichnet) als vertrauenswürdig akzeptiert. Jetzt müssen Sie den Windows 2000-Server so konfigurieren, dass er den Realm SHIPDEPT.MYCO.COM als vertrauenswürdig akzeptiert.

1. Melden Sie sich über Ihr Administratorkonto am Windows 2000-Server an.
2. Klicken Sie im Startmenü auf **Programme** → **Verwaltungstools** → **Active Directory-Domänen und Vertrauensstellungen**.
3. Klicken Sie auf der Seite **Active-Directory-Domänen und Vertrauensstellungen** mit der rechten Maustaste auf den Realm **ORDEPT.MYCO.COM** (wird manchmal als eine Windows-Domäne innerhalb der Windows-Schnittstelle bezeichnet) und wählen Sie **Eigenschaften** aus.
4. Klicken Sie auf der Indexzunge **Vertrauensbeziehung** in der Tabelle **Domänen, denen diese Domäne vertraut** auf **Hinzufügen**.
5. Geben Sie auf der Seite **Vertraute Domänen hinzufügen** im Feld **Vertraute Domäne** die Zeichenfolge `SHIPDEPT.MYCO.COM` ein. Geben Sie `shipord1` als Kennwort ein.
6. Das Dialogfenster **Active Directory** erscheint mit der Nachricht, dass zur Domäne MYCO.COM keine Verbindung hergestellt werden kann. Da die Domäne MYCO.COM eine interoperable Nicht-Windows-Domäne ist und Sie diese Seite der Vertrauensbeziehung konfigurieren möchten, klicken Sie auf **OK**, um das Dialogfenster zu schließen.
7. Klicken Sie auf der Indexzunge **Vertrauensbeziehung** in der Tabelle **Domänen, die dieser Domäne vertrauen** auf **Hinzufügen**.
8. Geben Sie auf der Seite **Vertraute Domänen hinzufügen** im Feld **Vertraute Domäne** die Zeichenfolge `SHIPDEPT.MYCO.COM` ein. Geben Sie `shipord2` als Kennwort ein.
9. Das Dialogfenster **Active Directory** erscheint mit der Nachricht, dass zur Domäne MYCO.COM keine Verbindung hergestellt werden kann. Da die Domäne MYCO.COM eine interoperable Nicht-Windows-Domäne ist und Sie diese Seite der Vertrauensbeziehung konfigurieren möchten, klicken Sie auf **OK**, um das Dialogfenster zu schließen.
10. Klicken Sie auf **OK**.

Jetzt müssen Sie den Realm SHIPDEPT.MYCO.COM auf der iSeries A definieren.

### Schritt 6: Den Realm SHIPDEPT.MYCO.COM zur iSeries A hinzufügen

Sie müssen den Realm SHIPDEPT.MYCO.COM auf der iSeries A definieren, damit die iSeries A feststellen kann, wo sich der i5/OS PASE-Kerberos-Server im Realm SHIPDEPT.MYCO.COM befindet.

1. Erweitern Sie im iSeries Navigator den Eintrag **iSeries A** → **Sicherheit** → **Netzwerkauthentifizierungsservice**.
2. Klicken Sie mit der rechten Maustaste auf **Realms**, und wählen Sie **Realm hinzufügen...** aus.
3. Geben Sie im Dialogfenster **Realm hinzufügen** die folgenden Informationen an, und klicken Sie auf **OK**.
   - **Hinzuzufügender Realm**: `SHIPDEPT.MYCO.COM`
   - **KDC**: `iseriesb.shipdept.myco.com`
   - **Port**: 88
4. Klicken Sie auf **Realms**, um die Liste der Realms im rechten Teilfenster anzuzeigen. Vergewissern Sie sich, dass der Realm SHIPDEPT.MYCO.COM in der Liste erscheint.

Sie haben jetzt die Schritte zur Konfiguration einer Cross-Realm-Vertrauensbeziehung zwischen den Realms ORDEPT.MYCO.COM und SHIPDEPT.MYCO.COM durchgeführt.

## Szenario: Konfiguration des Netzwerkauthentifizierungsservice an mehrere Systeme weitergeben

### Situation

Sie sind der Systemadministrator für ein Großunternehmen, das Kfz-Teile herstellt. Sie verwalten gegenwärtig fünf iSeries-Systeme mit dem iSeries Navigator. Ein System fungiert als zentrales System, das Daten speichert und die anderen Systeme verwaltet. Der Sicherheitsadministrator für Ihr Unternehmen hat soeben einen Netzwerkauthentifizierungsservice auf einem neuen System zur Teilnahme an einer Windows 2000-Domäne konfiguriert. Der Service authentifiziert Benutzer für das Unternehmen. Der Sicherheitsadministrator hat die Konfiguration des Netzwerkauthentifizierungsservice auf diesem System getestet und ein Service-Ticket für diesen iSeries-Server abgerufen. Sie möchten die Konfiguration des Netzwerkauthentifizierungsservice zwischen diesen von Ihnen verwalteten Systemen, vereinfachen.

Mit dem Assistenten für Funktionssynchronisation möchten Sie die Konfiguration des Netzwerkauthentifizierungsservice vom Modellsystem auf Ihre anderen Systeme anwenden. Der Assistent für Funktionssynchronisation beschleunigt und vereinfacht die Konfiguration des Netzwerkauthentifizierungsservice im gesamten Netzwerk, da Sie nicht jedes System separat konfigurieren müssen.

Da eines der Systeme i5/OS Version 5 Release 2 (V5R2) verwendet und dieses Release den Assistenten für Funktionssynchronisation nicht unterstützt, müssen Sie dieses System mit dem Assistenten für den Netzwerkauthentifizierungsservice konfigurieren. Sie müssen dieses System so konfigurieren, dass es mit der Konfiguration des Netzwerkauthentifizierungsservice auf Ihrem Modellsystem übereinstimmt.

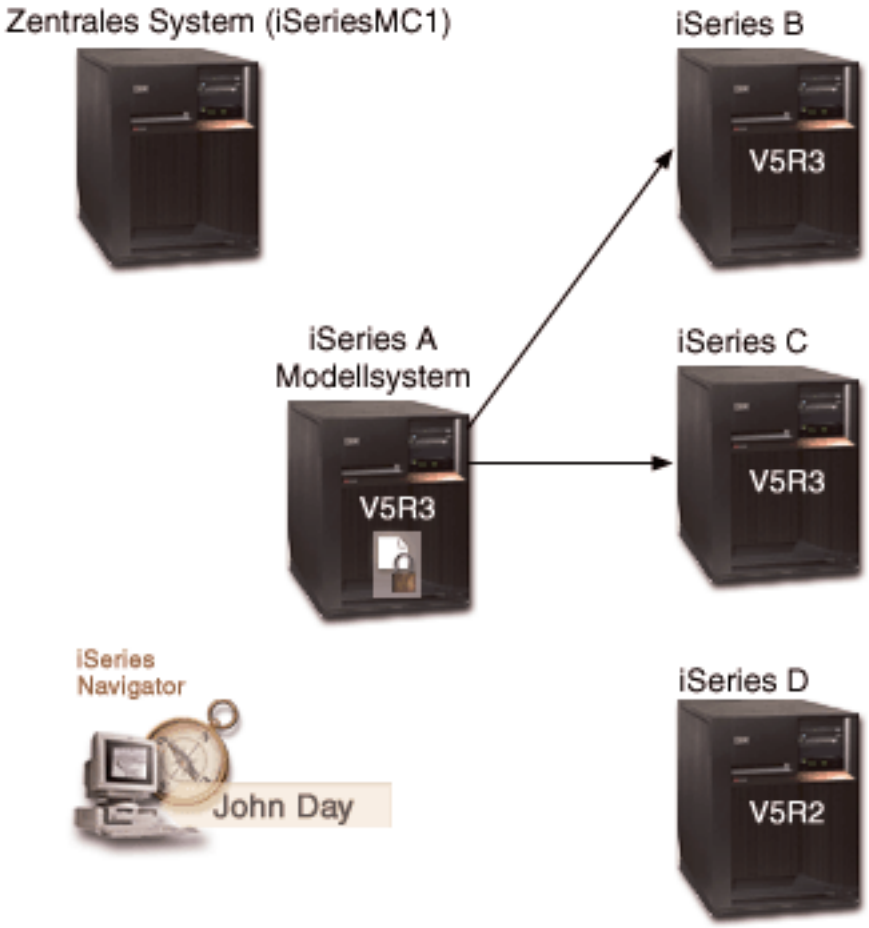
### Ziele

In diesem Szenario verfolgt MyCo, Inc. drei verschiedene Ziele:

1. Die Konfiguration des Netzwerkauthentifizierungsservice im Netzwerk soll vereinfacht werden.
2. Alle iSeries-Systeme sollten auf denselben Kerberos-Server verweisen.
3. Das V5R2-System soll ebenfalls für die Teilnahme am Kerberos-Realm konfiguriert werden.

## Details

Die folgende Abbildung veranschaulicht die Details für dieses Szenario.




**iSeriesMC1 - Zentrales System**

- Wird unter i5/OS Version 5 Release 3 (V5R3) mit den folgenden Optionen und Lizenzprogrammen ausgeführt:
  - i5/OS Host-Server (5722-SS1 Option 12)
  - iSeries Access für Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3)
- Speichert und plant für jedes der Endpunktsysteme Tasks hinsichtlich der Synchronisationseinstellungen und führt diese aus.

**iSeries A - Modellsystem**

- Wird unter i5/OS Version 5 Release 3 (V5R3) mit den folgenden Optionen und Lizenzprogrammen ausgeführt:
  - i5/OS Host-Server (5722-SS1 Option 12)
  - iSeries Access für Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3)
- Ist das Modellsystem für die Weitergabe der Konfiguration des Netzwerkauthentifizierungsservice an Endpunktsysteme.

**iSeries B - Endpunktsystem**

- Wird unter i5/OS Version 5 Release 3 (V5R3) mit den folgenden Optionen und Lizenzprogrammen ausgeführt:
  - i5/OS Host-Server (5722-SS1 Option 12)
  - iSeries Access für Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3)
- Ist eines der Endpunktsysteme für die Weitergabe der Konfiguration des Netzwerkauthentifizierungsservice.

**iSeries C - Endpunktsystem**

- Wird unter i5/OS Version 5 Release 3 (V5R3) mit den folgenden Optionen und Lizenzprogrammen ausgeführt:
  - i5/OS Host-Server (5722-SS1 Option 12)
  - iSeries Access für Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3)
- Ist eines der Endpunktsysteme für die Weitergabe der Konfiguration des Netzwerkauthentifizierungsservice.

**iSeries D - Endpunktsystem**

- Wird unter i5/OS Version 5 Release 2 (V5R2) mit den folgenden Optionen und Lizenzprogrammen ausgeführt:
  - i5/OS Host-Server (5722-SS1 Option 12)
  - iSeries Access für Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3)
- Die folgenden vorläufigen Programmkorrekturen (PTFs) für V5R2 wurden angelegt:
  - SI08977
  - SI08979
- Erfordert eine separate Konfiguration des Netzwerkauthentifizierungsservice mit dem Assistenten für den Netzwerkauthentifizierungsservice im iSeries Navigator.

**Client-PC**

- Wird unter iSeries Access für Windows V5R3 (5722-XE1) ausgeführt.
- Wird unter iSeries Navigator V5R3 mit den folgenden Unterkomponenten ausgeführt:

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

**Windows 2000-Server (nicht in der Grafik dargestellt)**

- Fungiert als Kerberos-Server für das Netzwerk (kdc1.myco.com).
- Alle Benutzer wurden Microsoft Windows Active Directory hinzugefügt.

## Voraussetzungen und Annahmen

**iSeriesMC1 - 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 iSeries Navigator den Eintrag für Ihren **iSeries-Server → 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 Basissystemsicherheit wurden auf iSeries A konfiguriert und getestet.
4. Die Standardeinstellungen im iSeries Navigator wurden nicht dahingehend geändert, dass das Öffnen des Fensters "Task-Status" beim Starten einer Task inaktiviert wird. Gehen Sie wie folgt vor, um sicherzustellen, dass die Standardeinstellungen nicht geändert wurden:

   a. Klicken Sie im iSeries Navigator mit der rechten Maustaste auf **Ihr zentrales System**, und wählen Sie **Benutzervorgaben** aus.

   b. Vergewissern Sie sich auf der Seite **Allgemein**, dass die Option **Fenster 'Task-Status' automatisch öffnen, wenn eine meiner Tasks gestartet wird** ausgewählt ist.

5. 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 Szenario: Alle Verbindungen zum Management Central-Server mit SSL sichern.

**iSeries A - Voraussetzungen des Modellsystems**

1. Bei diesem Szenario wird vorausgesetzt, dass der Netzwerkauthentifizierungsservice auf dem Modellsystem (iSeries A) richtig konfiguriert ist.
2. 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 iSeries Navigator den Eintrag für Ihren **iSeries-Server → Konfiguration und Service → Software → Installierte Produkte**.

   b. Vergewissern Sie sich, dass alle erforderlichen Lizenzprogramme installiert sind.

3. Die gesamte erforderliche Hardwareplanung und -konfiguration wurde durchgeführt.
4. TCP/IP und Basissystemsicherheit wurden auf Ihrem iSeries-Server konfiguriert und getestet.
5. 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 Szenario: Alle Verbindungen zum Management Central-Server mit SSL sichern.

**iSeries B, iSeries C und iSeries D - Voraussetzungen für Endpunktsystem**

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 iSeries Navigator den Eintrag für Ihren **iSeries-Server → 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 Basissystemsicherheit wurden auf Ihrem iSeries-Server 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 Szenario: Alle Verbindungen zum Management Central-Server mit SSL sichern.

**Windows 2000-Server (nicht in der Grafik dargestellt)**

1. Die gesamte erforderliche Hardwareplanung und -konfiguration wurde durchgeführt.
2. TCP/IP wurde auf dem Server konfiguriert und getestet.
3. Windows-Domäne wurde konfiguriert und getestet.
4. Alle Benutzer im Netzwerk wurden über Active Directory zu einer Windows-Domäne hinzugefügt.

## Konfigurationsschritte

Sie müssen die folgenden Tasks ausführen, um mit dem Assistenten für Funktionssynchronisation die Konfiguration des Netzwerkauthentifizierungsservice an Endpunktsysteme weiterzugeben:

1. Planungsarbeitsblatt ausfüllen.
2. Systemverwaltungsgruppe erstellen.
3. Systemeinstellungen vom Modellsystem (iSeries A) an iSeries B und iSeries C weitergeben.
4. Netzwerkauthentifizierungsservice auf iSeries D konfigurieren.
5. Die Principals für Endpunktsysteme zur Windows 2000-Domäne hinzufügen.

Wenn Sie den Management Central-Server so konfigurieren möchten, dass er den Netzwerkauthentifizierungsservice nutzt, müssen Sie einige zusätzliche Tasks ausführen. Detaillierte Anweisungen hierzu finden Sie unter „Szenario: Kerberos-Authentifizierung zwischen Management Central-Servern verwenden" auf Seite 41.

## Details zum Szenario: Konfiguration des Netzwerkauthentifizierungsservice an mehrere Systeme weitergeben

Die folgenden Tasks sind erforderlich, um den iSeries Navigator zur Weitergabe der Konfiguration eines Netzwerkauthentifizierungsservice an Endpunktsysteme verwenden zu können. Lesen Sie den Abschnitt Voraussetzungen und Annahmen und vergewissern Sie sich, dass Sie alle erforderlichen Tasks ausgeführt haben, bevor Sie das folgende Szenario durcharbeiten:

## Schritt 1: Planungsarbeitsblätter ausfüllen

Die folgenden Arbeitsblätter veranschaulichen die Art der Informationen, die Sie benötigen, um mit dem iSeries Navigator die Konfiguration ausgehend von einem Modellsystem an Zielsysteme weitergeben zu können.

*Tabelle 8. Netzwerkauthentifizierungsservice weitergeben - Arbeitsblatt für Voraussetzungen*

| **Arbeitsblatt für Voraussetzungen** | **Antworten** |
|---|---|
| Arbeiten Sie mit i5/OS V5R3 (5722-SS1) oder einer späteren Version für die folgenden Systeme?<br>• Zentrales System<br>• iSeries A<br>• iSeries B<br>• iSeries C | Ja |
| Wurden die aktuellsten vorläufigen Programmkorrekturen (PTFs) angelegt? | Ja |
| Verwenden Sie für die iSeries D i5/OS V5R2 (5722-SS1) oder später? | Ja |
| Haben Sie die aktuellsten vorläufigen Programmkorrekturen (PTFs) für iSeries D angelegt?<br>• SI08977<br>• SI08979 | |
| Sind die folgenden Optionen und Lizenzprogramme auf allen iSeries-Systemen installiert?<br>• i5/OS Host-Server (5722-SS1 Option 12)<br>• iSeries Access für Windows (5722-XE1)<br>• Cryptographic Access Provider (5722-AC3) | Ja |
| Ist iSeries Access für Windows V5R3 (5722-XE1) auf dem Administrator-PC installiert? | Ja |
| Ist iSeries Navigator V5R3 auf dem Administrator-PC installiert?<br>• Ist die Unterkomponente "Netzwerk" des iSeries Navigator auf dem PC des Administrators installiert?<br>• Ist die Unterkomponente "Sicherheit" des iSeries Navigator auf dem PC des Administrators installiert? | Ja |
| Ist das aktuellste Service-Pack von IBM @server iSeries Access für Windows installiert?<br><br>Sie können das aktuellste Service-Pack über iSeries Access abrufen. | Ja |
| Besitzen Sie 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.<br>1. Microsoft Windows 2000-Server<br>**Anmerkung:** Microsoft Windows 2000-Server verwendet die Kerberos-Authentifizierung als Standardsicherheitsmechanismus.<br>2. Windows (R) Server 2003<br>3. i5/OS PASE (ab V5R3)<br>4. AIX-Server<br>5. zSeries | Ja, Windows 2000-Server |
| Für Windows 2000-Server und Windows (R) Server 2003: Sind Windows-Unterstützungstools installiert (beinhalten das Tool ktpass)? | Ja |

*Tabelle 8. Netzwerkauthentifizierungsservice weitergeben - Arbeitsblatt für Voraussetzungen (Forts.)*

| Arbeitsblatt für Voraussetzungen | Antworten |
|---|---|
| Beträgt die Abweichung zwischen der Systemzeit der iSeries und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung größer, lesen Sie Systemzeiten synchronisieren. | Ja |

*Tabelle 9. Planungsarbeitsblatt für Funktionssynchronisation*

| Fragen | Antworten |
|---|---|
| Wie lautet der Name der Systemverwaltungsgruppe? | Systemverwaltungsgruppe MyCo |
| Welche Systeme werden in diese Systemverwaltungsgruppe aufgenommen? | iSeries B, iSeries C, iSeries D |
| Welche Funktionen sollen an diese Systemverwaltungsgruppe weitergegeben werden? | Netzwerkauthentifizierungsservice |
| Für welche Services möchten Sie Chiffrierschlüsseleinträge erstellen?<br>• i5/OS-Kerberos-Authentifizierung<br>• LDAP<br>• iSeries IBM HTTP-Server<br>• iSeries NetServer | i5/OS-Kerberos-Authentifizierung |
| Wie lauten die Service-Principal-Namen für die iSeries-Systeme, an die Sie die Konfiguration weitergeben möchten? | krbsvr400/iseriesa.myco.com@MYCO.COM<br>krbsvr400/iseriesb.myco.com@MYCO.COM<br>krbsvr400/iseriesc.myco.com@MYCO.COM<br>krbsvr400/iseriesd.myco.com@MYCO.COM |
| Wie lauten die Kennwörter, die jedem dieser Principals zugeordnet sind?<br>**Anmerkung:** Alle Kennwörter dienen als Beispiele und sollten nicht in einer tatsächlichen Konfiguration verwendet werden. | Das Kennwort für die Principals für die iSeries A, B und C lautet `iseriesa123`. Das Kennwort für den Principal für die iSeries D lautet `iseriesd123`. |
| Wie lautet der vollständig qualifizierte Hostname für jeden iSeries-Server?<br>**Anmerkung:** Alle Hostnamen dienen als Beispiele und sollten nicht in einer tatsächlichen Konfiguration verwendet werden. | iseriesa.myco.com<br>iseriesb.myco.com<br>iseriesc.myco.com<br>iseriesd.myco.com |
| Wie lautet der Name der Windows 2000-Domäne?<br>**Anmerkung:** Eine Windows 2000-Domäne ist mit einem Kerberos-Realm vergleichbar. Das Microsoft Active Directory verwendet die Kerberos-Authentifizierung als Standardsicherheitsmechanismus. | MYCO.COM |

*Tabelle 10. Planungsarbeitsblatt für den Netzwerkauthentifizierungsservice von iSeries D*

| Fragen | Antworten |
|---|---|
| Wie lautet der Name des Kerberos-Standard-Realms, zu dem Ihre iSeries gehören soll?<br>**Anmerkung:** Eine Windows 2000-Domäne ist mit einem Kerberos-Realm vergleichbar. Das Microsoft Active Directory verwendet die Kerberos-Authentifizierung als Standardsicherheitsmechanismus. | 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<br>**Port:** 88<br>**Anmerkung:** Dies ist der Standardport für den Kerberos-Server. |

*Tabelle 10. Planungsarbeitsblatt für den Netzwerkauthentifizierungsservice von iSeries D (Forts.)*

| Fragen | Antworten |
|---|---|
| Möchten Sie einen Kennwortserver für diesen Standard-Realm konfigurieren? Wenn ja, beantworten Sie die folgenden Fragen:<br><br>Wie<br>lautet der Name des Kennwortservers für diesen Kerberos-Server?<br>An welchem Port ist der Kennwortserver empfangsbereit? | Ja<br><br>**Kennwortserver:**<br>kdc1.myco.com<br>**Port:** 464<br>**Anmerkung:** Dies ist der Standardport für den Kennwortserver. |
| Für welche Services möchten Sie Chiffrierschlüsseleinträge erstellen?<br>• i5/OS-Kerberos-Authentifizierung<br>• LDAP<br>• iSeries IBM HTTP-Server<br>• iSeries NetServer | i5/OS-Kerberos-Authentifizierung |
| Wie lautet das Kennwort für Ihre(n) i5/OS-Service-Principal(s)?<br>**Anmerkung:** Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Sie dürfen nicht in einer tatsächlichen Konfiguration verwendet werden. | iseriesd123 |

## Schritt 2: Systemverwaltungsgruppe erstellen

Bevor Sie die Konfiguration des Netzwerkauthentifizierungsservice an ein Zielsystem weitergeben können, müssen Sie eine Systemverwal- tungsgruppe für alle Endpunktsysteme erstellen. Eine Systemverwaltungsgruppe ist eine Sammlung von Systemen, die Sie verwalten und auf die Sie ähnliche Einstellungen und Attribute, wie z. B. die Konfiguration des Netzwerkauthentifizierungsservice, anwenden können.

1. Erweitern Sie im iSeries Navigator den Eintrag **Management Central (iSeriesMC1)**.
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 `Systemverwaltungsgruppe` `MyCo` ein, und geben Sie eine Beschreibung für diese Systemverwaltungsgruppe ein.
4. Wählen Sie aus der Liste **Verfügbares System iSeries B**, **iSeries C** und **iSeries D** aus, und klicken Sie anschließend auf **Hinzufügen**. Auf diese Weise werden diese Systeme der Liste **Ausgewählte Systeme** hinzugefügt. Klicken Sie auf **OK**.
5. Erweitern Sie den Eintrag **Systemverwaltungsgruppen**, um zu überprüfen, ob Ihre Systemverwaltungsgruppe hinzugefügt wurde.

Sie haben jetzt eine Systemverwaltungsgruppe für Endpunktsysteme erstellt. Der nächste Schritt besteht darin, die Konfiguration des Netzwerkauthentifizierungsservice an die Server in dieser Systemverwaltungsgruppe weiterzugeben.

## Schritt 3: Systemeinstellungen ausgehend vom Modellsystem (iSeries A) an iSeries B und iSeries C weitergeben

Der Assistent für Funktionssynchronisation im iSeries Navigator ermöglicht Ihnen, Systemeinstellungen, wie z. B. die Konfiguration des Netzwerkauthentifizierungsservice, an mehrere Endpunktsysteme weiterzugeben. Führen Sie diese Tasks aus, um die Konfiguration des Netzwerkauthentifizierungsservice an die Zielsysteme weiterzugeben:

1. Erweitern Sie in iSeries Navigator den Eintrag expand **Management Central (iSeriesMC1)** → **Systemverwaltungsgruppen**.

2. Klicken Sie mit der rechten Maustaste auf **Systemverwaltungsgruppe MyCo**, und wählen Sie **Systemwerte → Funktionen synchronisieren** aus. Auf diese Weise wird der **Assistent für Funktionssynchronisation** gestartet.
3. Überprüfen Sie auf der **Begrüßungsseite** die Informationen zum Assistenten für Funktionssynchronisation, und klicken Sie auf **Weiter**. Auf der **Begrüßungsseite** sind die Funktionen aufgelistet, die Sie später im Assistenten synchronisieren können.

   **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 Szenario: Alle Verbindungen zum Management Central-Server mit SSL sichern.
4. Wählen Sie auf der Seite **Modellsystem iSeries A** als Modellsystem aus, und klicken Sie dann auf **Weiter**. Dieses Modellsystem wird als Basis für die Synchronisation der Konfiguration des Netzwerkauthentifizierungsservice mit anderen Systemen verwendet.
5. Wählen Sie auf der Seite **Zielsysteme und -gruppen** die Option **Systemverwaltungsgruppe MyCo** aus. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Zu aktualisierende Komponenten** die Option **Netzwerkauthentifizierungsservice (Kerberos)** aus. Klicken Sie auf **Konfiguration prüfen**. Klicken Sie nach der Überprüfung der Konfiguration auf **Weiter**.

   **Anmerkung:** Wenn die Überprüfung des Netzwerkauthentifizierungsservice nicht durchgeführt werden kann, liegt möglicherweise ein Fehler in der Konfiguration des Netzwerkauthentifizierungsservice auf dem Modellsystem vor. Zum Beheben dieses Fehlers müssen Sie die Konfiguration auf dem Modellsystem prüfen, die Konfiguration korrigieren und dann zu Schritt 2 in diesen Anweisungen zurückkehren.
7. Wählen Sie auf der Seite **Netzwerkauthentifizierungsservice** die Option **i5/OS-Kerberos-Authentifizierung** aus, und geben Sie in den Feldern **Kennwort** und **Kennwort bestätigen** die Zeichenfolge `iseriesa123` ein. Klicken Sie 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 nach der Beendigung dieses Assistenten die Chiffrierschlüsseleinträge stattdessen manuell zu einzelnen Systemen hinzufügen und für jedes System ein anderes Kennwort eingeben.
8. Überprüfen Sie auf der Seite **Zusammenfassung**, dass die entsprechenden Einstellungen auf dieser Seite aufgelistet sind. Klicken Sie auf **Fertig stellen**.
9. Standardmäßig wird ein Dialogfenster angezeigt, das angibt, dass die Task "Funktionen synchronisieren" gestartet wurde. Wenn Sie die Standardeinstellung geändert haben, wird dieses Dialogfenster nicht angezeigt. Klicken Sie auf **OK**.
10. Das Dialogfenster für den **Status der Funktionssynchronisation** wird angezeigt. Vergewissern Sie sich, dass die Task ausgeführt wurde.

    Die Task wurde auf allen Endpunktsystemen außer iSeries D ausgeführt. Da die iSeries D i5/OS Version 5 Release 2 verwendet, wird der Assistent für Funktionssynchronisierung nicht unterstützt.

    Zum Beheben dieses Fehlers müssen Sie den Netzwerkauthentifizierungsservice auf iSeries D manuell so konfigurieren, dass er mit der Konfiguration auf dem Modellsystem (iSeries A) übereinstimmt.

Sie haben die Konfiguration des Netzwerkauthentifizierungsservice von iSeries A an iSeries B und C weitergegeben und müssen jetzt die entsprechenden Assistenten im iSeries Navigator verwenden, um iSeries D separat für den Netzwerkauthentifizierungsservice zu konfigurieren.

## Schritt 4: Netzwerkauthentifizierungsservice auf der iSeries D konfigurieren

Sie müssen den Netzwerkauthentifizierungsservice auf iSeries D manuell so konfigurieren, dass er mit der Konfiguration auf dem Modellsystem (iSeries A) übereinstimmt.

**Anmerkung:** Alle in diesem Szenario verwendeten Kennwörter dienen nur als Beispiele. Sie dürfen nicht in einer tatsächlichen Konfiguration verwendet werden.

Führen Sie die folgenden Schritte durch, um den Netzwerkauthentifizierungsservice zu konfigurieren:

1. Erweitern Sie im iSeries Navigator den Eintrag **iSeries D → Sicherheit**.
2. Klicken Sie mit der rechten Maustaste auf **Netzwerkauthentifizierungsservice**, und wählen Sie **Konfigurieren** aus, um den Konfigurationsassistenten zu starten. **Anmerkung:** Nach der Konfiguration des Netzwerkauthentifizierungsservice lautet diese Option **Rekonfigurieren**.
3. Die **Begrüßungsseite** enthält Informationen zu den vom Assistenten erstellten Objekten. Klicken Sie auf **Weiter**.
4. 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**.
5. 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**.
6. Wählen Sie auf der Seite **Kennwortserverinformationen angeben** die Option **Ja** aus, um die iSeries D so zu konfigurieren, dass sie auf den für den Standard-Realm konfigurierten Kennwortserver verweist. Der Kennwortserver ermöglicht Principals die Änderung von Kennwörtern auf dem Kerberos-Server und wurde bereits konfiguriert. Geben Sie im Feld **Kennwortserver** den Wert `kdc1.myco.com` ein. Der Kennwortserver hat den Standardport 464. Klicken Sie auf **Weiter**.
7. Wählen Sie auf der Seite **Chiffrierschlüsseleinträge auswählen** die Option **i5/OS-Kerberos-Authentifizierung** aus. Klicken Sie auf **Weiter**.
8. Geben Sie auf der Seite **i5/OS-Chiffrierschlüsseleintrag erstellen** ein Kennwort ein und bestätigen Sie es. Beispiel: `iseriesd123`. Klicken Sie auf **Weiter**.
9. Wählen Sie auf der Seite **Stapeldatei erstellen** die Option **Nein** aus.
10. Auf der Seite **Zusammenfassung** können Sie die Details zur Konfiguration des Netzwerkauthentifizierungsservice überprüfen. Klicken Sie auf **Fertig stellen**.

Sie haben den Netzwerkauthentifizierungsservice auf allen Systemen konfiguriert und müssen jetzt für jedes Ihrer Systeme den i5/OS-Service-Principal zum Kerberos-Server hinzufügen.

## Schritt 5: Die Principals für Endpunktsysteme zur Windows 2000-Domäne hinzufügen

Führen Sie die folgenden Schritte durch, um die Service-Principals für die Endpunktsysteme hinzuzufügen:

**iSeries B**

1. Erweitern Sie auf dem Windows 2000-Server den Eintrag **Verwaltungstools → Active Directory-Benutzer und -Computer**.
2. Wählen Sie als Domäne **MYCO.COM** aus, und erweitern Sie den Eintrag **Aktion → Neu → Benutzer**.

   **Anmerkung:** Diese Windows-Domäne muss mit dem Namen des Standard-Realms übereinstimmen, den Sie bei der Konfiguration des Netzwerkauthentifizierungsservice angegeben haben.
3. Geben Sie im Feld **Name** den Wert `iseriesb` ein, um den iSeries-Server für diese Windows-Domäne anzugeben. Damit wird ein neues Benutzerkonto für iSeries B hinzugefügt.

4. Rufen Sie die Eigenschaften für den Active Directory-Benutzer iseriesb auf. Wählen Sie auf der Indexzunge **Konto** die Option **Konto wird für Delegierungszwecke vertraut** aus. Damit wird dem i5/OS-Service-Principal der Zugriff auf andere Services im Namen eines angemeldeten Benutzers gestattet.
5. Auf dem Windows 2000-Server müssen Sie das soeben erstellte Benutzerkonto mit dem Befehl **ktpass** dem i5/OS-Service-Principal zuordnen. Das Tool ktpass befindet sich im Ordner **Servicetools** auf der Installations-CD für Windows (R) 2000-Server. Geben Sie bei einer Windows-Eingabeaufforderung Folgendes ein:

```
ktpass -mapuser iseriesb -pass iseriesa123 -princ krbsvr400/iseriesb.myco.com@MYCO.COM -mapop set
```

**iSeries C**

1. Erweitern Sie auf dem Windows 2000-Server den Eintrag **Verwaltungstools** → **Active Directory-Benutzer und -Computer**.
2. Wählen Sie als Domäne **MYCO.COM** aus, und erweitern Sie den Eintrag **Aktion** → **Neu** → **Benutzer**.

   **Anmerkung:** Diese Windows-Domäne muss mit dem Namen des Standard-Realms übereinstimmen, den Sie bei der Konfiguration des Netzwerkauthentifizierungsservice angegeben haben.
3. Geben Sie im Feld **Name** den Wert `iseriesc` ein, um den iSeries-Server für diese Windows-Domäne anzugeben. Damit wird ein neues Benutzerkonto für iSeries C hinzugefügt.
4. Rufen Sie die Eigenschaften für den Active Directory-Benutzer iseriesc auf. Wählen Sie auf der Indexzunge **Konto** die Option **Konto wird für Delegierungszwecke vertraut** aus. Damit wird dem i5/OS-Service-Principal der Zugriff auf andere Services im Namen eines angemeldeten Benutzers gestattet.
5. Auf dem Windows 2000-Server müssen Sie das soeben erstellte Benutzerkonto mit dem Befehl **ktpass** dem i5/OS-Service-Principal zuordnen. Das Tool ktpass befindet sich im Ordner **Servicetools** auf der Installations-CD für Windows (R) 2000-Server. Geben Sie bei einer Windows-Eingabeaufforderung Folgendes ein:

```
ktpass -mapuser iseriesc -pass iseriesa123 -princ krbsvr400/iseriesc.myco.com@MYCO.COM -mapop set
```

**iSeries D**

1. Erweitern Sie auf dem Windows 2000-Server den Eintrag **Verwaltungstools** → **Active Directory-Benutzer und -Computer**.
2. Wählen Sie als Domäne **MYCO.COM** aus, und erweitern Sie den Eintrag **Aktion** → **Neu** → **Benutzer**.

   **Anmerkung:** Diese Windows-Domäne muss mit dem Namen des Standard-Realms übereinstimmen, den Sie bei der Konfiguration des Netzwerkauthentifizierungsservice angegeben haben.
3. Geben Sie im Feld **Name** den Wert `iseriesd` ein, um den iSeries-Server für diese Windows-Domäne anzugeben. Damit wird ein neues Benutzerkonto für iSeries D hinzugefügt.
4. Rufen Sie die Eigenschaften für den Active Directory-Benutzer iseriesd auf. Wählen Sie auf der Indexzunge **Konto** die Option **Konto wird für Delegierungszwecke vertraut** aus. Damit wird dem i5/OS-Service-Principal der Zugriff auf andere Services im Namen eines angemeldeten Benutzers gestattet.
5. Auf dem Windows 2000-Server müssen Sie das soeben erstellte Benutzerkonto mit dem Befehl **ktpass** dem i5/OS-Service-Principal zuordnen. Das Tool ktpass befindet sich im Ordner **Servicetools** auf der Installations-CD für Windows (R) 2000-Server. Geben Sie bei einer Windows-Eingabeaufforderung Folgendes ein:

```
ktpass -mapuser iseriesd -pass iseriesd123 -princ krbsvr400/iseriesd.myco.com@MYCO.COM -mapop set
```

Sie haben die Weitergabe der Konfiguration des Netzwerkauthentifizierungsservice an mehrere Systeme abgeschlossen. Wenn Sie den Management Central-Server so konfigurieren möchten, dass er den Netzwerkauthentifizierungsservice nutzt, müssen Sie einige zusätzliche Tasks ausführen. Detaillierte Anweisungen hierzu finden Sie unter „Szenario: Kerberos-Authentifizierung zwischen Management Central-Servern verwenden” auf Seite 41.

# Szenario: Kerberos-Authentifizierung zwischen Management Central-Servern verwenden

## Situation

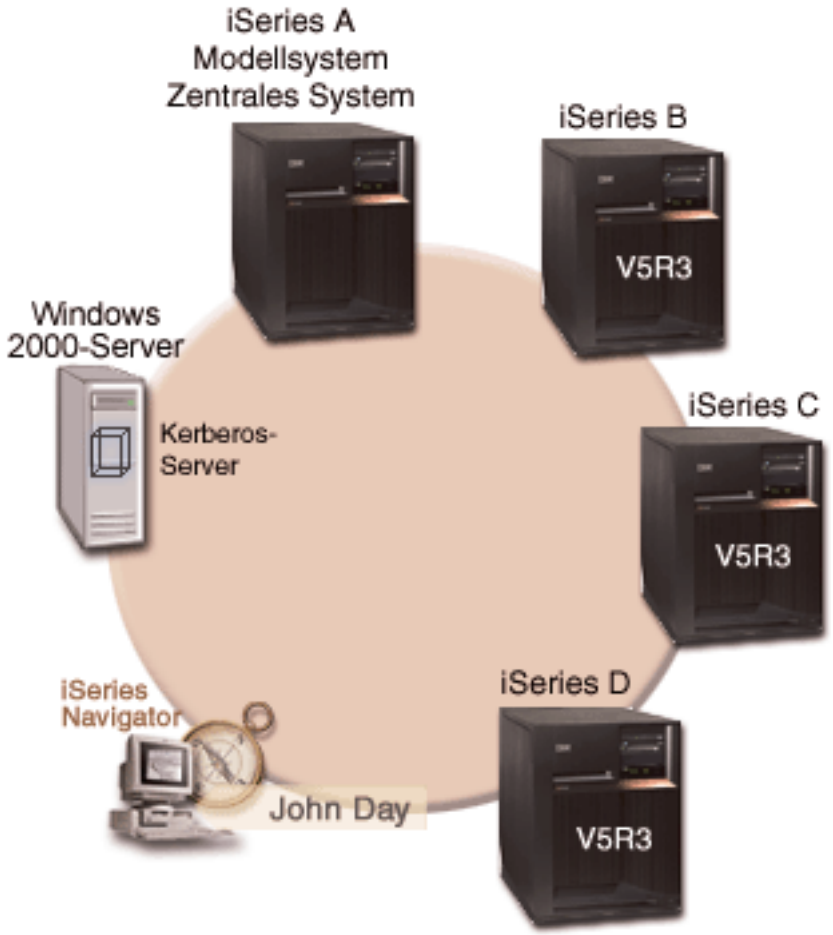
Sie sind als Netzwerkadministrator für ein mittelständisches Unternehmen der Teileproduktion tätig. Sie verwalten gegenwärtig vier iSeries Systeme mit dem iSeries Navigator auf einem Client-PC. Sie möchten, dass die Management Central-Serverjobs die Kerberos-Authentifizierung anstelle anderer Authentifizierungsmethoden, die Sie in der Vergangenheit verwendet haben, nämlich der Kennwortsynchronisation, verwenden.

## Ziele

In diesem Szenario besteht das Ziel für MyCo, Inc. darin, die Kerberos-Authentifizierung zwischen Management Central-Servern zu verwenden.

## Details

Die folgende Grafik veranschaulicht die Details zu diesem Szenario.




**iSeries A - Modellsystem und zentrales System**

- Wird unter i5/OS Version 5 Release 3 (V5R3) mit den folgenden Optionen und Lizenzprogrammen ausgeführt:
  - i5/OS Host-Server (5722-SS1 Option 12)
  - iSeries Access für Windows (5722-XE1)

- Cryptographic Access Provider (5722-AC3)
- Der i5/OS-Service-Principal, krbsvr400/iseriesa.myco.com@MYCO.COM, und das zugeordnete Kennwort wurden zur Chiffrierschlüsseldatei hinzugefügt.
- Speichert und plant für jedes der Endpunktsysteme Tasks hinsichtlich der Synchronisationseinstellungen und führt diese aus.

**iSeries B - Endpunktsystem**
- Wird unter i5/OS Version 5 Release 3 (V5R3) mit den folgenden Optionen und Lizenzprogrammen ausgeführt:
  - i5/OS Host-Server (5722-SS1 Option 12)
  - iSeries Access für Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3)
- Der i5/OS-Service-Principal, krbsvr400/iseriesb.myco.com@MYCO.COM, und das zugeordnete Kennwort wurden zur Chiffrierschlüsseldatei hinzugefügt.

**iSeries C - Endpunktsystem**
- Wird unter i5/OS Version 5 Release 3 (V5R3) mit den folgenden Optionen und Lizenzprogrammen ausgeführt:
  - i5/OS Host-Server (5722-SS1 Option 12)
  - iSeries Access für Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3)
- Der i5/OS-Service-Principal krbsvr400/iseriesc.myco.com@MYCO.COM, und das zugeordnete Kennwort wurden zur Chiffrierschlüsseldatei hinzugefügt.

**iSeries D - Endpunktsystem**
- Wird unter i5/OS Version 5 Release 3 (V5R3) mit den folgenden Optionen und Lizenzprogrammen ausgeführt:
  - i5/OS Host-Server (5722-SS1 Option 12)
  - iSeries Access für Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3)
- Der i5/OS-Service-Principal, krbsvr400/iseriesd.myco.com@MYCO.COM, und das zugeordnete Kennwort wurden zur Chiffrierschlüsseldatei hinzugefügt.

**Windows 2000-Server**
- Fungiert als Kerberos-Server für diese Systeme.
- Die folgenden i5/OS-Service-Principals wurden dem Windows 2000-Server hinzugefügt:
  - krbsvr400/iseriesa.myco.com@MYCO.COM
  - krbsvr400/iseriesb.myco.com@MYCO.COM
  - krbsvr400/iseriesc.myco.com@MYCO.COM
  - krbsvr400/iseriesd.myco.com@MYCO.COM

**Client-PC**
- Wird unter iSeries Access für Windows V5R3 (5722-XE1) ausgeführt.
- Wird unter iSeries Navigator V5R3 mit den folgenden Unterkomponenten ausgeführt:

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

## Voraussetzungen und Annahmen

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 iSeries Navigator den Eintrag für Ihren **iSeries-Server → 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 Basissystemsicherheit wurden auf jedem dieser Server konfiguriert und getestet.
4. Die Standardeinstellungen im iSeries Navigator wurden nicht dahingehend geändert, dass das Öffnen des Fensters "Task-Status" beim Starten einer Task gestoppt wird. Gehen Sie wie folgt vor, um sicherzustellen, dass die Standardeinstellungen nicht geändert wurden:

   a. Klicken Sie im iSeries Navigator mit der rechten Maustaste auf **Ihr zentrales System**, und wählen Sie **Benutzervorgaben** aus.

   b. Vergewissern Sie sich auf der Seite **Allgemein**, dass die Option **Fenster 'Task-Status' automatisch öffnen, wenn eine meiner Tasks gestartet wird** ausgewählt ist.

5. Dieses Szenario basiert auf der Annahme, dass der Netzwerkauthentifizierungsservice auf allen Systemen mit dem Assistenten für Funktionssynchronisation im iSeries Navigator konfiguriert wurde. Dieser Assistent gibt die Konfiguration des Netzwerkauthentifizierungsservice von einem Modellsystem an mehrere Zielsysteme weiter. Der Abschnitt „Szenario: Konfiguration des Netzwerkauthentifizierungsservice an mehrere Systeme weitergeben" auf Seite 30 enthält detaillierte Information zur Verwendung des Assistenten für Funktionssynchronisation.

## Konfigurationsschritte

1. Planungsarbeitsblätter ausfüllen
2. Zentrales System zur Verwendung der Kerberos-Authentifizierung konfigurieren
3. Systemverwaltungsgruppe MyCo2 erstellen
4. Inventar der Systemwerte erfassen
5. Kerberos-Einstellungen im iSeries Navigator vergleichen und aktualisieren
6. Management Central-Server auf dem zentralen System und den Zielsystemen erneut starten
7. Kerberos-Service-Principal für jedes Endpunktsystem der Datei für anerkannte Gruppen zuordnen
8. Prüfen, ob die Kerberos-Principals der Datei für anerkannte Gruppen hinzugefügt werden
9. Gesicherte Verbindungen zulassen
10. Schritte 4 bis 6 für Zielsysteme wiederholen
11. Authentifizierung auf den Endpunktsystemen testen.

## Details zum Szenario: Kerberos-Authentifizierung zwischen Management Central-Servern verwenden

Es wird angenommen, dass Sie in Ihrem Netzwerk einen Kerberos-Server konfiguriert haben und auf jedem iSeries-Server den Netzwerkauthentifizierungsservice so konfiguriert haben, dass er auf den Kerberos-Server verweist. Sie können den Netzwerkauthentifizierungsservice für jede iSeries einzeln konfigurieren oder den Assistenten für Funktionsynchronisation im iSeries Navigator verwenden, um die Konfiguration an andere Systeme weiterzugeben.

Im Abschnitt „Szenario: Konfiguration des Netzwerkauthentifizierungsservice an mehrere Systeme weitergeben" auf Seite 30 wird detailliert beschrieben, wie die Konfiguration des Netzwerkauthentifizierungsservice mit dem Assistenten für Funktionssynchronisation weitergegeben wird.

## Schritt 1: Planungsarbeitsblätter ausfüllen

Die folgenden Planungsarbeitsblätter veranschaulichen die Art der Informationen, die Sie benötigen, um Ihre Systeme für die Verwendung der Kerberos-Authentifizierung zu aktivieren.

*Tabelle 11. Kerberos-Authentifizierung zwischen Management Central-Servern verwenden - Arbeitsblatt für Voraussetzungen*

| Arbeitsblatt für Voraussetzungen | Antworten |
|---|---|
| Verwenden Sie i5/OS V5R3 (5722-SS1) oder eine spätere Version für alle Systeme? | Ja |
| Wurden die aktuellsten vorläufigen Programmkorrekturen (PTFs) angelegt? | Ja |
| Sind die folgenden Optionen und Lizenzprogramme auf allen iSeries-Systemen installiert?<br>• i5/OS Host-Server (5722-SS1 Option 12)<br>• iSeries Access für Windows (5722-XE1)<br>• Cryptographic Access Provider (5722-AC3) | Ja |
| Ist iSeries Access für Windows V5R3 (5722-XE1) auf dem Administrator-PC installiert? | Ja |
| Ist iSeries Navigator V5R3 auf dem Administrator-PC installiert?<br>• Ist die Unterkomponente "Netzwerk" des iSeries Navigator auf dem PC des Administrators installiert?<br>• Ist die Unterkomponente "Sicherheit" des iSeries Navigator auf dem PC des Administrators installiert? | Ja |
| Ist das aktuellste Service-Pack von IBM @server iSeries Access für Windows installiert?<br><br>Sie können das aktuellste Service-Pack über iSeries Access abrufen. | Ja |
| Besitzen Sie 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.<br>1. Microsoft Windows 2000-Server<br>**Anmerkung:** Microsoft Windows 2000-Server verwendet die Kerberos-Authentifizierung als Standardsicherheitsmechanismus.<br>2. Windows (R) Server 2003<br>3. i5/OS PASE (ab V5R3)<br>4. AIX-Server<br>5. zSeries | Ja, Windows 2000-Server |
| Für Windows 2000-Server und Windows (R) Server 2003: Sind Windows-Unterstützungstools installiert (beinhalten das Tool ktpass)? | Ja |
| Beträgt die Abweichung zwischen der Systemzeit der iSeries und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung größer, lesen Sie Systemzeiten synchronisieren. | Ja |

*Tabelle 12. Kerberos-Authentifizierung zwischen Management Central-Servern verwenden - Planungsarbeitsblatt*

| Fragen | Antworten |
|---|---|
| Wie lautet der Name der Systemverwaltungsgruppe? | Systemverwaltungsgruppe MyCo2 |
| Welche Systeme werden in diese Systemverwaltungsgruppe aufgenommen? | iSeries A, iSeries B, iSeries C, iSeries D |
| Wie lauten die Service-Principal-Namen für die iSeries-Systeme? | krbsvr400/iseriesa.myco.com@MYCO.COM<br>krbsvr400/iseriesb.myco.com@MYCO.COM<br>krbsvr400/iseriesc.myco.com@MYCO.COM<br>krbsvr400/iseriesd.myco.com@MYCO.COM |

## Schritt 2: Zentrales System zur Verwendung der Kerberos-Authentifizierung konfigurieren

iSeries A ist das Modellsystem und das zentrale System für die anderen Zielsysteme.Führen Sie die folgenden Tasks aus, um die Kerberos-Authentifizierung auf dem zentralen System zu konfigurieren.

1. Klicken Sie im iSeries Navigator mit der rechten Maustaste auf **Management Central (iSeriesA)**, und wählen Sie **Eigenschaften** aus.
2. Wählen Sie auf der Indexzunge **Sicherheit** die Option **Kerberos-Authentifizierung verwenden** aus, und setzen Sie die Authentifizierungsstufe auf **Zur anerkannten Gruppe hinzufügen**.
3. Wählen Sie im Feld **Identitätsabgleich** die Option **Nicht verwenden** aus, und klicken Sie auf **OK**. Diese Einstellung ermöglicht Ihnen, die Verwendung von Enterprise Identity Mapping (EIM) durch Management Central-Server zu aktivieren bzw. zu inaktivieren, um für Ihre Endpunktsysteme eine Einzelanmeldungsumgebung zu aktivieren. Wenn Sie für Ihre Endpunktsysteme die Einzelanmeldung aktivieren möchten, lesen Sie Szenario: Management Central-Server für eine Einzelanmeldungsumgebung konfigurieren. Das Szenario veranschaulicht diese Konfiguration.

   **Anmerkung:** Die Anmerkung am Ende der Seite **Sicherheit** weist darauf hin, dass die Einstellungen beim nächsten Start der Management Central-Server wirksam werden. Führen Sie jetzt keinen Neustart der Server durch. Im Szenario wird erläutert, wann der Zeitpunkt gekommen ist, die Server in einem nachfolgenden Schritt erneut zu starten.
4. Es erscheint ein Dialogfenster, in dem angezeigt wird, dass die Änderungen an diesen Einstellungen nur dieses zentrale System betreffen und dass Kerberos richtig konfiguriert sein muss, bevor diese Einstellungen von den Management Central-Serverjobs verwendet werden können. Klicken Sie auf **OK**. Sie haben die Kerberos-Authentifizierung für das zentrale System aktiviert.

Sie haben die Einstellungen im zentralen System geändert, damit dieses die Kerberos-Authentifizierung durchführen kann. Jetzt müssen Sie eine Systemverwaltungsgruppe erstellen, damit Sie diese Einstellungen auf die Zielsysteme anwenden können.

## Schritt 3: Systemverwaltungsgruppe MyCo2 erstellen

Bevor Sie die richtigen Einstellungen auf die anderen Systeme in Ihrem Netzwerk anwenden können, müssen Sie eine Systemverwaltungsgruppe für alle Endpunktsysteme erstellen. Eine Systemverwaltungsgruppe ist eine Sammlung von Systemen, die Sie verwalten und auf die Sie ähnliche Einstellungen und Attribute, wie z. B. die Konfiguration des Netzwerkauthentifizierungsservice, anwenden können.

1. Erweitern Sie im iSeries Navigator den Eintrag **Management Central (iSeries A)**.
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 `Systemverwaltungsgruppe MyCo2` ein. Geben Sie eine Beschreibung für diese Systemverwaltungsgruppe an.

4. Wählen Sie aus der Liste **Verfügbares System** iSeries A, iSeries B, iSeries C, und iSeries D aus und klicken Sie auf **Hinzufügen**. Auf diese Weise werden diese Systeme der Liste **Ausgewählte Systeme** hinzugefügt.
5. Klicken Sie auf **OK**.
6. Erweitern Sie den Eintrag **Systemverwaltungsgruppen**, um zu überprüfen, ob Ihre Systemverwaltungsgruppe hinzugefügt wurde.

Sie haben die Systemverwaltungsgruppe MyCo2 erstellt und müssen jetzt die aktuellen Einstellungen für die Kerberos-Authentifizierung erfassen.

## Schritt 4: Inventar der Systemwerte erfassen

Sie müssen die Funktion ″Inventar erfassen″ im iSeries Navigator verwenden, um für die Zielsysteme in der Systemverwaltungsgruppe MyCo2 die Einstellungen für die Kerberos-Authentifizierung hinzuzufügen. Gehen Sie wie folgt vor, um das Inventar für die Systemverwaltungsgruppe MyCo2 zu erfassen:

1. Erweitern Sie im iSeries Navigator den Eintrag **Management Central (iSeriesA)** → **Systemverwaltungsgruppen**.
2. Klicken Sie mit der rechten Maustaste auf **Systemverwaltungsgruppe MyCo2**, und wählen Sie **Inventar** → **Erfassen** aus.
3. Wählen Sie auf der Seite **Inventar erfassen - Systemverwaltungsgruppe MyCo2** die Option **Systemwerte** aus. Klicken Sie auf **OK**.
4. Standardmäßig wird ein Dialogfenster angezeigt, das angibt, dass die Task ″Funktionen synchronisieren - Inventar erfassen″ gestartet wurde. Wenn Sie die Standardeinstellung geändert haben, wird dieses Dialogfenster nicht angezeigt. Klicken Sie auf **OK**.
5. Lesen Sie auf der Seite **Inventarstatus erfassen** alle angezeigten Statuswerte, und beheben Sie alle möglicherweise auftretenden Fehler. Details zu spezifischen Statuswerten, die sich auf die Inventarerfassung beziehen und auf dieser Seite erscheinen, erhalten Sie, wenn Sie **Hilfe** → **Hilfe für Task-Status...** auswählen. Wählen Sie auf der Hilfeseite **Task-Status** die Option **Inventar** aus. Auf dieser Seite werden alle möglichen Statuswerte mit detaillierten Beschreibungen sowie Informationen zur Fehlerbehebung angezeigt.
6. Schließen Sie das Statusfenster, wenn die Inventarerfassung durchgeführt werden konnte.

Nachdem Sie das Inventar der Systemwerte erfasst haben, müssen Sie diese Kerberos-Einstellungen auf jedes Zielsystem in der Systemverwaltungsgruppe MyCo2 anwenden.

## Schritt 5: Kerberos-Einstellungen im iSeries Navigator vergleichen und aktualisieren

Nachdem Sie das Inventar der Systemwerte erfasst haben, müssen Sie die auf dem zentralen System ausgewählten Kerberos-Einstellungen auf jedes Zielsystem in der Systemverwaltungsgruppe MyCo2 anwenden. Gehen Sie wie folgt vor, um die Zielsysteme in der Systemverwaltungsgruppe MyCo2 zu aktualisieren:

1. Erweitern Sie im iSeries Navigator den Eintrag **Management Central (iSeriesA)** → **Systemverwaltungsgruppen**.
2. Klicken Sie mit der rechten Maustaste auf **Systemverwaltungsgruppe MyCo2**, und wählen Sie **Systemwerte** → **Vergleichen und aktualisieren** aus.
3. Füllen Sie die Felder im Dialogfenster **Vergleichen und aktualisieren - Systemverwaltungsgruppe MyCo2** aus:
   - Wählen Sie die **iSeries A** für das Feld **Modellsystem** aus.
   - Wählen Sie **Management Central** für das Feld **Kategorie** aus.

- Wählen Sie aus der Liste **Zu vergleichende Einträge** die Optionen **Kerberos-Authentifizierung zum Überprüfen von Anforderungen verwenden** und **Zuverlässigkeitsstufe der Kerberos-Authentifizierung** aus.

4. Vergewissern Sie sich, dass die Zielsysteme in der Systemverwaltungsgruppe MyCo2 in der Liste der Zielsysteme angezeigt werden, und klicken Sie auf **OK**, um die Aktualisierung zu starten. Auf diese Weise wird jedes System in der Systemverwaltungsgruppe MyCo2 mit den Einstellungen für die Kerberos-Authentifizierung, die auf dem Modellsystem ausgewählt wurden, aktualisiert.
5. Standardmäßig wird ein Dialogfenster angezeigt, das angibt, dass die Task "Vergleichen und aktualisieren" gestartet wurde. Wenn Sie die Standardeinstellung geändert haben, wird dieses Dialogfenster nicht angezeigt. Klicken Sie auf **OK**.
6. Vergewissern Sie sich im Statusdialogfenster **Werte aktualisieren**, dass die Aktualisierung auf allen Systemen ausgeführt wird, und schließen Sie das Dialogfenster.

Nachdem Sie die Aktualisierung durchgeführt haben, müssen Sie die Management Central-Server auf dem zentralen System und den Zielsystemen erneut starten

## Schritt 6: Management Central-Server auf dem zentralen System und den Zielsystemen erneut starten

Nachdem Sie die Aktualisierung für jedes Zielsystem in der Systemverwaltungsgruppe beendet haben, müssen Sie alle Management Central-Server auf dem zentralen Systemen und den Zielsystemen erneut starten. Gehen Sie wie folgt vor, um die Management Central-Server erneut zu starten:

1. Erweitern Sie im iSeries Navigator den Eintrag **Meine Verbindungen** → **iSeriesA** → **Netzwerk** → **Server** → **TCP/IP**.
2. Klicken Sie mit der rechten Maustaste auf **Management Central**, und wählen Sie **Stoppen** aus. Warten Sie, bis der Management Central-Server gestoppt wurde. Drücken Sie F5, um die Anzeige zu aktualisieren und den Status im rechten Teilfenster anzuzeigen. Wenn der Server gestoppt wurde, sollte der Status **Gestoppt** angezeigt werden.
3. Klicken Sie mit der rechten Maustaste auf **Management Central**, und wählen Sie **Starten** aus. Auf diese Weise werden die Management Central-Server auf dem zentralen System erneut gestartet.
4. Wiederholen Sie die Schritte 1-3 auf den Zielsystemen: iSeries B, iSeries C und iSeries D.

Nachdem Sie den Management Central-Server erneut gestartet haben, müssen Sie für alle Zielsysteme eine Datei für anerkannte Gruppen konfigurieren.

## Schritt 7: Kerberos-Service-Principal für jedes Endpunktsystem der Datei für anerkannte Gruppen zuordnen

Nach dem Neustart aller Management Central-Server müssen Sie für alle Endpunktsysteme den Kerberos-Service-Principal des zentralen Systems zur Datei für anerkannte Gruppen hinzufügen. Gehen Sie wie folgt vor, um den Service-Principal zu den Endpunktsystemen hinzuzufügen:

1. Führen Sie vom zentralen System einen fernen Befehl, wie z. B. DSPLIBL (Bibliotheksliste anzeigen), für alle Endpunktsysteme aus. Jedes Endpunktsystem fügt automatisch den Kerberos-Service-Principal des zentralen Systems zu seiner individuellen Datei für anerkannte Gruppen hinzu, da auf jedem Endpunktsystem die Authentifizierungsstufe **Zur anerkannten Gruppe hinzufügen** ausgewählt ist.

   **Anmerkung:** Sie können vom zentralen System aus jeden fernen Befehl für ein Endpunktsystem ausführen, damit der Management Central-Serverjob auf dem Endpunktsystem die notwendigen Kerberos-Service-Principals in der Datei für anerkannte Gruppen aufzuzeichnet. Der Befehl DSPLIBL (Bibliotheksliste anzeigen) wird nur als Beispiel verwendet.
2. Wenn Sie mit einem Modell- oder Quellensystem Tasks ausführen, wie z. B. Fixes senden, Benutzer senden, Zeit synchronisieren, müssen Sie diese Tasks so ausführen, dass die richtigen Kerberos-Service-Principals den entsprechenden Dateien für anerkannte Gruppen hinzugefügt werden.

Für dieses Szenario möchten Sie einen fernen Befehl für alle Endpunktsysteme auszuführen, um auf jedem Endpunktsystem den Kerberos-Service-Principal der Datei für anerkannte Gruppen hinzuzufügen. Führen Sie die folgenden Schritte durch, um einen fernen Befehl auszuführen:

1. Erweitern Sie im iSeries Navigator den Eintrag **Management Central (iSeriesA)** → **Systemverwaltungsgruppen**.
2. Klicken Sie mit der rechten Maustaste auf **Systemverwaltungsgruppe MyCo2**, und wählen Sie **Befehl ausführen** aus.
3. Geben Sie auf der Seite **Befehl ausführen - Systemverwaltungsgruppe MyCo2** im Feld **Auszuführende Befehle** die Zeichenfolge `dsplibl` ein, und klicken Sie auf **OK**, um die Befehls-Task sofort zu starten. Sie können auch auf **Vorherige Befehle** klicken, um einen Befehl aus einer Liste von zuvor ausgeführten Befehlen auszuwählen, oder Sie können auf **Eingabeaufforderung** klicken, um Hilfe bei der Eingabe oder der Auswahl eines i5/OS-Befehls zu erhalten.
4. Standardmäßig wird ein Dialogfenster angezeigt, das angibt, dass die Task "Befehl ausführen" gestartet wurde. Wenn Sie die Standardeinstellung geändert haben, wird dieses Dialogfenster nicht angezeigt. Klicken Sie auf **OK**.
5. Vergewissern Sie sich im Statusdialogfenster **Befehl ausführen**, dass der Befehl auf allen Systemen ausgeführt wird und schließend Sie das Dialogfenster.

Wenn Sie diese Schritte durchgeführt haben, können Sie überprüfen, ob der Kerberos-Principal auf jedem der Endpunktsysteme zur Datei für anerkannte Gruppen hinzugefügt wurde.

## Schritt 8: Prüfen, ob die Kerberos-Principals zur Datei für anerkannte Gruppen hinzugefügt werden

Wenn Sie den fernen Befehl ausgeführt haben, können Sie überprüfen, ob der Kerberos-Service-Principal des zentralen Systems sich auf jedem der Endpunktsysteme in der Datei für anerkannte Gruppen befindet.

1. Erweitern Sie im iSeries Navigator den Eintrag **iSeries B** → **Dateisysteme** → **Integrated File System** → **Root** → **QIBM** → **UserData** → **OS400** → **MGTC** → **config**.
2. Klicken Sie mit der rechten Maustaste auf **McTrustedGroup.conf**, und wählen Sie **Bearbeiten** aus, um den Dateiinhalt anzuzeigen.

   **Anmerkung:** Wenn **Bearbeiten** inaktiviert ist, müssen Sie die Option aktivieren. Führen Sie dazu die folgenden Schritte durch:

   a. Klicken Sie mit der rechten Maustaste auf **Integrated File System**, und wählen Sie **Eigenschaften** aus.
   b. Wählen Sie im Dialogfenster **Eigenschaften für Integrated File System** die Option **Alle Dateien** für **Bearbeitungsoptionen aktivieren für:** aus und klicken Sie auf **OK**.
3. Vergewissern Sie sich, dass der Kerberos-Service-Principal des zentralen Systems als Mitglied der anerkannten Gruppe von Management Central aufgelistet ist.

Wiederholen Sie diese Schritte für iSeries C und iSeries D, um zu überprüfen, ob der Kerberos-Service-Principal des zentralen Systems zu jedem der Zielsysteme hinzugefügt wurde.

Wenn Sie sich vergewissert haben, dass der Service-Principal des zentralen Systems auf jedem der Zielsysteme zur Datei für anerkannte Gruppen hinzugefügt wurde, müssen Sie gesicherte Verbindungen für das zentrale System zulassen.

## Schritt 9: Gesicherte Verbindungen für das zentrale System zulassen

Nachdem der ferne Befehl für die Endpunktsysteme ausgeführt wurde, müssen Sie gesicherte Verbindungen zwischen Management Central-Servern zulassen. Auf diese Weise wird sichergestellt, dass nur das zentrale System für die Systemverwaltungsgruppe MyCo2 (iSeries A) Tasks für die Zielsysteme ausführen kann.

1. Klicken Sie im iSeries Navigator mit der rechten Maustaste auf **Management Central (iSeriesA)**, und wählen Sie **Eigenschaften** aus.
2. Wählen Sie auf der Indexzunge **Sicherheit** die Option **Kerberos-Authentifizierung verwenden** aus, und setzen Sie die Authentifizierungsstufe auf **Nur gesicherte Verbindungen zulassen**.
3. Wählen Sie im Feld **Identitätsabgleich** die Option **Nicht verwenden** aus.
4. Es erscheint ein Dialogfenster, in dem angezeigt wird, dass die Änderungen an diesen Einstellungen nur dieses zentrale System betreffen und dass Kerberos richtig konfiguriert sein muss, bevor diese Einstellungen von den Management Central-Serverjobs verwendet werden können. Klicken Sie auf **OK**.

Nachdem Sie gesicherte Verbindungen für das zentrale System zugelassen haben, müssen Sie die Schritte 4 bis 6 wiederholen.

## Schritt 10: Schritte 4 bis 6 für Zielsysteme wiederholen

Nachdem Sie gesicherte Verbindungen für das zentrale System zugelassen haben, müssen Sie die Schritte 4 bis 6 in diesem Szenario wiederholen, um diese Änderungen auf die Zielsysteme in der Systemverwaltungsgruppe MyCo2 anzuwenden. Auf diese Weise stellen Sie sicher, dass die Zielsysteme so konfiguriert sind, dass sie gesicherte Verbindungen zulassen. Führen Sie folgende Schritte durch:

- Schritt 4: Inventar der Systemwerte erfassen
- Schritt 5: Kerberos-Einstellungen im iSeries Navigator vergleichen und aktualisieren
- Schritt 6: Management Central-Server auf dem zentralen System und den Zielsystemen erneut starten

Nachdem Sie die Schritte 4 bis 6 wiederholt haben, müssen Sie die Authentifizierung auf den Endpunktsystemen testen.

## Schritt 11: Authentifizierung auf den Endpunktsystemen testen

Sobald die Server erneut gestartet werden, verwenden die Systeme Kerberos zur Authentifizierung und die anerkannte Gruppe zur Berechtigung. Damit ein System eine Anforderung akzeptiert und ausführt, prüft dieses System, ob das anfordernde System einen gültigen Kerberos-Principal besitzt. Es prüft ebenfalls, ob es den Kerberos-Principal als vertrauenswürdig akzeptieren kann, indem es abgleicht, ob der Principal in seiner Liste anerkannter Gruppen aufgeführt ist.

**Anmerkung:** Sie müssen diese Schritte auf allen Zielsystemen mit den folgenden i5/OS-Service-Principals wiederholen:

- krbsvr400/iseriesa.myco.com@MYCO.COM
- krbsvr400/iseriesb.myco.com@MYCO.COM
- krbsvr400/iseriesc.myco.com@MYCO.COM
- krbsvr400/iseriesd.myco.com@MYCO.COM

.

Gehen Sie wie folgt vor, um sich zu vergewissern, dass die Kerberos-Authentifizierung auf den Endpunktsystemen funktioniert:

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

1. Schließen Sie alle Sitzungen des iSeries Navigator.
2. Geben Sie in einer Befehlszeile `QSH` ein, um den Qshell Interpreter zu starten.
3. Geben Sie `keytab list` ein, um eine Liste der Principals, die in der Chiffrierschlüsseldatei registriert sind, anzuzeigen. Sie sollten etwa die folgenden Ergebnisse sehen:

```
Principal: krbsvr400/iseriesa.myc.com@MYCO.COM
  Key version: 2
  Key type: 56-bit DES using key derivation
  Entry timestamp: 200X/05/29-11:02:58
```

4. Geben Sie `kinit -k krbsvr400/iseriesa.myco.com@MYCO.COM` ein, um ein Ticket-granting Ticket vom Kerberos-Server anzufordern. Mit diesem Befehl wird geprüft, ob Ihr iSeries-Server ordnungsgemäß konfiguriert wurde und das Kennwort in der Chiffrierschlüsseldatei mit dem auf dem Kerberos-Server gespeicherten Kennwort übereinstimmt.Ist dies der Fall, kann der Befehl QSH ohne Fehler angezeigt werden.
5. 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-Cache für Berechtigungsnachweise angezeigt und geprüft, ob ein gültiges Ticket für den i5/OS-Service-Principal erstellt und in den Cache für Berechtigungsnachweise auf dem iSeries-System aufgenommen wurde.

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

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

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

Sie haben jetzt die Tasks ausgeführt, die erforderlich sind, um Ihre Management Central-Serverjobs so zu konfigurieren, dass sie zwischen Endpunktsystemen die Kerberos-Authentifizierung verwenden.

## Szenario: Einzelanmeldung für i5/OS aktivieren

### Situation

Sie sind als Netzwerkadministrator für ein Unternehmen tätig. Ihre Aufgabe besteht darin, das Unternehmensnetzwerk sowie die Netzwerksicherheit für Ihr Unternehmen einschließlich der Auftragsannahme 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 in der Auftragsannahme verwenden Windows 2000 und i5/OS und benötigen mehrere Kennwörter für die verschiedenen Anwendungen, mit denen sie täglich arbeiten. 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 Auftragsannahme. 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 Auftragsannahme. 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 jedoch nicht, dass die Windows 2000-IDs und i5/OS-Benutzerprofile identisch sind. Außerdem möchten Sie kein Kennwort-Caching und keine Kennwort-Synchronisation 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 in der Auftragsannahme 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 richtige Berechtigungsstufe für die Ausführung der Anwendung für 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 in der Auftragsannahme, die ähnliche Berechtigungen benötigen, einem einzigen i5/OS-Benutzerprofil mit der richtigen Berechtigungsstufe für die Anwendung für 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 untereinnander 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 to his i5/OS-Benutzerprofil zuzuordnen. Sie können die Aktivität des Administrators aufgrund 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:

- Vereinfacht den Authentifizierungsprozess für Benutzer.
- Vereinfacht die Verwaltung des Zugriffs auf Anwendungen.
- Verringert den Systemaufwand für die Verwaltung des Zugriffs auf Server im Netzwerk.
- Verringert das Sicherheitsrisiko hinsichtlich des Kennwortdiebstahls.
- Macht Mehrfachanmeldungen überflüssig.
- Vereinfacht die Verwaltung von Benutzeridentitäten im Netzwerk.

## Ziele

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

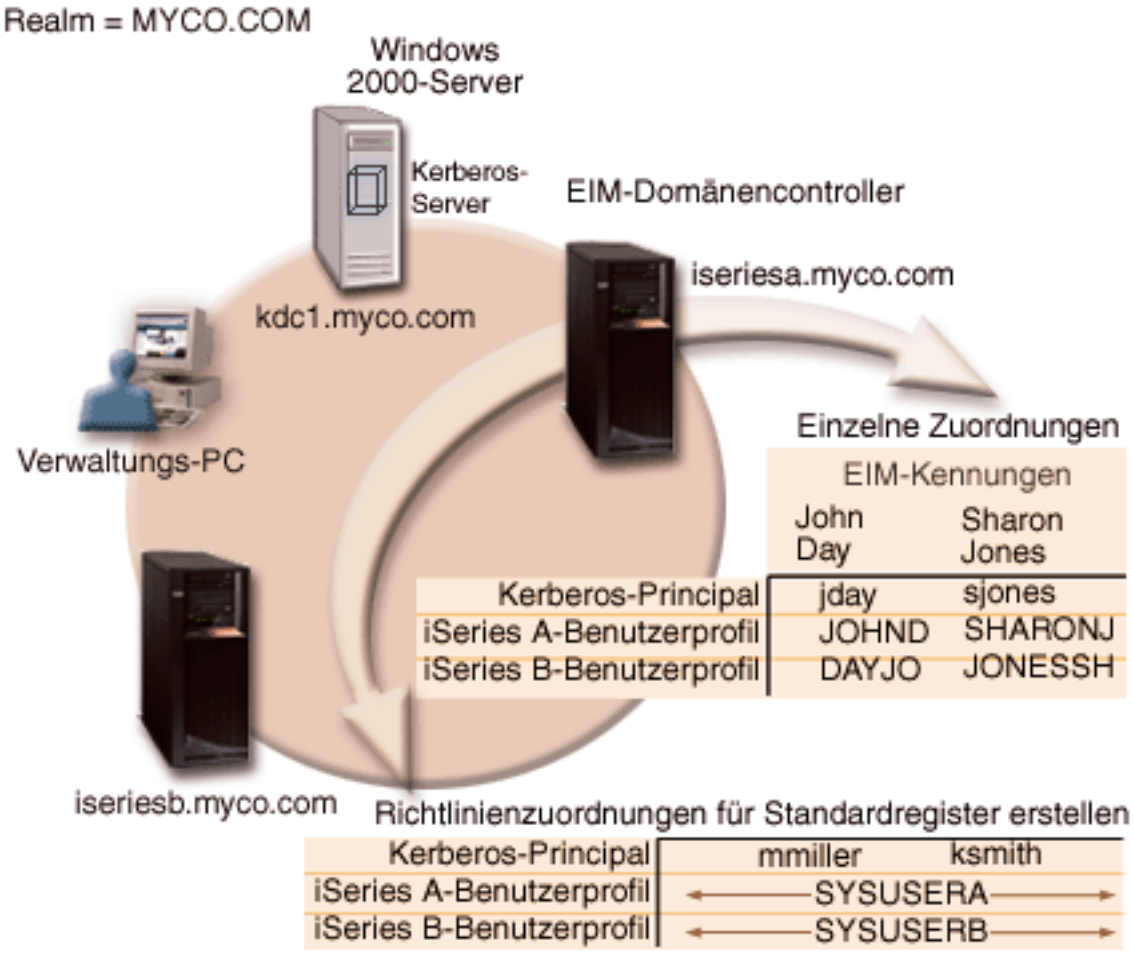
Die Ziele dieses Szenarios sind:

- iSeries A und iSeries B müssen zum Realm MYCO.COM gehören, um die Benutzer und Services, die zur Einzelanmeldungsumgebnug gehören, authentifizieren zu können.Wenn Sie die Systeme für die Verwendung von Kerberos aktivieren möchten, müssen die iSeries A und die iSeries B für den Netzwerkauthentifizierungsservice konfiguriert werden.
- Der IBM Directory Server für iSeries (LDAP) auf iSeries 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 geeignete Berechtigung für den Benutzerzugriff auf die Anwendung für Inventarabfrage besitzen.
- Abhängig von den Sicherheitsrichtlinien müssen zwei Administratoren, John Day und Sharon Jones, die auch über Benutzeridentitäten im Kerberos-Register verfügen, Kennungszuordnungen besitzen, um diese Kennungen den entsprechenden 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 für IBM iSeries Access für Windows-Anwendungen einschließlich iSeries 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 der iSeries A ausführen.
  - Der Registerdefinitionsname ISERIESA.MYCO.COM für das i5/OS-Register auf der iSeries A. Sie definieren diesen Namen, wenn Sie den EIM-Konfigurationsassistenten auf der iSeries A ausführen.
  - Der Registerdefinitionsname ISERIESB.MYCO.COM für das i5/OS-Register auf der iSeries B. Sie definieren diesen Namen, wenn Sie den EIM-Konfigurationsassistenten auf der iSeries B ausführen.
- Zwei Richtlinienzuordnungen für Standardregister:

**Anmerkung:** Eine EIM-Suchoperation bewirkt, 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 Kennungzuordnung zugeordnet. In diesem Szenario verfügen zwei Netzwerkadministratoren, John Day und Sharon Jones, über Benutzeridentitäten im Register MYCO.COM, das die Quelle der Richtlinienzuordnungen für Standardregister 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 Richtlinienzuordnung für Standardregister ordnet alle Benutzeridentitäten im Register MYCO-.COM des Windows 2000-Servers einem einzigen i5/OS-Benutzerprofil mit dem Namen SYSUSERA im Register ISERIESA.MYCO.COM auf der iSeries A zu. In diesem Szenario bezeichnen mmiller und ksmith zwei dieser Benutzeridentitäten.
  - Eine Richtlinienzuordnung für Standardregister ordnet alle Benutzeridentitäten im Register MYCO-.COM des Windows 2000-Servers einem einzigen i5/OS-Benutzerprofil mit dem Namen SYSUSERB im Register ISERIESB.MYCO.COM auf der iSeries B zu. In diesem Szenario bezeichnen mmiller und ksmith zwei dieser Benutzeridentitäten.
- 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, die ein Kerberos-Principal im Register des Windows 2000-Servers ist.
  - Eine Zielzuordnung für die Benutzeridentität JOHND, die ein Benutzerprofil im i5/OS-Register auf der iSeries A ist.
  - Eine Zielzuordnung für die Benutzeridentität DAYJO, die ein Benutzerprofil im i5/OS-Register auf der iSeries B ist.
- Für die EIM-Kennung Sharon Jones sind die folgenden Kennungszuordnungen definiert:
  - Eine Quellenzuordnung für die Benutzeridentität sjones, die ein Kerberos-Principal im Register des Windows 2000-Servers ist.
  - Eine Zielzuordnung für die Benutzeridentität SHARONJ, die ein Benutzerprofil im i5/OS-Register auf der iSeries A ist.
  - Eine Zielzuordnung für die Benutzeridentität JONESSH, die ein Benutzerprofil im i5/OS-Register auf der iSeries B ist.

**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 jedem der iSeries-Systeme einem einzigen i5/OS-Benutzerprofil zugeordnet.

**iSeries A**

- Wird unter i5/OS Version 5 Release 3 (V5R3) mit den folgenden Optionen und Lizenzprogrammen ausgeführt:
  - i5/OS Host-Server (5722-SS1 Option 12)
  - Qshell Interpreter (5722-SS1 Option 30)
  - iSeries Access für Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3)

**Anmerkung:** Sie können dieses Szenario mit einem V5R2-Server implementieren. Allerdings weichen die Konfigurationsschritte dann leicht ab. Dieses Szenario veranschaulicht außerdem einige der Funktionen für die Einzelanmeldung, die nur in V5R3 verfügbar sind, wie z. B. die Richtlinienzuordnungen. Der Abschnitt Neuerungen in V5R3 enthält weitere Informationen zu funktionalen Erweiterungen bei der Einzelanmeldung für V5R3.

- Der Directory-Server auf der iSeries A wird als EIM-Domänencontroller für die neue EIM-Domäne, MyCo-EIM-Domäne, konfiguriert.
- Nimmt an der EIM-Domäne MyCo-EIM-Domäne teil.
- Der Name des Service-Principals lautet `krbsvr400/iseriesa.myco.com@MYCO.COM`.
- Der vollständig qualifizierte Hostname lautet `iseriesa.myco.com`. Dieser Name ist in einem einzigen Domain Name System (DNS) registriert, auf den alle PCs und Server im Netzwerk verweisen.
- In Ausgangsverzeichnissen auf der iSeries A sind die Caches der Kerberos-Berechtigungsnachweise für i5/OS-Benutzerprofile gespeichert.

**iSeries B**

- Wird unter i5/OS Version 5 Release 3 (V5R3) mit den folgenden Optionen und Lizenzprogrammen ausgeführt:
  - i5/OS Host-Server (5722-SS1 Option 12)
  - Qshell Interpreter (5722-SS1 Option 30)
  - iSeries Access für Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3)
- Hat den vollständig qualifizierten Hostnamen `iseriesb.myco.com`. Dieser Name ist in einem einzigen Domain Name System (DNS) registriert, auf den alle PCs und Server im Netzwerk zeigen.
- Der Principal-Name für die iSeries B lautet `krbsvr400/iseriesb.myco.com@MYCO.COM`.
- Nimmt an der EIM-Domäne MyCo-EIM-Domäne teil.
- In Ausgangsverzeichnissen auf der iSeries B sind die Caches der Kerberos-Berechtigungsnachweise für i5/OS-Benutzerprofile gespeichert.

**Verwaltungs-PC**

- Wird unter dem Betriebssystem Microsoft Windows 2000 ausgeführt.
- Wird unter iSeries Access für Windows V5R3 (5722-XE1) ausgeführt.
- Wird unter iSeries Navigator mit den folgenden installierten Unterkomponenten ausgeführt:
  - 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 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 iSeries Navigator den Eintrag für Ihren **iSeries-Server** → **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 nicht zuvor auf der iSeries A konfiguriert worden sein.

   **Anmerkung:** Die Anweisungen in diesem Szenario basieren auf der Annahme, dass der Directory-Server nicht zuvor auf der iSeries A konfiguriert wurde. Wurde der Directory-Server bereits konfiguriert, können Sie diese Anweisungen leicht abgeändert immer noch verwenden. Diese Änderungen sind an den entsprechenden Stellen in den Konfigurationsschritten vermerkt.
5. Ein DNS-Server wird für die Auflösung der Hostnamen im Netzwerk verwendet. Es werden keine Hosttabellen für die Auflösung der Hostnamen verwendet.

   **Anmerkung:** Die Verwendung von Hosttabellen mit Kerberos-Authentifizierung kann zu Fehlern bei der Namensauflösung oder anderen Problemen führen. Ausführliche Informationen zur Auflösung von Hostnamen mit der Kerberos-Authentifizierung finden Sie unter „Hinweise zur Auflösung von Hostnamen" auf Seite 95.

## Konfigurationsschritte

**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. Lesen Sie die folgenden Themen, um sich mit den Begriffen und Konzepten im Zusammenhang mit der Einzelanmeldung vertraut zu machen:

- Enterprise Identity Mapping (EIM)
- Netzwerkauthentifizierungsservice

1. Planungsarbeitsblätter ausfüllen
2. Basiskonfiguration für Einzelanmeldung für die iSeries A erstellen
3. Die iSeries B zur Teilnahme an der EIM-Domäne konfigurieren und die iSeries B für Netzwerkauthentifizierungsservice konfigurieren
4. Beide i5/OS-Service-Principals zum Kerberos-Server hinzufügen
5. Benutzerprofile für die iSeries A und iSeries B erstellen
6. Ausgangsverzeichnisse für die iSeries A und die iSeries B erstellen
7. Netzwerkauthentifizierungsservice für die iSeries A und die iSeries B testen
8. EIM-Kennungen für zwei Administratoren, John Day und Sharon Jones, erstellen
9. Kennungszuordnungen für John Day erstellen
10. Kennungszuordnungen für Sharon Jones erstellen
11. Richtlinienzuordnung für Standardregister erstellen
12. Register für die Teilnahme an Suchoperationen und die Verwendung von Richtlinienzuordnungen aktivieren
13. EIM-Identitätsabgleiche testen
14. iSeries Access für Windows-Anwendungen für die Verwendung der Kerberos-Authentifizierung konfigurieren
15. Konfiguration von Netzwerkauthentifizierungsservice und EIM überprüfen
16. (Optional) Hinweise für die Phase nach der Konfiguration

## Details zum Szenario: Einzelanmeldung für i5/OS aktivieren
## Schritt 1: Planungsarbeitsblätter ausfüllen

Die folgenden Planungsarbeitsblätter wurden basierend auf den allgemeinen Planungsarbeitsblättern der Einzelanmeldung an dieses Szenario angepasst. Diese Planungsarbeitsblätter veranschaulichen die Infor-

mationen, die Sie aufzeichnen, sowie die Entscheidungen, die Sie treffen müssen, wenn Sie die Konfiguration der von diesem Szenario beschriebenen Einzelanmeldungsfunktion vorbereiten. Um ein erfolgreiches Setup 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 der Einzelanmeldung, wie z. B. dem Netzwerkauthentifizierungsservice und EIM (Enterprise Identity Mapping), vertraut sein, um dieses Szenario verwenden zu können. Lesen Sie die folgenden Themen, um sich mit den Begriffen und Konzepten im Zusammenhang mit der Einzelanmeldung vertraut zu machen:

- Enterprise Identity Mapping (EIM)
- Netzwerkauthentifizierungsservice

*Tabelle 13. Arbeitsblatt für Voraussetzungen*

| **Arbeitsblatt für Voraussetzungen** | **Antworten** |
|---|---|
| Arbeiten Sie mit i5/OS V5R3 (5722-SS1) oder einer späteren Version? | Ja |
| Sind die folgenden Optionen und Lizenzprogramme auf der iSeries A und der iSeries B installiert?<br>• i5/OS Host Servers (5722-SS1 Option 12)<br>• Qshell Interpreter (5722-SS1 Option 30)<br>• iSeries Access für Windows (5722-XE1)<br>• Cryptographic Access Provider (5722-AC3) | Ja |
| Ist eine Anwendung installiert, die auf allen PCs, die sich in der Einzelanmeldungsumgebung befinden, für die Einzelanmeldung aktiviert ist?<br>**Anmerkung:** In diesem Szenario wurde für alle in der Umgebung befindlichen PCs iSeries Access für Windows (5722-XE1) installiert. | Ja |
| Ist iSeries Navigator auf dem Administrator-PC installiert?<br>• Ist die Unterkomponente "Netzwerk" von iSeries Navigator auf dem PC, der für die Verwaltung der Einzelanmeldung verwendet wird, installiert?<br>• Ist die Unterkomponente "Sicherheit" von iSeries Navigator auf dem PC, der für die Verwaltung der Einzelanmeldung verwendet wird, installiert?<br>• Ist die Unterkomponente "Benutzer und Gruppen" von iSeries Navigator auf dem PC, der für die Verwaltung der Einzelanmeldung verwendet wird, installiert? | Ja |
| Ist das aktuellste Service-Pack von IBM @server iSeries Access für Windows installiert?<br>Dieses Service-Pack finden Sie auf der Webseite iSeries Access. | Ja |
| Besitzt der Administrator für Einzelanmeldung die Sonderberechtigungen *SECADM, *ALLOBJ und *IOSYSCFG? | Ja |

*Tabelle 13. Arbeitsblatt für Voraussetzungen (Forts.)*

| Arbeitsblatt für Voraussetzungen | Antworten |
|---|---|
| Fungiert eines der folgenden Systeme als Kerberos-Server (auch als KDC bezeichnet)? Wenn ja, geben Sie an, um welches System es sich handelt.<br>1. Microsoft Windows 2000-Server<br>**Anmerkung:** Microsoft Windows 2000-Server verwendet die Kerberos-Authentifizierung als Standardsicherheitsmechanismus.<br>2. Windows (R) Server 2003<br>3. i5/OS PASE (ab V5R3)<br>4. AIX-Server<br>5. zSeries | Ja, Windows 2000-Server |
| Sind alle PCs Ihres Netzwerks in einer Windows 2000-Domäne konfiguriert? | Ja |
| Wurden die aktuellsten vorläufigen Programmkorrekturen (PTFs) angelegt? | Ja |
| Beträgt die Abweichung zwischen der Systemzeit der iSeries und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung größer, lesen Sie „Systemzeiten synchronisieren" auf Seite 118. | Ja |

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

*Tabelle 14. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung für die iSeries A*

| Planungsarbeitsblatt für die Konfiguration der iSeries 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?<br>• System zu einer vorhandenen Domäne hinzufügen<br>• Neue Domäne erstellen und System hinzufügen | Neue Domäne erstellen und System hinzufügen |
| Wo möchten Sie die EIM-Domäne konfigurieren? | Auf dem lokalen Directory-Server<br>**Anmerkung:** Bei Auswahl dieser Option wird der Directory-Server auf demselben System konfiguriert, auf dem Sie gegenwärtig EIM konfigurieren. |
| Möchten Sie den Netzwerkauthentifizierungsservice konfigurieren?<br>**Anmerkung:** Sie müssen den Netzwerkauthentifizierungsservice konfigurieren, um die Einzelanmeldung zu konfigurieren. | Ja |
| Der Assistent für den Netzwerkauthentifizierungsservice wird im EIM-Konfigurationsassistenten geöffnet. Verwenden Sie die folgenden Informationen, um den Assistenten für den Netzwerkauthentifizierungsservice auszuführen. | |
| Wie lautet der Name des Kerberos-Standard-Realms, zu dem Ihre iSeries gehören soll?<br>**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 |

*Tabelle 14. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung für die iSeries A (Forts.)*

| **Planungsarbeitsblatt für die Konfiguration der iSeries A** | **Antworten** |
|---|---|
| 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`<br>**Port:** `88`<br>**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:<br><br>Wie lautet der Name des Kennwortservers für diesen Kerberos-Server?<br>An welchem Port ist der Kennwortserver empfangsbereit? | Ja<br><br>**Kennwortserver:**<br>`kdc1.myco.com`<br>**Port:** `464`<br>**Anmerkung:** Dies ist der Standardport für den Kennwortserver. |
| Für welche Services möchten Sie Chiffrierschlüsseleinträge erstellen?<br>• i5/OS-Kerberos-Authentifizierung<br>• LDAP<br>• iSeries IBM HTTP-Server<br>• iSeries NetServer | i5/OS-Kerberos-Authentifizierung |
| Wie lautet das Kennwort für Ihre(n) Service-Principal(s)? | `iseriesa123`<br>**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 die iSeries A zum Kerberos-Register zu automatisieren? | Ja |
| Möchten Sie den 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.<br>**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`<br>**Registrierter Name:** `cn=Administrator`<br>**Kennwort:** `mycopwd`<br>**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? | `MyCo-EIM-Domäne` |
| Möchten Sie einen übergeordneten registrierten Namen für die EIM-Domäne angeben? | Nein |
| Welche Benutzerregister möchten Sie zur EIM-Domäne hinzufügen? | Lokales i5/OS--ISERIESA.MYCO.COM<br>Kerberos--KDC1.MYCO.COM<br>**Anmerkung:** Sie dürfen die Option **Bei Kerberos-Benutzeridentifikationen muss die Groß-/Kleinschreibung beachtet werden** nicht auswählen, wenn sie vom Assistenten angeboten wird. |

*Tabelle 14. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung für die iSeries A (Forts.)*

| Planungsarbeitsblatt für die Konfiguration der iSeries A | Antworten |
|---|---|
| Welchen EIM-Benutzer soll die iSeries A bei der Ausführung von EIM-Operationen verwenden? Dies ist der Systembenutzer.<br>**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:**<br>`Registrierter Name`<br>**Registrierter Name:** `cn=Administrator`<br>**Kennwort:** `mycopwd`<br>**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 die iSeries B an der EIM-Domäne teilnehmen kann und Sie den Netzwerkauthentifizierungsservice auf der iSeries B konfigurieren können.

*Tabelle 15. Planungsarbeitsblatt für die Konfiguration der iSeries B*

| Planungsarbeitsblatt für die Konfiguration der iSeries B | Antworten |
|---|---|
| Verwenden Sie die folgenden Informationen, um den EIM-Konfigurationsassistenten für die iSeries B auszuführen: | |
| Wie möchten Sie EIM auf Ihrem System konfigurieren? | System zu einer vorhandenen Domäne hinzufügen |
| Möchten Sie den Netzwerkauthentifizierungsservice konfigurieren?<br>**Anmerkung:** Sie müssen den Netzwerkauthentifizierungsservice konfigurieren, um die Einzelanmeldung zu konfigurieren. | Ja |
| Der Assistent für den Netzwerkauthentifizierungsservice wird im EIM-Konfigurationsassistenten geöffnet. Verwenden Sie die folgenden Informationen, um den Assistenten für den Netzwerkauthentifizierungsservice auszuführen:<br>**Anmerkung:** Sie können den Assistenten für den Netzwerkauthentifizierungsservice im EIM-Konfigurationsassistenten öffnen. | |
| Wie lautet der Name des Kerberos-Standard-Realms, zu dem Ihre iSeries gehören soll?<br>**Anmerkung:** Eine Windows 2000-Domäne entspricht einem Kerberos-Realm. Das Microsoft Active Directory verwendet die Kerberos-Authentifizierung als Standardsicherheitsmechanismus. | `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`<br>**Port:** `88`<br>**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:<br><br>Wie lautet der Name des Kennwortservers für diesen Kerberos-Server?<br>An welchem Port ist der Kennwortserver empfangsbereit? | Ja<br><br>**Kennwortserver:**<br>`kdc1.myco.com`<br>**Port:** `464`<br>**Anmerkung:** Dies ist der Standardport für den Kennwortserver. |
| Für welche Services möchten Sie Chiffrierschlüsseleinträge erstellen?<br>• i5/OS-Kerberos-Authentifizierung<br>• LDAP<br>• iSeries IBM HTTP-Server<br>• iSeries NetServer | i5/OS-Kerberos-Authentifizierung |

*Tabelle 15. Planungsarbeitsblatt für die Konfiguration der iSeries B (Forts.)*

| **Planungsarbeitsblatt für die Konfiguration der iSeries B** | **Antworten** |
|---|---|
| Wie lautet das Kennwort für Ihre(n) i5/OS-Service-Principal(s)? | iseriesb123<br>**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 die iSeries B zum Kerberos-Register zu automatisieren? | Ja |
| Möchten Sie den 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 die iSeries B auszuführen: | |
| Wie lautet der Name des EIM-Domänencontrollers für die EIM-Domäne, die Sie dem System hinzufügen möchten? | iseriesa.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.<br>**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`<br>**Registrierter Name:** `cn=Administrator`<br>**Kennwort:** `mycopwd`<br>**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? | `MyCo-EIM-Domäne` |
| 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--ISERIESB.MYCO.COM |
| Welchen EIM-Benutzer soll die iSeries B bei der Ausführung von EIM-Operationen verwenden? Dies ist der Systembenutzer.<br>**Anmerkung:** In einem früheren Status dieses Szenarios haben Sie den EIM-Konfigurationsassistenten verwendet, um den Directory-Server auf der iSeries 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`<br>**Registrierter Name:** `cn=Administrator`<br>**Kennwort:** `mycopwd`<br>**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 16. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung - Benutzerprofile*

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

*Tabelle 17. 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 | ISERIESA.MYCO.COM | JOHND | Ziel | Name des i5/OS-Benutzerprofils auf der iSeries A |
| John Day | ISERIESB.MYCO.COM | DAYJO | Ziel | Name des i5/OS-Benutzerprofils auf der iSeries B |
| Sharon Jones | MYCO.COM | sjones | Quelle | Benutzeridentität für Kerberos-Anmeldung (Windows 2000) |
| Sharon Jones | ISERIESA.MYCO.COM | SHARONJ | Ziel | Name des i5/OS-Benutzerprofils auf der iSeries A |
| Sharon Jones | ISERIESB.MYCO.COM | JONESSH | Ziel | Name des i5/OS-Benutzerprofils auf der iSeries B |

*Tabelle 18. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung - EIM-Domänendaten - Richtlinienzuordnungen*

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

## Schritt 2: Basiskonfiguration für Einzelanmeldung für die iSeries 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 der Directory-Server nicht zuvor auf der iSeries A konfiguriert wurde. Wurde der Directory-Server bereits konfiguriert, können Sie diese Anweisungen leicht abgeändert immer noch verwenden. Diese Änderungen sind an den entsprechenden Stellen in den Konfigurationsschritten vermerkt.

Verwenden Sie die Informationen in den Arbeitsblättern, um EIM und den Netzwerkauthentifizierungsservice auf der iSeries A zu konfigurieren. Dieser Schritt setzt sich aus folgenden Tasks zusammen:

- Eine neue EIM-Domäne erstellen.
- Den Directory-Server auf der iSeries A als EIM-Domänencontroller konfigurieren.

- Den Netzwerkauthentifizierungsservice konfigurieren.
- EIM-Registerdefinitionen für das i5/OS-Register und das Kerberos-Register auf der iSeries A erstellen.
- Die iSeries A zur Teilnahme an der EIM-Domäne konfigurieren.

1. Erweitern Sie im iSeries Navigator den Eintrag **iSeries 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 Option **Neue Domäne erstellen und System hinzufügen**. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Position der EIM-Domäne angeben** die Option **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 Option **Ja** aus.

      **Anmerkung:** Auf diese Weise wird der Assistent für den Netzwerkauthentifizierungsservice geöffnet. Mit diesem Assistenten können Sie verschiedene i5/OS-Schnittstellen und -Services zur Teilnahme am Kerberos-Realm 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 Option **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 Option **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: `iseriesa123`. Dieses Kennwort wird verwendet, wenn der Service-Principal von der iSeries 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 Option **Ja** aus, machen Sie die folgenden Angaben, und klicken Sie auf **Weiter**:
      - **Stapeldatei:** Fügen Sie am Ende des standardmäßig verwendeten Stapeldateinamens die Zeichenfolge `iseriesa` an. Beispiel: `C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigiseriesa.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** anstelle 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: `MyCo-EIM-Domäne`.
8. Wählen Sie auf der Seite **Übergeordneten registrierten Namen für Domäne angeben** die Option **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** die Optionen **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 Benennungsplan für Registerdefinitionen 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 eine Basiskonfiguration von EIM und Netzwerkauthentifizierungsservice auf der iSeries A erstellt. Der nächste Schritt besteht darin, die iSeries B zur Teilnahme an der soeben erstellten EIM-Domäne zu konfigurieren.

## Schritt 3: Die iSeries B zur Teilnahme an der EIM-Domäne konfigurieren und die iSeries B für den Netzwerkauthentifizierungsservice konfigurieren

Nachdem Sie eine neue Domäne erstellt und den Netzwerkauthentifizierungsservice auf der iSeries A konfiguriert haben, müssen Sie die iSeries B zur Teilnahme an der EIM-Domäne konfigurieren. Außerdem müssen Sie den Netzwerkauthentifizierungsservice auf der iSeries B konfigurieren. Verwenden Sie die Informationen aus Ihren Arbeitsblättern, um diesen Schritt durchzuführen.

1. Erweitern Sie im iSeries Navigator den Eintrag **iSeries 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 Option **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 Option **Ja** aus.

      **Anmerkung:** Auf diese Weise wird der Assistent für den Netzwerkauthentifizierungsservice geöffnet. Mit diesem Assistenten können Sie verschiedene i5/OS-Schnittstellen und -Services zur Teilnahme am Kerberos-Realm 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 Option **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 Option **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: `iseriesa123`. Dieses Kennwort wird verwendet, wenn der Service-Principal von der iSeries 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 Option **Ja** aus, machen Sie die folgenden Angaben, und klicken Sie auf **Weiter**:
      - **Stapeldatei:** Fügen Sie am Ende des standardmäßig verwendeten Stapeldateinamens die Zeichenfolge `iseriesb` an. Beispiel: `C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigiseriesb.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**: `iseriesa.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, das Sie zuvor in diesem Szenario auf der iSeries 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: `MyCo-EIM-Domäne`.
8. Wählen Sie auf der Seite **Registerinformationen** die Option **Lokales i5/OS** aus und heben Sie die Auswahl **Kerberos-Register** auf. (Das Kerberos-Register wurde beim Erstellen der Domäne MyCo-EIM 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 Benennungsplan für Registerdefinitionen 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, das Sie zuvor in diesem Szenario auf der iSeries 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 jetzt die iSeries B zur Teilnahme an der Domäne und zur Verwendung des Netzwerkauthentifizierungsservice konfiguriert.

## Schritt 4: 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 `ftp kdc1.myco.com` ein. Auf diese Weise starten Sie eine FTP-Sitzung auf Ihrem PC. Sie werden aufgefordert, den Benut- zernamen und das Kennwort des Administrators einzugeben.
2. Geben Sie bei der FTP-Eingabeaufforderung `lcd "C:\Documents and Settings\All Users\Documents\IBM\Client Access"` ein. Drücken Sie die Eingabetaste. Sie sollten die Nachricht `Lokales Verzeichnis jetzt C:\Documents and Settings\All Users\Documents\IBM\Client Access` empfangen.
3. Geben Sie bei der FTP-Eingabeaufforderung `cd \meinVerzeichnis` ein. *meinVerzeichnis* bezeichnet ein auf kdc1.myco.com befindliches Verzeichnis.
4. Geben Sie bei der FTP-Eingabeaufforderung `put NASConfigiseriesa.bat` ein. Sie sollten diese Nachricht empfangen: `226 Transfer complete`.
5. Geben Sie `quit` ein, um die FTP-Sitzung zu verlassen.

Wiederholen Sie diese Schritte, um die Datei NASConfigiseriesb.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 wurde.
2. Suchen Sie die Datei `NASConfigiseriesa.bat` und klicken Sie doppelt auf die Datei, um sie auszuführen.
3. Wiederholen Sie diese Schritte für `NASConfigiseriesb.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 den Eintrag **Verwaltungstools → Active Directory-Benutzer und -Computer → Benutzer**.
   b. Vergewissern Sie sich, dass die iSeries 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 **iseriesa_1_krbsvr400** und **iseriesb_1_krbsvr400**. Dies sind 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 Indexzunge **Konto** die Option **Konto wird für Delegierungszwecke vertraut** aus.

      **Anmerkung:** Dieser optionale Schritt ermöglicht Ihrem System, die Berechtigungen 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. In einem Netzwerk, das mit mehreren Ebenen arbeitet, ist dies nützlich.

Sie haben die i5/OS-Service-Principals zum Kerberos-Server hinzugefügt und können jetzt Benutzerprofile auf den iSeries-Systemen erstellen.

## Schritt 5: Benutzerprofile auf der iSeries A und der iSeries B erstellen

Die Benutzer im Kerberos-Register MYCO.COM sollen einem einzigen i5/OS-Benutzerprofil auf den iSeries-Systemen zugeordnet werden. Daher müssen Sie ein i5/OS-Benutzerprofil auf der iSeries A und der iSeries B erstellen.

Verwenden Sie die Informationen aus Ihren Arbeitsblättern, um ein Benutzerprofil für diese Benutzer zu erstellen:

1. Erweitern Sie im iSeries Navigator den Eintrag **iSeries 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** `SYSUSERA` ein.
4. Wählen Sie im Feld **Kennwort** die Option **Kein Kennwort (Anmeldung nicht zulässig)** aus.
5. Klicken Sie auf **Funktionsspektrum**.
6. Wählen Sie auf der Seite **Berechtigungen** im Feld **Berechtigungsklasse** die Option **Benutzer** aus. Klicken Sie auf **OK** und dann auf **Hinzufügen**.

Wiederholen Sie diese Schritte auf der iSeries B, geben Sie jedoch `SYSUSERB` im Feld **Benutzername** ein.

Sie haben die Benutzerprofile auf der iSeries A und der iSeries B erstellt und sind jetzt in der Lage, Ausgangsverzeichnisse für alle i5/OS-Benutzerprofile zu erstellen.

## Schritt 6: Ausgangsverzeichnisse auf der iSeries A und der iSeries B erstellen

Jeder Benutzer, der eine Verbindung zu i5/OS und i5/OS-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 iSeries-Befehlszeile Folgendes ein: `CRTDIR '/home/Benutzerprofil'`, wobei `Benutzerprofil` den Namen des i5/OS-Benutzerprofils für den Benutzer bezeichnet. Beispiel: `CRTDIR '/home/SYSUSERA'`. Auf diese Weise wird ein Ausgangsverzeichnis für das Benutzerprofil auf der iSeries A erstellt, das alle Active Directory-Benutzer enthält.

Wiederholen Sie diesen Befehl auf der iSeries B, geben Sie jedoch SYSUSERB ein, um ein Ausgangsverzeichnis für das Benutzerprofil auf der iSeries B zu erstellen.

Sie haben die Ausgangsverzeichnisse erstellt und können jetzt die Konfiguration des Netzwerkauthentifizierungsservice auf den iSeries-Systemen testen.

## Schritt 7: Netzwerkauthentifizierungsservice auf der iSeries A and iSeries B testen

Nachdem Sie die Tasks zur Konfiguration des Netzwerkauthentifizierungsservice für beide Systeme ausgeführt haben, müssen Sie überprüfen, ob Ihre Konfigurationen für die iSeries A und iSeries B ordnungsgemäß funktionieren. Sie können dies tun, indem Sie die folgenden Schritte zur Anforderung eines Ticket-granting Ticket für die Principals der iSeries A und der iSeries B durchführen:

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

1. Geben Sie in einer Befehlszeile `QSH` ein, um den Qshell Interpreter zu starten.

2. Geben Sie `keytab list` ein, um eine Liste der Principals, die in der Chiffrierschlüsseldatei registriert sind, anzuzeigen. In diesem Szenario sollte krbsvr400/iseriesa.myco.com@MYCO.COM als Name des Principals für die iSeries A erscheinen.
3. Geben Sie `kinit -k krbsvr400/iseriesa.myco.com@MYCO.COM` ein, um ein Ticket-granting Ticket vom Kerberos-Server anzufordern. Mit diesem Befehl wird geprüft, ob Ihr iSeries-Server ordnungsgemäß konfiguriert wurde und das Kennwort in der Chiffrierschlüsseldatei mit dem auf dem Kerberos-Server 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-Cache für Berechtigungsnachweise angezeigt und geprüft, ob ein gültiges Ticket für den i5/OS-Service-Principal erstellt und in den Cache für Berechtigungsnachweise auf dem iSeries-System aufgenommen wurde.

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

Default principal: krbsvr400/iseriesa.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 Schritte mit dem Service-Principal-Namen für die iSeries B: krbsvr400/iseriesb.myco.com@MYCO.COM

Sie haben den Netzwerkauthentifizierungsservice auf der iSeries A und der iSeries B getestet und können jetzt für jeden der Administratoren eine EIM-Kennung erstellen.

## Schritt 8: EIM-Kennungen für zwei Administratoren, John Day und Sharon Jones, erstellen

Bei der Konfiguration der Testumgebung für die Einzelanmeldung müssen Sie EIM-Kennungen für zwei Ihrer Administratoren erstellen, damit sich beide mit ihren Windows-Benutzeridentitäten bei i5/OS anmelden können. In diesem Szenario erstellen Sie zwei EIM-Kennungen, John Day und Sharon Jones. Führen Sie die folgenden Schritte durch, um die EIM-Kennungen zu erstellen:

1. Erweitern Sie im iSeries Navigator den Eintrag **iSeries 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. Geben Sie die folgenden Informationen an, und klicken Sie auf **OK**, um eine Verbindung zum Domänencontroller herzustellen:

   - **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** `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.

Sie haben für beide Administratoren eine EIM-Kennung erstellt und müssen jetzt Kennungszuordnungen erstellen, mit denen Benutzeridentitäten den Kennungen zugeordnet werden. Erstellen Sie zuerst die Kennungszuordnungen für John Day.

## Schritt 9: 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 Teilnahme an 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 i5/OS-Benutzerprofil JOHND, das die Person John Day als Benutzeridentität zur Anmeldung beim iSeries Navigator und anderen i5/OS-Anwendungen auf der iSeries A verwendet. 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 DAYJO, das die Person John Day als Benutzeridentität zur Anmeldung beim iSeries Navigator und anderen i5/OS-Anwendungen auf der iSeries B verwendet. 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 der iSeries A den Eintrag **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** Informationen 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 **Zuordnungen hinzufügen** zu schließen.

   Führen Sie die folgenden Schritte durch, um eine Zielzuordnung zum i5/OS-Benutzerprofil von John Day auf der iSeries A zu erstellen:
6. Klicken Sie auf der Seite **Zuordnungen** auf **Hinzufügen**.
7. Geben Sie im Dialogfenster **Zuordnung hinzufügen** Informationen an oder klicken Sie auf **Durchsuchen...**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **OK**:
   - **Register**: `ISERIESA.MYCO.COM`
   - **Benutzer**: `JOHND`
   - **Zuordnungsart**: `Ziel`
8. Klicken Sie auf **OK**, um das Dialogfenster **Zuordnungen hinzufügen** zu schließen.

Führen Sie die folgenden Schritte durch, um eine Zielzuordnung zum i5/OS-Benutzerprofil von John Day auf der iSeries B zu erstellen:

9. Klicken Sie auf der Seite **Zuordnungen** auf **Hinzufügen**.
10. Geben Sie im Dialogfenster **Zuordnung hinzufügen** Informationen an oder klicken Sie auf **Durchsuchen...**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **OK**:
    - **Register**: `ISERIESB.MYCO.COM`
    - **Benutzer**: `DAYJO`
    - **Zuordnungsart**: `Ziel`
11. Klicken Sie auf **OK**, um das Dialogfenster **Zuordnungen hinzufügen** zu schließen.
12. Klicken Sie auf **OK**, um das Dialogfenster **Eigenschaften** zu schließen.

Sie haben die Kennungszuordnungen erstellt, die die Benutzeridentitäten von John Day seiner EIM-Kennung zuordnen, und können jetzt ähnliche Zuordnungen für Sharon Jones erstellen.

## Schritt 10: 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. Die Kennungszuordnungen ermöglichen dem Benutzer, richtige Konfiguration vorausgesetzt, die Teilnahme an 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, das die Person Sharon Jones als Benutzeridentität zur Anmeldung beim iSeries Navigator und anderen i5/OS-Anwendungen auf der iSeries A verwendet. 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, das die Person Sharon Jones als Benutzeridentität zur Anmeldung beim iSeries Navigator und anderen i5/OS-Anwendungen auf der iSeries B verwendet. 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 der iSeries A den Eintrag **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** Informationen 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 **Zuordnungen hinzufügen** zu schließen.

Führen Sie die folgenden Schritte durch, um eine Zielzuordnung zum i5/OS-Benutzerprofil von Sharon Jones auf der iSeries A zu erstellen:

6. Klicken Sie auf der Seite **Zuordnungen** auf **Hinzufügen**.
7. Geben Sie im Dialogfenster **Zuordnung hinzufügen** Informationen an oder klicken Sie auf **Durchsuchen...**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **OK**:
   - **Register**: `ISERIESA.MYCO.COM`
   - **Benutzer**: `SHARONJ`
   - **Zuordnungsart**: `Ziel`
8. Klicken Sie auf **OK**, um das Dialogfenster **Zuordnungen hinzufügen** zu schließen.

Führen Sie die folgenden Schritte durch, um eine Zielzuordnung zum i5/OS-Benutzerprofil von Sharon Jones auf der iSeries B zu erstellen:

9. Klicken Sie auf der Seite **Zuordnungen** auf **Hinzufügen**.
10. Geben Sie im Dialogfenster **Zuordnung hinzufügen** Informationen an oder klicken Sie auf **Durchsuchen...**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **OK**:
    - **Register**: `ISERIESB.MYCO.COM`
    - **Benutzer**: `JONESSH`
    - **Zuordnungsart**: `Ziel`
11. Klicken Sie auf **OK**, um das Dialogfenster **Zuordnungen hinzufügen** zu schließen.
12. Klicken Sie auf **OK**, um das Dialogfenster **Eigenschaften** zu schließen.

Sie haben die Kennungszuordnungen erstellt, mit denen die Benutzeridentitäten von Sharon Jones ihrer EIM-Kennung zugeordnet werden. Jetzt können Sie die Richtlinienzuordnungen für das Standardregister erstellen, die alle Benutzer des Kerberos-Registers einem bestimmten Benutzerprofil in allen iSeries-Benutzerregistern zuordnen.

## Schritt 11: Richtlinienzuordnungen für Standardregister erstellen

Sie möchten alle Microsoft Active Directory-Benutzer auf dem Windows 2000-Server dem Benutzerprofil SYSUSERA auf der iSeries A und dem Benutzerprofil SYSUSERB auf der iSeries 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 Richtlinienzuordnung erstellen, die alle Benutzeridentitäten (für die keine Kennungszuordnungen vorhanden sind) im Kerberos-Register MYCO.COM einem einzelnen i5/OS-Benutzerprofil auf iSeries A zuordnet.

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 Benutzeridentitäten in diesem Register verschiedenen Zielbenutzeridentitäten zu, je nach iSeries-System, auf das der Kerberos-Benutzer zugreift:

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

Verwenden Sie die Informationen aus Ihren Arbeitsblättern, um zwei Richtlinienzuordnungen für Standardregister zu erstellen:

**Anmerkung**: Bevor Sie jedoch Richtlinienzuordnungen verwenden können, müssen Sie die Domäne zur Verwendung von Richtlinienzuordnungen für Abgleichsuchoperationen aktivieren. Sie haben die Möglichkeit, diese Aktivierung bei der Erstellung Ihrer Richtlinienzuordnung durchzuführen. Gehen Sie dazu wie folgt vor:

1. Erweitern Sie im iSeries Navigator den Eintrag **iSeries A → Netzwerk → Enterprise Identity Mapping → Domänenverwaltung**.
2. Klicken Sie mit der rechten Maustaste auf **MyCo-EIM-Domäne**, und wählen Sie **Abgleichrichtlinie...** aus.
3. Wählen Sie auf der Seite **Allgemein** die Option **Abgleichsuchen mit Hilfe von Richtlinienzuordnungen für Domäne MyCo-EIM-Domäne aktivieren** aus.

   Führen Sie die folgenden Schritte durch, um die Richtlinienzuordnung für Standardregister für die Benutzer, die dem Benutzerprofil SYSUSERA auf der iSeries A zugeordnet werden sollen, zu erstellen:
4. Klicken Sie auf der Seite **Register** auf **Hinzufügen**.
5. Geben Sie im Dialogfenster **Richtlinienzuordnung für Standardregister hinzufügen** Informationen an oder klicken Sie auf **Durchsuchen...**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **OK**:
   - **Quellenregister**: `MYCO.COM`
   - **Zielregister**: `ISERIESA.MYCO.COM`
   - **Zielbenutzer**: `SYSUSERA`
6. Klicken Sie auf **OK**, um das Dialogfenster **Abgleichrichtlinie** zu schließen.

   Führen Sie die folgenden Schritte durch, um die Richtlinienzuordnung für Standardregister für die Benutzer, die dem Benutzerprofil SYSUSERB auf der iSeries B zugeordnet werden sollen, zu erstellen:
7. Klicken Sie auf der Seite **Register** auf **Hinzufügen**.
8. Geben Sie im Dialogfenster **Richtlinienzuordnung für Standardregister hinzufügen** Informationen an oder klicken Sie auf **Durchsuchen...**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **OK**:
   - **Quellenregister**: `MYCO.COM`
   - **Zielregister**: `ISERIESB.MYCO.COM`
   - **Zielbenutzer**: `SYSUSERB`
9. Klicken Sie auf **OK**, um das Dialogfenster **Abgleichrichtlinie** zu schließen.

Sie haben die Richtlinienzuordnungen für Standardregister erstellt und können jetzt die Register zur Teilnahme an Suchoperationen und zur Verwendung der Richtlinienzuordnungen aktivieren.

## Schritt 12: Register für die Teilnahme an Suchoperation und die Verwendung von Richtlinienzuordnungen aktivieren

Mit EIM können Sie die Teilnahme der einzelnen Register an EIM steuern. 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 an Abgleichsuchoperationen teilnehmen soll. Wenn Sie Richtlinienzuordnungen für ein Register verwenden möchten, müssen Sie deren Verwendung für das gegebene Register aktivieren und das Register für die Teilnahme an Suchoperationen aktivieren.

Führen Sie die folgenden Schritte durch, um Register für die Verwendung von Richtlinienzuordnungen und für die Teilnahme an Suchoperationen zu aktivieren:

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

1. Erweitern Sie im iSeries Navigator den Eintrag **iSeries 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 Option **Abgleichsuchen mit Hilfe von Richtlinienzuordnungen für Register MYCO aktivieren** aus. Klicken Sie auf **OK**.

Führen Sie die folgenden Schritte durch, um das Register ISERIESA.MYCO.COM für die Teilnahme an Abgleichsuchoperationen und die Verwendung von Richtlinienzuordnungen zu aktivieren:

1. Erweitern Sie im iSeries Navigator den Eintrag **iSeries A → Netzwerk → Enterprise Identity Mapping → Domänenverwaltung → MyCoEimDomain → Benutzerregister**.
2. Klicken Sie mit der rechten Maustaste auf **ISERIESA.MYCO.COM**, und wählen Sie **Abgleichrichtlinie...** aus.
3. Wählen Sie auf der Seite **Allgemein** die Option **Abgleichsuchen mit Hilfe von Richtlinienzuordnungen für Register ISERIESA.MYCO.COM aktivieren** und dann **Richtlinienzuordnungen verwenden** aus. Klicken Sie auf **OK**.

Wiederholen Sie diese Schritte, um das Register ISERIESB.MYCO.COM für die Teilnahme an Abgleichsuchoperationen und die Verwendung von Richtlinienzuordnungen zu aktivieren, wählen Sie jedoch auf der Seite **Allgemein** die Option **Abgleichsuchen mit Hilfe von Richtlinienzuordnungen für Register ISERIESB.MYCO.COM aktivieren** und dann **Richtlinienzuordnungen verwenden** aus. Klicken Sie auf **OK**.

Sie haben die EIM-Konfiguration für Register und Benutzer abgeschlossen und sollten jetzt die resultierenden Abgleiche testen, um sich zu vergewissern, dass sie wie geplant funktionieren.

## Schritt 13: 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 Richtlinienzuordnung des Standardregisters 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 iSeries Navigator den Eintrag **iSeries 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. Geben Sie die folgenden Informationen an, und klicken Sie auf **OK**, um eine Verbindung zum Domänencontroller herzustellen:
   - **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 **MyCo-EIM-Domäne**, und wählen Sie **Abgleich testen...** aus.
3. Geben Sie im Dialogfenster **Abgleich testen** Informationen an oder klicken Sie auf **Durchsuchen...**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **Test**:
   - **Quellenregister**: `MYCO.COM`
   - **Quellenbenutzer**: `jday`
   - **Zielregister**: `ISERIESA.MYCO.COM`

4. Die Ergebnisse werden im Abschnitt **Gefundener Abgleich** der Seite wie folgt angezeigt:

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

5. Klicken Sie auf **Schließen**.

Wiederholen Sie diese Schritte, wählen Sie jedoch für das Feld **Zielregister** die Option `ISERIESB.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 iSeries Navigator den Eintrag **iSeries 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. Geben Sie die folgenden Informationen an, und klicken Sie auf **OK**, um eine Verbindung zum Domänencontroller herzustellen:

   - **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 **MyCo-EIM-Domäne**, und wählen Sie **Abgleich testen...** aus.
3. Geben Sie im Dialogfenster **Abgleich testen** Informationen an oder klicken Sie auf **Durchsuchen...**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **Test**:
   - **Quellenregister**: `MYCO.COM`
   - **Quellenbenutzer**: `sjones`
   - **Zielregister**: `ISERIESA.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** die Option `ISERIESB.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 Richtlinienzuordnung für Standardregister verwendete Abgleiche testen**

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

1. Erweitern Sie im iSeries Navigator den Eintrag **iSeries 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. Geben Sie die folgenden Informationen an, und klicken Sie auf **OK**, um eine Verbindung zum Domänencontroller herzustellen:

   - **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 **MyCo-EIM-Domäne**, und wählen Sie **Abgleich testen...** aus.
3. Geben Sie im Dialogfenster **Abgleich testen** Informationen an oder klicken Sie auf **Durchsuchen...**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **Test**:
   - **Quellenregister**: `MYCO.COM`
   - **Quellenbenutzer**: `mmiller`
   - **Zielregister**: `ISERIESA.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 einzelnen für die Richtlinienzuordnung für Standardregister verwendeten Abgleiche, mit denen Ihre Benutzer dem Profil SYSUSERB auf der iSeries B zugeordnet werden, zu testen:

1. Erweitern Sie im iSeries Navigator den Eintrag **iSeries 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. Geben Sie die folgenden Informationen an, und klicken Sie auf **OK**, um eine Verbindung zum Domänencontroller herzustellen:

   - **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 **MyCo-EIM-Domäne**, und wählen Sie **Abgleich testen...** aus.
3. Geben Sie im Dialogfenster **Abgleich testen** Informationen an oder klicken Sie auf **Durchsuchen...**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **Test**:
   - **Quellenregister**: `MYCO.COM`
   - **Quellenbenutzer**: `ksmith`
   - **Zielregister**: `ISERIESB.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, lesen Sie Fehlerbehebung für EIM, um Lösungen für diese Probleme zu finden.

Sie haben die EIM-Identitätsabgleiche getestet und können jetzt iSeries Access für Windows-Anwendungen zur Verwendung der Kerberos-Authentifizierung konfigurieren.

## Schritt 14: iSeries Access für Windows-Anwendungen zur Verwendung der Kerberos-Authentifizierung konfigurieren

Basierend auf Ihren Zielen für Einzelanmeldung müssen alle Benutzer in der Auftragsannahme die Kerberos-Authentifizierung durchführen, bevor sie mit dem iSeries Navigator auf die iSeries A und die iSeries B zugreifen können. Daher müssen Sie iSeries Access für Windows zur Verwendung der Kerberos-Authentifizierung konfigurieren.

Führen Sie die folgenden Schritte durch, um iSeries Access für Windows-Anwendungen zur Verwendung der Kerberos-Authentifizierung zu konfigurieren:

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

1. Melden Sie sich an der Windows (R) 2000-Domäne an, indem Sie sich am PC anmelden.
2. Klicken Sie mit der rechten Maustaste im iSeries Navigator auf dem PC auf den Eintrag **iSeries A**, und wählen Sie **Eigenschaften** aus.
3. Wählen Sie auf der Seite **Verbindung** die Option **Kerberos-Principal-Namen verwenden, keine Anforderung** aus. So können iSeries Access für Windows-Verbindungen den Namen und das Kennwort des Kerberos-Principals für die Authentifizierung 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 iSeries Navigator, und starten Sie ihn erneut.

Wiederholen Sie diese Schritte für die iSeries B.

Sie haben iSeries Access für Windows-Anwendungen zur Verwendung der Kerberos-Authentifizierung konfiguriert und können jetzt die Umgebung für die Einzelanmeldung überprüfen.

## Schritt 15: Netzwerkauthentifizierungsservice und EIM-Konfiguration 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 iSeries Navigator den Eintrag **iSeries A**, um eine Verbindung zur iSeries A herzustellen.
2. Drücken Sie F5, um die Anzeige zu aktualisieren.
3. Suchen Sie im rechten Teilfenster die `iSeries A` in der Spalte **Name** und vergewissern Sie sich, dass das i5/OS-Benutzerprofil von John Day, `JOHND`, als entsprechender Eintrag in der Spalte **Angemeldeter Benutzer** angezeigt wird.

Aufgrund der Zuordnungen, die für die EIM-Kennung John Day definiert wurden, konnte iSeries Navigator EIM verwenden, um den Kerberos-Principal jday zum iSeries A-Benutzerprofil JOHND hinzuzufügen. Die Verbindung der iSeries Navigator-Sitzung für die iSeries A läuft jetzt unter dem Namen JOHND.

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

## Schritt 16: (Optional) Hinweise für die Phase nach der Konfiguration

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 der iSeries A und der iSeries B 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, die eine geeignetere und begrenzte Zugriffsberechtigung für EIM-Daten besitzen. Die Anzahl der zusätzlichen Benutzer, die Sie definieren, ist davon abhängig, in welchem Maße die Sicherheitsstrategie eine Trennung von Sicherheitsaufgaben und Verantwortlichkeiten für die Sicherheit vorsieht. Normalerweise werden mindestens zwei der 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. Mit diesem registrierten Namen des EIM-Administrators kann eine Verbindung zum Domänencontroller herstellt werden, wenn alle Aspekte der EIM-Domäne mit dem iSeries Navigator verwaltet werden.
- **Mindestens ein Benutzer, der alle folgenden Zugriffsberechtigungen besitzt**:
  - Kennungsadministrator
  - Registeradministrator
  - EIM-Abgleichoperation

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

**Anmerkung:** Wenn Sie diesen neuen registrierten Namen des Systembenutzers anstelle des registrierten Namens des LDAP-Administrators verwenden, müssen Sie die Eigenschaften der EIM-Konfiguration für jedes System ändern. Für dieses Szenario müssen Sie die Eigenschaften der

EIM-Konfiguration sowohl für die iSeries A als auch die iSeries B ändern. Unter Eigenschaften der EIM-Konfiguration verwalten wird erläutert, wie Sie den registrierten Namen des Systembenutzers ändern können.

## Konzepte

Der Netzwerkauthentifizierungsservice unterstützt Kerberos-Protokoll- und GSS-APIs (GSS = Generic Security Service), die die Benutzerauthentifizierung in einem Netzwerk zur Verfügung stellen. Da es zahlreiche Quellen mit Informationen zu diesen beiden Protokollen gibt, werden hier nur die grundlegenden Voraussetzungen erläutert, die sich speziell auf Ihren iSeries-Server beziehen. Definitionen der in den vorliegenden Informationen verwendeten Kerberos-Begriffe finden Sie im Abschnitt Terminologie für Netzwerkauthentifizierungsservice.

Die folgenden Abschnitte enthalten weitere Informationen über die Konzepte des Netzwerkauthentifizierungsservice:

Funktionsweise des Netzwerkauthentifizierungsservice
Es wird erläutert, wie der Netzwerkauthentifizierungsservice und die Kerberos-Authentifizierung in einem Netzwerk funktionieren.

Protokolle für Netzwerkauthentifizierungsservice
Es wird erläutert, wie das Kerberos-Protokoll gemeinsam mit GSS-APIs zur Bereitstellung von Authentifizierungs- und Sicherheitsservices eingesetzt wird. Hier finden Sie außerdem weitere Ressourcen zu diesen Protokollen.

Umgebungsvariablen für Netzwerkauthentifizierungsservice
Es wird erläutert, wie die Leistung des Netzwerkauthentifizierungsservice und der Kerberos- und GSS-APIs durch die Verwendung von Umgebungsvariablen beeinflusst werden kann.

## Terminologie für Netzwerkauthentifizierungsservice

Im Zusammenhang mit dem Netzwerkauthentifizierungsservice wird die folgende Kerberos-Terminologie verwendet:

**Weiterleitbare Tickets** Mithilfe weiterleitbarer Tickets kann ein Server die Berechtigungsnachweise des Requesters an einen anderen Service weiterleiten. Dazu muss das ursprüngliche TGT (Ticket-granting Ticket) mit der Weiterleitungsoption angefordert worden sein, und dem Server muss es erlaubt sein, Berechtigungsnachweise zu delegieren.

**Kerberos-Server oder KDC (Key Distribution Center - Instanz zur Schlüsselverteilung)** Ein Netzwerkservice, der Tickets und temporäre Sitzungsschlüssel zur Verfügung stellt. 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. Der Authentifizierungsserver stellt Ticket-granting Tickets aus, und der Ticket-granting Server stellt Service-Tickets aus. Wichtig ist, dass eine sichere Maschine als Kerberos-Server dient, da ansonsten durch unberechtigten Zugriff auf den Kerberos-Server Ihr gesamter Realm gefährdet werden könnte.

**Chiffrierschlüsseltabelle** Eine Datei auf dem Hostsystem des Service. Jeder Eintrag in der Datei enthält den Namen des Service-Principals und einen geheimen Schlüssel. Auf der iSeries wird bei der Konfiguration des Netzwerkauthentifizierungsservice eine Chiffrierschlüsseltabelle erstellt.Wenn ein Service die Authentifizierung für eine iSeries mit konfiguriertem Netzwerkauthentifizierungsservice anfordert, überprüft diese iSeries, ob die Chiffrierschlüsseltabellendatei die Berechtigungsnachweise für den betreffenden Service enthält. Um sicherzustellen, dass Benutzer und Services richtig authentifiziert werden, müssen sie sowohl auf dem Kerberos-Server als auch auf dem iSeries-Server vorhanden sein. Die Einträge werden der Schlüsseltabelle während der Endverarbeitung des Assistenten für den Netzwerkauthentifizierungsservice hinzugefügt. Sie können Einträge auch durch Eingabe des Befehls `keytab` im Qshell-Interpreter einer zeichenorientierten Schnittstelle hinzufügen.

**Anmerkung:** Dieser DNS-Name muss mit dem auf der Maschine definierten Hostnamen identisch sein. Weitere Informationen über die Zusammenarbeit von DNS und Kerberos finden Sie unter „Hinweise zur Auflösung von Hostnamen" auf Seite 95.

**Kennwortserver** Ermöglicht Clients (Principals) eine ferne Änderung ihres Kennworts auf dem Kerberos-Server. Der Kennwortserver wird normalerweise auf derselben Maschine ausgeführt wie der Kerberos-Server.

**Principal** Der Name eines Benutzers oder Services in einem Kerberos-Realm. Als Benutzer wird eine Person bezeichnet, die einen Service benutzt, um eine bestimmte Anwendung oder eine Gruppe von Betriebssystemservices zu identifizieren. Unter i5/OS wird der Service-Principal **krbsvr400** für die Identifikation des Service verwendet, der von den iSeries Access für Windows-, QFileSrv.400- und Telnet-Servern bei der Authentifizierung des Clients für die iSeries benutzt wird.

**Proxy-fähige Tickets** Ein Proxy-fähiges Ticket ist ein Ticket-granting Ticket (TGT), mit dem ein Ticket für einen Service erhältlich ist, für den andere IP-Adressen gelten als die im TGT enthaltenen. Im Unterschied zu weiterleitbaren Tickets kann vom aktuellen TGT kein neues TGT weitervermittelt werden; es können nur Service-Tickets weitervermittelt werden. Mithilfe weiterleitbarer Tickets kann die vollständige Identität (TGT) an eine andere Maschine übertragen werden, wohingegen mit Proxy-fähigen Tickets lediglich bestimmte Tickets übertragen werden können. Unter Verwendung Proxy-fähiger Tickets kann ein Service eine Task im Namen eines Principals ausführen. Der Service muss in der Lage sein, die Identität des Principals für einen bestimmten Zweck anzunehmen. Ein Proxy-fähiges Ticket teilt dem Kerberos-Server mit, dass er ein neues Ticket für eine andere Netzwerkadresse auf der Basis des ursprünglichen Ticket-granting Tickets ausstellen kann. Für Proxy-fähige Tickets ist kein Kennwort erforderlich.

**Realm** Eine Gruppe von Benutzern und Servern, für die ein bestimmter Kerberos-Server die authentifizierende Instanz darstellt.

**Realm-Vertrauensbeziehung** Das Kerberos-Protokoll durchsucht entweder die Konfigurationsdatei (z. B. **krb5.conf**), um die Realm-Vertrauensbeziehung festzustellen, oder es sucht standardmäßig innerhalb der Realm-Hierarchie nach Vertrauensbeziehungen. Durch Verwendung **sicherer Realms** im Netzwerkauthentifizierungsservice kann dieser Prozess umgangen und eine Verknüpfung zur Authentifizierung erstellt werden. Die Realm-Vertrauensbeziehung kann in Netzwerken verwendet werden, bei denen sich die Realms in unterschiedlichen Domänen befinden. Wenn ein Unternehmen beispielsweise einen Realm bei NY.MYCO.COM und einen anderen bei LA.MYCO.COM hat, kann zwischen diesen beiden Realms eine Vertrauensbeziehung aufgebaut werden. Wenn zwei Realms sich gegenseitig vertrauen, müssen die zugeordneten Kerberos-Server einen Schlüssel gemeinsam benutzen. Bevor eine Verknüpfung hergestellt werden kann, müssen die Kerberos-Server so eingerichtet werden, dass sie sich gegenseitig vertrauen.

**Erneuerbare Tickets** Manchmal möchte eine Anwendung oder ein Service über Tickets verfügen, die über einen längeren Zeitraum gültig sind. Die längere Gültigkeitsdauer erhöht aber auch die Wahrscheinlichkeit eines Diebstahls der Berechtigungsnachweise, die bis zum Verfall des Tickets gültig sind. Um dies zu verhindern und Anwendungen die Möglichkeit zu bieten, Tickets mit längerer Gültigkeitsdauer zu erhalten, werden erneuerbare Tickets verwendet. Erneuerbare Tickets haben nämlich zwei Verfallszeiten. Die erste betrifft die aktuelle Instanz des Tickets und die zweite das späteste zulässige Verfallsdatum des Tickets.

**Service-Ticket** Ein Ticket, das einen Principal für einen Service authentifiziert.

**Ticket-granting Service (TGS)** Ein vom Kerberos-Server zur Verfügung gestellter Service, der Service-Tickets ausstellt.

**Ticket-granting Ticket (TGT)** Ein Ticket, das den Zugriff auf den Ticket-granting Service auf dem Kerberos-Server ermöglicht. Ticket-granting Tickets werden dem Principal vom Kerberos-Server übergeben, nachdem der Principal eine erfolgreiche Anforderung an den Authentifizierungsserver gestellt hat. In einer Windows (R) 2000-Umgebung meldet sich ein Benutzer beim Netzwerk an, woraufhin der Kerberos-Server den Namen und das verschlüsselte Kennwort des Principals verifiziert und ein Ticket-granting Ticket an den Benutzer sendet. Von einem iSeries-Server können Benutzer ein Ticket anfordern, indem sie den Befehl kinit im Qshell-Interpreter der zeichenorientierten Schnittstelle verwenden.

## Funktionsweise des Netzwerkauthentifizierungsservice

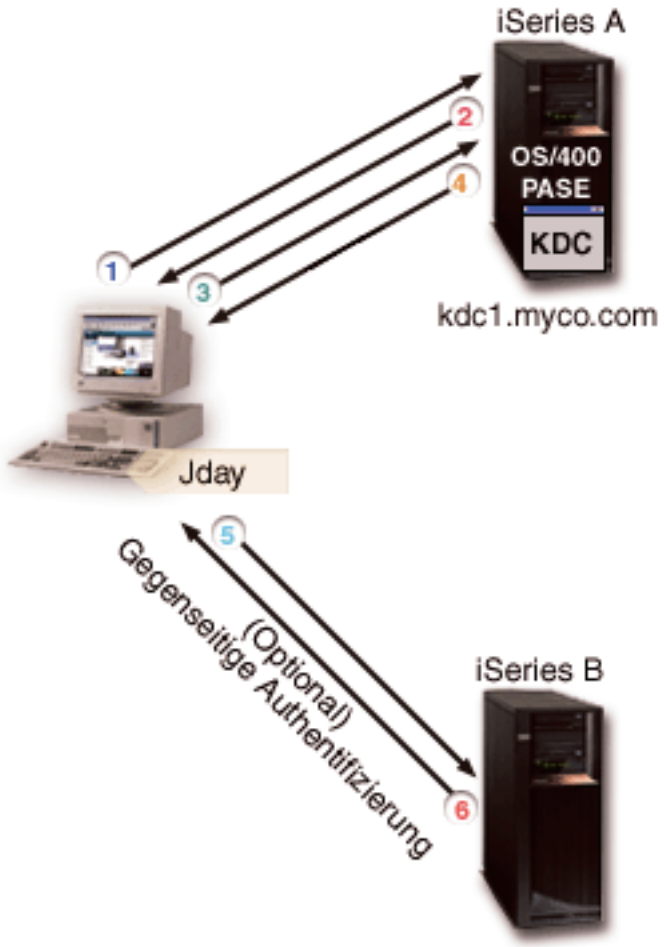
Das Kerberos-Protokoll stellt eine Authentifizierungsmethode für Benutzer und Services in Ihrem Netzwerk zur Verfügung. Als Netzwerkadministrator können Sie den Netzwerkauthentifizierungsservice so konfigurieren, dass Ihr iSeries-System Kerberos-Tickets als Authentifizierungsform anerkennt. Die iSeries und mehrere iSeries-spezifische Anwendungen fungieren als Client/Server innerhalb eines Kerberos-Netzwerks, die Tickets für die Authentifizierung von Benutzern und Services anfordern. Das Kerberos-Protokoll gibt Benutzern und Services die Möglichkeit, ihre Identität innerhalb eines Netzwerks nachzuweisen (authentifizieren), berechtigt sie jedoch nicht für Ressourcen auf diesem Netzwerk. Spezielle Berechtigungen für i5/OS-Funktionen werden nach wie vor über Benutzerprofile gesteuert, die unter i5/OS erstellt wurden.

Wenn sich ein Benutzer unter Verwendung von Kerberos authentifiziert, erhält er ein erstmaliges Ticket, das als Ticket-granting Ticket (TGT) bezeichnet wird. Der Benutzer kann anschließend mit diesem TGT ein Service-Ticket anfordern, um auf andere Services und Anwendungen auf dem Netzwerk zuzugreifen. Für eine erfolgreiche Authentifizierung muss ein Administrator die Benutzer, i5/OS-Service-Principals und Anwendungen registrieren, die das Kerberos-Protokoll auf dem Kerberos-Server verwenden. Die iSeries kann entweder als Server dienen, auf dem Principals die Authentifizierung für Services anfordern, oder sie kann als Client dienen, der Tickets für Anwendungen und Services auf dem Netzwerk anfordert. Die folgenden Grafiken zeigen den Verarbeitungsablauf in beiden Fällen.

**iSeries als Server**

Diese Grafik zeigt die Funktionsweise der Authentifizierung, wenn eine iSeries als Server in einem Kerberos-Netzwerk dient. Der auch als KDC (Key Distribution Center - Instanz zur Schlüsselverteilung) bezeichnete Kerberos-Server in i5/OS PASE stellt Tickets für den Principal jday aus.

Principal jday möchte auf eine Anwendung auf der iSeries A zugreifen. In diesem Fall wird Enterprise Identity Mapping (EIM) auf dem Server verwendet, um den Kerberos-Principal einem i5/OS-Benutzerprofil zuzuordnen. Diese Vorgehensweise gilt für alle iSeries-Serverfunktionen, die die Kerberos-Authentifizierung unterstützen, wie beispielsweise IBM @server iSeries Access für Windows.



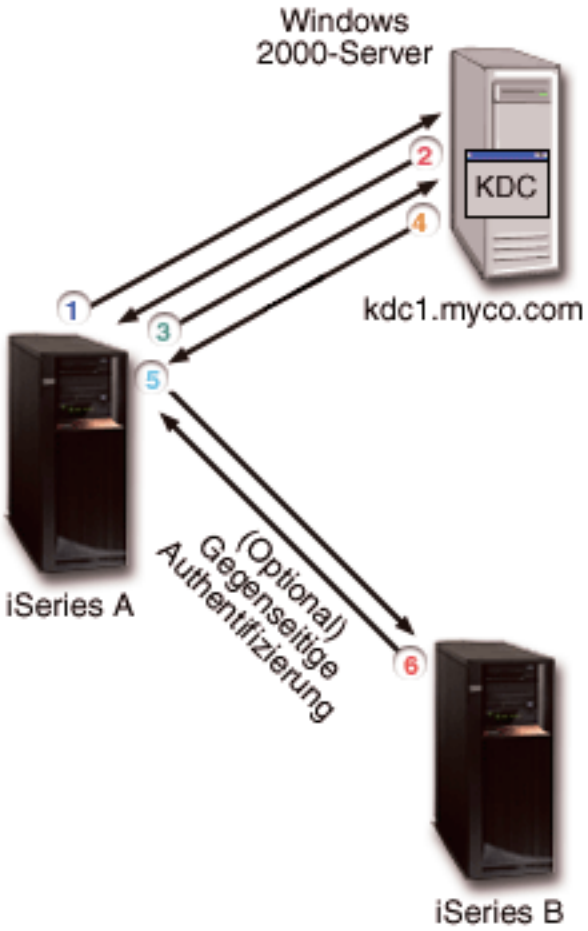

Die folgende Beschreibung gibt Ihnen eine Übersicht über die Funktionsweise des Authentifizierungsprozesses innerhalb eines Netzwerks:

1. Der Benutzer jday authentifiziert sich gegenüber dem Kerberos-Server, indem er bei der Anmeldung im Kerberos-Realm einen Principal und ein Kennwort angibt. Daraufhin wird vom Kerberos-Server ein Ticket-granting Ticket (TGT) angefordert.
2. Der Kerberos-Server prüft den Namen des Principals und das Kennwort und sendet ein TGT an jday.
3. Jday benötigt Zugriff auf eine Anwendung auf einem iSeries-Server. Die Kerberos-Clientanwendung auf dem PC von jday sendet ihr TGT an den Kerberos-Server, um ein Service-Ticket für die entsprechende Anwendung oder den Service, wie beispielsweise iSeries Navigator, anzufordern. Die Workstation des Benutzers verwaltet dessen Cache für Berechtigungsnachweise, der Tickets und andere Informationen zur Identität das Benutzers enthält. Diese Berechtigungsnachweise werden nach Bedarf aus dem Cache gelesen, und neue Berechtigungsnachweise werden hier gespeichert. Damit wird der Anwendung die Verantwortung abgenommen, ihre Berechtigungsnachweise selbst verwalten zu müssen.
4. Der Kerberos-Server antwortet mit dem Service-Ticket.
5. Die Anwendung sendet das Service-Ticket an den iSeries-Service, um den Benutzer zu authentifizieren.
6. Die Serveranwendung prüft das Ticket, indem sie die APIs für den Netzwerkauthentifizierungsservice aufruft; wahlweise kann sie zwecks gegenseitiger Authentifizierung auch eine Rückantwort an den Client senden.

7. Unter Verwendung einer EIM-Zuordnung wird der Kerberos-Principal anschließend dem i5/OS-Benutzerprofil zugeordnet.

**iSeries als Client**

Diese Grafik zeigt die Funktionsweise der Authentifizierung, wenn eine iSeries als Client in einem Kerberos-Netzwerk dient. In dieser Grafik stellt der Kerberos-Server, der sich auf dem Windows 2000-Server befindet, Tickets für den Benutzer aus, der sich für Kerberos authentifiziert hat. Die iSeries A kann für andere Services authentifiziert werden. In diesem Beispiel wird EIM auf der iSeries B verwendet, um den Kerberos-Principal einem iSeries-Benutzerprofil zuzuordnen. Diese Vorgehensweise gilt für alle iSeries-Serverfunktionen, die die Kerberos-Authentifizierung unterstützen, wie beispielsweise QFileSvr.400.




Die folgende Beschreibung gibt Ihnen eine Übersicht über die Funktionsweise des Authentifizierungsprozesses innerhalb eines Netzwerks:

1. Der Principal jday meldet sich bei der iSeries A an und fordert ein Ticket-granting Ticket an, indem er den Befehl kinit im Qshell Interpreter ausführt. Die iSeries sendet diese Anforderung an den Kerberos-Server.
2. Der Kerberos-Server prüft den Namen des Principals und das Kennwort und sendet ein Ticket an jday.
3. Jday benötigt Zugriff auf eine Anwendung auf der iSeries B. Durch Aufrufen der APIs für den Netzwerkauthentifizierungsservice sendet die Anwendung das TGT von jday an den Kerberos-Server, um ein Service-Ticket für die jeweilige Anwendung oder den Service anzufordern. Die lokale Maschine des Principals verwaltet einen Cache für Berechtigungsnachweise, der Tickets,

Sitzungsschlüssel und andere Informationen zur Identität das Benutzers enthält. Diese Berechtigungsnachweise werden nach Bedarf aus dem Cache gelesen, und neue Berechtigungsnachweise werden hier gespeichert. Damit wird der Anwendung die Verantwortung abgenommen, ihre Berechtigungsnachweise selbst verwalten zu müssen.

4. Der Kerberos-Server antwortet mit dem Service-Ticket. **Anmerkungen:** Dem Kerberos-Server muss ein Principal für die iSeries B hinzugefügt werden, und der Netzwerkauthentifizierungsservice muss ebenfalls auf der iSeries B konfiguriert sein.
5. Die Anwendung sendet das Service-Ticket an den iSeries-Service, um den Benutzer zu authentifizieren.
6. Die Serveranwendung prüft das Ticket, indem sie die APIs für den Netzwerkauthentifizierungsservice aufruft; wahlweise kann sie zwecks gegenseitiger Authentifizierung auch eine Rückantwort an den Client senden.
7. Unter Verwendung einer EIM-Zuordnung wird der Kerberos-Principal anschließend dem i5/OS-Benutzerprofil zugeordnet.

# Protokolle für Netzwerkauthentifizierungsservice

Der Netzwerkauthentifizierungsservice verwendet das Kerberos-Protokoll gemeinsam mit GSS-APIs (GSS = Generic Security Services) zur Bereitstellung von Authentifizierungs- und Sicherheitsservices. Die folgenden Abschnitte enthalten eine allgemeine Beschreibung dieser Protokolle und ihrer Verwendungsweise auf der iSeries. Vollständige Informationen über diese Standards erhalten Sie über die Links auf die zugehörigen Requests for Comments und andere externe Quellen.

## Kerberos-Protokoll

Das Kerberos-Protokoll bietet die Authentifizierung durch eine dritte Partei, wobei der Benutzer seine Identität gegenüber einem zentralen Server nachweist, der als Kerberos-Server oder KDC (Key Distribution Center - Instanz zur Schlüsselverteilung) bezeichnet wird und Tickets für den Benutzer ausstellt. Anhand dieser Tickets kann der Benutzer dann seine Identität auf dem Netzwerk nachweisen. Durch das Ticket wird die Notwendigkeit mehrerer Anmeldungen an verschiedenen Systemen hinfällig. Die von der iSeries unterstützten Anwendungsprogrammierschnittstellen (APIs) für den Netzwerkauthentifizierungsservice wurden am Massachusetts Institute of Technology entwickelt und sind zum bestehenden Branchenstandard für die Verwendung des Kerberos-Protokolls geworden.

### Voraussetzungen für die Sicherheitsumgebung

Das Kerberos-Protokoll geht davon aus, dass der gesamte Datenaustausch in einer Umgebung stattfindet, in der Pakete nach Belieben eingefügt, geändert oder abgefangen werden können. Verwenden Sie Kerberos als eine Schicht eines umfassenden Sicherheitsplans. Obwohl Sie mit dem Kerberos-Protokoll Benutzer und Anwendungen im gesamten Netzwerk authentifizieren können, müssen Sie sich auch der Grenzen dieses Protokolls bewusst sein, wenn Sie Ihre Ziele hinsichtlich der Netzwerksicherheit definieren:

- Das Kerberos-Protokoll schützt nicht vor Denial-of-Service-Attacken. Das Protokoll enthält Stellen, an denen ein Eindringling verhindern kann, dass eine Anwendung die korrekten Authentifizierungsschritte ausführt. Das Aufdecken und Abwehren solcher Attacken überlässt man am besten Administratoren und Benutzern.
- Die gemeinsame Benutzung und der Diebstahl von Schlüsseln kann Attacken in Form betrügerischen Auftretens ermöglichen. Wenn es Eindringlingen gelingt, sich den Schlüssel eines Principals anzueignen, können sie sich als dieser Benutzer oder Service ausgeben. Um dieses Sicherheitsrisiko zu minimieren, untersagen Sie Benutzern die gemeinsame Benutzung ihrer Schlüssel und dokumentieren Sie diese Richtlinie in Ihren Sicherheitsbestimmungen.
- Das Kerberos-Protokoll schützt nicht vor Angriffen auf die typischen Schwachstellen von Kennwörtern, wie beispielsweise die Möglichkeit des Erratens. Wenn ein Benutzer ein leicht zu erratendes Kennwort wählt, kann ein Angreifer erfolgreich eine offline durchgeführte Attacke auf das

Wörterverzeichnis starten, indem er wiederholt versucht, Nachrichten zu entschlüsseln, die mit einem Schlüssel codiert sind, der vom Kennwort des Benutzers abgeleitet ist.

**Kerberos-Quellen**

RFCs (Requests for Comments) sind schriftlich niedergelegte Definitionen von Protokollstandards und vorgesehenen Standards für das Internet. Die folgenden RFCs können zum besseren Verständnis des Kerberos-Protokolls beitragen:

**RFC 1510**
RFC 1510: The Kerberos Network Authentication Service (V5) enthält die formale IETF-Definition (IETF = Engineering Task Force) des Kerberos Network Authentication Service (V5). Sie können die genannten RFCs mithilfe der RFC-Indexsuchmaschine auf der Website RFC Editor anzeigen. Suchen Sie nach der gewünschten RFC-Nummer. Die Ergebnisanzeige der Suchmaschine enthält den entsprechenden RFC-Titel mit Autor, Datum und Status.

**Kerberos: The Network Authentication Protocol (V5)**
Die vom Massachusetts Institute of Technology herausgegebene offizielle Dokumentation des Kerberos-Protokolls stellt Programmierinformationen zur Verfügung und beschreibt die Protokollfunktionen.

## Generic Security Services (GSS)-APIs

Generic Security Service Application Programmable Interfaces (GSS-APIs) stellen generische Sicherheitsservices zur Verfügung und werden von einer Reihe von Sicherheitstechnologien wie beispielsweise dem Kerberos-Protokoll unterstützt. Dadurch können GSS-Anwendungen in verschiedene Umgebungen portiert werden. Aus diesem Grund wird empfohlen, diese APIs anstelle der Kerberos-APIs zu verwenden. Sie können Anwendungen, die GSS-APIs verwenden, erstellen, um mit anderen Anwendungen und Clients im selben Netzwerk zu kommunizieren. Jede der miteinander kommunizierenden Anwendungen spielt bei diesem Austausch eine Rolle. Mit GSS-APIs können Anwendungen die folgenden Operationen durchführen:

- Die Benutzer-ID einer anderen Anwendung feststellen.
- Zugriffsberechtigungen an andere Anwendungen delegieren.
- Sicherheitsservices, wie beispielsweise Vertraulichkeit und Integrität, auf Nachrichtenbasis anwenden.

**GSS-API-Quellen**

RFCs (Requests for Comments) sind schriftlich niedergelegte Definitionen von Protokollstandards und vorgesehenen Standards für das Internet. Die folgenden RFCs können zum besseren Verständnis der GSS-APIs beitragen:

**RFC 2743**
RFC 2743: Generic Security Service Application Program Interface Version 2, Update 1, enthält die formale IETF-Definition (IETF = Engineering Task Force) von GSS-APIs.

**RFC 1509**
RFC 1509: Generic Security Service API: C-bindings enthält die formale IETF-Definition von GSS-APIs.

**RFC 1964**
RFC 1964: The Kerberos Version 5 GSS API Mechanism enthält die IETF-Definitionen von Kerberos Version 5 und GSS-API-Spezifikationen.

Sie können die genannten RFCs mithilfe der RFC-Indexsuchmaschine auf der Website RFC Editor anzeigen. Suchen Sie nach der gewünschten RFC-Nummer. Die Ergebnisanzeige der Suchmaschine enthält den entsprechenden RFC-Titel mit Autor, Datum und Status.

## Umgebungsvariablen für Netzwerkauthentifizierungsservice

Im Netzwerkauthentifizierungsservice können Sie mithilfe von Umgebungsvariablen die Leistung der GSS-APIs und der Kerberos-Protokoll-APIs beeinflussen. Sie können Umgebungsvariablen verwenden, um die Konfiguration zu ändern und den Netzwerkauthentifizierungsservice auf Ihrem Netzwerk zu verwalten. i5/OS unterstützt mehrere Verwendungsmöglichkeiten von Umgebungsvariablen.

Die Umgebung kann mit CL-Befehlen, C-APIs oder Qshell-Befehlen geändert werden:

**CL-Befehle**

- ADDENVVAR
- CHGENVVAR
- RMVENVVAR
- WRKENVVAR

Ein Beispiel für den Einsatz von Umgebungsvariablen mit dem CL-Befehl ADDENVVAR finden Sie unter „API-Trace-Tool" auf Seite 145. Mit dieser Gruppe von Umgebungsvariablen können Sie eine Protokolldatei erstellen, in der alle Kerberos- und GSS-API-Aufrufe aufgezeichnet werden. Mit dem API-Trace-Tool können Sie kompliziertere Probleme, die im Zusammenhang mit den Kerberos-fähigen Anwendungen auftreten, Probleme, die bei der Konfiguration des Netzwerkauthentifizierungsservice und Probleme, die bei Anforderungen von Kerberos-Tickets auftreten können, beheben.

**C-APIs**

- getenv()
- putenv()

Beschreibungen und Beispiele dieser APIs finden Sie in den Anmerkungen zur Verwendung der APIs getenv() und putenv().

**Qshell-Befehle**

- export -s env_var_name=Wert

Außerdem können Sie eine Umgebungsvariablendatei (envar-Datei) definieren, die Einträge im **Format** Umgebungsvariable=Wert enthält. Alle über die Qshell-Umgebung oder mit den CL-Befehlen definierten Variablen überschreiben die entsprechenden Variablen in der envar-Datei. Mit der Umgebungsvariablen _EUV_ENVAR_FILE kann die Adresse der Datei angegeben werden, die diese Einträge enthält.

**_EUV_ENVAR_FILE**

Der Name der Datei, die Definitionen von Umgebungsvariablen enthält. Wird diese Variable nicht angegeben, wird standardmäßig die envar-Datei verwendet, die sich im Ausgangsverzeichnis (Umgebungsvariable _EUV_HOME oder HOME) befindet.

Jede Zeile der Datei besteht aus dem Variablennamen, gefolgt von einem Gleichheitszeichen (=), auf das wiederum der Variablenwert ohne Leerzeichen oder sonstige Interpunktion folgt. Als Variablenwert gilt alles, was hinter dem Gleichheitszeichen bis zum Zeilenende steht (einschließlich eingebetteter und abschließender Leerzeichen). Zeilen, die mit einem Nummernzeichen (#) beginnen, gelten als Kommentarzeilen. Eine Zeile kann durch einen umgekehrten Schrägstrich (\) am Zeilenende fortgesetzt werden. Auf den umgekehrten Schrägstrich darf kein abschließendes Leerzeichen folgen. `_EUV_` muss in Spalte 1 beginnen.

Umgebungsvariablen werden erst gesetzt, wenn eine Funktion innerhalb der Sicherheitslaufzeit zum ersten Mal aufgerufen wird. Daher bietet sich diese Datei hauptsächlich an, um Umgebungsvariablen zu setzen, die von Funktionen innerhalb der Sicherheitslaufzeit verwendet werden; mit der Datei können aber auch Umgebungsvariablen gesetzt werden, die von der Anwendung verwendet werden. In diesem Fall sollte sich die Anwendung erst auf die Werte der Umgebungsvariablen verlassen, nachdem die Sicherheitslaufzeit initialisiert wurde. Das Benutzerprofil, unter

dem dieses Programm läuft, muss die Berechtigung *X für jedes vor dieser Datei stehende Verzeichnis im Pfad und die Berechtigung *R für diese Datei selbst besitzen.

**_EUV_HOME und HOME**
Das Ausgangsverzeichnis der Sicherheitslaufzeit nimmt den Wert der Umgebungsvariablen _EUV-_HOME an. Wird diese Variable nicht angegeben, wird das Ausgangsverzeichnis mit der Variablen HOME festgelegt. Wird keine der Umgebungsvariablen angegeben, wird das Ausgangsverzeichnis verwendet, das in dem momentan aktiven Benutzerprofil konfiguriert ist. Wenn kein Ausgangsverzeichnis vorhanden ist, wird das aktuelle Arbeitsverzeichnis benutzt. Geben Sie als allgemeine Zugriffsberechtigung für dieses Verzeichnis nur *EXCLUDE oder *R an.

**_EUV_SEC_KRB5CCNAME_FILE**
Der Name der Datei, mit der der Kerberos-Standardcache für Berechtigungsnachweise gesucht wird. Wird diese Variable nicht angegeben, wird standardmäßig die Datei krb5ccname im Ausgangsverzeichnis für die Sicherheitslaufzeit verwendet. Das aktive Benutzerprofil muss die Berechtigung *X für jedes Verzeichnis im Pfadnamen besitzen, das vor dieser Datei steht. Wenn die Datei noch nicht vorhanden ist, muss das aktive Benutzerprofil die Berechtigung *WX für das Parentverzeichnis besitzen, in dem diese Datei enthalten ist. Der Benutzer muss sicherstellen, dass die allgemeine Zugriffsberechtigung für das Parentverzeichnis eingeschränkt wird, um Benutzer mit betrügerischer Absicht daran zu hindern, die verwendete Cachedatei für Berechtigungsnachweise zu ändern.

**_EUV_SVC_MSG_LOGGING**
Das Ziel der Nachrichtenprotokollierung. Gültige Werte sind:

**NO_LOGGING**
Alle Nachrichten werden unterdrückt. Dies ist der Standardwert.

**STDOUT_LOGGING**
Alle Nachrichten (Informations- und Fehlernachrichten) werden in stdout, Fehlernachrichten in stderr aufgezeichnet.

**STDERR_LOGGING**
Informationsnachrichten werden in stdout und Fehlernachrichten in stderr aufgezeichnet.

**_EUV_SVC_MSG_LEVEL**
Die Nachrichtenstufe, die für die Protokollierung ausschlaggebend ist. Nachrichten, die diese Bedingung nicht erfüllen, werden unterdrückt. Standardmäßig werden alle Nachrichten protokolliert. Gültige Werte sind:

**FATAL**
Es werden nur Nachrichten zu nicht behebbaren Fehlern protokolliert.

**ERROR**
Es werden nur Nachrichten zu nicht behebbaren Fehlern und Fehlernachrichten protokolliert.

**USER** Es werden nur Nachrichten zu nicht behebbaren Fehlern, Fehlernachrichten und Benutzernachrichten protokolliert.

**WARNING**
Es werden nur Nachrichten zu nicht behebbaren Fehlern, Fehlernachrichten, Benutzernachrichten und Warnungen protokolliert.

**NOTICE**
Es werden nur Nachrichten zu nicht behebbaren Fehlern, Fehlernachrichten, Benutzernachrichten, Warnungen und Hinweisnachrichten protokolliert.

**VERBOSE**
Alle Nachrichten werden protokolliert.

**_EUV_SVC_STDOUT_FILENAME**
Der vollständig qualifizierte Name der Datei für Standardausgabenachrichten. Wenn diese

Umgebungsvariable nicht definiert wird, werden Nachrichten in stdout aufgezeichnet. Das aktive Benutzerprofil muss die Berechtigung *X für jedes im Pfad vor dieser Datei stehende Verzeichnis und die Berechtigung *WX für das Parentverzeichnis besitzen, in dem diese Datei enthalten ist.

**_EUV_SVC_STDERR_FILENAME**
Der vollständig qualifizierte Name der Datei für Standardfehlernachrichten. Wenn diese Umgebungsvariable nicht definiert wird, werden Nachrichten in stderr aufgezeichnet. Das aktive Benutzerprofil muss die Berechtigung *X für jedes im Pfad vor dieser Datei stehende Verzeichnis und die Berechtigung *WX für das Parentverzeichnis besitzen, in dem diese Datei enthalten ist.

**_EUV_SVC_DBG_MSG_LOGGING**
Gibt an, ob Debugnachrichten generiert werden. Standardmäßig werden Debugnachrichten unterdrückt. Die Protokollierung von Debugnachrichten sollte nur aktiviert werden, wenn sie vom IBM-Service angefordert wird, denn sie kann die Leistung erheblich beeinträchtigen.Gültige Werte sind:

- 0 Debugnachrichten unterdrücken
- 1 Debugnachrichten aufzeichnen

**_EUV_SVC_DBG**

Die Unterkomponenten und Stufen für die Debugnachrichten. Debugnachrichten für eine bestimmte Unterkomponente werden nur protokolliert, wenn die Unterkomponente in die _EUV_SVC_DBG-Liste aufgenommen wird und die Nachrichtenstufe der angegebenen Stufe entspricht oder höher als diese ist. Verwenden Sie einen Stern (*), um alle Unterkomponenten anzugeben.

Die Einträge in der Liste der Unterkomponenten besteht aus dem Namen der jeweiligen Unterkomponente gefolgt von einem Punkt und der Debugstufe. Sie können mehrere durch Komma voneinander getrennte Unterkomponenten angeben. Beispiel: _EUV_SVC_DBG=*.1,KRB_CCACHE.8 aktiviert Debugstufe 1 für alle Unterkomponenten und Debugstufe 8 für die Unterkomponente KRB_CCACHE. Es können die folgenden Unterkomponenten angegeben werden:

- KRB_API
- KRB_GENERAL
- KRB_CCACHE
- KRB_RCACHE
- KRB_CRYPTO
- KRB_GSSAPI
- KRB_KEYTAB
- KRB_LIB
- KRB_ASN1
- KRB_OS
- KRB_KDC
- KRB_KDB
- KRB_KUT

**_EUV_SVC_DBG_FILENAME**
Der vollständig qualifizierte Name der Datei für Debugnachrichten. Wenn diese Umgebungsvariable nicht definiert wird, werden Debugnachrichten in der Datei aufgezeichnet, die von _EUV_SVC_STDOUT_FILENAME angegeben wird. Wird _EUV_SVC_STDOUT_FILENAME nicht angegeben, werden Debugnachrichten in stdout aufgezeichnet. Das aktive Benutzerprofil muss die Berechtigung *X für jedes im Pfad vor dieser Datei stehende Verzeichnis und die Berechtigung *WX für das Parentverzeichnis besitzen, in dem diese Datei enthalten ist.

**KRB5_CONFIG**
Eine oder mehrere durch Doppelpunkt voneinander getrennte Konfigurationsdateien. Die

Standardkonfigurationsdatei ist /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf. Das aktive Benutzerprofil muss die Berechtigung *X für jedes im Pfad vor dieser Datei stehende Verzeichnis und die Berechtigung *R für die Konfigurationsdateien besitzen.

**KRB5CCNAME**
Der Standardname der Cachedatei für Berechtigungsnachweise, der im Format Typ:Name angegeben wird. Die unterstützten Dateitypen sind FILE und MEMORY. Standardmäßig erfolgt das Caching FILE-basierter Berechtigungsnachweise im Verzeichnis /QIBM/UserData/OS400/NetworkAuthentication/creds. Wenn der Standardwert verwendet wird, ist keine Definition der Berechtigung erforderlich. Wenn eine FILE-basierte Cachedatei für Berechtigungsnachweise angegeben wird, muss das aktive Benutzerprofil die Berechtigung *X für jedes Verzeichnis im Pfad besitzen. Beim erstmaligen Erstellen der Cachedatei benötigt das aktive Benutzerprofil die Berechtigung *WX für das Parentverzeichnis und die Berechtigung *RW für die Cachedatei. Zum Löschen der Cachedatei benötigt das aktive Benutzerprofil die Berechtigung *OBJEXIST.

**KRB5_KTNAME**
Der Standardname für die Chiffrierschlüsseltabelle. Wird diese Umgebungsvariable nicht angegeben, wird die vom Eintrag default_keytab_name in der Konfigurationsdatei angegebene Datei verwendet. Wenn der Konfigurationseintrag nicht angegeben wird, gilt die Standarddatei /QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab. Das aktive Benutzerprofil muss die Berechtigung *X für jedes Verzeichnis im Pfad besitzen. Beim Erstellen der Datei benötigt es außerdem die Berechtigung *WX für das Parentverzeichnis. Zum Aktualisieren der Datei benötigt das aktive Benutzerprofil die Berechtigung *RW. Spezifische Berechtigungen werden unter den Qshell-Befehlen und den Laufzeit-APIs dokumentiert.

**KRB5RCACHETYPE**
Der Standardtyp für den Replay-Cache. Er nimmt standardmäßig den Wert dfl an

**KRB5RCACHENAME**
Der Standardname für den Replay-Cache. Erfolgt keine Angabe, generiert die Kerberos-Ausführungszeit einen Namen.

**KRB5RCACHEDIR**
Das Standardverzeichnis für den Replay-Cache. Es nimmt standardmäßig den Wert /QIBM/UserData/OS400/NetworkAuthentication/replay an

## Netzwerkauthentifizierungsservice planen

Bevor Sie den Netzwerkauthentifizierungsservice oder eine Kerberos-Lösung auf Ihrem Netzwerk implementieren können, müssen Sie die erforderlichen Planungsaufgaben durchführen. Zunächst müssen Sie die entsprechenden Informationen über die Systeme und Benutzer auf Ihrem Netzwerk zusammenstellen. Es stehen Ihnen mehrere Planungsarbeitsblätter zur Verfügung, die Ihnen bei der Konfiguration des Netzwerkauthentifizierungsservice in Ihrem Netzwerk helfen sollen.

**Anmerkung:** Es gibt zahlreiche unterschiedliche Kerberos-Authentifizierungslösungen, die in Ihrem Unternehmen eingesetzt werden können. Die nachfolgenden Informationen beziehen sich hauptsächlich auf die Planung einer iSeries-Implementierung und auf die Dinge, die beim Netzwerkauthentifizierungsservice zu beachten sind, wenn ein Kerberos-Server verwendet wird, der im Microsoft Windows Active Directory oder in i5/OS PASE konfiguriert wurde.

Informationen über die Konfiguration eines Kerberos-Servers im Microsoft Windows Active Directory finden Sie unter Microsoft Windows 2000 Help 

Die Kerberos-Authentifizierung wird von den nachfolgend aufgeführten IBM @server unterstützt. Informationen über plattformspezifische Kerberos-Implementierungen finden Sie in den folgenden Quellen:

- **pSeries**

- IBM Network Authentication Service Version 1.3 for AIX: Administrator's and User's Guide
- IBM Network Authentication Service Version 1.3 for AIX: Application Development Reference

**Anmerkung:** Die genannten Dokumentationen finden Sie auf der CD: AIX 5L Expansion Pack and Bonus Pack.

- **zSeries**
  - z/OS Security Server Network Authentication Service

Die folgenden Tasks unterstützen Sie bei der Planung des Netzwerkauthentifizierungsservice:

1. „Kerberos-Server planen"
2. „Realms planen" auf Seite 92
3. „Principal-Namen planen" auf Seite 93
4. „Hinweise zur Auflösung von Hostnamen" auf Seite 95
5. „Planungsarbeitsblätter für Netzwerkauthentifizierungsservice" auf Seite 101

## Kerberos-Server planen

Ein Kerberos-Server, der auch als KDC (Key Distribution Center - Instanz zur Schlüsselverwaltung) bezeichnet wird, unterhält eine Datenbank mit Principals und deren Kennwörtern. Ein Kerberos-Server besteht aus dem Authentifizierungsserver und dem Ticket-granting Server. Wenn sich ein Principal bei einem Kerberos-Netzwerk anmeldet, prüft der Authentifizierungsserver den Principal und stellt ihm ein Ticket-granting Ticket aus. Wenn Sie planen, die Kerberos-Authentifizierung zu verwenden, müssen Sie entscheiden, welches System als Kerberos-Server konfiguriert werden soll.

**Anmerkung:** Die Informationen über den Netzwerkauthentifizierungsservice betreffen in erster Linie Kerberos-Server, die entweder in i5/OS PASE oder Windows 2000-Server aktiv sind. Wenn nicht anders angegeben, wird bei den meisten Szenarios und Beispielen vorausgesetzt, dass ein Windows 2000-Server als Kerberos-Server definiert wurde. Wenn Sie ein anderes Betriebssystem oder Anwendungen eines anderen Herstellers für die Kerberos-Authentifizierung benutzen, ziehen Sie die entsprechende Dokumentation zu Rate.

Die folgende Liste enthält nähere Angaben zur Kerberos-Serverunterstützung der drei wichtigsten Betriebssysteme:

**Microsoft Windows 2000 und Windows Server 2003**
Sowohl Microsoft Windows 2000 als auch Windows Server 2003 unterstützen die Kerberos-Authentifizierung als Standardsicherheitsmechanismus. Wenn Administratoren Benutzer und Services über Microsoft Windows Active Directory hinzufügen, erstellen sie eigentlich Kerberos-Principals für diese Benutzer und Services. Wenn sich in Ihrem Netzwerk ein Windows 2000- oder 2003-Server befindet, dann ist bereits ein Kerberos-Server integriert. Informationen über die Verwendungsweise der Kerberos-Authentifizierung auf Microsoft Windows-Servern finden Sie unter Microsoft Windows Help.

**AIX und i5/OS PASE**
Sowohl AIX als auch i5/OS PASE unterstützen einen Kerberos-Server über den Befehl kadmin. Administratoren müssen die PASE-Umgebung aufrufen (durch Eingabe von `call QP2TERM`), um den PASE-Kerberos-Server zu konfigurieren und zu verwalten. i5/OS PASE stellt eine Laufzeitumgebung für AIX-Anwendungen zur Verfügung, wie beispielsweise einen Kerberos-Server. Die folgenden Dokumentationen können Ihnen bei der Konfiguration und Verwaltung eines Kerberos-Servers in AIX helfen.

- IBM Network Authentication Service Version 1.3 for AIX: Administrator's and User's Guide
- IBM Network Authentication Service Version 1.3 for AIX: Application Development Reference

**Anmerkung:** Diese Dokumentation finden Sie auf der CD: AIX 5L Expansion Pack and Bonus Pack. 

**z/OS** Security Server Network Authentication Service für z/OS ist das IBM z/OS-Programm, das auf Kerberos Version 5 basiert. Network Authentication Service für z/OS stellt Kerberos-Sicherheitsservices zur Verfügung; ein Middlewareprogramm ist dafür nicht erforderlich. Diese Services unterstützen einen nativen Kerberos-Server. z/OS Security Server Network Authentication Service Administration  enthält nähere Informationen über die Konfiguration und Verwaltung eines z/OS-Kerberos-Servers.

Unabhängig davon, welches Betriebssystem den Kerberos-Server zur Verfügung stellt, müssen Sie die Server-Ports für den Kerberos-Server bestimmen, den Zugriffsschutz für den Kerberos-Server bereitstellen und sicherstellen, dass die Systemzeiten von Clients und Kerberos-Server synchronisiert sind.

**Server-Ports bestimmen**
Der Netzwerkauthentifizierungsservice verwendet standardmäßig Port 88 für den Kerberos-Server. In den Konfigurationsdateien des Kerberos-Servers können aber auch andere Ports angegeben werden. Verifizieren Sie die Portnummer in den Kerberos-Konfigurationsdateien auf dem Kerberos-Server.

**Zugriffsschutz für Kerberos-Server bereitstellen**
Der Kerberos-Server muss sich auf einem sicheren dedizierten System befinden, um sicherzugehen, dass kein Unbefugter auf die Datenbank mit den Principals und Kennwörtern zugreift. Benutzer sollten nur begrenzten Zugriff auf den Kerberos-Server haben. Wenn das System, auf dem sich der Kerberos-Server befindet, außerdem noch für andere Zwecke verwendet wird (z. B. als Web- oder FTP-Server), könnte jemand Sicherheitslücken in diesen Anwendungen ausnutzen, um Zugriff auf die Datenbank zu erlangen, die auf dem Kerberos-Server gespeichert ist. Für einen Kerberos-Server in Microsoft Windows Active Directory kann wahlweise ein Kennwortserver konfiguriert werden, mit dessen Hilfe Principals ihre eigenen Kennwörter, die auf dem Kerberos-Server gespeichert sind, verwalten und aktualisieren können. Wenn Sie einen Kerberos-Server in i5/OS PASE konfiguriert haben und die iSeries nicht für die Kerberos-Authentifizierung dedizieren können, sollten Sie sich vergewissern, dass nur Ihr Administrator Zugriff auf die Kerberos-Konfiguration hat.

**Systemzeiten synchronisieren**
Die Kerberos-Authentifizierung setzt voraus, dass die Systemzeiten synchronisiert sind. Kerberos weist alle Authentifizierungsanforderungen von einem System oder Client zurück, dessen Systemzeit nicht innerhalb der angegebenen maximalen Zeitabweichung des Kerberos-Servers liegt. Da jedes Ticket die Uhrzeit beinhaltet, zu der es an einen Principal gesendet wurde, können Hacker ein und dasselbe Ticket nicht zu einem späteren Zeitpunkt erneut senden, um sich auf diese Weise unbefugt für das Netzwerk zu authentifizieren. Das iSeries-System weist Tickets von einem Kerberos-Server ebenfalls zurück, wenn sich dessen Uhrzeit nicht innerhalb der maximalen Zeitabweichung befindet, die bei der Konfiguration des Netzwerkauthentifizierungsservice festgelegt wurde. Der Standardwert für die maximale Zeitabweichung beträgt 300 Sekunden (fünf Minuten). Bei der Konfiguration des Netzwerkauthentifizierungsservice wird die maximale Zeitabweichung auf diesen Standardwert gesetzt; wenn nötig, kann dieser Wert jedoch geändert werden. Es ist nicht empfehlenswert den Wert auf mehr als 300 Sekunden zu erhöhen. Nähere Informationen über das Arbeiten mit Systemzeiten finden Sie unter Systemzeiten synchronisieren.

*Tabelle 19. Beispiel eines Planungsarbeitsblatts für Kerberos-Server.* Dieses Planungsarbeitsblatt ist ein Beispiel dafür, wie ein Administrator den Kerberos-Server für ein Netzwerk geplant haben könnte.

| Fragen | Antworten |
|---|---|
| Unter welchem Betriebssystem soll der Kerberos-Server konfiguriert werden?<br>• Windows (R) 2000-Server<br>• Windows (R) Server 2003<br>• AIX Server<br>• i5/OS PASE (ab V5R3)<br>• zSeries | i5/OS PASE |
| Wie lautet der vollständig qualifizierte Domänenname für den Kerberos-Server? | iseriesa.myco.com |
| Sind die Systemzeiten der PCs und Systeme, die mit dem Kerberos-Server verbunden sind, synchronisiert? Wie hoch ist die maximale Zeitabweichung? | Ja 300 Sekunden |

## Realms planen

Im Kerberos-Protokoll bestehen Realms aus mehreren Maschinen und Services, die einen einzigen Authentifizierungsserver verwenden, der als Kerberos-Server oder KDC (Key Distribution Center - Instanz zur Schlüsselverteilung) bezeichnet wird. Realms werden einzeln verwaltet. Die Anwendungen und Services innerhalb eines Realms dienen normalerweise dem gleichen Verwendungszweck. Die Beantwortung der folgenden allgemeinen Fragen kann Ihnen bei der Planung von Realms in Ihrem Unternehmen helfen:

**Wie groß ist meine derzeitige Umgebung?**
Die Größe Ihrer Umgebung bestimmt die Anzahl der benötigten Realms. In einem größeren Unternehmen können Sie die Einrichtung mehrerer Realms in Betracht ziehen, die auf Organisationseinheiten oder die Verwendungsweise bestimmter Systeme innerhalb des Unternehmens basieren. Sie können beispielsweise Realms für verschiedene Abteilungen in Ihrem Unternehmen einrichten, wie etwa die Personalabteilung, den Kundenservice oder den Versand. Sie können außerdem Realms für eine Gruppe von Maschinen oder Services erstellen, die vergleichbare Funktionen ausführen. Kleinere Unternehmen benötigen normalerweise nur einen oder zwei Realms.

**Welches Wachstum erwarte ich für meine Umgebung?**
Wenn Ihre Planung ein rasches Anwachsen des Unternehmens vorsieht, könnten Sie mehrere Realms einrichten, die kleinere Organisationseinheiten innerhalb Ihres Unternehmens repräsentieren. Wenn Sie ein geringeres Wachstum erwarten, können Sie nur ein oder zwei Realms definieren, die auf der derzeitigen Unternehmensgröße basieren.

**Wie viele Administratoren werden für die Verwaltung dieser Realms benötigt?**
Unabhängig von der Größe Ihres Unternehmens müssen Sie sicherstellen, dass Sie über genügend geschultes Personal für die Einrichtung und Verwaltung der benötigten Realms verfügen.

## Realms benennen

Entsprechend der Konventionen des Kerberos-Protokolls stimmen Realm-Namen mit dem Domänennamen überein, werden jedoch normalerweise in Großbuchstaben angegeben, wie beispielsweise MYCO-.COM. In Netzwerken mit mehreren Realms können Sie einen Realm-Namen erstellen, der einen beschreibenden Namen und den Domänennamen in Großbuchstaben beinhaltet. Beispiel: Sie könnten die beiden Realms HR.MYCO.COM und SHIPPING.MYCO.COM eingerichtet haben, die jeweils eine bestimmte Abteilung in Ihrem Unternehmen repräsentieren.

Die Verwendung von Großbuchstaben ist nicht immer erforderlich, doch bei einigen Kerberos-Implementationen ist die Beachtung dieser Konvention zwingend. So sind beispielsweise für Realm-Namen in einem Microsoft Windows Active Directory Großbuchstaben zwingend erforderlich. Wenn Sie den Netzwerkauthentifizierungsservice auf der iSeries zur Teilnahme an einem Kerberos-Realm konfigurieren, der im Microsoft Windows Active Directory konfiguriert ist, müssen Sie den Realm-Namen in Großbuchstaben eingeben.

Für einen Kerberos-Server, der in i5/OS PASE konfiguriert ist, können Sie Realm-Namen in Groß- oder Kleinbuchstaben erstellen. Wenn Sie jedoch den Aufbau einer Vertrauensbeziehung zwischen einem Kerberos-Server, der in Microsoft Windows Active Directory und einem Kerberos-Server, der in i5/OS PASE konfiguriert ist, planen, müssen die Realm-Namen in Großbuchstaben eingegeben werden.

*Tabelle 20. Beispiel eines Planungsarbeitsblatts für Kerberos-Realms*

| Fragen | Antworten |
|---|---|
| Wie viele Realms werden benötigt? | Zwei |
| Wie sollen die Realms organisiert werden? | Derzeit verfügt das Unternehmen über einen Windows 2000-Server, der Benutzer in der Auftragsannahme authentifiziert. Die Versandabteilung verwendet einen Kerberos-Server in i5/OS PASE. Jede Abteilung soll Ihren eigenen Realm erhalten. |
| Welche Benennungskonvention soll für Realms gelten? | Es wird ein Kurzname für die Abteilung in Großbuchstaben gefolgt vom Windows 2000-Domänennamen in Großbuchstaben verwendet.ORDEPT.MYCO.COM steht beispielsweise für die Auftragsannahme und SHIPDEPT.MYCO.COM für die Versandabteilung. |

## Principal-Namen planen

Principals sind Namen von Benutzern oder Services in einem Kerberos-Netzwerk. Principal-Namen setzen sich aus dem Benutzer- oder Servicenamen und dem Namen des Realms zusammen, zu dem der Benutzer oder Service gehört. Wenn Mary Jones den Realm MYCO.COM verwendet, dann könnte ihr Principal-Name jonesm@MYCO.COM lauten. Mary Jones verwendet diesen Principal-Namen und das zugehörige Kennwort, um von einem zentralisierten Kerberos-Server authentifiziert zu werden. Alle Principals werden dem Kerberos-Server hinzugefügt, auf dem eine Datenbank mit allen Benutzern und Services innerhalb eines Realms geführt wird.

Principal-Namen sollten auf der Grundlage einer konsistenten Benennungskonvention zugeordnet werden, die sowohl aktuelle als auch zukünftige Benutzer berücksichtigt. Richten Sie sich bei der Festlegung einer Benennungskonvention für Ihre Principals nach folgenden Vorschlägen:

- Nachname und Anfangsbuchstabe des Vornamens
- Anfangsbuchstabe des Vornamens und vollständiger Nachname
- Vorname und Anfangsbuchstabe des Nachnamens
- Anwendungs- oder Servicenamen mit Kenn-Nummern, wie beispielsweise database1

### i5/OS-Principal-Namen

Bei der Konfiguration des Netzwerkauthentifizierungsservice auf der iSeries können die Principal-Namen wahlweise erstellt werden. Jeder dieser Principals repräsentiert Services, die sich auf dem iSeries-Server befinden. Bei der Konfiguration des Netzwerkauthentifizierungsservice wird für jeden erstellten Service-Principal ein Chiffrierschlüsseltabelleneintrag auf dem iSeries-System erstellt. In diesem Eintrag werden der bei der Konfiguration angegebene Name und das verschlüsselte Kennwort des Service-Principals gespeichert. Beachten Sie unbedingt, dass alle i5/OS-Service-Principals dem Kerberos-Server hinzugefügt werden müssen, nachdem der Netzwerkauthentifizierungsservice konfiguriert wurde. Die Methode, die zum Hinzufügen von i5/OS-Principals zum Kerberos-Server verwendet wird, richtet sich danach, welcher

Kerberos-Server in Ihrem Unternehmen konfiguriert wurde. Die Vorgehensweise beim Hinzufügen eines i5/OS-Principal-Namens zu einer Windows 2000-Domäne oder einem Kerberos-Server in i5/OS PASE wird unter „Dem Kerberos-Server i5/OS-Principals hinzufügen" auf Seite 114 erläutert. Im Folgenden werden alle i5/OS-Service-Principals beschrieben, die bei der Konfiguration des Netzwerkauthentifizierungsservice erstellt werden:

**i5/OS-Kerberos-Authentifizierung**
Wenn Sie einen Chiffrierschlüsseleintrag für die i5/OS Kerberos-Authentifizierung erstellen möchten, wird der Service-Principal in einem der folgenden Formate in der Chiffrierschlüsseldatei erstellt: **krbsvr400/iSeries vollständig qualifizierter Domänenname@REALM-NAME** oder **krbsvr400/iSeries Hostname@REALM-NAME**. Ein gültiger Service-Principal für die i5/OS Kerberos-Authentifizierung wäre beispielsweise krbsvr400/iseriesa.myco.com@MYCO.COM oder krbsvr400/iseriesa@MYCO.COM. i5/OS generiert den Principal auf der Basis des Hostnamens, der entweder auf dem DNS-Server oder auf dem iSeries-Server vorhanden ist, je nachdem, wie die iSeries für die Auflösung von Hostnamen konfiguriert ist.

Der Service-Principal wird für mehrere i5/OS-Schnittstellen wie QFileSrv.400, Telnet, Distributed Relational Database Architecture (DRDA), iSeries NetServer und IBM @server iSeries Access für Windows einschließlich iSeries Navigator verwendet. Für jede dieser Anwendungen können zusätzliche Konfigurationsschritte zur Aktivierung der Kerberos-Authentifizierung erforderlich sein.

**LDAP** Außer dem i5/OS-Service-Principal-Namen kann während der Konfiguration des Netzwerkauthentifizierungsservice wahlweise noch IBM Directory Server für iSeries (LDAP) konfiguriert werden. Der LDAP-Principal-Name lautet **ldap/iSeries vollständig qualifizierter Domänenname@REALM-NAME**. Ein gültiger LDAP-Principal-Name wäre beispielsweise ldap/iseriesa.myco.com@MYCO.COM. Dieser Principal-Name bezeichnet den Directory-Server, der sich auf diesem iSeries-System befindet.

**Anmerkung:** In früheren Releases erstellte der Assistent für den Netzwerkauthentifizierungsservice einen Chiffrierschlüsseleintrag für den LDAP-Service. Wenn Sie den LDAP-Principal bereits zuvor konfiguriert haben und den Netzwerkauthentifizierungsservice erneut konfigurieren oder über die EIM-Schnittstelle auf den Assistenten zugreifen, werden Sie aufgefordert, für den Principal-Namen Kleinbuchstaben zu verwenden.

Wenn Sie planen, die Kerberos-Authentifizierung für den Directory-Server zu verwenden, müssen Sie nicht nur den Netzwerkauthentifizierungsservice konfigurieren sondern auch die Eigenschaften des Directory-Servers so ändern, dass die Kerberos-Authentifizierung akzeptiert wird. Wenn die Kerberos-Authentifizierung verwendet wird, ordnet der Directory-Server dem Kerberos-Pincipalnamen den registrierten Namen (DN) des Servers zu. Für die Zuordnung des Server-DN können Sie eine der folgenden Methoden auswählen:

- Der Server kann einen DN auf der Basis des Kerberos-Principal-Namens erstellen. Wenn Sie sich für diese Möglichkeit entscheiden, generiert eine Kerberos-Identität im Format principal@realm einen DN im Format ibm-kn=principal@realm. ibm-kn= ist äquivalent zu ibm-kerberosName=.
- Der Server kann das Verzeichnis nach einem registrierten Namen (DN) durchsuchen, der einen Eintrag für den Kerberos-Principal und -Realm enthält. Wenn Sie sich für diese Möglichkeit entscheiden, durchsucht der Server das Verzeichnis nach einem Eintrag mit dieser Kerberos-Identität.

Nähere Informationen über die Konfiguration der Kerberos-Authentifizierung für den Directory-Server finden Sie unter IBM Directory Server für iSeries (LDAP).

**HTTP-Server (powered by Apache)**
Außer dem i5/OS-Service-Principal-Namen können während der Konfiguration des Netzwerkauthentifizierungsservice zusätzliche Service-Principals für HTTP-Server (powered by Apache) konfiguriert werden. Der HTTP-Principal-Name lautet **HTTP/iSeries vollständig qualifizierter**

**Domänenname@REALM-NAME**. Dieser Principal-Name bezeichnet die HTTP-Server-Instanzen auf der iSeries, die Kerberos für die Authentifizierung von Webbenutzern einsetzen werden.Um die Kerberos-Authentifizierung für eine HTTP-Server-Instanz anwenden zu können, sind außerdem weitere Konfigurationsschritte für den HTTP-Server erforderlich.

Die Homepage HTTP-Server: Dokumentation enthält Informationen über die Verwendung der Kerberos-Authentifizierung für den HTTP-Server.

**iSeries NetServer**

Für iSeries NetServer können Sie außerdem mehrere NetServer-Principals erstellen, die automatisch der Chiffrierschlüsseldatei auf der iSeries hinzugefügt werden. Jeder dieser NetServer-Principals repräsentiert alle potenziellen Clients, die Sie für die Verbindung mit iSeries NetServer verwenden könnten. Die folgende Tabelle enthält die iSeries NetServer-Principal-Namen und die entsprechenden Clients:

*Tabelle 21. iSeries NetServer-Pincipal-Namen*

| Clientverbindung | iSeries NetServer-Principal-Name |
|---|---|
| Windows XP | cifs/iSeries vollständig qualifizierter Domänenname<br>cifs/iSeries Hostname<br>cifs/QiSeries Hostname<br>cifs/qiSeries Hostname<br>cifs/IP-Adresse |
| Windows 2000 | HOST/iSeries vollständig qualifizierter Domänenname<br>HOST/iSeries Hostname<br>HOST/QiSeries Hostname<br>HOST/qiSeries Hostname<br>HOST/IP-Adresse |

Weitere Informationen über die Verwendung der Kerberos-Authentifizierung für diese Anwendung finden Sie unter iSeries NetServer.

**Beispiel eines Planungsarbeitsblatts**

*Tabelle 22. Beispiel eines Planungsarbeitsblatts für Principals*

| Fragen | Antworten |
|---|---|
| Welche Benennungskonvention soll für Kerberos-Principals verwendet werden, die Benutzer in Ihrem Netzwerk repräsentieren? | Erster Buchstabe des Vornamens gefolgt von den ersten fünf Buchstaben des Nachnamens in Kleinbuchstaben. Beispiel: mjones |
| Welche Benennungskonvention gilt für Anwendungen auf Ihrem Netzwerk? | Beschreibender Name gefolgt von einer Zahl. Beispiel: database123 |
| Für welche i5/OS-Services soll die Kerberos-Authentifizierung verwendet werden? | 1. i5/OS Kerberos-Authentifizierung für die folgenden Services: iSeries Access für Windows, iSeries Navigator, NetServer und Telnet.<br>2. HTTP-Server (powered by Apache)<br>3. LDAP |
| Wie lauten die i5/OS-Principal-Namen für jeden dieser i5/OS-Services? | 1. krbsvr400/iseriesa.myco.com@MYCO.COM<br>2. HTTP/iseriesa.myco.com@MYCO.COM<br>3. ldap/iseriesa.myco.com@MYCO.COM |

## Hinweise zur Auflösung von Hostnamen

In einer Kerberos-Umgebung verwenden sowohl der Client als auch der Server eine Form der Hostnamensauflösung, um den Hostnamen des Systems festzustellen, auf dem sich eine bestimmte Anwendung oder ein bestimmter Service befindet.

Wenn die iSeries-Server und die PCs einen DNS-Server (DNS = Domain Name System) verwenden, ist zu beachten, dass sie denselben DNS-Server für die Hostnamensauflösung verwenden müssen; wenn sie mehr als einen DNS-Server verwenden, ist zu beachten, dass die Hostnamen auf beiden DNS-Servern übereinstimmen müssen. Wenn Ihr iSeries-System oder PC Hostnamen lokal auflöst (aus einer lokalen Hosttabelle oder Datei), kann es vorkommen, dass ein anderer Hostname aufgelöst wird als der entsprechende Hostname, der auf dem DNS-Server aufgezeichnet ist. Dies kann zu einem Fehler im Netzwerkauthentifizierungsservice führen.

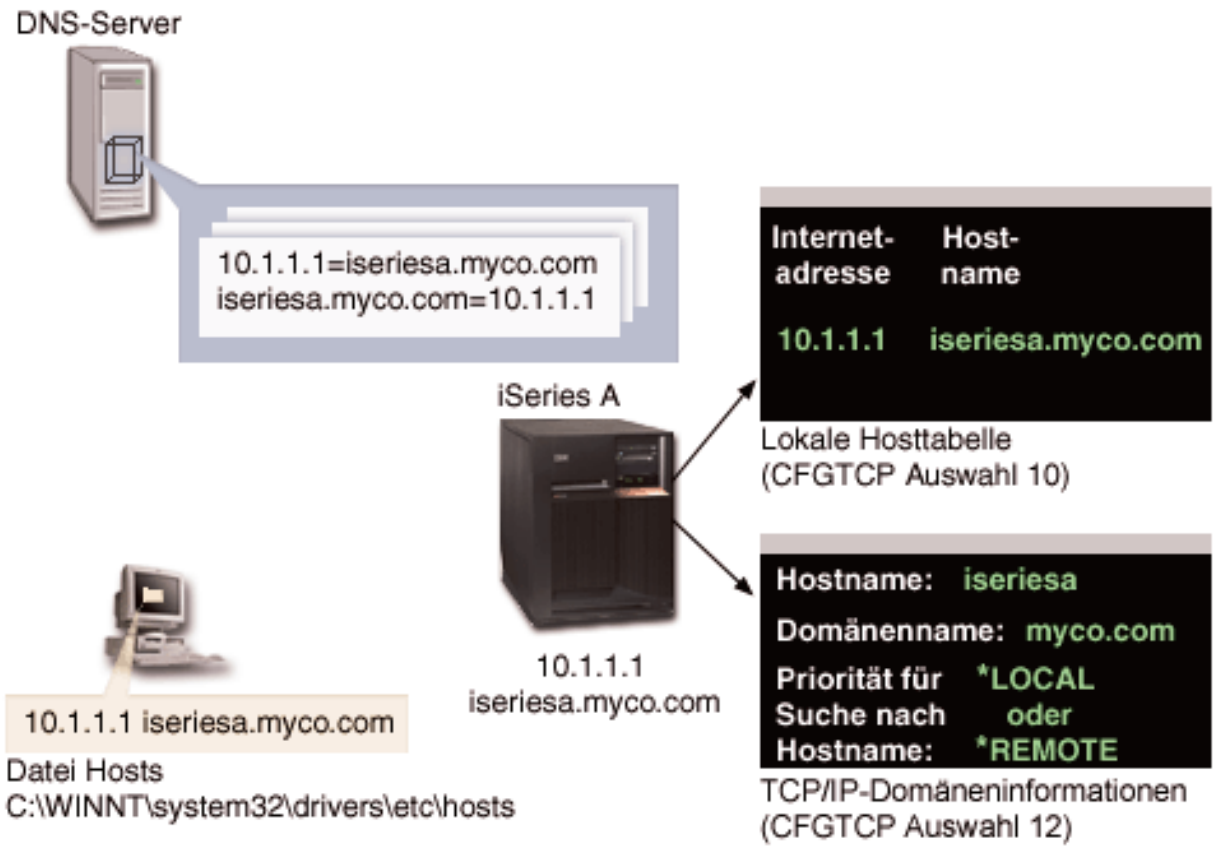
Um sicherzustellen, dass die Kerberos-Authentifizierung und die Hostnamensauflösung fehlerfrei für die Kerberos-fähigen Anwendungen funktionieren, müssen Sie prüfen, ob Ihre PCs und iSeries-Server denselben Hostnamen für das System auflösen, auf dem sich die Serviceanwendung befindet.Im folgenden Beispiel wird dieses System als iSeries A bezeichnet.

Die nachfolgenden Anweisungen zeigen, wie festgestellt wird, ob die PCs und iSeries-Systeme denselben Namen für die iSeries A auflösen. Nehmen Sie die Beispielarbeitsblätter zur Hand, während Sie die Anweisungen befolgen.

Sie können Ihre eigenen Informationen in die leeren Arbeitsblätter eintragen, wenn Sie diese Schritte für Ihren Kerberos-Realm ausführen.

Die Grafik zeigt die Systemdateien und Sätze, die die Hostnamensinformationen im folgenden Beispiel enthalten.

**Anmerkung:** Die IP-Adresse 10.1.1.1 ist eine allgemein zugängliche IP-Adresse. Diese Adresse dient nur als Beispiel.



**Details**

**DNS-Server**

- Enthält Datenressourcensätze, die angeben, dass IP-Adresse `10.1.1.1` mit dem Hostnamen `iseriesa.myco.com` korreliert, der IP-Adresse und dem Hostnamen für die iSeries A.
- Kann vom PC, der iSeries A oder von beiden für die Hostauflösung verwendet werden.

**Anmerkung:** Dieses Beispiel veranschaulicht die Verwendung eines einzigen DNS-Servers. In Ihrem Netzwerk können jedoch auch mehrere DNS-Server verwendet werden. Z. B. kann Ihr PC einen DNS-Server für die Auflösung von Hostnamen und Ihr iSeries-Server einen anderen DNS-Server verwenden.Sie müssen feststellen, wie viele DNS-Server Ihr Realm für die Hostauflösung verwendet, und diese Informationen Ihrer Situation entsprechend anpassen.

**PC**

- Wird unter dem Betriebssystem Windows 2000 ausgeführt.
- Repräsentiert sowohl den PC, der für die Verwaltung des Netzwerkauthentifizierungsservice verwendet wird, als auch den PC, der von einem Benutzer ohne Sonderberechtigung zur Ausführung von Routineaufgaben verwendet wird.
- Enthält die Datei `hosts`, die angibt, dass IP-Adresse `10.1.1.1` mit dem Hostnamen `iseriesa.myco.com` korreliert.

**Anmerkung:** Die Datei hosts befindet sich in den folgenden Ordnern:

- Betriebssystem Windows 2000: C:\WINNT\system32\drivers\etc\hosts
- Betriebssystem Windows XP: C:\WINDOWS\system32\drivers\etc\hosts

**iSeries A**

- Wird unter i5/OS Version 5 Release 3 (V5R3) ausgeführt.
- Enthält eine Serviceanwendung, auf die Sie unter Verwendung des Netzwerkauthentifizierungsservice (Kerberos-Authentifizierung) zugreifen müssen.
- Im Menü CFGTCP (TCP konfigurieren) liefern die Auswahlmöglichkeiten 10 und 12 die folgenden Informationen für die iSeries A:
  - Auswahl 10 (Mit TCP/IP-Hosttabelleneinträgen arbeiten):
    - **Internet-Adresse**: `10.1.1.1`
    - **Hostname**: `iseriesa.myco.com`
  - Auswahl 12 (TCP/IP-Domäneninformationen ändern):
    - **Hostname**: `iseriesa`
    - **Domänenname**: `myco.com`
    - **Priorität für Suche nach Hostname**: `*LOCAL` oder `*REMOTE`

**Anmerkung:** Der Parameter *Priorität für Suche nach Hostname* hat entweder den Wert *LOCAL oder *REMOTE, je nachdem, wie TCP/IP vom Netzwerkadministrator für die Ausführung der Hostnamensauflösung auf dem Server konfiguriert wurde.

*Tabelle 23. Beispiel: Arbeitsblatt für die Hostnamensauflösung auf dem PC*

| **Auf dem PC den Hostnamen für die iSeries A feststellen** | | |
|---|---|---|
| **Schritt** | **Quelle** | **Hostname** |
| 1.a.1 | PC-Datei hosts | iseriesa.myco.com |

*Tabelle 23. Beispiel: Arbeitsblatt für die Hostnamensauflösung auf dem PC (Forts.)*

| **Auf dem PC den Hostnamen für die iSeries A feststellen** | | |
|---|---|---|
| 1.b.1 | DNS-Server | iseriesa.myco.com |

*Tabelle 24. Beispiel: Arbeitsblatt für die Hostnamensauflösung auf der iSeries*

| **Auf der iSeries A den Hostnamen für die iSeries A feststellen** | | |
|---|---|---|
| **Schritt** | **Quelle** | **Hostname** |
| 2.a.2 | iSeries A<br>CFGTCP Auswahl 12 | **Hostname**: iseriesa<br>**Domänenname**: myco.com |
| **Anmerkung:** Wert für *Priorität für Suche nach Hostname*: *LOCAL oder *REMOTE | | |
| 2.b.2 | iSeries A<br>CFGTCP Auswahl 10 | iseriesa.myco.com |
| 2.c.1 | DNS-Server | iseriesa.myco.com |

*Tabelle 25. Beispiel: Arbeitsblatt für übereinstimmende Hostnamen*

| **Diese drei Hostnamen müssen exakt übereinstimmen** | |
|---|---|
| **Schritt** | **Hostname** |
| Schritt 1 | iseriesa.myco.com |
| Schritt 2.a.2 | iseriesa<br>myco.com |
| 2d | iserisa.myco.com |

*Tabelle 26. Arbeitsblatt für die Hostnamensauflösung auf dem PC*

| **Auf dem PC dem Hostnamen für den iSeries-Server feststellen** | | |
|---|---|---|
| **Schritt** | **Quelle** | **Hostname** |
| 1.a.1 | PC-Datei hosts | |
| 1.b.1 | DNS-Server | |

*Tabelle 27. Arbeitsblatt für die Hostnamensauflösung auf der iSeries*

| **Auf dem iSeries-Server den Hostnamen für die iSeries feststellen** | | |
|---|---|---|
| **Schritt** | **Quelle** | **Hostname** |
| 2.a.2 | iSeries<br>CFGTCP Auswahl 12 | **Hostname**:<br>**Domänenname**: |
| Wert für *Priorität für Suche nach Hostname* beachten: *LOCAL oder *REMOTE | | |
| 2.b.2 | iSeries<br>CFGTCP Auswahl 10 | |
| 2.c.1 | DNS-Server | |

*Tabelle 28. Arbeitsblatt für übereinstimmende Hostnamen*

| **Diese drei Hostnamen müssen exakt übereinstimmen** | |
|---|---|
| **Schritt** | **Hostname** |
| Schritt 1 | |
| Schritt 2.a.2 | |
| 2d | |

Führen Sie die folgenden Schritte durch, um sicherzustellen, dass die PCs und iSeries-Systeme denselben Hostnamen für die die iSeries A auflösen:

1. Stellen Sie auf dem PC den vollständig qualifizierten TCP/IP-Hostnamen für die iSeries A fest.

   **Anmerkung:** Je nachdem, wie das Netzwerk verwaltet wird, können Sie diesen Schritt auch auf anderen PCs ausführen, die zur Einzelanmeldungsumgebung gehören.

   a. Öffnen Sie im Windows Explorer auf dem PC die Datei `hosts` unter einer der folgenden Adressen:
      - Betriebssystem Windows 2000: C:\WINNT\system32\drivers\etc\hosts
      - Betriebssystem Windows XP: C:\WINDOWS\system32\drivers\etc\hosts

      **Anmerkung:** Wenn auf dem PC keine Datei `hosts` vorhanden ist, verwendet er möglicherweise einen DNS-Server zur Auflösung von Hostnamen. Fahren Sie in diesem Fall mit Schritt 1b fort.

      1) Notieren Sie den ersten Hostnamenseintrag für die iSeries A auf dem Arbeitsblatt; beachten Sie dabei die Groß-/Kleinschreibung. Beispiel: `iseriesa.myco.com`.

         **Anmerkung:** Wenn die Datei hosts keinen Eintrag für die iSeries A enthält, verwendet Ihr PC möglicherweise einen DNS-Server zur Auflösung von Hostnamen. Fahren Sie in diesem Fall mit Schritt 1b fort.

   b. Verwenden Sie NSLOOKUP für die Abfrage des DNS-Servers.

      **Anmerkung:** Überspringen Sie diesen Schritt, wenn Sie in der PC-Datei `hosts` einen Hostnamenseintrag gefunden haben, und fahren Sie mit Schritt 2 fort. (Beim Auflösen von Hostnamen für den PC durch das Betriebssystem hat die Datei `hosts` Vorrang vor DNS-Servern.)

      1) Geben Sie bei einer Eingabeaufforderung `NSLOOKUP` ein, und drücken Sie die Eingabetaste. Geben Sie bei der NSLOOKUP-Eingabeaufforderung `10.1.1.1` ein, um den DNS-Server für die iSeries A abzufragen. Notieren Sie den vom DNS-Server zurückgegebenen Hostnamen; beachten Sie die Groß-/Kleinschreibung. Beispiel: `iseriesa.myco.com`.
      2) Geben Sie bei der NSLOOKUP-Eingabeaufforderung `iseriesa.myco.com` ein. Dabei muss es sich um den vom DNS-Server im vorherigen Schritt zurückgegebenen Hostnamen handeln. Vergewissern Sie sich, dass der DNS-Server die IP-Adresse zurückgibt, die Sie erwarten. Beispiel: `10.1.1.1`.

         **Anmerkung:** Wenn NSLOOKUP nicht die erwarteten Ergebnisse liefert, ist Ihre DNS-Konfiguration unvollständig. Gibt NSLOOKUP beispielsweise eine IP-Adresse zurück, die von der in Schritt 1.b.1 eingegebenen Adresse abweicht, müssen Sie den DNS-Administrator informieren, damit der Fehler behoben wird, bevor Sie mit den nächsten Schritten fortfahren können.

2. Stellen Sie auf der iSeries A den vollständig qualifizierten TCP/IP-Hostnamen fest.
   a. TCP/IP-Domäneninformationen

1) Geben Sie bei der Eingabeaufforderung `CFGTCP` ein und geben Sie Auswahl 12 (TCP/IP-Domänen ändern) an.
2) Notieren Sie die Werte für die Parameter *Hostname* und *Domänenname*; beachten Sie dabei die Groß-/Kleinschreibung. Beispiel:
   - **Hostname**: `iseriesa`
   - **Domänenname**: `myco.com`
3) Notieren Sie den Wert für den Parameter *Priorität für Suche nach Hostname*.
   - `*LOCAL` - Das Betriebssystem durchsucht zuerst die lokale Hosttabelle (entspricht der Datei `hosts` auf dem PC). Wenn in der Hosttabelle kein übereinstimmender Eintrag gefunden wird und ein DNS-Server konfiguriert ist, durchsucht das Betriebssystem anschließend diesen DNS-Server.
   - `*REMOTE` - Das Betriebssystem durchsucht zuerst den DNS-Server. Wenn im DNS-Server kein übereinstimmender Eintrag gefunden wird, durchsucht das Betriebssystem anschließend die lokale Hosttabelle.

b. TCP/IP-Hosttabelle
1) Geben Sie bei der Eingabeaufforderung `CFGTCP` ein und geben Sie Auswahl 10 (Mit TCP/IP-Hosttabelleneinträgen arbeiten) an.
2) Notieren Sie den Wert in der Spalte *Hostname*, der der iSeries A entspricht (IP-Adresse 10.1.1.1); beachten Sie dabei die Groß-/Kleinschreibung. Beispiel: `iseriesa.myco.com`.

   **Anmerkung:** Wenn Sie in der Hosttabelle keinen Eintrag für die iSeries A finden können, fahren Sie mit dem nächsten Schritt fort.

c. DNS-Server
1) Geben Sie bei einer Eingabeaufforderung `NSLOOKUP` ein, und drücken Sie die Eingabetaste. Geben Sie bei der NSLOOKUP-Eingabeaufforderung `10.1.1.1` ein, um den DNS-Server für die iSeries A abzufragen. Notieren Sie den vom DNS-Server zurückgegebenen Hostnamen; beachten Sie die Groß-/Kleinschreibung. Beispiel: `iseriesa.myco.com`.
2) Geben Sie bei der NSLOOKUP-Eingabeaufforderung `iseriesa.myco.com` ein. Dabei muss es sich um den vom DNS-Server im vorherigen Schritt zurückgegebenen Hostnamen handeln. Vergewissern Sie sich, dass der DNS-Server die IP-Adresse zurückgibt, die Sie erwarten. Beispiel: `10.1.1.1`.

   **Anmerkung:** Wenn NSLOOKUP nicht die erwarteten Ergebnisse liefert, ist Ihre DNS-Konfiguration unvollständig. Gibt NSLOOKUP beispielsweise eine IP-Adresse zurück, die von der in Schritt 2.c.1 eingegebenen Adresse abweicht, müssen Sie den DNS-Administrator informieren, damit der Fehler behoben wird, bevor Sie mit den nächsten Schritten fortfahren können.

d. Legen Sie fest, welcher Hostname für die iSeries A, basierend auf ihrer TCP/IP-Konfiguration, gelten soll.
   - Lautet der Wert für den Parameter *Priorität für Suche nach Hostname* `*LOCAL`, verwenden Sie den Eintrag aus der lokalen Hosttabelle (Schritt 2.b.2).
   - Lautet der Wert für den Parameter *Priorität für Suche nach Hostname* `*REMOTE`, verwenden Sie den Eintrag aus dem DNS-Server (Schritt 2.c.1).
   - Wenn nur eine dieser Quellen einen Eintrag für die iSeries A enthält, dann verwenden Sie diesen Eintrag.

3. Vergleichen Sie die Ergebnisse der folgenden Schritte:
   - Schritt 1 - Name, den der PC für die iSeries A verwendet.

     **Anmerkung:** Wenn Sie in der PC-Datei hosts einen Eintrag für die iSeries A gefunden haben, verwenden Sie diesen. Andernfalls verwenden Sie den Eintrag vom DNS-Server.
   - Schritt 2.a.2 - Name, den die iSeries A selbst innerhalb ihrer TCP/IP-Konfiguration aufruft.
   - Schritt 2d - Name, den die iSeries A selbst auf der Basis der Hostnamensauflösung aufruft.

Alle drei genannten Einträge müssen exakt übereinstimmen, einschließlich Groß-/Kleinschreibung. Wenn die Ergebnisse nicht exakt übereinstimmen, erhalten Sie eine Fehlernachricht, die besagt, dass ein **Chiffrierschlüsseleintrag** nicht gefunden werden kann.

## Planungsarbeitsblätter für Netzwerkauthentifizierungsservice

Um den Netzwerkauthentifizierungsservice richtig zu konfigurieren, müssen Sie die Voraussetzungen kennen und die erforderlichen Planungsschritte ausführen. Im Folgenden finden Sie ein Arbeitsblatt für die Voraussetzungen und ein Arbeitsblatt für die Planung, damit Sie sich vergewissern können, dass alle erforderlichen Schritte durchgeführt werden. Verwenden Sie die Arbeitsblätter als Hilfsmittel für die Planung einer Kerberos-Implementierung und die Konfiguration des Netzwerkauthentifizierungsservice.

### Arbeitsblatt für Voraussetzungen

Verwenden Sie dieses Arbeitsblatt, um sicherzustellen, dass alle erforderlichen Voraussetzungen erfüllt wurden. Sie sollten alle Fragen nach den Voraussetzungen mit Ja beantworten können, bevor Sie mit den Konfigurationstasks beginnen.

*Tabelle 29. Arbeitsblatt für Voraussetzungen*

| Fragen | Antworten |
|---|---|
| Arbeiten Sie mit i5/OS V5R3 (5722-SS1) oder einer späteren Version? | |
| Ist Cryptographic Access Provider (5722-AC3) auf Ihren iSeries-Systemen installiert? | |
| Ist iSeries Access für Windows (5722-XE1) auf dem PC des Administrators und auf Ihren iSeries-Systemen installiert? | |
| Ist die Unterkomponente "Sicherheit" des iSeries Navigator auf dem PC des Administrators installiert? | |
| Ist die Unterkomponente "Netzwerk" des iSeries Navigator auf dem PC des Administrators installiert? | |
| Ist das aktuellste Service-Pack von IBM @server iSeries Access für Windows installiert?<br><br>Dieses Service-Pack finden Sie auf der Webseite iSeries Access. | |
| Verfügen Sie über die Sonderberechtigungen *SECADM, *ALLOBJ und *IOSYSCFG? | |
| Ist eines der folgenden Produkte auf einem sicheren System installiert, das als Kerberos-Server dienen soll? Welches?<br>1. Windows (R) 2000-Server<br>2. Windows (R) Server 2003<br>3. AIX Server<br>4. i5/OS PASE (ab V5R3)<br>5. zSeries | |
| Für Windows (R) 2000-Server und Windows (R) Server 2003: Sind Windows-Unterstützungstools installiert (beinhalten das Tool ktpass)? | |
| Wenn sich Ihr Kerberos-Server auf einem Windows 2000- oder 2003-Server befindet: Sind alle PCs in Ihrem Netzwerk in einer Windows-Domäne konfiguriert? | |
| Wurden die neuesten PTFs (temporäre Programmkorrekturen) angelegt? | |
| Beträgt die Abweichung zwischen der Systemzeit der iSeries und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung höher, siehe „Systemzeiten synchronisieren" auf Seite 118. | |

*Tabelle 30. Planungsarbeitsblatt für Kerberos-Server*

| Fragen | Antworten |
|---|---|
| Unter welchem Betriebssystem soll der Kerberos-Server konfiguriert werden?<br>• Windows (R) 2000-Server<br>• Windows (R) Server 2003<br>• AIX Server<br>• i5/OS PASE (ab V5R3)<br>• zSeries | |
| Wie lautet der vollständig qualifizierte Domänenname für den Kerberos-Server? | |
| Sind die Systemzeiten der PCs und Systeme, die mit dem Kerberos-Server verbunden sind, synchronisiert? Wie hoch ist die maximale Zeitabweichung? | |

*Tabelle 31. Planungsarbeitsblatt für Kerberos-Realm*

| Fragen | Antworten |
|---|---|
| Wie viele Realms werden benötigt? | |
| Wie sollen die Realms organisiert werden? | |
| Welche Benennungskonvention soll für Realms gelten? | |

*Tabelle 32. Planungsarbeitsblatt für Principal*

| Fragen | Antworten |
|---|---|
| Welche Benennungskonvention soll für Kerberos-Principals gelten, die Benutzer in Ihrem Netzwerk repräsentieren? | |
| Welche Benennungskonvention gilt für Anwendungen auf Ihrem Netzwerk? | |
| Für welche i5/OS-Services soll die Kerberos-Authentifizierung verwendet werden? | |
| Wie lauten die i5/OS-Principal-Namen für jeden dieser i5/OS-Services? | |

*Tabelle 33. Arbeitsblatt für Hostnamensauflösung*

| Frage | Antwort |
|---|---|
| Verwenden die PCs und die iSeries denselben DNS-Server zur Auflösung von Hostnamen? | |
| Verwenden Sie eine lokale Hosttabelle auf der iSeries zur Auflösung von Hostnamen? | |
| Lösen Ihr PC und Ihr iSeries-Server denselben Hostnamen für den iSeries-Server auf? Siehe „Hinweise zur Auflösung von Hostnamen" auf Seite 95. | |

Das folgende Planungsarbeitsblatt veranschaulicht, welche Informationen Sie benötigen, bevor Sie mit der Konfiguration des Kerberos-Servers in i5/OS PASE und des Netzwerkauthentifizierungsservice beginnen können. Alle Fragen auf dem Arbeitsblatt für die Voraussetzungen müssen beantwortet werden, bevor Sie mit der Konfiguration des Kerberos-Servers in i5/OS PASE fortfahren.

*Tabelle 34. Planungsarbeitsblatt für i5/OS PASE*

| Fragen | Antworten |
|---|---|
| Ist PASE installiert? | |
| Wie lautet der Name des Standard-Realms? | |
| Wie heißt der Kerberos-Server für diesen Kerberos-Standard-Realm? An welchem Port ist der Kerberos-Server empfangsbereit? | |
| Welche Benennungskonvention gilt für Kerberos-Principals, die Benutzer in Ihrem Netzwerk repräsentieren? | |
| Wie lauten die Principal-Namen der Benutzer in Ihrem Netzwerk? | |

Verwenden Sie das folgende Planungsarbeitsblatt, um alle Informationen zusammenzustellen, die Sie benötigen, bevor Sie mit der Konfiguration des Netzwerkauthentifizierungsservice beginnen können. Alle Fragen auf dem Arbeitsblatt für die Voraussetzungn müssen beantwortet werden, bevor Sie mit der Konfiguration des Netzwerkauthentifizierungsservice fortfahren.

*Tabelle 35. Planungsarbeitsblatt für Netzwerkauthentifizierungsservice*

| Fragen | Antworten |
|---|---|
| Wie lautet der Name des Kerberos-Standard-Realms, zu dem Ihre iSeries gehören soll?<br>**Anmerkung:** Eine Windows 2000-Domäne ist mit einem Kerberos-Realm vergleichbar.Microsoft Active Directory verwendet die Kerberos-Authentifizierung als Sicherheitsmechanismus. | |
| Verwenden Sie Microsoft Active Directory? | |
| Wie heißt der Kerberos-Server für diesen Kerberos-Standard-Realm? An welchem Port ist der Kerberos-Server empfangsbereit? | |
| Soll ein Kennwortserver für den Standard-Realm konfiguriert werden? Wenn ja, beantworten Sie die folgenden Fragen:<br><br>Wie lautet der Name des Kennwortservers<br>für diesen Kerberos-Server?<br>Auf welchem Port ist der Kennwortserver empfangsbereit? | |
| Für welche Services sollen Chiffrierschlüsseleinträge erstellt werden?<br>• i5/OS-Kerberos-Authentifizierung<br>• LDAP<br>• iSeries IBM HTTP-Server<br>• iSeries NetServer | |
| Wenn Sie einen Service-Principal für die i5/OS Kerberos-Authentifizierung erstellen möchten: wie lautet dessen Kennwort? | |
| Wenn Sie einen Service-Principal für LDAP erstellen möchten: wie lautet dessen Kennwort? | |
| Wenn Sie einen Service-Principal für den HTTP-Server erstellen möchten: wie lautet dessen Kennwort? | |
| Wenn Sie einen Service-Principal für NetServer erstellen möchten: wie lautet dessen Kennwort?<br>**Anmerkung:** Bei Ausführung des Assistenten für den Netzwerkauthentifizierungsservice werden mehrere Principals für iSeries NetServer ersetllt. Notieren Sie diese hier, sobald sie im Assistenten angezeigt werden. Die Namen dieser Principals werden benötigt, um sie dem Kerberos-Server hinzufügen zu können. | |

Tabelle 35. Planungsarbeitsblatt für Netzwerkauthentifizierungsservice (Forts.)

| Fragen | Antworten |
|---|---|
| Möchten Sie eine Stapeldatei erstellen, um das Hinzufügen der Service-Principals zum Microsoft Active Directory zu automatisieren? | |
| Möchten Sie den i5/OS-Service-Principals in der Stapeldatei Kennwörter hinzufügen? | |

## Netzwerkauthentifizierungsservice konfigurieren

Der Netzwerkauthentifizierungsservice ermöglicht dem iSeries-Server die Teilnahme an einem vorhandenen Kerberos-Netzwerk. Von daher setzt der Netzwerkauthentifizierungsservice voraus, dass ein Kerberos-Server auf einem sicheren System in Ihrem Netzwerk konfiguriert ist.

**Kerberos-Server konfigurieren**

Derzeit kann ein Kerberos-Server in i5/OS Portable Application Solutions Environment (i5/OS PASE) konfiguriert werden. Neben dieser i5/OS-Unterstützung interagiert der iSeries-Server auch mit dem Microsoft Windows 2000-Server, dem Windows 2003-Server und dem AIX-Server sowie mit zSeries. Lernen Sie anhand der folgenden Informationen, wie ein Kerberos-Server auf den einzelnen Plattformen konfiguriert wird:

- Microsoft Windows Help
- z/OS Security Server Network Authentication Service
- IBM Network Authentication Service Version 1.3 for AIX: Administrator's and User's Guide

  **Anmerkung:** Diese Dokumentation finden Sie auf der CD: AIX 5L Expansion Pack and Bonus Pack.

**Kerberos-Server in i5/OS PASE konfigurieren**

1. „Kerberos-Server in i5/OS PASE konfigurieren"
2. „Verschlüsselungswerte auf dem Kerberos-Server ändern" auf Seite 105
3. „Kerberos-Server stoppen und erneut starten" auf Seite 106
4. „Host-, Benutzer- und Service-Principals erstellen" auf Seite 106
5. „Windows 2000- und Windows XP-Workstations konfigurieren" auf Seite 107
6. „Sekundären Kerberos-Server konfigurieren" auf Seite 108

**Netzwerkauthentifizierungsservice auf dem iSeries-Server konfigurieren**

1. „Netzwerkauthentifizierungsservice konfigurieren" auf Seite 112
2. „Dem Kerberos-Server i5/OS-Principals hinzufügen" auf Seite 114
3. „Ausgangsverzeichnis erstellen" auf Seite 116
4. „Netzwerkauthentifizierungsservice testen" auf Seite 117

## Kerberos-Server in i5/OS PASE konfigurieren

i5/OS unterstützt einen Kerberos-Server in i5/OS Portable Application Solutions Environment (PASE). i5/OS PASE stellt eine integrierte Laufzeitumgebung für AIX-Anwendungen zur Verfügung. Sie können einen Kerberos-Server von Ihrem iSeries-System aus konfigurieren und verwalten. Führen Sie folgende Tasks aus, um einen Kerberos-Server in i5/OS PASE zu konfigurieren:

1. Geben Sie in einer zeichenorientierten Schnittstelle `call QP2TERM` in der Eingabeaufforderung ein. Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.

2. Geben Sie in der Befehlszeile `export PATH=$PATH:/usr/krb5/sbin` ein. Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.
3. Geben Sie in der Befehlszeile `config.krb5 -S -d iseriesa.myco.com -r MYCO.COM` ein. `-d` ist der DNS Ihres Netzwerks und `-r` ist der Name des Realms. (In diesem Beispiel ist myco.com der DNS-Name und MYCO.COM der Realmname.) Dieser Befehl aktualisiert die Datei krb5.config mit dem Domänennamen und dem Realm für den Kerberos-Server, erstellt die Kerberos-Datenbank innerhalb des integrierten Dateisystems und konfiguriert den Kerberos-Server in i5/OS PASE. Sie werden aufgefordert, ein Hauptkennwort für die Datenbank und ein Kennwort für den Principal admin/admin hinzuzufügen, das für die Verwaltung des Kerberos-Servers verwendet wird.

   **Anmerkung:** In V5R3 können Kerberos-Principals nur in der vorhandenen Datenbank gespeichert werden. Das LDAP-Verzeichnis-Plug-in wird derzeit nicht unterstützt.
4. (Optional) Wenn der Kerberos-Server und der Verwaltungsserver beim IPL automatisch gestartet werden sollen, müssen zwei weitere Schritte durchgeführt werden. Sie müssen eine Jobbeschreibung erstellen und einen Eintrag für den automatisch zu startenden Job hinzufügen.

   Führen Sie die folgenden Schritte durch, um i5/OS für das automatische Starten des Kerberos-Servers und des Verwaltungsservers während eines IPL zu konfigurieren:

   a. Erstellen Sie eine Jobbeschreibung.

      Geben Sie in einer i5/OS-Befehlszeile Folgendes ein: `CRTJOBD JOBD(QGPL/KRB5PASE) JOBQ(QSYS/QSYSNOMAX) TEXT('KDC und Admin-Server in PASE starten') USER(`*xxxxxx*`) RQSDTA('QSYS/CALL PGM(QSYS/QP2SHELL) PARM(''/usr/krb5/sbin/start.krb5'')') SYNTAX(*NOCHK) INLLIBL(*SYSVAL) ENDSEV( 30)`, wobei *xxxxxx* das i5/OS-Benutzerprofil mit der Berechtigung *ALLOBJ ist.

   b. Fügen Sie einen Eintrag für den automatisch zu startenden Job hinzu.

      Geben Sie in der Befehlszeile `ADDAJE SBSD(QSYS/QSYSWRK) JOB(KRB5PASE) JOBD(QGPL/KRB5PASE)` ein.

**Anmerkung:** Statt beim IPL können die Server auch manuell nach dem IPL gestartet werden. Führen Sie dazu die folgenden Schritte durch:

1. Geben Sie in einer zeichenorientierten Schnittstelle `call QP2TERM` ein, um die interaktive Shell-Umgebung i5/OS PASE aufzurufen.
2. Geben Sie in der Befehlszeile `/usr/krb5/sbin/start.krb5` ein, um die Server zu starten.

**Die weiteren Schritte**

Wenn Sie Windows 2000- oder Windows XP-Workstations mit einem Kerberos-Server verwenden, der nicht durch Windows 2000 Active Directory konfiguriert ist (wie beispielsweise ein Kerberos-Server in i5/OS PASE), müssen Sie sowohl auf dem Kerberos-Server als auch auf der Workstation mehrere Konfigurationsschritte ausführen, damit die Kerberos-Authentifizierung einwandfrei funktioniert.

„Verschlüsselungswerte auf dem Kerberos-Server ändern"

## Verschlüsselungswerte auf dem Kerberos-Server ändern

Die Standardverschlüsselungseinstellungen des Kerberos-Servers müssen geändert werden, damit Clients am i5/OS PASE-Kerberos-Server authentifiziert werden können und ein Betrieb mit Windows-Workstations möglich ist. Zum Ändern der Standardverschlüsselungseinstellungen müssen Sie die Datei kdc.conf im Verzeichnis /etc/krb5 editieren. Gehen Sie dazu wie folgt vor:

1. Geben Sie in einer zeichenorientierten Schnittstelle `edtf '/var/krb5/krb5kdc/kdc.conf'` ein, um auf die Datei kdc.conf zuzugreifen.
2. Ändern Sie die folgenden Zeilen in der Datei kdc.conf:

```
supported_enctypes = des3-cbc-sha1:normal
des-cbc-md5:normal des-cbc-crc:normal
kdc_supported_enctypes = des3-cbc-sha1:normal
des-cbc-md5:normal des-cbc-crc:normal
```

in

```
supported_enctypes = des-cbc-md5:normal
kdc_supported_enctypes = des-cbc-md5:normal
```

**Die weiteren Schritte**

„Kerberos-Server stoppen und erneut starten"

## Kerberos-Server stoppen und erneut starten

Der Kerberos-Server muss in i5/OS PASE gestoppt und erneut gestartet werden, damit die zuvor geänderten Verschlüsselungswerte aktualisiert werden. Führen Sie die folgenden Schritte durch:

1. Geben Sie in einer zeichenorientierten Schnittstelle `call QP2TERM` in der Befehlszeile ein. Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.
2. Geben Sie in der Befehlszeile `export PATH=$PATH:/usr/krb5/sbin` ein. Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.
3. Geben Sie in der Befehlszeile stop.krb5 ein. Mit diesem Befehl wird der Kerberos-Server gestoppt.
4. Geben Sie in der Befehlszeile start.krb5 ein. Mit diesem Befehl wird der Kerberos-Server gestartet.

**Die weiteren Schritte**

„Host-, Benutzer- und Service-Principals erstellen"

## Host-, Benutzer- und Service-Principals erstellen

Mit dieser Prozedur wird Folgendes erstellt:

- Host-Principals für Windows 2000- und Windows XP-Workstations
- Benutzer-Principals auf dem Kerberos-Server
- Ein Service-Principal auf dem Kerberos-Server

Damit eine Windows 2000- oder Windows XP-Workstation und ein Kerberos-Server in i5/OS PASE zusammenarbeiten können, müssen Sie dem Kerberos-Realm einen Host-Principal für die Workstation hinzufügen. Damit Benutzer für Services im Netzwerk authentifiziert werden können, müssen Sie sie als Principals zum Kerberos-Server hinzufügen. Diese Host-Principals werden auf dem Kerberos-Server gespeichert und zur Validierung von Benutzern im Netzwerk verwendet. Damit i5/OS Kerberos-Tickets akzeptieren kann, müssen Sie diese als Principals zum Kerberos-Server hinzufügen. Führen Sie die folgenden Tasks durch:

**Anmerkung:** Die hier verwendeten Benutzernamen, Hostnamen und Kennwörter dienen nur als Beispiel.

1. Geben Sie in einer zeichenorientierten Schnittstelle `call QP2TERM` in der Befehlszeile ein. Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.
2. Geben Sie in der Befehlszeile `export PATH=$PATH:/usr/krb5/sbin` ein. Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.
3. Geben Sie in der Befehlszeile `kadmin -p admin/admin` ein, und drücken Sie die Eingabetaste.
4. Melden Sie sich mit dem Kennwort des Administrators an.
5. Geben Sie bei der kadmin-Eingabeaufforderung `addprinc -pw secret1 host/pc1.myco.com` ein. Mit diesem Befehl wird ein Host-Principal für den PC in Ihrem Netzwerk erstellt. Wiederholen Sie diesen Schritt für alle PCs in Ihrem Netzwerk.

6. Geben Sie `addprinc -pw secret jonesm` ein. Mit diesem Befehl wird ein Principal für den Benutzer Mary Jones erstellt. Wiederholen Sie diesen Schritt für alle Benutzer.
7. Geben Sie bei der kadmin-Eingabeaufforderung `addprinc -pw iseriesa123 krbsvr400/iseriesa.myco.com` ein. Mit diesem Befehl wird ein Service-Principal für den Kerberos-Server erstellt.
8. Geben Sie `quit` ein, um die kadmin-Schnittstelle zu verlassen, und drücken Sie F3 (Verlassen), um die PASE-Umgebung zu verlassen.

**Die weiteren Schritte**

„Windows 2000- und Windows XP-Workstations konfigurieren"

## Windows 2000- und Windows XP-Workstations konfigurieren

Nachdem Sie einen Host-Principal für Ihre Windows 2000-Workstation auf dem Kerberos-Server in i5/OS PASE erstellt haben, müssen Sie die Client-Workstations konfigurieren. Sie müssen diese Clients einer Arbeitsgruppe hinzufügen, indem Sie den Kerberos-Realm und den Kerberos-Server auf der Workstation festlegen. Sie müssen außerdem ein Kennwort festlegen, das der Workstation zugeordnet wird. Führen Sie die folgenden Schritte durch, um die Workstations zu konfigurieren:

**Anmerkung:** Die hier verwendeten Benutzernamen, Hostnamen und Kennwörter dienen nur als Beispiel.

1. Geben Sie in einer Befehlszeile auf der Windows 2000-Workstation Folgendes ein:

```
C:> ksetup /setdomain REALM.NAME.COM
C:> ksetup /addkdc REALM.NAME.COM kdc1.hostname.com
```

   Beispiel: Der Administrator für MyCo, Inc würde Folgendes eingeben:

```
C:> ksetup /setdomain MYCO.COM
C:> ksetup /addkdc MYCO.COM kdc1.myco.com
```

   .
2. Legen Sie das Kennwort des Kontos der lokalen Maschine fest, indem Sie bei der Eingabeaufforderung der Windows 2000-Workstation Folgendes eingeben:

```
C:> ksetup /setmachpassword password
```

   Dieses Kennwort muss mit dem Kennwort übereinstimmen, das beim Erstellen des Host-Principals `pc1.myco.com` verwendet wurde. Beispiel: Der Benutzer für MyCo, Inc würde Folgendes eingeben:

```
C:> ksetup /setmachpassword secret1
```

3. Ordnen Sie den Kerberos-Benutzer einem lokalen Benutzer zu, indem Sie bei der Eingabeaufforderung der Windows 2000-Workstation Folgendes eingeben:

```
C:> ksetup /mapuser jonesm@MYCO.COM maryjones
```

4. Starten Sie den Computer neu, damit die Änderungen in Kraft treten.

**Die weiteren Schritte**

Wenn die iSeries einen in i5/OS PASE konfigurierten Server verwenden soll, müssen Sie den Netzwerkauthentifizierungsservice konfigurieren.

Wahlweise können Sie noch einen sekundären Kerberos-Server konfigurieren, der als Sicherungsserver dient, falls der primäre Kerberos-Server einmal ausfällt oder derart ausgelastet ist, dass er nicht alle Anforderungen verarbeiten kann. Detaillierte Anweisungen hierzu finden Sie unter „Sekundären Kerberos-Server konfigurieren".

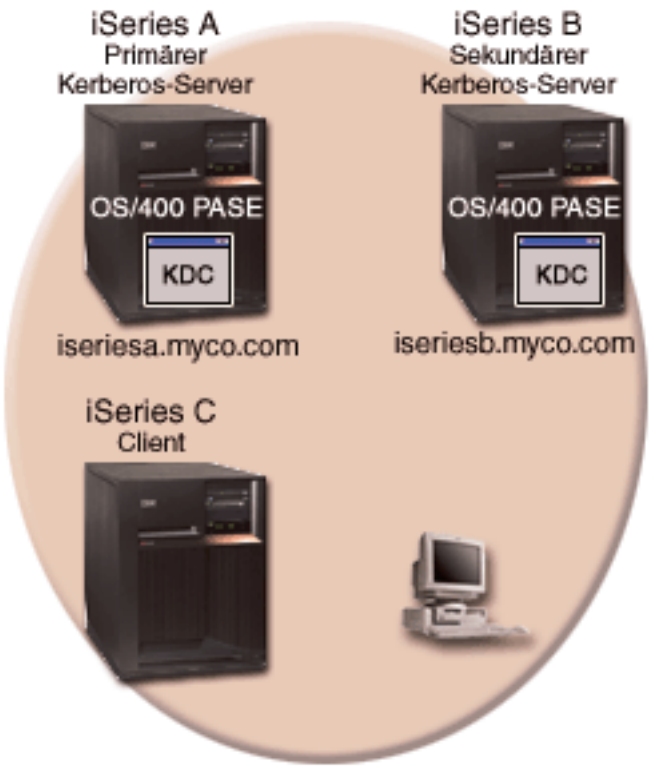
## Sekundären Kerberos-Server konfigurieren

Nach der Konfiguration des primären Kerberos-Servers in i5/OS PASE, können Sie wahlweise noch einen sekundären Kerberos-Server konfigurieren, der als Sicherungsserver dient, falls der primäre Kerberos-Server einmal ausfällt oder derart ausgelastet ist, dass er nicht alle Anforderungen verarbeiten kann.

Beispiel: Die iSeries A dient derzeit als Kerberos-Server. Sie möchten jetzt die iSeries B als sekundären (Sicherungs-) Kerberos-Server konfigurieren.

**Anmerkung:** Ein Kerberos-Server wird auch als KDC (Key Distribution Center - Instanz zur Schlüsselverteilung) bezeichnet.

Die folgende Abbildung zeigt die iSeries-Server, die in den nachfolgenden Anweisungen beschrieben werden.




**Details**

- Die Abbildung zeigt die Server so, wie sie sich nach der Konfiguration eines sekundären Kerberos-Servers darstellen:
  - Die iSeries A fungiert als der primäre Kerberos-Server, der in i5/OS PASE konfiguriert ist.
  - Die iSeries B fungiert als der sekundäre Kerberos-Server, der in i5/OS PASE konfiguriert ist.
  - Die iSeries C fungiert als Client, der die iSeries B als Kerberos-Server verwendet.

Führen Sie die folgenden Schritte durch, um die iSeries B als sekundären Kerberos-Server in i5/OS PASE zu konfigurieren:

1. Konfigurieren Sie die iSeries B als Client.
   a. Geben Sie in einer zeichenorientierten Schnittstelle auf der iSeries B `call QP2TERM` ein.

      Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.
   b. Geben Sie in der Befehlszeile Folgendes ein:
      `export PATH=$PATH:/usr/krb5/sbin`

      Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.
   c. Geben Sie in der Befehlszeile Folgendes ein:
      `config.krb5 -C -d myco.com -r MYCO.COM -s iseriesa.myco.com -c iseriesa.myco.com`
2. Fügen Sie dem Kerberos-Server auf der iSeries A einen i5/OS-Principal für die iSeries A und die iSeries B hinzu.
   a. Geben Sie in einer zeichenorientierten Schnittstelle auf der iSeries A `call QP2TERM` ein.

      Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.
   b. Geben Sie in der Befehlszeile Folgendes ein:
      `export PATH=$PATH:/usr/krb5/sbin`

      Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.
   c. Geben Sie in der Befehlszeile `kadmin -p admin/admin` ein.
   d. Melden Sie sich mit dem Kennwort des Administrators an. Beispiel: `secret`.
   e. Geben Sie in der Befehlszeile Folgendes ein:
      `addprinc -randkey -clearpolicy host/iseriesa.myco.com`
   f. Geben Sie in der Befehlszeile Folgendes ein:
      `addprinc -randkey -clearpolicy host/iseriesb.myco.com`
3. Erstellen Sie auf der iSeries A und der iSeries B eine Chiffrierschlüsseldatei.
   a. Geben Sie in einer zeichenorientierten Schnittstelle auf der iSeries A `call QP2TERM` ein.

      Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.
   b. Geben Sie in der Befehlszeile Folgendes ein:
      `export PATH=$PATH:/usr/krb5/sbin`

      Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.
   c. Geben Sie in der Befehlszeile `kadmin -p admin/admin` ein.
   d. Melden Sie sich mit dem Kennwort des Administrators an. Beispiel: `secret`.
   e. Geben Sie in der Befehlszeile Folgendes ein:
      `ktadd host/iseriesa.myco.com@MYCO.COM`

   Wiederholen Sie diese Schritte auf der iSeries B, geben Sie jedoch `ktadd host/iseriesb.myco.com@MYCO.COM` ein.
4. Erstellen Sie auf der iSeries A und der iSeries B eine Zugriffssteuerungslistendatei.

   Sie müssen auf jedem iSeries-Server eine Datei mit dem Namen /var/krb5/krb5kdc/kpropd.acl erstellen, die eine Liste der Host-Principals enthält, die berechtigt sind, die Datenbank des Netzwerkauthentifizierungsservice vom primären Kerberos-Server (iSeries A) auf die iSeries B zu replizieren.

   Führen Sie die folgenden Schritte durch, um diese Datei zu erstellen:
   a. Geben Sie in einer zeichenorientierten Schnittstelle auf der iSeries A `call QP2TERM` ein.

      Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.
   b. Geben Sie in der Befehlszeile Folgendes ein:
      `export PATH=$PATH:/usr/krb5/sbin`

Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.

c. Geben Sie in der Befehlszeile Folgendes ein:
```
echo "host/iseriesa.myco.com@MYCO.COM" > /var/krb5/krb5kdc/kpropd.acl
```
Mit diesem Befehl wird die Zugriffssteuerungslistendatei auf der iSeries A erstellt oder ersetzt.

d. Geben Sie in der Befehlszeile Folgendes ein:
```
echo "host/iseriesb.myco.com@MYCO.COM" >> /var/krb5/krb5kdc/kpropd.acl
```
Mit diesem Befehl wird der Host-Principal für die iSeries B an die Zugriffssteuerungslistendatei auf der iSeries A angefügt.

Wiederholen Sie die Schritte a bis d, um die Zugriffssteuerungslistendatei auf der iSeries B zu erstellen.

Drücken Sie F3 (Verlassen), um die PASE-Umgebung zu verlassen.

5. Fügen Sie mit dem Befehl ADDSRVTBLE sowohl dem primären Kerberos-Server (iSeries A) als auch der iSeries B Services hinzu.

Um die Services hinzuzufügen, geben Sie folgende Befehle in der i5/OS-Befehlszeile auf der iSeries A ein:

```
ADDSRVTBLE SERVICE('kerberos') PORT(88) PROTOCOL('udp')
    TEXT('Kerberos-Authentifizierung (udp)') ALIAS('kdc')
ADDSRVTBLE SERVICE('kerberos') PORT(88) PROTOCOL('tcp')
    TEXT('Kerberos-Authentifizierung (tcp)') ALIAS('kdc')
ADDSRVTBLE SERVICE('krb5_prop') PORT(754) PROTOCOL('tcp') TEXT('Kerberos-Weitergabe')
ADDSRVTBLE SERVICE('kerberos-adm') PORT(749) PROTOCOL('tcp') TEXT('Kerberos 5 admin/changepw')
ADDSRVTBLE SERVICE('kerberos-adm') PORT(749) PROTOCOL('udp') TEXT('Kerberos 5 admin/changepw')
```

**Anmerkung:** Diese Einträge repräsentieren die Standardports. Wenn Sie andere Ports verwenden möchten, müssen Sie diese explizit angeben.

Wiederholen Sie diese Schritte auf der iSeries B.

6. Starten Sie den Dämon kpropd auf der iSeries B.

Es gibt zwei Möglichkeiten, diesen Dämon zu starten. Er kann manuell oder bei jedem IPL des Systems automatisch gestartet werden. Die folgenden Informationen enthalten Anweisungen für beide Möglichkeiten.

**Anmerkung:** In einer Produktionsumgebung werden Sie den Dämon kpropd in der Regel automatisch bei jedem IPL starten wollen.

**Dämon kpropd manuell starten**

Führen Sie die folgenden Schritte durch, um den Dämon kprod manuell zu starten:

a. Geben Sie in einer zeichenorientierten Schnittstelle auf der iSeries B `call QP2TERM` ein.
Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.

b. Geben Sie in der Befehlszeile Folgendes ein:
```
export PATH=$PATH:/usr/krb5/sbin
```
Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.

c. Geben Sie in der Befehlszeile Folgendes ein:
```
kpropd -S
```

**Dämon kpropd für automatisches Starten konfigurieren**

Wahlweise können Sie den Dämon kpropd für ein automatisches Starten während eines IPL konfigurieren. Dazu müssen Sie folgendermaßen eine Jobbeschreibung erstellen und den Eintrag für den automatisch zu startenden Job hinzufügen:

a. Geben Sie in der i5/OS-Befehlszeile den nachfolgenden Befehl ein. *xxxxxx* ist das i5/OS-Benutzerprofil mit der Berechtigung *ALLOBJ. `CRTJOBD JOBD(QGPL/KRB5PROPD) JOBQ(QSYS/QSYSNOMAX) TEXT('Weitergabedämon krb5 starten') USER(xxxxxx) RQSDTA('QSYS/CALL PGM(QSYS/QP2SHELL) PARM(''/usr/krb5/sbin/kpropd -S'')') SYNTAX(*NOCHK) INLLIBL(*SYSVAL) ENDSEV( 30)`

Geben Sie in der Befehlszeile Folgendes ein:
`ADDAJE SBSD(QSYS/QSYSWRK) JOB(KRB5PROPD) JOBD(QGPL/KRB5PROPD)`

7. Replizieren Sie die Datenbank vom primären Kerberos-Server (iSeries A) auf die iSeries B.

   Dazu müssen Sie folgendermaßen einen Speicherauszug der Datenbank auf dem primären Kerberos-Server erstellen und die Datenbank dann manuell auf die iSeries B kopieren:

   a. Geben Sie in einer zeichenorientierten Schnittstelle auf der iSeries A `call QP2TERM` ein.

      Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.

   b. Geben Sie in der Befehlszeile Folgendes ein:
      `export PATH=$PATH:/usr/krb5/sbin`

      Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.

   c. Geben Sie in der Befehlszeile Folgendes ein:
      `kdb5_util dump /var/krb5/krb5kdc/slave_datatrans`

      Mit diesem Befehl wird ein Speicherauszug der Datenbank auf dem primären Kerberos-Server erstellt.

      **Anmerkung:** /var/krb5/krb5kdc/slave_datatrans dient nur als Beispiel für den Namen der Speicherauszugsdatei. Der tatsächliche Datei- oder Verzeichnisname kann anders lauten.

   d. Geben Sie in der Befehlszeile Folgendes ein:
      `kprop -f /var/krb5/krb5kdc/slave_datatrans iseriesb.myco.com`

      Mit diesem Befehl wird die Datenbank vom primären Kerberos-Server auf die iSeries B kopiert.

8. Kopieren Sie die KDC-Konfigurationsdatei vom primären Kerberos-Server auf die iSeries B.

   Die KDC-Konfigurationsdatei (kdc.conf) befindet sich in /var/krb5/krb5kdc/kdc.conf auf dem primären Kerberos-Server. Sie müssen diese Datei unter Verwendung von FTP (File Transfer Protocol) vom primären Kerberos-Server auf die iSeries B kopieren.

   Führen Sie die folgenden Schritte durch, um die KDC-Konfigurationsdatei vom primären Kerberos-Server auf die iSeries B zu kopieren:

   a. Geben Sie in der i5/OS-Befehlszeile auf dem primären Kerberos-Server (iSeries A) `ftp iseriesb.myco.com` ein. Mit diesem Befehl wird eine FTP-Sitzung gestartet. Sie werden aufgefordert, Ihren Benutzernamen und Ihr Kennwort einzugeben.

   b. Geben Sie bei der FTP-Eingabeaufforderung Folgendes ein:
      `namefmt 1`

   c. Geben Sie bei der FTP-Eingabeaufforderung Folgendes ein:
      `cd /var/krb5/krb5kdc`

   d. Geben Sie bei der FTP-Eingabeaufforderung Folgendes ein:
      `put /var/krb5/krb5kdc/kdc.conf kdc.conf`

   e. Geben Sie bei der FTP-Eingabeaufforderung Folgendes ein:
      `quit`

9. Erstellen Sie auf der iSeries B eine verdeckte Datei.

   Diese wird für die KDC-Authentifizierung beim Neustart und bei anderen Gelegenheiten verwendet.

   Führen Sie die folgenden Schritte durch, um die verdeckte Datei zu erstellen:

   a. Geben Sie in einer zeichenorientierten Schnittstelle auf der iSeries B `call QP2TERM` ein.

Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.

b. Geben Sie in der Befehlszeile Folgendes ein:
```
export PATH=$PATH:/usr/krb5/sbin
```
Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.

c. Geben Sie in der Befehlszeile Folgendes ein:
```
kdb5_util stash
```
Sie werden aufgefordert, das Hauptkennwort für die Datenbank einzugeben.

10. Starten Sie den KDC-Dämon auf der iSeries B.

Es gibt zwei Möglichkeiten, diesen Dämon zu starten. Er kann manuell oder bei jedem IPL des Systems automatisch gestartet werden. Die folgenden Informationen enthalten Anweisungen für beide Möglichkeiten.

**KDC-Dämon manuell starten**

Um den KDC-Dämon auf der iSeries B zu starten, geben Sie `start.krb5 krb5kdc` in der Befehlszeile der interaktiven Shell-Umgebung QP2TERM ein.

**KDC-Dämon für automatisches Starten konfigurieren**

Wahlweise können Sie den KDC-Dämon für ein automatisches Starten während eines IPL konfigurieren. Dazu müssen Sie folgendermaßen eine Jobbeschreibung erstellen und den Eintrag für den automatisch zu startenden Job hinzufügen:

a. Geben Sie in der i5/OS-Befehlszeile den nachfolgenden Befehl ein. *xxxxxx* ist das i5/OS-Benutzerprofil mit der Berechtigung *ALLOBJ.
```
CRTJOBD JOBD(QGPL/KRB5KDC)
JOBQ(QSYS/QSYSNOMAX) TEXT('KDC-Dämon krb5 starten') USER(xxxxxx) RQSDTA('QSYS/CALL
PGM(QSYS/QP2SHELL) PARM(''/usr/krb5/sbin/start.krb5 krb5kdc'')') SYNTAX(*NOCHK)
INLLIBL(*SYSVAL) ENDSEV( 30)
```

b. Geben Sie in der Befehlszeile Folgendes ein:
```
ADDAJE SBSD(QSYS/QSYSWRK) JOB(KRB5KDC) JOBD(QGPL/KRB5KDC)
```

**Anmerkung:** Auf dem sekundären Kerberos-Server wird nur der Kerberos-Server (krb5kdc) ausgeführt, nicht der Verwaltungsserver (kadmin).

11. Ändern Sie den Client so, dass er den sekundären Kerberos-Server verwendet.

Wenn der iSeries-Client (iSeries C) den sekundären Kerberos-Server zur Authentifizierung verwenden soll, müssen die Eigenschaften auf der iSeries C geändert werden. Führen Sie die folgenden Schritte durch, um den Client so zu ändern, dass er den sekundären Kerberos-Server verwenden kann:

a. Erweitern Sie im iSeries Navigator **iSeries C** → **Sicherheit** → **Netzwerkauthentifizierungsservice** → **Realms**.

b. Klicken Sie im rechten Teilfenster mit der rechten Maustaste auf **MY.COM** und wählen Sie **Eigenschaften** aus.

c. Geben Sie auf der Seite **Allgemein** den Wert `iseriesb.myco.com` im Feld **KDC** und `88` im Feld **Port** ein. Klicken Sie auf **Hinzufügen**. Klicken Sie auf **OK**.

## Netzwerkauthentifizierungsservice konfigurieren

Bevor Sie den Netzwerkauthentifizierungsservice konfigurieren, sollten Sie die folgenden Tasks ausführen:

- Füllen Sie alle erforderlichen Planungsarbeitsblätter aus.
- Wenn Ihre PCs und iSeries-Systeme die Hostnamensauflösung durchführen, stellen Sie sicher, dass sie dieselben Hostnamen für Ihre iSeries-Systeme auflösen. Weitere Informationen zu dieser Task finden Sie unter „Hinweise zur Auflösung von Hostnamen" auf Seite 95.

- Konfigurieren Sie einen Kerberos-Server auf einem sicheren System in Ihrem Netzwerk. Wenn Sie einen Kerberos-Server in i5/OS PASE konfiguriert haben, vergewissern Sie sich, dass Sie alle erforderlichen Konfigurationsschritte für die Server- und Client-Workstations ausgeführt haben, bevor Sie die Netzwerkauthentifizierung auf dem iSeries-Server konfigurieren. Einzelheiten zur Konfiguration eines Kerberos-Servers in i5/OS PASE finden Sie unter „Kerberos-Server in i5/OS PASE konfigurieren" auf Seite 104.

  Sie können einen Kerberos-Server auch auf dem Microsoft Windows 2000-Server und dem Windows-Server 2003 sowie auf z/OS konfigurieren. Informationen dazu finden Sie in der entsprechenden Dokumentation zur Kerberos-Konfiguration für das System, das als Kerberos-Server dienen soll.

  Es wird empfohlen, den Kerberos-Server vor dem Netzwerkauthentifizierungsservice auf der iSeries zu konfigurieren.

Führen Sie die folgenden Schritte durch, um den Netzwerkauthentifizierungsservice zu konfigurieren:

1. Erweitern Sie im iSeries Navigator **Ihren iSeries-Server** → **Sicherheit**.
2. Klicken Sie mit der rechten Maustaste auf **Netzwerkauthentifizierungsservice** und wählen Sie **Konfigurieren** aus, um den Konfigurationsassistenten zu starten. **Anmerkung:** Nachdem der Netzwerkauthentifizierungsservice konfiguriert wurde, lautet diese Auswahl **Rekonfigurieren**.
3. Informieren Sie sich auf der **Begrüßungsseite** darüber, welche Objekte vom Assistenten erstellt werden. Klicken Sie auf **Weiter**.
4. Geben Sie auf der Seite **Realm-Informationen angeben** im Feld **Standard-Realm** den Namen des Standard-Realms ein. Wenn Sie das Microsoft Active Directory für die Kerberos-Authentifizierung verwenden, wählen Sie **Microsoft Active Directory wird für Kerberos-Authentifizierung verwendet** aus. Klicken Sie auf **Weiter**.
5. Geben Sie auf der Seite **KDC-Informationen angeben** den Namen des Kerberos-Servers für diesen Realm im Feld **KDC** und 88 im Feld **Port** ein. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Kennwortserverinformationen angeben** entweder **Ja** oder **Nein** für die Definition eines Kennwortservers aus. Mit dem Kennwortserver können Principals Kennwörter auf dem Kerberos-Server ändern. Wenn Sie **Ja** auswählen, geben Sie den Namen des Kennwortservers im Feld **Kennwortserver** ein. Der Standardport für den Kennwortserver ist 464. Klicken Sie auf **Weiter**.
7. Wählen Sie auf der Seite **Chiffrierschlüsseleinträge auswählen** die **i5/OS Kerberos-Authentifizierung** aus. Sie können außerdem Chiffrierschlüsseleinträge für den Verzeichnisservice (LDAP), iSeries NetServer und iSeries HTTP-Server erstellen, wenn diese Services die Kerberos-Authentifizierung verwenden sollen.

   **Anmerkung:** In diesem Fall sind für einige dieser Services zusätzliche Konfigurationsschritte erforderlich.

   Klicken Sie auf **Weiter**.
8. Geben Sie auf der Seite **i5/OS-Chiffrierschlüsseleintrag erstellen** ein Kennwort ein und bestätigen Sie es. Klicken Sie auf **Weiter**. **Anmerkung:** Dieses Kennwort verwenden Sie auch, wenn Sie die i5/OS-Principals zum Kerberos-Server hinzufügen.
9. Wählen Sie **Ja** auf der Seite **Stapeldatei erstellen** aus.

   **Anmerkung:** Diese Seite wird nur angezeigt, wenn Sie in Schritt 4 oben **Microsoft Active Directory wird für Kerberos-Authentifizierung verwendet** ausgewählt haben.
10. Aktualisieren Sie im Feld **Stapeldatei** den Verzeichnispfad. Sie können auf **Durchsuchen** klicken, um den entsprechenden Verzeichnispfad zu lokalisieren, und den Pfad in dem Feld editieren.
11. Wählen Sie **Ja** im Feld **Kennwort einfügen** aus. Dies garantiert, dass alle Kennwörter, die dem i5/OS-Service-Principal zugeordnet sind, in die Stapeldatei eingefügt werden. Beachten Sie, dass Kennwörter in Klartext angezeigt werden und von jedem gelesen werden können, der über den Lesezugriff für die Stapeldatei verfügt.

    **Anmerkung:** Sie können dem Microsoft Active Directory auch manuell die vom Assistenten generierten Service-Principals hinzufügen. Unter „Dem Kerberos-Server i5/OS-Principals

hinzufügen" wird erläutert, wie die i5/OS-Service-Principals manuell dem Microsoft Active Directory hinzugefügt werden.

12. Überprüfen Sie die Konfigurationsdetails für den Netzwerkauthentifizierungsservice auf der Seite **Zusammenfassung**. Klicken Sie auf **Fertig stellen**.

Der Netzwerkauthentifizierungsservice ist jetzt konfiguriert.

**Die weiteren Schritte**

„Dem Kerberos-Server i5/OS-Principals hinzufügen"

## Dem Kerberos-Server i5/OS-Principals hinzufügen

Nachdem Sie den Netzwerkauthentifizierungsservice auf Ihrer iSeries konfiguriert haben, müssen Sie Ihre i5/OS-Principals zum Kerberos-Server hinzufügen. Der Netzwerkauthentifizierungsservice stellt den i5/OS-Principal-Namen **krbsvr400** für den Server und die i5/OS-Anwendungen zur Verfügung. Der Name des Principals, der i5/OS repräsentiert, lautet krbsrv400/*iSeries Hostname*@REALM-NAME, wobei *iSeries Hostname* entweder der vollständig qualifizierte Hostname oder die Kurzform des Hostnamens für den iSeries-Server ist. Dieser Principal-Name muss dem Kerberos-Server hinzugefügt werden, damit Kerberos-Clientantwendungen Service-Tickets anfordern und empfangen können. In den Konfigurationsszenarios hat beispielsweise der Administrator für MyCo den Service-Principal krbsvr400/iseriesa.myco.com@MYCO.COM zum Kerberos-Server des Unternehmens hinzugefügt.

Die Vorgehensweise beim Hinzufügen des i5/OS-Principals richtet sich danach, unter welchem Betriebssystem der Kerberos-Server konfiguriert wurde. Die folgenden Anweisungen betreffen das Hinzufügen des i5/OS-Principals zu einem Kerberos-Server in i5/OS PASE oder einer Windows 2000-Domäne. Wenn wahlweise außerdem Service-Principals für IBM Directory Server für iSeries (LDAP), iSeries NetServer oder HTTP-Server erstellt wurden, müssen auch diese dem Kerberos-Server hinzugefügt werden.

### i5/OS PASE

Wenn sich der Kerberos-Server in i5/OS PASE befindet, können Sie i5/OS-Service-Principals mit dem Befehl QP2TERM hinzufügen. Dieser öffnet eine interaktive Shell-Umgebung, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht. Führen Sie die folgenden Schritte durch, um einen i5/OS-Service-Principal zu einem Kerberos-Server in i5/OS PASE hinzuzufügen:

1. Geben Sie in einer zeichenorientierten Schnittstelle call QP2TERM ein.
2. Geben Sie in der Befehlszeile `export PATH=$PATH:/usr/krb5/sbin` ein. Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.
3. Geben Sie in der Befehlszeile kadmin -p admin/admin ein.
4. Melden Sie sich mit Ihrem Benutzernamen und Kennwort an.
5. Geben Sie in der kadmin-Befehlszeile `addprinc -pw secret krbsvr400/iSeries vollständig qualifizierter Hostname@REALM ein`, wobei `secret` das Kennwort für den i5/OS-Service-Principal ist. Beispiel: `krbsvr400/iseriesa.myco.com@MYCO.COM` könnte ein gültiger Name für einen i5/OS-Service-Principal sein.

### Microsoft Windows Active Directory

Sie haben zwei Möglichkeiten, um einen i5/OS-Service-Principal zu einem Kerberos-Server hinzuzufügen: Mit dem Assistenten für den Netzwerkauthentifizierungsservice oder manuell.

Mit dem Assistenten für den Netzwerkauthentifizierungsservice können Sie wahlweise eine Stapeldatei mit dem Namen `NASConfig.bat` erstellen. Diese enthält alle Principal-Namen für die Services, die Sie während der Konfiguration ausgewählt haben. Die zugehörigen Kennwörter können Sie ebenfalls in die Stapeldatei einfügen.

**Anmerkung:** Wenn Sie die Kennwörter einfügen, können diese von jedem gelesen werden, der über den Lesezugriff für die Stapeldatei verfügt. Es wird daher empfohlen, die Stapeldatei sofort nach Gebrauch wieder vom Kerberos-Server und Ihrem PC zu löschen. Wenn Sie keine Kennwörter in die Stapeldatei einfügen, werden Sie zur Eingabe eines Kennworts aufgefordert, wenn die Stapeldatei auf dem Windows-Server ausgeführt wird.

**Vom Assistenten generierte Stapeldatei verwenden**

1. Öffnen Sie auf der Windows 2000-Workstation, die der Administrator zur Konfiguration des Netzwerkauthentifizierungsservice verwendet hat, eine Eingabeaufforderung und geben Sie `ftp Server` ein, wobei *Server* der Hostname für den Kerberos-Server ist. 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 bei der FTP-Eingabeaufforderung `lcd "C:\Documents and Settings\All Users\Documents\IBM\Client Access"` ein. Drücken Sie die Eingabetaste.

   **Anmerkung:** Dies ist ein Beispiel für ein Verzeichnis, das die Stapeldatei enthalten könnte. Daraufhin sollte die Nachricht `Lokales Verzeichnis jetzt C:\Documents and Settings\All Users\Documents\IBM\Client Access` angezeigt werden.
3. Geben Sie bei der FTP-Eingabeaufforderung `binary` ein. Das bedeutet, dass es sich bei der zu übertragenden Datei um eine Binärdatei handelt.
4. Geben Sie bei der FTP-Eingabeaufforderung `cd \mydirectory` ein, wobei *mydirectory* ein Verzeichnis auf dem Windows-Server ist, auf dem die Stapeldatei gespeichert werden soll.
5. Geben Sie bei der FTP-Eingabeaufforderung `put NASConfig.bat` ein. Daraufhin sollte die Nachricht: `226 Übertragung abgeschlossen` (oder ähnlicher Wortlaut) angezeigt werden.
6. Öffnen Sie auf dem Windows 2000-Server das Verzeichnis, in das die Stapeldatei übertragen wurde.
7. Lokalisieren Sie die Datei `NASConfig.bat` und führen Sie sie durch Doppelklicken aus.
8. Überprüfen Sie im Anschluss, ob der i5/OS-Principal-Name dem Microsoft Windows Active Directory hinzugefügt wurde. Führen Sie dazu die folgenden Schritte durch:
   a. Erweitern Sie auf dem Windows 2000-Server **Start** → **Programme** → **Verwaltungstools** → **Active Directory-Benutzer und -Computer** → **Benutzer**.
   b. Vergewissern Sie sich, dass die iSeries über ein Benutzerkonto verfügt, indem Sie die entsprechende Windows 2000-Domäne auswählen.

      **Anmerkung:** Diese Windows-Domäne muss mit dem Namen des Standard-Realms übereinstimmen, den Sie bei der Konfiguration des Netzwerkauthentifizierungsservice angegeben haben.
   c. Suchen Sie aus der angezeigten Benutzerliste den Namen heraus, der dem soeben hinzugefügten Service-Principal entspricht.
   d. (Optional) Rufen Sie die Eigenschaften Ihrer Active Directory-Benutzer auf. Wählen Sie auf der Indexzunge **Konto** den Eintrag **Konto wird für Delegierungszwecke vertraut** aus.

      **Anmerkung:** Dieser optionale Schritt ermöglicht Ihrem System, den Berechtigungsnachweis 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.

**Service-Principal manuell dem Microsoft Windows Active Directory hinzufügen**

Sie können dem Microsoft Windows Active Directory i5/OS-Principals auch manuell hinzufügen. Verwenden Sie dazu den Befehl ktpass. Dieser Befehl wird mit den Windows-Unterstützungstools ausgeliefert und muss auf dem System installiert werden, das als Kerberos-Server dient.

1. Erweitern Sie auf dem Windows 2000-Server **Start → Programme → Verwaltungstools → Active Directory-Benutzer und -Computer**.
2. Wählen Sie die Windows 2000-Domäne aus, zu der Sie das iSeries-Benutzerkonto hinzufügen möchten, und erweitern Sie **Aktion → Neu → Benutzer**.

   **Anmerkung:** Diese Windows 2000-Domäne sollte mit dem Namen des Standard-Realms übereinstimmen, den Sie bei der Konfiguration des Netzwerkauthentifizierungsservice angegeben haben.
3. Geben Sie im Feld **Name** einen Namen ein, der die iSeries für diese Windows 2000-Domäne identifiziert. Damit wird ein neues Benutzerkonto für die iSeries hinzugefügt. Sie könnten beispielsweise den Namen `krbsvr400iseriesa` oder `httpiseriesa` als gültiges Benutzerkonto eingeben.
4. Greifen Sie auf die Eigenschaften des Active Directory-Benutzers zu, den Sie in Schritt 3 erstellt haben. Wählen Sie auf der Indexzunge **Konto** den Eintrag **Konto wird für Delegierungszwecke vertraut** aus. Damit wird dem i5/OS-Service-Principal der Zugriff auf andere Services im Namen eines angemeldeten Benutzers gestattet.
5. Sie müssen das soeben erstellte Benutzerkonto mit dem Befehl **ktpass** dem i5/OS-Service-Principal zuordnen. Das Tool ktpass befindet sich im Ordner **Servicetools** auf der Installations-CD für Windows (R) 2000-Server. Führen Sie folgende Task durch, um das Benutzerkonto zuzuordnen:
   a. Geben Sie bei einer Eingabeaufforderung Folgendes ein:

      ```
      ktpass -mapuser krbsvr400iseriesa -pass secret -princ krbsvr400/iseries-domain-name@REALM
          -mapop set
      ```

      **Anmerkung:** `krbsvr400iseriesa` steht für den Namen des Benutzerkontos, der in Schritt 3 erstellt wurde, und `secret` ist das Kennwort, das Sie bei der Konfiguration des Netzwerkauthentifizierungsservice für den i5/OS-Principal eingegeben haben.

**Die weiteren Schritte**

„Ausgangsverzeichnis erstellen"

## Ausgangsverzeichnis erstellen

Nachdem Sie den i5/OS-Principal zum Kerberos-Server hinzugefügt haben, müssen Sie für jeden Benutzer, der eine Verbindung zu i5/OS-Anwendungen herstellt, ein Ausgangsverzeichnis (`/home`) erstellen. Dieses Verzeichnis enthält den Namen des Kerberos-Cache für Berechtigungsnachweise, der dem Benutzer zugeordnet ist. Jeder Benutzer sollte entweder Eigner seines Verzeichnisses sein oder über die entsprechende Berechtigung zum Erstellen von Dateien in seinem Verzeichnis verfügen.

Gehen Sie folgendermaßen vor, um ein Ausgangsverzeichnis für einen Benutzer zu erstellen:

Geben Sie in einer i5/OS-Befehlszeile `CRTDIR '/home/Benutzerprofil'` ein, wobei `Benutzerprofil` das i5/OS-Benutzerprofil des Benutzers ist.

**Anmerkung:** Soll dieses Benutzerprofil als EIM-Zielzuordnung verwendet werden, muss das Benutzerprofil vorhanden sein, und das Kennwort kann auf *NONE gesetzt werden.

**Die weiteren Schritte**

„Netzwerkauthentifizierungsservice testen" auf Seite 117

### Netzwerkauthentifizierungsservice testen

Nachdem Sie die Ausgangsverzeichnisse für jeden Benutzer erstellt haben, der eine Verbindung zu den i5/OS-Anwendungen herstellt, können Sie die Konfiguration des Netzwerkauthentifizierungsservice testen, indem Sie ein Ticket-granting Ticket für Ihren i5/OS-Principal anfordern. Bevor Sie dies tun, sollten Sie sich jedoch vergewissern, ob Sie die folgenden Bedingungen erfüllt haben:

- Sind alle Voraussetzungen für den Netzwerkauthentifizierungsservice erfüllt?
- Ist auf der iSeries ein Ausgangsverzeichnis für den Benutzer vorhanden, der das Ticket anfordert? Einzelheiten hierzu finden Sie unter „Ausgangsverzeichnis erstellen" auf Seite 116.
- Liegt Ihnen das richtige Kennwort für den i5/OS-Principal vor? Dieses Kennwort wurde bei der Konfiguration des Netzwerkauthentifizierungsservice erstellt und sollte in Ihren Planungsarbeitsblättern enthalten sein.
- Haben Sie den i5/OS-Principal zum Kerberos-Server hinzugefügt? Einzelheiten hierzu finden Sie unter „Dem Kerberos-Server i5/OS-Principals hinzufügen" auf Seite 114.

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

1. Geben Sie in einer Befehlszeile `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. Es sollten die folgenden Ergebnisse angezeigt werden:

```
Principal: krbsvr400/iseriesa.myco.com@MYCO.COM
  Key version: 2
  Key type: 56-bit DES using key derivation
  Entry timestamp: 200X/05/29-11:02:58
```

3. Geben Sie `kinit -k krbsvr400/vollständig qualifizierter Hostname@REALM-NAME` ein, um vom Kerberos-Server ein Ticket-granting Ticket anzufordern. krbsvr400/iseriesa.myco.com@MYCO.COM könnte beispielsweise ein gültiger Principal-Name für die iSeries sein. Mit diesem Befehl wird geprüft, ob Ihr iSeries-Server richtig konfiguriert wurde und das Kennwort in der Chiffrierschlüsseldatei mit dem auf dem Kerberos-Server gespeicherten Kennwort übereinstimmt. Wenn dies alles stimmt, wird der Befehl QSH ohne Fehler ausgeführt.
4. Geben Sie `klist` ein, um zu prüfen, ob der Standard-Principal krbsvr400/vollständig qualifizierter Hostname@REALM-NAME lautet. Mit diesem Befehl wird der Inhalt eines Kerberos-Cache für Berechtigungsnachweise angezeigt und geprüft, ob ein gültiges Ticket für den iSeries-Service-Principal erstellt und in den Cache für Berechtigungsnachweise auf dem iSeries-System aufgenommen wurde.

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

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

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

#### Die weiteren Schritte

Enterprise Identity Mapping (EIM) konfigurieren Dieser Schritt ist optional, wenn Sie den Netzwerkauthentifizierungsservice für Ihre eigenen Anwendungen verwenden. Er wird jedoch empfohlen, wenn Sie von IBM gelieferte Anwendungen verwenden, um eine Einzelanmeldungsumgebung zu erstellen.

## Netzwerkauthentifizierungsservice verwalten

Nachdem Sie den Netzwerkauthentifizierungsservice konfiguriert haben, können Sie Tickets anfordern, mit Chiffrierschlüsseldateien arbeiten und die Hostnamensauflösung verwalten. Sie können außerdem mit Dateien für Berechtigungsnachweise arbeiten und Konfigurationsdateien sichern. In den folgenden Abschnitten wird beschrieben, wie diese Tasks ausgeführt werden:

**Verwaltungstasks für den Netzwerkauthentifizierungsservice**

Im Folgenden finden Sie eine kurze Zusammenstellung der Tasks, die von einem Administrator im iSeries Navigator ausgeführt werden können. Weitere aufgabenbezogene Informationen finden Sie im iSeries Navigator-Hilfetext zum Netzwerkauthentifizierungsservice.

**Anmerkung:** Der Abschnitt „Haftungsausschluss für Programmcode" auf Seite 2 enthält wichtige rechtliche Hinweise.

- „Systemzeiten synchronisieren"
- „Realms hinzufügen" auf Seite 119
- „Realms löschen" auf Seite 119
- „Kerberos-Server zu Realm hinzufügen" auf Seite 120
- „Kennwortserver hinzufügen" auf Seite 120
- „Vertrauensbeziehung zwischen Realms aufbauen" auf Seite 120
- „Hostauflösung ändern" auf Seite 121
- „Einstellungen für Verschlüsselung hinzufügen" auf Seite 121
- „Realms in der DNS-Datenbank definieren" auf Seite 135
- „Realms im LDAP-Server definieren" auf Seite 137

**iSeries-Benutzertasks**

Die iSeries kann auch als Client in einem Kerberos-fähigen Netzwerk fungieren. Benutzer können sich bei der iSeries anmelden und Kerberos-bezogene Tasks über den Qshell-Interpreter ausführen. Für die folgenden allgemeinen Tasks, die von iSeries-Benutzern ausgeführt werden können, werden mehrere Qshell-Befehle verwendet.

**Anmerkung:** Wenn Sie den PC5250-Emulator im iSeries Navigator verwenden, müssen Sie den Systemwert für **Ferne Anmeldung** ändern, damit Sie die Anmeldung umgehen können. Gehen Sie folgendermaßen vor, um den Systemwert für **Ferne Anmeldung** zu ändern:

1. Erweitern Sie im iSeries Navigator **iSeries-Server** → **Konfiguration und Service** → **Systemwerte** → **Anmeldung**.
2. Wählen Sie auf der Seite **Fern** die Einträge **Umgehen der Anmeldung zulassen** und **Quellen- und Zielbenutzer-IDs müssen übereinstimmen** aus und klicken Sie auf **OK**.

- „Ausgangsverzeichnis erstellen" auf Seite 116
- „Ticket-granting Tickets anfordern oder verlängern" auf Seite 122
- „Kerberos-Kennwörter ändern" auf Seite 129
- „Chiffrierschlüsseldateien verwalten" auf Seite 127
- „Verfallene Cachedateien für Berechtigungsnachweise löschen" auf Seite 131
- „Cache für Berechtigungsnachweise anzeigen" auf Seite 124
- „Kerberos-Service-Einträge in LDAP-Verzeichnissen verwalten" auf Seite 133

## Systemzeiten synchronisieren

Im Netzwerkauthentifizierungsservice beträgt der Standardwert für die maximal zulässige Differenz zwischen zwei Systemzeiten 5 Minuten (300 Sekunden). Die Differenz kann über die Eigenschaften des Netzwerkauthentifizierungsservice geändert werden.

Bevor Sie die Systemzeiten synchronisieren, stellen Sie die Systemzeit mithilfe des Systemwerts QTIMZON Ihrer Zeitzone entsprechend ein. Sie können die Systemzeiten synchronisieren, indem Sie die auf dem Kerberos-Server eingestellte Uhrzeit ändern oder die iSeries-Systemzeit mit dem Systemwert QTIME ändern. Damit die Systemzeiten in einem Netzwerk synchronisiert bleiben, sollten Sie jedoch in jedem

Fall Simple Network Time Protocol (SNTP) konfigurieren. Mithilfe von SNTP können mehrere Systeme ihre Uhrzeit nach einem einzigen Zeitserver ausrichten. Gehen Sie folgendermaßen vor, um SNTP zu konfigurieren:

Um SNTP auf einer iSeries zu konfigurieren, geben Sie `CHGNTPA` in einer Befehlszeile ein.

Um SNTP auf Windows (R)-Systemen zu konfigurieren, zeigen Sie die Konfigurationsdaten für einen SNTP-Server mit **NET HELP TIME** an.

## Realms hinzufügen

Zu den Aufgaben des Netzwerkadministrators gehört das Hinzufügen eines neuen Realms zur Konfiguration des Netzwerkauthentifizierungsservice. Bevor Sie der iSeries-Konfiguration einen Realm hinzufügen können, muss der Kerberos-Server für den neuen Realm konfiguriert werden. Bevor Sie der iSeries-Netzwerkauthentifizierungsservicetask einen Realm hinzufügen können, benötigen Sie den Realm-Namen, den Namen des Kerberos-Servers und den Port, an dem er empfangsbereit ist.

Führen Sie die folgenden Schritte durch, um dem Netzwerkauthentifizierungsservice einen Realm hinzuzufügen:

1. Wählen Sie im iSeries Navigator **Ihren iSeries-Server → Sicherheit → Netzwerkauthentifizierungsservice** aus.
2. Klicken Sie mit der rechten Maustaste auf **Realms** und wählen Sie **Realm hinzufügen** aus.
3. Geben Sie im Feld **Hinzuzufügender Realm** den Hostnamen des Realms an, den Sie hinzufügen möchten. Ein gültiger Realm-Name wäre beispielsweise: MYCO.COM.
4. Geben Sie den Namen des Kerberos-Servers für den Realm, den Sie hinzufügen, im Feld **KDC** ein. Ein gültiger Name wäre beispielsweise: kdc1.myco.
5. Geben Sie die Portnummer ein, an der der Kerberos-Server für Anforderungen empfangsbereit ist. Gültige Portnummern liegen zwischen 1 und 65535. Der Standardport für den Kerberos-Server ist 88.
6. Klicken Sie auf **OK**.

## Realms löschen

Zu den Aufgaben des Netzwerkadministrators gehört das Löschen von Realms aus der Konfiguration des Netzwerkauthentifizierungsservice, wenn sie nicht mehr benötigt oder benutzt werden. Es kann auch vorkommen, dass ein Standard-Realm entfernt werden muss, um den Systembetrieb nach einem iSeries-nativen Anwendungsproblem wiederherzustellen.

Beispiel: Wenn Sie den Netzwerkauthentifizierungsservice konfiguriert haben, ohne den Kerberos-Server im Netzwerk einzurichten, gehen QFileSvr.400 und Distributed Data Management (DDM) davon aus, dass Sie die Kerberos-Authentifizierung verwenden. Bevor Sie die Authentifizierung für die genannten Produkte einrichten, sollten Sie den Standard-Realm löschen, den Sie bei der Konfiguration des Netzwerkauthentifizierungsservice angegeben haben.

Führen Sie die folgenden Schritte durch, um einen Realm für den Netzwerkauthentifizierungsservice zu löschen:

1. Erweitern Sie im iSeries Navigator **Ihren iSeries-Server → Sicherheit → Netzwerkauthentifizierungsservice → Realms**.
2. Klicken Sie mit der rechten Maustaste auf den Namen des Realms, den Sie löschen möchten, und wählen Sie **Löschen** aus.
3. Klicken Sie auf **OK**, um die Auswahl zu bestätigen.

## Kerberos-Server zu Realm hinzufügen

Als Netzwerkadministrator können Sie einen Kerberos-Server einem Realm hinzufügen, für den der Netzwerkauthentifizierungsservice verwendet wird. Vorher müssen Sie jedoch den Namen des Servers kennen und wissen, an welchem Port er empfangsbereit ist.

Führen Sie die folgenden Schritte durch, um einem Realm eine Instanz zur Schlüsselverteilung (sprich: Kerberos-Server) hinzuzufügen:

1. Erweitern Sie im iSeries Navigator **Ihren iSeries-Server** —> **Sicherheit** —> **Netzwerkauthentifizierungsservice** —> **Realms**.
2. Klicken Sie mit der rechten Maustaste auf den Namen des Realms im rechten Teilfenster und wählen Sie **Eigenschaften** aus.
3. Geben Sie auf der Indexzunge **Allgemein** den Namen des Kerberos-Servers, der diesem Realm hinzugefügt werden soll, im Feld **KDC** ein. Der Kerberos-Server ist für alle Realms erforderlich. Eine gültige Eingabe wäre beispielsweise kdc2.myco.com.
4. Geben Sie die Portnummer ein, an der der Kerberos-Server für Anforderungen empfangsbereit ist. Gültige Portnummern liegen zwischen 1 und 65535. Der Standardport für den Kerberos-Server ist 88.
5. Klicken Sie auf **Hinzufügen**. Der neue Kerberos-Server erscheint in der Liste **Instanzen zur Schlüsselverteilung (KDC) für diesen Realm**.
6. Klicken Sie auf **OK**.

## Kennwortserver hinzufügen

Mithilfe des Kennwortservers können Kerberos-Principals ihr Kennwort ändern. Derzeit wird die optionale Konfiguration eines Kennwortservers nicht von i5/OS PASE unterstützt. Um Kennwörter für Principals auf einem i5/OS PASE-Kerberos-Server zu ändern, müssen Sie die PASE-Umgebung aufrufen (call QP2TERM) und den Befehl „kpasswd" auf Seite 130 eingeben. Anhand der folgenden Anweisungen können Sie die Konfiguration des Netzwerkauthentifizierungsservice aktualisieren, so dass sie auf einen zusätzlichen oder neuen Kennwortserver für den Standard-Realm zeigt. Führen Sie die folgenden Schritte durch, um einem Realm einen Kennwortserver hinzuzufügen:

1. Erweitern Sie im iSeries Navigator **Ihren iSeries-Server** —> **Sicherheit** —> **Netzwerkauthentifizierungsservice** —> **Realms**.
2. Klicken Sie mit der rechten Maustaste auf den Namen des Realms im rechten Teilfenster und wählen Sie **Eigenschaften** aus.
3. Geben Sie auf der Indexzunge **Kennwortserver** den Namen des Kennwortservers ein. Ein gültiger Name wäre beispielsweise: psvr.myco.com.
4. Geben Sie die Portnummer für den Kennwortserver ein. Gültige Portnummern liegen zwischen 1 und 65535. Der Standardport für den Kennwortserver ist 464.
5. Klicken Sie auf **Hinzufügen**. Der neue Kennwortserver wird der Liste hinzugefügt.
6. Klicken Sie auf **OK**.

## Vertrauensbeziehung zwischen Realms aufbauen

Der Aufbau einer Vertrauensbeziehung ermöglicht dem Kerberos-Protokoll eine Verknüpfung mit der Authentifizierung. Diese Funktion ist optional, da das Kerberos-Protokoll standardmäßig die Realm-Hierarchie nach Vertrauensbeziehungen durchsucht. Diese Funktion bietet sich an, wenn Realms in unterschiedlichen Domänen vorhanden sind, und dieser Prozess beschleunigt werden soll. Um sichere Realms einzurichten, muss jeder Kerberos-Server für jeden Realm einen gemeinsamen Schlüssel benutzen. Bevor eine Vertrauensbeziehung innerhalb des Netzwerkauthentifizierungsservice aufgebaut werden kann, müssen die Kerberos-Server so konfiguriert werden, dass sie einander vertrauen. Führen Sie die folgenden Schritte durch, um eine Vertrauensbeziehung zwischen Realms aufzubauen:

1. Erweitern Sie im iSeries Navigator **Ihren iSeries-Server** —> **Sicherheit** —> **Netzwerkauthentifizierungsservice** —> **Realm**.

2. Klicken Sie mit der rechten Maustaste auf den Namen des Realms im rechten Teilfenster und wählen Sie **Eigenschaften** aus.
3. Geben Sie auf der Indexzunge **Sichere Realms** die Namen der Realms ein, zwischen denen Sie eine Vertrauensbeziehung aufbauen möchten. Gültige Namen für eine Vertrauensbeziehung wären beispielsweise: ORDEPT.MYCO.COM und SHIPDEPT.MYCO.COM.
4. Klicken Sie auf **Hinzufügen**. Damit wird die Vertrauensbeziehung der Tabelle hinzugefügt.
5. Klicken Sie auf **OK**.

## Hostauflösung ändern

Beim Netzwerkauthentifizierungsservice können ein LDAP-Server, ein Domain Name System (DNS) und statische Zuordnungen angegeben werden, die der Konfigurationsdatei hinzugefügt werden, um Host- und Realm-Namen aufzulösen. Es können auch alle drei Methoden ausgewählt werden, um Hostnamen aufzulösen. In diesem Fall überprüft der Netzwerkauthentifizierungsservice zuerst den Directory-Server, dann die DNS-Einträge und zum Schluss die statischen Zuordnungen, um Hostnamen aufzulösen.

Führen Sie die folgenden Schritte durch, um die Methode zur Hostnamensauflösung zu ändern:

1. Erweitern Sie im iSeries Navigator **Ihren iSeries-Server** —> **Sicherheit**.
2. Klicken Sie mit der rechten Maustaste auf **Netzwerkauthentifizierungsservice** und wählen Sie **Eigenschaften** aus.
3. Wählen Sie auf der Seite **Hostauflösung** entweder **LDAP-Suchfunktion verwenden**, **DNS-Suchfunktion verwenden** oder **Statische Zuordnungen verwenden** aus.
4. Wenn Sie für die Art der Hostauflösung **LDAP-Suchfunktion verwenden** auswählen, geben Sie den Namen des Directory-Servers und den entsprechenden Port ein. Beispielsweise wäre ldapsrv.myco-.com ein gültiger Name für den Directory-Server. Gültige Portnummern liegen zwischen 1 und 65535. Der Standardport für den Directory-Server ist 389.Nachdem Sie angegeben haben, dass ein LDAP-Server für die Hostnamensauflösung verwendet werden soll, müssen Sie sicherstellen, dass der Realm richtig in dem LDAP-Server definiert ist. Weitere Informationen finden Sie unter „Realms im LDAP-Server definieren" auf Seite 137.
5. Wenn Sie für die Art der Hostauflösung **DNS-Suchfunktion verwenden** auswählen, muss DNS für die Zuordnung von Realm-Namen konfiguriert sein. Nachdem Sie angegeben haben, dass ein DNS-Server für die Hostnamensauflösung verwendet werden soll, müssen Sie sicherstellen, dass der Realm richtig in dem DNS-Server definiert ist. Weitere Informationen finden Sie unter „Realms in der DNS-Datenbank definieren" auf Seite 135.
6. Wenn Sie für die Art der Hostauflösung **Statische Zuordnungen verwenden** auswählen, geben Sie den Realm-Namen und den entsprechenden DNS-Namen ein. Beispielsweise könnte der Hostname mypc.mycompanylan.com und der Realm-Name MYCO.COM lauten. Sie können einem bestimmten Realm auch generische Hostnamen zuordnen. Beispiel: Wenn alle Maschinen, die mit myco.lan.com enden, Mitglieder im Realm MYCO.COM sind, könnten Sie `myco.lan.com` als DNS-Name und MYCO-.COM als Realm eingeben. Dadurch wird in der Konfigurationsdatei eine Zuordnung zwischen dem Realm-Namen und dem DNS-Namen erstellt. Klicken Sie auf **Hinzufügen**, um eine statische Zuordnung zwischen dem DNS- und dem Realm-Namen in der Konfigurationsdatei zu erstellen.
7. Nachdem Sie die zugehörigen Informationen für die ausgewählte Art der Hostauflösung eingegeben haben, klicken Sie auf **OK**.

## Einstellungen für Verschlüsselung hinzufügen

Es können Verschlüsselungsarten für Ticket-granting Tickets (TGT) und Ticket-granting Service (TGS) ausgewählt werden. Die Verschlüsselung verdeckt Daten, die über ein Netzwerk gesendet werden, indem sie deren Identifizierung verhindert. Ein Client verschlüsselt Daten und der Server entschlüsselt sie. Um sicherzustellen, dass die Verschlüsselung richtig funktioniert, müssen Sie die dieselbe Verschlüsselungsart verwenden, die auf dem Kerberos-Server oder der anderen übertragenden Anwendung angegeben ist. Wenn diese Verschlüsselungsarten nicht übereinstimmen, findet keine Verschlüsselung statt. Sie können sowohl für TGT als auch für TGS Verschlüsselungswerte hinzufügen. **Anmerkung:** Die Standardver-

schlüsselungswerte für TGT und TGS lauten des-cbc-crc bzw. des-cbc-md5. Die Standardwerte werden bei der Konfiguration festgelegt. Sie können der Konfiguration andere Werte für Tickets hinzufügen, indem Sie die folgenden Schritte durchführen:

1. Erweitern Sie im iSeries Navigator **Ihren iSeries-Server** —> **Sicherheit**.
2. Klicken Sie mit der rechten Maustaste auf **Netzwerkauthentifizierungsservice** und wählen Sie **Eigenschaften** aus.
3. Wählen Sie auf der Seite **Tickets** den Verschlüsselungswert aus der Liste der verfügbaren Verschlüsselungswerte für Ticket-granting Ticket oder Ticket-granting Service aus.
4. Klicken Sie entweder auf **Hinzufügen vor** oder **Hinzufügen nach**, um die Verschlüsselungsart der Liste der ausgewählten Verschlüsselungsarten hinzuzufügen. Jede der ausgewählten Verschlüsselungsarten wird entsprechend der Reihenfolge in der Liste ausprobiert. Wenn eine Verschlüsselungsart nicht funktioniert, wird die nächste versucht.
5. Klicken Sie auf **OK**.

## Ticket-granting Tickets anfordern oder verlängern

Mit dem Befehl **kinit** wird ein Kerberos Ticket-granting Ticket angefordert oder verlängert. Wird der Befehl **kinit** ohne Ticketoptionen angegeben, gelten die in der Kerberos-Konfiguration angegebenen Optionen für den Kerberos-Server.

Wird ein vorhandenes Ticket nicht mehr verlängert, wird der Cache für Berechtigungsnachweise erneut initialisiert und erhält das neue, vom Kerberos-Server empfangene Ticket-granting Ticket. Wird in der Befehlszeile kein Principal-Name angegeben, wird der Name dem Cache für Berechtigungsnachweise entnommen. Der neue Cache für Berechtigungsnachweise wird zum Standardcache für Berechtigungsnachweise, es sei denn, der Cachename wird über die Option `-c` angegeben.

Ticket-Zeitwerte werden im Format *nwndnhnmns* ausgedrückt, wobei *n* für eine Zahl, *w* für Wochen, *d* für Tage, *h* für Stunden, *m* für Minuten und *s* für Sekunden steht. Die Komponenten müssen zwar in der genannten Reihenfolge angegeben werden, einzelne Komponenten können aber weggelassen werden (*4h5m* steht beispielsweise für 4 Stunden und 5 Minuten, *1w2h* für 1 Woche und 2 Stunden). Wird nur eine Zahl angegeben, gilt ″Stunden″ als Standardwert.

Führen Sie die folgenden Schritte durch, um ein Ticket-granting Ticket mit einer Laufzeit von 5 Stunden für Principal jday anzufordern:

Geben Sie in der Qshell-Befehlszeile Folgendes ein:

```
kinit -l 5h Jday
```

Oder

Geben Sie in einer i5/OS-Befehlszeile für die Steuersprache (CL) Folgendes ein:

```
call qsys/qkrbkinit parm('-l' '5h' 'jday')
```

Die Anmerkungen zur Verwendung von kinit enthalten weitere Informationen über das Format und die für diesen Qshell-Befehl geltenden Einschränkungen.

### kinit

**Syntax**

```
kinit [-r Zeit] [-R] [-p] [-f] [-A] [-l Zeit] [-c Cache] [-k] [-t Chiffrierschlüssel]
[Principal]
```

Standardwert für allgemeine Berechtigung: *USE

Mit dem Qshell-Befehl **kinit** wird ein Kerberos Ticket-granting Ticket angefordert oder erneuert.

### Optionen

**-r Zeit** Das Zeitintervall für die Erneuerung eines Tickets. Nach Ablauf dieses Intervalls kann das Ticket nicht mehr erneuert werden. Diese Erneuerungszeit muss größer sein als die Endzeit. Wird diese Option nicht angegeben, ist das Ticket nicht erneuerbar (dennoch kann weiterhin ein erneuerbares Ticket generiert werden, sofern die angeforderte Laufzeit die maximale Laufzeit des Tickets übersteigt).

**-R** Ein vorhandenes Ticket soll erneuert werden. Wenn Sie ein vorhandenes Ticket erneuern, können Sie keine weiteren Ticketoptionen angeben.

**-p** Das Ticket kann ein Proxy sein. Wird diese Option nicht angegeben, kann das Ticket kein Proxy sein.

**-f** Das Ticket kann weitergeleitet werden. Wird diese Option nicht angegeben, kann das Ticket nicht weitergeleitet werden.

**-A** Das Ticket enthält keine Liste mit Clientadressen. Wird diese Option nicht angegeben, enthält das Ticket eine Liste mit den lokalen Hostadressen. Wenn ein ursprüngliches Ticket eine Adressliste enthält, kann es nur an einer der in dieser Liste enthaltenen Adressen verwendet werden.

**-l Zeit** Das Endzeitintervall für das Ticket. Wenn dieses Intervall abgelaufen ist, kann das Ticket nicht mehr verwendet werden, es sei denn, es wird erneuert. Wird diese Option nicht angegeben, wird das Intervall auf 10 Stunden gesetzt.

**-c Cache** Der Name des Cache für Berechtigungsnachweise, der vom Befehl kinit verwendet wird. Wird diese Option nicht angegeben, verwendet der Befehl den Standardcache für Berechtigungsnachweise.

**-k** Der Schlüssel für den Ticket-Principal wird einer Schlüsseltabelle entnommen. Wird diese Option nicht angegeben, werden Sie vom System zur Eingabe des Kennworts für den Ticket-Principal aufgefordert.

**-t Chiffrierschlüssel** Der Name der Schlüsseltabelle. Wird diese Option nicht angegeben, aber die Option `-k` angeben, verwendet das System die Standardschlüsseldatei. Die Option `-t` impliziert die Option `-k`.

**Principal** Der Ticket-Principal. Wird in der Befehlszeile kein Principal angegeben, wird der Principal dem Cache für Berechtigungsnachweise entnommen.

### Berechtigungen

| Referenzobjekt | Erforderliche Berechtigung |
|---|---|
| Jedes Verzeichnis im Pfadnamen, das der Chiffrierschlüsseldatei vorangeht, wenn die Option `-t` angegeben wird | *X |
| Chiffrierschlüsseldatei, wenn `-t` angegeben wird | *R |
| Jedes Verzeichnis im Pfadnamen, das dem zu verwendenden Cache für Berechtigungsnachweise vorangeht | *X |

| Referenzobjekt | Erforderliche Berechtigung |
|---|---|
| Parentverzeichnis der Cachedatei, wenn diese von der Umgebungsvariablen **KRB5CCNAME** angegeben und die Datei erstellt wird | *WX |
| Cachedatei für Berechtigungsnachweise | *RW |
| Jedes Verzeichnis in den Pfaden zu den Konfigurationsdateien | *X |
| Konfigurationsdateien | *R |

Damit zur Kerberos-Ausführungszeit die Cachedatei für Berechtigungsnachweise von jedem ausführenden Prozess gefunden werden kann, wird der Name der Cachedatei normalerweise im Ausgangsverzeichnis unter dem Dateinamen **krb5ccname** gespeichert. Die Speicherposition der Cachedatei kann durch Setzen der Umgebungsvariablen **_EUV_SEC_KRB5CCNAME_FILE** überschrieben werden. Um auf diese Datei zugreifen zu können, benötigt das Benutzerprofil die Berechtigung ***X** für jedes Verzeichnis im Pfad und die Berechtigung ***R** für die Datei, in der der Cachename gespeichert ist. Wenn der Benutzer erstmalig einen Cache für Berechtigungsnachweise erstellt, benötigt das Benutzerprofil die Berechtigung ***WX** für das Parentverzeichnis.

**Nachrichten**

- Für die Option `Optionsname` ist ein Wert erforderlich.
- `Befehlsoption` ist keine gültige Befehlsoption.
- Beim Erneuern oder Überprüfen von Tickets sind keine Optionen zulässig.
- Name des Standardcaches für Berechtigungsnachweise kann nicht abgerufen werden.
- Cache für Berechtigungsnachweise `Dateiname` kann nicht aufgelöst werden.
- Kein ursprüngliches Ticket verfügbar.
- Name des Principals muss angegeben werden.
- Ticket kann nicht aus Cache für Berechtigungsnachweise `Dateiname` abgerufen werden.
- Ursprüngliches Ticket ist nicht erneuerbar.
- Option `Optionswert` ist für Anforderung `Anforderungsname` nicht gültig.
- Ursprüngliche Berechtigungsnachweise können nicht abgerufen werden.
- Name des Principals kann nicht syntaktisch analysiert werden.
- Chiffrierschlüsseltabelle `Dateiname` kann nicht aufgelöst werden.
- Kennwort für `Principal-Name` ist falsch.
- Kennwort kann nicht gelesen werden.
- Ursprüngliche Berechtigungsnachweise können nicht im Cache für Berechtigungsnachweise `Dateiname` gespeichert werden.
- Der Zeitdeltawert ist ungültig.

Unter „Ticket-granting Tickets anfordern oder verlängern” auf Seite 122 finden Sie ein Beispiel für die Verwendungsweise dieses Befehls.

## Cache für Berechtigungsnachweise anzeigen

Mit dem Befehl **klist** wird der Inhalt eines Kerberos-Cache für Berechtigungsnachweise angezeigt.

Führen Sie die folgenden Schritte durch, um alle Einträge im Standardcache für Berechtigungsnachweise aufzulisten und die Ticketmarkierungen anzuzeigen:

Geben Sie in einer Qshell-Befehlszeile Folgendes ein:

```
klist -f -a
```

Oder

Geben Sie in einer i5/OS-Befehlszeile für die Steuersprache (CL) Folgendes ein:

```
call qsys/krbklist parm('-f' '-a')
```

Die Hinweise zur Verwendung von klist enthalten weitere Informationen über das Format und die für diesen Qshell-Befehl geltenden Einschränkungen.

## klist

**Syntax**

```
klist [-a] [-e] [-c] [-f] [-s] [-k] [-t] [-K] [Dateiname]
```

Standardwert für allgemeine Berechtigung: *USE

Mit dem Befehl **klist** wird der Inhalt eines Kerberos-Cache für Berechtigungsnachweise oder einer Chiffrierschlüsseldatei angezeigt.

**Optionen**

**-a** Alle Tickets im Cache für Berechtigungsnachweise, einschließlich abgelaufener Tickets, anzeigen. Wird diese Option nicht angegeben, werden abgelaufene Tickets nicht aufgelistet. Diese Option ist nur gültig, wenn der Inhalt eines Cache für Berechtigungsnachweise aufgelistet wird.

**-e** Die Verschlüsselungsart für den Sitzungsschlüssel und das Ticket anzeigen. Diese Option ist nur gültig, wenn der Inhalt eines Cache für Berechtigungsnachweise aufgelistet wird.

**-c** Die Tickets in einem Cache für Berechtigungsnachweise auflisten. Wird weder die Option `-c` noch die Option `-k` angegeben, ist dies der Standardwert. Diese Option und die Option `-k` schließen sich gegenseitig aus.

**-f** Die Ticketmarkierungen unter Verwendung der folgenden Abkürzungen anzeigen:

| Abkürzung | Bedeutung |
|---|---|
| **F** | Ticket kann weitergeleitet werden |
| **f** | Weitergeleitetes Ticket |
| **P** | Ticket kann ein Proxy sein |
| **p** | Proxy-Ticket |
| **D** | Ticket kann rückdatiert werden |
| **d** | Rückdatiertes Ticket |
| **R** | Erneuerbares Ticket |
| **I** | Ursprüngliches Ticket |
| **i** | Ticket ungültig |
| **A** | Vorab-Authentifizierung verwendet |
| **O** | Server kann Delegierter sein |
| **C** | Transitliste vom Kerberos-Server überprüft |

Diese Option ist nur gültig, wenn der Inhalt eines Cache für Berechtigungsnachweise aufgelistet wird.

**-s** Befehlsausgabe unterdrücken, aber Exitstatus auf 0 setzen, wenn im Cache für Berechtigungsnachweise ein gültiges Ticket-granting Ticket gefunden wird. Diese Option ist nur gültig, wenn der Inhalt eines Cache für Berechtigungsnachweise aufgelistet wird.

**-k** Die Einträge einer Chiffrierschlüsseltabelle auflisten. Diese Option und die Option **-c** schließen sich gegenseitig aus.

**-t** Zeitmarken für Chiffrierschlüsseltabelleneinträge anzeigen. Diese Option ist nur gültig, wenn der Inhalt einer Chiffrierschlüsseltabelle aufgelistet wird.

**-K** Den Chiffrierschlüsselwert für jeden Tabelleneintrag anzeigen. Diese Option ist nur gültig, wenn der Inhalt einer Chiffrierschlüsseltabelle aufgelistet wird.

**Dateiname** Gibt den Namen des Cache für Berechtigungsnachweise oder der Chiffrierschlüsseltabelle an. Wird kein Dateiname angegeben, wird der Standardcache für Berechtigungsnachweise oder die Standardchiffrierschlüsseltabelle verwendet.

**Berechtigungen**

| **Referenzobjekt** | **Erforderliche Berechtigung** |
|---|---|
| Jedes Verzeichnis im Pfadnamen, das der Datei vorangeht, wenn die Option `-k` angegeben wird | *X |
| Chiffrierschlüsseldatei, wenn `-k` angegeben wird | *R |
| Jedes Verzeichnis im Pfadnamen, das dem Cache für Berechtigungsnachweise vorangeht, wenn die Option `-k` nicht angegeben wird | *X |
| Cache für Berechtigungsnachweise, wenn die Option `-k` nicht angegeben wird | *R |

Damit zur Kerberos-Ausführungszeit die Cachedatei für Berechtigungsnachweise von jedem laufenden Prozess gefunden werden kann, wird der Name der Cachedatei normalerweise im Ausgangsverzeichnis unter dem Dateinamen **krb5ccname** gespeichert. Die Speicherposition der Cachedatei kann durch Setzen der Umgebungsvariablen **_EUV_SEC_KRB5CCNAME_FILE** überschrieben werden. Um auf diese Datei zugreifen zu können, benötigt das Benutzerprofil die Berechtigung ***X** für jedes Verzeichnis im Pfad und die Berechtigung ***R** für die Datei, in der der Cachename gespeichert ist. Wenn der Benutzer erstmalig einen Cache für Berechtigungsnachweise erstellt, benötigt das Benutzerprofil die Berechtigung ***WX** für das Parentverzeichnis.

**Nachrichten**

- Für die Option `Optionsname` ist ein Wert erforderlich.
- `Befehlsoption` ist keine gültige Befehlsoption.
- `Befehlsoption eins` und `Befehlsoption zwei` können nicht gemeinsam angegeben werden.
- Kein Standardcache für Berechtigungsnachweise gefunden.
- Cache für Berechtigungsnachweise `Dateiname` kann nicht aufgelöst werden.
- Name des Principals kann nicht aus Cache für Berechtigungsnachweise `Dateiname` abgerufen werden.
- Ticket kann nicht aus Cache für Berechtigungsnachweise `Dateiname` abgerufen werden.
- Ticket kann nicht decodiert werden.
- Keine Standardchiffrierschlüsseltabelle gefunden.
- Chiffrierschlüsseltabelle `Dateiname` kann nicht aufgelöst werden.

Unter „Cache für Berechtigungsnachweise anzeigen" auf Seite 124 finden Sie ein Beispiel für die Verwendungsweise dieses Befehls.

## Chiffrierschlüsseldateien verwalten

Als Netzwerkadministrator sind Sie für die Verwaltung der Chiffrierschlüsseldatei, die auch als Schlüsseltabelle bezeichnet wird, auf dem iSeries-Server verantwortlich. Zur Verwaltung der Chiffrierschlüsseldatei und der zugehörigen Einträge können Sie entweder die zeichenorientierte Schnittstelle oder den iSeries Navigator verwenden:

**Chiffrierschlüsseldateien mit der zeichenorientierten Schnittstelle verwalten**

Mit dem Befehl keytab werden Schlüssel einer Schlüsseltabelle hinzugefügt, gelöscht oder aufgelistet.

Führen Sie die folgenden Schritte durch, um beispielsweise einen Schlüssel für den Service-Principal krbsvr400 auf dem Host kdc1.myco.com in Realm MYCO.COM hinzuzufügen:

Geben Sie in einer Qshell-Befehlszeile Folgendes ein:

```
keytab add krbsvr400/kdc1.myco.com@MYCO.COM
```

Oder

Geben Sie in einer i5/OS-Befehlszeile für die Steuersprache (CL) Folgendes ein:

```
call qsys/qkrbkeytab parm('add' 'krbsvr400/kdc1.myco.com@MYCO.COM')
```

Sie werden aufgefordert, das Kennwort einzugeben, das verwendet wurde, als der Service für den Kerberos-Server definiert wurde.

Die Hinweise zur Verwendung von „keytab" auf Seite 128 enthalten weitere Informationen über das Format und die für diesen Qshell-Befehl geltenden Einschränkungen.

**Chiffrierschlüsseldateien mit dem iSeries Navigator verwalten**

Sie können auch den iSeries Navigator verwenden, um der Schlüsseltabelle Chiffrierschlüsseleinträge hinzuzufügen.

Mithilfe des iSeries Navigator können Sie Chiffrierschlüsseleinträge für die folgenden Services hinzufügen:

- i5/OS Kerberos-Authentifizierung
- LDAP
- HTTP-Server (powered by Apache)
- iSeries NetServer

Führen Sie die folgenden Schritte durch, um der Chiffrierschlüsseldatei einen Chiffrierschlüsseleintrag hinzuzufügen:

1. Erweitern Sie im iSeries Navigator Ihren **iSeries-Server** → **Sicherheit**.
2. Klicken Sie mit der rechten Maustaste auf **Netzwerkauthentifizierungsservice** und wählen Sie **Chiffrierschlüssel verwalten...** aus. Damit wird ein Teil des Assistenten für den Netzwerkauthentifizierungsservice gestartet, der Ihnen das Hinzufügen von Chiffrierschlüsseleinträgen ermöglicht.
3. Wählen Sie auf der Seite **Chiffrierschlüsseleinträge auswählen** die Servicetypen aus, für die Chiffrierschlüsseleinträge hinzugefügt werden sollen. Beispiel: i5/OS-Kerberos-Authentifizierung. Klicken Sie auf **Weiter**.

4. Geben Sie auf der Seite **i5/OS-Chiffrierschlüsseleintrag erstellen** ein Kennwort ein und bestätigen Sie es. Dieses Kennwort sollte mit demjenigen übereinstimmen, das Sie verwenden, wenn Sie dem Kerberos-Server den zugeordneten Service-Principal hinzufügen. Falls Sie in Schritt 3 einen anderen Servicetyp, wie beispielsweise LDAP, HTTP-Server (powered by Apache) oder iSeries NetServer ausgewählt haben, werden außerdem Seiten angezeigt, auf denen Sie Chiffrierschlüsseleinträge für diese Services erstellen können.
5. Die Seite **Zusammenfassung** enthält die Liste der i5/OS-Services und Service-Principals, die der Chiffrierschlüsseldatei als Chiffrierschlüsseleinträge hinzugefügt werden.

## keytab

**Syntax**

```
keytab add principal [-p Kennwort] [-v Version] [-k Chiffrierschlüssel] keytab delete
principal [-v Version] [-k Chiffrierschlüssel] keytab list [Principal] [-k
Chiffrierschlüssel]
```

Standardwert für allgemeine Berechtigung: *USE

Mit dem Qshell-Befehl **keytab** wird eine Chiffrierschlüsseltabelle verwaltet.

**Optionen**

**-k** Der Name der Chiffrierschlüsseltabelle. Wird diese Option nicht angegeben, wird die Standardschlüsseltabelle verwendet.

**-p** Das Kennwort angeben. Wird diese Option nicht angegeben, werden die Benutzer zur Eingabe des Kennworts aufgefordert, wenn sie der Schlüsseltabelle einen Eintrag hinzufügen.

**-v** Die Versionsnummer des Schlüssels. Wird diese Option beim Hinzufügen eines Schlüssels nicht angegeben, wird die nächste Versionsnummer zugeordnet. Wird diese Option beim Löschen eines Schlüssels nicht angegeben, werden alle Schlüssel für den Principal gelöscht.

**Principal** Der Name des Principals. Wird diese Option beim Auflisten der Schlüsseltabelle nicht angegeben, werden alle Principals angezeigt.

**Berechtigungen**

| Referenzobjekt | Erforderliche Berechtigung |
|---|---|
| Jedes Verzeichnis im Pfadnamen, das der zu öffnenden Ziel-Chiffrierschlüsseldatei vorangeht | *X |
| Parentverzeichnis der Ziel-Chiffrierschlüsseldatei, wenn "add" angegeben wird und die Chiffrierschlüsseldatei noch nicht vorhanden ist | *WX |
| Chiffrierschlüsseldatei, wenn "list" angegeben wird | *R |
| Zielchiffrierschlüsseldatei, wenn "add" oder "delete" angegeben wird | *RW |
| Jedes Verzeichnis in den Pfaden zu den Konfigurationsdateien | *X |
| Konfigurationsdateien | *R |

**Nachrichten**

- *add*, *delete*, *list* oder *merge* angeben.

- *Befehlsoption* ist keine gültige Befehlsoption.
- *Befehlsoption eins* und *Befehlsoption zwei* können nicht gemeinsam angegeben werden.
- Option *Optionswert* ist für Anforderung *Anforderungsname* nicht gültig.
- Für die Option *Optionsname* ist ein Wert erforderlich.
- Name des Principals kann nicht syntaktisch analysiert werden.
- Der Name des Principals muss angegeben werden.
- Kennwort kann nicht gelesen werden.
- Keine Standardchiffrierschlüsseltabelle gefunden.
- Chiffrierschlüsseltabelle *Chiffrierschlüsseltabelle* kann nicht aufgelöst werden.
- Eintrag aus Chiffrierschlüsseltabelle *Chiffrierschlüsseltabelle* kann nicht gelesen werden.
- Eintrag aus Chiffrierschlüsseltabelle *Chiffrierschlüsseltabelle* kann nicht entfernt werden.
- Eintrag kann Chiffrierschlüsseltabelle *Chiffrierschlüsseltabelle* nicht hinzugefügt werden.
- Keine Einträge für Principal *Name des Principals* gefunden.
- Wert ist keine gültige Zahl.
- Die Schlüsselversion muss zwischen 1 und 255 liegen.
- Schlüsselversion *Schlüsselversion* für Principal *Name des Principals* nicht gefunden.

Unter „Chiffrierschlüsseldateien verwalten" auf Seite 127 finden Sie ein Beispiel für die Verwendungsweise dieses Befehls.

## Kerberos-Kennwörter ändern

Mit dem Befehl **kpasswd** wird das Kennwort für den angegebenen Kerberos-Principal mithilfe des Kennwortänderungsservice geändert. Sie müssen sowohl das aktuelle als auch das neue Kennwort für den Principal angeben. Der Kennwortserver wendet alle gültigen Kennwortrichtlinien auf das neue Kennwort an, bevor das bestehende geändert wird. Der Kennwortserver wird bei der Installation und Konfiguration des Kerberos-Servers konfiguriert. Weitere Informationen finden Sie in der Dokumentation zu diesem System.

**Anmerkung:** Von i5/OS PASE wird kein Kennwortserver unterstützt. Um ein Kennwort für einen Principal zu ändern, der auf dem Kerberos-Server gespeichert ist, müssen Sie die PASE-Umgebung aufrufen (call QP2TERM) und den Befehl kpasswd eingeben.

Der Name des Kennwortservers kann bei der Konfiguration des Netzwerkauthentifizierungsservice angegeben werden. Wenn bei der Konfiguration kein Name angegeben wurde, kann ein Kennwortserver hinzugefügt werden.

Es ist nicht zulässig, mit dem Befehl **kpasswd** das Kennwort für einen Ticket-granting Service-Principal (krbtgt/realm) zu ändern.

**Führen Sie die folgenden Schritte durch, um das Kennwort für den Standard-Principal zu ändern:**

Geben Sie in einer Qshell-Befehlszeile Folgendes ein:

```
kpasswd
```

Oder

Geben Sie in einer Befehlszeile Folgendes ein:

```
call qsys/qkrbkpsswd
```

**Führen Sie die folgenden Schritte durch, um das Kennwort für einen anderen Principal zu ändern:**

Geben Sie in einer Qshell-Befehlszeile Folgendes ein:

```
kpasswd jday@myco.com
```

**Führen Sie die folgenden Schritte durch, um das Kennwort für einen anderen Principal in i5/OS PASE zu ändern:**

1. Geben Sie in einer zeichenorientierten Schnittstelle `call QP2TERM` ein. Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.
2. Geben Sie in der Befehlszeile `export PATH=$PATH:/usr/krb5/sbin` ein. Dieser Befehl verweist auf die Kerberos-Scripts, die zur Ausführung der ausführbaren Dateien benötigt werden.
3. Geben Sie bei der QSH-Eingabeaufforderung `kadmin -p admin/admin` ein. Drücken Sie die Eingabetaste.
4. Melden Sie sich mit dem Benutzernamen und dem Kennwort des Administrators an.
5. Geben Sie `kpasswd jday@myco.com` ein. Sie werden aufgefordert, das Kennwort für diesen Principal zu ändern.

Oder

Geben Sie in einer Befehlszeile Folgendes ein:

```
call qsys/qkrbkpsswd parm ('jday@myco.com')
```

Weitere Informationen über die Verwendungsweise dieses Befehls finden Sie unter „kpasswd".

## kpasswd

**Syntax**

```
kpasswd [-A ] [Principal]
```

Standardwert für allgemeine Berechtigung: *USE

Mit dem Qshell-Befehl kpasswd wird das Kennwort für einen Kerberos-Principal geändert.

**Optionen**

**-A** Das von dem Befehl kpasswd verwendete ursprüngliche Ticket enthält keine Liste mit Clientadressen. Das Ticket enthält eine Liste mit lokalen Hostadressen, wenn diese Option nicht angegeben wird. Wenn ein ursprüngliches Ticket eine Adressliste enthält, kann es nur an einer der in dieser Liste enthaltenen Adressen verwendet werden.

**Principal**

Der Principal, dessen Kennwort geändert werden soll. Der Principal wird dem Standardcache für Berechtigungsnachweise entnommen, wenn der Principal nicht in der Befehlszeile angegeben wird.

**Nachrichten**

- Principal %3$s ist ungültig.
- Standardcache für Berechtigungsnachweise `Dateiname` kann nicht gelesen werden.
- Es ist kein Standardcache für Berechtigungsnachweise vorhanden.
- Ticket kann nicht aus Cache für Berechtigungsnachweise `Dateiname` abgerufen werden.
- Kennwort kann nicht gelesen werden.
- Kennwortänderung abgebrochen.
- Kennwort für `Principal-Name` ist falsch.
- Ursprüngliches Ticket kann nicht abgerufen werden.
- Anforderung zum Ändern des Kennworts fehlgeschlagen.

Unter „Kerberos-Kennwörter ändern" auf Seite 129 finden Sie ein Beispiel für die Verwendungsweise dieses Befehls.

## Verfallene Cachedateien für Berechtigungsnachweise löschen

Mit dem Befehl **kdestroy** wird eine Kerberos-Cachedatei für Berechtigungsnachweise gelöscht. Alte Berechtigungsnachweise müssen von den Benutzern regelmäßig mithilfe dieses Befehls gelöscht werden.

Bei Angabe der Option *-e* überprüft der Befehl **kdestroy** alle Cachedateien für Berechtigungsnachweise im Standardcacheverzeichnis (**/QIBM/UserData/OS400/NetworkAuthentication/creds**). Alle Dateien, die nur verfallene Tickets enthalten, die seit dem *Zeitdelta* abgelaufen sind, werden gelöscht. Das *Zeitdelta* wird im Format *nwndnhnmns* ausgedrückt, wobei *n* für eine Zahl, *w* für Wochen, *d* für Tage, *h* für Stunden, *m* für Minuten und *s* für Sekunden steht. Die Komponenten müssen zwar in der genannten Reihenfolge angegeben werden, einzelne Komponenten können aber weggelassen werden (*4h5m* steht beispielsweise für 4 Stunden und 5 Minuten, *1w2h* für 1 Woche und 2 Stunden). Wird nur eine Zahl angegeben, gilt "Stunden" als Standardwert.

**Um den Standardcache für Berechtigungsnachweise zu löschen**, geben Sie Folgendes in einer Qshell-Befehlszeile ein:

```
kdestroy
```

Oder

Geben Sie in einer i5/OS-Befehlszeile für die Steuersprache (CL) Folgendes ein:

```
call qsys/qkrbkdstry
```

Führen Sie die folgenden Schritte aus, **um alle Cachedateien für Berechtigungsnachweise zu löschen, die verfallene Tickets enthalten, die älter sind als einen Tag:**

Geben Sie in einer Qshell-Befehlszeile Folgendes ein:

```
kdestroy -e 1d
```

Oder

Geben Sie in einer CL-Befehlszeile Folgendes ein:

```
call qsys/qkrbkdstry parm ('e' '-1d')
```

Die Anmerkungen zur Verwendung von „kdestroy" enthalten weitere Informationen über das Format und die für diesen Qshell-Befehl geltenden Einschränkungen.

## kdestroy

**Syntax**

```
kdestroy [-c Cachename] [-e Zeitdelta]
```

Standardwert für allgemeine Berechtigung: *USE

Mit dem Qshell-Befehl **kdestroy** wird ein Kerberos-Cache für Berechtigungsnachweise gelöscht.

**Optionen**

**-c Cachename** Der Name des Cache für Berechtigungsnachweise, der gelöscht werden soll. Wenn keine Befehlsoptionen angegeben werden, wird der Standardcache für Berechtigungsnachweise gelöscht. Diese Option und die Option `-e` schließen sich gegenseitig aus.

**-e Zeitdelta** Alle Cachdateien für Berechtigungsnachweise, die abgelaufene Tickets enthalten, werden gelöscht, sofern das Verfallsdatum der Tickets mindestens so lange zurückliegt wie der `Zeitdeltawert`.

**Berechtigungen**

Wenn der Typ des Cache für Berechtigungsnachweise **FILE** lautet (**krb5_cc_resolve()** enthält Informationen über Cachetypen), wird die Cachedatei für Berechtigungsnachweise im Verzeichnis /QIBM/UserData/OS400/NetworkAuthentication/creds erstellt. Die Position der Cachedatei für Berechtigungsnachweise kann durch Setzen der Umgebungsvariablen KRB5CCNAME geändert werden.

Wenn sich die Cachedatei für Berechtigungsnachweise nicht im Standardverzeichnis befindet, sind die folgenden Berechtigungen erforderlich:

| Referenzobjekt | Erforderliche Datenberechtigung | Erforderliche Objektberechtigung |
|---|---|---|
| Jedes Verzeichnis im Pfadnamen, das dem Cache für Berechtigungsnachweise vorangeht | *X | Keine |
| Parentverzeichnis des Cache für Berechtigungsnachweise | *WX | Keine |
| Cachedatei für Berechtigungsnachweise | *RW | *OBJEXIST |
| Jedes Verzeichnis in den Pfaden zu den Konfigurationsdateien | *X | Keine |
| Konfigurationsdateien | *R | Keine |

Wenn sich die Cachedatei für Berechtigungsnachweise im Standardverzeichnis befindet, sind die folgenden Berechtigungen erforderlich:

| Referenzobjekt | Erforderliche Datenberechtigung | Erforderliche Objektberechtigung |
|---|---|---|
| Alle Verzeichnisse im Pfadnamen | *X | Keine |
| Cachedatei für Berechtigungsnachweise | *RW | Keine |
| Jedes Verzeichnis in den Pfaden zu den Konfigurationsdateien | *X | Keine |
| Konfigurationsdateien | *R | Keine |

Damit vom Kerberos-Protokoll die Cachedatei für Berechtigungsnachweise von jedem laufenden Prozess gefunden werden kann, wird der Name der Cachedatei normalerweise im Ausgangsverzeichnis unter dem Dateinamen krb5ccname gespeichert. Für den Benutzer, der die Kerberos-Authentifizierung auf der iSeries verwenden möchte, muss ein Ausgangsverzeichnis definiert sein. Dies ist standardmäßig /home/. Mithilfe dieser Datei wird nach dem Standardcache für Berechtigungsnachweise gesucht, wenn keine Befehlsoptionen angegeben werden. Die Speicherposition der Cachedatei kann durch Setzen der Umgebungsvariablen _EUV_SEC_KRB5CCNAME_FILE überschrieben werden. Um auf diese Datei zugreifen zu können, benötigt das Benutzerprofil die Berechtigung ***X** für jedes Verzeichnis im Pfad und die Berechtigung ***R** für die Datei, in der der Cachedateiname gespeichert ist.

**Nachrichten**

- Cache für Berechtigungsnachweise *Name der Cachedatei* kann nicht aufgelöst werden.
- Cache für Berechtigungsnachweise *Name der Cachedatei* kann nicht gelöscht werden.
- Die Funktion *Funktionsname* hat einen Fehler festgestellt.
- Ticket kann nicht aus Cache für Berechtigungsnachweise *Dateiname* abgerufen werden.
- Für die Option *Optionsname* ist ein Wert erforderlich.
- *Befehlsoption* ist keine gültige Befehlsoption.
- *Befehlsoption eins* und *Befehlsoption zwei* dürfen nicht gemeinsam angegeben werden.
- Kein Standardcache für Berechtigungsnachweise gefunden.
- Der Zeitdeltawert *Wert* ist ungültig.

Unter „Verfallene Cachedateien für Berechtigungsnachweise löschen" auf Seite 131 finden Sie ein Beispiel für die Verwendungsweise dieses Befehls.

## Kerberos-Service-Einträge in LDAP-Verzeichnissen verwalten

Mit dem Befehl **ksetup** werden Kerberos-Service-Einträge im LDAP-Server-Verzeichnis verwaltet. Folgende Unterbefehle werden unterstützt:

**addhost Hostname Realm-Name** Mit diesem Unterbefehl wird ein Hosteintrag für den angegebenen Realm hinzugefügt. Der vollständig qualifizierte Hostname sollte verwendet werden, damit er richtig aufgelöst wird, unabhängig davon, welche Standard-DNS-Domäne auf den Kerberos-Clients aktiv ist. Wird kein Realm-Name angegeben, wird der Standard-Realm verwendet.

**addkdc Hostname:Portnummer Realm-Name** Mit diesem Unterbefehl wird dem Kerberos-Server ein Eintrag für den angegebenen Realm hinzugefügt. Wenn noch kein Hosteintrag vorhanden ist, wird einer erstellt. Wenn keine Portnummer angegeben wird, gilt Portnummer 88. Verwenden Sie den vollständig qualifizierten Hostnamen, damit er richtig aufgelöst wird, unabhängig davon, welche Standard-DNS-Domäne auf den Kerberos-Clients aktiv ist. Wird kein Realm-Name angegeben, wird der Standard-Realm verwendet.

**delhost Hostname Realm-Name** Mit diesem Unterbefehl werden ein Hosteintrag und alle zugeordneten Spezifikationen für den Kerberos-Server aus dem angegebenen Realm gelöscht. Wird kein Realm-Name angegeben, wird der Standard-Realm verwendet.

**delkdc Hostname Realm-Name** Mit diesem Unterbefehl wird ein Eintrag im Kerberos-Server für den angegebenen Host gelöscht. Der Hosteintrag selbst wird nicht gelöscht. Wird kein Realm-Name angegeben, wird der Standard-Realm verwendet.

**listhost Realm-Name** Mit diesem Unterbefehl werden die Hosteinträge für einen Realm aufgelistet. Wird kein Realm-Name angegeben, wird der Standard-Realm verwendet.

**listkdc Realm-Name** Mit diesem Unterbefehl werden die Einträge im Kerberos-Server für einen Realm aufgelistet. Wird kein Realm-Name angegeben, wird der Standard-Realm verwendet.

**exit** Mit diesem Unterbefehl wird der Befehl ksetup beendet.

**Beispiele**

Führen Sie die folgenden Schritte durch, um den Host kdc1.myco.com zum Server ldapserv.myco.com hinzufügen (als Kerberos-Server für Realm MYCO.COM); dabei wird die LDAP-Administrator-ID ″Administrator″ und das Kennwort ″verysecret″ verwendet:

Geben Sie in einer Qshell-Befehlszeile Folgendes ein: `ksetup -h ldapserv.myco.com -n CN=Administrator -p verysecret`

Oder

1. Geben Sie in einer i5/OS-Befehlszeile Folgendes ein:

   ```
   call qsys/qkrbksetup parm('-h' 'ldapserv.myco.com' '-n' 'CN=Administrator' '-p'
   'verysecret')
   ```

2. Wenn die Verbindung zum Directory Services (LDAP)-Server hergestellt werden konnte, wird eine Eingabeaufforderung für Unterbefehle angezeigt. Geben Sie Folgendes ein:

   ```
   addkdc kdc1.myco.com MYCO.COM
   ```

Die Hinweise zur Verwendung von „ksetup” enthalten weitere Informationen über das Format und die für diesen Qshell-Befehl geltenden Einschränkungen.

## ksetup

**Syntax**

```
ksetup -h Hostname -n BIND-Name -p BIND-Kennwort -e
```

Standardwert für allgemeine Berechtigung: *USE

Mit dem Qshell-Befehl **ksetup** werden Kerberos-Service-Einträge im Directory-Server für einen Kerberos-Realm verwaltet.

**Optionen**

**-h** Der Hostname für den Directory-Server. Wird diese Option nicht angegeben, wird der in der Kerberos-Konfiguration angegebene Directory-Server verwendet.

**-n**

**-p** Das Kennwort, das beim BIND mit dem Directory-Server verwendet werden soll. Wird diese Option nicht angegeben, wird das Kennwort über die Umgebungsvariable LDAP_BINDPW abgerufen.

**-e** Jede Befehlszeile in stdout zurückmelden. Diese Option ist sinnvoll, wenn stdin in eine Datei umgeleitet wird.

**Berechtigungen**

| Referenzobjekt | Erforderliche Berechtigung |
|---|---|
| Jedes Verzeichnis in den Pfaden zu den Konfigurationsdateien | *X |
| Konfigurationsdateien | *R |

**Nachrichten**

- `Unterbefehl` ist kein gültiger Unterbefehl.
- Gültige Unterbefehle sind `addhost`, `addkdc`, `delhost`, `delkdc`, `listhost`, `listkdc`, `exit`.
- `Befehlsoption eins` und `Befehlsoption zwei` können nicht gemeinsam angegeben werden.
- LDAPclient kann nicht initialisiert werden.
- BIND mit Directory-Server nicht möglich.
- Der Realm-Name muss angegeben werden.
- Der Hostname muss angegeben werden.
- Zu viele positionsgebundene Parameter.
- Host `Host` ist bereits vorhanden.
- Root-Domäne `Domäne` ist nicht definiert.
- Realm-Name `Realm` ist ungültig.
- Die Funktion `LDAP-Funktionsname` hat einen Fehler festgestellt.
- Nicht genügend Speicher verfügbar.
- Hostname `Host` ist ungültig.
- Portnummer `Port` ist ungültig.
- Host `Host` ist nicht definiert.
- Kein Kerberos-Server für Host `Host` definiert.
- Realm-Name konnte nicht abgerufen werden.

Unter „Kerberos-Service-Einträge in LDAP-Verzeichnissen verwalten” auf Seite 133 finden Sie ein Beispiel für die Verwendungsweise dieses Befehls.

## Realms in der DNS-Datenbank definieren

Der Netzwerkauthentifizierungsservice ermöglicht Ihnen die Verwendung des DNS-Servers zur Auflösung von Hostnamen. Sie müssen dazu einen Serversatz (SRV) und einen Textsatz (TXT) für jede KDC (Instanz zur Schlüsselverteilung) im Realm hinzufügen. Das Kerberos-Protokoll verwendet bei der Suche nach einem SRV-Satz den Realm-Namen als DNS-Suchnamen.

Führen Sie die folgenden Schritte durch, um Realms für DNS zu definieren:

1. In der Konfigurationsdatei angeben, dass DNS verwendet werden soll.
2. Fügen Sie dem DNS-Server für jeden KDC-Server im Realm SRV-Sätze hinzu. Die Kerberos-Ausführungszeit verwendet bei der Suche nach einem SRV-Satz den Realm-Namen als Suchnamen. Beach-

ten Sie, dass die Groß-/Kleinschreibung bei DNS-Suchvorgängen keine Rolle spielt, so dass es keine unterschiedlichen Realms geben darf, deren Namen sich lediglich aufgrund der Groß-/Kleinschreibung unterscheiden.

Das allgemeine Format des Kerberos-SRV-Satzes lautet:

```
Service.Protokoll.Realm TTL Klasse SRV Priorität Wertigkeit Port Ziel
```

Die _kerberos-Service-Einträge definieren KDC-Instanzen, und die _kpasswd-Service-Einträge definieren Änderungsservice-Instanzen für Kennwörter.

Die Einträge werden nach Priorität verarbeitet (0 ist die höchste Priorität). Einträge mit gleicher Priorität werden in wahlfreier Reihenfolge verarbeitet. Die _udp-Protokollsätze sind für _kerberos- und _kpasswd-Einträge erforderlich.

3. Fügen Sie TXT-Sätze hinzu, um Hostnamen und Realm-Namen einander zuzuordnen. Bei der Suche nach einem TXT-Satz beginnt das Kerberos-Protokoll mit dem Hostnamen. Wenn kein TXT-Satz gefunden werden kann, wird der erste Kennsatz entfernt, und die Suche wird mit dem neuen Namen wiederholt. Dieser Prozess wird so lange wiederholt, bis ein TXT-Satz gefunden oder die Root erreicht wird. Beachten Sie, dass beim Realm-Namen im TXT-Satz die Groß-/Kleinschreibung beachtet wird.

   Das allgemeine Format eines TXT-Satzes lautet folgendermaßen:

   ```
   Service.Name TTL Klasse TXT Realm
   ```

Im Konfigurationsbeispiel können Sie die Beispiel-KDCs für die beiden Realms definieren, indem Sie die folgenden Sätze hinzufügen:

```
_kerberos._udp.deptxyz.bogusname.com IN SRV 0 0 88 kdc1.deptxyz.bogusname.com
_kerberos._tcp.deptxyz.bogusname.com IN SRV 0 0 88 kdc1.deptxyz.bogusname.com
_kerberos._udp.deptabc.bogusname.com IN SRV 0 0 88 kdc2.deptabc.bogusname.com
_kerberos._tcp.deptabc.bogusname.com IN SRV 0 0 88 kdc2.deptabc.bogusname.com
_kpasswd._udp.deptxyz.bogusname.com IN SRV 0 0 464 kdc1.deptxyz.bogusname.com
_kpasswd._tcp.deptxyz.bogusname.com IN SRV 0 0 464 kdc1.deptxyz.bogusname.com
_kpasswd._udp.deptabc.bogusname.com IN SRV 0 0 464 kdc2.deptxyz.bogusname.com
_kpasswd._tcp.deptabc.bogusname.com IN SRV 0 0 464 kdc2.deptxyz.bogusname.com
```

Im Konfigurationsbeispiel können - gemäß dem allgemeinen Format eines Kerberos-TXT-Satzes - Hosts in den Domänen deptxyz und deptabc ihren entsprechenden Realms mit den folgenden Anweisungen zugeordnet werden:

```
_kerberos.deptxyz.bogusname.com  IN  TXT  DEPTXYZ.BOGUSNAME.COM
_kerberos.deptabc.bogusname.com  IN  TXT  DEPTABC.BOGUSNAME.COM
```

Im Folgenden finden Sie ein Beispiel für die Konfigurationsdatei **krb5.conf**, in der die Verwendung der DNS-Suchfunktion angegeben wird:

Lesen Sie den „Haftungsausschluss für Programmcode” auf Seite 2; er enthält wichtige rechtliche Informationen.

**Beispiel für Konfigurationsdatei krb5.conf**

```
; krb5.conf - Kerberos V5 configuration file DO NOT REMOVE THIS LINE
;
[libdefaults]
;  Der Standard-Realm-Wert
;-default_realm = REALM1.ROCHESTER.IBM.COM
default_realm = DEPTXYZ.BOGUSNAME.COM
; System für Verwendung der DNS-Suchfunktion definieren
use_dns_lookup = 1
```

```
[realms]
;
; Hier könnten dieselben Realm-Informationen konfiguriert werden, doch
; würden sie nur verwendet, wenn die DNS-Suchfunktion fehlschlägt.
;
[domain_realm]
;  Hostnamen in Realm-Namen konvertieren. Es können einzelne Hostnamen
;  angegeben werden. Domänensuffixe können mit führendem Punkt angegeben
;  werden und gelten für alle Hostnamen, die mit diesem Suffix enden.
;
; Mit DNS wird aufgelöst, zu welchem Realm ein bestimmter Hostname gehört.
;
[capaths]
;  Konfigurierbare Authentifizierungspfade definieren die Vertrauensbeziehungen
;  zwischen Client und Servern. Jeder Eintrag steht für einen Client-Realm
;  und besteht aus den Vertrauensbeziehungen für jeden Server, auf den
;  über diesen Realm zugegriffen werden kann. Ein Server kann mehrmals
;  aufgelistet werden, wenn mehrere Vertrauensbeziehungen vorhanden sind.
;  Geben Sie '.' für eine Direktverbindung an.
;-REALM1.ROCHESTER.IBM.COM = {
;-    REALM2.ROCHESTER.IBM.COM = .
;;}
DEPTXYZ.BOGUSNAME.COM = {
 DEPTABC.BOGUSNAME.COM = .
}
```

## Realms im LDAP-Server definieren

Der Netzwerkauthentifizierungsservice ermöglicht Ihnen die Verwendung des LDAP-Servers, um einen Hostnamen in einen Kerberos-Realm aufzulösen und den KDC für einen Kerberos-Realm zu suchen. Wenn Sie LDAP für die Suche nach diesen Informationen verwenden, müssen Sie die Informationen im LDAP-Server definieren. Dazu müssen Sie die folgenden Tasks ausführen:

1. In der Konfigurationsdatei angeben, dass LDAP verwendet werden soll.

   Im iSeries Navigator angeben, welcher Directory-Server zur Auflösung von Hostnamen verwendet werden soll. Hiermit wird die Konfigurationsdatei **krb5.conf** in **/QIBM/UserData/OS400/NetworkAuthentication/krb5.conf** aktualisiert. Der Name des Directory-Servers wird der Sektion [libdefaults] in der Konfigurationsdatei hinzugefügt. Im Folgenden finden Sie ein Beispiel für diese Konfigurationsdatei:

   **Beispiel für Konfigurationsdatei krb5.conf**

   ```
   ; krb5.conf - Kerberos V5 configuration file DO NOT REMOVE THIS LINE
   ;
   [libdefaults]
   ;  Der Standard-Realm-Wert
   ;-default_realm = REALM1.ROCHESTER.IBM.COM
   default_realm = DEPTXYZ.BOGUSNAME.COM
   ; System für Verwendung der LDAP-Suchfunktion definieren
   use_ldap_lookup = 1
   ldap_server = dirserv.bogusname.com
   [realms]
   ;
   ; Hier könnten dieselben Realm-Informationen konfiguriert werden, doch
   ; würden sie nur verwendet, wenn die LDAP-Suchfunktion fehlschlägt.
   ;
   [domain_realm]
   ;  Hostnamen in Realm-Namen konvertieren. Es können einzelne Hostnamen
   ;  angegeben werden. Domänensuffixe können mit führendem Punkt angegeben
   ;  werden und gelten für alle Hostnamen, die mit diesem Suffix enden.
   ;
   ```

```
; Mit LDAP wird aufgelöst, zu welchem Realm ein bestimmter Hostname gehört.
; Sie könnten hier ebenfalls definiert werden, doch würden sie nur verwendet,
; wenn die LDAP-Suchfunktion fehlschlägt.
;
[capaths]
;  Konfigurierbare Authentifizierungspfade definieren die Vertrauensbeziehungen
;  zwischen Client und Servern. Jeder Eintrag steht für einen Client-Realm
;  und besteht aus den Vertrauensbeziehungen für jeden Server, auf den
;  über diesen Realm zugegriffen werden kann. Ein Server kann mehrmals
;  aufgelistet werden, wenn mehrere Vertrauensbeziehungen vorhanden sind.
;  Geben Sie '.' für eine Direktverbindung an.
;-REALM1.ROCHESTER.IBM.COM = {
;-    REALM2.ROCHESTER.IBM.COM = .
;;}
DEPTXYZ.BOGUSNAME.COM = {
 DEPTABC.BOGUSNAME.COM = .
}
```

Der Abschnitt „Haftungsausschluss für Programmcode" auf Seite 2 enthält wichtige rechtliche Hinweise.

2. **Kerberos für den LDAP-Server definieren**

   a. Auf dem LDAP-Server muss ein Domänenobjekt vorhanden sein, dessen Name mit dem Kerberos-Realm-Namen übereinstimmt. Lautet der Kerberos-Realm-Name beispielsweise DEPTABC.BOGUSNAME.COM, dann muss im Verzeichnis ein Objekt mit dem Namen dc=DEPTABC,dc=BOGUSNAME,dc=com vorhanden sein. Wenn dieses Objekt nicht vorhanden ist, müssen Sie möglicherweise zunächst der LDAP-Serverkonfiguration ein Suffix hinzufügen. Gültige Suffixe für diesen Objektnamen sind dc=DEPTABC,dc=BOGUSNAME,dc=COM oder einer der Parenteinträge (dc=BOGUSNAME,dc=COM oder dc=COM). Das Suffix für einen i5/OS LDAP-Server kann mit dem iSeries Navigator hinzugefügt werden.

      Führen Sie die folgenden Schritte durch, um ein Suffix hinzuzufügen:
      1) Erweitern Sie im iSeries Navigator **Ihren iSeries-Server** → **Netzwerk** → **Server** → **TCP/IP**.
      2) Klicken Sie mit der rechten Maustaste auf **IBM Directory Server** und wählen Sie **Eigenschaften** aus.
      3) Geben Sie auf der Seite **Datenbank/Suffix** das Suffix an, das hinzugefügt werden soll.

   b. Fügen Sie das Domänenobjekt für den Realm im LDAP-Verzeichnis mit dem Befehl **LDAPADD** hinzu.

   c. Fahren Sie mit dem Konfigurationsbeispiel für zwei Realms mit der Bezeichnung DEPTABC.BOGUSNAME.COM und DEPTXYZ.BOGUSNAME.COM fort, indem Sie einer Datei im Integrated File System die folgenden Zeilen hinzufügen:

      ```
      dn: dc=BOGUSNAME,dc=COM
      dc: BOGUSNAME
      objectClass: domain

      dn: dc=DEPTABC,dc=BOGUSNAME,dc=COM
      dc: DEPTABC
      objectClass: domain

      dn: dc=DEPTXYZ,dc=BOGUSNAME,dc=COM
      dc: DEPTXYZ
      objectClass: domain
      ```

   d. Wenn der Name der IFS-Datei **/tmp/addRealms.ldif** lautet, dann geben Sie unter Annahme derselben Voraussetzungen wie im vorherigen Beispiel die folgenden Befehle ein:

      ```
      STRQSH  ldapadd -h dirserv.bogusname.com -D cn=Administrator
        -w verysecret -c -f
      /tmp/addRealms.ldif
      ```

   e. Definieren Sie die KDC-Einträge für Ihre Realms und definieren Sie wahlweise Hostnameneinträge, um jeden Host in Ihrem Netzwerk einem bestimmten Realm-Namen zuzuordnen.

Dazu können Sie den Befehl **ksetup** mit den Unterbefehlen **addkdc** und **addhost** verwenden. Fahren Sie mit dem Konfigurationsbeispiel fort und geben Sie die folgenden Befehle ein:

```
STRQSH
ksetup -h dirserv.bogusname.com -n cn=Administrator
  -p verysecret
addkdc kdc1.deptxyz.bogusname.com DEPTXYZ.BOGUSNAME.COM
addkdc kdc2.deptxyz.bogusname.com DEPTXYZ.BOGUSNAME.COM
addkdc kdc1.deptabc.bogusname.com DEPTABC.BOGUSNAME.COM
addhost database.deptxyz.bogusname.com
  DEPTXYZ.BOGUSNAME.COM
```

Wiederholen Sie diese Eingaben für jeden Host in jedem Realm.

**LDAP-Schema**

**Anmerkung:**

Der i5/OS LDAP-Server (IBM Directory Server) wird mit einem bereits definierten LDAP-Schema ausgeliefert. Wenn Sie jedoch einen anderen LDAP-Server als IBM Directory Server verwenden, können Sie Ihr eigenes Schema auf diesem Server definieren.Dabei können Ihnen die folgenden Informationen helfen.

Für den Netzwerkauthentifizierungsservice gelten die folgenden LDAP-Schemadefinitionen:

- Ganzzahlige Werte werden als nummerische Zeichenfolge mit Vorzeichen und einer maximalen Länge von 11 Zeichen dargestellt.
- Boolesche Werte werden durch die Zeichenfolgen ″TRUE″ und ″FALSE″ dargestellt.
- Zeitwerte werden als 15 Byte umfassende Zeichenfolgen im Format ″JJJJMMTThhmmssZ″ dargestellt. Alle Zeitangaben werden als UTC-Werte dargestellt.

**LDAP-Objektklassen**

| Objekt | Erforderlich | Zulässig |
|---|---|---|
| domain | dc | description seeAlso |
| ibmCom1986-Krb-KerberosService | serviceName ibmCom1986-Krb-KerberosRealm | ipServicePort description seeAlso |
| domain | dc objectClass | description seeAlso |

**LDAP-Attribute**

| Attribut | Typ | Größe | Wert |
|---|---|---|---|
| dc | caseIgnoreString | 64 | Einzelwert |
| description | caseIgnoreString | 1024 | Mehrere Werte |
| ibmCom1986-Krb-KerberosRealm | caseExactString | 256 | Einzelwert |
| ipServicePort | Ganzzahliger Wert | 11 | Einzelwert |
| seeAlso | DN | 1000 | Mehrere Werte |
| serviceName | caseIgnoreString | 256 | Einzelwert |

## Fehlerbehebung

In diesem Abschnitt finden Sie Links auf Informationen zur Behebung häufig auftretender Probleme, die den Netzwerkauthentifizierungsservice, Enterprise Identity Mapping (EIM) und die von IBM gelieferten Anwendungen betreffen, die die Kerberos-Authentifizierung unterstützen.

1. Alle Voraussetzungen wurden erfüllt.
2. Vergewissern Sie sich, dass der Benutzer über ein Benutzerprofil auf der iSeries und über einen Principal auf dem Kerberos-Server verfügt. Auf der iSeries vergewissern Sie sich, dass der Benutzer vorhanden ist, indem Sie "Benutzer und Gruppen" im iSeries Navigator öffnen oder `WRKUSRPRF` in einer Befehlszeile eingeben. Auf Windows (R)-Systemen vergewissern Sie sich, dass der Benutzer vorhanden ist, indem Sie auf den Ordner "Active Directory (R)-Benutzer und -Computer" zugreifen.
3. Überprüfen Sie, ob die iSeries mit dem Kerberos-Server Kontakt hat, indem Sie den Befehl kinit im Qshell-Interpreter ausführen. Wenn der Befehl kinit nicht ausgeführt werden kann, stellen Sie fest, ob der i5/OS-Service-Principal auf dem Kerberos-Server registriert wurde. Wenn nicht, können Sie den i5/OS-Principal zum Kerberos-Server hinzufügen.

Folgende Themen enthalten Informationen über spezielle Verfahren zur Fehlerbehebung:

Fehler und Fehlerbehebung beim Netzwerkauthentifizierungsservice
In diesem Abschnitt finden Sie häufig auftretende Fehler, auf die Sie im iSeries Navigator stoßen können. Für jeden Fehler stehen Wiederherstellungsinformationen zur Verfügung.

Fehler und Fehlerbehebung bei der Anwendungsverbindung
In diesem Abschnitt finden Sie häufig auftretende Fehler, auf die Sie stoßen können, wenn Sie den Netzwerkauthentifizierungsservice für andere iSeries Navigator-Anwendungen, wie beispielsweise Management Central, verwenden. Für jeden Fehler stehen Wiederherstellungsinformationen zur Verfügung.

API-Trace-Tool
In diesem Abschnitt wird erläutert, wie Sie Umgebungsvariablen einsetzen können, um ein Tool zu generieren, das einen Trace aller Kerberos- und Generic Security Services (GSS)-API-Aufrufe durchführt. Dieser API-Trace hilft Ihnen bei der Feststellung und Behebung von Fehlern sowohl in den von IBM gelieferten Anwendungen als auch in Ihren eigenen Kerberos-fähigen Anwendungen.

Fehlerbehebung für Kerberos-Server in i5/OS PASE
Dieser Abschnitt enthält Informationen zur Fehlerbehebung für einen Kerberos-Server in i5/OS PASE. Es wird die Verwendung einer Fehlerprotokolldatei erläutert, die auf dem Kerberos-Server generiert wird und Beschreibungen und Wiederherstellungsinformationen für viele häufig auftretende Fehler enthält.

## Fehler und Fehlerbehebung beim Netzwerkauthentifizierungsservice

Die folgenden Nachrichten können während der Arbeit mit dem Assistenten für den Netzwerkauthentifizierungsservice angezeigt werden oder wenn Sie die Eigenschaften des Netzwerkauthentifizierungsservice im iSeries Navigator verwalten.

*Tabelle 36. Fehler und Fehlerbehebung beim Netzwerkauthentifizierungsservice*

| Fehler | Wiederherstellung |
|---|---|
| KRBWIZ_CONFIG_FILE_FORMAT_ERROR Das Format der Konfigurationsdatei für den Netzwerkauthentifizierungsservice ist fehlerhaft. | Den Netzwerkauthentifizierungsservice rekonfigurieren. Siehe Netzwerkauthentifizierungsservice konfigurieren. |
| KRBWIZ_CRYPTO_NOT_INSTALLED Das erforderliche Verschlüsselungsprodukt ist auf dem System nicht installiert. | Cryptographic Access Provider (5722-AC3) auf dem System installieren. |
| KRBWIZ_ERROR_READ_CONFIG_FILE Fehler beim Lesen der Konfigurationsdatei für Netzwerkauthentifizierungsservice. | Den Netzwerkauthentifizierungsservice rekonfigurieren. Siehe Netzwerkauthentifizierungsservice konfigurieren. |

*Tabelle 36. Fehler und Fehlerbehebung beim Netzwerkauthentifizierungsservice (Forts.)*

| Fehler | Wiederherstellung |
|---|---|
| KRBWIZ_ERROR_WRITE_CONFIG_FILE Fehler beim Schreiben in die Konfigurationsdatei für Netzwerkauthentifizierungsservice. | Der Service für das Schreiben in die Konfigurationsdatei ist nicht verfügbar. Vorgang später wiederholen. |
| KRBWIZ_PASSWORD_MISMATCH Neues Kennwort und Prüfkennwort nicht identisch. | Neues Kennwort erneut eingeben und bestätigen. |
| KRBWIZ_PORT_ERROR Die Portnummer muss im Bereich von 1 bis 65535 liegen. | Eine Portnummer zwischen 1 und 65535 eingeben. |
| KRBWIZ_ERROR_WRITE_KEYTAB Fehler beim Schreiben in die Chiffrierschlüsseldatei. | Der Service für das Schreiben in die Chiffrierschlüsseldatei ist vorübergehend nicht verfügbar. Vorgang später wiederholen. |
| KRBWIZ_NOT_AUTHORIZED_CONFIGURE Keine Berechtigung für die Konfiguration des Netzwerkauthentifizierungsservice. | Vergewissern Sie sich, dass Sie über die folgenden Berechtigungen verfügen: *ALLOBJ und *SECADM. |
| KrbPropItemExists Das Element ist bereits vorhanden. | Ein neues Element eingeben. |
| KrbPropKDCInListRequired KDC muss in der Liste enthalten sein. | Angegebener Kerberos-Server ist in der Liste nicht vorhanden. Wählen Sie einen Kerberos-Server aus der Liste aus. |
| KrbPropKDCValueRequired Ein KDC-Name muss eingegeben werden. | Einen gültigen Namen für den Kerberos-Server eingeben. Der Kerberos-Server muss auf einem sicheren System im Netzwerk konfiguriert sein. |
| KrbPropPwdServerRequired Ein Kennwortservername muss eingegeben werden. | Einen gültigen Namen für den Kennwortserver eingeben. |
| KrbPropRealmRequired Ein Realm-Name muss eingegeben werden. | Den Namen des Realms eingeben, zu dem dieses System gehört. |
| KrbPropRealmToTrustRequired Für den sicheren Realm muss ein Name eingegeben werden. | Den Namen des Realms eingeben, für den eine Vertrauensbeziehung aufgebaut wird. |
| KrbPropRealmValueRequired Ein Realm-Name muss eingegeben werden. | Einen gültigen Namen für den Realm eingeben. |
| CPD3E3F Fehler &2 bei Netzwerkauthentifizierungsservice aufgetreten. | Siehe die entsprechenden Wiederherstellungsinformationen für diese Nachricht. |

## Fehler und Fehlerbehebung bei der Anwendungsverbindung

Die folgenden Nachrichten (oder Nachrichten mit einem ähnlichen Wortlaut) könnten angezeigt werden, wenn Sie mit Anwendungen arbeiten, die den Netzwerkauthentifizierungsservice verwenden.

*Tabelle 37. Häufige Fehler in Kerberos-fähigen i5/OS-Schnittstellen.*

| Problem | Wiederherstellung |
|---|---|
| Name des Standardcaches für Berechtigungsnachweise kann nicht abgerufen werden. | Stellen Sie fest, ob der Benutzer, der bei der iSeries angemeldet ist, über ein Verzeichnis im Ausgangsverzeichnis (/home) verfügt.Wenn kein Verzeichnis für den Benutzer vorhanden ist, erstellen Sie ein Ausgangsverzeichnis für den Cache für Berechtigungsnachweise. |
| CPD3E3F Fehler &2 bei Netzwerkauthentifizierungsservice aufgetreten. | Siehe die entsprechenden Wiederherstellungsinformationen für diese Nachricht. |

*Tabelle 37. Häufige Fehler in Kerberos-fähigen i5/OS-Schnittstellen. (Forts.)*

| Problem | Wiederherstellung |
|---|---|
| Keine DRDA/DDM-Verbindung auf einem iSeries-System möglich, für das zuvor eine Verbindung bestanden hat. | Überprüfen Sie, ob der Standard-Realm vorhanden ist, der bei der Konfiguration des Netzwerkauthentifizierungsservice angegeben wurde. Wenn kein Standard-Realm und kein Kerberos-Server konfiguriert wurden, ist die Konfiguration des Netzwerkauthentifizierungsservice falsch, und es können keine DRDA/DDM-Verbindungen hergestellt werden. Sie können eine der folgenden Tasks ausführen, um diesen Fehler zu beheben:<br>1. Gehen Sie folgendermaßen vor, wenn Sie nicht mit der Kerberos-Authentifizierung arbeiten:<br>a. Löschen Sie den bei der Konfiguration des Netzwerkauthentifizierungsservice angegebenen Standard-Realm.<br>2. Gehen Sie folgendermaßen vor, wenn Sie mit der Kerberos-Authentifizierung arbeiten:<br>a. Rekonfigurieren Sie den Netzwerkauthentifizierungsservice und geben Sie den Standard-Realm und den Kerberos-Server an, den Sie in Schritt 1 erstellt haben.<br>b. Konfigurieren Sie (siehe „Schritt 14: iSeries Access für Windows-Anwendungen zur Verwendung der Kerberos-Authentifizierung konfigurieren" auf Seite 77) iSeries Access für Windows-Anwendungen so, dass sie die Kerberos-Authentifizierung verwenden. Dadurch wird die Kerberos-Authentifizierung für alle iSeries Access für Windows-Anwendungen, einschließlich DRDA/DDM, konfiguriert. |

*Tabelle 37. Häufige Fehler in Kerberos-fähigen i5/OS-Schnittstellen. (Forts.)*

| Problem | Wiederherstellung |
|---|---|
| Keine QFileSvr.400-Verbindung auf einem iSeries-System möglich, für das zuvor eine Verbindung bestanden hat. | Überprüfen Sie, ob der Standard-Realm vorhanden ist, der bei der Konfiguration des Netzwerkauthentifizierungsservice angegeben wurde. Wenn kein Standard-Realm und kein Kerberos-Server konfiguriert wurden, ist die Konfiguration des Netzwerkauthentifizierungsservice falsch, und es können keine QFileSvr.400-Verbindungen hergestellt werden. Sie können eine der folgenden Tasks ausführen, um diesen Fehler zu beheben:<br>1. Gehen Sie folgendermaßen vor, wenn Sie nicht mit der Kerberos-Authentifizierung arbeiten:<br>a. Löschen Sie den bei der Konfiguration des Netzwerkauthentifizierungsservice angegebenen Standard-Realm.<br>2. Gehen Sie folgendermaßen vor, wenn Sie mit der Kerberos-Authentifizierung arbeiten:<br>a. Konfigurieren Sie den Standard-Realm und den Kerberos-Server auf einem sicheren System im Netzwerk. Weitere Informationen finden Sie in der Dokumentation zu diesem System.<br>b. Rekonfigurieren Sie den Netzwerkauthentifizierungsservice und geben Sie den Standard-Realm und den Kerberos-Server an, den Sie in Schritt 1 erstellt haben.<br>c. Konfigurieren Sie (siehe „Schritt 14: iSeries Access für Windows-Anwendungen zur Verwendung der Kerberos-Authentifizierung konfigurieren" auf Seite 77) iSeries Access für Windows-Anwendungen so, dass sie die Kerberos-Authentifizierung verwenden. Dadurch wird die Kerberos-Authentifizierung für alle iSeries Access für Windows-Anwendungen, einschließlich DRDA/DDM, konfiguriert. |
| | |
| CWBSY1011 Berechtigungsnachweise für Kerberos-Client nicht gefunden. | Der Benutzer hat kein Ticket-granting Ticket (TGT). Dieser Verbindungsfehler tritt auf dem Client-PC auf, wenn sich ein Benutzer nicht bei einer Windows (R) 2000-Domäne anmeldet. Um diesen Fehler zu beheben, melden Sie sich bei der Windows (R) 2000-Domäne an. |
| Fehler beim Prüfen der Verbindungseinstellungen aufgetreten. URL enthält keinen Host. **Anmerkung:** Dieser Fehler tritt auf, wenn Sie mit Enterprise Identity Mapping (EIM) arbeiten. | Gehen Sie folgendermaßen vor, um diesen Fehler zu beheben:<br>1. Erweitern Sie im iSeries Navigator **Ihre iSeries**—> **Netzwerk**—>**Server**—> **TCP/IP**.<br>2. Klicken Sie mit der rechten Maustaste auf **Verzeichnis** und wählen Sie **Eigenschaften** aus.<br>3. Prüfen Sie auf der Seite **Allgemein**, ob der registrierte Name und das Kennwort des Administrators mit den entsprechenden Angaben übereinstimmen, die Sie bei der EIM-Konfiguration gemacht haben. |

*Tabelle 37. Häufige Fehler in Kerberos-fähigen i5/OS-Schnittstellen. (Forts.)*

| Problem | Wiederherstellung |
|---|---|
| Fehler beim Ändern der Konfiguration für lokalen Directory-Server aufgetreten. GLD0232: Konfiguration kann keine überlappenden Suffixe enthalten. **Anmerkung:** Dieser Fehler tritt auf, wenn Sie mit Enterprise Identity Mapping (EIM) arbeiten. | Gehen Sie folgendermaßen vor, um diesen Fehler zu beheben:<br>1. Erweitern Sie im iSeries Navigator **Ihre iSeries**—> **Netzwerk**—>**Server**—> **TCP/IP**.<br>2. Klicken Sie mit der rechten Maustaste auf **Verzeichnis** und wählen Sie **Eigenschaften** aus.<br>3. Entfernen Sie auf der Seite **Datenbank/Suffixe** alle **ibm-eimDomainName**-Einträge und rekonfigurieren Sie EIM. |
| Fehler beim Prüfen der Verbindungseinstellungen aufgetreten. Beim Aufrufen eines iSeries-Programms kam es zu einer Ausnahmebedingung. Das aufgerufene Programm ist eimConnect. Details: com.ibm.as400.data.PcmlException. **Anmerkung:** Dieser Fehler tritt auf, wenn Sie mit Enterprise Identity Mapping (EIM) arbeiten. | Gehen Sie folgendermaßen vor, um diesen Fehler zu beheben:<br>1. Erweitern Sie im iSeries Navigator **Ihre iSeries**—> **Netzwerk**—>**Server**—> **TCP/IP**.<br>2. Klicken Sie mit der rechten Maustaste auf **Verzeichnis** und wählen Sie **Eigenschaften** aus.<br>3. Entfernen Sie auf der Seite **Datenbank/Suffixe** alle **ibm-eimDomainName**-Einträge und rekonfigurieren Sie EIM. |
| Kerberos-Ticket vom fernen System kann nicht authentifiziert werden.<br>**Anmerkung:** Dieser Fehler tritt auf, wenn Sie Management Central-Systeme für die Verwendung der Kerberos-Authentifizierung konfigurieren. | Überprüfen Sie, ob Kerberos auf allen Systemen richtig konfiguriert ist. Dieser Fehler kann auf einen Sicherheitsverstoß hinweisen. Wiederholen Sie die Anforderung; bleibt das Problem weiterhin bestehen, informieren Sie den Service. |
| Kerberos-Service-Ticket kann nicht abgerufen werden.<br>**Anmerkung:** Dieser Fehler tritt auf, wenn Sie Management Central-Systeme für die Verwendung der Kerberos-Authentifizierung konfigurieren. | Überprüfen Sie für jedes Ihrer Systeme, ob sich der Kerberos-Principal krbsvr400/iSeries vollständig qualifizierter Hostname@REALM sowohl auf dem Kerberos-Server als auch in der Chiffrierschlüsseldatei befindet. Um zu überprüfen, ob sich der Kerberos-Principal auf dem Kerberos-Server befindet, siehe „Dem Kerberos-Server i5/OS-Principals hinzufügen" auf Seite 114. Um zu überprüfen, ob sich der Name des Kerberos-Service-Principals in der Chiffrierschlüsseldatei befindet, siehe „Chiffrierschlüsseldateien verwalten" auf Seite 127. |
| Kerberos-Principal befindet sich nicht in zuverlässiger Gruppe.<br>**Anmerkung:** Dieser Fehler tritt auf, wenn Sie Management Central-Systeme für die Verwendung der Kerberos-Authentifizierung konfigurieren. | Fügen Sie den Kerberos-Principal für das System, das versucht, eine Verbindung zu diesem System herzustellen, der Datei für anerkannte Gruppen hinzu. Gehen Sie folgendermaßen vor, um diesen Fehler zu beheben:<br>1. Definieren Sie das zentrale System für die Verwendung der Kerberos-Authentifizierung.<br>2. Erfassen Sie das Systemwerte-Inventar.<br>3. Vergleichen und aktualisieren Sie.<br>4. Starten Sie die Management Central-Server auf dem zentralen System und den Zielsystemen erneut.<br>5. Konfigurieren Sie die Datei für die anerkannte Gruppe für alle Endpunktsysteme.<br>6. Erlauben Sie sichere Verbindungen.<br>7. Starten Sie die Management Central-Server auf dem zentralen System und den Zielsystemen erneut.<br>8. Testen Sie die Authentifizierung auf Management Central-Servern. |

# API-Trace-Tool

Der Netzwerkauthentifizierungsservice stellt ein API-Trace-Tool zur Verfügung, mit dem ein Administrator eine Datei erstellen kann, die alle Kerberos- und Generic Security Services (GSS)-API-Aufrufe enthält. Mithilfe dieses Tools können Sie kompliziertere Fehler beheben, die Ihre eigenen Kerberos-fähigen Anwendungen betreffen und bei der Konfiguration des Netzwerkauthentifizierungsservice sowie bei Anforderungen für Kerberos-Tickets auftreten könnten. Das Tool kann unter Verwendung von Umgebungsvariablen erstellt und veranlasst werden, eine Protokolldatei im Ausgangsverzeichnis des Benutzers zu generieren.

**Anmerkung:** Diese Schritte können Sie nur ausführen, wenn das Ausgangsverzeichnis vorhanden ist.

## API-Trace-Tool konfigurieren

Um das API-Trace-Tool in eine Datei zu schreiben, führen Sie die folgenden Schritte auf dem iSeries-Server aus, auf dem der Netzwerkauthentifizierungsservice konfiguriert ist:

1. Geben Sie in der zeichenorientierten Schnittstelle `ADDENVVAR` (Umgebungsvariable hinzufügen) ein.
2. Geben Sie in der Anzeige **Umgebungsvariable hinzufügen (ADDENVVAR)** `_EUV_SVC_MSG_LOGGING` im Feld **Umgebungsvariable** ein.
3. Geben Sie im Feld **Anfangswert** `STDOUT_LOGGING` ein. Drücken Sie die Eingabetaste.
4. Geben Sie in der zeichenorientierten Schnittstelle `ADDENVVAR` (Umgebungsvariable hinzufügen) ein.
5. Geben Sie in der Anzeige **Umgebungsvariable hinzufügen (ADDENVVAR)** `_EUV_SVC_MSG_LEVEL` im Feld **Umgebungsvariable** ein.
6. Geben Sie im Feld **Anfangswert** `VERBOSE` ein. Drücken Sie die Eingabetaste.
7. Geben Sie in der zeichenorientierten Schnittstelle `ADDENVVAR` (Umgebungsvariable hinzufügen) ein.
8. Geben Sie in der Anzeige **Umgebungsvariable hinzufügen (ADDENVVAR)** `_EUV_SVC_STDOUT_FILENAME` im Feld **Umgebungsvariable** ein.
9. Geben Sie im Feld **Anfangswert** `/home/Benutzerprofil/trace.txt` ein, wobei `Benutzerprofil` der Name des Benutzerprofils ist. Drücken Sie die Eingabetaste.
10. Geben Sie in der zeichenorientierten Schnittstelle `ADDENVVAR` (Umgebungsvariable hinzufügen) ein.
11. Geben Sie in der Anzeige **Umgebungsvariable hinzufügen (ADDENVVAR)** `_EUV_SVC_DBG_MSG_LOGGING` im Feld **Umgebungsvariable** ein.
12. Geben Sie im Feld **Anfangswert** `1` ein.
13. Geben Sie in der zeichenorientierten Schnittstelle `ADDENVVAR` (Umgebungsvariable hinzufügen) ein.
14. Geben Sie in der Anzeige **Umgebungsvariable hinzufügen (ADDENVVAR)** `_EUV_SVC_DBG_TRACE` im Feld **Umgebungsvariable** ein.
15. Geben Sie im Feld **Anfangswert** `1` ein.
16. Geben Sie in der zeichenorientierten Schnittstelle `ADDENVVAR` (Umgebungsvariable hinzufügen) ein.
17. Geben Sie in der Anzeige **Umgebungsvariable hinzufügen (ADDENVVAR)** `_EUV_SVC_DBG` im Feld **Umgebungsvariable** ein.
18. Geben Sie im Feld **Anfangswert** `*.9` ein. Drücken Sie die Eingabetaste.

## Auf die API-Traceprotokolldatei zugreifen

Nachdem Sie das API-Trace-Tool konfiguriert haben, können Sie jetzt auf die Datei zugreifen, um mit der Fehlerbehebung zu beginnen. Führen Sie die folgenden Schritte durch, um auf diese Datei zuzugreifen:

1. Geben Sie in der zeichenorientierten Schnittstelle `wrklnk ('home/Benutzerprofil')` ein, wobei `Benutzerprofil` der Name des Benutzerprofils ist.
2. Wählen Sie im Dialogfeld **Mit Objektverbindung arbeiten** Option 5 aus, um den Inhalt der Datei trace.txt anzuzeigen, die in diesem Verzeichnis gespeichert ist.
3. Das folgende Beispiel zeigt einen Teil einer Protokolldatei.

```
Ansehen: /home/day/trace.txt
 Satz:          1   v.    5430 um  14           Spalte :    1    140 um  79
 Strg:

 ***************Datenanfang***************
030515 08:53:13 (00000003) DBG1 KRB/KRB_GENERAL: Version 5, Release 3, Service level V5R3M0
030515 08:53:13 (00000003) DBG1 KRB/KRB_GENERAL: STDOUT handle=4, STDERR handle==-1,
DEBUG handle=4
030515 08:53:13 (00000003) DBG6 KRB/KRB_GENERAL: Using variant character table for code set 37
030515 08:53:13 (00000003) DBG1 KRB/KRB_API: --> krb5_init_context()
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Updating profile from
QIBM/USERDATA/OS400/NETWORKAUTHENTICATION/krb5.conf
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   [libdefaults]
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   default_keytab_name = /
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   default_realm = MYCO.COM
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   [realms]
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   MYCO.COM = {
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   kdc = kdc1.myco.com:88
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   kpasswd_server = kdc1.myco.com:464
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   }
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   [domain_realm]

F3=Verlassen  F10=Hex anzeigen  F12=Verlassen  F15=Services  F16=Neu suchen
F19=Links     F20=Rechts
```

Informationen über spezielle Fehlernachrichten im API-Trace finden Sie unter der entsprechenden API im Information Center. Sie haben die folgenden Möglichkeiten, auf die Informationen über diese APIs zuzugreifen:

- API Finder
- Network Authentication Service Application Programmable Interfaces (APIs)
- Generic Security Service Application Programmable Interfaces (GSS-APIs)

## Fehlerbehebung für Kerberos-Server in i5/OS PASE

Bei der Konfiguration eines Kerberos-Servers in i5/OS PASE werden der Authentifizierungsserver und der Verwaltungsserver erstellt. Diese Server schreiben Status- und Informationsnachrichten in eine Protokolldatei, die sich im Verzeichnis /var/krb5/log befindet. Die Protokolldatei krb5kdc.log enthält Nachrichten, die dem Administrator bei der Behebung von Problemen bei Konfigurations- und Authentifizierungsanforderungen helfen können.

### Auf Kerberos-Server-Protokolldateien in i5/OS PASE zugreifen

Führen Sie auf dem iSeries-Server, auf dem Sie den Kerberos-Server in i5/OS PASE konfiguriert haben, die folgenden Schritte durch:

- Geben Sie in einer zeichenorientierten Schnittstelle `QP2TERM` ein. Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, die Ihnen das Arbeiten mit i5/OS PASE-Anwendungen ermöglicht.
- Geben Sie in der Befehlszeile `cd /var/krb5/log` ein.
- Geben Sie in der Befehlszeile `cat /krb5kdc.log` ein. Damit wird die Datei krb5kdc.log geöffnet, die Fehlernachrichten für die i5/OS PASE-KDC enthält.

### Beispiel für Protokolldatei krb5kdc.log

Das folgende Beispielprotokoll enthält mehrere Nachrichten.

```
$
AS_REQ (3 etypes {16 3 1}) 10.1.1.2(88): NEEDED_PREAUTH:
jday@ISERIESA.MYCO.COM for kadmin/changepw@ISERIESA.MYCO.COM,
Zusätzliche Vorab-Authentifizierung erforderlich

Apr 30 14:18:08 iseriesa.myco.com /usr/krb5/sbin/krb5kdc[334](info):
AS_REQ (3 etypes {16 3 1}) 10.1.1.2(88): ISSUE: authtime 1051730288,
etypes {rep=16 tkt=16 ses=16}, jday@ISERIESA.MYCO.COM for
kadmin/changepw@ISERIESA.MYCO.COM

Apr 30 14:18:56 iseriesa.myco.com /usr/krb5/sbin/krb5kdc[334](Notice):
AS_REQ (3 etypes {16 3 1}) 10.1.1.2(88): NEEDED_PREAUTH:
jday@ISERIESA.MYCO.COM for kadmin/changepw@ISERIESA.MYCO.COM,
Zusätzliche Vorab-Authentifizierung erforderlich

Apr 30 14:18:56 iseriesa.myco.com /usr/krb5/sbin/krb5kdc[334](info):
DISPATCH: Wiederholungsattacke gefunden und erneut übertragen
$
```

## Referenzinformationen

Im Folgenden finden Sie eine Reihe zugehöriger Themen aus dem Information Center sowie externe Websites, die sich auf den Netzwerkauthentifizierungsservice beziehen.

**Information Center-Themen**

- Network Authentication Service Application Programmable Interfaces (APIs)
- Generic Security Service Application Programmable Interfaces (GSS-APIs)
- Enterprise Identity Mapping (EIM)
- Einzelanmeldung

**Websites**

Die folgenden Websites und Dokumentationen enthalten weitere Informationen zur Konfiguration eines Kerberos-Servers mit einem bestimmten Betriebssystem.

- Microsoft Windows 2000 Help 
- z/OS Security Server Network Authentication Service 
- IBM Network Authentication Service Version 1.3 for AIX: Administrator's and User's Guide

  **Anmerkung:** Diese Dokumentation finden Sie auf der CD: AIX 5L Expansion Pack and Bonus Pack. 

**Request for Comments (RFCs)**

RFCs (Requests for Comments) sind schriftlich niedergelegte Definitionen von Protokollstandards und vorgesehenen Standards für das Internet. Die folgenden RFCs können zum Verständnis des Kerberos-Protokolls und der zugehörigen Funktionen beitragen:

**RFC 1510**
RFC 1510: The Kerberos Network Authentication Service (V5) enthält die formale IETF-Definition (IETF = Engineering Task Force) des Kerberos-V5-Protokolls.

**RFC 2743**
RFC 2743: Generic Security Service Application Program Interface Version 2, Update 1, enthält die formale IETF-Definition der GSS-APIs.

**RFC 1509**
RFC 1509: Generic Security Service API: C-bindings enthält die formale IETF-Definition von GSS-APIs.

**RFC 1964**
RFC 1964: The Kerberos Version 5 GSS-API Mechanism enthält die IETF-Definitionen von Kerberos Version 5 und GSS-API-Spezifikationen.

Sie können die genannten RFCs mithilfe der RFC-Indexsuchmaschine auf der Website RFC Editor anzeigen. Suchen Sie nach der gewünschten RFC-Nummer. Die Ergebnisanzeige der Suchmaschine enthält den entsprechenden RFC-Titel mit Autor, Datum und Status.

## Besondere Vertragsbedingungen

### Besondere Vertragsbedingungen für Netzwerkauthentifizierungsservice (5722-SS1)

Die folgenden Vertragsbedingungen gelten nur für den Code des Netzwerkauthentifizierungsservice, der im Serviceprogramm QKRBGSS in Bibliothek QSYS, in der Teildatei KRB5 in Datei H in Bibliothek QSYSINC sowie in den Nachrichtenkatalogen skrbdll.cat und skrbkut.cat im Verzeichnis /QIBM/ProdData/OS400/NetworkAuthentication/ enthalten ist.

Der Objektcode des Netzwerkauthentifizierungsservice wird von IBM ohne Wartung (auf ″as-is″-Basis) und ohne jede Gewährleistung für die Handelsüblichkeit und die Verwendungsfähigkeit für einen bestimmten Zweck lizenziert.

IBM übernimmt keine Gewährleistung dafür, dass die Verwendung dieses Codes keine Urheberrechte, Geschäftsgeheimnisse, Patente oder sonstigen gewerblichen Schutzrechte, Eigentumsrechte oder Vertragsrechte anderer Firmen verletzt.

Entwickler müssen die folgenden Hinweise berücksichtigen:



Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided ″as is″ without express or implied warranty.

Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Neither M.I.T., the Open Computing Security Group, nor CyberSAFE Corporation make any representations about the suitability of this software for any purpose. It is provided ″as is″ without express or implied warranty.

Copyright 1995, 1996 by Richard P. Basch. All Rights Reserved. Copyright 1995, 1996 by Lehman Brothers, Inc. All Rights Reserved.

Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Richard P. Basch, Lehman Brothers and M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Richard P. Basch, Lehman Brothers and M.I.T. make no representations about the suitability of this software for any purpose. It is provided ″as is″ without express or implied warranty.

These special terms and conditions apply only to network authentication service code as described above, and to no other part of i5/OS or Licensed Internal Code.

## Besondere Vertragsbedingungen für Netzwerkauthentifizierungsservice (5722-AC3)

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. An Stelle der Produkte, Programme oder Services können auch andere ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Europe
Director of Licensing
92066 Paris La Defense Cedex
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs)

bekannt gegeben. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

Director of Licensing
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung sowie der Allgemeinen Geschäftsbedingungen der IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten der IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele der IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Musteranwendungsprogramme, die in Quellensprache geschrieben sind. Sie dürfen diese Musterprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, verwenden, vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Musterprogramme geschrieben werden.

Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. IBM kann deshalb die Zuverlässigkeit, Wartungsfreundlichkeit und Funktion dieser Programme nicht gewährleisten.

Kopien oder Teile der Musterprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

© (Name Ihrer Firma) (Jahr). Teile des vorliegenden Codes wurden aus Musterprogrammen der IBM Corp. abgeleitet.© Copyright IBM Corp. 1990, 2002 Alle Rechte vorbehalten.

Wird dieses Buch als Softcopy (Book) angezeigt, erscheinen keine Fotografien oder Farbabbildungen.

Der folgende Copyrightvermerk und Genehmigungsnachweis gilt für Teile der vorliegenden Informationen, die vom Massachusetts Institute of Technology stammen.

Copyright (C) 1985-1999 by the Massachusetts Institute of Technology.

Export of software employing encryption from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Furthermore if you modify this software you must label your software as modified software and not distribute it in such a fashion that it might be confused with the original MIT software. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided ″as is″ without express or implied warranty.

The following copyright and permission notice applies to the OpenVision Kerberos Administration system located in kadmin/create, kadmin/dbutil, kadmin/passwd, kadmin/server, lib/kadm5, and portions of lib/rpc:

Copyright, OpenVision Technologies, Inc., 1996, All Rights Reserved.

WARNING: Retrieving the OpenVision Kerberos Administration system source code, as described below, indicates your acceptance of the following terms. If you do not agree to the following terms, do not retrieve the OpenVision Kerberos administration system. You may freely use and distribute the Source Code and Object Code compiled from it, with or without modification, but this Source Code is provided to you ″AS IS″ EXCLUSIVE OF ANY WARRANTY, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY OTHER WARRANTY, WHETHER EXPRESS OR IMPLIED. IN NO EVENT WILL OPENVISION HAVE ANY LIABILITY FOR ANY LOST PROFITS, LOSS OF DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, THOSE RESULTING FROM THE USE OF THE SOURCE CODE, OR THE FAILURE OF THE SOURCE CODE TO PERFORM, OR FOR ANY OTHER REASON.

OpenVision retains all copyrights in the donated Source Code. OpenVision also retains copyright to derivative works of the Source Code, whether created by OpenVision or by a third party. The OpenVision copyright notice must be preserved if derivative works are made based on the donated Source Code. OpenVision Technologies, Inc. has donated this Kerberos Administration system to MIT for inclusion in the standard Kerberos 5 distribution. This donation underscores our commitment to continuing Kerberos technology development and our gratitude for the valuable work which has been performed by MIT and the Kerberos community.

Kerberos V5 includes documentation and software developed at the University of California at Berkeley, which includes this copyright notice:

Copyright (C) 1983 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

Permission is granted to make and distribute verbatim copies of this manual provided the copyright notices and this permission notice are preserved on all copies.

Permission is granted to copy and distribute modified versions of this manual under the conditions for verbatim copying, provided also that the entire resulting derived work is distributed under the terms of a permission notice identical to this one. Permission is granted to copy and distribute translations of this manual into another language, under the above conditions for modified versions.

The following copyrights and permission notices apply to portions of software used in Network Authentication Service Version 1.3.

Copyright (C) 1986 Gary S. Brown.

You may use this program, or code or tables extracted from it, as desired without restriction.

Copyright (C) 1998 by the FundsXpress, INC. All rights reserved. Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of FundsXpress not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. FundsXpress makes no representations about the suitability of this software for any purpose. It is provided ″as is″ without express or implied warranty.

THIS SOFTWARE IS PROVIDED ″AS IS″ AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright (c) 1990 Dennis Ferguson. All rights reserved.

Commercial use is permitted only if products which are derived from or include this software are made available for purchase and/or use in Canada. Otherwise, redistribution and use in source and binary forms are permitted.

might be confused with the original M.I.T. software. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided ″as is″ without express or implied warranty.

Copyright 1995 by Richard P. Basch. All Rights Reserved.

Copyright 1995 by Lehman Brothers, Inc. All Rights Reserved.

Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Richard P. Basch, Lehman Brothers and M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Richard P. Basch, Lehman Brothers and M.I.T. make no representations about the suitability of this software for any purpose. It is provided ″as is″ without express or implied warranty.

Copyright 1995 by OpenVision Technologies, Inc.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of OpenVision not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. OpenVision makes no representations about the suitability of this software for any purpose. It is provided ″as is″ without express or implied warranty.

OPENVISION DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL OPENVISION BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (C) 1990, RSA Data Security, Inc.

All rights reserved. License to copy and use this software is granted provided that it is identified as the ″RSA Data Security, Inc. MD4 Message Digest Algorithm ″ in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as ″derived from the RSA Data Security, Inc. MD4 Message Digest Algorithm″ in all material mentioning or referencing the derived work. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided ″as is″ without express or implied warranty of any kind. These notices must be retained in any copies of any part of this documentation and/or software.

Sun Microsystems

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part. Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.
2550 Garcia Avenue
Mountain View, California 94043

Copyright 1987, 1989 by the Student Information Processing Board of the Massachusetts Institute of Technology

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the names of M.I.T. and the M.I.T. S.I.P.B. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Furthermore if you modify this software you must label your software as modified software and not distribute it in such a fashion that it might be confused with the original M.I.T. software. M.I.T. and the M.I.T. S.I.P.B. make no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright (c) 1987, 1993 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1994 by the University of Southern California.

EXPORT OF THIS SOFTWARE from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting. WITHIN THAT CONSTRAINT, permission to copy, modify, and

distribute this software and its documentation in source and binary forms is hereby granted, provided that any documentation or other materials related to such distribution or use acknowledge that the software was developed by the University of Southern California.

DISCLAIMER OF WARRANTY. THIS SOFTWARE IS PROVIDED ″AS IS″. The University of Southern California MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. By way of example, but not limitation, the University of Southern California MAKES NO REPRESENTATIONS OR WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE. The University of Southern California shall not be held liable for any liability nor for any direct, indirect, or consequential damages with respect to any claim by the user or distributor of the ksu software.

KSU was written by: Air Medvinsky, ari@isi.edu

## Marken

Folgende Namen sind in gewissen Ländern (oder Regionen) Marken der International Business Machines Corporation:

- AIX
- IBM
- SecureWay
- Tivoli
- VisualAge

Kerberos ist eine Marke des Massachusetts Institute of Technology (MIT).

Microsoft, Windows, Windows NT und das Logo von Windows sind in gewissen Ländern (oder Regionen) Marken der Microsoft Corporation.

Andere Namen von Unternehmen, Produkten oder Services können Marken oder Servicemarken anderer Unternehmen sein.

# Anhang. Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

| IBM Europe
| Director of Licensing
| 92066 Paris La Defense Cedex
| France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt; die Verwendung dieser Websites geschieht auf eigene Verantwortung.

| Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Ver-
| pflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

| Director of Licensing
| Software Interoperability Coordinator, Department 49XA
| 3605 Highway 52 N
| Rochester, MN 55901
| U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete, der IBM Lizenzvereinbarung für Maschinencode oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht der IBM dar, unterliegen Änderungen oder können zurückgenommen werden, und repräsentieren nur die Ziele der IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Diese Veröffentlichung dient nur zu Planungszwecken. Die in dieser Veröffentlichung enthaltenen Informationen können geändert werden, bevor die beschriebenen Produkte verfügbar sind.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogrammes illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Musteranwendungsprogramme, die in Quellensprache geschrieben sind. Sie dürfen diese Musterprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, verwenden, vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Musterprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. IBM kann deshalb die Zuverlässigkeit, Wartungsfreundlichkeit und Funktion dieser Programme nicht gewährleisten.

Vorbehaltlich einer gesetzlichen Gewährleistung, die nicht ausgeschlossen werden kann, geben IBM, die 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, die Programmentwickler und Lieferanten in folgenden Fällen haftbar, auch wenn auf die Möglichkeit solcher Schäden hingewiesen wurde:

1. Verlust oder Beschädigung von Daten;
2. 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.

Kopien oder Teile der Musterprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:



## Informationen zur Programmierschnittstelle

Unter dem Thema Netzwerkauthentifizierungsservice sind die Programmierschnittstellen dokumentiert, mit deren Hilfe der Kunde Programme schreiben kann, mit denen er auf die Services von Version 5, Release 3, Modifikation 0 von i5/OS (5722–SS1) zugreifen kann.

## Marken

Folgende Namen sind in gewissen Ländern (oder Regionen) Marken der International Business Machines Corporation:

AIX
AIX 5L
Distributed Relational Database Architecture
DRDA
e (logo)server
eServer
IBM
i5/OS
iSeries
NetServer
OS/400
pSeries
SecureWay
Tivoli
VisualAge
xSeries
z/OS
zSeries

Microsoft, Windows, Windows NT und das Windows-Logo sind in gewissen Ländern Marken der Microsoft Corporation.

Andere Namen von Unternehmen, Produkten oder Services können Marken oder Servicemarken anderer Unternehmen sein.

## Bedingungen für den Download und das Drucken von Veröffentlichungen

Die Berechtigungen zur Nutzung der Informationen, die Sie zum Download ausgewählt haben, werden Ihnen auf der Basis der folgenden Bedingungen und abhängig von Ihrem Einverständnis mit diesen Bedingungen gewährt:

**Persönliche Nutzung:** Sie dürfen diese Informationen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Informationen oder Teile davon ohne ausdrückliche Genehmigung von IBM nicht weitergeben, anzeigen oder abgeleitete Arbeiten davon erstellen.

**Kommerzielle Nutzung:** Sie dürfen diese Informationen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Informationen oder Teile der Informationen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens nicht vervielfältigen, weitergeben, anzeigen oder abgeleitete Arbeiten davon erstellen.

Abgesehen von den hier gewährten Berechtigungen erhalten Sie keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Informationen oder andere darin enthaltene 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 Informationen 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 Vorschriften, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren. IBM ÜBERNIMMT KEINE GEWÄHRLEISTUNG FÜR DEN INHALT DIESER INFORMATIONEN. DIE INFORMATIONEN WERDEN OHNE WARTUNG (AUF ″AS-IS″-BASIS) UND OHNE JEDE GEWÄHRLEISTUNG FÜR DIE HANDELSÜBLICHKEIT UND DIE VERWENDUNGSFÄHIGKEIT FÜR EINEN BESTIMMTEN ZWECK ZUR VERFÜGUNG GESTELLT.

Das gesamte Material ist urheberrechtlich geschützt durch die IBM Corporation.

Durch Herunterladen und Drucken von Informationen von dieser Site erklären Sie sich mit diesen Bedingungen einverstanden.