System i

Sicherheit Netzwerkauthentifizierungsservice

Version 6 Release 1

System i

Sicherheit
Netzwerkauthentifizierungsservice

Version 6 Release 1

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen", auf Seite 145 gelesen werden.

Diese Ausgabe bezieht sich auf Version 6, Release 1, Modifikation 0 von IBM i5/OS (Produktnummer 5761–SS1) und alle nachfolgenden Releases und Modifikationen, es sei denn, es erfolgen anders lautende Angaben in neuen Ausgaben. Diese Version kann nicht auf allen RISC-Modellen (RISC = Reduced Instruction Set Computer) ausgeführt werden. Auf CICS-Modellen ist sie nicht ausführbar.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM System i Security Network authenticationf, Version 6 Release 1,
herausgegeben von International Business Machines Corporation, USA

Herausgegeben von:
SW TSC Germany
Kst. 2877
Februar 2008

Inhaltsverzeichnis

Kapitel 1. Netzwerkauthentifizierungsservice 1

Neuerungen in V6R1 1
PDF-Datei für den Netzwerkauthentifizierungsservice 2
Konzepte für Netzwerkauthentifizierungsservice . . 3
Kerberos-Konzepte 3
Funktionsweise des Netzwerkauthentifizierungsservice 4
Protokolle für Netzwerkauthentifizierungsservice 8
Umgebungsvariablen für Netzwerkauthentifizierungsservice 9
Szenarios: Netzwerkauthentifizierungsservice in einem Kerberos-Netzwerk verwenden 14
Szenario: Kerberos-Server in i5/OS PASE konfigurieren 14
Planungsarbeitsblätter ausfüllen 16
Kerberos-Server in i5/OS PASE konfigurieren 19
Verschlüsselungswerte auf dem i5/OS PASE-Kerberos-Server ändern 19
Kerberos-Server in i5/OS PASE stoppen und erneut starten. 19
Host-Principals für Windows 2000-, Windows XP- und Windows Vista-Workstations erstellen 20
Benutzer-Principals auf dem Kerberos-Server erstellen 20
Service-Principal von System A zum Kerberos-Server hinzufügen 21
Windows 2000-, Windows XP- und Windows Vista-Workstations konfigurieren 21
Netzwerkauthentifizierungsservice konfigurieren 22
Ausgangsverzeichnis für Benutzer auf System A erstellen. 22
Netzwerkauthentifizierungsservice testen . . 22
Szenario: Netzwerkauthentifizierungsservice konfigurieren 23
Planungsarbeitsblätter ausfüllen 25
Netzwerkauthentifizierungsservice auf System A konfigurieren 27
Principal von System A zum Kerberos-Server hinzufügen 28
Ausgangsverzeichnis für Benutzer auf System A erstellen. 29
Netzwerkauthentifizierungsservice auf System A testen 29
Szenario: Cross-Realm-Vertrauensbeziehung konfigurieren 30
Planungsarbeitsblätter ausfüllen 33
Ordnungsgemäßen Start des Kerberos-Servers in i5/OS PASE auf System B überprüfen . . 35
Principal für Cross-Realm-Vertrauensbeziehung auf dem i5/OS PASE-Kerberos-Server erstellen 36
Verschlüsselungswerte auf dem i5/OS PASE-Kerberos-Server ändern 36
Windows 2000-Server zur Anerkennung von SHIPDEPT.MYCO.COM konfigurieren . . . 37
Realm SHIPDEPT.MYCO.COM zu System A hinzufügen 37
Szenario: Konfiguration des Netzwerkauthentifizierungsservice an mehrere Systeme weitergeben . 38
Planungsarbeitsblätter ausfüllen 42
Systemverwaltungsgruppe erstellen 45
Systemeinstellungen vom Modellsystem (System A) an System B und System C weitergeben 45
Netzwerkauthentifizierungsservice auf System D konfigurieren 46
Principals für Endpunktsysteme zur Windows 2000-Domäne hinzufügen. 47
Szenario: Kerberos-Authentifizierung zwischen Management Central-Servern verwenden . . . 48
Planungsarbeitsblätter ausfüllen 51
Zentrales System zur Verwendung der Kerberos-Authentifizierung konfigurieren 52
Systemverwaltungsgruppe MyCo2 erstellen . 53
Systemwerte-Inventar erfassen 53
Kerberos-Einstellungen im System i Navigator vergleichen und aktualisieren 53
Management Central-Server auf dem zentralen System und den Zielsystemen erneut starten . 54
Kerberos-Service-Principal für jeden Endpunkt zur Datei für anerkannte Gruppen hinzufügen 54
Hinzufügung der Kerberos-Principals zur Datei für anerkannte Gruppen überprüfen . . 55
Gesicherte Verbindungen für das zentrale System zulassen 55
Schritte 4 bis 6 für Zielsysteme wiederholen 56
Authentifizierung auf den Endpunktsystemen testen 56
Szenario: Einzelanmeldung für i5/OS aktivieren 57
Planungsarbeitsblätter ausfüllen 62
Einzelanmeldungsbasiskonfiguration für System A erstellen 68
System B zur Nutzung der EIM-Domäne und für den Netzwerkauthentifizierungsservice konfigurieren. 70
Beide i5/OS-Service-Principals zum Kerberos-Server hinzufügen 72
Benutzerprofile auf System A und System B erstellen 73
Ausgangsverzeichnisse auf System A und System B erstellen 73
Netzwerkauthentifizierungsservice auf System A und System B testen 73
EIM-Kennungen für die beiden Administratoren John Day und Sharon Jones erstellen . . 74
Kennungszuordnungen für John Day erstellen 74
Kennungszuordnungen für Sharon Jones erstellen 75

Standardrichtlinienzuordnung für Register erstellen 77
Register für die Teilnahme an Suchoperationen und die Verwendung von Richtlinienzuordnungen aktivieren 78
EIM-Identitätsabgleiche testen 78
System i Access für Windows-Anwendungen für den Einsatz der Kerberos-Authentifizierung konfigurieren 81
Netzwerkauthentifizierungsservice und EIM-Konfiguration überprüfen 82
Hinweise zur Konfigurationsnachbereitung . . 82
Netzwerkauthentifizierungsservice planen 83
Kerberos-Server planen 83
Realms planen 85
Principal-Namen planen 87
Hinweise zur Auflösung von Hostnamen . . . 89
Hostnamen auflösen 93
Planungsarbeitsblätter für Netzwerkauthentifizierungsservice 95
Netzwerkauthentifizierungsservice konfigurieren . . 98
Kerberos-Server in i5/OS PASE konfigurieren . . 99
Verschlüsselungswerte auf dem Kerberos-Server ändern 100
Kerberos-Server stoppen und erneut starten 100
Host-, Benutzer- und Service-Principals erstellen 100
Windows 2000-, Windows XP- und Windows Vista-Workstations konfigurieren 101
Sekundären Kerberos-Server konfigurieren 102
Netzwerkauthentifizierungsservice konfigurieren 104
i5/OS-Principals zum Kerberos-Server hinzufügen 105
Ausgangsverzeichnis erstellen 108
Konfiguration des Netzwerkauthentifizierungsservice testen 108
Netzwerkauthentifizierungsservice verwalten. . . 109
Systemzeiten synchronisieren 110
Realms hinzufügen 110
Realms löschen 110
Kerberos-Server zu Realm hinzufügen 111
Kennwortserver hinzufügen 111
Vertrauensbeziehung zwischen Realms aufbauen 112
Hostauflösung ändern 112
Einstellungen für Verschlüsselung hinzufügen 113
Ticket-granting Tickets anfordern oder verlängern 113
kinit 114
Cache für Berechtigungsnachweise anzeigen . . 116
klist 116
Chiffrierschlüsseldateien verwalten 118
keytab 119
Kerberos-Kennwörter ändern 121
kpasswd 122
Verfallene Cachedateien für Berechtigungsnachweise löschen 122
kdestroy 123
Kerberos-Service-Einträge in LDAP-Verzeichnissen verwalten 125
ksetup 126
Realms in der DNS-Datenbank definieren . . . 127
Realms im LDAP-Server definieren 128
Schema auf einem LDAP-Server definieren 130
Fehler beim Netzwerkauthentifizierungsservice beheben 131
Fehler und Fehlerbehebung beim Netzwerkauthentifizierungsservice 131
Fehler und Fehlerbehebung bei der Anwendungsverbindung 132
API-Trace-Tool 136
API-Trace-Tool konfigurieren 136
Auf die API-Traceprotokolldatei zugreifen 137
Fehler des Kerberos-Servers in i5/OS PASE beheben 137
Befehle für den Netzwerkauthentifizierungsservice 138
Referenzinformationen für Netzwerkauthentifizierungsservice 139

Kapitel 2. Besondere Vertragsbedingungen 141

Anhang. Bemerkungen 145
Informationen zu Programmierschnittstellen . . . 146
Marken 146
Bedingungen 147

Kapitel 1. Netzwerkauthentifizierungsservice

Der Netzwerkauthentifizierungsservice ermöglicht es dem System i-Produkt und verschiedenen System i-Services wie z. B. dem Lizenzprogramm System i Access für Windows, für die Authentifizierung an Stelle einer Kombination aus Benutzername und Kennwort optional ein Kerberos-Ticket zu verwenden.

Das Kerberos-Protokoll, das vom Massachusetts Institute of Technology entwickelt wurde, erlaubt es einem Principal (Benutzer oder Service), seine Identität gegenüber einem anderen Service in einem nicht gesicherten Netzwerk 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. Nachdem ein Principal authentifiziert ist, gibt der Kerberos-Server ein Ticket-granting Ticket (TGT) an den Benutzer aus. Wenn ein Benutzer auf eine Anwendung oder einen Service im Netzwerk zugreifen muss, sendet die Kerberos-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-Standards sind
- GSS-APIs (GSS = Generic Security Service) laut RFCs 1509, 1964 und 2743

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

Neuerungen in V6R1

Lesen Sie die neuen oder erheblich geänderten Informationen in der Themensammlung zum Netzwerkauthentifizierungsservice.

Neue Kerberos-CL-Befehle

In V6R1 wurden die folgenden Kerberos-CL-Befehle (CL = Command Language; Steuersprache) hinzugefügt. Diese Befehle können über die Befehlszeile für CL-Befehle von i5/OS ausgeführt werden.

- Befehl ADDKRBKTE (Kerberos-Schlüsseleintrag hinzufügen)
- Befehl ADDKRBTKT (Kerberos-Ticket hinzufügen)

- Befehl CHGKRBPWD (Kerberos-Kennwort ändern)
- Befehl DLTKRBCCF (Kerberos-Cachedatei für Berechtigungsnachweise löschen)
- Befehl DSPKRBCCF (Kerberos-Cachedatei für Berechtigungsnachweise anzeigen)
- Befehl DSPKRBKTE (Schlüsseleinträge anzeigen)
- Befehl RMVKRBKTE (Kerberos-Schlüsseleintrag entfernen)

Weitere Informationen zu diesen Befehlen finden Sie in der Themensammlung zur Steuersprache (CL) und in den folgenden Themen zum Netzwerkauthentifizierungsservice:

- „Kerberos-Kennwörter ändern" auf Seite 121
- „Verfallene Cachedateien für Berechtigungsnachweise löschen" auf Seite 122
- „Cache für Berechtigungsnachweise anzeigen" auf Seite 116
- „Ticket-granting Tickets anfordern oder verlängern" auf Seite 113
- „Chiffrierschlüsseldateien verwalten" auf Seite 118

Neuer Service-Principal für den NFS-Server

Bei NFS (Network File System) handelt es sich um ein Protokoll, das einem Computer den Zugriff auf Dateien über ein Netzwerk in derselben Weise ermöglicht, wie dies beim Zugriff auf die lokalen Platten der Fall wäre. Auf der System i-Plattform können Sie nun Chiffrierschlüsseltabelleneinträge für den NFS-Server hinzufügen und aktualisieren. Weitere Informationen hierzu finden Sie in „Principal-Namen planen" auf Seite 87.

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.

In PDF-Dateien sind möglicherweise Änderungsmarkierungen (|) am linken Rand zu sehen. Diese kennzeichnen neue oder geänderte Informationen.

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

PDF-Datei für den Netzwerkauthentifizierungsservice

Sie können diese Informationen als PDF-Datei anzeigen und drucken.

Zum Anzeigen oder Herunterladen der PDF-Version dieses Dokuments wählen Sie Netzwerkauthentifizierungsservice (ca. 1.792 KB) aus.

Sie können die folgenden PDF-Dateien mit Referenzinformationen anzeigen oder herunterladen:

- Einzelanmeldung (1.147 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 (2.836 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.

Weitere Informationen

Diese Dokumentation finden Sie auf der CD AIX 5L Expansion Pack and Bonus Pack  oder auf der CD für *Network Authentication Enablement*:

- Handbücher:
  – *IBM Network Authentication ServiceAIX, Linux, and Solaris Administrator's and User's Guide*.
  – *IBM Network Authentication Service AIX, Linux, and Solaris Application Development Reference*.

PDF-Dateien speichern

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

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

Adobe Reader herunterladen

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

Konzepte für Netzwerkauthentifizierungsservice

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 Kerberos-Protokollen und GSS-APIs gibt, werden hier nur die grundlegenden Voraussetzungen erläutert, die sich speziell auf Ihre System i-Umgebung beziehen.

Kerberos-Konzepte

Der Netzwerkauthentifizierungsservice verwendet die Fachbegriffe des Kerberos-Protokolls. Hierzu gehören z. B. KDC, Principal, Chiffrierschlüsseltabelle und Kerberos-Tickets.

KDC, Principal und Chiffrierschlüsseltabelle

Das Key Distribution Center (KDC), das auch als Kerberos-Server bezeichnet wird, besteht aus dem Authentifizierungsserver und dem Ticket-granting Server. 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.

In einem Kerberos-Realm bezeichnet der Begriff *Principal* den Namen eines Benutzers oder Service. Unter dem Betriebssystem i5/OS wird der Service-Principal krbsvr400 verwendet, um den Service zu identifizieren, der von System i Access für Windows-, QFileSrv.400- und Telnet-Servern benutzt wird, um den Client gegenüber der System i-Plattform zu authentifizieren.

Die Chiffrierschlüsseltabelle besteht aus Einträgen, die den Namen des Service-Principals und dessen geheimen Schlüssel enthalten. Unter dem Betriebssystem i5/OS wird bei der Konfiguration des Netz-

werkauthentifizierungsservice eine Chiffrierschlüsseltabelle erstellt. Wenn ein Service die Authentifizierung für ein System mit konfiguriertem Netzwerkauthentifizierungsservice anfordert, überprüft das Betriebssystem, 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 unter i5/OS erstellt worden sein. Die Einträge werden der Chiffrierschlüsseltabelle während der Verarbeitung 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 89.

Kerberos-Tickets

Ein *Kerberos-Ticket* ist ein transparenter Anwendungsmechanismus, der die Identität eines einleitenden Principals an die zugehörige Zieleinheit überträgt. Ein einfaches Ticket enthält die Identität des Principals, einen Sitzungsschlüssel, eine Zeitmarke und weitere Informationen, die anhand des geheimen Schlüssels der Zieleinheit versiegelt werden. Kerberos-Tickets können verlängert und weitergeleitet werden oder sind proxyfähig.

Mit Hilfe weiterleitbarer Tickets kann die vollständige Identität (TGT) an eine andere Maschine übertragen werden, wohingegen mit proxyfähigen Tickets lediglich bestimmte Tickets übertragen werden können. Unter Verwendung proxyfähiger 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 proxyfähiges Ticket teilt dem Kerberos-Server mit, dass er auf der Basis des ursprünglichen Ticket-granting Tickets ein neues Ticket für eine andere Netzwerkadresse ausstellen kann. Für proxyfähige Tickets ist kein Kennwort erforderlich.

In bestimmten Fällen benötigt eine Anwendung oder ein Service Tickets, 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.

Funktionsweise des Netzwerkauthentifizierungsservice

Das System i-Produkt kann als Server oder Client im Kerberos-Netzwerk fungieren. Hierbei sollten Sie sich in beiden Fällen unbedingt mit den Authentifizierungsprozessen und dem Verarbeitungsablauf bei den Tickets vertraut machen.

Das Kerberos-Protokoll stellt eine Authentifizierungsmethode für Benutzer und Services in Ihrem Netzwerk zur Verfügung. Als Netzwerkadministrator können Sie den Netzwerkauthentifizierungsservice so konfigurieren, dass Ihre System i-Plattform Kerberos-Tickets als Authentifizierungsform anerkennt. Das System i-Produkt und mehrere systemspezifische 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 über Benutzerprofile verwaltet, die unter dem Betriebssystem i5/OS erstellt werden.

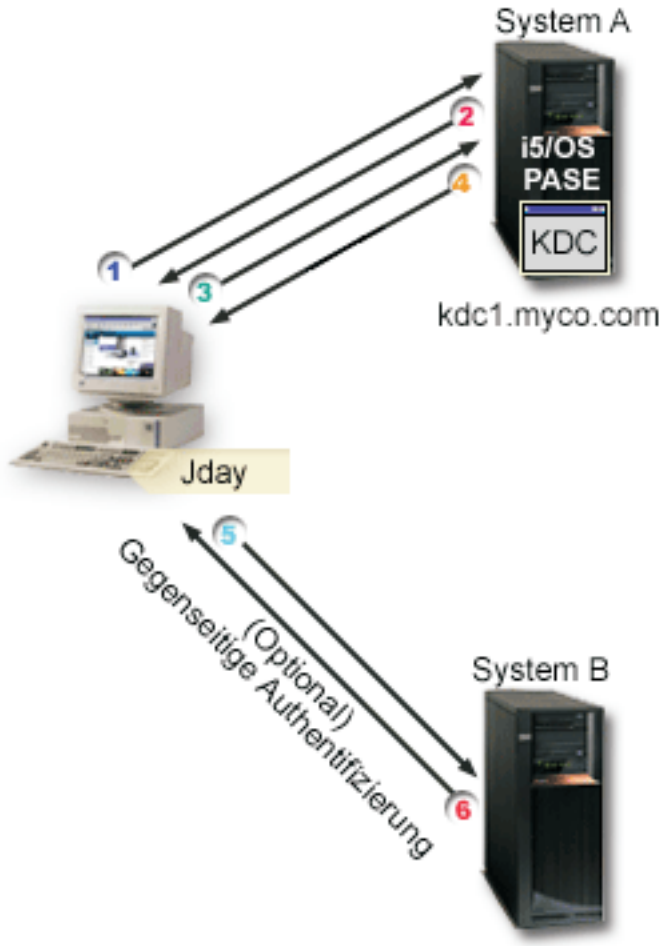
Wenn sich ein Benutzer unter Verwendung von Kerberos authentifiziert, erhält er ein erstmaliges Ticket, das als Ticket-granting Ticket (TGT) bezeichnet wird. Der Benutzer kann anschließend mit diesem TGT

ein Service-Ticket anfordern, um auf andere Services und Anwendungen im 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. Das System i-Produkt kann entweder als Server dienen, auf dem Principals die Authentifizierung für Services anfordern, oder es kann als Client dienen, der Tickets für Anwendungen und Services im Netzwerk anfordert. Die folgenden Grafiken zeigen den Verarbeitungsablauf in beiden Fällen.

System i-Produkt als Server

Diese Grafik zeigt die Funktionsweise der Authentifizierung, wenn ein System i-Produkt 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.

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



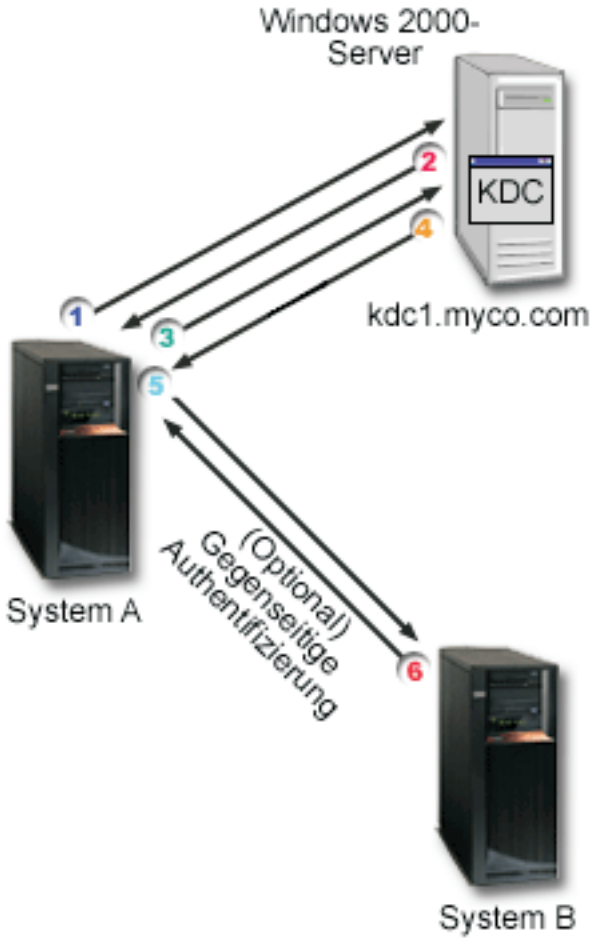
Die folgende Beschreibung gibt Ihnen eine Übersicht über die Funktionsweise des Authentifizierungsprozesses innerhalb eines Netzwerks:

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 der System i-Plattform. Die Kerberos-Clientanwendung auf dem PC von jday sendet sein TGT an den Kerberos-Server, um ein Service-Ticket für die entsprechende Anwendung oder den Service, wie beispielsweise den System i 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 System i-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.

System i-Produkt als Client

Diese Grafik zeigt die Funktionsweise der Authentifizierung, wenn ein System i-Produkt 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. System A kann für andere Services authentifiziert werden. In diesem Beispiel wird EIM auf System B verwendet, um den Kerberos-Principal einem Benutzerprofil zuzuordnen. Diese Vorgehensweise gilt für alle System i-Funktionen, 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 System A an und fordert ein Ticket-granting Ticket an, indem er den Befehl kinit im Qshell Interpreter ausführt. Das System sendet diese Anforderung an den Kerberos-Server.
2. Der Kerberos-Server prüft den Namen des Principals und das Kennwort und sendet ein Ticket-granting Ticket an jday.
3. Jday benötigt Zugriff auf eine Anwendung auf System 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.

   Anmerkung: Dem Kerberos-Server muss ein Service-Principal für System B hinzugefügt werden. Außerdem muss auf System B auch der Netzwerkauthentifizierungsservice konfiguriert werden.
5. Die Anwendung sendet das Server-Ticket an den System i-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.

Dieses Thema enthält eine allgemeine Beschreibung der Protokolle für den Netzwerkauthentifizierungsservice und zur Verwendung dieser Protokolle in der System i-Umgebung. 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 Benutzer ihre Identität gegenüber einem zentralen Server nachweisen, der als Kerberos-Server oder KDC (Key Distribution Center - Instanz zur Schlüsselverteilung) bezeichnet wird und Tickets für Benutzer ausstellt. Anhand dieser Tickets können die Benutzer dann ihre Identität innerhalb des Netzwerks nachweisen. Durch das Ticket wird die Notwendigkeit mehrerer Anmeldungen an verschiedenen Systemen hinfällig. Die von der System i-Umgebung unterstützten APIs für den Netzwerkauthentifizierungsservice wurden am Massachusetts Institute of Technology entwickelt und sind zum De-facto-Standard 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 mit Hilfe der RFC-Indexsuchmaschine auf der Website für den 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 Application Programming Interfaces (GSS-APIs)

Generic Security Services Application Programming 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 an Stelle 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 mit Hilfe der RFC-Indexsuchmaschine auf der Website für den 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 mit Hilfe 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. Das Betriebssystem i5/OS unterstützt mehrere Verwendungsmöglichkeiten von Umgebungsvariablen.

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 136. 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 für die Sicher-

heitslaufzeit mit Hilfe 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 Parent-Verzeichnis besitzen, in dem diese Datei enthalten ist. Der Benutzer muss sicherstellen, dass die allgemeine Zugriffsberechtigung für das Parent-Verzeichnis 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 Parent-Verzeichnis 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 Parent-Verzeichnis 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 Parent-Verzeichnis 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.

Die Datei krb5.conf ist in einzelne Abschnitte untergliedert, deren Name in eckigen Klammern angegeben ist. Innerhalb dieser Abschnitte werden die Gruppenwerte in geschweiften Klammern dargestellt. In V5R4 und in früheren Versionen können die eckigen und geschweiften Klammern durch die entsprechenden Trigraphen ersetzt werden. Die geltenden Zuordnungen sind in der folgenden Tabelle aufgeführt.

Zeichen	Trigraph
[(linke eckige Klammer)	??(
] (rechte eckige Klammer)	??)
{ (linke geschweifte Klammer)	??<
} (rechte geschweifte Klammer)	??>

Standardmäßig werden auf den Systemen, die mit i5/OS V6R1 arbeiten, jedoch eckige und geschweifte Klammern an Stelle der entsprechenden Trigraphen verwendet. Wenn Sie nicht mit einem Java-Kerberos-Client arbeiten, können Sie Ihr System für die Verwendung von Trigraphen konfigurieren. Zur Verwendung von Trigraphen auf dem System können Sie den ersten Buchstaben des Datenbereichs QUSRSYS/QKRBTRIGRA von der Standardeinstellung N in Y ändern, indem Sie den CL-Befehl CHGDTAARA (Datenbereich ändern) eingeben.

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 Parent-Verzeichnis 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, verwendet das System 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 Parent-Verzeichnis. Zum Aktualisieren der Datei benötigt das aktive Benutzerprofil die Berechtigung *RW. Spezifische Berechtigungen, die erforderlich sind, 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. Standardmäßig wird das Verzeichnis /QIBM/UserData/OS400/NetworkAuthentication/replay verwendet.

Szenarios: Netzwerkauthentifizierungsservice in einem Kerberos-Netzwerk verwenden

Im Folgenden werden allgemeine Szenarios aufgeführt, in denen der Netzwerkauthentifizierungsservice dem Betriebssystem i5/OS die Nutzung eines Kerberos-Netzwerks ermöglicht.

Szenario: Kerberos-Server in i5/OS PASE konfigurieren

Im vorliegenden Szenario können Sie sich mit den Zielen, Voraussetzungen und Arbeitsschritten zur Konfiguration eines Kerberos-Servers vertraut machen.

Situation

Sie arbeiten in Ihrem Unternehmen als Administrator und sind für die Sicherheitsverwaltung eines mittelgroßen Netzwerks verantwortlich. Sie möchten Benutzer über ein zentrales System 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 Windows 2000 Server Kerberos verwendet, um Benutzer für eine Windows-Domäne zu authentifizieren. Dies erhöht jedoch die Kosten im Rahmen Ihres knappen IT-Budgets. Anstatt eine Windows 2000-Domäne zur Benutzerauthentifizierung zu verwenden, haben Sie beschlossen, einen Kerberos-Server in Ihrer System i-Umgebung 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 zum Authentifizieren von Benutzern in Ihrem Netzwerk eingesetzt werden, die mit Windows 2000-, Windows XP- und Windows Vista-Workstations arbeiten.

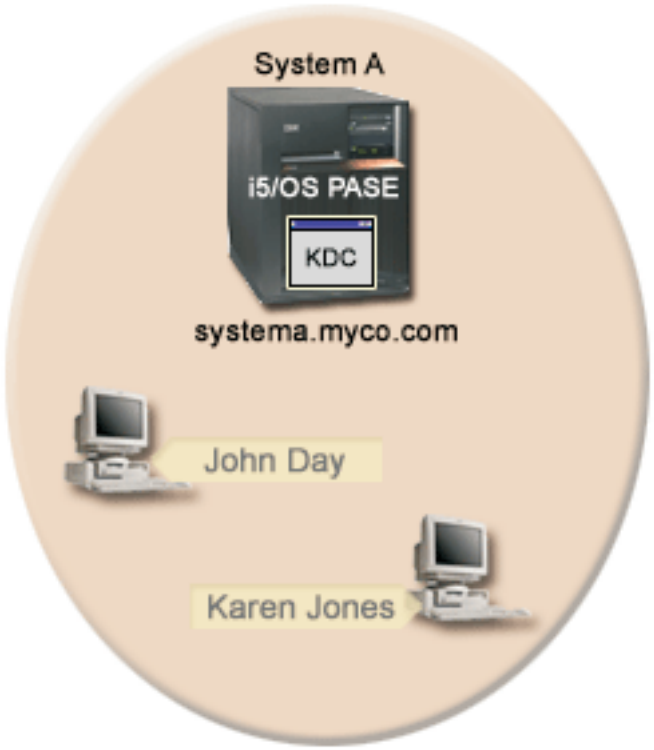
Ziele

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, Windows XP und Windows Vista ausführen, zur Nutzung des in i5/OS PASE konfigurierten Kerberos-Realms konfigurieren
- Netzwerkauthentifizierungsservice auf System A konfigurieren
- Authentifizierung in Ihrem Netzwerk testen

Details

Die folgende Abbildung veranschaulicht die Netzwerkumgebung für dieses Szenario.



System A

- Fungiert als Kerberos-Server (kdc1.myco.com) für das Netzwerk, wird auch als KDC (Key Distribution Center) bezeichnet.
- Verwendet i5/OS ab Version 5 Release 3 (V5R3) mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12)
  - i5/OS PASE (5722-SS1 Option 33 oder 5761-SS1 Option 33)
  - Qshell Interpreter (5722-SS1 Option 30 oder 5761-SS1 Option 30)
  - Network Authentication Enablement (5722-NAE oder 5761-NAE), wenn Sie mit einer Produktversion ab V5R4 arbeiten
  - Cryptographic Access Provider (5722-AC3), wenn Sie mit V5R3 arbeiten
  - System i Access für Windows (5722-XE1 oder 5761-XE1)
- Hat den vollständig qualifizierten Hostnamen systema.myco.com.

Client-PCs

- **Für alle PCs in diesem Szenario:**
  - Arbeiten mit den Betriebssystemen Windows 2000, Windows XP und Windows Vista.
  - Windows 2000-Unterstützungstools (beinhalten den Befehl ksetup) sind installiert.
- **Für Administrator-PC:**
  - System i Access für Windows (5722-XE1 oder 5761-XE1) ist installiert.
  - System i Navigator mit den Unterkomponenten ″Sicherheit″ und ″Netzwerk″ ist installiert.

Voraussetzungen und Annahmen

Dieses Szenario behandelt schwerpunktmäßig die Tasks, die zur Konfiguration eines Kerberos-Servers in i5/OS PASE ausgeführt werden müssen.

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

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

   a. Erweitern Sie im System i Navigator den Eintrag für *Ihr System* → **Konfiguration und Service** → **Software** → **Installierte Produkte**.
   b. Vergewissern Sie sich, dass alle erforderlichen Lizenzprogramme installiert sind.
2. Die gesamte erforderliche Hardwareplanung und -konfiguration wurde durchgeführt.
3. TCP/IP-Verbindungen wurden konfiguriert und in Ihrem Netzwerk getestet.
4. Für die Auflösung der Hostnamen im Netzwerk wird ein einziger DNS-Server verwendet. Es werden keine Hosttabellen für die Auflösung der Hostnamen verwendet.

   Anmerkung: Die Verwendung von Hosttabellen bei der Kerberos-Authentifizierung kann zu Fehlern bei der Namensauflösung oder anderen Problemen führen. Ausführliche Informationen zur Auflösung von Hostnamen bei der Kerberos-Authentifizierung finden Sie unter „Hinweise zur Auflösung von Hostnamen" auf Seite 89.

Konfigurationsschritte

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

Planungsarbeitsblätter ausfüllen

Vor der Konfiguration des Kerberos-Servers und des Netzwerkauthentifizierungsservice in i5/OS PASE müssen Sie die folgenden Planungsarbeitsblätter ausfüllen.

Alle Fragen auf dem Arbeitsblatt für Voraussetzungen müssen mit Ja beantwortet werden, bevor Sie mit der Konfiguration des Netzwerkauthentifizierungsservice fortfahren.

Tabelle 1. Planungsarbeitsblatt für Voraussetzungen

Fragen	Antworten
Arbeiten Sie mit i5/OS V5R3 oder einer späteren Version des Produkts (5722-SS1) oder benutzen Sie V6R1 (5761-SS1)?	Ja
Sind auf System A die folgenden Optionen und Lizenzprogramme installiert: • i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12) • i5/OS PASE (5722-SS1 Option 33 oder 5761-SS1 Option 33) • Qshell Interpreter (5722-SS1 Option 30 oder 5761-SS1 Option 30) • Network Authentication Enablement (5722-NAE oder 5761-NAE), wenn Sie mit einer Produktversion ab V5R4 arbeiten • Cryptographic Access Provider (5722-AC3), wenn Sie mit i5/OS V5R3 arbeiten • System i Access für Windows (5722-XE1 oder 5761-XE1)	Ja
Ist auf allen PCs Windows 2000, Windows XP oder Windows Vista installiert?	Ja
Sind die Windows 2000-Unterstützungstools (beinhalten den Befehl ksetup) auf allen PCs installiert?	Ja
Ist System i Access für Windows (5722-XE1 oder 5761-XE1) auf dem PC des Administrators installiert?	Ja

Tabelle 1. Planungsarbeitsblatt für Voraussetzungen (Forts.)

Fragen	Antworten
Ist System i Navigator auf dem Administrator-PC installiert? • Ist die Unterkomponente "Sicherheit" des System i Navigator auf dem PC des Administrators installiert? • Ist die Unterkomponente "Netzwerk" des System i Navigator auf dem PC des Administrators installiert?	Ja Ja Ja
Ist das aktuellste Service-Pack für System i Access für Windows installiert? Sie können das aktuellste Service-Pack über die Website für System i 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 das System i-Produkt und den Kerberos-Server?	Ja
Unter welchem Betriebssystem möchten Sie den Kerberos-Server konfigurieren? 1. Windows 2000 Server 2. Windows Server 2003 3. AIX Server 4. i5/OS PASE (ab V5R3) 5. z/OS	i5/OS PASE
Wurden die neuesten PTFs (vorläufigen Programmkorrekturen) angelegt?	Ja
Beträgt die Abweichung zwischen der Systemzeit des System i-Systems und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung größer, lesen Sie die Informationen unter „Systemzeiten synchronisieren" auf Seite 110.	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.

Tabelle 2. Planungsarbeitsblatt für Kennwörter

Entität	Kennwort
i5/OS PASE-Administrator: admin/admin **Anmerkung:** i5/OS PASE gibt `admin/admin` als Standardbenutzernamen für den Administrator an.	secret
i5/OS PASE-Datenbankmaster	pasepwd
Windows 2000-Workstations: • pc1.myco.com (PC von John Day) • pc2.myco.com (PC von Karen Jones)	secret1 secret2
Kerberos-Benutzer-Principals: • day@MYCO.COM • jones@MYCO.COM	123day 123jones
i5/OS-Service-Principal für System A: krbsvr400/systema.myco.com@MYCO.COM	systema123

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 Voraussetzungen und dem Planungsarbeitsblatt für Kenn-

wörter 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 **Port:** 88 **Anmerkung:** Dies ist der Standardport für den Kerberos-Server.
Möchten Sie einen Kennwortserver für diesen Standard-Realm konfigurieren?	Nein **Anmerkung:** Gegenwärtig werden Kennwortserver von i5/OS PASE oder AIX nicht unterstützt.
Für welche Services möchten Sie Chiffrierschlüsseleinträge erstellen? • i5/OS-Kerberos-Authentifizierung • LDAP • IBM HTTP-Server • i5/OS NetServer • NFS-Server	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? Welches Kennwort möchten Sie für den i5/OS PASE-Administrator angeben?	Benutzername: admin/admin Kennwort: secret
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: • John Day • Karen Jones	day@MYCO.COM jones@MYCO.COM
Wie lauten die i5/OS-Benutzerprofilnamen für diese Benutzer: • John Day • Karen Jones	JOHND KARENJ
Wie lauten die Windows 2000-Benutzernamen für diese Benutzer: • John Day • Karen Jones	johnday karenjones
Wie lauten die Hostnamen für diese Windows 2000-Workstations: • PC von John Day • PC von Karen Jones	pc1.myco.com pc2.myco.com

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

Fragen	Antworten
Wie lautet der Name des i5/OS-Service-Principals für System A?	krbsvr400/systema.myco.com@MYCO.COM **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.

Kerberos-Server in i5/OS PASE konfigurieren

Zur Konfiguration eines Kerberos-Servers in i5/OS PASE auf System A sollten Sie die Informationen heranziehen, die in Ihren Planungsarbeitsblättern dokumentiert sind.

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

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 `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 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, die folgenden Kennwörter einzugeben:
   - Hauptkennwort für Datenbank: `pasepwd`
   - Kennwort für Principal admin/admin: `secret`
4. Drücken Sie F3 (Verlassen), um die PASE-Umgebung zu verlassen.

Verschlüsselungswerte auf dem i5/OS PASE-Kerberos-Server ändern

Für den Einsatz auf Windows-Workstations müssen die Standardverschlüsselungseinstellungen auf dem Kerberos-Server so geändert werden, dass Clients auf dem i5/OS PASE-Kerberos-Server authentifiziert werden können.

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
arcfour-hmac:normal aes256-cts:normal
des-cbc-md5:normal des-cbc-crc:normal
```

   in

```
supported_enctypes = des-cbc-crc:normal dec-cbc-md5:normal
```

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, um den Kerberos-Server zu stoppen und erneut zu starten:

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.

Host-Principals für Windows 2000-, Windows XP- und Windows Vista-Workstations erstellen

Sie müssen die Host-Principals, die Kerberos zur Authentifizierung der PC-Benutzer verwendet, erstellen.

Wenn Sie bereits mit i5/OS PASE arbeiten, 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.

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. Führen Sie die folgenden Schritte durch, um Benutzer-Principals 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 einer kadmin-Eingabeaufforderung `addprinc -pw 123day day` ein.

Nach Abschluss dieser Schritte wird die folgende Nachricht ausgegeben:

```
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 dabei jedoch als Principal-Namen `jones` und als Kennwort `123jones` ein.

Service-Principal von System A zum Kerberos-Server hinzufügen

Damit i5/OS-Schnittstellen Kerberos-Tickets akzeptieren können, müssen Sie diese als Principals zum Kerberos-Server hinzufügen.

Führen Sie die folgenden Schritte durch, um den Service-Principal hinzuzufügen. Wenn Sie sich bereits in der kadmin-Umgebung befinden, können Sie die Schritte 1 bis 4 überspringen.

1. Geben Sie in einer zeichenorientierten Schnittstelle in der Befehlszeile `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 -pw systema123 krbsvr400/systema.myco.com` ein. Daraufhin erhalten Sie die folgende Nachricht:

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

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

Windows 2000-, Windows XP- und Windows Vista-Workstations konfigurieren

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 Einzelanmeldungsumgebung zu erstellen, müssen Sie diesen Schritt durchführen. Ist das nicht der Fall, fahren Sie mit Schritt 9 (Netzwerkauthentifizierungsservice konfigurieren) fort.

Konfigurieren 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.

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.

6. 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`

   Zugehörige Konzepte

   Szenario: Einzelanmeldungstestumgebung erstellen

Netzwerkauthentifizierungsservice konfigurieren

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

1. Erweitern Sie im System i Navigator den Eintrag für **System 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 Auswahl **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. Klicken Sie auf **Weiter**.
5. Geben Sie auf der Seite 'KDC-Informationen angeben' im Feld **KDC** für den Kerberos-Server den Wert `kdc1.myco.com` und im Feld **Port** den Wert `88` ein. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite 'Kennwortserverinformationen angeben' die Einstellung **Nein** aus. Klicken Sie auf **Weiter**.
7. Wählen Sie auf der Seite 'Chiffrierschlüsseleinträge auswählen' **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: `systema123`. Dieses Kennwort wird verwendet, wenn System 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**.

Ausgangsverzeichnis für Benutzer auf System A erstellen

Jeder Benutzer, der eine Verbindung zum Betriebssystem i5/OS und zu i5/OS-Anwendungen herstellen möchte, benötigt ein Verzeichnis im Ausgangsverzeichnis (/home). Dieses Verzeichnis enthält den Namen des Kerberos-Caches für Berechtigungsnachweise, der dem Benutzer zugeordnet ist.

Führen Sie die folgenden Schritte durch, um ein Ausgangsverzeichnis für die Benutzer auf System A zu erstellen:

1. 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.
2. Wiederholen Sie den Befehl für Karen Jones, geben Sie dabei jedoch ihr i5/OS-Benutzerprofil `KARENJ` an.

Netzwerkauthentifizierungsservice testen

Zum Testen der Konfiguration des Netzwerkauthentifizierungsservice müssen Sie ein Ticket-granting Ticket für Ihren i5/OS-Principal und andere Principals innerhalb Ihres Netzwerks 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 anzuzeigen, die in der Chiffrierschlüsseldatei registriert sind. Die folgenden Ergebnisse sollten angezeigt werden:

```
Principal: krbsvr400/systema.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/systema.myco.com@MYCO.COM` ein, um ein Ticket-granting Ticket vom Kerberos-Server anzufordern. Mit diesem Befehl wird geprüft, ob Ihr System richtig konfiguriert wurde und das Kennwort in der Chiffrierschlüsseldatei mit dem auf dem Kerberos-Server gespeicherten Kennwort übereinstimmt. Wenn die Prüfung erfolgreich verläuft, dann werden für den Befehl QSH keine Fehler ausgegeben.
4. Geben Sie `klist` ein, um sicherzustellen, dass der Standard-Principal krbsvr400/systema.myco.com@MYCO.COM lautet. Mit diesem Befehl wird der Inhalt eines Kerberos-Caches für Berechtigungsnachweise angezeigt und geprüft, ob ein gültiges Ticket für den i5/OS-Service-Principal erstellt und in den Cache für Berechtigungsnachweise auf dem System aufgenommen wurde.

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

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

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

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

Szenario: Netzwerkauthentifizierungsservice konfigurieren

Im Folgenden erfahren Sie, welche Voraussetzungen zum Hinzufügen des Netzwerkauthentifizierungsservice zu Ihrem Netzwerk erfüllt werden müssen und zu welchem Zweck dieser Service hinzugefügt wird.

Situation

Sie sind ein Netzwerkadministrator, der das Netzwerk für die Auftragsannahmeabteilung in Ihrem Unternehmen verwaltet. Sie haben kürzlich ein System i-Produkt zum Netzwerk hinzugefügt, auf dem verschiedene Anwendungen ausgeführt werden sollen, die für Ihre Abteilung erforderlich sind. In Ihrem Netzwerk verwalten Sie Benutzer mit Microsoft 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 Systeme im Netzwerk wird verringert.
- Das Sicherheitsrisiko durch Kennwortdiebstahl wird verringert.

Ziele

In diesem Szenario möchte MyCo, Inc. ein System i-Produkt zu einem vorhandenen Realm hinzufügen, in dem ein Windows 2000-Server als Kerberos-Server fungiert. Die System i-Plattform enthält verschiedene

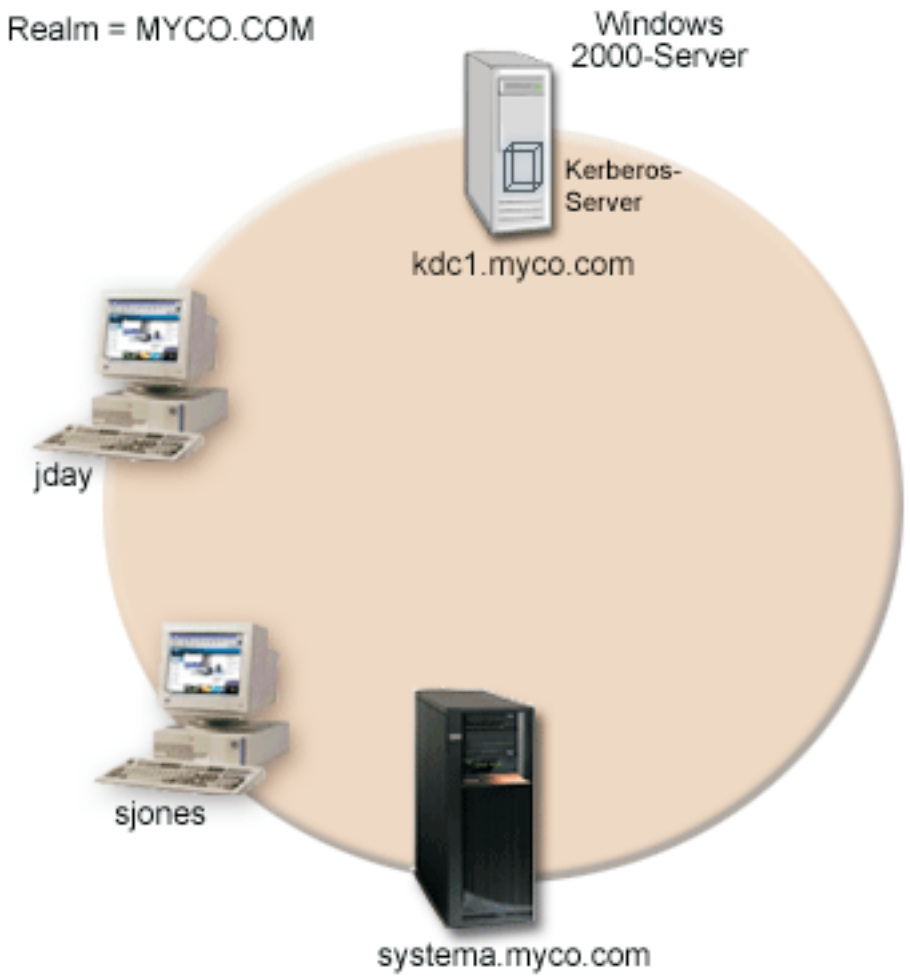
geschäftskritische Anwendungen, auf die nur die richtigen Benutzer Zugriff haben sollen. Benutzer müssen vom Kerberos-Server authentifiziert werden, um die Zugriffsberechtigung für diese Anwendungen zu erhalten.

Dieses Szenario hat die folgenden Ziele:

- Der System i-Plattform soll die Nutzung eines vorhandenen Kerberos-Servers ermöglicht werden.
- Es sollen sowohl Principal-Namen als auch Benutzernamen im Netzwerk zugelassen werden.
- Kerberos-Benutzern soll die Änderung eigener Kennwörter auf dem Kerberos-Server ermöglicht werden.

Details

Die folgende Abbildung veranschaulicht die Netzwerkkenndaten von MyCo.



System A

- Arbeitet mit i5/OS ab V5R3 mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12)
  - Qshell Interpreter (5722-SS1 Option 30 oder 5761-SS1 Option 30)
  - System i Access für Windows (5722-XE1 oder 5761-XE1)

  - Network Authentication Enablement (5722-NAE oder 5761-NAE), wenn Sie mit einer Produktversion ab V5R4 arbeiten
  - Cryptographic Access Provider (5722-AC3), wenn Sie mit V5R3 arbeiten
- Der Principal-Name für System A lautet krbsvr400/systema.myco.com@MYCO.COM.

Windows 2000-Server
- Fungiert als Kerberos-Server für den Realm MYCO.COM.
- Der vollständig qualifizierte Hostname des Kerberos-Servers lautet kdc1.myco.com.

Client-PCs
- Verwenden Windows 2000.
- Auf dem PC zur Verwaltung des Netzwerkauthentifizierungsservice sind die folgenden Produkte installiert:
  - System i Access für Windows (5722-XE1 oder 5761-XE1)
  - System i 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 die erforderlichen Lizenzprogramme installiert wurden:

   a. Erweitern Sie im System i Navigator den Eintrag für ***Ihr System*** → **Konfiguration und Service** → **Software** → **Installierte Produkte**.
   b. Vergewissern Sie sich, dass alle erforderlichen Lizenzprogramme installiert sind.
2. Die gesamte erforderliche Hardwareplanung und -konfiguration wurde durchgeführt.
3. TCP/IP und die Basissystemsicherheit wurden auf jedem dieser Server konfiguriert und getestet.
4. Für die Auflösung der Hostnamen im Netzwerk wird ein einziger DNS-Server verwendet. Es werden keine Hosttabellen für die Auflösung der Hostnamen verwendet.

   Anmerkung: Die Verwendung von Hosttabellen bei der Kerberos-Authentifizierung kann zu Fehlern bei der Namensauflösung oder anderen Problemen führen. Ausführliche Informationen zur Auflösung von Hostnamen bei der Kerberos-Authentifizierung finden Sie unter „Hinweise zur Auflösung von Hostnamen” auf Seite 89.

Konfigurationsschritte

Führen Sie die folgenden Schritte aus, um den Netzwerkauthentifizierungsservice auf Ihrem System zu konfigurieren.

Planungsarbeitsblätter ausfüllen

Vor der Konfiguration des Netzwerkauthentifizierungsservice müssen Sie die folgenden Planungsarbeitsblätter ausfüllen.

Alle Fragen 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
Ist auf Ihrem System i5/OS V5R3 oder eine spätere Version des Produkts (5722-SS1) oder V6R1 (5761-SS1) installiert?	Ja

Tabelle 4. Arbeitsblatt für Voraussetzungen (Forts.)

Fragen	Antworten
Sind die folgenden Lizenzprogramme auf System A installiert: • i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12) • Qshell Interpreter (5722-SS1 Option 30 oder 5761-SS1 Option 30) • System i Access für Windows (5722-XE1 oder 5761-XE1) • Network Authentication Enablement (5722-NAE oder 5761-NAE), wenn Sie mit i5/OS ab V5R4 arbeiten • Cryptographic Access Provider (5722-AC3), wenn Sie mit i5/OS V5R3 arbeiten	Ja
Ist Windows 2000 auf Ihren PCs installiert?	Ja
Ist System i Access für Windows (5722-XE1 oder 5761-XE1) auf dem PC des Administrators installiert?	Ja
Ist System i Navigator auf dem Administrator-PC installiert? • Ist die Unterkomponente "Sicherheit" des System i Navigator auf dem PC des Administrators installiert? • Ist die Unterkomponente "Netzwerk" des System i Navigator auf dem PC des Administrators installiert?	Ja Ja Ja
Ist das aktuellste Service-Pack für System i Access für Windows installiert? Sie können das aktuellste Service-Pack über die Website für System i Access abrufen.	Ja
Verfügen Sie über 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? 1. Windows 2000 Server 2. Windows Server 2003 3. AIX Server 4. i5/OS PASE (ab V5R3) 5. z/OS	Ja, Windows 2000 Server
Sind alle PCs Ihres Netzwerks in einer Windows 2000-Domäne konfiguriert? **Anmerkung:** Eine Windows 2000-Domäne ist mit einem Kerberos-Realm vergleichbar. Das Microsoft Active Directory verwendet die Kerberos-Authentifizierung als Standardsicherheitsmechanismus.	Ja
Wurden die neuesten PTFs (vorläufigen Programmkorrekturen) angelegt?	Ja
Beträgt die Abweichung zwischen der Systemzeit des System i-Systems und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung größer, lesen Sie die Informationen unter „Systemzeiten synchronisieren" auf Seite 110.	Ja

Tabelle 5. Planungsarbeitsblatt für Netzwerkauthentifizierungsservice

Fragen	Antworten
Wie lautet der Name des Kerberos-Standard-Realms, zu dem Ihr System gehören soll? **Anmerkung:** Eine Windows 2000-Domäne ist mit einem Kerberos-Realm vergleichbar. 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 **Port:** 88 **Anmerkung:** Dies ist der Standardport für den Kerberos-Server.

Tabelle 5. Planungsarbeitsblatt für Netzwerkauthentifizierungsservice (Forts.)

Fragen	Antworten
Möchten Sie einen Kennwortserver für diesen Standard-Realm konfigurieren? Wenn ja, beantworten Sie die folgenden Fragen: Wie lautet der Name des Kennwortservers für diesen Kerberos-Server? An welchem Port ist der Kennwortserver empfangsbereit?	Ja **Kennwortserver:** kdc1.myco.com **Port:** 464 **Anmerkung:** Dies ist der Standardport für den Kennwortserver.
Für welche Services möchten Sie Chiffrierschlüsseleinträge erstellen? • i5/OS-Kerberos-Authentifizierung • LDAP • IBM HTTP-Server • i5/OS NetServer • NFS-Server	i5/OS-Kerberos-Authentifizierung
Welches Kennwort soll für Ihre i5/OS-Service-Principals verwendet werden?	systema123
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 SHARONJ

Netzwerkauthentifizierungsservice auf System A konfigurieren

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

1. Erweitern Sie im System i Navigator den Eintrag für **System 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 Auswahl **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** für den Kerberos-Server den Wert `kdc1.myco.com` und im Feld **Port** den Wert `88` ein. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite 'Kennwortserverinformationen angeben' die Einstellung **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' **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: `systema123`. Dieses Kennwort wird verwendet, wenn System A zum Kerberos-Server hinzugefügt wird. Klicken Sie auf **Weiter**.
9. Optional: Wählen Sie auf der Seite 'Stapeldatei erstellen' die Einstellung **Ja** aus, um diese Datei zu erstellen, und machen Sie die folgenden Angaben:
   - **Stapeldatei:** Fügen Sie am Ende des standardmäßig verwendeten Stapeldateinamens die Zeichenfolge `systema` an. Beispiel: `C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystema.bat`.

- Wählen Sie **Kennwort einfügen** aus. Dies garantiert, dass alle Kennwörter, die dem i5/OS-Service-Principal zugeordnet sind, in die Stapeldatei eingefügt werden. Beachten Sie, dass Kennwörter in Klartext angezeigt werden und von jeder Person mit Lesezugriffsberechtigung für die Stapeldatei gelesen werden können. Daher wird empfohlen, dass Sie die Stapeldatei nach dem Gebrauch unverzüglich vom Kerberos-Server und von Ihrem PC löschen.

  Anmerkung: Alternativ dazu können Sie Service-Principals, die vom Assistenten generiert wurden, manuell zum Kerberos-Server hinzufügen. Informationen zum manuellen Hinzufügen des i5/OS-Service-Principals zum Kerberos-Server finden Sie in „i5/OS-Principals zum Kerberos-Server hinzufügen" auf Seite 105.

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

Principal von System A zum Kerberos-Server hinzufügen

Sie können dem Kerberos-Server manuell einen i5/OS-Service-Principal hinzufügen. Wie im folgenden Szenario dargestellt, können Sie auch die in Schritt 2 erstellte Stapeldatei verwenden, um den Principal hinzuzufügen.

Zur Verwendung der Stapeldatei müssen Sie diese mit Hilfe von 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:

1. Vom Assistenten erstellte FTP-Stapeldatei.
   a. 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. Mit diesem Befehl wird eine FTP-Sitzung auf Ihrem PC gestartet. Sie werden aufgefordert, den Benutzernamen und das Kennwort des Administrators einzugeben.
   b. Geben Sie bei der FTP-Eingabeaufforderung `lcd "C:\Documents and Settings\All Users\Documents\IBM\Client Access"` ein. Drücken Sie die Eingabetaste. Daraufhin sollte die Nachricht `Lokales Verzeichnis jetzt C:\Documents and Settings\All Users\Documents\IBM\Client Access` angezeigt werden.
   c. Geben Sie bei der FTP-Eingabeaufforderung `binary` ein. Das bedeutet, dass es sich bei der zu übertragenden Datei um eine Binärdatei handelt.
   d. Geben Sie bei der FTP-Eingabeaufforderung `cd \meinVerzeichnis` ein. *meinVerzeichnis* bezeichnet ein auf kdc1.myco.com befindliches Verzeichnis.
   e. Geben Sie bei der FTP-Eingabeaufforderung `put NASConfigsystema.bat` ein. Daraufhin sollte die Nachricht: `226 Übertragung abgeschlossen` (oder ähnlicher Wortlaut) angezeigt werden.
2. Stapeldatei auf kdc1.myco.com ausführen.
   a. Öffnen Sie auf dem Windows 2000-Server den Ordner, in den Sie die Stapeldateien übertragen haben.
   b. Suchen Sie die Datei NASConfigsystema.bat, und führen Sie sie durch Doppelklicken aus.
   c. 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:
      1) Erweitern Sie auf dem Windows 2000-Server **Start** → **Programme** → **Verwaltungstools** → **Active Directory-Benutzer und -Computer** → **Benutzer**.
      2) Vergewissern Sie sich, dass das System 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.
      3) Suchen Sie in der angezeigten Benutzerliste den Eintrag **systema_1_krbsvr400**. Dies ist das Benutzerkonto, das für den i5/OS-Principal-Namen generiert wurde.

4) **Optional:** Rufen Sie die Eigenschaften der Active Directory-Benutzer auf. Wählen Sie auf der Indexzunge **Konto** die Auswahl **Konto wird für Delegierungszwecke vertraut** aus.

   Anmerkung: Dieser optionale Schritt ermöglicht es 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.

Ausgangsverzeichnis für Benutzer auf System A erstellen

Jeder Benutzer, der eine Verbindung zu i5/OS und zu i5/OS-Anwendungen herstellen möchte, benötigt ein Verzeichnis im Ausgangsverzeichnis (/home). Dieses Verzeichnis enthält den Namen des Kerberos-Caches für Berechtigungsnachweise, der dem Benutzer zugeordnet ist.

Gehen Sie folgendermaßen vor, um ein Ausgangsverzeichnis für einen Benutzer zu erstellen:

1. Geben Sie in einer i5/OS-Befehlszeile `CRTDIR '/home/Benutzerprofil'` ein, wobei `Benutzerprofil` der Name des i5/OS-Benutzerprofils des Benutzers ist. Beispiel: `CRTDIR '/home/JOHND'` für den Benutzer John Day.
2. Wiederholen Sie den Befehl für Sharon Jones, geben Sie dabei jedoch ihr i5/OS-Benutzerprofil `SHARONJ` an.

Netzwerkauthentifizierungsservice auf System A testen

Um sicherzustellen, dass der Netzwerkauthentifizierungsservice ordnungsgemäß konfiguriert wurde, müssen Sie ein Ticket-granting Ticket für den Principal von System A anfordern.

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. Die folgenden Ergebnisse sollten angezeigt werden:

```
Principal: krbsvr400/systema.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/systema.myco.com@MYCO.COM` ein, um ein Ticket-granting Ticket vom Kerberos-Server anzufordern. Mit diesem Befehl wird geprüft, ob Ihr System richtig konfiguriert wurde und das Kennwort in der Chiffrierschlüsseldatei mit dem auf dem Kerberos-Server gespeicherten Kennwort übereinstimmt. Wenn die Prüfung erfolgreich verläuft, dann werden für den Befehl QSH keine Fehler ausgegeben.
4. Geben Sie `klist` ein, um sicherzustellen, dass der Standard-Principal krbsvr400/systema.myco.com@MYCO.COM lautet. Mit diesem Befehl wird der Inhalt eines Kerberos-Caches für Berechtigungsnachweise angezeigt und geprüft, ob ein gültiges Ticket für den i5/OS-Service-Principal erstellt und in den Cache für Berechtigungsnachweise auf dem System aufgenommen wurde.

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

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

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

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

Szenario: Cross-Realm-Vertrauensbeziehung konfigurieren

Im Folgenden erfahren Sie, welche Voraussetzungen zum Konfigurieren einer Cross-Realm-Vertrauensbeziehung in Ihrem Netzwerk erfüllt werden müssen und zu welchem Zweck diese Konfiguration dient.

Situation

Sie sind Sicherheitsadministrator für ein Großhandelsunternehmen. Gegenwärtig verwalten Sie die Sicherheit für Systeme, die von Mitarbeitern der Auftragsannahme- und der Versandabteilung verwendet werden. Sie haben einen Kerberos-Server für die Auftragsannahmeabteilung konfiguriert. Sie haben den Netzwerkauthentifizierungsservice in der System i-Umgebung in dieser Abteilung so konfiguriert, dass er auf diesen Kerberos-Server verweist. Die Versandabteilung arbeitet mit einem System i-Produkt, das einen in i5/OS PASE konfigurierten Kerberos-Server besitzt. Sie haben auf diesem System i-Produkt den Netzwerkauthentifizierungsservice auch so konfiguriert, dass er auf den Kerberos-Server in i5/OS PASE verweist.

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

Ziele

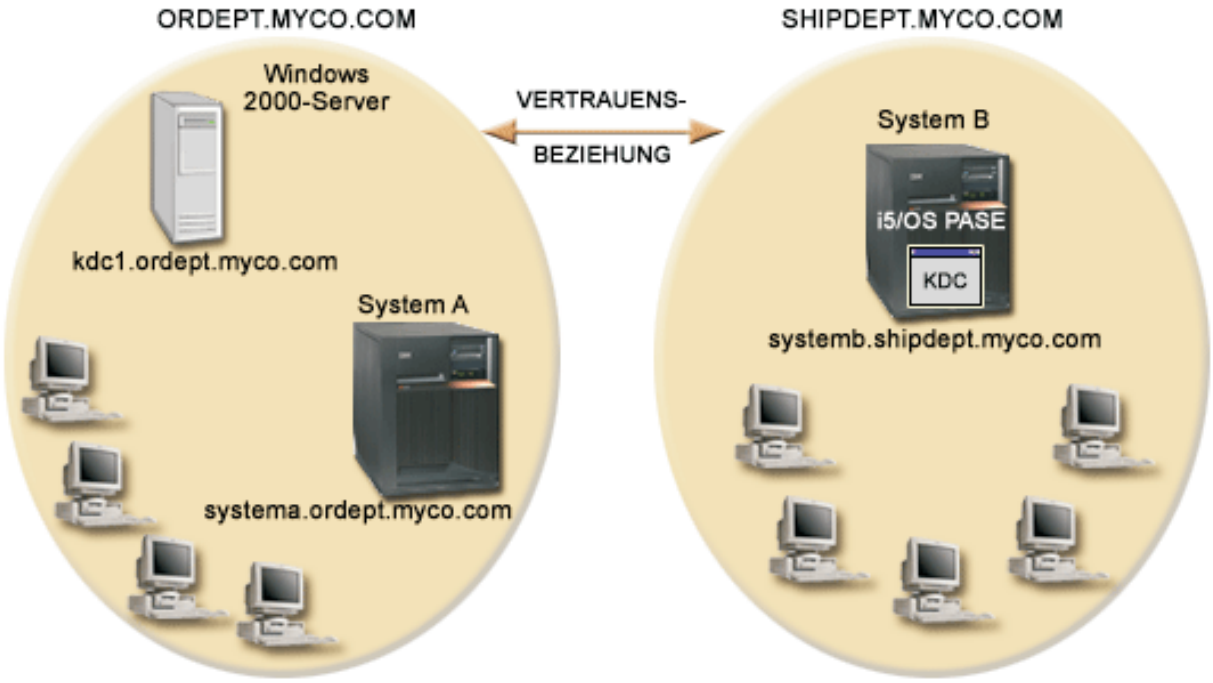
In diesem Szenario möchte MyCo, Inc. eine Vertrauensbeziehung zwischen zwei bereits bestehenden Kerberos-Realms herstellen. Ein Realm besteht aus einem Windows 2000-Server, der als Kerberos-Server für die Auftragsannahmeabteilung fungiert. Dieser Server authentifiziert Benutzer, die in dieser Abteilung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

Dieses Szenario hat die folgenden Ziele:

- Clients und Hosts in jedem Netzwerk die Zugriffsberechtigung für das jeweils andere Netzwerk erteilen
- Authentifizierung in Netzwerken vereinfachen
- Ticket-Delegierung für Benutzer und Services in beiden Netzwerken zulassen

Details

Im Folgenden finden Sie eine detaillierte Beschreibung der Umgebung, die in diesem Szenario verwendet wird, einschließlich einer Abbildung, die die Topologie und alle wichtigen Elemente dieser Umgebung sowie deren wechselseitige Beziehungen veranschaulicht.



Auftragsannahmeabteilung

System A

- Arbeitet mit i5/OS ab V5R3 mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12)
  - System i Access für Windows (5722-XE1 oder 5761-XE1)
  - Network Authentication Enablement (5722-NAE oder 5761-NAE), wenn Sie mit i5/OS ab V5R4 arbeiten
  - Cryptographic Access Provider (5722-AC3), wenn Sie mit i5/OS V5R3 arbeiten
- Der Netzwerkauthentifizierungsservice ist für die Nutzung des Realms ORDEPT.MYCO.COM konfiguriert. Der i5/OS-Principal krbsrv400/systema.ordept.myco.com@ORDEPT.MYCO.COM wurde zur Windows 2000-Domäne hinzugefügt.
- System A hat den vollständig qualifizierten Hostnamen systema.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 Auftragsannahmeabteilung 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:
  - System i Access für Windows (5722-XE1 oder 5761-XE1)
  - System i Navigator und die folgenden Unterkomponenten:
    - Sicherheit
    - Netzwerk

Versandabteilung

System B

- Arbeitet mit i5/OS V5R3 mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS PASE (5722-SS1 Option 33)
  - Cryptographic Access Provider (5722-AC3)
  - System i 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 Nutzung des Realms SHIPDEPT.MYCO.COM konfiguriert. Der i5/OS-Principal krbsrv400/systemb.shipdept.myco.com@SHIPDEPT.MYCO.COM wurde dem i5/OS PASE-Kerberos-Server hinzugefügt.
- System B und der i5/OS PASE-Kerberos-Server verwenden den vollständig qualifizierten Hostnamen systemb.shipdept.myco.com gemeinsam.
- Jeder Benutzer, der in der Versandabteilung arbeitet, wurde auf dem i5/OS PASE-Kerberos-Server mit einem Principal-Namen und einem entsprechenden Kennwort definiert.

Client-PCs

- Verwenden das Betriebssystem Windows 2000.
- Auf dem PC zur Verwaltung des Netzwerkauthentifizierungsservice sind die folgenden Produkte installiert:
  - System i Access für Windows (5722-XE1 oder 5761-XE1)
  - System i 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.

System 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 System i Navigator den Eintrag für ***Ihr System*** → **Konfiguration und Service** → **Software** → **Installierte Produkte**.
   b. Vergewissern Sie sich, dass alle erforderlichen Lizenzprogramme installiert sind.
2. Die gesamte erforderliche Hardwareplanung und -konfiguration wurde durchgeführt.
3. TCP/IP und die Basissystemsicherheit wurden auf System A konfiguriert und getestet.
4. Der Netzwerkauthentifizierungsservice wurde konfiguriert und getestet.
5. Für die Auflösung der Hostnamen im Netzwerk wird ein einziger DNS-Server verwendet. Es werden keine Hosttabellen für die Auflösung der Hostnamen verwendet.

   Anmerkung: Die Verwendung von Hosttabellen bei der Kerberos-Authentifizierung kann zu Fehlern bei der Namensauflösung oder anderen Problemen führen. Ausführliche Informationen zur Auflösung von Hostnamen bei der Kerberos-Authentifizierung finden Sie unter „Hinweise zur Auflösung von Hostnamen" auf Seite 89.

System 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 System i Navigator den Eintrag für ***Ihr System*** → **Konfiguration und Service** → **Software** → **Installierte Produkte**.
   b. Vergewissern Sie sich, dass alle erforderlichen Lizenzprogramme installiert sind.
2. Die gesamte erforderliche Hardwareplanung und -konfiguration wurde durchgeführt.
3. TCP/IP und die Basissystemsicherheit wurden auf Ihrem System 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 Auftragsannahmeabteilung 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.

Planungsarbeitsblätter ausfüllen

Vor der Definition einer Cross-Realm-Vertrauensbeziehung müssen Sie die folgenden Planungsarbeitsblätter ausfüllen.

Alle Fragen auf dem Arbeitsblatt für die Voraussetzungen müssen mit Ja beantwortet werden, bevor Sie mit der Konfiguration einer Cross-Realm-Vertrauensbeziehung fortfahren.

Tabelle 6. Planungsarbeitsblatt für Voraussetzungen

Fragen	Antworten
Ist auf Ihrem System i5/OS V5R3 oder eine spätere Version des Produkts (5722-SS1) oder V6R1 (5761-SS1) installiert?	Ja
Sind auf System A die folgenden Optionen und Lizenzprogramme installiert: • i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12) • System i Access für Windows (5722-XE1 oder 5761-XE1) • Network Authentication Enablement (5722-NAE oder 5761-NAE), wenn Sie mit i5/OS ab V5R4 arbeiten • Cryptographic Access Provider (5722-AC3), wenn Sie mit i5/OS V5R3 arbeiten	Ja
Sind die folgenden Lizenzprogramme auf System B installiert: • System i Access für Windows (5722-XE1 oder 5761-XE1) • Network Authentication Enablement (5722-NAE oder 5761-NAE), wenn Sie mit i5/OS ab V5R4 arbeiten • Cryptographic Access Provider (5722-AC3), wenn Sie mit i5/OS V5R3 arbeiten • i5/OS PASE (5722-SS1 Option 33 oder 5761-SS1 Option 33)	Ja
Ist auf allen PCs Windows 2000 installiert?	Ja
Ist System i Access für Windows (5722-XE1 oder 5761-XE1) auf dem PC installiert, der zur Verwaltung des Netzwerkauthentifizierungsservice verwendet wird?	Ja

Tabelle 6. Planungsarbeitsblatt für Voraussetzungen (Forts.)

Fragen	Antworten
Sind der System i Navigator und die folgenden Unterkomponenten auf dem PC installiert, der zur Verwaltung des Netzwerkauthentifizierungsservice verwendet wird? • Sicherheit • Netzwerk	Ja
Ist das aktuellste Service-Pack für System i Access für Windows installiert? Sie können das aktuellste Service-Pack über die Website für System i Access  abrufen.	Ja
Besitzen Sie die Sonderberechtigung *ALLOBJ für die Systeme?	Ja
Besitzen Sie die Administratorberechtigung für den Windows 2000-Server?	Ja
Ist der DNS konfiguriert und verwenden Sie die richtigen Hostnamen für die System i-Plattform und den Kerberos-Server?	Ja
Unter welchem Betriebssystem möchten Sie den Kerberos-Server konfigurieren? 1. Windows 2000 Server 2. Windows Server 2003 3. AIX Server 4. i5/OS PASE (ab V5R3) 5. z/OS	i5/OS PASE
Wurden die neuesten PTFs (vorläufigen Programmkorrekturen) angelegt?	Ja
Beträgt die Abweichung zwischen der Systemzeit des System i-Systems und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung größer, lesen Sie die Informationen unter „Systemzeiten synchronisieren" auf Seite 110.	Ja

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

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? • Der Kerberos-Realm, der den Windows 2000-Server als Kerberos-Server verwendet • Der Kerberos-Realm, der System B als Kerberos-Server (konfiguriert in i5/OS PASE) verwendet	ORDEPT.MYCO.COM SHIPDEPT.MYCO.COM
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? Welches Kennwort möchten Sie für den i5/OS PASE-Administrator angeben? **Anmerkung:** Dieses Kennwort muss mit dem Kennwort übereinstimmen, das Sie bei der Einrichtung des Kerberos-Servers in i5/OS PASE verwendet haben.	Benutzername: admin/admin Kennwort: secret

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

Planungsarbeitsblatt für Cross-Realm-Vertrauensbeziehung	**Antworten**
Wie lauten die Principal-Namen, die zur Konfiguration der Cross-Realm-Vertrauensbeziehung verwendet werden? Wie lautet das Kennwort für jeden dieser Principals?	Principal: krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM Kennwort: shipord1 Principal: krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO .COM Kennwort: shipord2
Wie lauten die vollständig qualifizierten Hostnamen für die einzelnen Kerberos-Server dieser Realms? • ORDEPT.MYCO.COM • SHIPDEPT.MYCO.COM	kdc1.ordept.myco.com systemb.shipdept.myco.com
Weichen die Systemzeiten aller Systeme nicht mehr als fünf Minuten voneinander ab? Ist die Abweichung größer, lesen Sie die Informationen unter „Systemzeiten synchronisieren" auf Seite 110.	Ja

Ordnungsgemäßen Start des Kerberos-Servers in i5/OS PASE auf System B überprüfen

Vor der Konfiguration einer Cross-Realm-Vertrauensbeziehung müssen Sie überprüfen, ob 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 System B `call QP2TERM` ein. Mit diesem Befehl wird eine interaktive Shell-Umgebung geöffnet, in der Sie mit i5/OS PASE-Anwendungen arbeiten können.
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.

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

Principal für Cross-Realm-Vertrauensbeziehung auf dem i5/OS PASE-Kerberos-Server erstellen

Führen Sie die folgenden Schritte durch, um einen Principal für eine Cross-Realm-Vertrauensbeziehung auf dem i5/OS PASE-Kerberos-Server zu 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, dieses Kennwort erneut einzugeben. Außerdem erhalten Sie die folgende Nachricht:

   ```
   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, dieses Kennwort erneut einzugeben. Außerdem erhalten Sie die folgende Nachricht:

   ```
   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.

Verschlüsselungswerte auf dem i5/OS PASE-Kerberos-Server ändern

Für den Einsatz auf Windows-Workstations müssen die Standardverschlüsselungseinstellungen des Kerberos-Servers geändert werden, damit Clients auf dem i5/OS PASE-Kerberos-Server authentifiziert werden können.

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
   arcfour-hmac:normal aes256-cts:normal
   des-cbc-md5:normal des-cbc-crc:normal
   ```

   in

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

Windows 2000-Server zur Anerkennung von SHIPDEPT.MYCO.COM konfigurieren

Sie haben System B so konfiguriert, dass es den Realm ORDEPT.MYCO.COM als vertrauenswürdig akzeptiert. Jetzt müssen Sie den Windows 2000-Server so konfigurieren, dass er den Realm SHIPDEPT-.MYCO.COM als vertrauenswürdig akzeptiert.

Führen Sie die folgenden Schritte durch, um den Windows 2000-Server zu konfigurieren:

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 innerhalb der Windows-Schnittstelle auch als Windows-Domäne 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**.

Realm SHIPDEPT.MYCO.COM zu System A hinzufügen

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

Führen Sie die folgenden Schritte durch, um den Realm SHIPDEPT.MYCO.COM zu definieren:

1. Erweitern Sie im System i Navigator den Eintrag für **System 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**.
   a. **Hinzuzufügender Realm**: `SHIPDEPT.MYCO.COM`
   b. **KDC**: `systemb.shipdept.myco.com`
   c. **Port**: 88
4. Klicken Sie auf **Realms**, um die Liste der Realms im rechten Fensterbereich 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

Im Folgenden erfahren Sie, welche Voraussetzungen zur Weitergabe der Konfiguration des Netzwerkauthentifizierungsservice an mehrere Systeme erfüllt werden müssen und zu welchem Zweck diese Weitergabe dient.

Situation

Sie sind der Systemadministrator für ein Großunternehmen, das Kfz-Teile herstellt. Sie verwalten gegenwärtig fünf System i-Plattformen mit dem System i 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 Nutzung 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 diese System i-Plattform abgerufen. Sie möchten die Konfiguration des Netzwerkauthentifizierungsservice zwischen diesen von Ihnen verwalteten Systemen vereinfachen.

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

Da eines der Systeme OS/400 Version 5 Release 2 (V5R2) verwendet und dieses Release den Assistenten für die Funktionssynchronisation nicht unterstützt, müssen Sie das V5R2-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.

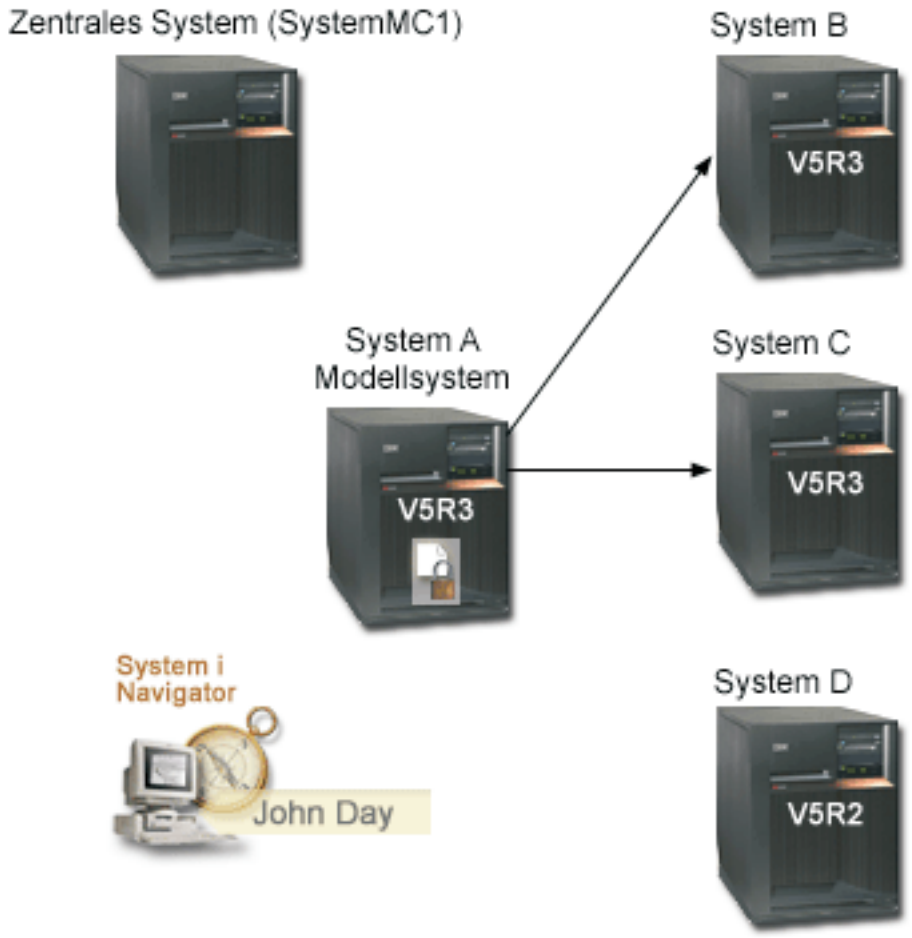
Ziele

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

1. Die Konfiguration des Netzwerkauthentifizierungsservice im Netzwerk soll vereinfacht werden.
2. Alle System i-Plattformen sollen auf denselben Kerberos-Server verweisen.
3. Das V5R2-System soll ebenfalls für die Nutzung des Kerberos-Realms konfiguriert werden.

Details

Die folgende Abbildung veranschaulicht die Details für dieses Szenario.



SystemMC1 : Zentrales System

- Arbeitet mit i5/OS ab V5R3 mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12)
  - System i Access für Windows (5722-XE1 oder 5761-XE1)
  - Network Authentication Enablement (5722-NAE oder 5761-NAE), wenn Sie mit i5/OS ab V5R4 arbeiten
  - Cryptographic Access Provider (5722-AC3), wenn Sie mit i5/OS V5R3 arbeiten
- Speichert und plant für jedes der Endpunktsysteme Tasks hinsichtlich der Synchronisationseinstellungen und führt diese aus.

System A: Modellsystem

- Arbeitet mit i5/OS ab V5R3 mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12)
  - System i Access für Windows (5722-XE1 oder 5761-XE1)
  - Network Authentication Enablement (5722-NAE oder 5761-NAE), wenn Sie mit i5/OS ab V5R4 arbeiten
  - Cryptographic Access Provider (5722-AC3), wenn Sie mit i5/OS V5R3 arbeiten

- Ist das Modellsystem für die Weitergabe der Konfiguration des Netzwerkauthentifizierungsservice an Endpunktsysteme.

System B: Endpunktsystem
- Arbeitet mit i5/OS ab V5R3 mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12)
  - System i Access für Windows (5722-XE1 oder 5761-XE1)
  - Network Authentication Enablement (5722-NAE oder 5761-NAE), wenn Sie mit i5/OS ab V5R4 arbeiten
  - Cryptographic Access Provider (5722-AC3), wenn Sie mit i5/OS V5R3 arbeiten
- Ist eines der Endpunktsysteme für die Weitergabe der Konfiguration des Netzwerkauthentifizierungsservice.

System C: Endpunktsystem
- Arbeitet mit i5/OS V5R3 mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS-Host-Server (5722-SS1 Option 12)
  - System i Access für Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3)
- Ist eines der Endpunktsysteme für die Weitergabe der Konfiguration des Netzwerkauthentifizierungsservice.

System D: Endpunktsystem
- Arbeitet mit OS/400 V5R2 mit den folgenden installierten Optionen und Lizenzprogrammen:
  - 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
- Arbeitet mit System i Access für Windows (5722-XE1 oder 5761-XE1).
- Arbeitet mit System i Navigator mit den folgenden Unterkomponenten:

  Anmerkung: Diese Unterkomponenten werden nur für einen PC benötigt, der zur Verwaltung des Netzwerkauthentifizierungsservice verwendet wird.
  - Netzwerk
  - Sicherheit

Windows 2000-Server (nicht in der Grafik dargestellt)
- Fungiert als Kerberos-Server für das Netzwerk (kdc1.myco.com).
- Alle Benutzer wurden zu Microsoft Active Directory hinzugefügt.

Anmerkung: Der Name des im vorliegenden Szenario verwendeten KDC-Servers (**kdc1.myco.com**) ist frei erfunden.

Voraussetzungen und Annahmen

SystemMC1 : 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 diese Lizenzprogramme installiert wurden:

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

   b. Vergewissern Sie sich, dass alle erforderlichen Lizenzprogramme installiert sind.
2. Die gesamte erforderliche Hardwareplanung und -konfiguration wurde durchgeführt.
3. TCP/IP und die Basissystemsicherheit wurden auf System A konfiguriert und getestet.
4. Die Standardeinstellungen im System i Navigator wurden nicht dahingehend geändert, dass das Öffnen des Fensters 'Task-Status' beim Starten einer Task inaktiviert ist. Gehen Sie wie folgt vor, um sicherzustellen, dass die Standardeinstellungen nicht geändert wurden:

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

   b. Vergewissern Sie sich auf der Seite 'Allgemein', dass **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 Systemen zu schützen.

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

System A: Voraussetzungen des Modellsystems

1. Bei diesem Szenario wird vorausgesetzt, dass der Netzwerkauthentifizierungsservice auf dem Modellsystem (System 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 diese Lizenzprogramme installiert wurden:

   a. Erweitern Sie im System i Navigator den Eintrag für ***Ihr System*** → **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 die Basissystemsicherheit wurden auf Ihrem System konfiguriert und getestet.
5. SSL (Secure Sockets Layer) wurde konfiguriert, um die Datenübertragung zwischen diesen Systemen zu schützen.

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

System B, System C und System D: Voraussetzungen des Endpunktsystems

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

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

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. Die 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 Schritte durchführen, um mit dem Assistenten für die Funktionssynchronisation die Konfiguration des Netzwerkauthentifizierungsservice an Endpunktsysteme weiterzugeben.

Planungsarbeitsblätter ausfüllen

Bevor Sie den System i Navigator verwenden können, um die Konfiguration ausgehend von einem Modellsystem an verschiedene Zielsysteme weiterzugeben, müssen Sie die folgenden Planungsarbeitsblätter ausfüllen.

Alle Fragen müssen mit Ja beantwortet werden, bevor Sie mit der Weitergabe des Netzwerkauthentifizierungsservice fortfahren.

Tabelle 8. Netzwerkauthentifizierungsservice weitergeben - Arbeitsblatt für Voraussetzungen

Arbeitsblatt für Voraussetzungen	Antworten
Arbeiten Sie auf den folgenden Systemen mit i5/OS V5R3 oder einer späteren Version des Produkts (5722-SS1) oder benutzen Sie V6R1 (5761-SS1)? • Zentrales System • System A • System B • System C	Ja
Wurden die neuesten PTFs (vorläufigen Programmkorrekturen) angelegt?	Ja
Werden auf System D OS/400 V5R2 und i5/OS ab V5R3 ausgeführt?	Ja

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

Arbeitsblatt für Voraussetzungen	**Antworten**
Haben Sie für System D die aktuellsten vorläufigen Programmkorrekturen (PTFs) einschließlich der folgenden PTFs angelegt? • SI08977 • SI08979	
Sind die folgenden Optionen und Lizenzprogramme auf allen System i-Modellen installiert? • i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12) • System i Access für Windows (5722-XE1 oder 5761-XE1) • Network Authentication Enablement (5722-NAE oder 5761-NAE), wenn Sie mit i5/OS ab V5R4 arbeiten • Cryptographic Access Provider (5722-AC3), wenn Sie mit i5/OS V5R3 arbeiten	Ja
Ist System i Access für Windows (5722-XE1 oder 5761-XE1) auf dem PC des Administrators installiert?	Ja
Ist System i Navigator auf dem PC des Administrators installiert? • Ist die Unterkomponente "Netzwerk" des System i Navigator auf dem PC des Administrators installiert? • Ist die Unterkomponente "Sicherheit" des System i Navigator auf dem PC des Administrators installiert?	Ja
Ist das aktuellste Service-Pack für IBM System i Access für Windows installiert? Sie können das aktuellste Service-Pack über die Website für System i Access abrufen.	Ja
Verfügen Sie über die Sonderberechtigungen *SECADM, *ALLOBJ und *IOSYSCFG?	Ja
Fungiert eines der folgenden Systeme als Kerberos-Server? Wenn ja, geben Sie an, um welches System es sich handelt. 1. Microsoft Windows 2000 Server **Anmerkung:** Microsoft Windows 2000 Server verwendet die Kerberos-Authentifizierung als Standardsicherheitsmechanismus. 2. Windows Server 2003 3. i5/OS PASE (ab V5R3) 4. AIX-Server 5. z/OS	Ja, Windows 2000 Server
Für Windows 2000 Server und Windows Server 2003: Sind Windows-Unterstützungstools (enthalten das Tool ktpass) installiert?	Ja
Beträgt die Abweichung zwischen der Systemzeit des System i-Systems 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?	System B, System C, System D
Welche Funktionen sollen an diese Systemverwaltungsgruppe weitergegeben werden?	Netzwerkauthentifizierungsservice

Tabelle 9. Planungsarbeitsblatt für Funktionssynchronisation (Forts.)

Fragen	Antworten
Für welche Services möchten Sie Chiffrierschlüsseleinträge erstellen? • i5/OS-Kerberos-Authentifizierung • LDAP • IBM HTTP-Server • i5/OS NetServer • NFS-Server	i5/OS-Kerberos-Authentifizierung
Wie lauten die Service-Principal-Namen für die Systeme, an die Sie die Konfiguration weitergeben möchten?	krbsvr400/systema.myco.com@MYCO.COM krbsvr400/systemb.myco.com@MYCO.COM krbsvr400/systemc.myco.com@MYCO.COM krbsvr400/systemd.myco.com@MYCO.COM
Wie lauten die Kennwörter, die jedem dieser Principals zugeordnet sind?	Das Kennwort für die Principals für die Systeme A, B und C lautet `systema123`. Das Kennwort für den Principal für System D lautet `systemd123`.
Wie lautet der vollständig qualifizierte Hostname der verschiedenen System i-Plattformen?	systema.myco.com systemb.myco.com systemc.myco.com systemd.myco.com
Wie lautet der Name der Windows 2000-Domäne? **Anmerkung:** Eine Windows 2000-Domäne ist mit einem Kerberos-Realm vergleichbar. Microsoft Active Directory verwendet die Kerberos-Authentifizierung als Sicherheitsmechanismus.	MYCO.COM

Tabelle 10. Planungsarbeitsblatt für den Netzwerkauthentifizierungsservice für System D

Fragen	Antworten
Wie lautet der Name des Kerberos-Standard-Realms, zu dem Ihre System i-Plattform gehört? **Anmerkung:** Eine Windows 2000-Domäne ist mit einem Kerberos-Realm vergleichbar. Microsoft Active Directory verwendet standardmäßig als Sicherheitsmechanismus die Kerberos-Authentifizierung.	MYCO.COM
Verwenden Sie Microsoft Active Directory?	Ja
Welcher Kerberos-Server wird für diesen Kerberos-Standard-Realm verwendet? An welchem Port ist der Kerberos-Server empfangsbereit?	**KDC:** kdc1.myco.com **Port:** 88 **Anmerkung:** Dies ist der Standardport für den Kerberos-Server.
Möchten Sie einen Kennwortserver für diesen Standard-Realm konfigurieren? Wenn ja, beantworten Sie die folgenden Fragen: Wie lautet der Name des Kennwortservers für diesen Kerberos-Server? An welchem Port ist der Kennwortserver empfangsbereit?	Ja **Kennwortserver:** kdc1.myco.com **Port:** 464 **Anmerkung:** Dies ist der Standardport für den Kennwortserver.
Für welche Services möchten Sie Chiffrierschlüsseleinträge erstellen? • i5/OS-Kerberos-Authentifizierung • LDAP • IBM HTTP-Server • i5/OS NetServer	i5/OS-Kerberos-Authentifizierung
Wie lautet das Kennwort für Ihre i5/OS-Service-Principals?	systemd123

Systemverwaltungsgruppe erstellen

Bevor Sie die Konfiguration des Netzwerkauthentifizierungsservice an ein Zielsystem weitergeben 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. Führen Sie die folgenden Schritte durch, um eine Systemverwaltungsgruppe zu erstellen:

1. Erweitern Sie im System i Navigator den Eintrag für **Management Central (SystemMC1)**.
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 System B**, **System C** und **System 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 für **Systemverwaltungsgruppen**, um zu überprüfen, ob Ihre Systemverwaltungsgruppe hinzugefügt wurde.

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

Zur Weitergabe von Systemeinstellungen an mehrere Endpunktsysteme können Sie den Assistenten für die Funktionssynchronisation im System i Navigator verwenden. Mit diesem Assistenten können Sie Systemeinstellungen wie beispielsweise die Konfiguration des Netzwerkauthentifizierungsservice weitergeben.

Führen Sie die folgenden Schritte durch, um die Konfiguration des Netzwerkauthentifizierungsservice an die Zielsysteme weiterzugeben:

1. Erweitern Sie im System i Navigator den Eintrag für **Management Central (SystemMC1)** → **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 die Funktionssynchronisation** gestartet.
3. Überprüfen Sie auf der Begrüßungsseite die Informationen zum Assistenten für die Funktionssynchronisation, und klicken Sie dann auf **Weiter**. Auf der Begrüßungsseite sind die Funktionen aufgelistet, die Sie später im Assistenten synchronisieren können.

   Anmerkung: Wenn Sie die Konfiguration des Netzwerkauthentifizierungsservice an andere Systeme weitergeben, werden sensible Daten wie Kennwörter über das Netzwerk gesendet. Sie sollten SSL verwenden, um diese Informationen zu schützen, insbesondere, wenn diese beim Senden das lokale Netzwerk (Local Area Network, LAN) verlassen. Ausführliche Informationen finden Sie unter Scenario: Securing all connections to your Management Central server with SSL.
4. Wählen Sie auf der Seite 'Modellsystem' System A als Modellsystem aus, und klicken Sie dann auf **Weiter**. Dieses Modellsystem wird als Basis für die Synchronisation der Konfiguration des Netzwerkauthentifizierungsservice mit anderen Systemen verwendet.
5. Wählen Sie auf der Seite 'Zielsysteme und -gruppen' **Systemverwaltungsgruppe MyCo** aus. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite 'Zu aktualisierende Komponenten' **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' **i5/OS-Kerberos-Authentifizierung** aus, und geben Sie in den Feldern **Kennwort** und **Kennwort bestätigen** die Zeichenfolge `systema123` 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', ob 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. Nehmen Sie an, dass die Task auf allen Endpunktsystemen mit Ausnahme von System D erfolgreich ausgeführt werden konnte. Da System D mit OS/400 V5R2 arbeitet, unterstützt es den Assistenten für die Funktionssynchronisation nicht.

    Zum Beheben dieses Fehlers müssen Sie den Netzwerkauthentifizierungsservice auf System D manuell so konfigurieren, dass seine Einstellungen mit der Konfiguration auf dem Modellsystem (System A) übereinstimmen.

Netzwerkauthentifizierungsservice auf System D konfigurieren

Sie müssen den Netzwerkauthentifizierungsservice auf System D so konfigurieren, dass seine Einstellungen mit den Konfigurationseinstellungen auf System A übereinstimmen.

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

1. Erweitern Sie im System i Navigator den Eintrag für **System 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 Auswahl **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 Einstellung **Ja** aus, um System D so zu konfigurieren, dass es auf den für den Standard-Realm konfigurierten Kennwortserver verweist. Der Kennwortserver wurde bereits konfiguriert. Er ermöglicht Principals die Änderung von Kennwörtern auf dem Kerberos-Server. Geben Sie im Feld **Kennwortserver** den Wert `kdc1.myco.com` ein. Der Standardport für den Kennwortserver ist 464. Klicken Sie auf **Weiter**.
7. Wählen Sie auf der Seite 'Chiffrierschlüsseleinträge auswählen' **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: `systemd123`. Klicken Sie auf **Weiter**.
9. Optional: Wählen Sie auf der Seite 'Stapeldatei erstellen' die Einstellung **Nein** aus.
10. Auf der Seite 'Zusammenfassung' können Sie die Details zur Konfiguration des Netzwerkauthentifizierungsservice überprüfen. Klicken Sie auf **Fertig stellen**.

Principals für Endpunktsysteme zur Windows 2000-Domäne hinzufügen

Im Folgenden sind die Arbeitsschritte aufgeführt, die zum Hinzufügen von Principals für Endpunktsysteme ausgeführt werden müssen.

1. **Schritte für System B**
   a. Erweitern Sie auf dem Windows 2000-Server den Eintrag für **Verwaltungstools** → **Active Directory-Benutzer und -Computer**.
   b. 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.

   c. Geben Sie im Feld **Name** die Zeichenfolge `systemb` ein, um die System i-Plattform für diese Windows-Domäne zu identifizieren. Damit wird ein neues Benutzerkonto für System B hinzugefügt.
   d. Rufen Sie die Eigenschaften für den Active Directory-Benutzer systemb auf. Wählen Sie auf der Indexzunge **Konto** die Auswahl **Konto wird für Delegierungszwecke vertraut** aus. Damit wird dem i5/OS-Service-Principal der Zugriff auf andere Services im Namen eines angemeldeten Benutzers gestattet.
   e. 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 2000 Server. Geben Sie an einer Windows-Eingabeaufforderung den folgenden Befehl ein:

      ```
      ktpass -mapuser systemb -pass systema123 -princ krbsvr400/systemb.myco.com@MYCO.COM
      -mapop set
      ```

2. **Schritte für System C**
   a. Erweitern Sie auf dem Windows 2000-Server den Eintrag für **Verwaltungstools** → **Active Directory-Benutzer und -Computer**.
   b. 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.

   c. Geben Sie im Feld **Name** die Zeichenfolge `systemc` ein, um die System i-Plattform für diese Windows-Domäne zu identifizieren. Damit wird ein neues Benutzerkonto für System C hinzugefügt.
   d. Rufen Sie die Eigenschaften für den Active Directory-Benutzer systemc auf. Wählen Sie auf der Indexzunge **Konto** die Auswahl **Konto wird für Delegierungszwecke vertraut** aus. Damit wird dem i5/OS-Service-Principal der Zugriff auf andere Services im Namen eines angemeldeten Benutzers gestattet.
   e. 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 2000 Server. Geben Sie an einer Windows-Eingabeaufforderung den folgenden Befehl ein:

      ```
      ktpass -mapuser systemc -pass systema123 -princ krbsvr400/systemc.myco.com@MYCO.COM
      -mapop set
      ```

3. **Schritte für System D**
   a. Erweitern Sie auf dem Windows 2000-Server den Eintrag für **Verwaltungstools** → **Active Directory-Benutzer und -Computer**.
   b. Wählen Sie als Domäne **MYCO.COM** aus, und erweitern Sie den Eintrag für **Aktion** → **Neu** → **Benutzer**.

      Anmerkung: Diese Windows-Domäne muss mit dem Namen des Standard-Realms übereinstimmen, den Sie bei der Konfiguration des Netzwerkauthentifizierungsservice angegeben haben.
   c. Geben Sie im Feld **Name** die Zeichenfolge `systemd` ein, um die System i-Plattform für diese Windows-Domäne zu identifizieren. Damit wird ein neues Benutzerkonto für System D hinzugefügt.
   d. Rufen Sie die Eigenschaften für den Active Directory-Benutzer systemd auf. Wählen Sie auf der Indexzunge **Konto** die Auswahl **Konto wird für Delegierungszwecke vertraut** aus. Damit wird dem i5/OS-Service-Principal der Zugriff auf andere Services im Namen eines angemeldeten Benutzers gestattet.
   e. 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 2000 Server. Geben Sie an einer Windows-Eingabeaufforderung den folgenden Befehl ein:

      ```
      ktpass -mapuser systemd -pass systemd123 -princ krbsvr400/systemd.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. Einzelheiten hierzu finden Sie unter „Szenario: Kerberos-Authentifizierung zwischen Management Central-Servern verwenden".

Szenario: Kerberos-Authentifizierung zwischen Management Central-Servern verwenden

Im Folgenden erfahren Sie, welche Voraussetzungen zur Verwendung der Kerberos-Authentifizierung zwischen Management Central-Servern erfüllt werden müssen und zu welchem Zweck diese dient.

Situation

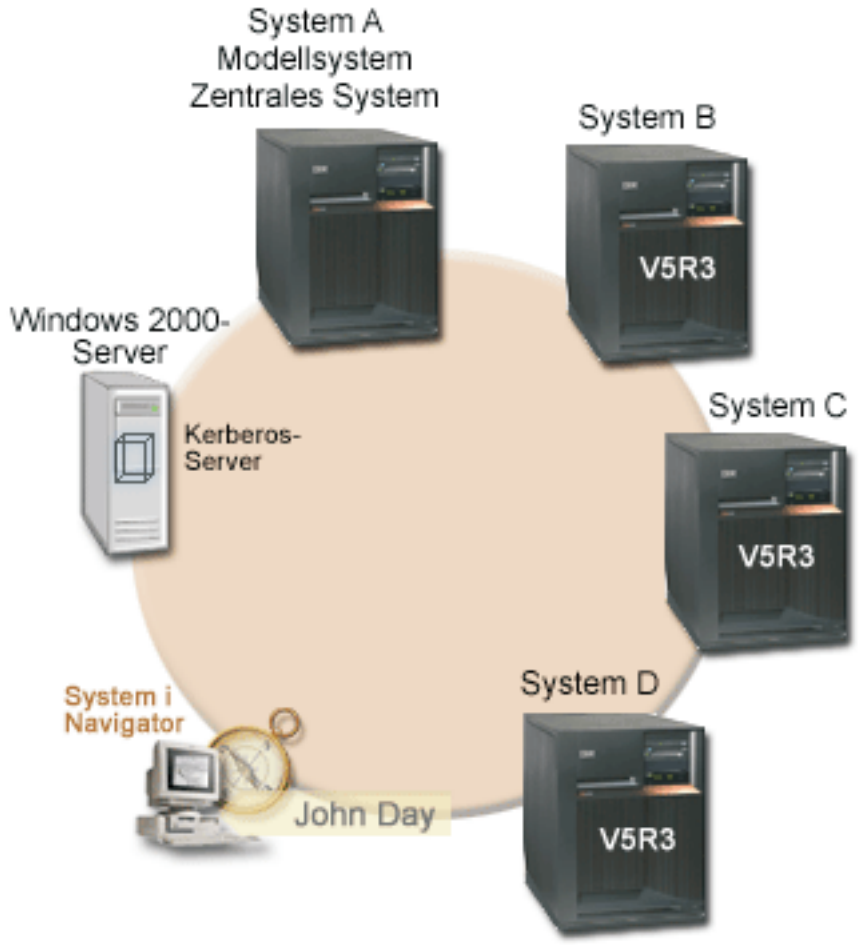
Sie sind als Netzwerkadministrator für ein mittelständisches Unternehmen der Teileproduktion tätig. Sie verwalten gegenwärtig vier System i-Produkte mit dem System i Navigator auf einem Client-PC. Sie möchten, dass die Management Central-Serverjobs die Kerberos-Authentifizierung an Stelle anderer Authentifizierungsmethoden, 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.



System A: Modellsystem und zentrales System

- Arbeitet mit i5/OS ab V5R3 mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12)
  - System i Access für Windows (5722-XE1 oder 5761-XE1)
  - Network Authentication Enablement (5722-NAE oder 5761-NAE), wenn Sie mit i5/OS ab V5R4 arbeiten
  - Cryptographic Access Provider (5722-AC3), wenn Sie mit i5/OS V5R3 arbeiten
- Der i5/OS-Service-Principal krbsvr400/systema.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.

System B: Endpunktsystem

- Arbeitet mit i5/OS ab V5R3 mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12)
  - System i Access für Windows (5722-XE1 oder 5761-XE1)

- Network Authentication Enablement (5722-NAE oder 5761-NAE), wenn Sie mit i5/OS ab V5R4 arbeiten
- Cryptographic Access Provider (5722-AC3), wenn Sie mit i5/OS V5R3 arbeiten

• Der i5/OS-Service-Principal krbsvr400/systemb.myco.com@MYCO.COM und das zugeordnete Kennwort wurden zur Chiffrierschlüsseldatei hinzugefügt.

System C: Endpunktsystem

• Arbeitet mit i5/OS V5R4 mit den folgenden installierten Optionen und Lizenzprogrammen:
- i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12)
- System i Access für Windows (5722-XE1 oder 5761-XE1)
- Network Authentication Enablement (5722-NAE oder 5761-NAE)

• Der i5/OS-Service-Principal krbsvr400/systemc.myco.com@MYCO.COM und das zugeordnete Kennwort wurden zur Chiffrierschlüsseldatei hinzugefügt.

System D: Endpunktsystem

• Arbeitet mit i5/OS ab V5R3 mit den folgenden installierten Optionen und Lizenzprogrammen:
- i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12)
- System i Access für Windows (5722-XE1 oder 5761-XE1)
- Cryptographic Access Provider (5722-AC3)

• Der i5/OS-Service-Principal krbsvr400/systemd.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/systema.myco.com@MYCO.COM
- krbsvr400/systemb.myco.com@MYCO.COM
- krbsvr400/systemc.myco.com@MYCO.COM
- krbsvr400/systemd.myco.com@MYCO.COM

Client-PC

• Arbeitet mit System i Access für Windows (5722-XE1 oder 5761-XE1).

• Arbeitet mit System i Navigator mit den folgenden Unterkomponenten:

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

4. Die Standardeinstellungen im System i Navigator wurden nicht dahingehend geändert, dass das Öffnen des Fensters 'Task-Status' beim Starten einer Task verhindert wird. Gehen Sie wie folgt vor, um sicherzustellen, dass die Standardeinstellungen nicht geändert wurden:
   a. Klicken Sie im System i Navigator mit der rechten Maustaste auf ***Ihr zentrales System***, und wählen Sie dann **Benutzervorgaben** aus.
   b. Vergewissern Sie sich auf der Seite 'Allgemein', dass **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 die Funktionssynchronisation im System i 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 38 enthält detaillierte Information zur Verwendung des Assistenten für die Funktionssynchronisation.

Konfigurationsschritte

Um die Kerberos-Authentifizierung zwischen Management Central-Servern zu konfigurieren, müssen Sie die folgenden Schritte durchführen.

Planungsarbeitsblätter ausfüllen

In den folgenden Planungsarbeitsblättern ist die Art der Informationen aufgeführt, 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 auf allen System i-Plattformen i5/OS V5R3 oder eine spätere Version dieses Produkts (5722-SS1), oder arbeiten Sie mit V6R1 (5761-SS1)?	Ja
Wurden die neuesten PTFs (vorläufigen Programmkorrekturen) angelegt?	Ja
Sind die folgenden Optionen und Lizenzprogramme auf allen System i-Modellen installiert? • i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12) • System i Access für Windows (5722-XE1 oder 5761-XE1) • Network Authentication Enablement (5722-NAE oder 5761-NAE), wenn Sie mit i5/OS ab V5R4 arbeiten • Cryptographic Access Provider (5722-AC3), wenn Sie mit i5/OS V5R3 arbeiten	Ja
Ist System i Access für Windows (5722-XE1 oder 5761-XE1) auf dem PC des Administrators installiert?	Ja
Ist System i Navigator auf dem PC des Administrators installiert? • Ist die Unterkomponente "Netzwerk" des System i Navigator auf dem PC des Administrators installiert? • Ist die Unterkomponente "Sicherheit" des System i Navigator auf dem PC des Administrators installiert?	Ja
Ist das aktuellste Service-Pack für IBM System i Access für Windows installiert? Sie können das aktuellste Service-Pack über die Website für System i Access abrufen.	Ja
Verfügen Sie über die Sonderberechtigungen *SECADM, *ALLOBJ und *IOSYSCFG?	Ja

Tabelle 11. Kerberos-Authentifizierung zwischen Management Central-Servern verwenden - Arbeitsblatt für Voraussetzungen (Forts.)

Arbeitsblatt für Voraussetzungen	Antworten
Fungiert eines der folgenden Systeme als Kerberos-Server? Wenn ja, geben Sie an, um welches System es sich handelt. 1. Microsoft Windows 2000 Server **Anmerkung:** Microsoft Windows 2000 Server verwendet die Kerberos-Authentifizierung als Standardsicherheitsmechanismus. 2. Windows Server 2003 3. i5/OS PASE (ab V5R3) 4. AIX-Server 5. z/OS	Ja, Windows 2000 Server
Für Windows 2000 Server und Windows Server 2003: Sind Windows-Unterstützungstools (enthalten das Tool ktpass) installiert?	Ja
Beträgt die Abweichung zwischen der Systemzeit des System i-Systems und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung größer, lesen Sie die Informationen unter „Systemzeiten synchronisieren" auf Seite 110.	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?	System A, System B, System C, System D
Wie lauten die Service-Principal-Namen der System i-Plattformen?	krbsvr400/systema.myco.com@MYCO.COM krbsvr400/systemb.myco.com@MYCO.COM krbsvr400/systemc.myco.com@MYCO.COM krbsvr400/systemd.myco.com@MYCO.COM

Zentrales System zur Verwendung der Kerberos-Authentifizierung konfigurieren

System A ist das Modellsystem und das zentrale System für die anderen Zielsysteme.

Führen Sie die folgenden Schritte durch, um die Kerberos-Authentifizierung auf dem zentralen System zu konfigurieren:

1. Erweitern Sie im System i Navigator den Eintrag für **Management Central (System A)**, und wählen Sie dann **Eigenschaften** aus.
2. Wählen Sie auf der Indexzunge **Sicherheit** die Auswahl **Kerberos-Authentifizierung verwenden** aus, und setzen Sie die Authentifizierungsstufe auf **Zur anerkannten Gruppe hinzufügen**.
3. Wählen Sie im Feld **Identitätsabgleich** die Auswahl **Nicht verwenden** aus, und klicken Sie auf **OK**. Diese Einstellung ermöglicht es 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 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.

Systemverwaltungsgruppe MyCo2 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.

Bevor Sie die richtigen Einstellungen auf die anderen Systeme in Ihrem Netzwerk anwenden können, müssen Sie eine Systemverwaltungsgruppe für alle Endpunktsysteme erstellen.

1. Erweitern Sie im System i Navigator den Eintrag für **Management Central (System 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** System A, System B, System C und System D aus, und klicken Sie dann auf **Hinzufügen**. Auf diese Weise werden diese Systeme der Liste **Ausgewählte Systeme** hinzugefügt. Klicken Sie auf **OK**.
5. Erweitern Sie den Eintrag für **Systemverwaltungsgruppen**, um zu überprüfen, ob Ihre Systemverwaltungsgruppe hinzugefügt wurde.

Systemwerte-Inventar erfassen

Sie müssen die Funktion ″Inventar erfassen″ im System i 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 System i Navigator den Eintrag für **Management Central (System A)** → **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' **Systemwerte** aus. Klicken Sie auf **OK**. 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**.
4. Lesen Sie auf der Seite 'Inventarstatus erfassen' alle angezeigten Statuswerte, und beheben Sie alle möglicherweise auftretenden Fehler. Details zu bestimmten 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 Auswahl **Inventar** aus. Auf dieser Seite werden alle möglichen Statuswerte mit detaillierten Beschreibungen sowie Informationen zur Fehlerbehebung angezeigt.
5. Schließen Sie das Statusfenster, wenn die Inventarerfassung durchgeführt werden konnte.

Kerberos-Einstellungen im System i 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 System i Navigator den Eintrag für **Management Central (System A)** → **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:
   a. Wählen Sie **System A** für das Feld **Modellsystem** aus.
   b. Wählen Sie **Management Central** für das Feld **Kategorie** aus.
   c. Wählen Sie aus der Liste **Zu vergleichende Einträge** die Einträge **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.

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 System i Navigator den Eintrag für **Meine Verbindungen** → **System A** → **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 Fensterbereich 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: System B, System C und System D.

Kerberos-Service-Principal für jeden Endpunkt zur Datei für anerkannte Gruppen hinzufügen

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.

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. 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.

Anmerkung: 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 ausführen, 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 System i Navigator den Eintrag für **Management Central (System A)** → **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 schließen Sie das Dialogfenster.

Hinzufügung der Kerberos-Principals zur Datei für anerkannte Gruppen überprüfen

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 System i Navigator den Eintrag für **System 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.
   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 Auswahl **Alle Dateien** für **Bearbeitungsoptionen aktivieren für:** aus, und klicken Sie dann auf **OK**.
3. Vergewissern Sie sich, dass der Kerberos-Service-Principal des zentralen Systems als Mitglied der anerkannten Gruppe von Management Central aufgelistet ist.
4. Wiederholen Sie diese Schritte für System C und D, um zu überprüfen, ob der Kerberos-Service-Principal des zentralen Systems zu jedem der Zielsysteme hinzugefügt wurde.

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.

Führen Sie die folgenden Schritte durch, um gesicherte Verbindungen zuzulassen. Auf diese Weise wird sichergestellt, dass nur das zentrale System für die Systemverwaltungsgruppe MyCo2 (System A) Tasks für die Zielsysteme ausführen kann.

1. Erweitern Sie im System i Navigator den Eintrag für **Management Central (System A)**, und wählen Sie dann **Eigenschaften** aus.
2. Wählen Sie auf der Indexzunge **Sicherheit** die Auswahl **Kerberos-Authentifizierung verwenden** aus, und geben Sie als Authentifizierungsstufe **Nur gesicherte Verbindungen zulassen** an.
3. Wählen Sie im Feld **Identitätsabgleich** die Auswahl **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**.

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:

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

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/systema.myco.com@MYCO.COM
- krbsvr400/systemb.myco.com@MYCO.COM
- krbsvr400/systemc.myco.com@MYCO.COM
- krbsvr400/systemd.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 System i 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 anzuzeigen, die in der Chiffrierschlüsseldatei registriert sind. Daraufhin sollten die folgenden oder ähnliche Ergebnisse angezeigt werden:

```
Principal: krbsvr400/systema.myco.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/systema.myco.com@MYCO.COM` ein, um ein Ticket-granting Ticket vom Kerberos-Server anzufordern. Mit diesem Befehl wird geprüft, ob Ihr System richtig konfiguriert wurde und das Kennwort in der Chiffrierschlüsseldatei mit dem auf dem Kerberos-Server gespeicherten Kennwort übereinstimmt. Wenn die Prüfung erfolgreich verläuft, dann werden für den Befehl QSH keine Fehler ausgegeben.
5. Geben Sie `klist` ein, um sicherzustellen, dass der Standard-Principal krbsvr400/systema.myco.com@MYCO.COM lautet. Mit diesem Befehl wird der Inhalt eines Kerberos-Caches für Berechtigungsnachweise angezeigt und geprüft, ob ein gültiges Ticket für den i5/OS-Service-Principal erstellt und in den Cache für Berechtigungsnachweise auf dem System aufgenommen wurde.

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

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

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

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

Im Folgenden erfahren Sie, welche Voraussetzungen zum Aktivieren der Einzelanmeldung für das Betriebssystem i5/OS erfüllt werden müssen und zu welchem Zweck diese Aktivierung durchgeführt wird.

Situation

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

Die Mitarbeiter der Auftragsannahmeabteilung verwenden Windows 2000 und i5/OS 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 Auftragsannahmeabteilung. Sie wissen, dass die meisten Mitarbeiter dieselbe Art von Berechtigung benötigen, um auf die Anwendung zur Abfrage des Inventarstatus zugreifen zu können. Es erscheint Ihnen überflüssig und zeitaufwändig, einzelne Benutzerprofile und zahlreiche Kennwörter, die in dieser Situation erforderlich sind, zu verwalten. Darüber hinaus wissen Sie, dass es für alle Mitarbeiter von Vorteil wäre, wenn sie weniger Benutzer-IDs und Kennwörter verwenden müssten. Gehen Sie wie folgt vor:

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

Sie wissen, dass i5/OS die Einzelanmeldung unterstützt. Diese Lösung bietet Ihren Benutzern die Möglichkeit, nach einmaliger Anmeldung auf mehrere Anwendungen und Services zuzugreifen, für die normalerweise bei der Anmeldung mehrere Benutzer-IDs und Kennwörter angegeben werden müssten. Da die Benutzer zur Ausführung ihrer Arbeit weniger Benutzer-IDs und Kennwörter benötigen, müssen Sie auch weniger Kennwortprobleme lösen. Die Einzelanmeldung scheint eine ideale Lösung zu sein, da sie die Kennwortverwaltung auf folgende Weise vereinfacht:

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

authentifizieren zu müssen. Dennoch möchten Sie sicherstellen, dass die Benutzer mit der richtigen Berechtigungsstufe auf die Anwendungen zugreifen können. Zur Erreichung dieses Ziels erstellen Sie eine Richtlinienzuordnung, mit der die Windows 2000-Benutzeridentitäten für diese Benutzergruppe einem einzigen i5/OS-Benutzerprofil zugeordnet werden, das über die 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 der Auftragsannahmeabteilung, 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 untereinander genau und einzeln zugeordnet werden, da der Administrator eine hohe Berechtigungsstufe besitzt.

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

Dieses Szenario hat folgende Vorteile:

- Vereinfacht den Authentifizierungsprozess für Benutzer.
- Vereinfacht die Verwaltung des Zugriffs auf Anwendungen.
- Verringert den Systemaufwand für die Verwaltung des Zugriffs auf die Systeme 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 der Auftragsannahmeabteilung aktivieren möchte.

Die Ziele dieses Szenarios sind:

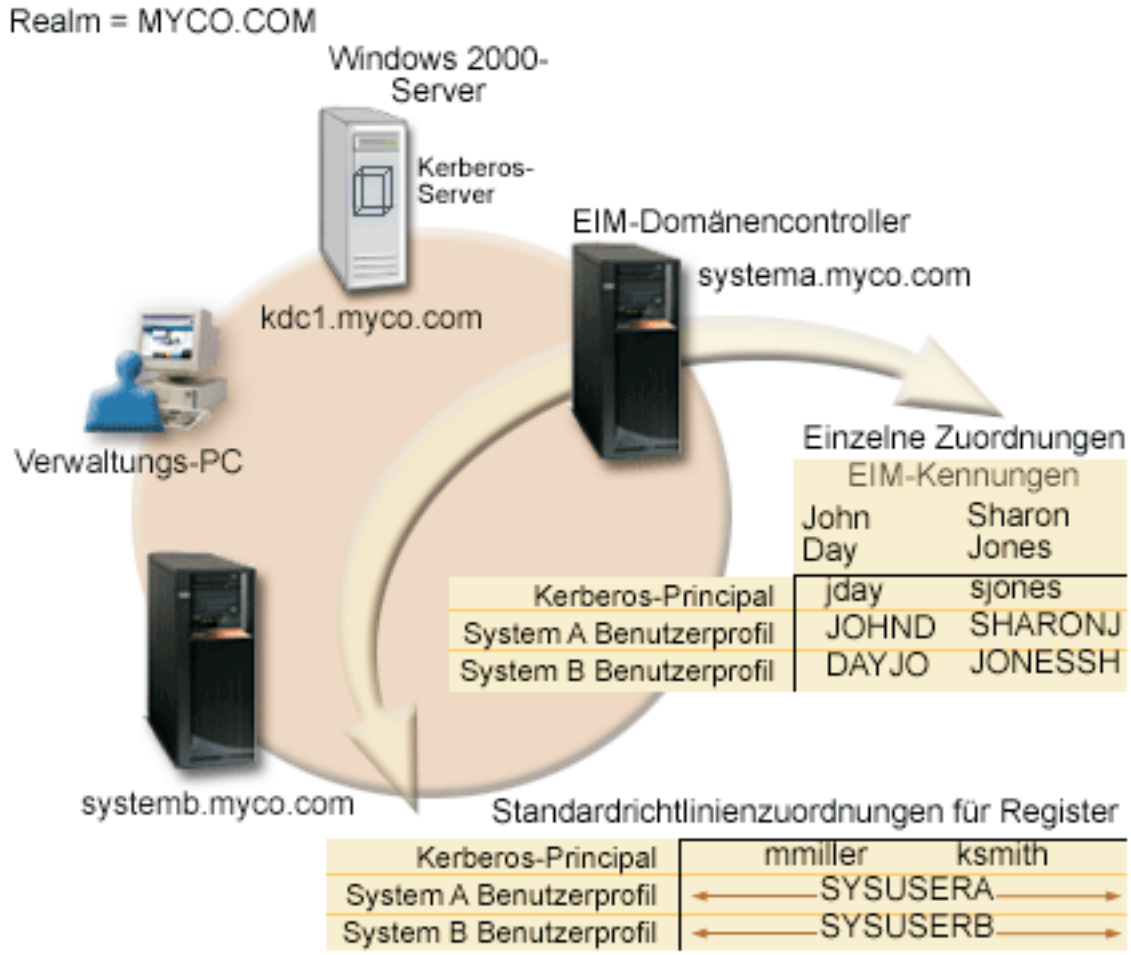
- System A und System B müssen zum Realm MYCO.COM gehören, um die Benutzer und Services, die zur Einzelanmeldungsumgebung gehören, authentifizieren zu können. Wenn Sie die Systeme für die Verwendung von Kerberos aktivieren möchten, müssen System A und System B für den Netzwerkauthentifizierungsservice konfiguriert werden.
- IBM Directory Server for i5/OS (LDAP) auf System A muss als Domänencontroller für die neue EIM-Domäne fungieren.

  Anmerkung: Unter dem Thema "Domänen" wird beschrieben, wie zwei verschiedene Domänenarten, eine EIM-Domäne und eine Windows 2000-Domäne, in die Einzelanmeldungsumgebung integriert werden können.

- Alle Benutzeridentitäten im Kerberos-Register müssen einem einzigen i5/OS-Benutzerprofil zugeordnet werden können. Das Benutzerprofil muss die korrekte 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 ihren i5/OS-Benutzerprofilen mit der Sonderberechtigung *SECADM zuzuordnen. Diese Eins-zu-eins-Abgleiche ermöglichen Ihnen, die Jobs und Objekte, die auf dem System ausgeführt werden, für diese Benutzeridentitäten genau zu überwachen.
- Ein Kerberos-Service-Principal muss verwendet werden, um die Benutzer für IBM System i Access für Windows-Anwendungen einschließlich System i Navigator zu authentifizieren.

Details

Die folgende Abbildung veranschaulicht die Netzwerkumgebung für dieses Szenario.



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

EIM-Domänendaten, die für das Unternehmen definiert sind

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

  - Ein Registerdefinitionsnamen von SYSTEMA.MYCO.COM für das i5/OS-Register auf System A. Sie definieren diesen Namen, wenn Sie den EIM-Konfigurationsassistenten auf System A ausführen.
  - Ein Registerdefinitionsnamen von SYSTEMB.MYCO.COM für das i5/OS-Register auf System B. Sie definieren diesen Namen, wenn Sie den EIM-Konfigurationsassistenten auf System B ausführen.
- Zwei Standardrichtlinienzuordnungen für Register (siehe hierzu EIM-Zuordnungen):

  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 Kennungszuordnung zugeordnet. In diesem Szenario verfügen zwei Netzwerkadministratoren, John Day und Sharon Jones, über Benutzeridentitäten im Register MYCO.COM, das die Quelle der Standardrichtlinienzuordnungen für Register ist. Diese Administratoren besitzen jedoch, wie unten dargestellt, auch Kennungszuordnungen für ihre Benutzeridentitäten im Register MYCO.COM. Die Kennungszuordnungen stellen sicher, dass die Benutzeridentitäten im Register MYCO.COM nicht über die Richtlinienzuordnungen abgeglichen werden. Die Kennungszuordnungen stellen hingegen sicher, dass ihre Benutzeridentitäten im Register MYCO.COM einzeln anderen spezifischen einzelnen Benutzeridentitäten zugeordnet werden.

  - Eine Standardrichtlinienzuordnung für Register ordnet alle Benutzeridentitäten im Windows 2000-Server-Register MYCO.COM einem einzigen i5/OS-Benutzerprofil mit dem Namen SYSUSERA im Register SYSTEMA.MYCO.COM auf System A zu. In diesem Szenario bezeichnen mmiller und ksmith zwei dieser Benutzeridentitäten.
  - Eine Standardrichtlinienzuordnung für Register ordnet alle Benutzeridentitäten im Windows 2000-Server-Register MYCO.COM einem einzigen i5/OS-Benutzerprofil mit dem Namen SYSUSERB im Register SYSTEMB.MYCO.COM auf System 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 System A darstellt.
  - Eine Zielzuordnung für die Benutzeridentität DAYJO, die ein Benutzerprofil im i5/OS-Register auf System B darstellt.
- 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 System A darstellt.
  - Eine Zielzuordnung für die Benutzeridentität JONESSH, die ein Benutzerprofil im i5/OS-Register auf System B darstellt.

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 Active Directory-Benutzer, die keine Kennungszuordnungen besitzen, werden auf allen System i-Plattformen einem einzigen i5/OS-Benutzerprofil zugeordnet.

System A

- Arbeitet mit i5/OS ab V5R3 mit den folgenden installierten Optionen und Lizenzprogrammen:

  - i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12)
  - Qshell Interpreter (5722-SS1 Option 30 oder 5761-SS1 Option 30)
  - System i Access für Windows (5722-XE1 oder 5761-XE1)
  - Network Authentication Enablement (5722-NAE oder 5761-NAE), wenn Sie mit i5/OS V5R4 arbeiten
  - Cryptographic Access Provider (5722-AC3), wenn Sie mit i5/OS V5R3 arbeiten

  Anmerkung: Sie können dieses Szenario auf einem System implementieren, das mit OS/400 V5R2 arbeitet. Allerdings weichen einige der Konfigurationsschritte dann leicht ab. Darüber hinaus veranschaulicht dieses Szenario einige der Funktionen für die Einzelanmeldung, die nur in i5/OS ab V5R3 verfügbar sind, z. B. die Richtlinienzuordnungen.
- Der Directory-Server auf System A wird als EIM-Domänencontroller für die neue EIM-Domäne MyCo-EimDomain konfiguriert.
- Nimmt an der EIM-Domäne MyCo-EIM-Domäne teil.
- Hat den Service-Principal-Namen `krbsvr400/systema.myco.com@MYCO.COM`.
- Hat den vollständig qualifizierten Hostnamen `systema.myco.com`. Dieser Name ist in einem einzigen Domain Name System (DNS) registriert, auf das alle PCs und Server im Netzwerk zeigen.
- In Ausgangsverzeichnissen auf System A ist der Cache für Berechtigungsnachweise für i5/OS-Benutzerprofile gespeichert.

System B
- Arbeitet mit i5/OS ab V5R3 mit den folgenden installierten Optionen und Lizenzprogrammen:
  - i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12)
  - Qshell Interpreter (5722-SS1 Option 30 oder 5761-SS1 Option 30)
  - System i Access für Windows (5722-XE1 oder 5761-XE1)
  - Network Authentication Enablement (5722-NAE oder 5761-NAE), wenn Sie mit i5/OS ab V5R4 arbeiten
  - Cryptographic Access Provider (5722-AC3), wenn Sie mit i5/OS V5R3 arbeiten
- Hat den vollständig qualifizierten Hostnamen `systemb.myco.com`. Dieser Name ist in einem einzigen Domain Name System (DNS) registriert, auf das alle PCs und Server im Netzwerk zeigen.
- Der Principal-Name für System B lautet `krbsvr400/systemb.myco.com@MYCO.COM`.
- Nimmt an der EIM-Domäne MyCo-EIM-Domäne teil.
- In Ausgangsverzeichnissen auf System B ist der Cache für Berechtigungsnachweise für i5/OS-Benutzerprofile gespeichert.

Verwaltungs-PC
- Wird unter dem Betriebssystem Microsoft Windows 2000 ausgeführt.
- Arbeitet mit System i Access für Windows (5722-XE1 oder 5761-XE1).
- Arbeitet mit System i Navigator mit den folgenden installierten Unterkomponenten:
  - Netzwerk
  - Sicherheit
  - Benutzer und Gruppen
- Fungiert als primäres Anmeldesystem für den Administrator.
- Konfiguriert als Bestandteil des Realms MYCO.COM (Windows-Domäne).

Voraussetzungen und Annahmen

Zur erfolgreichen 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 diese Lizenzprogramme installiert wurden:

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

      Anmerkung: Die APIs für den Netzwerkauthentifizierungsservice unterstützen Jobumgebungen für die meisten EBCDIC-CCSIDs. Die CCSIDs 290 und 5026 werden allerdings nicht unterstützt, da bei den Kleinbuchstaben a bis z eine Varianz auftritt.
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 System A konfiguriert worden sein.

   Anmerkung: Die Anweisungen in diesem Szenario basieren auf der Annahme, dass der Directory-Server nicht zuvor auf System 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. Für die Auflösung der Hostnamen im Netzwerk wird ein einziger DNS-Server verwendet. Es werden keine Hosttabellen für die Auflösung der Hostnamen verwendet.

   Anmerkung: Die Verwendung von Hosttabellen bei der Kerberos-Authentifizierung kann zu Fehlern bei der Namensauflösung oder anderen Problemen führen. Ausführliche Informationen zur Auflösung von Hostnamen bei der Kerberos-Authentifizierung finden Sie unter „Hinweise zur Auflösung von Hostnamen" auf Seite 89.

Konfigurationsschritte

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 - Konzepte
- Konzepte für Netzwerkauthentifizierungsservice

Führen Sie die folgenden Schritte durch, um die Einzelanmeldung auf Ihrem System zu konfigurieren.

Zugehörige Konzepte

Übersicht zur Einzelanmeldung

Domänen

Planungsarbeitsblätter ausfüllen

Diese Planungsarbeitsblätter veranschaulichen die Informationen, die Sie aufzeichnen, sowie die Entscheidungen, die Sie treffen müssen, wenn Sie die Konfiguration der von diesem Szenario beschriebenen Einzelanmeldungsfunktion vorbereiten.

Die folgenden Planungsarbeitsblätter wurden basierend auf den allgemeinen Planungsarbeitsblättern der Einzelanmeldung an dieses Szenario angepasst. Um eine erfolgreiche Implementierung sicherzustellen, sollten Sie für alle vorausgesetzten Elemente im Arbeitsblatt die Antwort "Ja" geben können. Außerdem sollten Sie alle Informationen, die zur Fertigstellung der Arbeitsblätter erforderlich sind, aufzeichnen, bevor Sie Konfigurationsaufgaben ausführen.

Anmerkung: Die APIs für den Netzwerkauthentifizierungsservice unterstützen Jobumgebungen für die meisten EBCDIC-CCSIDs. Die CCSIDs 290 und 5026 werden allerdings nicht unterstützt, da bei den Kleinbuchstaben a bis z eine Varianz auftritt.

Tabelle 13. Arbeitsblatt für Voraussetzungen der Einzelanmeldung

Arbeitsblatt für Voraussetzungen	**Antworten**
Ist auf Ihrem System i5/OS V5R3 oder eine spätere Version des Produkts (5722-SS1) oder V6R1 (5761-SS1) installiert?	Ja
Sind auf System A und System B die folgenden Optionen und Lizenzprogramme installiert: • i5/OS-Host-Server (5722-SS1 Option 12 oder 5761-SS1 Option 12) • Qshell Interpreter (5722-SS1 Option 30 oder 5761-SS1 Option 30) • System i Access für Windows (5722-XE1 oder 5761-XE1) • Network Authentication Enablement (5722-NAE oder 5761-NAE), wenn Sie mit i5/OS ab V5R4 arbeiten • Cryptographic Access Provider (5722-AC3), wenn Sie mit i5/OS V5R3 arbeiten	Ja
Ist eine Anwendung installiert, die auf allen PCs, die sich in der Einzelanmeldungsumgebung befinden, für die Einzelanmeldung aktiviert ist? **Anmerkung:** In diesem Szenario wurde für alle teilnehmenden PCs System i Access für Windows (5722-XE1 oder 5761-XE1) installiert.	Ja
Ist System i Navigator auf dem PC des Administrators installiert? • Wird die Unterkomponente "Netzwerk" des System i Navigator, die auf dem PC installiert ist, für die Verwaltung der Einzelanmeldung verwendet? • Wird die Unterkomponente "Sicherheit" des System i Navigator, die auf dem PC installiert ist, für die Verwaltung der Einzelanmeldung verwendet? • Wird die Unterkomponente "Benutzer und Gruppen" des System i Navigator, die auf dem PC installiert ist, für die Verwaltung der Einzelanmeldung verwendet?	Ja
Ist das aktuellste Service-Pack für System i Access für Windows installiert? Sie können das aktuellste Service-Pack über die Website für System i Access abrufen.	Ja
Besitzt der Administrator für Einzelanmeldung die Sonderberechtigungen *SECADM, *ALLOBJ und *IOSYSCFG?	Ja
Fungiert eines der folgenden Systeme als Kerberos-Server (auch als KDC bezeichnet)? Wenn ja, geben Sie an, um welches System es sich handelt. 1. Microsoft Windows 2000 Server **Anmerkung:** Microsoft Windows 2000 Server verwendet die Kerberos-Authentifizierung als Standardsicherheitsmechanismus. 2. Windows Server 2003 3. i5/OS PASE (ab V5R3) 4. AIX-Server 5. z/OS	Ja, Windows 2000 Server
Sind alle PCs Ihres Netzwerks in einer Windows 2000-Domäne konfiguriert?	Ja
Wurden die neuesten PTFs (vorläufigen Programmkorrekturen) angelegt?	Ja

Tabelle 13. Arbeitsblatt für Voraussetzungen der Einzelanmeldung (Forts.)

Arbeitsblatt für Voraussetzungen	Antworten
Beträgt die Abweichung zwischen der Systemzeit des System i-Systems und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung größer, lesen Sie die Informationen unter „Systemzeiten synchronisieren" auf Seite 110.	Ja

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

Tabelle 14. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung für System A

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

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

Planungsarbeitsblatt für die Konfiguration von System A	**Antworten**
Für welche Services sollen Chiffrierschlüsseleinträge erstellt werden? • i5/OS-Kerberos-Authentifizierung • LDAP • IBM HTTP-Server • i5/OS NetServer • NFS-Server	i5/OS-Kerberos-Authentifizierung
Wie lautet das Kennwort für Ihre(n) Service-Principal(s)?	`systema123`
Möchten Sie eine Stapeldatei erstellen, um das Hinzufügen der Service-Principals für System 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. **Anmerkung:** Geben Sie den registrierten Namen und das Kennwort des LDAP-Administrators an, um sicherzustellen, dass der Assistent eine ausreichende Berechtigung zur Verwaltung der EIM-Domäne und der darin enthaltenen Objekte besitzt.	**Port:** `389` **Registrierter Name:** `cn=Administrator` **Kennwort:** `mycopwd`
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--SYSTEMA.MYCO.COM Kerberos--KDC1.MYCO.COM **Anmerkung:** Sie dürfen die Auswahl **Bei Kerberos-Benutzeridentifikationen muss die Groß-/Kleinschreibung beachtet werden** nicht auswählen, wenn sie vom Assistenten angeboten wird.
Welchen EIM-Benutzer soll System A bei der Ausführung von EIM-Operationen verwenden? Dies ist der Systembenutzer. **Anmerkung:** Wenn Sie den Directory-Server nicht vor der Konfiguration der Einzelanmeldung konfiguriert haben, können Sie als registrierten Namen für den Systembenutzer nur die Kombination aus dem registrierten Namen und dem Kennwort des LDAP-Administrators bereitstellen.	**Benutzerart:** `Registrierter Name` **Registrierter Name:** `cn=Administrator` **Kennwort:** `mycopwd`

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

Tabelle 15. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung für System B

Planungsarbeitsblatt für die Konfiguration von System B	**Antworten**
Verwenden Sie die folgenden Informationen, um den EIM-Konfigurationsassistenten für System B auszuführen:	

Tabelle 15. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung für System B (Forts.)

Planungsarbeitsblatt für die Konfiguration von System B	**Antworten**
Wie möchten Sie EIM auf Ihrem System konfigurieren?	System zu einer vorhandenen Domäne hinzufügen
Möchten Sie den Netzwerkauthentifizierungsservice konfigurieren? **Anmerkung:** Sie müssen den Netzwerkauthentifizierungsservice konfigurieren, um die Einzelanmeldung konfigurieren zu können.	Ja
Der Assistent für den Netzwerkauthentifizierungsservice wird über den EIM-Konfigurationsassistenten gestartet. Verwenden Sie die folgenden Informationen, um den Assistenten für den Netzwerkauthentifizierungsservice auszuführen: **Anmerkung:** Der Assistent für den Netzwerkauthentifizierungsservice kann unabhängig vom EIM-Konfigurationsassistenten gestartet werden.	
Wie lautet der Name des Kerberos-Standard-Realms, zu dem Ihr System i-Produkt gehören soll? **Anmerkung:** Eine Windows 2000-Domäne entspricht einem Kerberos-Realm. Microsoft Active Directory verwendet standardmäßig als Sicherheitsmechanismus die Kerberos-Authentifizierung.	`MYCO.COM`
Verwenden Sie Microsoft Active Directory?	Ja
Welcher Kerberos-Server wird für diesen Kerberos-Standard-Realm verwendet? An welchem Port ist der Kerberos-Server empfangsbereit?	**KDC:** `kdc1.myco.com` **Port:** `88` **Anmerkung:** Dies ist der Standardport für den Kerberos-Server.
Möchten Sie einen Kennwortserver für diesen Standard-Realm konfigurieren? Wenn ja, beantworten Sie die folgenden Fragen: Wie lautet der Name des Kennwortservers für diesen Kerberos-Server? An welchem Port ist der Kennwortserver empfangsbereit?	Ja **Kennwortserver:** `kdc1.myco.com` **Port:** `464` **Anmerkung:** Dies ist der Standardport für den Kennwortserver.
Für welche Services sollen Chiffrierschlüsseleinträge erstellt werden? • i5/OS-Kerberos-Authentifizierung • LDAP • IBM HTTP-Server • i5/OS NetServer • NFS-Server	i5/OS-Kerberos-Authentifizierung
Wie lautet das Kennwort für Ihre i5/OS-Service-Principals?	systemb123
Möchten Sie eine Stapeldatei erstellen, um das Hinzufügen der Service-Principals für System 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 System B auszuführen:	
Wie lautet der Name des EIM-Domänencontrollers für die EIM-Domäne, die Sie dem System hinzufügen möchten?	systema.myco.com
Möchten Sie die Verbindung mit SSL oder TLS sichern?	Nein
An welchem Port ist der EIM-Domänencontroller empfangsbereit?	389

Tabelle 15. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung für System B (Forts.)

Planungsarbeitsblatt für die Konfiguration von System B	Antworten
Über welchen Benutzer möchten Sie eine Verbindung zum Domänencontroller herstellen? Dies ist der Benutzer der Verbindung. **Anmerkung:** Geben Sie den registrierten Namen und das Kennwort des LDAP-Administrators an, um sicherzustellen, dass der Assistent eine ausreichende Berechtigung zur Verwaltung der EIM-Domäne und der darin enthaltenen Objekte besitzt.	**Benutzerart:** `Registrierter Name und Kennwort` **Registrierter Name:** `cn=Administrator` **Kennwort:** `mycopwd`
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--SYSTEMB.MYCO.COM
Welchen EIM-Benutzer soll System B bei der Ausführung von EIM-Operationen verwenden? Dies ist der Systembenutzer. **Anmerkung:** In einer früheren Phase dieses Szenarios haben Sie den EIM-Konfigurationsassistenten verwendet, um den Directory-Server auf System A zu konfigurieren. Auf diese Weise haben Sie einen registrierten Namen und ein Kennwort für den LDAP-Administrator erstellt. Dies ist der einzige registrierte Name, der für den Directory-Server definiert ist. Daher müssen Sie diesen registrierten Namen und das Kennwort hier angeben.	**Benutzerart:** `Registrierter Name und Kennwort` **Registrierter Name:** `cn=Administrator` **Kennwort:** `mycopwd`

Tabelle 16. Planungsarbeitsblatt für die Konfiguration der Einzelanmeldung - Benutzerprofile

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

Tabelle 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	SYSTEMA.MYCO.COM	JOHND	Ziel	i5/OS-Benutzerprofil auf System A
John Day	SYSTEMB.MYCO.COM	DAYJO	Ziel	i5/OS-Benutzerprofil auf System B
Sharon Jones	MYCO.COM	sjones	Quelle	Benutzeridentität für Kerberos-Anmeldung (Windows 2000)
Sharon Jones	SYSTEMA.MYCO.COM	SHARONJ	Ziel	i5/OS-Benutzerprofil auf System A
Sharon Jones	SYSTEMB.MYCO.COM	JONESSH	Ziel	i5/OS-Benutzerprofil auf System B

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

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

Einzelanmeldungsbasiskonfiguration für System A erstellen

Der EIM-Konfigurationsassistent hilft Ihnen bei der Erstellung einer EIM-Basiskonfiguration. Er 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 System 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 System A zu konfigurieren. Dieser Schritt setzt sich aus folgenden Tasks zusammen:

- Eine neue EIM-Domäne erstellen.
- Den Directory-Server auf System A als EIM-Domänencontroller konfigurieren.
- Den Netzwerkauthentifizierungsservice konfigurieren.
- EIM-Registerdefinitionen für das i5/OS-Register und das Kerberos-Register auf System A erstellen.
- System A zur Nutzung der EIM-Domäne konfigurieren.

1. Erweitern Sie im System i Navigator den Eintrag für **System A → Netzwerk → Enterprise Identity Mapping**.
2. Klicken Sie mit der rechten Maustaste auf **Konfiguration**, und wählen Sie **Konfigurieren** aus, um den EIM-Konfigurationsassistenten zu starten.
3. Wählen Sie auf der Begrüßungsseite **Neue Domäne erstellen und System hinzufügen** aus. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite 'Position der EIM-Domäne angeben' **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 Einstellung **Ja** aus.

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

b. Geben Sie auf der Seite 'Realm-Informationen angeben' im Feld **Standard-Realm** den Wert `MYCO.COM` ein, und wählen Sie **Microsoft Active Directory wird für Kerberos-Authentifizierung verwendet** aus. Klicken Sie auf **Weiter**.

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

d. Wählen Sie auf der Seite 'Kennwortserverinformationen angeben' die Einstellung **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' **i5/OS-Kerberos-Authentifizierung** aus. Klicken Sie auf **Weiter**.

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

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

   - **Stapeldatei:** Fügen Sie am Ende des standardmäßig verwendeten Stapeldateinamens die Zeichenfolge `systema` an. Beispiel: `C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystema.bat`.
   - Wählen Sie **Kennwort einfügen** aus. Dies garantiert, dass alle Kennwörter, die dem i5/OS-Service-Principal zugeordnet sind, in die Stapeldatei eingefügt werden. Beachten Sie, dass Kennwörter in Klartext angezeigt werden und von jeder Person mit Lesezugriffsberechtigung für die Stapeldatei gelesen werden können. Daher wird empfohlen, dass Sie die Stapeldatei nach dem Gebrauch unverzüglich vom Kerberos-Server und von Ihrem PC löschen.

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

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

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

   Hinweise:

   - Wenn Sie den Directory-Server vor dem Beginn dieses Szenarios konfiguriert haben, erscheint an Stelle der Seite 'Directory-Server konfigurieren' die Seite 'Benutzer für Verbindung angeben'. In diesem Fall müssen Sie den registrierten Namen und das Kennwort für den LDAP-Administrator angeben.
   - Wenn Sie auf Systemen, die mit i5/OS V6R1 arbeiten, mehrere Directory-Server konfiguriert haben, werden die Seiten 'Directory-Server-Instanz angeben' und 'Benutzer für Verbindung angeben' angezeigt. In diesem Fall müssen Sie die registrierten Namen und die Kennwörter für den LDAP-Administrator angeben.

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

7. Geben Sie auf der Seite 'Domäne angeben' im Feld **Domäne** den Namen der Domäne ein. Beispiel: `MyCo-EIM-Domäne`.

8. Wählen Sie auf der Seite 'Übergeordneten registrierten Namen für Domäne angeben' die Einstellung **Nein** aus. Klicken Sie auf **Weiter**.

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

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

   Hinweise:

   - 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`

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

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

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

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

1. Erweitern Sie im System i Navigator den Eintrag für **System B** → **Netzwerk** → **Enterprise Identity Mapping**.
2. Klicken Sie mit der rechten Maustaste auf **Konfiguration**, und wählen Sie **Konfigurieren** aus, um den Konfigurationsassistenten zu starten.
3. Wählen Sie auf der Begrüßungsseite **System zu einer vorhandenen Domäne hinzufügen** aus. 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 Einstellung **Ja** aus.

      Anmerkung: Auf diese Weise wird der Assistent für den Netzwerkauthentifizierungsservice gestartet. Mit diesem Assistenten können Sie verschiedene i5/OS-Schnittstellen und -Services zur Nutzung eines Kerberos-Netzwerks 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** als Namen des Kerberos-Servers den Wert `kdc1.myco.com` und im Feld **Port** den Wert `88` ein. Klicken Sie auf **Weiter**.
   d. Wählen Sie auf der Seite 'Kennwortserverinformationen angeben' die Einstellung **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' **i5/OS-Kerberos-Authentifizierung** aus. Klicken Sie auf **Weiter**.

f. Geben Sie auf der Seite 'i5/OS-Chiffrierschlüsseleintrag erstellen' ein Kennwort (z. B. `systema123`) ein, und bestätigen Sie es. Klicken Sie anschließend auf **Weiter**. Dieses Kennwort wird verwendet, wenn der Service-Principal von System A zum Kerberos-Server hinzugefügt wird.

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

   - **Stapeldatei:** Fügen Sie am Ende des standardmäßig verwendeten Stapeldateinamens die Zeichenfolge `systemb` an. Geben Sie beispielsweise `C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystemb.bat` ein.
   - Wählen Sie **Kennwort einfügen** aus. Dies garantiert, dass alle Kennwörter, die dem i5/OS-Service-Principal zugeordnet sind, in die Stapeldatei eingefügt werden. Beachten Sie, dass Kennwörter in Klartext angezeigt werden und von jeder Person mit Lesezugriffsberechtigung für die Stapeldatei gelesen werden können. Daher wird empfohlen, dass Sie die Stapeldatei nach dem Gebrauch unverzüglich vom Kerberos-Server und von Ihrem PC löschen.

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

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

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

   Anmerkung: Geben Sie die Werte für den registrierten Namen des LDAP-Administrators sowie für dessen Kennwort an, die Sie zuvor in diesem Szenario auf System A definiert haben.

   a. **Benutzerart**: `Registrierter Name und Kennwort`
   b. **Registrierter Name**: `cn=Administrator`
   c. **Kennwort**: `mycopwd`
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' **Lokales i5/OS** aus, und heben Sie die Auswahl von **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.

   Hinweise:
   - 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 die Werte für den registrierten Namen des LDAP-Administrators sowie für dessen Kennwort an, die Sie zuvor in diesem Szenario auf System A definiert haben.

   a. **Benutzerart**: `Registrierter Name und Kennwort`

b. **Registrierter Name**: `cn=Administrator`

c. **Kennwort**: `mycopwd`

10. Bestätigen Sie auf der Seite 'Zusammenfassung' die EIM-Konfiguration. Klicken Sie auf **Fertig stellen**.

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

Sie können die erforderlichen i5/OS-Service-Principals manuell zum Kerberos-Server hinzufügen. Wie im folgenden Szenario dargestellt, können Sie auch eine Stapeldatei verwenden, um diese hinzuzufügen.

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:

1. Erstellen Sie die FTP-Stapeldateien.
   a. 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. Mit diesem Befehl wird eine FTP-Sitzung auf Ihrem PC gestartet. Sie werden aufgefordert, den Benutzernamen und das Kennwort des Administrators einzugeben.
   b. 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.
   c. Geben Sie bei der FTP-Eingabeaufforderung `cd \meinVerzeichnis` ein. *meinVerzeichnis* bezeichnet ein auf kdc1.myco.com befindliches Verzeichnis.
   d. Geben Sie bei der FTP-Eingabeaufforderung `put NASConfigsystema.bat` ein. Daraufhin wird die Nachricht `226 Übertragung abgeschlossen` (oder ähnlicher Wortlaut) angezeigt.
   e. Geben Sie `quit` ein, um die FTP-Sitzung zu verlassen.
2. Beide Stapeldateien auf kdc1.myco.com ausführen
   a. Öffnen Sie auf dem Windows 2000-Server das Verzeichnis, in das die Stapeldateien übertragen wurde.
   b. Suchen Sie die Datei `NASConfigsystema.bat`, und führen Sie sie durch Doppelklicken aus.
   c. Wiederholen Sie die Schritte 1a bis 2b für `NASConfigsystemb.bat`.
   d. Vergewissern Sie sich nach der Ausführung der Dateien, dass der i5/OS-Principal zum Kerberos-Server hinzugefügt wurde. Führen Sie dazu die folgenden Schritte durch:
      1) Erweitern Sie auf dem Windows 2000-Server den Eintrag für **Verwaltungstools → Active Directory-Benutzer und -Computer → Benutzer**.
      2) Vergewissern Sie sich, dass die System i-Plattform 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.
      3) Suchen Sie in der angezeigten Benutzerliste die Einträge **systema_1_krbsvr400** und **systemb_1_krbsvr400**. Dies sind die Benutzerkonten, die für den i5/OS-Principal-Namen generiert wurden.
      4) Rufen Sie die Eigenschaften der Active Directory-Benutzer auf. Wählen Sie auf der Indexzunge **Konto** die Auswahl **Konto wird für Delegierungszwecke vertraut** aus.

         Anmerkung: Dieser optionale Schritt ermöglicht es Ihrem System, die Berechtigungsnachweise eines Benutzers an andere Systeme zu delegieren oder weiterzuleiten. Folglich

kann der i5/OS-Service-Principal im Namen des Benutzers auf Services zuzugreifen, die sich auf mehreren Systemen befinden. Dies ist besonders in einem Netzwerk mit mehreren Ebenen von Vorteil.

Benutzerprofile auf System A und System B erstellen

Die Benutzer im Kerberos-Register MYCO.COM sollen alle einem einzigen i5/OS-Benutzerprofil auf Ihren System i-Plattformen zugeordnet werden. Daher müssen Sie ein i5/OS-Benutzerprofil auf System A und System B erstellen.

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

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

Ausgangsverzeichnisse auf System A und System B erstellen

Jeder Benutzer, der eine Verbindung zu i5/OS und zu 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 die folgenden Schritte durch, um ein Ausgangsverzeichnis für einen Benutzer zu erstellen:

1. Geben Sie in der Befehlszeile von System A `CRTDIR '/home/Benutzerprofil'` ein, wobei `Benutzerprofil` den Namen des i5/OS-Benutzerprofils für den Benutzer bezeichnet. Beispiel: `CRTDIR '/home/SYSUSERA'`.
2. Wiederholen Sie diesen Befehl auf System B, geben Sie dabei jedoch `SYSUSERB` ein, um ein Ausgangsverzeichnis für das Benutzerprofil auf System B zu erstellen.

Netzwerkauthentifizierungsservice auf System A und System B testen

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

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

Anmerkung: Vergewissern Sie sich, dass Sie ein Ausgangsverzeichnis für Ihr 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 anzuzeigen, die in der Chiffrierschlüsseldatei registriert sind. In diesem Szenario sollte krbsvr400/systema.myco.com@MYCO.COM als Name des Principals für System A erscheinen.
3. Geben Sie `kinit -k krbsvr400/systema.myco.com@MYCO.COM` ein, um ein Ticket-granting Ticket vom Kerberos-Server anzufordern. Mit diesem Befehl wird geprüft, ob Ihr System ordnungsgemäß konfiguriert wurde und das Kennwort in der Chiffrierschlüsseldatei mit dem auf dem Kerberos-Server gespeicherten Kennwort übereinstimmt. Wenn die Prüfung erfolgreich verläuft, dann werden für den Befehl kinit keine Fehler ausgegeben.

4. Geben Sie `klist` ein, um sicherzustellen, dass der Standard-Principal krbsvr400/systema.myco.com@MYCO.COM lautet. Mit diesem Befehl wird der Inhalt eines Kerberos-Caches für Berechtigungsnachweise angezeigt und geprüft, ob ein gültiges Ticket für den i5/OS-Service-Principal erstellt und in den Cache für Berechtigungsnachweise auf dem System aufgenommen wurde.

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

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

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

EIM-Kennungen für die beiden 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 System i Navigator den Eintrag für **System A** → **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung** → **MyCoEimDomain**.

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

   a. **Benutzerart:** `Registrierter Name`
   b. **Registrierter Name**: `cn=Administrator`
   c. **Kennwort**: `mycopwd`
2. Klicken Sie mit der rechten Maustaste auf **Kennungen**, und wählen Sie dann **Neue Kennung** aus.
3. Geben Sie im Dialogfenster **Neue EIM-Kennung** im Feld **Kennung** `John Day` ein. Klicken Sie auf **OK**.
4. Wiederholen Sie die Schritte 2 bis 4, geben Sie jedoch im Feld **Kennung** den Namen `Sharon Jones` ein.

Kennungszuordnungen für John Day erstellen

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

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

- Eine Quellenzuordnung für den Kerberos-Principal ″jday″, die Benutzeridentität, die 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 der Benutzer John Day als Benutzeridentität zur Anmeldung beim System i Navigator und anderen i5/OS-Anwendungen auf System 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 der Benutzer John Day als Benutzeridentität zur Anmeldung beim System i Navigator und anderen i5/OS-Anwendungen auf System 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 System A den Eintrag für **Netzwerk → Enterprise Identity Mapping → Domänenverwaltung → MyCoEimDomain → Kennungen**.
2. Klicken Sie mit der rechten Maustaste auf **John Day**, und wählen Sie **Eigenschaften** aus.
3. Klicken Sie auf der Seite 'Zuordnungen' auf **Hinzufügen**.
4. Geben Sie im Dialogfenster **Zuordnung hinzufügen** Informationen an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **OK**:
   a. **Register**: `MYCO.COM`
   b. **Benutzer**: `jday`
   c. **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 System 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**:
   a. **Register**: `SYSTEMA.MYCO.COM`
   b. **Benutzer**: `JOHND`
   c. **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 System 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**:
    a. **Register**: `SYSTEMB.MYCO.COM`
    b. **Benutzer**: `DAYJO`
    c. **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.

Kennungszuordnungen für Sharon Jones erstellen

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

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

- Eine Quellenzuordnung für den Kerberos-Principal "sjones", die Benutzeridentität, die 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 Benutzerin Sharon Jones als Benutzeridentität zur Anmeldung beim System i Navigator und anderen i5/OS-Anwendungen auf System 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 Benutzerin Sharon Jones als Benutzeridentität zur Anmeldung beim System i Navigator und anderen i5/OS-Anwendungen auf System 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 System A den Eintrag für **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung** → **MyCoEimDomain** → **Kennungen**.
2. Klicken Sie mit der rechten Maustaste auf **Sharon Jones**, und wählen Sie **Eigenschaften** aus.
3. Klicken Sie auf der Seite 'Zuordnungen' auf **Hinzufügen**.
4. Geben Sie im Dialogfenster **Zuordnung hinzufügen** Informationen an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **OK**:
   a. **Register**: `MYCO.COM`
   b. **Benutzer**: `sjones`
   c. **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 System 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**:
   a. **Register**: `SYSTEMA.MYCO.COM`
   b. **Benutzer**: `SHARONJ`
   c. **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 System 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**:
    a. **Register**: `SYSTEMB.MYCO.COM`
    b. **Benutzer**: `JONESSH`
    c. **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.

Standardrichtlinienzuordnung für Register erstellen

Sie können Richtlinienzuordnungen verwenden, um Abgleiche direkt zwischen einer Gruppe von Benutzern und einer einzelnen Zielbenutzeridentität zu erstellen.

Sie wollen, dass alle Microsoft Active Directory-Benutzer auf dem Windows 2000-Server eine Zuordnung zum Benutzerprofil SYSUSERA auf System A und zum Benutzerprofil SYSUSERB auf System B erhalten. In diesem Fall können Sie eine Standardrichtlinienzuordnung für Register erstellen, die alle Benutzeridentitäten (für die keine Kennungszuordnungen vorhanden sind) im Kerberos-Register MYCO.COM einem einzigen i5/OS-Benutzerprofil auf System 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 abhängig davon, auf welche System i-Plattform der Kerberos-Benutzer zugreift, Benutzeridentitäten in diesem Register verschiedenen Zielbenutzeridentitäten zu.

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

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

Bevor Sie Richtlinienzuordnungen verwenden können, müssen Sie zuerst die Domäne zur Verwendung von Richtlinienzuordnungen für Abgleichsuchoperationen aktivieren.

Führen Sie die folgenden Schritte durch, um die Domäne zur Verwendung von Richtlinienzuordnungen für Abgleichsuchoperationen zu aktivieren:

1. Erweitern Sie im System i Navigator den Eintrag für **System 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' **Abgleichsuchen mit Hilfe von Richtlinienzuordnungen für Domäne MyCo-EIM-Domäne aktivieren** aus.

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

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

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

1. Klicken Sie auf der Seite 'Register' auf **Hinzufügen**.
2. Geben Sie im Dialogfenster **Standardrichtlinienzuordnung für Register hinzufügen** Informationen an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **OK**:
   a. **Quellenregister**: `MYCO.COM`

b. **Zielregister**: SYSTEMB.MYCO.COM
c. **Zielbenutzer**: SYSUSERB

3. Klicken Sie auf **OK**, um das Dialogfenster **Abgleichrichtlinie** zu schließen.

Register für die Teilnahme an Suchoperationen und die Verwendung von Richtlinienzuordnungen aktivieren

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.

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.

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 System i Navigator den Eintrag für **System A** → **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung** → **MyCoEimDomain** → **Benutzerregister**.
2. Klicken Sie mit der rechten Maustaste auf **MYCO.COM**, und wählen Sie **Abgleichrichtlinie** aus.
3. Wählen Sie auf der Seite 'Allgemein' **Abgleichsuchen für Register MYCO.COM aktivieren** aus. Klicken Sie auf **OK**.

   Führen Sie die folgenden Schritte durch, um das Register SYSTEMA.MYCO.COM für die Teilnahme an Abgleichsuchoperationen und die Verwendung von Richtlinienzuordnungen zu aktivieren:
4. Erweitern Sie im System i Navigator den Eintrag für **System A** → **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung** → **MyCoEimDomain** → **Benutzerregister**.
5. Klicken Sie mit der rechten Maustaste auf **SYSTEMA.MYCO.COM**, und wählen Sie **Abgleichrichtlinie** aus.
6. Wählen Sie auf der Seite 'Allgemein' **Abgleichsuchen für Register SYSTEMA.MYCO.COM aktivieren** und dann **Richtlinienzuordnungen verwenden** aus. Klicken Sie auf **OK**.
7. Wiederholen Sie die Schritte 1 bis 6, um das Register SYSTEMB.MYCO.COM für die Teilnahme an Abgleichsuchoperationen und die Verwendung von Richtlinienzuordnungen zu aktivieren, wählen Sie jedoch auf der Seite 'Allgemein' **Abgleichsuchen für Register SYSTEMB.MYCO.COM aktivieren** und dann **Richtlinienzuordnungen verwenden** aus. Klicken Sie auf **OK**.

EIM-Identitätsabgleiche testen

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

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

Abgleiche für John Day testen

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

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

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

a. **Benutzerart:** `Registrierter Name`
b. **Registrierter Name**: `cn=Administrator`
c. **Kennwort**: `mycopwd`

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**:
   a. **Quellenregister**: `MYCO.COM`
   b. **Quellenbenutzer**: `jday`
   c. **Zielregister**: `SYSTEMA.MYCO.COM`

   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

4. Klicken Sie auf **Schließen**.
5. Wiederholen Sie diese Schritte, wählen Sie jedoch für das Feld **Zielregister** die Auswahl `SYSTEMB.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:

6. Erweitern Sie im System i Navigator den Eintrag für **System A** → **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung** → **MyCoEimDomain**.

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

   a. **Benutzerart:** `Registrierter Name`
   b. **Registrierter Name**: `cn=Administrator`
   c. **Kennwort**: `mycopwd`
7. Klicken Sie mit der rechten Maustaste auf **MyCo-EIM-Domäne**, und wählen Sie **Abgleich testen** aus.
8. Geben Sie im Dialogfenster **Abgleich testen** Informationen an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **Test**:

a. **Quellenregister**: `MYCO.COM`
b. **Quellenbenutzer**: `sjones`
c. **Zielregister**: `SYSTEMA.MYCO.COM`

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

9. Klicken Sie auf **Schließen**.
10. Wiederholen Sie die Schritte 1 auf Seite 78 bis 9, wählen Sie jedoch für das Feld **Zielregister** den Wert `SYSTEMB.MYCO.COM` aus. Die Ergebnisse werden im Abschnitt **Gefundener Abgleich** der Seite wie folgt angezeigt:

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

Für Standardrichtlinienzuordnung für Register verwendete Abgleiche testen

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

11. Erweitern Sie im System i Navigator den Eintrag für **System A** → **Netzwerk** → **Enterprise Identity Mapping** → **Domänenverwaltung** → **MyCoEimDomain**.

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

    a. **Benutzerart:** `Registrierter Name`
    b. **Registrierter Name**: `cn=Administrator`
    c. **Kennwort**: `mycopwd`
12. Klicken Sie mit der rechten Maustaste auf **MyCo-EIM-Domäne**, und wählen Sie **Abgleich testen** aus.
13. Geben Sie im Dialogfenster **Abgleich testen** Informationen an, oder klicken Sie auf **Durchsuchen**, um die folgenden Informationen auszuwählen. Klicken Sie anschließend auf **Test**:
    a. **Quellenregister**: `MYCO.COM`
    b. **Quellenbenutzer**: `mmiller`
    c. **Zielregister**: `SYSTEMA.MYCO.COM`

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

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

14. Klicken Sie auf **Schließen**.

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

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

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

   a. **Benutzerart:** `Registrierter Name`
   b. **Registrierter Name**: `cn=Administrator`
   c. **Kennwort**: `mycopwd`

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**:
   a. **Quellenregister**: `MYCO.COM`
   b. **Quellenbenutzer**: `ksmith`
   c. **Zielregister**: `SYSTEMB.MYCO.COM`

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

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

4. 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.

System i Access für Windows-Anwendungen für den Einsatz der Kerberos-Authentifizierung konfigurieren

Basierend auf Ihren Zielen für die Einzelanmeldung müssen alle Benutzer in der Auftragsannahmeabteilung die Kerberos-Authentifizierung durchführen, bevor sie mit dem System i Navigator auf System A und B zugreifen können. Aus diesem Grund müssen Sie System i Access für Windows so konfigurieren, dass die Kerberos-Authentifizierung verwendet werden kann.

Führen Sie die folgenden Schritte durch, um System i Access für Windows-Anwendungen für die 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 2000-Domäne an, indem Sie sich am PC anmelden.
2. Klicken Sie mit der rechten Maustaste im System i Navigator auf dem PC auf den Eintrag für **System A**, und wählen Sie **Eigenschaften** aus.
3. Wählen Sie auf der Seite 'Verbindung' **Kerberos-Principal-Namen verwenden, keine Anforderung** aus. So können System i 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 System i Navigator, und starten Sie ihn erneut.
5. Wiederholen Sie diese Schritte für System B.

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 System i Navigator den Eintrag für **System A**, um eine Verbindung zu System A herzustellen.
2. Drücken Sie F5, um die Anzeige zu aktualisieren.
3. Suchen Sie im rechten Fensterbereich in der Spalte **Name** nach `System A`, und vergewissern Sie sich, dass das i5/OS-Benutzerprofil von John Day (`JOHND`) in der Spalte **Angemeldeter Benutzer** als entsprechender Eintrag angezeigt wird. Der System i Navigator konnte mit Hilfe von EIM eine Zuordnung zwischen dem Kerberos-Principal jday und dem Benutzerprofil JOHND auf System A herstellen, weil für die EIM-Kennung John Day entsprechende Zuordnungen definiert wurden. Die Verbindung der System i Navigator-Sitzung für System A arbeitet nun unter dem Namen JOHND.
4. Wiederholen Sie diese Schritte für Sharon Jones und für mindestens eine der Benutzeridentitäten, die dem Benutzerprofil SYSUSERA oder SYSUSERB zugeordnet sind.

Hinweise zur Konfigurationsnachbereitung

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.

Nach Durchführung des Szenarios ist der registrierte Name (DN) für den LDAP-Administrator der einzige EIM-Benutzer, den Sie definiert haben und der von EIM verwendet werden kann. Der registrierte Name des LDAP-Administrators, den Sie für den Systembenutzer auf System A und System 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, für die Zugriffsberechtigungen für EIM-Daten definiert sind, die besser an die geltenden Anforderungen angepasst und eingeschränkt sind. 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 hergestellt werden, wenn alle Aspekte der EIM-Domäne mit dem System i Navigator verwaltet werden.
- **Mindestens ein Benutzer, der alle folgenden Zugriffsberechtigungen besitzt**:
  - Kennungsadministrator
  - Registeradministrator
  - EIM-Abgleichoperationen

  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 an Stelle 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 System A als auch für System B ändern. Informationen zur Änderung des registrierten Namens des Systembenutzers finden Sie in den Informationen zur Verwaltung der Eigenschaften der EIM-Konfiguration.

Zugehörige Konzepte

EIM-Zugriffssteuerung

IBM Directory Server for i5/OS (LDAP)

Zugehörige Tasks

EIM-Konfigurationseigenschaften verwalten

Netzwerkauthentifizierungsservice planen

Bevor Sie den Netzwerkauthentifizierungsservice oder eine Kerberos-Lösung auf Ihrem Netzwerk implementieren können, müssen Sie die erforderlichen Planungsaufgaben durchführen.

Um die Verwendung des Netzwerkauthentifizierungsservice und eine Kerberos-Implementierung zu planen, müssen Sie zunächst die entsprechenden Informationen über die Systeme und Benutzer Ihres Netzwerks 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 schwerpunktmäßig auf die Planung einer i5/OS-Implementierung und die Faktoren, die berücksichtigt werden müssen, wenn Sie den Netzwerkauthentifizierungsservice mit einem Kerberos-Server verwenden wollen, der unter Microsoft Active Directory oder i5/OS PASE konfiguriert ist.

Informationen zur Konfiguration eines Kerberos-Servers unter Microsoft Active Directory finden Sie unter Windows 2000 Server .

Die folgenden IBM Systeme unterstützen die Kerberos-Authentifizierung. Informationen über plattformspezifische Kerberos-Implementierungen finden Sie in den folgenden Quellen:

- **System p**
  - *IBM Network Authentication ServiceAIX, Linux, and Solaris Administrator's and User's Guide*.
  - *IBM Network Authentication Service AIX, Linux, and Solaris Application Development Reference*.

    Anmerkung: Die genannten Dokumentationen finden Sie auf der CD AIX 5L Expansion Pack and Bonus Pack.
- **System z**
  - z/OS Security Server Network Authentication Service Administration

Die folgenden Tasks unterstützen Sie bei der Planung des Netzwerkauthentifizierungsservice.

Kerberos-Server planen

Sie können den Einsatz eines Kerberos-Servers abhängig vom verwendeten Betriebssystem 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 auf dem 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 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 in diesen Betriebssystemen bereits ein Kerberos-Server integriert. Informationen über die Verwendungsweise der Kerberos-Authentifizierung auf Microsoft Windows-Servern finden Sie unter Windows 2000 Server .

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 wie beispielsweise einen Kerberos-Server zur Verfügung. Die folgenden Dokumentationen können Ihnen bei der Konfiguration und Verwaltung eines Kerberos-Servers in AIX helfen.

- *IBM Network Authentication Service AIX, Linux, and Solaris Administrator's and User's Guide*.
- *IBM Network Authentication Service AIX, Linux, and Solaris Application Development Reference*.

Anmerkung: Die genannten Dokumentationen 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 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 System i-Plattform 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. Die System i-Plattform 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 wird empfohlen, für diesen Wert nicht mehr als 300 Sekunden anzugeben. Nähere Informationen über das Arbeiten mit Systemzeiten finden Sie unter „Systemzeiten synchronisieren" auf Seite 110.

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? • Windows 2000 Server • Windows Server 2003 • AIX Server • i5/OS PASE (ab V5R3) • z/OS	i5/OS Portable Application Solutions Environment (PASE)
Wie lautet der vollständig qualifizierte Domänenname für den Kerberos-Server?	systema.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.
Soll ich das Produkt Network Authentication Enablement (5722-NAE oder 5761-NAE) installieren?	Ja, wenn Sie die Konfiguration eines Kerberos-Servers unter i5/OS PASE auf einem V5R4-System planen. Ab V5R4 wird der Netzwerkauthentifizierungsserver als separates Produkt unter der Bezeichnung *Network Authentication Enablement* (5722-NAE oder 5761-NAE) geliefert. Wenn Sie mit i5/OS V5R3 arbeiten, müssen Sie stattdessen Cryptographic Access Provider (5722-AC3) installieren, um einen Kerberos-Server in i5/OS PASE zu konfigurieren.

Realms planen

Die genaue Kenntnis der Abläufe Ihres Unternehmens vereinfacht die Planung der in der verwendeten Umgebung einzusetzenden Realms.

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 der 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 die Versandabteilung. Sie können außerdem Realms für eine Gruppe von Systemen oder Services erstellen, die ähnliche 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 einen 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 den 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. Bei einigen Kerberos-Implementierungen ist die Beachtung dieser Konvention jedoch zwingend vorgeschrieben. So sind beispielsweise für Realm-Namen in einem Microsoft Active Directory Großbuchstaben zwingend erforderlich. Wenn Sie den Netzwerkauthentifizierungsservice auf der System i-Plattform zur Nutzung eines Kerberos-Realms konfigurieren, der in Microsoft 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 Active Directory konfiguriert ist, 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 Auftragsannahmeabteilung authentifiziert. Die Versandabteilung verwendet einen Kerberos-Server in i5/OS PASE. Jede Abteilung soll Ihren eigenen Realm erhalten.

Tabelle 20. Beispiel eines Planungsarbeitsblatts für Kerberos-Realms (Forts.)

Fragen	Antworten
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 Auftragsannahmeabteilung 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 System i-Plattformen können die Principal-Namen wahlweise erstellt werden. Jeder dieser Principals repräsentiert Services, die unter dem Betriebssystem i5/OS implementiert sind. Bei der Konfiguration des Netzwerkauthentifizierungsservice wird für jeden erstellten Service-Principal ein Chiffrierschlüsseltabelleneintrag auf dem 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 Methoden, die zum Hinzufügen von i5/OS-Principals zum Kerberos-Server verwendet werden, richten 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 „i5/OS-Principals zum Kerberos-Server hinzufügen" auf Seite 105 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/*System i vollständig qualifizierter Domänenname@REALM-NAME* oder krbsvr400/*System i Hostname@REALM-NAME*. Ein gültiger Service-Principal für die i5/OS-Kerberos-Authentifizierung lautet beispielsweise krbsvr400/systema.myco.com@MYCO.COM oder krbsvr400/systema@MYCO.COM. i5/OS generiert den Principal auf der Basis des Hostnamens, der entweder auf dem DNS-Server oder auf der System i-Plattform festgestellt werden kann. Welcher Hostnamen verwendet wird, hängt von der Konfiguration der Hostnamenauflösung auf der System i-Plattform ab.

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

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

Anmerkung: In früheren Releases erstellte der Assistent für den Netzwerkauthentifizierungsservice einen Chiffrierschlüsseleintrag in Großschreibung 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-Principal-Namen 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 Tivoli Directory Server for i5/OS (LDAP).

HTTP-Server

Außer dem i5/OS-Service-Principal-Namen können während der Konfiguration des Netzwerkauthentifizierungsservice zusätzliche Service-Principals für den HTTP-Server (powered by Apache) konfiguriert werden. Der HTTP-Principal-Name lautet HTTP/*System i vollständig qualifizierter Domänenname@REALM-NAME*. Dieser Principal-Name bezeichnet die HTTP-Server-Instanzen auf der System i-Plattform, 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.

Auf der Homepage für die HTTP Server for i5/OS-Dokumentation finden Sie Informationen zur Verwendung der Kerberos-Authentifizierung für den HTTP-Server.

i5/OS NetServer

Für i5/OS NetServer können Sie außerdem mehrere NetServer-Principals erstellen, die automatisch der Chiffrierschlüsseldatei auf der System i-Plattform hinzugefügt werden. Jeder dieser NetServer-Principals repräsentiert alle potenziellen Clients, die Sie für die Verbindung mit NetServer verwenden können. Die folgende Tabelle enthält die NetServer-Principal-Namen und die entsprechenden Clients.

Tabelle 21. i5/OS NetServer-Principal-Namen

Clientverbindung	i5/OS NetServer-Principal-Name
Windows XP und Windows Vista	cifs/System i vollständig qualifizierter Domänenname cifs/System i Hostname cifs/QSystem i Hostname cifs/qSystem i Hostname cifs/IP-Adresse
Windows 2000	HOST/System i vollständig qualifizierter Domänenname HOST/System i Hostname HOST/QSystem i Hostname HOST/qSystem i Hostname HOST/IP-Adresse

Weitere Informationen über die Verwendung der Kerberos-Authentifizierung für diese Anwendung finden Sie unter i5/OS NetServer.

NFS-Server

Außer dem i5/OS-Service-Principal-Namen können Sie während der Konfiguration des Netzwerkauthentifizierungsservice einen NFS-Server (Network File System) konfigurieren. Der NFS-Principal-Name lautet nfs/*System i vollständig qualifizierter Domänenname@REALM-NAME*. Ein gültiger Principal-Name für den NFS-Server wäre beispielsweise nfs/systema.myco.com@MYCO.COM.

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?	Die i5/OS-Kerberos-Authentifizierung kann für die folgenden Services verwendet werden: 1. System i Access für Windows, System i Navigator, i5/OS NetServer und Telnet 2. HTTP-Server (powered by Apache) 3. LDAP 4. NFS-Server (Network File System)
Wie lauten die i5/OS-Principal-Namen für jeden dieser i5/OS-Services?	1. krbsvr400/systema.myco.com@MYCO.COM 2. HTTP/systema.myco.com@MYCO.COM 3. ldap/systema.myco.com@MYCO.COM 4. nfs/systema.myco.com/MYCO.COM

Hinweise zur Auflösung von Hostnamen

Um sicherzustellen, dass die Kerberos-Authentifizierung und die Hostnamenauflösung bei den Kerberos-fähigen Anwendungen fehlerfrei funktionieren, müssen Sie überprüfen, ob Ihre PCs und die System i-Plattformen für das System, auf dem sich die Serviceanwendung befindet, den gleichen Hostnamen auflösen.

In einer Kerberos-Umgebung verwenden sowohl der Client als auch der Server eine Form der Hostnamenauflösung, um den Hostnamen des Systems festzustellen, auf dem sich eine bestimmte Anwendung oder ein bestimmter Service befindet. Wenn die System i-Plattformen und die PCs einen DNS-Server

(DNS = Domain Name System) verwenden, ist zu beachten, dass sie denselben DNS-Server für die Hostnamenauflösung verwenden müssen; wenn sie mehr als einen DNS-Server verwenden, ist zu beachten, dass die Hostnamen auf beiden DNS-Servern übereinstimmen müssen. Wenn Ihre System i-Plattform oder Ihr 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 wurde. Dies kann zu einem Fehler im Netzwerkauthentifizierungsservice führen.

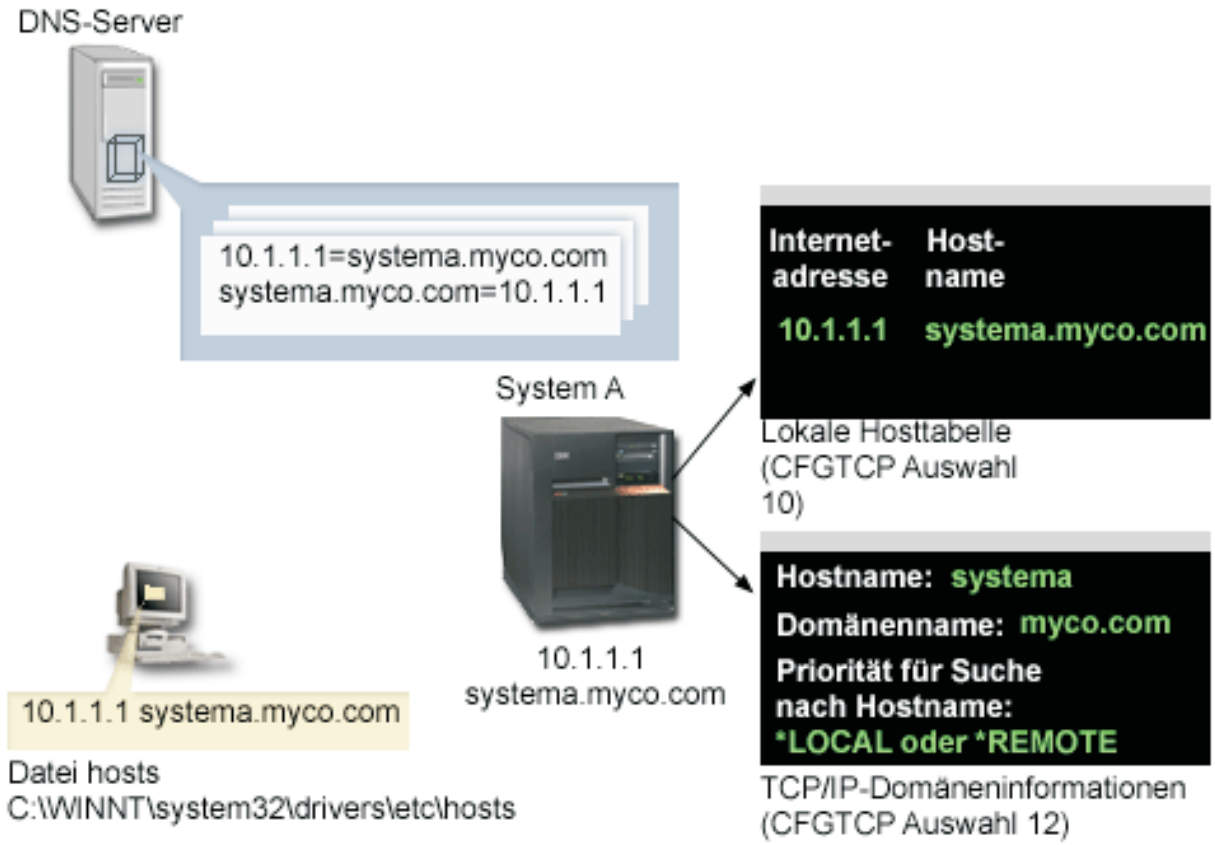
Um sicherzustellen, dass die Kerberos-Authentifizierung und die Hostnamenauflösung bei den Kerberos-fähigen Anwendungen fehlerfrei funktionieren, müssen Sie überprüfen, ob Ihre PCs und die System i-Plattformen für das System, auf dem sich die Serviceanwendung befindet, den gleichen Hostnamen auflösen. Im folgenden Beispiel wird dieses System als System A bezeichnet.

Die nachfolgenden Anweisungen zeigen, wie festgestellt wird, ob die PCs und System i-Plattformen denselben Namen für System A auflösen. Verwenden Sie zur Ausführung dieser Anweisungen die Beispielarbeitsblätter.

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 Hostnameninformationen 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 die IP-Adresse `10.1.1.1` mit dem Hostnamen `systema.myco.com` korreliert, der IP-Adresse und dem Hostnamen für System A.
- Kann vom PC, System 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. Ihr PC kann beispielsweise einen DNS-Server für die Auflösung von Hostnamen und Ihre System i-Plattform 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 `systema.myco.com` korreliert.

Anmerkung: Die Datei hosts befindet sich in den folgenden Ordnern:
- Betriebssystem Windows 2000: C:\WINNT\system32\drivers\etc\hosts
- Betriebssysteme Windows XP und Windows Vista: C:\WINDOWS\system32\drivers\etc\hosts

System A

- Arbeitet mit i5/OS V5R3.
- Enthält eine Serviceanwendung, auf die Sie unter Verwendung des Netzwerkauthentifizierungsservice (Kerberos-Authentifizierung) zugreifen müssen.
- Innerhalb des Menüs CFGTCP (TCP konfigurieren) liefern die Auswahlmöglichkeiten 10 und 12 die folgenden Informationen für System A:
  - Auswahl 10 (Mit TCP/IP-Hosttabelleneinträgen arbeiten):
    - **Internet-Adresse**: `10.1.1.1`
    - **Hostname**: `systema.myco.com`
  - Auswahl 12 (TCP/IP-Domäneninformationen ändern):
    - **Hostname**: `systema`
    - **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 Hostnamenauflösung auf dem System konfiguriert wurde.

Tabelle 23. Beispiel: Arbeitsblatt für die Hostnamenauflösung auf dem PC

Auf dem PC den Hostnamen für System A feststellen		
Schritt	**Quelle**	**Hostname**
1.a.1	PC-Datei hosts	systema.myco.com
1.b.1	DNS-Server	systema.myco.com

Tabelle 24. Beispiel: Arbeitsblatt für die Hostnamenauflösung für i5/OS

Auf System A den Hostnamen für System A feststellen		
Schritt	**Quelle**	**Hostname**
2.a.2	System A Menü CFGTCP, Auswahl 12	**Hostname**: `systema` **Domänenname**: `myco.com`
Anmerkung: Wert für *Priorität für Suche nach Hostname*: `*LOCAL` oder `*REMOTE`		
2.b.2	System A Menü CFGTCP, Auswahl 10	systema.myco.com
2.c.1	DNS-Server	systema.myco.com

Tabelle 25. Beispiel: Arbeitsblatt für übereinstimmende Hostnamen

Diese drei Hostnamen müssen exakt übereinstimmen	
Schritt	**Hostname**
Schritt 1	systema.myco.com
Schritt 2.a.2	systema myco.com
2d	systema.myco.com

Anhand der folgenden drei Arbeitsblätter können Sie überprüfen, ob Ihre PCs und System i-Plattformen für das System, auf dem die Serviceanwendung implementiert ist, den gleichen Hostnamen auflösen.

Tabelle 26. Arbeitsblatt für die Hostnamenauflösung auf dem PC

Auf dem PC den Hostnamen für die System i-Plattform feststellen		
Schritt	**Quelle**	**Hostname**
1.a.1	PC-Datei hosts	
1.b.1	DNS-Server	

Tabelle 27. Arbeitsblatt für die Hostnamenauflösung für i5/OS

Auf der System i-Plattform den Hostnamen für die System i-Plattform feststellen		
Schritt	**Quelle**	**Hostname**
2.a.2	System i Menü CFGTCP, Auswahl 12	**Hostname**: **Domänenname**:
Wert für *Priorität für Suche nach Hostname* beachten: `*LOCAL` oder `*REMOTE`		
2.b.2	System i Menü 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	

Hostnamen auflösen

Überprüfen Sie, ob auf Ihren PCs und auf Ihren System i-Plattformen die gleichen Hostnamen aufgelöst werden.

Verwenden Sie die zuvor dargestellten Beispielarbeitsblätter hierbei als Referenz. Führen Sie die folgenden Schritte durch, um sicherzustellen, dass die PCs und System i-Plattformen den gleichen Hostnamen für System A auflösen:

1. Stellen Sie auf dem PC den vollständig qualifizierten TCP/IP-Hostnamen für System 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.

      Notieren Sie den ersten Hostnamenseintrag für System A auf dem Arbeitsblatt; beachten Sie dabei die Groß-/Kleinschreibung, z. B. `systema.myco.com`.

      Anmerkung: Wenn die Datei hosts keinen Eintrag für System 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. (Die Datei `hosts` hat hierbei bei der Hostnamenauflösung für den PC durch das Betriebssystem Priorität gegenüber DNS-Servern.)

      1) Geben Sie bei einer Eingabeaufforderung `NSLOOKUP` ein, und drücken Sie die Eingabetaste. Geben Sie an der NSLOOKUP-Eingabeaufforderung `10.1.1.1` ein, um den DNS-Server für System A abzufragen. Notieren Sie den Hostnamen, der vom DNS-Server zurückgegeben wird, und beachten Sie hierbei die Groß-/Kleinschreibung, z. B. `systema.myco.com`.
      2) Geben Sie bei der NSLOOKUP-Eingabeaufforderung `systema.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, z. B. `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 System 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**: `systema`
         - **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 in der Spalte *Hostname* den Wert, der System A entspricht (IP-Adresse 10.1.1.1); beachten Sie dabei die Groß-/Kleinschreibung, z. B. `systema.myco.com`.

         Anmerkung: Wenn Sie in der Hosttabelle keinen Eintrag für System 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 an der NSLOOKUP-Eingabeaufforderung `10.1.1.1` ein, um den DNS-Server für System A abzufragen. Notieren Sie den Hostnamen, der vom DNS-Server zurückgegeben wird, und beachten Sie hierbei die Groß-/Kleinschreibung, z. B. `systema.myco.com`.
      2) Geben Sie bei der NSLOOKUP-Eingabeaufforderung `systema.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, z. B. `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 Hostnamenwert für System A, basierend auf seiner 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 System A enthält, dann verwenden Sie diesen Eintrag.
3. Vergleichen Sie die Ergebnisse der folgenden Schritte:
   a. Schritt 1: Der Name, den der PC für System A verwendet.

Anmerkung: Wenn Sie in der PC-Datei hosts einen Eintrag für System A finden, verwenden Sie diesen. Andernfalls verwenden Sie den Eintrag vom DNS-Server.

b. Schritt 2.a.2: Der Name, den System A selbst innerhalb seiner TCP/IP-Konfiguration aufruft.

c. Schritt 2d: Der Name, den System A selbst auf der Basis der Hostnamenauflösung 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, mit deren Hilfe Sie sich vergewissern können, dass alle erforderlichen Schritte durchgeführt wurden. 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 Konfigurations-Tasks beginnen.

Tabelle 29. Arbeitsblatt für Voraussetzungen

Fragen	Antworten
Ist auf Ihrem System i5/OS V5R3 oder eine spätere Version des Produkts (5722-SS1) oder V6R1 (5761-SS1) installiert?	
Wenn Sie i5/OS V5R3 verwenden: Ist Cryptographic Access Provider (5722-AC3) auf Ihren Systemen installiert? Wenn Sie i5/OS ab V5R4 verwenden: Ist Network Authentication Enablement (5722-NAE oder 5761-NAE) auf Ihren Systemen installiert?	
Ist System i Access für Windows (5722-XE1 oder 5761-XE1) auf dem PC des Administrators und auf Ihren Systemen installiert?	
Ist die Unterkomponente "Sicherheit" des System i Navigator auf dem PC des Administrators installiert?	
Ist die Unterkomponente "Netzwerk" des System i Navigator auf dem PC des Administrators installiert?	
Ist das aktuellste Service-Pack für IBM System i Access für Windows installiert? Sie können das aktuellste Service-Pack über die Website für System i Access abrufen.	
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? 1. Windows 2000 Server 2. Windows Server 2003 3. AIX Server 4. i5/OS PASE (ab V5R3) 5. z/OS	

Tabelle 29. Arbeitsblatt für Voraussetzungen (Forts.)

Fragen	Antworten
Für Windows 2000 Server und Windows Server 2003: Sind die Windows-Unterstützungstools (enthalten das Tool ktpass) auf dem System installiert, das als KDC (Key Distribution Center) verwendet wird?	
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 des System i-Systems und der Systemzeit des Kerberos-Servers maximal fünf Minuten? Ist die Abweichung größer, lesen Sie die Informationen unter „Systemzeiten synchronisieren" auf Seite 110.	

Tabelle 30. Planungsarbeitsblatt für Kerberos-Server

Fragen	Antworten
Unter welchem Betriebssystem soll der Kerberos-Server konfiguriert werden? • Windows 2000 Server • Windows Server 2003 • AIX Server • i5/OS PASE (ab V5R3) • z/OS	
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 Hostnamenauflösung

Frage	Antwort
Verwenden die PCs und die System i-Plattform denselben DNS-Server zur Auflösung von Hostnamen?	
Verwenden Sie zur Auflösung von Hostnamen auf der System i-Plattform eine lokale Hosttabelle?	
Lösen Ihr PC und Ihre System i-Plattform den gleichen Hostnamen für die System i-Plattform auf? Siehe „Hinweise zur Auflösung von Hostnamen" auf Seite 89.	

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 Voraussetzungen 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 Ihr System gehören soll? **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: Wie lautet der Name des Kennwortservers für diesen Kerberos-Server? Auf welchem Port ist der Kennwortserver empfangsbereit?	

Tabelle 35. Planungsarbeitsblatt für Netzwerkauthentifizierungsservice (Forts.)

Fragen	Antworten
Für welche Services sollen Chiffrierschlüsseleinträge erstellt werden? • i5/OS-Kerberos-Authentifizierung • LDAP • IBM HTTP-Server • i5/OS NetServer • NFS-Server	
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 i5/OS NetServer erstellen möchten: Wie lautet dessen Kennwort? **Anmerkung:** Wenn der Assistent für den Netzwerkauthentifizierungsservice angezeigt wird, werden mehrere Principals für i5/OS NetServer erstellt. Notieren Sie diese hier, sobald sie im Assistenten angezeigt werden. Die Namen dieser Principals werden benötigt, um sie dem Kerberos-Server hinzufügen zu können.	
Wenn Sie einen Service-Principal für den NFS-Server erstellen möchten: Wie lautet dessen Kennwort?	
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 System i-Produkt die Nutzung eines vorhandenen Kerberos-Netzwerks. Der Netzwerkauthentifizierungsservice setzt 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 die System i-Plattform auch mit dem Microsoft Windows 2000-, Windows 2003- sowie mit dem AIX-Server und mit z/OS. Machen Sie sich anhand der folgenden Informationen mit der Vorgehensweise zur Konfiguration eines Kerberos-Servers auf den einzelnen Plattformen vertraut:

- Windows 2000 Server
- z/OS Security Server Network Authentication Service Administration
- *IBM Network Authentication Service AIX, Linux, and Solaris Administrator's and User's Guide*

Anmerkung: Die genannten Dokumentationen 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" auf Seite 99
2. „Verschlüsselungswerte auf dem Kerberos-Server ändern" auf Seite 100

3. „Kerberos-Server stoppen und erneut starten” auf Seite 100
4. „Host-, Benutzer- und Service-Principals erstellen” auf Seite 100
5. „Windows 2000-, Windows XP- und Windows Vista-Workstations konfigurieren” auf Seite 101
6. „Sekundären Kerberos-Server konfigurieren” auf Seite 102

Netzwerkauthentifizierungsservice auf der System i-Plattform konfigurieren

1. „Netzwerkauthentifizierungsservice konfigurieren” auf Seite 104
2. „i5/OS-Principals zum Kerberos-Server hinzufügen” auf Seite 105
3. „Ausgangsverzeichnis erstellen” auf Seite 108
4. „Konfiguration des Netzwerkauthentifizierungsservice testen” auf Seite 108

Kerberos-Server in i5/OS PASE konfigurieren

Zur Bereitstellung einer integrierten Laufzeitumgebung für AIX-Anwendungen müssen Sie einen Kerberos-Server auf Ihrer System i-Plattform konfigurieren und verwalten.

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 über Ihre System i-Plattform konfigurieren und verwalten. Führen Sie die folgenden Schritte durch, 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 systema.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 und V5R4 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 so zu konfigurieren, dass der Kerberos-Server und der Verwaltungsserver während eines IPL automatisch gestartet werden.
   a. Erstellen Sie eine Jobbeschreibung.

      Geben Sie in einer i5/OS-Befehlszeile folgenden Befehl ein, wobei *xxxxxx* für das i5/OS-Benutzerprofil mit der Sonderberechtigung für alle Objekte (*ALLOBJ) steht:

      ```
      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)
      ```

   b. Fügen Sie einen Eintrag für den automatisch zu startenden Job hinzu. Geben Sie in der Befehlszeile folgenden Befehl ein:

      ```
      ADDAJE SBSD(QSYS/QSYSWRK) JOB(KRB5PASE) JOBD(QGPL/KRB5PASE).
      ```

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

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

Die weiteren Schritte

Wenn Sie Windows 2000-, Windows XP- oder Windows Vista-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

Für den Einsatz auf Windows-Workstations müssen die Standardverschlüsselungseinstellungen des Kerberos-Servers geändert werden, damit Clients auf dem i5/OS PASE-Kerberos-Server authentifiziert werden können.

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
arcfour-hmac:normal aes256-cts:normal
des-cbc-md5:normal des-cbc-crc:normal
```

in

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

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.

Host-, Benutzer- und Service-Principals erstellen

Im Folgenden wird die Vorgehensweise zur Erstellung von Host-Principals für Ihre Windows 2000-, Windows XP- und Windows Vista-Workstations und zur Erstellung von Benutzer- und Service-Principals auf Ihrem Kerberos-Server erläutert.

Damit eine Windows 2000-, Windows XP- oder Windows Vista-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 systema123 krbsvr400/systema.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.

Windows 2000-, Windows XP- und Windows Vista-Workstations konfigurieren

Um die Client-Workstations zu konfigurieren, müssen Sie den Kerberos-Realm und den Kerberos-Server definieren.

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 an 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.

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

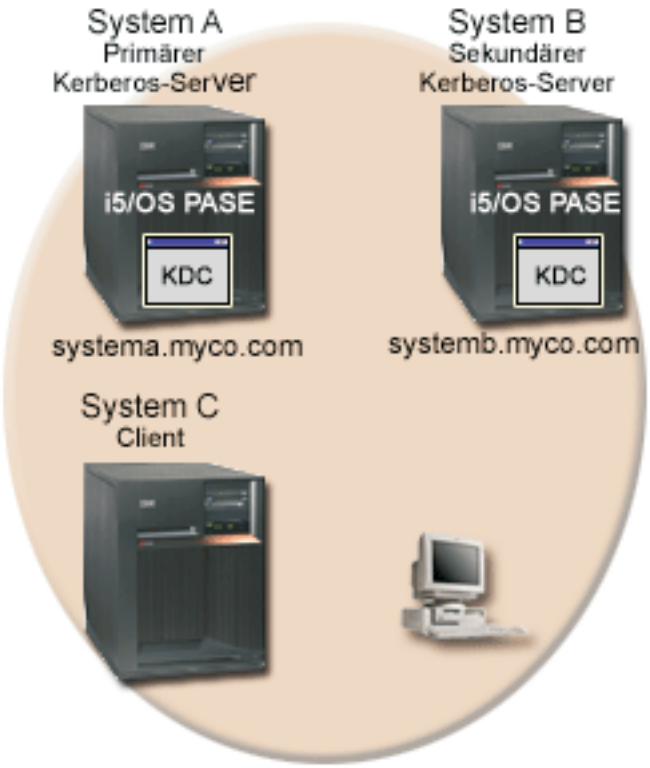
Sekundären Kerberos-Server konfigurieren

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 so stark ausgelastet ist, dass er nicht alle Anforderungen verarbeiten kann.

Beispiel: System A dient momentan als Kerberos-Server. Sie möchten jetzt das System B als sekundären Kerberos-Server (Sicherungsserver) konfigurieren.

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

Die folgende Abbildung zeigt die System i-Produkte, die in den nachfolgenden Anweisungen beschrieben werden.



Details

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

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

1. Konfigurieren Sie System B als Client.
   a. Geben Sie in einer zeichenorientierten Schnittstelle auf System 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 folgenden Befehl 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 -E -d rchland.ibm.com -r MYCO.COM -s lp16b1b.rchland.ibm.com
      ```
   d. Geben Sie das Administratorkennwort, z. B. `secret`, ein.

   Mit dem Befehl config.krb5 können Sie den Client sowie den primären und sekundären Server konfigurieren. Mit dem Attribut **-C** wird der Client auf System C konfiguriert, mit dem Attribut **-s** der primäre Kerberos-Server auf System A. Das Attribut **-E** dient zur Konfiguration des sekundären Kerberos-Servers auf System B.
2. Fügen Sie dem Kerberos-Server auf System A einen i5/OS-Principal für System A und B hinzu.
   a. Geben Sie in einer zeichenorientierten Schnittstelle auf System 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 folgenden Befehl ein:

      ```
      addprinc -randkey -clearpolicy host/systema.myco.com
      ```
   f. Geben Sie in der Befehlszeile folgenden Befehl ein:

      ```
      addprinc -randkey -clearpolicy host/systemb.myco.com
      ```
3. Geben Sie die Masterdatenbank vom primären an den sekundären Kerberos-Server weiter.
   a. Geben Sie in einer zeichenorientierten Schnittstelle auf System 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 folgenden Befehl 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:

      ```
      /usr/krb5/sbin/config.krb5 -P -r MYCO.COM -d rchland.ibm.com -e rchasrc2.rchland.ibm.com
      ```

      Tipp: Sie können den Befehl in der Nachricht, die auf dem primären Kerberos-System angezeigt wird, ausschneiden und einfügen.

Das Attribut **-P** dient zur Weitergabe der Masterdatenbank vom primären an den sekundären Kerberos-Server. Im Attribut **-r** wird der Realmname angegeben. Das Attribut **-d** dient zur Angabe des Namens der DNS-Domäne. Im Attribut **-e** wird der Hostname des sekundären Kerberos-Servers angegeben.

4. Prüfen Sie auf dem sekundären Kerberos-Server, ob die Masterdatenbank erfolgreich weitergegeben wurde.
   a. Geben Sie auf dem sekundären Kerberos-Server `Y` (Ja) ein, wenn Sie die folgende Systemanfrage erhalten: `Have you successfully run the above command?`
   b. Geben Sie das Masterkennwort der Datenbank, z. B. `pasepwd`, ein. Dieser Befehl dient zur Abnahme des Masterschlüssels.

Netzwerkauthentifizierungsservice konfigurieren

Im Folgenden erfahren Sie, welche Voraussetzungen zum Konfigurieren des Netzwerkauthentifizierungsservice auf Ihren System erfüllt werden müssen und welche Vorgehensweise zur Konfiguration angewendet werden kann.

Bevor Sie den Netzwerkauthentifizierungsservice konfigurieren, sollten Sie die folgenden Tasks ausführen:

- Füllen Sie alle erforderlichen Planungsarbeitsblätter aus.
- Wenn Ihre PCs und System i-Plattformen die Hostnamenauflösung durchführen, müssen Sie sich vergewissern, dass für Ihre System i-Produkte die gleichen Hostnamen aufgelöst werden. Weitere Informationen zu dieser Task finden Sie unter „Hinweise zur Auflösung von Hostnamen" auf Seite 89.
- 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 der System i-Plattform konfigurieren. Einzelheiten zur Konfiguration eines Kerberos-Servers in i5/OS PASE finden Sie in „Kerberos-Server in i5/OS PASE konfigurieren" auf Seite 99.

  Sie können einen Kerberos-Server auch unter Microsoft Windows 2000, Windows Server 2003 sowie unter 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 System i-Plattform zu konfigurieren.

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

1. Erweitern Sie im System i Navigator den Eintrag für *Ihr System* → **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 Auswahl **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 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' im Feld **KDC** den Namen des Kerberos-Servers für diesen Realm und im Feld **Port** den Wert 88 ein. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite 'Kennwortserverinformationen angeben' für die Definition eines Kennwortservers entweder **Ja** oder **Nein** aus. Mit dem Kennwortserver können Principals Kennwör-

ter 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' **i5/OS-Kerberos-Authentifizierung** aus. Sie können außerdem Chiffrierschlüsseleinträge für den Directory-Server (LDAP), i5/OS NetServer, den HTTP-Server und den NFS-Server (Network File System) 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 auf der Seite 'Stapeldatei erstellen' **Ja** 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 im Feld **Kennwort einfügen** die Einstellung **Ja** 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.

    Anmerkung: Sie können dem Microsoft Active Directory auch manuell die vom Assistenten generierten Service-Principals hinzufügen. Unter „i5/OS-Principals zum Kerberos-Server hinzufügen" wird erläutert, wie i5/OS-Service-Principals manuell zum Microsoft Active Directory hinzugefügt werden können.
12. Auf der Seite 'Zusammenfassung' können Sie die Details zur Konfiguration des Netzwerkauthentifizierungsservice überprüfen. Klicken Sie auf **Fertig stellen**.

Der Netzwerkauthentifizierungsservice ist jetzt konfiguriert.

Zugehörige Konzepte

„Netzwerkauthentifizierungsservice verwalten" auf Seite 109
Nachdem Sie den Netzwerkauthentifizierungsservice konfiguriert haben, können Sie Tickets anfordern, mit Chiffrierschlüsseldateien arbeiten und die Hostnamenauflösung verwalten. Sie können außerdem mit Dateien für Berechtigungsnachweise arbeiten und Konfigurationsdateien sichern.

i5/OS-Principals zum Kerberos-Server hinzufügen

Nachdem Sie den Netzwerkauthentifizierungsservice auf Ihrer System i-Plattform konfiguriert haben, müssen Sie Ihre i5/OS-Principals zum Kerberos-Server hinzufügen.

Der Netzwerkauthentifizierungsservice stellt den i5/OS-Principal-Namen **krbsvr400** für das System und die i5/OS-Anwendungen zur Verfügung. Der Name des Principals, der i5/OS repräsentiert, lautet krbsrv400/*System i Hostname@REALM-NAME*, wobei *System i Hostname* entweder der vollständig qualifizierte Hostname oder die Kurzform des Hostnamens für die System i-Plattform ist. Dieser Principal-Name muss dem Kerberos-Server hinzugefügt werden, damit Kerberos-Clientanwendungen Service-Tickets anfordern und empfangen können. In den Konfigurationsszenarios hat beispielsweise der Administrator für MyCo den Service-Principal krbsvr400/systema.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 in einer Windows 2000-Domäne. Wenn wahlweise außerdem Service-Principals für IBM Directory Server for i5/OS (LDAP), i5/OS NetServer und den NFS-Server (Network File System) oder den HTTP-Server erstellt wurden, müssen auch diese dem Kerberos-Server hinzugefügt werden.

1. 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:
   a. Geben Sie in einer zeichenorientierten Schnittstelle call QP2TERM ein.
   b. 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.
   c. Geben Sie in der Befehlszeile `kadmin -p admin/admin` ein.
   d. Melden Sie sich mit Ihrem Benutzernamen und Kennwort an.
   e. Geben Sie in der kadmin-Befehlszeile `addprinc -pw secret krbsvr400/System i vollständig qualifizierter Hostname@REALM` ein, wobei `secret` das Kennwort für den i5/OS-Service-Principal ist. Hierbei kann `krbsvr400/systema.myco.com@MYCO.COM` z. B. ein gültiger Name für einen i5/OS-Service-Principal sein.
2. Microsoft 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 des Netzwerkauthentifizierungsservice generierte Stapeldatei verwenden

   a. 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.
   b. 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.
   c. Geben Sie bei der FTP-Eingabeaufforderung `binary` ein. Das bedeutet, dass es sich bei der zu übertragenden Datei um eine Binärdatei handelt.
   d. 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.
   e. Geben Sie bei der FTP-Eingabeaufforderung `put NASConfig.bat` ein. Daraufhin sollte die Nachricht: `226 Übertragung abgeschlossen` (oder ähnlicher Wortlaut) angezeigt werden.
   f. Öffnen Sie auf dem Windows 2000-Server das Verzeichnis, in das die Stapeldatei übertragen wurde.
   g. Lokalisieren Sie die Datei `NASConfig.bat`, und führen Sie sie durch Doppelklicken aus.

h. Überprüfen Sie im Anschluss, ob der i5/OS-Principal-Name dem Microsoft Active Directory hinzugefügt wurde. Führen Sie dazu die folgenden Schritte durch:
   1) Erweitern Sie auf dem Windows 2000-Server **Start** → **Programme** → **Verwaltungstools** → **Active Directory-Benutzer und -Computer** → **Benutzer**.
   2) Vergewissern Sie sich, dass die System i-Plattform 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.
   3) Suchen Sie aus der angezeigten Benutzerliste den Namen heraus, der dem soeben hinzugefügten Service-Principal entspricht.
   4) Rufen Sie die Eigenschaften der Active Directory-Benutzer auf. Wählen Sie auf der Indexzunge **Konto** die Auswahl **Konto wird für Delegierungszwecke vertraut** aus.

      Anmerkung: Dieser optionale Schritt ermöglicht es 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 Active Directory hinzufügen Sie können dem Microsoft 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.

a. Erweitern Sie auf dem Windows 2000-Server **Start** → **Programme** → **Verwaltungstools** → **Active Directory-Benutzer und -Computer**.
b. Wählen Sie die Windows 2000-Domäne aus, zu der Sie das i5/OS-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.
c. Geben Sie im Feld **Name** einen Namen ein, der die System i-Plattform für diese Windows 2000-Domäne identifiziert. Damit wird ein neues Benutzerkonto für die System i-Plattform hinzugefügt. Sie könnten beispielsweise den Namen `krbsvr400systema` oder `httpsystema` als gültiges Benutzerkonto eingeben.
d. Greifen Sie auf die Eigenschaften des Active Directory-Benutzers zu, den Sie in Schritt 3 erstellt haben. Wählen Sie auf der Indexzunge **Konto** die Auswahl **Konto wird für Delegierungszwecke vertraut** aus. Damit wird dem i5/OS-Service-Principal der Zugriff auf andere Services im Namen eines angemeldeten Benutzers gestattet.
e. 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 2000 Server. Führen Sie folgende Task durch, um das Benutzerkonto zuzuordnen:
   1) Geben Sie bei einer Eingabeaufforderung Folgendes ein:

      ```
      ktpass -mapuser krbsvr400systema -pass secret -princ krbsvr400/system-domain-name@REALM
          -mapop set
      ```

      Anmerkung: In diesem Befehl steht `krbsvr400systema` für den Namen des Benutzerkontos, das in Schritt 3 erstellt wurde, und `secret` für das Kennwort, das Sie bei der Konfiguration des Netzwerkauthentifizierungsservice für den i5/OS-Principal eingegeben haben.

Zugehörige Konzepte

„Fehler beim Netzwerkauthentifizierungsservice beheben" auf Seite 131
Die vorliegenden Informationen zur Fehlerbehebung enthalten Angaben zu gelegentlich auftretenden Problemen, die den Netzwerkauthentifizierungsservice, Enterprise Identity Mapping (EIM) und die von IBM gelieferten Anwendungen betreffen, die die Kerberos-Authentifizierung unterstützen.

Ausgangsverzeichnis erstellen

Nachdem Sie den i5/OS-Principal zum Kerberos-Server hinzugefügt haben, müssen Sie ein Ausgangsverzeichnis (`/home`) für jeden Benutzer erstellen, der eine Verbindung zu den verfügbaren i5/OS-Anwendungen herstellt.

Dieses Verzeichnis enthält den Namen des Kerberos-Cache für Berechtigungsnachweise, der dem Benutzer zugeordnet ist. Jeder Benutzer sollte entweder Eigner dieses Verzeichnisses sein oder über die entsprechende Berechtigung zum Erstellen von Dateien in diesen Verzeichnis verfügen.

Führen Sie den folgenden Schritt durch, um ein Ausgangsverzeichnis für einen Benutzer zu erstellen:

1. 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.

Konfiguration des Netzwerkauthentifizierungsservice testen

Zum Testen der Konfiguration des Netzwerkauthentifizierungsservice müssen Sie ein Ticket-granting Ticket für Ihren i5/OS-Principal anfordern.

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 unter dem Betriebssystem i5/OS ein Ausgangsverzeichnis für den Benutzer vorhanden, der das Ticket anfordert? Einzelheiten hierzu finden Sie unter „Ausgangsverzeichnis erstellen".
- 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 „i5/OS-Principals zum Kerberos-Server hinzufügen" auf Seite 105.

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/systema.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/systema.myco.com@MYCO.COM ist beispielsweise ein gültiger Principal-Name für das System. Mit diesem Befehl wird geprüft, ob Ihr System richtig konfiguriert wurde und das Kennwort in der Chiffrierschlüsseldatei mit dem auf dem Kerberos-Server gespeicherten Kennwort übereinstimmt. Wenn die Prüfung erfolgreich verläuft, dann werden für den Befehl QSH keine Fehler ausgegeben.

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-Caches für Berechtigungsnachweise angezeigt und geprüft, ob ein gültiges Ticket für den i5/OS-Service-Principal erstellt und in den Cache für Berechtigungsnachweise auf dem System aufgenommen wurde.

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

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

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

Die weiteren Schritte

Enterprise Identity Mapping konfigurieren

Diese Task ist optional, wenn Sie den Netzwerkauthentifizierungsservice für Ihre eigenen Anwendungen verwenden. Die Ausführung dieser Task wird jedoch empfohlen, wenn Sie von IBM gelieferte Anwendungen benutzen, um eine Einzelanmeldungsumgebung zu erstellen.

Netzwerkauthentifizierungsservice verwalten

Nachdem Sie den Netzwerkauthentifizierungsservice konfiguriert haben, können Sie Tickets anfordern, mit Chiffrierschlüsseldateien arbeiten und die Hostnamenauflösung verwalten. Sie können außerdem mit Dateien für Berechtigungsnachweise arbeiten und Konfigurationsdateien sichern.

System i-Benutzer-Tasks

Die System i-Plattform kann auch als Client in einem Kerberos-fähigen Netzwerk fungieren. Benutzer können sich beim System anmelden und Kerberos-bezogene Tasks über den Qshell Interpreter ausführen. Für die folgenden allgemeinen Tasks, die von Benutzern ausgeführt werden können, werden mehrere Qshell-Befehle verwendet.

- „Ausgangsverzeichnis erstellen” auf Seite 108
- „Ticket-granting Tickets anfordern oder verlängern” auf Seite 113
- „Kerberos-Kennwörter ändern” auf Seite 121
- „Chiffrierschlüsseldateien verwalten” auf Seite 118
- „Verfallene Cachedateien für Berechtigungsnachweise löschen” auf Seite 122
- „Cache für Berechtigungsnachweise anzeigen” auf Seite 116
- „Kerberos-Service-Einträge in LDAP-Verzeichnissen verwalten” auf Seite 125

Anmerkung: Wenn Sie den PC5250-Emulator im System i 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 System i Navigator den Eintrag für ***Ihr System*** → **Konfiguration und Service** → **Systemwerte** → **Anmelden**.
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**.

Verwaltungs-Tasks für den Netzwerkauthentifizierungsservice

Im Folgenden sind die Tasks aufgeführt, die von einem Administrator im System i Navigator ausgeführt werden können. Weitere task-bezogene Informationen finden Sie im System i Navigator-Hilfetext zum Netzwerkauthentifizierungsservice.

Zugehörige Tasks

„Netzwerkauthentifizierungsservice konfigurieren" auf Seite 104
Im Folgenden erfahren Sie, welche Voraussetzungen zum Konfigurieren des Netzwerkauthentifizierungsservice auf Ihren System erfüllt werden müssen und welche Vorgehensweise zur Konfiguration angewendet werden kann.

Systemzeiten synchronisieren

Der Standardwert für die maximal zulässige Differenz zwischen zwei Systemzeiten beträgt im Netzwerkauthentifizierungsservice 5 Minuten (300 Sekunden). Die Differenz kann über die Eigenschaften des Netzwerkauthentifizierungsservice geändert werden.

Bevor Sie die Systemzeiten synchronisieren, stellen Sie die Systemzeit mit Hilfe des Systemwerts QTIMZON Ihrer Zeitzone entsprechend ein. Sie können diese Systemzeiten synchronisieren, indem Sie die auf dem Kerberos-Server eingestellte Uhrzeit ändern oder die System i-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. Mit Hilfe von SNTP können mehrere Systeme ihre Uhrzeit nach einem einzigen Zeitserver ausrichten.

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

- Um SNTP auf einer System i-Plattform zu konfigurieren, geben Sie in einer Befehlszeile `CHGNTPA` ein.
- Um auf Windows-Systemen SNTP zu konfigurieren, zeigen Sie die Konfigurationsdaten für einen SNTP-Server mit **NET HELP TIME** an.

Zugehörige Konzepte

Simple Network Time Protocol

Realms hinzufügen

Bevor Sie der i5/OS-Konfiguration einen Realm hinzufügen können, muss der Kerberos-Server für den neuen Realm konfiguriert werden. Um der Task für den i5/OS-Netzwerkauthentifizierungsservice einen Realm hinzuzufügen, 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. Erweitern Sie im System i Navigator den Eintrag für *Ihr System* → **Sicherheit** → **Netzwerkauthentifizierungsservice**.
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 eines nicht mehr benötigten Realms aus der Konfiguration des Netzwerkauthentifizierungsservice. Es kann auch vorkommen, dass ein Standard-Realm entfernt werden muss, um den Systembetrieb nach einem Fehler in einer Anwendung, die auf dem System integriert ist, 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 System i Navigator den Eintrag für *Ihr System* → **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

Ein Kerberos-Server kann mit Hilfe des Netzwerkauthentifizierungsservice zu einem Realm hinzugefügt werden. 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 ein KDC (Key Distribution Center - Instanz zur Schlüsselverteilung) hinzuzufügen:

1. Erweitern Sie im System i Navigator den Eintrag für *Ihr System* → **Sicherheit** → **Netzwerkauthentifizierungsservice** → **Realms**.
2. Klicken Sie mit der rechten Maustaste im rechten Fensterbereich auf den Namen des Realms, 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

Mit Hilfe des Kennwortservers können Kerberos-Principals ihr Kennwort ändern.

Derzeit wird die optionale Konfiguration eines Kennwortservers von i5/OS PASE nicht 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 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 System i Navigator den Eintrag für *Ihr System* → **Sicherheit** → **Netzwerkauthentifizierungsservice** → **Realms**.
2. Klicken Sie mit der rechten Maustaste im rechten Fensterbereich auf den Namen des Realms, 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**.

Zugehörige Verweise

„kpasswd" auf Seite 122

Mit dem Qshell-Befehl kpasswd wird das Kennwort für einen Kerberos-Principal geändert.

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 System i Navigator den Eintrag für *Ihr System* → **Sicherheit** → **Netzwerkauthentifizierungsservice** → **Realm**.
2. Klicken Sie mit der rechten Maustaste im rechten Fensterbereich auf den Namen des Realms, 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

Geben Sie zur Auflösung von Hostnamen und Realm-Namen einen LDAP-Server, ein DNS (Domain Name System) und statische Zuordnungen an.

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 Hostnamenauflösung zu ändern:

1. Erweitern Sie im System i Navigator den Eintrag für *Ihr System* → **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 Sie zur Auflösung von Hostnamen einen LDAP-Server verwenden wollen, müssen Sie überprüfen, ob der Realm auf dem LDAP-Server korrekt definiert wurde. Weitere Informationen hierzu finden Sie in „Realms im LDAP-Server definieren" auf Seite 128.
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 Sie zur

Auflösung von Hostnamen einen DNS-Server verwenden wollen, müssen Sie überprüfen, ob der Realm im DNS korrekt definiert wurde. Weitere Informationen hierzu finden Sie in „Realms in der DNS-Datenbank definieren" auf Seite 127.

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 Standardverschlüsselungswerte für TGT und TGS lauten des-cbc-crc bzw. des-cbc-md5. Die Standardwerte für die Verschlüsselung werden bei der Konfiguration festgelegt. Sie können der Konfiguration andere Werte für Tickets hinzufügen, indem Sie die folgenden Schritte durchführen:

1. Erweitern Sie im System i Navigator den Eintrag für *Ihr System* → **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 Verschlüsselungsarten für das Ticket-granting Ticket oder den 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. Sie können
| zum Anfordern und Zwischenspeichern von Ticket-granting Tickets auch den CL-Befehl ADDKRBTKT
| (Kerberos-Ticket hinzufügen) verwenden.

Befehl kinit

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 einen der folgenden Schritte durch, um ein Ticket-granting Ticket mit einer Laufzeit von 5 Stunden für den Principal jday anzufordern:

- Geben Sie in der Qshell-Befehlszeile `kinit -l 5h Jday` ein.
- Geben Sie in einer CL-Befehlszeile (CL = Control Language; Steuersprache) von i5/OS `call qsys/qkrbkinit parm('-l' '5h' 'jday')` ein.

Die Hinweise zur Verwendung von **kinit** für diesen Qshell-Befehl enthalten weitere Informationen zur Syntax und zu den geltenden Einschränkungen.

Befehl ADDKRBTKT (Kerberos-Ticket hinzufügen)

Sie können in der Befehlszeile von i5/OS den CL-Befehl ADDKRBTKT eingeben, um Ticket-granting Tickets anzufordern. Um beispielsweise ein weiterleitbares Ticket mit dem Principal krbsrv400/jday.myco.com und dem Standard-Realm hinzuzufügen, müssen Sie folgenden Befehl eingeben:

```
ADDKRBTKT PRINCIPAL('krbsrv400/jday.myco.com') PASSWORD('mypwd') ALWFWD(*YES)
```

Zugehörige Verweise

Befehl ADDKRBTKT (Kerberos-Ticket hinzufügen)

kinit

Mit dem Qshell-Befehl kinit wird ein Kerberos-Ticket-granting Ticket angefordert oder erneuert.

Syntax

```
kinit [-r Zeit] [-R] [-p] [-f] [-A] [-l Zeit] [-c Cache] [-k] [-t Chiffrierschlüssel]
[Principal]
```

Standardwert für allgemeine Berechtigung: *USE

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 Caches 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 Chiffrierschlüsseltabelle entnommen. Wird diese Option nicht angegeben, werden Sie vom System zur Eingabe des Kennworts für den Ticket-Principal aufgefordert.

-t Chiffrierschlüssel
Der Name der Chiffrierschlüsseltabelle. 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
Parent-Verzeichnis 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 Parent-Verzeichnis.

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″ 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. Sie
| können zum Anzeigen der Einträge im lokalen Cache für Berechtigungsnachweise auch den CL-Befehl
| DSPKRBCCF (Kerberos-Cachedatei für Berechtigungsnachweise anzeigen) verwenden.

Befehl klist

Führen Sie einen der folgenden Schritte durch, um alle Einträge im Standardcache für Berechtigungsnachweise aufzulisten und die Ticketmarkierungen anzuzeigen:

- Geben Sie in einer Qshell-Befehlszeile `klist -f -a` ein.
- Geben Sie in einer CL-Befehlszeile (CL = Control Language; Steuersprache) von i5/OS `call qsys/qkrbklist parm('-f' '-a')` ein.

Die Hinweise zur Verwendung von **klist** für diesen Qshell-Befehl enthalten weitere Informationen zur Syntax und zu den geltenden Einschränkungen.

| Befehl DSPKRBCCF (Kerberos-Cachedatei für Berechtigungsnachweise anzeigen)

| In einer CL-Befehlszeile von i5/OS können Sie auch den Befehl DSPKRBCCF (Kerberos-Cachedatei für
| Berechtigungsnachweise anzeigen) verwenden, um den Cache für Berechtigungsnachweise anzuzeigen.
| Um beispielsweise die Datei für den Standardcache für Berechtigungsnachweise anzuzeigen, müssen Sie
| den folgenden Befehl eingeben:

```
| DSPKRBCCF CCF(*DFT) OUTPUT(*)
```

Zugehörige Verweise

Befehl DSPKRBCCF (Kerberos-Cachedatei für Berechtigungsnachweise anzeigen)

klist

Mit dem Befehl klist wird der Inhalt eines Kerberos-Cache für Berechtigungsnachweise oder einer Chiffrierschlüsseldatei angezeigt.

Syntax

klist [-a] [-e] [-c] [-f] [-s] [-k] [-t] [-K] [Dateiname]

Standardwert für allgemeine Berechtigung: *USE

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 Caches für Berechtigungsnachweise aufgelistet wird.

-e Die Verschlüsselungsart für den Sitzungsschlüssel und das Ticket anzeigen. Diese Option ist nur gültig, wenn der Inhalt eines Caches 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 Caches 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 Caches 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 Chiffrierschlüsseltabelleneintrag anzeigen. Diese Option ist nur gültig, wenn der Inhalt einer Chiffrierschlüsseltabelle aufgelistet wird.

Dateiname
Gibt den Namen des Caches 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 Parent-Verzeichnis.

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 dekodiert werden.
- Keine Standardchiffrierschlüsseltabelle gefunden.
- Chiffrierschlüsseltabelle `Dateiname` kann nicht aufgelöst werden.

Unter "Cache für Berechtigungsnachweise anzeigen" finden Sie ein Beispiel für die Verwendungsweise dieses Befehls.

Chiffrierschlüsseldateien verwalten

Die Chiffrierschlüsseldatei kann entweder über die zeichenorientierte Schnittstelle oder mit dem System i Navigator verwaltet werden.

Als Netzwerkadministrator sind Sie für die Verwaltung der Chiffrierschlüsseldatei, die auch als Chiffrierschlüsseltabelle bezeichnet wird, und ihres Inhalts unter dem Betriebssystem i5/OS verantwortlich. Zur Verwaltung der Chiffrierschlüsseldatei und der zugehörigen Einträge können Sie entweder die zeichenorientierte Schnittstelle oder den System i Navigator verwenden.

Chiffrierschlüsseldateien mit der zeichenorientierten Schnittstelle verwalten

- Mit dem Befehl keytab werden Schlüssel zu einer Chiffrierschlüsseltabelle hinzugefügt, aus dieser gelöscht oder in dieser aufgelistet. Führen Sie einen der folgenden Schritte durch, um beispielsweise einen Schlüssel für den Service-Principal krbsvr400 auf dem Host kdc1.myco.com im Realm MYCO-.COM hinzuzufügen:
  - Geben Sie in einer Qshell-Befehlszeile `keytab add krbsvr400/kdc1.myco.com@MYCO.COM` ein.

– Geben Sie in einer CL-Befehlszeile (CL = Control Language; Steuersprache) von i5/OS `call qsys/qkrbkeytab parm('add' 'krbsvr400/kdc1.myco.com@MYCO.COM')` ein.

Sie werden aufgefordert, das Kennwort einzugeben, das verwendet wurde, als der Service für den Kerberos-Server definiert wurde.

Die Hinweise zur Verwendung von **keytab** für diesen Qshell-Befehl enthalten weitere Informationen zur Syntax und zu den geltenden Einschränkungen.

- In der CL-Befehlszeile können Sie auch die Befehle ADDKRBKTE (Kerberos-Schlüsseleintrag hinzufügen), DSPKRBKTE (Schlüsseleinträge anzeigen) und RMVKRBKTE (Kerberos-Schlüsseleintrag entfernen) verwenden, um die Chiffrierschlüsseldateien zu verwalten.

Chiffrierschlüsseldateien mit dem System i Navigator verwalten

Sie können auch den System i Navigator verwenden, um der Chiffrierschlüsseltabelle Chiffrierschlüsseleinträge hinzuzufügen. Mit Hilfe des System i Navigator können Sie Chiffrierschlüsseleinträge für die folgenden Services hinzufügen:

- i5/OS-Kerberos-Authentifizierung
- LDAP
- IBM HTTP-Server
- i5/OS NetServer
- NFS-Server

Führen Sie die folgenden Schritte durch, um der Chiffrierschlüsseldatei einen Chiffrierschlüsseleintrag hinzuzufügen:

1. Erweitern Sie im System i Navigator den Eintrag für ***Ihr System*** → **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, beispielsweise für die 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, i5/OS NetServer oder NFS-Server 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.

Zugehörige Verweise

Befehl ADDKRBKTE (Kerberos-Schlüsseleintrag hinzufügen)

Befehl DSPKRBKTE (Schlüsseleinträge anzeigen)

Befehl RMVKRBKTE (Kerberos-Schlüsseleintrag entfernen)

keytab

Mit dem Qshell-Befehl keytab wird eine Chiffrierschlüsseltabelle verwaltet.

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

Optionen

-k Der Name der Chiffrierschlüsseltabelle. Wird diese Option nicht angegeben, wird die Standardchiffrierschlüsseltabelle verwendet.

-p Das Kennwort angeben. Wird diese Option nicht angegeben, werden die Benutzer zur Eingabe des Kennworts aufgefordert, wenn sie der Chiffrierschlüsseltabelle 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 Chiffrierschlüsseltabelle nicht angegeben, werden alle Principals angezeigt.

Berechtigungen

Referenzobjekt	Erforderliche Berechtigung
Jedes Verzeichnis im Pfadnamen, das der zu öffnenden Ziel-Chiffrierschlüsseldatei vorangeht	*X
Parent-Verzeichnis 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" finden Sie ein Beispiel für die Verwendungsweise dieses Befehls.

Kerberos-Kennwörter ändern

Mit dem Befehl kpasswd wird das Kennwort für den angegebenen Kerberos-Principal mit Hilfe des Kennwortänderungsservice geändert. Sie können zum Ändern der Kerberos-Kennwörter auch den CL-Befehl CHGKRBPWD (Kerberos-Kennwort ändern) verwenden.

Befehl kpasswd

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, das 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 `kpasswd` ein.
- Geben Sie in einer Befehlszeile `call qsys/qkrbkpsswd` ein.

Führen Sie die folgenden Schritte durch, um das Kennwort für einen anderen Principal zu ändern:

- Geben Sie in einer Qshell-Befehlszeile `kpasswd jday@myco.com` ein.

Führen Sie die folgenden Schritte durch, um in i5/OS PASE das Kennwort für einen anderen Principal zu ändern:

In der zeichenorientierten Schnittstelle:

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.

In einer Befehlszeile:

Geben Sie in einer Befehlszeile `call qsys/qkrbkpsswd parm ('jday@myco.com')` ein.

Weitere Informationen zur Benutzung dieses Befehls finden Sie unter den Hinweisen zur Verwendung für den Befehl **passwd**.

Befehl CHGKRBPWD (Kerberos-Kennwort ändern)

In einer Befehlszeile von i5/OS können Sie auch den Befehl CHGKRBPWD (Kerberos-Kennwort ändern) verwenden, um Kerberos-Kennwörter zu ändern. Für den Kerberos-Principal jday im Realm myco.com können Sie beispielsweise den folgenden Befehl eingeben, um das Kennwort von ″myoldpwd″ in ″mynewpwd″ zu ändern:

```
CHGKRBPWD PRINCIPAL('jday' myco.com) CURPWD('myoldpwd') NEWPWD('mynewpwd') VFYPWD('mynewpwd')
```

Zugehörige Verweise

Befehl CHGKRBPWD (Kerberos-Kennwort ändern)

kpasswd

Mit dem Qshell-Befehl kpasswd wird das Kennwort für einen Kerberos-Principal geändert.

Syntax

```
kpasswd [-A ] [Principal]
```

Standardwert für allgemeine Berechtigung: *USE

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″ 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. Sie können zum Löschen des Caches für Berechtigungsnachweise auch den CL-Befehl DLTKRBCCF (Kerberos-Cachedatei für Berechtigungsnachweise löschen) verwenden. Alte Berechtigungsnachweise müssen von den Benutzern regelmäßig gelöscht werden.

Befehl kdestroy

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 Erreichen des Werts für das *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.

1. Gehen Sie wie folgt vor, um den Standardcache für Berechtigungsnachweise zu löschen:
   - Geben Sie in einer Qshell-Befehlszeile `kdestroy` ein.
   - Geben Sie in einer CL-Befehlszeile (CL = Control Language; Steuersprache) von i5/OS den Befehl `call qsys/qkrbkdstry` ein.
2. 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 `kdestroy -e 1d` ein.
   - Geben Sie in einer CL-Befehlszeile `call qsys/qkrbkdstry parm ('-e' '1d')` ein.

Die Hinweise zur Verwendung von **kdestroy** für diesen Qshell-Befehl enthalten weitere Informationen zur Syntax und zu den geltenden Einschränkungen.

Befehl DLTKRBCCF (Kerberos-Cachedatei für Berechtigungsnachweise löschen)

Sie können in der Befehlszeile von i5/OS den Befehl DLTKRBCCF eingeben, um den Cache für Berechtigungsnachweise zu löschen.

Geben Sie `DLTKRBCCF CCF(*DFT)` ein, um den Standardcache für Berechtigungsnachweise zu löschen.

Um alle Dateien des Caches für Berechtigungsnachweise zu löschen, deren abgelaufene Tickets älter als 1 Tag sind, müssen Sie `DLTKRBCCF CCF(*EXPIRED) EXPTIME(1440)` eingeben.

Zugehörige Verweise

Befehl DLTKRBCCF (Kerberos-Cachedatei für Berechtigungsnachweise löschen)

kdestroy

Mit dem Qshell-Befehl kdestroy wird ein Kerberos-Cache für Berechtigungsnachweise gelöscht.

Syntax

```
kdestroy [-c Cachename] [-e Zeitdelta]
```

Standardwert für allgemeine Berechtigung: *USE

Optionen

-c Cachename
Der Name des Caches 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 Cachedateien für Berechtigungsnachweise, die abgelaufene Tickets enthalten, werden gelöscht, sofern das Verfallsdatum der Tickets mindestens so lange zurückliegt wie der Wert für `Zeitdelta`.

Berechtigungen

Wenn der Typ des Caches für Berechtigungsnachweise **FILE** lautet (**krb5_cc_resolve()** enthält weitere 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
Parent-Verzeichnis des Caches 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 System i-Plattform verwenden möchte, muss ein Ausgangsverzeichnis definiert sein. Als Ausgangsverzeichnis wird standardmäßig /home/ verwendet. Mit Hilfe 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″ 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.

Zweck

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 auf dem 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 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.

Einschränkung: System i-Produkte unterstützen LDAP-Clients über die zeichenorientierte Schnittstelle. In i5/OS PASE wird diese Unterstützung jedoch nicht angeboten.

Beispiele

| Führen Sie die folgenden Schritte durch, um den Host kdc1.myco.com als Kerberos-Server für den Realm
| MYCO.COM zum Server ldapserv.myco.com hinzuzufügen. Dabei verwenden Sie die Directory-Server-
| Administrator-ID (LDAP) ″Administrator″ und das Kennwort ″verysecret″:

Geben Sie in einer Qshell-Befehlszeile Folgendes ein: `ksetup -h ldapserv.myco.com -n CN=Administrator -p verysecret`

Oder

1. Geben Sie in einer CL-Befehlszeile (CL = Control Language; Steuersprache) von i5/OS Folgendes ein:

```
call qsys/qkrbksetup parm('-h' 'ldapserv.myco.com' '-n' 'CN=Administrator' '-p' 'verysecret')
```

2. Wenn die Verbindung zum Directory-Server (LDAP) erfolgreich 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** für diesen Qshell-Befehl enthalten weitere Informationen zur Syntax und zu den geltenden Einschränkungen.

ksetup

Mit dem Qshell-Befehl ksetup werden Kerberos-Service-Einträge im Directory-Server für einen Kerberos-Realm verwaltet.

Syntax

```
ksetup -h Hostname -n BIND-Name -p BIND-Kennwort -e
```

Standardwert für allgemeine Berechtigung: *USE

Optionen

-h Der Hostname für den Directory-Server. Wird diese Option nicht angegeben, wird der in der Kerberos-Konfiguration angegebene Directory-Server verwendet.

-n Der registrierte Name, der beim BIND mit dem Directory-Server verwendet werden soll. Wird diese Option nicht angegeben, wird der Name über die Umgebungsvariable LDAP_BINDDN abgerufen.

-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` und `exit`.
- `Befehlsoption eins` und `Befehlsoption zwei` können nicht gemeinsam angegeben werden.
- LDAP-Client 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″ finden Sie ein Beispiel für die Verwendungsweise dieses Befehls.

Realms in der DNS-Datenbank definieren

Sie können Realms zur Auflösung von Hostnamen 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 jedes KDC (Key Distribution Center - 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-Laufzeitkomponente verwendet bei der Suche nach einem SRV-Satz den Realm-Namen als Suchnamen. Beachten Sie, dass die Groß-/Kleinschreibung bei DNS-Suchvorgängen keine Rolle spielt, so dass es keine unterschiedlichen Realms geben darf, deren Namen sich lediglich auf Grund 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:

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 das 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 System i 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 zum Abschnitt `libdefaults` 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 = .
}
```

2. Kerberos für den LDAP-Server definieren. 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 Parent-Einträge (dc=BOGUSNAME,dc=COM oder dc=COM). Das Suffix für einen i5/OS-LDAP-Server kann mit dem System i Navigator hinzugefügt werden.
   a. Führen Sie die folgenden Schritte durch, um ein Suffix hinzuzufügen:
      1) Erweitern Sie im System i Navigator den Eintrag für ***Ihr System*** → **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 wahlweise Hostnamenseinträge, 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.

Schema auf einem LDAP-Server definieren

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.

LDAP-Schema

Wenn Sie ein eigenes Schema auf einem LDAP-Server definieren wollen, dann sind die folgenden Informationen möglicherweise von Nutzen für Sie.

Für den Netzwerkauthentifizierungsservice gelten die folgenden LDAP-Schemadefinitionen:

- Ganzzahlige Werte werden als numerische 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

Attribut	Typ	Größe	Wert
ibmCom1986-Krb-KerberosRealm	caseExactString	256	Einzelwert
ipServicePort	Ganzzahliger Wert	11	Einzelwert
seeAlso	DN	1000	Mehrere Werte
serviceName	caseIgnoreString	256	Einzelwert

Fehler beim Netzwerkauthentifizierungsservice beheben

Die vorliegenden Informationen zur Fehlerbehebung enthalten Angaben zu gelegentlich auftretenden Problemen, die den Netzwerkauthentifizierungsservice, Enterprise Identity Mapping (EIM) und die von IBM gelieferten Anwendungen betreffen, die die Kerberos-Authentifizierung unterstützen.

1. Erfüllen Sie alle Voraussetzungen.
2. Vergewissern Sie sich, dass der Benutzer über ein Benutzerprofil auf der System i-Plattform und über einen Principal auf dem Kerberos-Server verfügt. Auf der System i-Plattform müssen Sie sich vergewissern, dass der Benutzer vorhanden ist. Öffnen Sie hierzu im System i Navigator 'Benutzer und Gruppen', oder geben Sie in einer Befehlszeile den Befehl WRKUSRPRF (Mit Benutzerprofilen arbeiten) ein. Auf Systemen, die mit einem Windows-Betriebssystem arbeiten, müssen Sie überprüfen, ob der Benutzer vorhanden ist. Greifen Sie hierzu auf den Ordner "Active Directory-Benutzer und -Computer" zu.
3. Überprüfen Sie, ob die System i-Plattform mit dem Kerberos-Server Kontakt hat, indem Sie den Befehl kinit im Qshell Interpreter ausführen. Wenn die Ausführung des Befehls kinit fehlschlägt, müssen Sie prüfen, ob der i5/OS-Service-Principal auf dem Kerberos-Server registriert wurde. Fall dies nicht der Fall ist, können Sie den i5/OS-Principal zum Kerberos-Server hinzufügen.

   Zugehörige Tasks

   „i5/OS-Principals zum Kerberos-Server hinzufügen" auf Seite 105
   Nachdem Sie den Netzwerkauthentifizierungsservice auf Ihrer System i-Plattform konfiguriert haben, müssen Sie Ihre i5/OS-Principals zum Kerberos-Server hinzufügen.

Fehler und Fehlerbehebung beim Netzwerkauthentifizierungsservice

Während der Verwendung des Assistenten für den Netzwerkauthentifizierungsservice oder beim Verwalten der Eigenschaften des Netzwerkauthentifizierungsservice im System i Navigator treten möglicherweise die folgenden Fehler auf. Wenden Sie die entsprechenden Fehlerbehebungsmaßnahmen an, die im Folgenden aufgelistet sind.

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. Einzelheiten hierzu finden Sie unter „Netzwerkauthentifizierungsservice konfigurieren" auf Seite 104.
KRBWIZ_ERROR_READ_CONFIG_FILE: Fehler beim Lesen der Konfigurationsdatei für Netzwerkauthentifizierungsservice.	Den Netzwerkauthentifizierungsservice rekonfigurieren. Einzelheiten hierzu finden Sie unter „Netzwerkauthentifizierungsservice konfigurieren" auf Seite 104.
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.

Tabelle 36. Fehler und Fehlerbehebung beim Netzwerkauthentifizierungsservice (Forts.)

Fehler	Wiederherstellung
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

Im Folgenden sind einige der häufigeren Fehler, die bei Kerberos-fähigen i5/OS-Schnittstellen auftreten können, sowie entsprechende Fehlerbehebungsmaßnahmen aufgeführt.

Tabelle 37. Gelegentlich auftretende Fehler bei 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 System i-Plattform 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. Gelegentlich auftretende Fehler bei Kerberos-fähigen i5/OS-Schnittstellen (Forts.)

Problem	Wiederherstellung
Keine DRDA/DDM-Verbindung auf einer System i-Plattform möglich, für die 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: 1. Gehen Sie folgendermaßen vor, wenn Sie nicht mit der Kerberos-Authentifizierung arbeiten: Löschen Sie den bei der Konfiguration des Netzwerkauthentifizierungsservice angegebenen Standard-Realm. 2. Gehen Sie folgendermaßen vor, wenn Sie mit der Kerberos-Authentifizierung arbeiten: a. Rekonfigurieren Sie den Netzwerkauthentifizierungsservice, und geben Sie den Standard-Realm und den Kerberos-Server an, die Sie in Schritt 1 erstellt haben. b. Konfigurieren Sie System i Access für Windows-Anwendungen für den Einsatz der Kerberos-Authentifizierung. Dadurch wird die Kerberos-Authentifizierung für alle System i Access für Windows-Anwendungen (einschließlich DRDA/DDM) aktiviert. (Weitere Informationen hierzu finden Sie in „Szenario: Einzelanmeldung für i5/OS aktivieren" auf Seite 57.)

Tabelle 37. Gelegentlich auftretende Fehler bei Kerberos-fähigen i5/OS-Schnittstellen (Forts.)

Problem	Wiederherstellung
Keine QFileSvr.400-Verbindung auf einer System i-Plattform möglich, für die 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: 1. Gehen Sie folgendermaßen vor, wenn Sie nicht mit der Kerberos-Authentifizierung arbeiten: Löschen Sie den bei der Konfiguration des Netzwerkauthentifizierungsservice angegebenen Standard-Realm. 2. Gehen Sie folgendermaßen vor, wenn Sie mit der Kerberos-Authentifizierung arbeiten: 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. b. Rekonfigurieren Sie den Netzwerkauthentifizierungsservice, und geben Sie den Standard-Realm und den Kerberos-Server an, die Sie in Schritt 1 erstellt haben. c. Konfigurieren Sie System i Access für Windows-Anwendungen für den Einsatz der Kerberos-Authentifizierung. Dadurch wird die Kerberos-Authentifizierung für alle System i Access für Windows-Anwendungen (einschließlich DRDA/DDM) aktiviert. (Weitere Informationen hierzu finden Sie in „Szenario: Einzelanmeldung für i5/OS aktivieren" auf Seite 57.)
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 2000-Domäne anmeldet. Um diesen Fehler zu beheben, melden Sie sich bei der Windows 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: 1. Erweitern Sie im System i Navigator den Eintrag für *Ihr System* → **Netzwerk** → **Server** → **TCP/IP**. 2. Klicken Sie mit der rechten Maustaste auf **Verzeichnis**, und wählen Sie **Eigenschaften** aus. 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. Gelegentlich auftretende Fehler bei 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: 1. Erweitern Sie im System i Navigator den Eintrag für *Ihr System* → **Netzwerk** → **Server** → **TCP/IP**. 2. Klicken Sie mit der rechten Maustaste auf **Verzeichnis**, und wählen Sie **Eigenschaften** aus. 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 i5/OS-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: 1. Erweitern Sie im System i Navigator den Eintrag für *Ihr System* → **Netzwerk** → **Server** → **TCP/IP**. 2. Klicken Sie mit der rechten Maustaste auf **Verzeichnis**, und wählen Sie **Eigenschaften** aus. 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. **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. Wenn der Fehler weiterhin auftritt, wenden Sie sich an die zuständige IBM Kundenunterstützung.
Kerberos-Service-Ticket kann nicht abgerufen werden. **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/*System i 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 „i5/OS-Principals zum Kerberos-Server hinzufügen" auf Seite 105. Um zu überprüfen, ob sich die Namen des Kerberos-Service-Principals in der Chiffrierschlüsseldatei befinden, sollten Sie die Informationen in „Chiffrierschlüsseldateien verwalten" auf Seite 118 lesen.

Tabelle 37. Gelegentlich auftretende Fehler bei Kerberos-fähigen i5/OS-Schnittstellen (Forts.)

Problem	Wiederherstellung
Kerberos-Principal befindet sich nicht in einer anerkannten Gruppe. **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: 1. Konfigurieren Sie das zentrale System für die Verwendung der Kerberos-Authentifizierung. 2. Erfassen Sie das Systemwerte-Inventar. 3. Vergleichen und aktualisieren Sie die verfügbaren Daten. 4. Starten Sie die Management Central-Server auf dem zentralen System und den Zielsystemen erneut. 5. Fügen Sie den Kerberos-Service-Principal für jedes Endpunktsystem zur Datei für anerkannte Gruppen hinzu. 6. Erlauben Sie sichere Verbindungen. 7. Starten Sie die Management Central-Server auf dem zentralen System und den Zielsystemen erneut. 8. Testen Sie die Authentifizierung auf den Management Central-Servern.

API-Trace-Tool

Sie können das API-Trace-Tool einrichten, um Fehler bei Aufrufen für Kerberos- und GSS-APIs (GSS = Generic Security Services) zu beheben.

Der Netzwerkauthentifizierungsservice stellt ein API-Trace-Tool zur Verfügung, mit dem ein Administrator eine Datei erstellen kann, die alle Kerberos- und GSS-API-Aufrufe (GSS = Generic Security Services) enthält. Mit Hilfe 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 der System i-Plattform aus, auf der der Netzwerkauthentifizierungsservice konfiguriert ist.

Führen Sie die folgenden Schritte durch, um das API-Trace-Tool zu konfigurieren:

1. Erstellen Sie im Ausgangsverzeichnis des Benutzers, für den die Tracefunktion ausgeführt werden soll, eine envar-Datei. Geben Sie hierzu z. B. Folgendes an: `/home/Benutzerprofilname/envar`.
2. Verwenden Sie in der zeichenorientierten Schnittstelle den Befehl `edtf /home/Benutzerprofilname/envar`, um die Datei zu bearbeiten.
3. Fügen Sie die folgenden Zeilen zur envar-Datei hinzu, und achten Sie darauf, dass diese in Spalte 1 beginnen:

```
_EUV_SVC_MSG_LOGGING=STDOUT_LOGGING
_EUV_SVC_MSG_LEVEL=VERBOSE
_EUV_SVC_STDOUT_FILENAME=/home/Benutzerprofilname/trace.txt
_EUV_SVC_DBG_MSG_LOGGING=1
_EUV_SVC_DBG_TRACE=1
_EUV_SVC_DBG=*.9
```

4. Wiederholen Sie die Ausführung des fehlgeschlagenen Befehls.
5. Zeigen Sie den Trace an, auf den mit _EUV_SVC_STDOUT_FILENAME verwiesen wird.

Nach Ausführung der Tracefunktion für den fehlgeschlagenen Befehl müssen Sie die envar-Datei löschen oder umbenennen, da andernfalls die Tracefunktion für alle Kerberos-Befehle ausgeführt wird, die vom Benutzer eingegeben werden.

Auf die API-Traceprotokolldatei zugreifen

Nachdem Sie das API-Trace-Tool konfiguriert haben, können Sie jetzt auf die Protokolldatei zugreifen, um mit der Fehlerbehebung zu beginnen.

Führen Sie die folgenden Schritte durch, um auf diese Protokolldatei zuzugreifen:

1. Geben Sie in der zeichenorientierten Schnittstelle `wrklnk ('home/Benutzerprofil')` ein, wobei `Benutzerprofil` der Name des Benutzerprofils ist.
2. Wählen Sie in der Anzeige **Mit Objektverbindung arbeiten** Auswahl 5 aus, um den Inhalt der Datei trace.txt anzuzeigen, die in diesem Verzeichnis gespeichert ist.

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.

Zugehörige Informationen

API Finder

Generic Security Service Application Programming Interfaces (GSS-APIs)

Network Authentication Service Application Programming Interfaces (APIs)

Fehler des Kerberos-Servers in i5/OS PASE beheben

Sie haben Zugriff auf Status- und Informationsprotokolldateien, mit deren Hilfe Sie Fehler des Kerberos-Servers in i5/OS PASE beheben können.

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 die Protokolldateien für den Kerberos-Server kann nur über die System i-Plattform zugegriffen werden, auf der der Kerberos-Server unter i5/OS PASE konfiguriert wurde. Führen Sie die folgenden Schritte durch, um auf die Protokolldateien zuzugreifen:

1. 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.
2. Geben Sie in der Befehlszeile `cd /var/krb5/log` ein.
3. Geben Sie in der Befehlszeile `cat /krb5kdc.log` ein. Damit wird die Datei krb5kdc.log geöffnet, die Fehlernachrichten für das 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@SYSTEMA.MYCO.COM for kadmin/changepw@SYSTEMA.MYCO.COM,
Zusätzliche Vorab-Authentifizierung erforderlich

Apr 30 14:18:08 systema.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@SYSTEMA.MYCO.COM for
kadmin/changepw@SYSTEMA.MYCO.COM

Apr 30 14:18:56 systema.myco.com /usr/krb5/sbin/krb5kdc[334](Notice):
AS_REQ (3 etypes {16 3 1}) 10.1.1.2(88): NEEDED_PREAUTH:
jday@SYSTEMA.MYCO.COM for kadmin/changepw@SYSTEMA.MYCO.COM,
Zusätzliche Vorab-Authentifizierung erforderlich

Apr 30 14:18:56 systema.myco.com /usr/krb5/sbin/krb5kdc[334](info):
DISPATCH: Wiederholungsattacke gefunden und erneut übertragen
$
```

Befehle für den Netzwerkauthentifizierungsservice

Diese Befehle vereinfachen das Konfigurieren und die Benutzung des Netzwerkauthentifizierungsservice.

Tabelle 38. Befehle für den Netzwerkauthentifizierungsservice

Befehl	Beschreibung
config.krb	Konfiguriert Server und Clients für den Netzwerkauthentifizierungsservice.
kadmin	Verwaltet die Datenbank für den Netzwerkauthentifizierungsservice.
kadmind_daemon	Startet den Verwaltungsserver für den Netzwerkauthentifizierungsservice.
kdb5_util	Ermöglicht einem Administrator die Ausführung einfacher Wartungsarbeiten in der Datenbank für den Netzwerkauthentifizierungsservice.
kdestroy	Löscht den Cache für Berechtigungsnachweise (d. h. die Chiffrierschlüsseltabelle).
kinit	Ruft ein Ticket-granting Ticket ab oder verlängert dieses.
klist	Zeigt den Inhalt des Caches für Berechtigungsnachweise oder der Chiffrierschlüsseltabelle an.
kpasswd	Ändert das Kennwort eines Principals.
krb5kdc	Startet das Multithread-Key Distribution Center (KDC) des Netzwerkauthentifizierungsservice.

Tabelle 38. Befehle für den Netzwerkauthentifizierungsservice (Forts.)

Befehl	Beschreibung
ksetup	Verwaltet die Einträge des Netzwerkauthentifizierungsservice im LDAP-Verzeichnis für einen Netzwerkauthentifizierungsservice-Realm.
ksu	Wechselt zu einer anderen Benutzer-ID.
ktutil	Ermöglicht dem Administrator das Lesen, Schreiben oder Bearbeiten von Einträgen in einer Chiffrierschlüsseldatei.
kvno	Zeigt die aktuelle Schlüsselversionsnummer für einen Principal an.
start.krb5	Startet den Server für den Netzwerkauthentifizierungsservice.
stop.krb5	Stoppt den Server für den Netzwerkauthentifizierungsservice.
unconfig.krb5	Dekonfiguriert die Clients und Services des Netzwerkauthentifizierungsservice.

Weitere Informationen zu diesen Befehlen finden Sie im Handbuch *IBM Network Authentication Service AIX, Linux, and Solaris Administrator's and User's Guide*.

Referenzinformationen für Netzwerkauthentifizierungsservice

Referenzinformationen zur Themensammlung für den Netzwerkauthentifizierungsservice sind in Produkthandbüchern, auf Websites und in anderen Themensammlungen des Information Centers enthalten. Sie können die bereitgestellten PDF-Dateien anzeigen oder drucken.

Handbücher

Wenn Sie die CD für das *AIX Expansion Pack* bestellen, können Sie auf die Dokumentation zum Netzwerkauthentifizierungsservice zugreifen. Obwohl die Handbücher für die Betriebssysteme AIX, Solaris und Linux geschrieben wurden, können viele der Befehle für den Netzwerkauthentifizierungsservice auch unter dem Betriebssystem i5/OS benutzt werden. Wenn Sie den Netzwerkauthentifizierungsservice auf Ihrem AIX-System installieren, dann wird die Dokumentation im Verzeichnis /usr/lpp/krb5/doc/pdf/en_US abgelegt.

Wenn Sie das Produkt Network Authentication Enablement (5722-NAE oder 5761-NAE) auf Ihrem System installieren, können Sie außerdem sowohl auf die PDF- als auch auf die HTML-Versionen dieser Handbücher zugreifen, die im Verzeichnis /usr/lpp/krb5/doc/ gespeichert sind.

- *IBM Network Authentication ServiceAIX, Linux, and Solaris Administrator's and User's Guide*.
- *IBM Network Authentication Service AIX, Linux, and Solaris Application Development Reference*.

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

Websites

Die folgenden Websites und Dokumentationen enthalten weitere Informationen zur Konfiguration eines Kerberos-Servers unter einem bestimmten Betriebssystem.

- Windows 2000 Server 
- z/OS Security Server Network Authentication Service Administration 

Weitere Information Center-Themen

- Network Authentication Service Application Programming Interfaces (APIs)
- Generic Security Service Application Programming Interfaces (GSS-APIs)
- Enterprise Identity Mapping (EIM)
- Einzelanmeldung

Request for Comments

Requests for Comments (RFCs) 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 1509
RFC 1509: Generic Security Service API: C-bindings enthält die formale IETF-Definition (IETF = Internet Engineering Task Force) von GSS-APIs.

RFC 1510
RFC 1510: The Kerberos Network Authentication Service (V5) enthält die formale IETF-Definition (IETF = Engineering Task Force) des Kerberos-V5-Protokolls.

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

RFC 2743
RFC 2743: Generic Security Service Application Program Interface Version 2, Update 1, enthält die formale IETF-Definition der GSS-APIs.

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

Zugehörige Verweise

„PDF-Datei für den Netzwerkauthentifizierungsservice" auf Seite 2
Sie können diese Informationen als PDF-Datei anzeigen und drucken.

Kapitel 2. Besondere Vertragsbedingungen

In den nachfolgenden Abschnitten finden Sie besondere Vertragsbedingungen und Marken, die für den Netzwerkauthentifizierungsservice gelten.

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. An Stelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
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 Dokument aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht von IBM dar, unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

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, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Musterprogramme geschrieben werden.

Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten.

Kopien oder Teile der Musterprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

© (Name Ihrer Firma) (Jahr). Teile des vorliegenden Codes wurden aus Musterprogrammen der IBM Corp. abgeleitet. © Copyright IBM Corp. _Jahr/Jahre angeben_. Alle Rechte vorbehalten.

Der folgende Copyrightvermerk und Genehmigungsnachweis gilt für Teile der vorliegenden Informationen, die vom Massachusetts Institute of Technology stammen.

Copyright © 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 beinhaltet Dokumentationsmaterial und Softwareprodukte, die an der University of California, Berkeley, entwickelt wurden und die den folgenden Copyrightvermerk umfassen:

Copyright © 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.

Es ist erlaubt, unveränderte Kopien dieses Handbuchs zu erstellen und zu vertreiben, vorausgesetzt, der Copyrightvermerk und diese Genehmigung bleiben auf allen Kopien erhalten.

Es ist erlaubt, veränderte Versionen dieses Handbuchs unter den Voraussetzungen für unverändertes Kopieren zu erstellen und zu vertreiben, sofern die gesamte resultierende Arbeit unter den Bedingungen

einer Genehmigung vertrieben wird, die mit dieser identisch ist. Es ist erlaubt, Übersetzungen dieses Handbuchs in eine andere Sprache unter den obigen Bedingungen für veränderte Versionen zu kopieren und zu vertreiben.

Marken

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

- AIX
- IBM
- Tivoli
- VisualAge

Kerberos ist eine Marke des Massachusetts Institute of Technology (MIT).

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

Linux ist eine Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Hersteller 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 zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. An Stelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete, der IBM Lizenzvereinbarung für Maschinencode oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht von IBM dar, unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Musteranwendungsprogramme, die in Quellensprache geschrieben sind. Sie dürfen diese Musterprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Musterprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten.

Kopien oder Teile der Musterprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

© (Name Ihrer Firma) (Jahr). Teile des vorliegenden Codes wurden aus Musterprogrammen der IBM Corp. abgeleitet. © Copyright IBM Corp. _Jahr/Jahre angeben_. Alle Rechte vorbehalten.

Informationen zu Programmierschnittstellen

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

Marken

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

AIX
AIX 5L
Distributed Relational Database Architecture

DRDA
i5/OS
IBM
IBM (Logo)
iSeries
NetServer
OS/400
Redbooks
System i
System p
System z
Tivoli
VisualAge
z/OS

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

Linux ist eine Marke von Linus Torvalds 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.

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

Bedingungen

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

Persönliche Nutzung: Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM weder weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Kommerzielle Nutzung: Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Abgesehen von den hier gewährten Berechtigungen erhalten Sie keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum.

IBM behält sich das Recht vor, die in diesem Dokument gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden. Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Verordnungen, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Veröffentlichungen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf ″as-is″-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit oder die Freiheit der Rechte Dritter zur Verfügung gestellt.