



System i

セキュリティー
ネットワーク認証サービス

バージョン 6 リリース 1





System i

セキュリティー
ネットワーク認証サービス

バージョン 6 リリース 1

お願い

本書および本書で紹介する製品をご使用になる前に、151ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM i5/OS (プロダクト番号 5761-SS1) のバージョン 6、リリース 1、モディフィケーション 0 に適用されます。また、改訂版で断りがない限り、それ以降のすべてのリリースおよびモディフィケーションに適用されます。このバージョンは、すべての RISC モデルで稼働するとは限りません。また CISC モデルでは稼働しません。

IBM 発行のマニュアルに関する情報のページ

<http://www.ibm.com/jp/manuals/>

こちらから、日本語版および英語版のオンライン・ライブラリーをご利用いただけます。また、マニュアルに関するご意見やご感想を、上記ページよりお送りください。今後の参考にさせていただきます。

(URL は、変更になる場合があります)

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： System i
Security
Network authentication service
Version 6 Release 1

発行： 日本アイ・ビー・エム株式会社

担当： ナショナル・ランゲージ・サポート

第1刷 2008.2

この文書では、平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財)日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、
平成角ゴシック体™W5、平成角ゴシック体™W7

© Copyright International Business Machines Corporation 1998, 2008. All rights reserved.

© Copyright IBM Japan 2008

目次

第 1 章 ネットワーク認証サービス 1

V6R1 の新機能	1
ネットワーク認証サービスの PDF ファイル	3
ネットワーク認証サービスの概念	3
Kerberos の概念	4
ネットワーク認証サービスでの処理方法	5
ネットワーク認証サービスのプロトコル	8
ネットワーク認証サービスの環境変数	10
シナリオ: Kerberos ネットワークでのネットワーク 認証サービスの使用	14
シナリオ: i5/OS PASE での Kerberos サーバーの セットアップ	14
計画ワークシートの完成	16
i5/OS PASE での Kerberos サーバーの構成	19
i5/OS PASE Kerberos サーバーでの暗号化値の 変更	19
i5/OS PASE での Kerberos サーバーの停止と 再始動	20
Windows 2000、Windows XP、および Windows Vista ワークステーションのホスト・ プリンシパルの作成	20
Kerberos サーバーでのユーザー・プリンシパル の作成	21
システム A サービス・プリンシパルの Kerberos サーバーへの追加	21
Windows 2000、Windows XP、および Windows Vista ワークステーションの構成	21
ネットワーク認証サービスの構成	22
システム A 上でのユーザーのホーム・ディレ クトリーの作成	23
ネットワーク認証サービスのテスト	23
シナリオ: ネットワーク認証サービスの構成	24
計画ワークシートの完成	26
システム A 上でのネットワーク認証サービス の構成	28
システム A プリンシパルの Kerberos サーバ ーへの追加	29
システム A 上でのユーザーのホーム・ディレ クトリーの作成	30
システム A 上でのネットワーク認証サービス のテスト	30
シナリオ: レルム間の信頼関係のセットアップ	31
計画ワークシートの完成	34
システム B 上の i5/OS PASE 内で Kerberos サーバーが開始済みであることの確認	36
i5/OS PASE Kerberos サーバー上でレルム間の 信頼のプリンシパルを作成	37
i5/OS PASE Kerberos サーバーでの暗号化値の 変更	38
SHIPDEPT.MYCO.COM を信頼するように Windows 2000 サーバーを構成	38

SHIPDEPT.MYCO.COM レルムのシステム A への追加	38
シナリオ: 複数システムにわたるネットワーク認 証サービス構成の伝搬	39
計画ワークシートの完成	43
システム・グループの作成	46
モデル・システム (システム A) からシステム B およびシステム C へのシステム設定値の伝 搬	47
システム D 上でのネットワーク認証サービス の構成	48
エンドポイント・システム用のプリンシパルを Windows 2000 ドメインに追加	48
シナリオ: マネージメント・セントラル・サーバ 一問での Kerberos 認証の使用	50
計画ワークシートの完成	53
Kerberos 認証を使用するセントラル・システム の設定	54
MyCo2 システム・グループの作成	55
システム値インベントリーの収集	55
System i ナビゲーターにおける Kerberos 設定 の比較と更新	56
セントラル・システムおよび受動システムでの マネージメント・セントラル・サーバーの再始 動	56
エンドポイントごとにトラステッド・グルー プ・ファイルに Kerberos サービス・プリンシ パルを追加	57
Kerberos プリンシパルがトラステッド・グルー プ・ファイルに追加されたことの検証	57
セントラル・システムへの信頼された接続を可 能にする	58
受動システムごとのステップ 4 から 6 の繰り 返し	58
エンドポイント・システムでの認証のテスト	58
シナリオ: i5/OS 用のシングル・サインオンを使 用可能にする	59
計画ワークシートの完成	65
システム A の基本シングル・サインオン構成 の作成	71
システム B を EIM ドメインに参加するよう 構成し、さらにネットワーク認証サービス用と してシステム B を構成	73
Kerberos サーバーへの両方の i5/OS サービ ス・プリンシパルの追加	75
システム A およびシステム B 上でユーザ ー・プロファイルを作成	76
システム A およびシステム B 上でホーム・ ディレクトリーを作成	76
システム A および B 上でのネットワーク認 証サービスのテスト	77

2 名の管理者 John Day と Sharon Jones 用の EIM ID の作成	77
John Day 用の ID アソシエーションの作成	78
Sharon Jones 用の ID アソシエーションの作成	79
デフォルト・レジストリー・ポリシー関連の作成	80
レジストリーの探索操作への参加とポリシー関連の使用可能化	81
EIM ID マッピングのテスト	82
Kerberos 認証を使用するよう System i Access for Windows アプリケーションを構成	85
ネットワーク認証サービスおよび EIM 構成の検証	85
構成終了後の考慮事項	86
ネットワーク認証サービスの計画	87
Kerberos サーバーの計画	87
レルムの計画	89
プリンシパル名の計画	90
ホスト名解決の考慮事項	93
ホスト名の解決	97
ネットワーク認証サービス計画ワークシート	99
ネットワーク認証サービスの構成	102
i5/OS PASE で Kerberos サーバーを構成する	103
Kerberos サーバー上での暗号化値の変更	104
Kerberos サーバーの停止と再始動	104
ホスト、ユーザー、およびサービスのプリンシパルの作成	104
Windows 2000、Windows XP、および Windows Vista ワークステーションの構成	105
2 次 Kerberos サーバーの構成	106
ネットワーク認証サービスの構成	108
Kerberos サーバーへの i5/OS プリンシパルの追加	110
ホーム・ディレクトリーの作成	112
ネットワーク認証サービス構成のテスト	112
ネットワーク認証サービスの管理	114
システム時刻の同期化	114
レルムの追加	115
レルムの削除	115
レルムへの Kerberos サーバーの追加	115

パスワード・サーバーの追加	116
レルム間の信頼関係の作成	116
ホスト解決の変更	117
暗号化設定の追加	117
チケット許可チケットの取得または更新	118
kinit	119
信任状キャッシュの表示	121
klist	121
keytab ファイルの管理	123
keytab	124
Kerberos パスワードの変更	125
kpasswd	127
有効期限が切れた信任状キャッシュ・ファイルの削除	127
kdestroy	128
LDAP ディレクトリー内の Kerberos サービス・エントリーの管理	130
ksetup	131
DNS データベースでのレルムの定義	132
LDAP サーバーでのレルムの定義	133
LDAP サーバーでのスキーマの定義	135
ネットワーク認証サービスのトラブルシューティング	136
ネットワーク認証サービスのエラーおよびリカバリー	136
アプリケーション接続の問題およびリカバリー	137
API トレース・ツール	141
API トレース・ツールのセットアップ	141
API トレース・ログ・ファイルへのアクセス	142
i5/OS PASE での Kerberos サーバーのトラブルシューティング	143
ネットワーク認証サービスのコマンド	143
ネットワーク認証サービスの関連情報	144

第 2 章 特別な条件 147

付録. 特記事項 151
プログラミング・インターフェース情報 152
商標 152
使用条件 153

第 1 章 ネットワーク認証サービス

ネットワーク認証サービスにより、System i™ 製品およびいくつかの System i サービス (System i Access for Windows® ライセンス・プログラムなど) は、ユーザー名とパスワードを置き換えるオプションとして Kerberos チケットを認証に使用できるようになります。

Kerberos プロトコルは、Massachusetts Institute of Technology により開発され、プリンシパル (ユーザーまたはサービス) が非セキュア・ネットワーク内の別のサービスに対して自分の ID を証明できるようにするものです。プリンシパルの認証は、Kerberos サーバーまたは鍵配布センター (KDC) と呼ばれる中央サーバーを通じて実行されます。

注: 本書では、一般的な用語である *Kerberos* サーバー を使用します。

ユーザーは、Kerberos サーバーに保管されているプリンシパルおよびパスワードを使用して認証されます。プリンシパルが認証されると、Kerberos サーバーはそのユーザーに対してチケット許可チケット (TGT) を出します。ユーザーがネットワーク上のアプリケーションまたはサービスにアクセスする必要がある時は、ユーザーの PC 上の Kerberos クライアント・アプリケーションは、ターゲットのサービスまたはアプリケーション用のサービス・チケットを入手するために、Kerberos サーバーに TGT を送り返します。すると、Kerberos クライアント・アプリケーションは、サービスまたはアプリケーションへ、入手したサービス・チケットを認証用に送信します。サービスまたはアプリケーションがチケットを受信すると、セキュリティー・コンテキストが確立され、その後ユーザーのアプリケーションはターゲット・サービスとデータを交換することができます。アプリケーションはユーザーを認証し、ネットワーク上の他のサービスへそのユーザーの ID を確実に転送することができます。ユーザーが既知となると、別個の機能がネットワーク・リソースの使用権限を検証するために必要になります。

ネットワーク認証サービスは、以下の仕様をインプリメントしています。

- Kerberos バージョン 5 プロトコル Request for Comment (RFC) 1510
- 業界で事実上の標準となっている数多くの Kerberos プロトコル・アプリケーション・プログラミング・インターフェース (API)
- RFC 1509、1964、2743 に定義された Generic Security Service (GSS) API

ネットワーク認証サービスの i5/OS® インプリメンテーションは、これらの RFC および Microsoft の Windows 2000 Security Service Provider Interface (SSPI) API に準拠した認証、委任、データ機密性のサービスとともに作動します。Microsoft® Active Directory は、Kerberos をデフォルトのセキュリティー・メカニズムとして使用します。ユーザーが Microsoft Active Directory に追加されると、そのユーザーの Windows 識別は、Kerberos プリンシパルと同等になります。ネットワーク認証サービスは、Microsoft Active Directory およびその Kerberos プロトコルのインプリメンテーションとの、相互運用性を提供します。

V6R1 の新機能

ネットワーク認証サービス・トピック・コレクションの新規情報または大幅に変更された情報をお読みください。

新規の Kerberos 制御言語コマンド

V6R1 では、以下の Kerberos CL コマンドが追加されています。これらのコマンドは、i5/OS CL コマンド行で実行できます。

- Kerberos Keytab エントリーの追加 (Add Kerberos Keytab Entry (ADDKRBKTE)) コマンド
- Kerberos チケット追加 (Add Kerberos Ticket (ADDKRBTKT)) コマンド
- Kerberos パスワード変更 (Change Kerberos Password (CHGKRBPWD)) コマンド
- Kerberos 信任状キャッシュ・ファイルの削除 (Delete Kerberos Credentials Cache File (DLTKRBCCF)) コマンド
- Kerberos 信任状キャッシュ・ファイルの表示 (Display Kerberos Credentials Cache File (DSPKRBBCCF)) コマンド
- Kerberos Keytab エントリーの表示 (Display Kerberos Keytab Entries (DSPKRBKTE)) コマンド
- Kerberos Keytab エントリーの除去 (Remove Kerberos Keytab Entry (RMVKRBKTE)) コマンド

これらのコマンドの詳細については、制御言語に関するトピック・コレクション、およびネットワーク認証サービスでの以下のトピックを参照してください。



- 125 ページの『Kerberos パスワードの変更』
- 127 ページの『有効期限が切れた信任状キャッシュ・ファイルの削除』
- 121 ページの『信任状キャッシュの表示』
- 118 ページの『チケット許可チケットの取得または更新』
- 123 ページの『keytab ファイルの管理』

ネットワーク・ファイル・システム・サーバー用の新規のサービス・プリンシパル

ネットワーク・ファイル・システムは、コンピューターが、ローカル・ディスク上にある場合と同様にネットワークを介してファイルにアクセスできるようにするためのプロトコルです。System i プラットフォームでは、ネットワーク・ファイル・システム・サーバー用のキー・テーブル・エントリーを追加したり、更新したりできるようになります。詳細については 90 ページの『プリンシパル名の計画』を参照してください。

新しい情報と変更された情報の表示方法

技術的な変更点を見やすくするために、本書では以下の表示を使用します。

-  新しい情報または変更された情報の開始を示す表示
-  新しい情報または変更された情報の終了を示す表示

PDF ファイルでは、新規および変更された情報の左マージンに、リビジョン・バー (I) が付いています。



今回のリリースの新しい情報と変更された情報に関するその他の情報を見つけるには、『プログラム資料説明書』を参照してください。

ネットワーク認証サービスの PDF ファイル


本書の PDF ファイルを表示し、印刷することができます。

本書の PDF 版を表示またはダウンロードするには、ネットワーク認証サービスを選択してください。

以下の関連トピックの PDF 版を表示またはダウンロードすることができます。

- シングル・サインオン  には、以下のトピックが含まれています。
 - ネットワーク認証サービスを、エンタープライズ識別マッピング (EIM) とともに使用してシングル・サインオン環境を可能にする方法を示すシナリオ。
 - シングル・サインオンおよびその利点を説明する概念的な情報。
- EIM (エンタープライズ識別マッピング)  には、以下のトピックが記載されています。
 - EIM の一般的なインプリメンテーションを示すシナリオ。
 - EIM を理解し計画する援助となる概念的な情報および計画のための情報。

その他の情報

この資料は、AIX 5L™ Expansion Pack and Bonus Pack  CD、または *Network Authentication Enablement* CD に収録されています。

- 資料:
 - *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*

PDF ファイルの保管

PDF をワークステーションに保管して、表示または印刷できるようにするには、以下の手順を実行します。

1. ご使用のブラウザで PDF リンクを右クリックします。
2. ローカル側に PDF を保管するオプションをクリックします。
3. PDF の保管先にしたいディレクトリーにナビゲートします。
4. 「保存」をクリックします。

Adobe Reader のダウンロード

これらの PDF を表示または印刷するには、ご使用のシステムに Adobe® Reader をインストールする必要があります。Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html)  から無料でダウンロードできます。

ネットワーク認証サービスの概念

ネットワーク認証サービスは、ネットワーク内でユーザー認証を提供する Kerberos プロトコルおよび Generic Security Service (GSS) API をサポートします。

Kerberos プロトコルおよび GSS API に関する情報は多数の情報源にあるため、このトピックではご使用の System i 環境に特に適用される基本を説明します。

Kerberos の概念

ネットワーク認証サービスは、Kerberos プロトコルの用語、例えば、KDC、プリンシパル、キー・テーブル、Kerberos チケット、などを使用します。

KDC、プリンシパル、およびキー・テーブル

鍵配布センター (KDC) は、Kerberos サーバーとも呼ばれるもので、認証サーバーとチケット許可サーバーから構成されます。認証サーバーはチケット許可チケットを出し、チケット許可サーバーはサービス・チケットを出します。Kerberos サーバーとしての役割を果たさせるには、セキュアなマシンを使用することが重要になります。だれかが Kerberos サーバーへのアクセスを取得すると、レルム全体が危険にさらされる可能性があります。

Kerberos のレルムでは、プリンシパルという語はユーザーまたはサービスの名前を示します。i5/OS オペレーティング・システムでは、クライアントから System i プラットフォームに対して認証するときに、System i Access for Windows、QFileSrv.400、および Telnet サーバーが使用するサービスを識別するために、krbsvr400 サービス・プリンシパルが使用されます。

キー・テーブルを構成する各エントリーには、サービスのプリンシパルの名前と機密鍵が含まれています。i5/OS オペレーティング・システムでは、ネットワーク認証サービスの構成時に、キー・テーブル・ファイルが作成されます。サービスがネットワーク認証サービスを構成してシステムへの認証を要求すると、そのオペレーティング・システムはそのサービスの信任状をキー・テーブル・ファイルで調べます。

ユーザーおよびサービスが正しく認証されるようにするには、ユーザーおよびサービスを Kerberos サーバーおよび i5/OS 上で作成しておく必要があります。「ネットワーク認証サービス」ウィザードのプロセス中に、キー・テーブルに対してエントリーが追加されます。文字ベース・インターフェースの Qshell インタープリターの中から keytab コマンドを使用することにより、キー・テーブルに対してエントリーを追加することもできます。

注: このドメイン名システム (DNS) 名は、マシン上で定義されているホスト名と同じである必要があります。DNS と Kerberos の連携の詳細については、93 ページの『ホスト名解決の考慮事項』を参照してください。

Kerberos チケット

Kerberos チケット は、開始プリンシパルの識別をそのターゲットに送信するための、透過性を持つアプリケーション・メカニズムです。シンプル・チケットには、プリンシパルの識別、セッション鍵、タイム・スタンプ、その他の情報が含まれており、ターゲットの秘密鍵を用いて封印されています。Kerberos チケットは、更新可能、転送可能、または委任可能です。

転送可能チケットは、完全な識別 (TGT) を別のマシンに転送させます。一方プロキシー可能チケットは、特定のチケットのみを転送させます。プロキシー可能チケットでは、プリンシパルに代わってサービスがタスクを実行できます。このサービスは、特定の目的のためのプリンシパルの識別をもつことが可能でなければなりません。プロキシー可能チケットは、元のチケット許可チケットを基にした新しいチケットを別のネットワーク・アドレスに出すことができることを Kerberos サーバーに通知します。プロキシー可能チケットを使用するときには、パスワードは必要ありません。

場合によっては、アプリケーションまたはサービスが、長期間にわたって有効なチケットをもちたいことがあります。ただし、長期間になると、チケットの信任状の有効期限が切れるまで有効である信任状が盗まれる可能性があります。更新可能チケットを使えば、アプリケーションは、長期間にわたって有効なチケットを取得できます。更新可能チケットには、2 つの有効期限があります。最初の有効期限はチケットの現行イ

インスタンスに適用され、2 番目の有効期限は許容される最後の有効期限に適用されます。

ネットワーク認証サービスでの処理方法

System i 製品は、Kerberos ネットワークにおいてサーバーまたはクライアントとして働くことができます。この両方の状態における認証プロセスとチケットの流れを理解しておく必要があります。

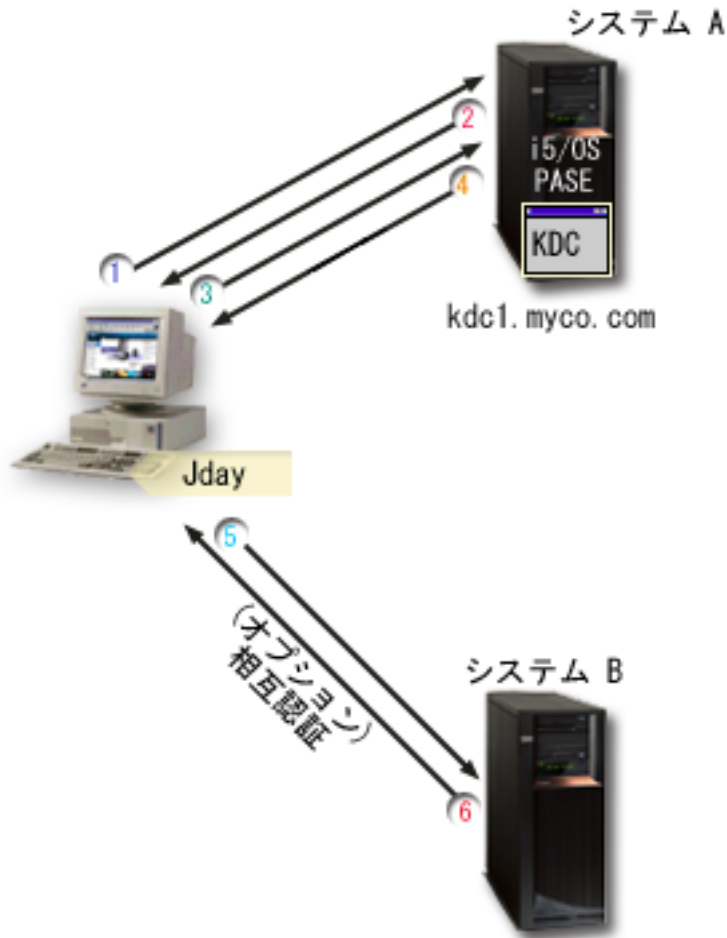
Kerberos プロトコルは、ネットワーク上でユーザーおよびサービスを認証する方法を提供します。ネットワーク管理者として、貴方は、認証の 1 形式として Kerberos チケットをご使用の System i プラットフォームが受け入れるように、ネットワーク認証サービスを構成することができます。System i 製品およびいくつかのシステム固有のアプリケーションは、Kerberos ネットワーク内で認証のためにユーザーおよびサービス向けのチケットを要求するクライアント/サーバーとしての役割を果たします。Kerberos プロトコルは、ユーザーおよびサービスが自分の ID をネットワーク全体に対して証明する (認証する) 手段を提供しますが、そのネットワーク上のリソースに対してユーザーおよびサービスを許可しません。i5/OS 機能に対する特定の権限は、i5/OS オペレーティング・システム上に作成されるユーザー・プロファイルによって維持されます。

ユーザーが Kerberos を使用して認証すると、そのユーザーにはチケット許可チケット (TGT) と呼ばれる初期チケットが出されます。そこで、ユーザーは、TGT を使用してサービス・チケットを要求して、ネットワーク上の他のサービスおよびアプリケーションにアクセスすることができます。認証が正常に機能できるように、管理者は Kerberos サーバーで Kerberos プロトコルを使用するユーザー、i5/OS サービス・プリンシパル、およびアプリケーションを登録する必要があります。System i 製品は、プリンシパルがサービスに対する認証を要求するサーバーとしての役割を果たすか、あるいはネットワーク上のアプリケーションおよびサービスへのチケットを要求するクライアントとしての役割を果たすか、いずれかが可能です。次の図に、これら 2 つの状況におけるチケットの流れを示します。

サーバーとしての System i 製品

この図は、System i 製品が Kerberos ネットワーク内でサーバーとしての役割を果たす場合の認証の働き方を示しています。この図で、i5/OS PASE にある Kerberos サーバーまたは鍵配布センター (KDC) は、プリンシパル jday に対してチケットを出します。

プリンシパル jday はシステム A 上のアプリケーションにアクセスしたいものとしします。この場合、エンタープライズ識別マッピング (EIM) がこのシステム上で使用されて、Kerberos プリンシパルが i5/OS ユーザー・プロファイルにマップされます。これは、System i Access for Windows などの、Kerberos 認証をサポートする任意の System i 機能によって行われます。



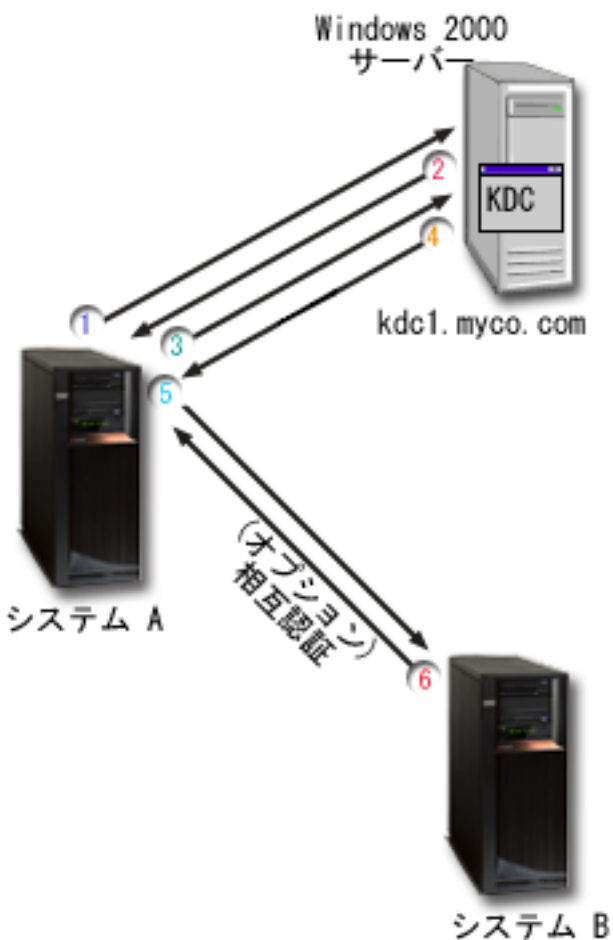
以下の説明では、ネットワーク内での認証プロセスの働き方を記載します。

1. ユーザー jday は、Kerberos レalmにサインインする際に、プリンシパルとパスワードを提供することにより、Kerberos サーバーに対して認証されます。これにより、Kerberos サーバーにチケット許可チケット (TGT) を求める要求が送信されます。
2. Kerberos サーバーは、そのユーザーのプリンシパル名およびパスワードの検証を行い、TGT を jday へ送信します。
3. jday は、System i プラットフォーム上のアプリケーションにアクセスする必要があります。 jday の PC 上の Kerberos クライアント・アプリケーションは、自分の TGT を Kerberos サーバーへ送信して、System i ナビゲーターなどの特定のアプリケーションまたはサービスへのサービス・チケットを要求します。このユーザーのワークステーションは、ユーザーのチケットおよび他の識別情報を保持する自分の信任状キャッシュを管理します。この信任状は、必要に応じてキャッシュから読み取られ、新しい信任状が取得されるとキャッシュに保管されます。このことによって、アプリケーションが信任状自体を管理する責任が取り除かれます。
4. Kerberos サーバーはサービス・チケットを使用して応答します。
5. アプリケーションは、サービス・チケットを System i サービスに送信してユーザーを認証します。
6. サーバー・アプリケーションは、ネットワーク認証サービス API を呼び出してチケットを検証し、オプションとして相互認証のためにクライアントに応答を返送することができます。

7. EIM アソシエーションを使用して、Kerberos プリンシパルが i5/OS ユーザー・プロファイルにマップされます。

クライアントとしての System i 製品

この図は、System i 製品が Kerberos ネットワーク内でクライアントとしての役割を果たす場合の認証の働き方を示しています。この図で、Windows 2000 サーバー上にある Kerberos サーバーは、Kerberos に対して認証されたユーザーに対してチケットを出します。システム A は他のサービスに対して認証されることができます。この例では、EIM をシステム B 上で使用して、Kerberos プリンシパルをユーザー・プロファイルへマップします。これは、QFileSvr.400 などの、Kerberos 認証をサポートする任意の System i 機能によって行われます。



以下の説明では、ネットワーク内での認証プロセスの働き方を記載します。

1. プリンシパル jday は、システム A にサインインしてから、Qshell インタープリターで kinit コマンドを実行することによってチケット許可チケットを要求します。システムは、この要求を Kerberos サーバーへ送信します。
2. Kerberos サーバーは、プリンシパル名およびパスワードの検証を行い、チケット許可チケットを jday へ送信します。
3. jday はシステム B 上のアプリケーションにアクセスする必要があります。ネットワーク認証サービス API を呼び出すことにより、アプリケーションは jday の TGT を Kerberos サーバーへ送信して、特定のアプリケーションまたはサービスへのサービス・チケットを要求します。プリンシパ

ルのローカル・マシンは、ユーザーのチケット、セッション鍵、および他の識別情報を保持する信任状キャッシュを管理します。この信任状は、必要に応じてキャッシュから読み取られ、新しい信任状が取得されるとキャッシュに保管されます。このことによって、アプリケーションが信任状自体を管理する責任が取り除かれます。

4. Kerberos サーバーはサービス・チケットを使用して応答します。

注: システム B 用のサービス・プリンシパルを Kerberos サーバーに追加し、ネットワーク認証サービスもシステム B 上で構成する必要があります。

5. アプリケーションは、サーバー・チケットを System i サービスに送信してユーザーを認証します。
6. サーバー・アプリケーションは、ネットワーク認証サービス API を呼び出してチケットを検証し、オプションとして相互認証のためにクライアントに応答を返送することができます。
7. EIM アソシエーションを使用し、Kerberos プリンシパルが i5/OS ユーザー・プロファイルにマップされます。

ネットワーク認証サービスのプロトコル

ネットワーク認証サービスは、認証に Kerberos プロトコルと Generic Security Services (GSS) API を使用して、認証およびセキュリティー・サービスを提供します。

このトピックでは、ネットワーク認証サービス・プロトコルの概要と、それらが System i 環境でどのように使用されるかを説明します。これらの規格に関する完全な説明については、関連する Request for Comment 標準および他の外部情報源へのリンクが提供されています。

Kerberos プロトコル

Kerberos プロトコルでは、サード・パーティー認証を提供して、ユーザーにチケットを出す、Kerberos サーバーまたは鍵配布センター (KDC) と呼ばれる中央のサーバーに対してユーザーが自身の ID を証明します。そこで、ユーザーは、このチケットを使用して自身の ID をネットワーク上で証明できます。このチケットは、複数の異なるシステムに複数回サインオンする必要を取り除きます。System i 環境がサポートする ネットワーク認証サービス API は、マサチューセッツ工科大学が考案し、Kerberos プロトコルを使用するための事実上の標準になっています。

セキュリティー環境の前提事項

Kerberos プロトコルは、どのデータ交換もパケットを自由に挿入、変更、インターセプトできる環境で行われているという前提に基づいています。Kerberos は全体的なセキュリティー計画の 1 つの層として使用してください。Kerberos プロトコルはネットワーク上のユーザーとアプリケーションの認証を可能にしますが、ネットワーク・セキュリティーの目標を定義する際には多少の制限事項があることに注意する必要があります。

- Kerberos プロトコルは、サービス妨害 (DOS) アタックに対しては保護しません。これらのプロトコル内には、侵入者が、アプリケーションが正しい認証手順に参加するのを妨害することのありえる個所があります。こうしたアタックの検出と解決策については、一般に管理者とユーザーに任せるのが最善です。
- キーの共用または盗用を通じて、偽名の使用のアタックが行われる可能性があります。侵入者が何らかの方法でプリンシパルのキーを盗んだ場合、該当のユーザーまたはサービスであるふりをすることがあります。こうした可能性を少なくするために、ユーザーがキーを共用することを禁止し、セキュリティーの規則にこの方針を明記してください。

- Kerberos プロトコルはパスワードの推測などの一般的なパスワードぜい弱点に対する保護は行いません。見破られやすいパスワードをユーザーが選んでいる場合、アタッカーはユーザーのパスワードから引き出したキーによって暗号化してあるメッセージを繰り返し暗号化解除を試みることによって、オフラインの辞書アタックをしかけ、成功する可能性があります。

Kerberos ソース

Requests for Comments (RFC) は、インターネットで使用されるプロトコル規格および提案された規格の定義を書面にしたものです。以下の RFC は、Kerberos プロトコルを理解する援助となります。

RFC 1510

RFC 1510 の内容: Kerberos ネットワーク認証サービス (V5)、Internet Engineering Task Force (IETF) が Kerberos ネットワーク認証サービス (V5) を正式に定義する。

リストされた RFC を表示するには、RFC editor  Web サイトにある RFC index search engine を参照してください。表示したい RFC の番号で検索します。この検索エンジンの結果として、対応する RFC のタイトル、作成者、日付、および状況が表示されます。

Kerberos: The Network Authentication Protocol (V5)

Kerberos プロトコルのマサチューセッツ工科大学の公式文書は、プログラミング情報を提供しており、プロトコルの機能について説明しています。

Generic Security Service (GSS) API

Generic Security Services Application Programming Interfaces (GSS API) は、一般的なセキュリティー・サービスを提供し、Kerberos プロトコルのようなセキュリティー・テクノロジー分野でサポートされます。これにより、GSS アプリケーションを複数の異なる環境に移植できます。このため、Kerberos API の代わりにこの API を使用することをお勧めします。GSS API を使って、同一ネットワーク内の他のアプリケーションおよびクライアントと通信するアプリケーションを作成できます。このやりとりでは、通信を行うアプリケーションがそれぞれの役割を果たします。アプリケーションは GSS API を使って以下のことを実行できます。

- 別のアプリケーションのユーザー ID を判別する。
- 別のアプリケーションにアクセス権限を委任する。
- 機密保持および保全性などのセキュリティー・サービスをメッセージごとに実行する。

GSS API ソース

Requests for Comments (RFC) は、インターネットで使用されるプロトコル規格および提案された規格の定義を書面にしたものです。以下の RFC は、GSS API を理解する援助となります。

RFC 2743


RFC 2743 の内容: Generic Security Service Application Program Interface バージョン 2、アップデート 1、Internet Engineering Task Force (IETF) が GSS API を正式に定義する。

RFC 1509

RFC 1509 の内容: Generic Security Service API : C-bindings。 Internet Engineering Task Force (IETF) が GSS API を正式に定義する。

RFC 1964

RFC 1964 の内容: Kerberos バージョン 5 GSS-API メカニズム。 Internet Engineering Task Force (IETF) が Kerberos バージョン 5 および GSS API の仕様を定義する。

リストされた RFC を表示するには、RFC editor  Web サイトにある RFC index search engine を参照してください。表示したい RFC の番号で検索します。この検索エンジンの結果として、対応する RFC のタイトル、作成者、日付、および状況が表示されます。

ネットワーク認証サービスの環境変数

ネットワーク認証サービスで環境変数を使用して、Generic Security Services (GSS) API および Kerberos プロトコル API の実行のしかたに影響を及ぼすことができます。

環境変数を使用して、ご使用のネットワーク上で、構成を変更しネットワーク認証サービスを管理することができます。i5/OS は、環境変数を処理するさまざまな方法をサポートします。

CL コマンド

- ADDENVVAR
- CHGENVVAR
- RMVENVVAR
- WRKENVVAR

CL コマンド ADDENVVAR を使用する環境変数の使用の一例として、141 ページの『API トレース・ツール』を参照してください。この環境変数のセットにより、各 Kerberos 呼び出しおよび GSS API 呼び出しをトレースするログ・ファイルを作成することができます。API トレース・ツールにより、Kerberos を使用できるアプリケーションに関係するより高度な問題、ネットワーク認証サービスの構成時に発生する可能性のある問題、および Kerberos チケット要求時に発生する可能性のある問題を、トラブルシューティングすることができます。

C API

- getenv()
- putenv()

これらの API の説明および例については、getenv() API および putenv() API の使用上の注意を参照してください。

Qshell commands

- export -s env_var_name=value

このほか、environment_variable=value の形式のエントリーを含む環境変数ファイル (envar ファイル) を定義することができます。Qshell 環境を通じて、または CL コマンドで定義された変数は、envar ファイル内の同じ変数をオーバーライドします。_EUV_ENVAR_FILE 環境変数を使用して、これらのエントリーを含むファイルのロケーションを指定することができます。

_EUV_ENVAR_FILE

環境変数定義を含むファイルの名前。この変数が設定されていない場合、デフォルトは、ホーム・ディレクトリーにある envar ファイルを使用することです (_EUV_HOME または HOME 環境変数によって指定される)。

ファイルの各行は、変数名、等号 (=)、変数値の順に指定され、ブランクや他の句読点は使用されません。変数値は、等号から行末までにあるすべてのもの (埋め込まれたブランクおよび末尾のブランクを含む) です。ポンド記号 (#) で始まる行はすべてコメント行として扱われます。行の終わりを円記号 (¥) にすることにより、行を継続できます。円記号の後に末尾ブランクを入れることはできません。_EUV_ は 1 桁目から始める必要があります。

環境変数は、セキュリティ・ランタイムで関数が初めて呼び出されるまで、設定されません。したがって、この変数は主としてセキュリティ・ランタイムのなかで関数が使用する環境変数を設定するのに役に立ちます。しかし、この変数はアプリケーションが使用する環境変数の設定にも使用できます。この場合、セキュリティ・ランタイムが初期化されるまでは、アプリケーションは新しい環境変数値を信頼してはなりません。このプログラムがその下で実行するユーザーのプロファイルは、このファイルに先行するパス内の各ディレクトリーに対して *X 権限を持っていないければならず、このファイルに対する *R 権限を持っていないければなりません。

_EUV_HOME と HOME

セキュリティ・ランタイムのホーム・ディレクトリーは `_EUV_HOME` 環境変数の値に設定されます。この変数が指定されていないときは、`HOME` 変数によってセキュリティ・ランタイムのホーム・ディレクトリーを決定します。どちらの環境変数も設定されていないければ、現在実行中のユーザー・プロファイル内で構成されているホーム・ディレクトリーが使われます。ホーム・ディレクトリーが存在していないときは、現行作業ディレクトリーが使われます。このディレクトリーへの共通アクセスは `*EXCLUDE` または `*R` に制限します。

_EUV_SEC_KRB5CCNAME_FILE

デフォルトの Kerberos 信任状キャッシュを見つけるために使用されるファイルの名前です。この変数が設定されていないときは、デフォルトは、セキュリティ・ランタイムのホーム・ディレクトリーにある `krb5ccname` ファイルを使用することです。実行するユーザー・プロファイルは、このファイルに先行するパス名の中の各ディレクトリーに対して *X 権限を持っていないければなりません。ファイルがまだ存在していないときは、実行するユーザー・プロファイルはこのファイルを含む親ディレクトリーに対して *WX 権限を持っていないければなりません。使用される信任状キャッシュ・ファイルが悪意あるユーザーによって変更されるのを防ぐため、親ディレクトリーへの共通アクセスを必ず制限する必要があります。

_EUV_SVC_MSG_LOGGING

メッセージがログされるターゲットです。有効な値は次のとおりです。

NO_LOGGING

すべてのメッセージを抑止します。これはデフォルトです。

STDOUT_LOGGING

すべてのメッセージ (通知メッセージとエラー・メッセージ) を `stdout` に書き出し、エラー・メッセージを `stderr` に書き出します。

STDERR_LOGGING

通知メッセージを `stdout` に書き出し、エラー・メッセージを `stderr` に書き出します。

_EUV_SVC_MSG_LEVEL

メッセージをログする時のメッセージのレベル。この基準を満たさないメッセージは抑止されます。デフォルトは、すべてのメッセージをログに記録することです。有効な値は次のとおりです。

FATAL

リカバリー不能のメッセージだけがログに記録されます。

ERROR

リカバリー不能のメッセージ、およびエラー・メッセージだけがログに記録されます。

USER リカバリー不能のメッセージ、エラー・メッセージ、およびユーザー・メッセージだけがログに記録されます。

WARNING

リカバリー不能のメッセージ、エラー・メッセージ、ユーザー・メッセージ、および警告メッセージだけがログに記録されます。

NOTICE

リカバリー不能のメッセージ、エラー・メッセージ、ユーザー・メッセージ、警告メッセージ、および通知メッセージだけがログに記録されます。

VERBOSE

すべてのメッセージがログに記録されます。

_EUV_SVC_STDOUT_FILENAME

標準出力メッセージを受け入れるファイルの完全修飾名。この環境変数が定義されていない場合、メッセージは `stdout` に書き出されます。現在実行中のユーザー・プロファイルは、このファイルに先行するパス内の各ディレクトリーに対して *X 権限を持っていないければならず、このファイルを含む親ディレクトリーに対して *WX 権限を持っていないければなりません。

_EUV_SVC_STDERR_FILENAME

標準エラー・メッセージを受け入れるファイルの完全修飾名。この環境変数が定義されない場合、メッセージは `stderr` に書き出されます。現在実行中のユーザー・プロファイルは、このファイルに先行するパス内の各ディレクトリーに対して *X 権限を持っていないければならず、このファイルを含む親ディレクトリーに対して *WX 権限を持っていないければなりません。

_EUV_SVC_DBG_MSG_LOGGING

デバッグ・メッセージを生成するかどうか。デフォルトではデバッグ・メッセージは抑止されます。デバッグ・メッセージのロギングは、IBM® サービスが要請しない限り、使用可能にはなりません。デバッグのロギングを行うと、パフォーマンスに重大な影響を与える可能性があります。有効な値は次のとおりです。

- 0 デバッグ・メッセージを抑止する。
- 1 デバッグ・メッセージを書き出す。

_EUV_SVC_DBG

デバッグ・メッセージのサブコンポーネントとレベル。特定のサブコンポーネントのデバッグ・メッセージは、そのサブコンポーネントが `_EUV_SVC_DBG` リストに入っており、デバッグ・メッセージのレベルが指定したレベル以上であるという条件がない限り、ログに記録されません。すべてのサブコンポーネントを指定するには、アスタリスク (*) を使います。

サブコンポーネントのリストは、ピリオドによって分離されたサブコンポーネント名とデバッグ・レベルから成り立ちます。エントリーをコンマで分離することにより、複数のサブコンポーネントを指定できます。例えば、`_EUV_SVC_DBG=*1,KRB_CCACHE.8` と指定すれば、すべてのサブコンポーネントについてはデバッグ・レベル 1 が有効になり、`KRB_CCACHE` サブコンポーネントについてはデバッグ・レベル 8 を有効にすることができます。以下のサブコンポーネントを指定できます。

- 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

デバッグ・メッセージを受け入れるファイルの完全修飾名。この環境変数が定義されていない場合、デバッグ・メッセージは `_EUV_SVC_STDOUT_FILENAME` で指定されたファイルに書き出されます。 `EUV_SVC_STDOUT_FILENAME` が指定されていない場合は、デバッグ・メッセージは `stdout` に書き出されます。現在実行中のユーザー・プロファイルは、このファイルに先行するパス内の各ディレクトリーに対して `*X` 権限を持っていないと、このファイルを含む親ディレクトリーに対して `*WX` 権限を持っていないとなりません。

KRB5_CONFIG

コロンで分離された、1 つまたは複数の構成ファイル名。デフォルトの構成ファイルは `/QIBM/UserData/OS400/NetworkAuthentication/krb5.conf` です。現在実行中のユーザー・プロファイルは、これらの構成ファイルに先行するパス内の各ディレクトリーに対して `*X` 権限を持っていないと、構成ファイルに対する `*R` 権限を持っていないとなりません。

`krb5.conf` ファイルは、いくつかのセクションに分割されており、それぞれ、大括弧に入れて名前が付いています。セクション内で、グループ値は中括弧に入れています。 `V5R4` およびそれ以前のリリースでは、次の表に示すように大括弧と中括弧の代わりに対応する 3 文字表記を使用することができます。

文字	3 文字表記
[(左大括弧)	??(
] (右大括弧)	??)
{ (左中括弧)	??<
} (右中括弧)	??>

ただし、デフォルトでは、`i5/OS V6R1` で実行されているシステムでは、3 文字表記のかわりに中括弧および大括弧を使用する構成になっています。 `Java™ Kerberos` クライアントを使用しない場合は、3 文字表記を使用するようシステムを設定できます。システムで 3 文字表記を使用する場合は、「データ領域変更 (`Change Data Area (CHGDTAARA)`)」 `CL` コマンドを使用して、`QUSRSYS/QKRBTRIGRA` データ域の最初の文字をデフォルトの `N` から `Y` に変更することができます。

KRB5CCNAME

信任状キャッシュ・ファイルのデフォルト名で、`type:name` として指定されます。サポートされるタイプは `FILE` と `MEMORY` です。デフォルトは、`/QIBM/UserData/OS400/NetworkAuthentication/creds` ディレクトリーの中で、`FILE` に基づいた信任状キャッシングを行うことです。デフォルトが使用される場合、権限のセットアップは不要です。 `FILE` に基づく信任状キャッシュ・ファイルを指定する場合、現在実行中のユーザー・プロファイルはパス内の各ディレクトリーに対して `*X` 権限を持っていないと、キャッシュ・ファイルを初めて作成する時には親ディレクトリーに対して `*WX` 権限が必要で、キャッシュ・ファイルに対しては `*RW` 権限が必要です。キャッシュ・ファイルを削除する時は、キャッシュ・ファイルに対する `*OBJEXIST` 権限が必要です。

KRB5_KTNAME

デフォルトのキー・テーブル名。指定されていない場合、構成ファイルの `default_keytab_name` 構成エントリーで指定されたファイルが使われます。この構成エントリーが指定されていない場合、デフォルトのファイルは `/QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab` です。現

在执行中のユーザー・プロファイルは、パス内の各ディレクトリーに対して *X 権限を持っていないければなりません。このファイルを作成する場合、親ディレクトリーに対して *WX 権限も必要です。ファイルを更新する場合は、ファイルに対する *RW 権限が必要です。必要な特定権限については、Qshell コマンドとランタイム API の資料に記載されています。

KRB5RCACHETYPE

デフォルトのリプレイ・キャッシュ・タイプ。デフォルトは dfl です。

KRB5RCACHENAME

デフォルトのリプレイ・キャッシュ名。指定されていない場合、Kerberos がランタイムに名前を生成します。

KRB5RCACHEDIR

デフォルトのリプレイ・キャッシュ・ディレクトリー。デフォルトは /QIBM/UserData/OS400/NetworkAuthentication/replay です。

シナリオ: Kerberos ネットワークでのネットワーク認証サービスの使用

これらは、i5/OS オペレーティング・システムが Kerberos ネットワークに参加できるように、ネットワーク認証サービスを使用する場合の一般的なシナリオです。

シナリオ: i5/OS PASE での Kerberos サーバーのセットアップ

Kerberos サーバーをセットアップするための目標、目的、前提条件、および構成手順を説明します。

状況

- | 貴方は、自社の中規模ネットワークのセキュリティーを管理する管理者です。セントラル・システムから、
- | ユーザーの認証を行いたいとします。ユーザーをエンタープライズ全体のリソースに対して認証する
- | Kerberos サーバーを作成することにしました。ご使用のネットワークで Kerberos ソリューションをインプ
- | リメントするために多数の選択肢を調べました。貴方は Windows 2000 サーバーがユーザーを Windows
- | ドメインに対して認証するために Kerberos を使用することを知っていますが、この選択肢では少額の IT
- | 予算に対する追加費用が生じます。Windows 2000 ドメインを使用してユーザーを認証するのではなく、
- | i5/OS ポータブル・アプリケーション・ソリューション環境 (PASE) で System i 環境に Kerberos サーバ
- | ーを構成することにしました。i5/OS PASE は、AIX® アプリケーション用の統合されたランタイム環境を
- | 提供します。自社独特の Kerberos サーバーを構成するために i5/OS PASE の柔軟性を用いるよう望んでい
- | ます。i5/OS PASE 内の Kerberos サーバーに、ネットワーク内の Windows 2000、Windows XP、および
- | Windows Vista ワークステーションを使用するユーザーを認証させるよう望んでいます。

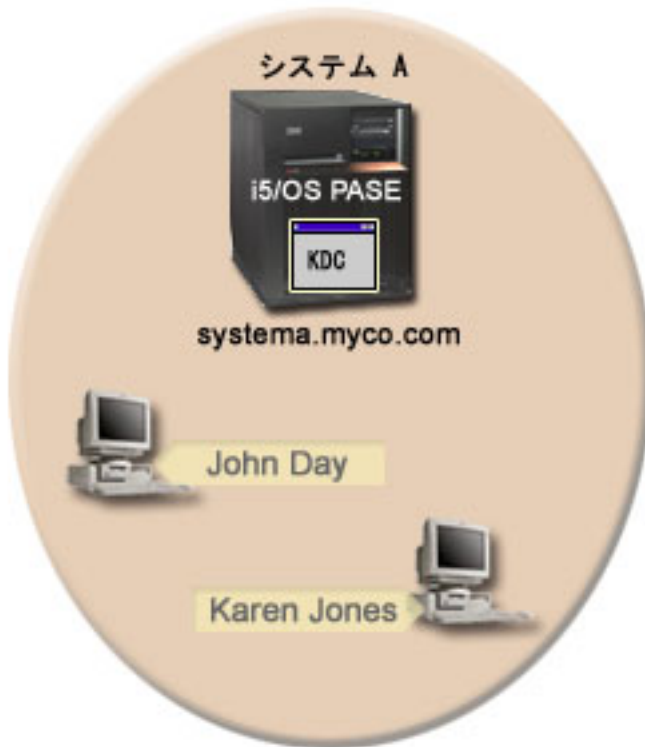
目的

このシナリオでは、MyCo, Inc. は、以下の目的を達成することにより、i5/OS PASE 内に Kerberos サーバーを確立しようとしています。

- i5/OS PASE 環境で Kerberos サーバーを構成する
- ネットワーク・ユーザーを Kerberos サーバーに追加する
- | • i5/OS PASE に構成される Kerberos レルムに参加させるために Windows 2000、Windows XP、および
- | Windows Vista オペレーティング・システムを稼働させるワークステーションを構成する
- ネットワーク認証サービスをシステム A 上に構成する
- ご使用のネットワークにおける認証をテストする

詳細

次の図は、このシナリオのネットワーク環境を示します。



システム A

- ネットワークの Kerberos サーバー (鍵配布センター (KDC) と呼ばれる) としての役割を果たす (kdc1.myco.com)。
- 次のオプションおよびライセンス・プログラムをインストールした i5/OS バージョン 5 リリース 3 (V5R3) 以降を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12 または 5761-SS1 オプション 12)
 - i5/OS PASE (5722-SS1 オプション 33 または 5761-SS1 オプション 33)
 - Qshell インタープリター (5722-SS1 オプション 30 または 5761-SS1 オプション 30)
 - Network Authentication Enablement (5722-NAE または 5761-NAE) (V5R4 以降を実行している場合)
 - Cryptographic Access Provider (5722-AC3) (V5R3 を実行している場合)
 - System i Access for Windows (5722-XE1 または 5761-XE1)
- 完全修飾ホスト名 systema.myco.com をもつ。

クライアント PC

- このシナリオにおけるすべての PC は、以下のとおり。
 - Windows 2000、Windows XP、および Windows Vista オペレーティング・システムを実行する。
 - Windows 2000 サポート・ツール (ksetup コマンドを提供する) がインストール済み。
- 管理者の PC は以下のとおり。
 - System i Access for Windows (5722-XE1 または 5761-XE1) がインストール済み。

- System i ナビゲーター は、セキュリティーおよびネットワークのサブコンポーネント付きでインストール済み。

前提条件および前提事項

このシナリオでは、i5/OS PASE 内に Kerberos サーバーを構成するタスクに焦点をあてて説明します。

1. ソフトウェアおよびオペレーティング・システムのインストールを含むすべてのシステム要件は、検証済みである。

必要なライセンス・プログラムがインストール済みであることを検証するには、以下の手順に従います。

- a. System i ナビゲーターで、「システム」 → 「構成およびサービス」 → 「ソフトウェア」 → 「インストール済みプロダクト」を展開する。
 - b. すべてのライセンス・プログラムがインストール済みであることを確認する。
2. 必要なハードウェアの計画とセットアップはすべて完了している。
 3. TCP/IP 接続がネットワーク上で構成されていて、テスト済みである。
 4. 単一の DNS サーバーが、ネットワークのホスト名解決に使用される。ホスト・テーブルは、ホスト名解決には使用されません。

注: Kerberos 認証でホスト・テーブルを使用すると、名前解決エラーまたはその他の問題が生じることがあります。Kerberos 認証でホスト名解決がどのように行われるかの詳細については、93 ページの『ホスト名解決の考慮事項』を参照してください。

構成手順

i5/OS PASE において Kerberos サーバーを構成し、ネットワーク認証サービスを構成するには、次の手順を完了します。

計画ワークシートの完成


i5/OS PASE 内で、Kerberos サーバーおよびネットワーク認証サービスを構成する前に、以下の作業計画シートに記入してください。

ネットワーク認証サービスのセットアップを進める前に、前提条件シートのすべてに「はい」と回答する必要があります。

表 1. 前提条件計画ワークシート

質問	回答
i5/OS V5R3 またはそれ以降 (5722-SS1)、または V6R1 (5761-SS1) を使用しているか?	はい

表 1. 前提条件計画ワークシート (続き)

質問	回答
<p>以下のオプションおよびライセンス・プログラムがシステム A にインストールされているか？</p> <ul style="list-style-type: none"> • i5/OS Host Servers (5722-SS1 オプション 12 または 5761-SS1 オプション 12) • i5/OS PASE (5722-SS1 オプション 33 または 5761-SS1 オプション 33) • Qshell インタープリター (5722-SS1 オプション 30 または 5761-SS1 オプション 30) • Network Authentication Enablement (5722-NAE または 5761-NAE) (V5R4 以降を使用している場合) • Cryptographic Access Provider (5722-AC3) (i5/OS V5R3 を実行している場合) • System i Access for Windows (5722-XE1 または 5761-XE1) 	はい
<p>ご使用のすべての PC に、Windows 2000、Windows XP、または Windows Vista がインストールされているか？</p>	はい
<p>使用しているすべての PC に Windows 2000 サポート・ツール (ksetup コマンドを提供) がインストールされているか？</p>	はい
<p>管理者の PC に System i Access for Windows (5722-XE1 または 5761-XE1) はインストール済みですか？</p>	はい
<p>System i ナビゲーター が管理者の PC にインストールされているか？</p> <ul style="list-style-type: none"> • 管理者の PC に System i ナビゲーター のセキュリティ・サブコンポーネントはインストール済みですか？ • 管理者の PC に System i ナビゲーター のネットワーク・サブコンポーネントはインストール済みですか？ 	はい はい はい
<p>最新の System i Access for Windows サービス・パックをインストール済みですか？ 最新の Service Pack については、System i Access  を参照してください。</p>	はい
<p>*SECADM、*ALLOBJ、および *IOSYSCFG の特殊権限を持っているか？ このシナリオで「ネットワーク認証サービス」ウィザードを使用するためには、これらの特殊権限を持つことが必要です。</p>	はい
<p>DNS を構成してあり、System i 製品と Kerberos サーバーに正しいホスト名があるか？</p>	はい
<p>Kerberos サーバーをどのオペレーティング・システム上に構成したいか？</p> <ol style="list-style-type: none"> 1. Windows 2000 サーバー 2. Windows サーバー 2003 3. AIX サーバー 4. i5/OS PASE (V5R3 以降) 5. z/OS® 	i5/OS PASE
<p>最新のプログラム一時修正 (PTF) を適用してあるか？</p>	はい
<p>System i システム時刻と Kerberos サーバーのシステム時刻との差が 5 分以内か？ そうでない場合は、114 ページの『システム時刻の同期化』を参照。</p>	はい

このシナリオでは、いくつかの異なるパスワードを指定する必要があります。以下の計画ワークシートは、このシナリオで使用する必要があるパスワードのリストを提供します。この表を、i5/OS PASE において Kerberos サーバーをセットアップする構成手順を実行する時に参照してください。

表 2. パスワード計画ワークシート

エンティティ	パスワード
i5/OS PASE 管理者: admin/admin 注: i5/OS PASE は、管理者のデフォルトのユーザー名として admin/admin を指定します。	secret
i5/OS PASE データベース・マスター	pasepwd
Windows 2000 ワークステーション • pc1.myco.com (John Day の PC) • pc2.myco.com (Karen Jones の PC)	secret1 secret2
Kerberos ユーザー・プリンシパル: • day@MYCO.COM • jones@MYCO.COM	123day 123jones
システム A 用の i5/OS サービス・プリンシパル: krbsvr400/systema.myco.com@MYCO.COM	systema123

以下の計画ワークシートは、i5/OS PASE における Kerberos サーバー、およびネットワーク認証サービスの構成を開始する前に必要な情報のタイプを示しています。i5/OS PASE において Kerberos サーバーの構成を進める前に、前提条件ワークシートおよびパスワード計画ワークシート上のすべてに回答する必要があります。

表 3. i5/OS PASE において Kerberos サーバーを構成しネットワーク認証サービスを構成するための計画ワークシート

質問	回答
Kerberos デフォルト・レルムの名前は ?	MYCO.COM
このデフォルト・レルムは Microsoft Active Directory 上にあるか ?	いいえ
この Kerberos デフォルト・レルムの Kerberos サーバー (鍵配布センター (KDC) とも呼ばれる) は ? Kerberos サーバーが listen するポートは ?	KDC: kdc1.myco.com ポート: 88 注: これは、Kerberos サーバーのデフォルト・ポートです。
このデフォルト・レルムにパスワード・サーバーを構成した いか ?	いいえ 注: 現在、パスワード・サーバーは、i5/OS PASE または AIX ではサポートされません。
どのサービス用に keytab エントリを作成したいか ? • i5/OS Kerberos 認証 • LDAP • IBM HTTP Server • i5/OS NetServer™ • ネットワーク・ファイルシステムのサーバー	i5/OS Kerberos 認証
Microsoft Active Directory へのサービス・プリンシパルの追加を自動化するバッチ・ファイルを作成したいか ?	適用外
i5/OS PASE 管理者のデフォルト・ユーザー名は ? i5/OS PASE 管理者に指定したいパスワードは ?	ユーザー名: admin/admin パスワード : secret
ネットワーク内のユーザーを表す、ご使用になるプリンシパルの命名規則は ?	ユーザーを表すプリンシパルは、小文字のファミリー名に大文字のレルム名が続いたものになる。

表 3. i5/OS PASE において Kerberos サーバーを構成しネットワーク認証サービスを構成するための計画ワークシート (続き)

質問	回答
以下のユーザーの Kerberos ユーザー・プリンシパル名は ? <ul style="list-style-type: none"> • John Day • Karen Jones 	day@MYCO.COM jones@MYCO.COM
以下のユーザーの i5/OS ユーザー・プロファイル名は ? <ul style="list-style-type: none"> • John Day • Karen Jones 	JOHND KARENJ
以下のユーザーの Windows 2000 ユーザー名は ? <ul style="list-style-type: none"> • John Day • Karen Jones 	johnday karenjones
以下の Windows 2000 ワークステーションのホスト名は ? <ul style="list-style-type: none"> • John Day の PC • Karen Jone の PC 	pc1.myco.com pc2.myco.com
システム A の i5/OS サービス・プリンシパルの名前は ?	krbsvr400/systema.myco.com@MYCO.COM 注: このサービス・プリンシパルの名前は、例として使用しているにすぎません。ご使用の構成において、i5/OS のホスト名およびドメインを、サービス・プリンシパルの名前に指定してください。

i5/OS PASE での Kerberos サーバーの構成

システム A の i5/OS PASE 上で Kerberos サーバーを構成するときは、作業計画シートからの情報を使用します。

i5/OS PASE 上で Kerberos サーバーを構成するには、次のステップを実行します:

1. 文字ベース・インターフェースで `call QP2TERM` と入力する。このコマンドは、ユーザーが i5/OS PASE アプリケーションを処理できるようにする対話式シェル環境をオープンします。
2. コマンド行で `export PATH=$PATH:/usr/krb5/sbin` と入力する。このコマンドは、実行可能ファイルを実行するために必要な Kerberos スクリプトを指します。
3. コマンド行で `config.krb5 -S -d myco.com -r MYCO.COM` と入力する。ここで `-d` は、ご使用のネットワークの DNS であり、`-r` は、レルム名です。(この例では、`myco.com` は、DNS 名であり、`MYCO.COM` は、レルム名です。) このコマンドは、Kerberos サーバーのドメイン名とレルムを使用して `krb5.config` ファイルを更新し、統合ファイル・システムの中に Kerberos データベースを作成し、i5/OS PASE 内で Kerberos サーバーを構成します。以下のパスワードを追加するよう求めるプロンプトが出されます。
 - データベース・マスター・パスワード: `pasepwd`
 - `admin/admin` プリンシパル・パスワード: `secret`
4. F3 (終了) を押して、PASE 環境を終了します。

i5/OS PASE Kerberos サーバーでの暗号化値の変更

Windows ワークステーションで作動するためには、クライアントが i5/OS PASE Kerberos サーバーに認証されるように、Kerberos サーバーでデフォルトの暗号化設定値を変更する必要があります。

デフォルト暗号化設定値を変更するには、`/etc/krb5` ディレクトリーにある `kdc.conf` ファイルを、次の手順を行って編集する必要があります。

1. 文字ベース・インターフェースで `edtf '/var/krb5/krb5kdc/kdc.conf'` と入力して `kdc.conf` ファイルにアクセスする。
2. `kdc.conf` ファイルの以下の行を

```
supported_enctypes = des3-cbc-sha1:normal  
arcfour-hmac:normal aes256-cts:normal  
des-cbc-md5:normal des-cbc-crc:normal
```

から次のように変更する。

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

i5/OS PASE での Kerberos サーバーの停止と再始動

変更したばかりの暗号化値を更新するには、i5/OS PASE において Kerberos サーバーを停止してから再始動する必要があります。

Kerberos サーバーを停止し、再始動するには、以下のステップを完了してください。

1. 文字ベース・インターフェースにおいて、コマンド行で `call QP2TERM` と入力する。このコマンドは、ユーザーが i5/OS PASE アプリケーションを処理できるようにする対話式シェル環境をオープンします。
2. コマンド行で `export PATH=$PATH:/usr/krb5/sbin` と入力する。このコマンドは、実行可能ファイルを実行するために必要な Kerberos スクリプトを指します。
3. コマンド行で、`stop.krb5` と入力します。このコマンドは、Kerberos サーバーを停止します。
4. コマンド行で、`start.krb5` と入力します。このコマンドは、Kerberos サーバーを開始します。

Windows 2000、Windows XP、および Windows Vista ワークステーションのホスト・プリンシパルの作成

Kerberos が PC ユーザーを認証するために使用するホスト・プリンシパルを作成する必要があります。

既に i5/OS PASE 環境になっている場合は、ステップ 1 および 2 をスキップしてください。ワークステーションごとに、ホスト・プリンシパルを作成するための以下の手順を完了します。

1. 文字ベース・インターフェースにおいて、コマンド行で `call QP2TERM` と入力する。このコマンドは、ユーザーが i5/OS PASE アプリケーションを処理できるようにする対話式シェル環境をオープンします。
2. コマンド行で `export PATH=$PATH:/usr/krb5/sbin` と入力する。このコマンドは、実行可能ファイルを実行するために必要な Kerberos スクリプトを指します。
3. コマンド行で `kadmin -p admin/admin` と入力し、Enter キーを押す。
4. 管理者のパスワードを使ってサインインする。例えば、`secret`。
5. `kadmin` プロンプトで、`addprinc -pw secret1 host/pc1.myco.com` と入力する。これにより、John Day の PC 用のホスト・プリンシパルが作成されます。
6. `kadmin` プロンプトで、`addprinc -pw secret2 host/pc2.myco.com` と入力する。これにより、Karen Jones の PC 用のホスト・プリンシパルが作成されます。
7. `quit` と入力して、`kadmin` インターフェースを終了する。

Kerberos サーバーでのユーザー・プリンシパルの作成

ご使用のネットワーク内のサービスに対してユーザーを認証する必要がある場合、それらのユーザーをプリンシパルとして Kerberos サーバーに追加する必要があります。

プリンシパルとは、ユーザー名とパスワードを意味する Kerberos 用語です。これらのプリンシパルは Kerberos サーバー上に保管され、ネットワーク内のユーザーの検証を行うために使用されます。ユーザーのプリンシパルを作成するには、以下のステップを実行してください。

1. 文字ベース・インターフェースにおいて、コマンド行で `call QP2TERM` と入力します。このコマンドは、ユーザーが i5/OS PASE アプリケーションを処理できるようにする対話式シェル環境をオープンします。
2. コマンド行で `export PATH=$PATH:/usr/krb5/sbin` と入力する。このコマンドは、実行可能ファイルを実行するために必要な Kerberos スクリプトを指します。
3. コマンド行で `kadmin -p admin/admin` と入力し、Enter キーを押す。
4. 管理者のパスワードを使ってサインインする。例えば、`secret`。
5. `kadmin` プロンプトで、`addprinc -pw 123day day` と入力する。

上記の手順を完了した後、次のようなメッセージが表示されます。

プリンシパル "day@MYCO.COM" が作成されました。(Principal "day@MYCO.COM" created.)

これにより、John Day 用のユーザー・プリンシパルが作成されます。

これらのステップを Karen Jones についても繰り返しますが、プリンシパル名は `jones`、パスワードは `123jones` を指定します。

システム A サービス・プリンシパルの Kerberos サーバーへの追加

Kerberos チケットを受信する i5/OS インターフェースごとに、それらを Kerberos サーバーに対してプリンシパルとして追加する必要があります。

サービス・プリンシパルを追加するには、以下のステップを踏んでください。既に `kadmin` 環境になっている場合は、ステップ 1 から 4 をスキップしてください。

1. 文字ベース・インターフェースにおいて、コマンド行で `call QP2TERM` と入力します。このコマンドは、ユーザーが i5/OS PASE アプリケーションを処理できるようにする対話式シェル環境をオープンします。
2. コマンド行で `export PATH=$PATH:/usr/krb5/sbin` と入力する。このコマンドは、実行可能ファイルを実行するために必要な Kerberos スクリプトを指します。
3. コマンド行で `kadmin -p admin/admin` と入力し、Enter キーを押す。
4. 管理者のパスワードを使ってサインインする。例えば、`secret`。
5. `kadmin` プロンプトで、`addprinc -pw systema123 krbsvr400/systema.myco.com` と入力する。次のように表現されたメッセージを受け取る。
プリンシパル "krbsvr400/systema.myco.com@MYCO.COM" が作成されました。
6. `quit` と入力して `kadmin` インターフェースを終了し、F3 (終了) を押して PASE 環境を終了する。

Windows 2000、Windows XP、および Windows Vista ワークステーションの構成

i5/OS PASE において Kerberos サーバーを構成する場合、このステップはオプションです。Kerberos サーバーの構成後にシングル・サインオン環境を作成する予定がある場合は、このステップを完了する必要があります。そうでない場合は、ステップ 9 (ネットワーク認証サービスの構成) にスキップします。

Kerberos レalmおよび Kerberos サーバーをワークステーション上で設定することにより、クライアント・ワークステーションをワークグループの一部として構成します。このワークステーションに関連づけられるパスワードも設定する必要があります。

ワークステーションを構成するには、以下の手順を完了してください。

1. Windows 2000 ワークステーションのコマンド・プロンプトから、以下のように入力する。

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

2. Windows 2000 ワークステーションのコマンド・プロンプトで以下のように入力することにより、ローカル・マシン・アカウント・パスワードを設定する。

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

3. John Day の Kerberos ユーザー・プリンシパル (day@MYCO.COM) を彼の Windows 2000 ユーザー名 (johnday) にマップする。Windows 2000 ワークステーション・コマンド・プロンプトで以下のように入力します。

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

4. John Day の Kerberos ユーザー・プリンシパルが彼の Windows 2000 ユーザー名にマップしていることを検証するために、Windows 2000 ワークステーション・コマンド・プロンプトで次のように入力する。

```
C:> ksetup
```

そして結果を表示します。

5. 変更を有効にするために、PC を再始動します。
6. この手順を Karen Jones のワークステーションについても繰り返しますが、以下の情報を指定します。
 - ローカル・マシン・アカウント・パスワード: secret2
 - Kerberos ユーザー・プリンシパル: jones@MYCO.COM
 - Windows 2000 ユーザー名: karenjones

関連概念

シナリオ: シングル・サインオンのテスト環境の作成

ネットワーク認証サービスの構成

ネットワーク認証サービスを構成するには、以下の手順を実行します。

1. System i ナビゲーター で、「システム A」 → 「セキュリティ」 と展開する。
2. 「ネットワーク認証サービス」を右クリックし、「構成」を選択して構成ウィザードを開始する。

注: ネットワーク認証サービスを構成した後では、このオプションは「再構成」になります。

3. ウィザードが作成するオブジェクトに関する情報について、「ようこそ」ページを検討する。「次へ」をクリックします。
4. 「レalm情報の指定 (Specify realm information)」ページで、「デフォルト・レalm」フィールドに MYCO.COM を入力する。「次へ」をクリックします。

5. 「KDC 情報の指定 (Specify KDC information)」 ページで、「KDC」フィールドに Kerberos サーバーとして `kdc1.myco.com` を入力し、「ポート」フィールドに `88` を入力する。「次へ」をクリックします。
6. 「パスワード情報の指定 (Specify password information)」 ページで、「いいえ」を選択する。「次へ」をクリックします。
7. 「keytab エントリーの選択」 ページで、「i5/OS Kerberos 認証」を選択する。「次へ」をクリックします。
8. 「i5/OS keytab エントリーの作成 (Create i5/OS keytab entry)」 ページで、パスワードを入力して確認してから、「次へ」をクリックする。例えば、`systema123`。このパスワードは、システム A が Kerberos サーバーに追加されるときに使用されます。
9. 「要約」 ページで、ネットワーク認証サービスの構成の詳細を検討する。「終了」をクリックします。

システム A 上でのユーザーのホーム・ディレクトリーの作成

i5/OS オペレーティング・システムおよび i5/OS アプリケーションに接続するユーザーごとに、`/home` ディレクトリーの中にディレクトリーが必要です。このディレクトリーには、ユーザーの Kerberos 信任状キャッシュの名前が入っています。

システム A 上にユーザーのホーム・ディレクトリーを作成するために、以下の手順を実行してください。

1. i5/OS コマンド行で、`CRTDIR '/home/user profile'` と入力します。ここで `user profile` は、ユーザーの i5/OS ユーザー・プロファイル名です。例えば、ユーザー John Day の場合は `CRTDIR '/home/JOHND'` です。
2. このコマンドを Karen Jones についても繰り返しますが、彼女の i5/OS ユーザー・プロファイルである `KARENJ` を指定します。

ネットワーク認証サービスのテスト

ネットワーク内の i5/OS プリンシパルおよびその他のプリンシパル用のチケット許可チケットを要求して、ネットワーク認証サービス構成をテストします。

注: このテストを行う前に、必ず i5/OS ユーザー・プロファイル用のホーム・ディレクトリーを作成しておいてください。

ネットワーク認証サービス構成をテストするには、以下の手順を行います。

1. コマンド行で `QSH` と入力して、`Qshell` インタープリターを開始する。
2. `keytab list` と入力して、`keytab` ファイルに登録されているプリンシパルのリストを表示する。次の結果が表示されるはずですが。

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

3. `kinit -k krbsvr400/systema.myco.com@MYCO.COM` と入力して、Kerberos サーバーからチケット許可チケットを要求する。このコマンドは、ご使用のシステムが正しく構成されており、`keytab` ファイル内のパスワードが Kerberos サーバーに保管されているパスワードと一致することを検証します。正しく入力されれば、`QSH` コマンドがエラーなしに表示されます。
4. `klist` と入力し、デフォルトのプリンシパルが `krbsvr400/systema.myco.com@MYCO.COM` であることを検証する。このコマンドにより、Kerberos 信任状キャッシュの内容が表示され、i5/OS サービス・プリンシパルに有効な許可証が作成され、かつシステムの信任状キャッシュに入れられていることが検査されます。

```
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
```

```
$
```

ご使用のシステムを Kerberos サーバーに構成するために必要な手順は完了しました。Kerberos を使用して、MYCO.COM レルム内のユーザーの認証を行うことができます。

シナリオ: ネットワーク認証サービスの構成

ご使用のネットワークにネットワーク認証サービスを追加する場合の前提条件と目的を、以下で説明します。

状況

貴方は、自社の受注部門のネットワークを管理するネットワーク管理者です。最近、ネットワークに System i 製品を追加して、いくつかのアプリケーションを自分の部門に配置しました。ネットワークでは、Microsoft Windows 2000 上の Microsoft Active Directory を使用してユーザーを管理します。現在、すべてのユーザーが Microsoft Windows 2000 オペレーティング・システムを稼働させているワークステーションを持っています。Generic Security Service (GSS) API を使用する独自の Kerberos 使用可能アプリケーションがあります。

このシナリオには、以下の利点があります。

- ユーザーの認証プロセスを単純化する。
- ネットワーク内のシステムへのアクセス管理のオーバーヘッドを軽減する。
- パスワードが盗まれる危険性を最小に抑える。

目的

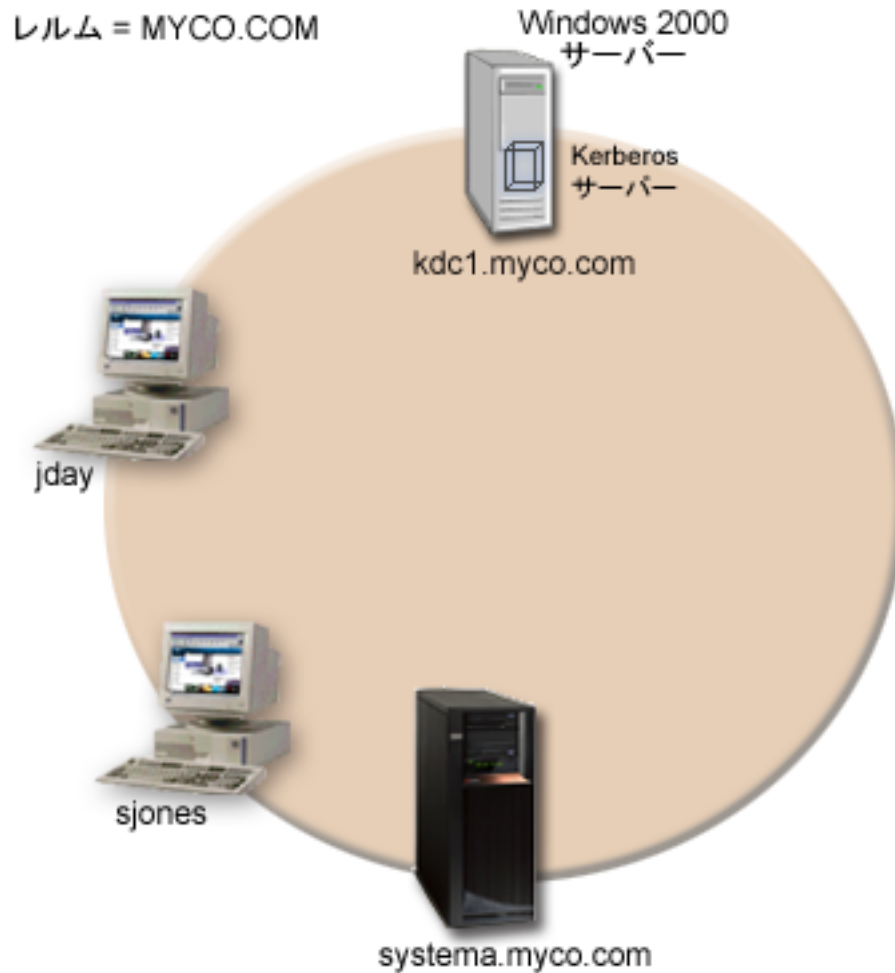
このシナリオでは、MyCo, Inc. は、Windows 2000 サーバーが Kerberos サーバーとしての役割を果たす既存のレルムに、System i 製品を追加しようとしています。System i プラットフォームには、正しいユーザーによりアクセスされる必要があるクリティカルなビジネス・アプリケーションがいくつか含まれています。ユーザーがこれらのアプリケーションへのアクセス権を取得するには、Kerberos サーバーにより認証される必要があります。

このシナリオの目的は、次のとおりです。

- System i プラットフォームが既存の Kerberos サーバーに参加できるようにする。
- ネットワーク内でプリンシパル名およびユーザー名の両方を許可する。
- Kerberos ユーザーが Kerberos サーバー上の自分のパスワードを変更できるようにする。

詳細

次の図は、MyCo ネットワークの特性を示しています。



システム A

- 次のオプションおよびライセンス・プログラムがインストールされている i5/OS V5R3 またはそれ以降を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12 または 5761-SS1 オプション 12)
 - Qshell インタープリター (5722-SS1 オプション 30 または 5761-SS1 オプション 30)
 - System i Access for Windows (5722-XE1 または 5761-XE1)
 - Network Authentication Enablement (5722-NAE または 5761-NAE) (V5R4 以降を使用している場合)
 - Cryptographic Access Provider (5722-AC3) (V5R3 を実行している場合)
- システム A のプリンシパル名は `krbsvr400/systema.myco.com@MYCO.COM` です。

Windows 2000 サーバー

- MYCO.COM レルムの Kerberos サーバーとしての役割を果たす。

- Kerberos サーバーの完全修飾ホスト名は、 kdc1.myco.com。

クライアント PC

- Windows 2000 を稼働させている。
- ネットワーク認証サービスを管理するのに使用される PC には、以下の製品がインストールされている。
 - System i Access for Windows (5722-XE1 または 5761-XE1)
 - System i ナビゲーター およびセキュリティーのサブコンポーネントとネットワークのサブコンポーネント。

前提条件および前提事項

1. ソフトウェアおよびオペレーティング・システムのインストールを含むすべてのシステム要件は、検証済みである。

必要なライセンス・プログラムがインストール済みであることを検証するには、以下の手順に従います。

- a. System i ナビゲーターで、「システム」 → 「構成およびサービス」 → 「ソフトウェア」 → 「インストール済みプロダクト」を展開する。
 - b. すべてのライセンス・プログラムがインストール済みであることを確認する。
2. 必要なハードウェアの計画とセットアップはすべて完了している。
 3. これらのサーバーのそれぞれにおいて、TCP/IP および基本的なシステム・セキュリティーが構成されており、テスト済みである。
 4. 単一の DNS サーバーが、ネットワークのホスト名解決に使用される。ホスト・テーブルは、ホスト名解決には使用されません。

注: Kerberos 認証でホスト・テーブルを使用すると、名前解決エラーまたはその他の問題が生じることがあります。Kerberos 認証でホスト名解決がどのように行われるかの詳細については、93 ページの『ホスト名解決の考慮事項』を参照してください。

構成手順

ご使用のシステム上でネットワーク認証サービスを構成するには、以下の手順を実行します。

計画ワークシートの完成

ネットワーク認証サービスを構成する前に、以下の作業計画シートに記入してください。

ネットワーク認証サービスのセットアップを進める前に、前提条件ワークシートのすべてに「はい」と回答する必要があります。

表 4. 前提条件ワークシート

質問	回答
ご使用の i5/OS は、V5R3、またはそれ以降 (5722-SS1)、あるいは V6R1 (5761-SS1) であるか ?	はい

表 4. 前提条件ワークシート (続き)

質問	回答
以下のライセンス・プログラムがシステム A にインストールされているか？ <ul style="list-style-type: none"> • i5/OS Host Servers (5722-SS1 オプション 12 または 5761-SS1 オプション 12) • Qshell インタープリター (5722-SS1 オプション 30 または 5761-SS1 オプション 30) • System i Access for Windows (5722-XE1 または 5761-XE1) • Network Authentication Enablement (5722-NAE または 5761-NAE) (i5/OS V5R4 以降を使用している場合) • Cryptographic Access Provider (5722-AC3) (i5/OS V5R3 を実行している場合) 	はい
ご使用の PC に、Windows 2000 がインストールされているか？	はい
管理者の PC に System i Access for Windows (5722-XE1 または 5761-XE1) はインストール済みですか？	はい
System i ナビゲーター が管理者の PC にインストールされているか？ <ul style="list-style-type: none"> • 管理者の PC に System i ナビゲーター のセキュリティー・サブコンポーネントはインストール済みですか？ • 管理者の PC に System i ナビゲーター のネットワーク・サブコンポーネントはインストール済みですか？ 	はいはいはい
最新の System i Access for Windows サービス・パックをインストール済みですか？ 最新の Service Pack については、System i Access  を参照してください。	はい
*SECADM、*ALLOBJ、および *IOSYSCFG の特殊権限を持っているか？	はい
以下のいずれかを、Kerberos サーバーとしての役割を果たすセキュア・システムにインストールしてあるか？ インストールされていれば、どれか？ <ol style="list-style-type: none"> 1. Windows 2000 サーバー 2. Windows サーバー 2003 3. AIX サーバー 4. i5/OS PASE (V5R3 以降) 5. z/OS 	はい、Windows 2000 サーバー
ネットワーク内のすべての PC が Windows 2000 ドメインに構成されているか？ 注: Windows 2000 ドメインは、Kerberos レルムと同様です。Microsoft Active Directory は、Kerberos 認証をデフォルトのセキュリティー・メカニズムとして使用します。	はい
最新のプログラム一時修正 (PTF) を適用してあるか？	はい
System i システム時刻と Kerberos サーバーのシステム時刻との差が 5 分以内か？ そうでない場合は、114 ページの『システム時刻の同期化』を参照。	はい

表 5. ネットワーク認証サービス計画ワークシート

質問	回答
ご使用のシステムが属する Kerberos のデフォルト・レルムの名前は何かですか？ 注: Windows 2000 ドメインは、Kerberos レルムと同様です。Microsoft Active Directory は、Kerberos 認証をデフォルトのセキュリティー・メカニズムとして使用します。	MYCO.COM
Microsoft Active Directory を使用しているか？	はい

表 5. ネットワーク認証サービス計画ワークシート (続き)

質問	回答
Kerberos デフォルト・レルムの Kerberos サーバーは ? Kerberos サーバーが listen するポートは ?	KDC: kdc1.myco.com ポート: 88 注: これは、Kerberos サーバーのデフォルト・ポートです。
このデフォルト・レルムにパスワード・サーバーを構成したいか ? 「はい」であれば、以下の質問に回答してください。 この Kerberos サーバーのパスワード・サーバーの名前は ? パスワード・サーバーが listen するポートは ?	はい パスワード・サーバー: kdc1.myco.com ポート: 464 注: これは、パスワード・サーバーのデフォルト・ポートです。
どのサービス用に keytab エントリーを作成したいか ? <ul style="list-style-type: none"> • i5/OS Kerberos 認証 • LDAP • IBM HTTP Server • i5/OS NetServer • ネットワーク・ファイルシステムのサーバー 	i5/OS Kerberos 認証
i5/OS サービス・プリンシパル用に使用したいパスワードは ?	systema123
Microsoft Active Directory へのサービス・プリンシパルの追加を自動化するバッチ・ファイルを作成したいか ?	はい
John Day と Sharon Jones の i5/OS ユーザー・プロファイル名は ?	JOHND SHARONJ

システム A 上でのネットワーク認証サービスの構成

ネットワーク認証サービスを構成するには、以下の手順に従います。

1. System i ナビゲーター で、「システム A」 → 「セキュリティ」と展開する。
2. 「ネットワーク認証サービス」を右クリックし、「構成」を選択して構成ウィザードを開始する。

注: ネットワーク認証サービスを構成した後では、このオプションは「再構成」になります。
3. ウィザードが作成するオブジェクトに関する情報について、「よろこそ」ページを検討する。「次へ」をクリックします。
4. 「レルム情報の指定 (Specify realm information)」ページで、「デフォルト・レルム」フィールドに MYCO.COM を入力し、「Microsoft Active Directory を Kerberos 認証に使用する (Microsoft Active Directory is used for Kerberos authentication)」を選択する。「次へ」をクリックします。
5. 「KDC 情報の指定 (Specify KDC information)」ページで、「KDC」フィールドに Kerberos サーバーとして kdc1.myco.com を入力し、「ポート」フィールドに 88 を入力する。「次へ」をクリックします。
6. 「パスワード情報の指定 (Specify password information)」ページで、「はい」を選択する。「パスワード・サーバー」フィールドに kdc1.myco.com を入力し、「ポート」フィールドに 464 を入力します。「次へ」をクリックします。
7. 「keytab エントリーの選択」ページで、「i5/OS Kerberos 認証」を選択する。「次へ」をクリックします。

8. 「i5/OS keytab エントリーの作成 (Create i5/OS keytab entry)」 ページで、パスワードを入力して確認する。例えば、systema123。このパスワードは、システム A が Kerberos サーバーに追加されるときに使用されます。「次へ」をクリックします。
 9. オプション: 「バッチ・ファイルの作成 (Create batch file)」 ページで、このファイルを作成するために「はい」を選択し、以下の情報を指定する。
 - 「バッチ・ファイル (Batch file)」: テキスト systema を、デフォルトのバッチ・ファイル名の終わりに追加する。例えば、C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystema.bat
 - 「パスワードの組み込み (Include password)」を選択する。この結果、i5/OS サービス・プリンシパルに関連するパスワードは、すべてバッチ・ファイルに組み込まれます。パスワードは平文で表示され、バッチ・ファイルに対する読み取りアクセスを持っていれば誰でも読み取れる、ということに注意することが重要です。したがって、バッチ・ファイルは、使用した後に Kerberos サーバーと PC から削除することをお勧めします。
- 注: あるいは、ウィザードにより生成されるサービス・プリンシパルを手動で Kerberos サーバーに追加することもできます。i5/OS サービス・プリンシパルを Kerberos サーバーに手動で追加する方法を知りたい場合には、110 ページの『Kerberos サーバーへの i5/OS プリンシパルの追加』を参照してください。
10. 「要約」 ページで、ネットワーク認証サービスの構成の詳細を検討する。「終了」をクリックします。

システム A プリンシパルの Kerberos サーバーへの追加

i5/OS サービス・プリンシパルを Kerberos サーバーに手動で追加できます。このシナリオで説明するように、ステップ 2 で作成したバッチ・ファイルを使用して、プリンシパルを追加することもすることもできます。

バッチ・ファイルを使用するには、ファイル転送プロトコル (FTP) を使用してそれを Kerberos サーバーにコピーして実行する必要があります。バッチ・ファイルを使用して Kerberos サーバーにプリンシパルを追加するには、以下の手順を行います。

1. ウィザードによって作成されたバッチ・ファイルを FTP でファイル転送する
 - a. 管理者がネットワーク認証サービスを構成するために使用した Windows 2000 ワークステーション上で、コマンド・プロンプトをオープンし、ftp kdc1.myco.com と入力する。これにより FTP セッションが PC 上で開始されます。管理者のユーザー名とパスワードを求めるプロンプトが出されません。
 - b. FTP プロンプトで lcd "C:¥Documents and Settings¥All Users¥Documents¥IBM¥Client Access" と入力する。Enter キーを押します。メッセージ「現在のローカル・ディレクトリーは C:¥Documents and Settings¥All Users¥Documents¥IBM¥Client Access (Local directory now C:¥Documents and Settings¥All Users¥Documents¥IBM¥Client Access)」を受け取るはずです。
 - c. FTP プロンプトで binary と入力する。これは、転送されるファイルがバイナリーであることを示します。
 - d. FTP プロンプトで cd ¥mydirectory と入力する。ここで mydirectory は、kdc1.myco.com 上にあるディレクトリーです。
 - e. FTP プロンプトで put NASConfigsystema.bat と入力する。メッセージ「226 転送が完了しました (226 Transfer complete)」を受け取るはずです。
2. kdc1.myco.com 上でバッチ・ファイルを実行する
 - a. Windows 2000 サーバー上で、バッチ・ファイルを転送したフォルダーをオープンする。
 - b. NASConfigsystema.bat ファイルを見つけ、それをダブルクリックして、実行します。

- c. ファイルの実行後、次の手順を行って、i5/OS プリンシパルが Kerberos サーバーに追加されたことを検査します。

- 1) Windows 2000 サーバー上で、「スタート」 → 「プログラム」 → 「管理ツール」 → 「Active Directory ユーザーとコンピュータ」 → 「ユーザー」と展開する。
- 2) 該当する Windows ドメインを選択して、システムにユーザー・アカウントがあることを検査します。

注: この Windows ドメインは、ネットワーク認証サービス構成に指定したデフォルト・レルム名と同じでなければなりません。

- 3) 表示されたユーザーのリストで、**systema_1_krbsvr400** を見つけます。これは、i5/OS プリンシパル名に生成されたユーザー・アカウントです。
- 4) オプション: Active Directory ユーザーのプロパティにアクセスします。「アカウント」タブから、「アカウントの委任は承認されています (Account is trusted for delegation)」を選択します。

注: このオプションのステップは、ご使用のシステムがユーザーの信任状を他のシステムに委任または転送することができるようにします。その結果、i5/OS サービス・プリンシパルは、ユーザーに代わって複数のシステムのサービスにアクセスすることができます。これは、多重階層ネットワークにおいて役立ちます。

システム A 上でのユーザーのホーム・ディレクトリーの作成

i5/OS および i5/OS アプリケーションに接続する各ユーザーには、/ホーム・ディレクトリーのディレクトリーが必要です。このディレクトリーには、ユーザーの Kerberos 信任状キャッシュの名前が入っています。

ユーザーのホーム・ディレクトリーを作成するには、以下の手順を実行してください。

1. i5/OS コマンド行で CRTDIR '/home/user profile' と入力します。ここで、user profile は、ユーザーの i5/OS ユーザー・プロファイル名です。例えば、ユーザー John Day の場合は CRTDIR '/home/JOHND' です。
2. このコマンドを Sharon Jones についても繰り返しますが、彼女の i5/OS ユーザー・プロファイルである SHARONJ を指定します。

システム A 上でのネットワーク認証サービスのテスト

システム A プリンシパルのチケット許可チケットを要求して、ネットワーク認証サービスが正常に構成されていることを検証します。

ネットワーク認証サービスをテストするには、以下の手順を行います。

1. コマンド行で QSH と入力して、Qshell インタープリターを開始する。
2. keytab list と入力して、keytab ファイルに登録されているプリンシパルのリストを表示する。次の結果が表示されるはずですが。

```
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. kinit -k krbsvr400/systema.myc.com@MYCO.COM と入力して、Kerberos サーバーからチケット許可チケットを要求する。このコマンドは、ご使用のシステムが正しく構成されており、keytab ファイル内

のパスワードが Kerberos サーバーに保管されているパスワードと一致することを検証します。正しく入力されれば、QSH コマンドがエラーなしに表示されます。

4. klist と入力し、デフォルトのプリンシパルが `krbsvr400/systema.myco.com@MYCO.COM` であることを検証する。このコマンドにより、Kerberos 信任状キャッシュの内容が表示され、i5/OS サービス・プリンシパルに有効な許可証が作成され、かつシステムの信任状キャッシュに入れられていることが検査されます。

```
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
$
```

システム A 上でネットワーク認証サービスを構成するために必要なタスクが完了しました。

シナリオ: レルム間の信頼関係のセットアップ

ネットワーク上にレルム間の信頼関係をセットアップするための前提条件と目的を以下で説明します。

状況

貴方は大規模な卸会社のセキュリティ管理者です。現在、貴方は受注部門と出荷部門の従業員によって使用されるシステムのセキュリティを管理しています。貴方は受注部門用の Kerberos サーバーを構成しました。受注部門の System i 環境には、その Kerberos サーバーを指すネットワーク認証サービスを構成しました。出荷部門は、i5/OS PASE 内に構成された Kerberos サーバーを持つ System i 製品からなります。この System i 製品上でも、i5/OS PASE 内の Kerberos サーバーを指すネットワーク認証サービスを構成しました。

双方のレルムのユーザーは各部門にあるシステムに保管されているサービスを使用する必要があるため、ユーザーがどちらの Kerberos レルムにいるかに関係なく、各部門の双方の Kerberos サーバーがユーザーを認証できるようにする必要があります。

目的

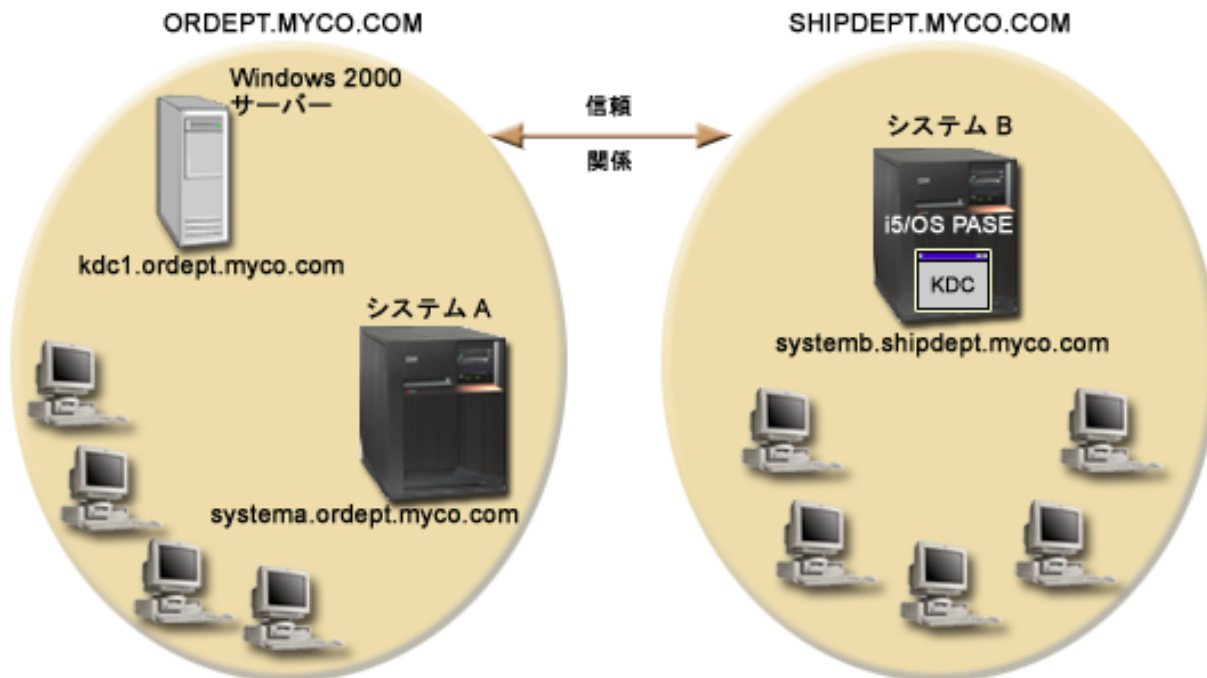
このシナリオでは、MyCo, Inc. は、2 つの既存の Kerberos レルム間の信頼関係を確立しようとしています。一方のレルムは、受注部門用の Kerberos サーバーとしての役割を果たす Windows 2000 サーバーからなります。このサーバーは、受注部門内のユーザーを System i プラットフォーム上にあるサービスに対して認証します。他方のレルムは、1 つの System i プラットフォーム上の i5/OS PASE 内に構成される Kerberos サーバーからなり、出荷部門内のユーザーに対してサービスを提供します。ユーザーは、両方の部門のサービスに対して認証される必要があります。

このシナリオの目的は、次のとおりです。

- 各ネットワーク上のクライアントおよびホストに、他方のネットワークに対するアクセスを与える
- ネットワーク間の認証を単純化する
- 双方のネットワークでユーザーおよびサービスのチケット委任を可能にする

詳細

この環境の接続形態およびすべての主要な要素とそれら相互の関係を示す図を含む、このシナリオが記述している環境の詳細な説明。



受注部門

システム A

- 次のオプションおよびライセンス・プログラムがインストールされている i5/OS V5R3 またはそれ以降を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12 または 5761-SS1 オプション 12)
 - System i Access for Windows (5722-XE1 または 5761-XE1)
 - Network Authentication Enablement (5722-NAE または 5761-NAE) (i5/OS V5R4 以降を使用している場合)
 - Cryptographic Access Provider (5722-AC3) (i5/OS V5R3 を実行している場合)
- レルム ORDEPT.MYCO.COM に参加するために、ネットワーク認証サービスが構成済み。i5/OS プリンシパル `krbsrv400/systema.ordept.myco.com@ORDEPT.MYCO.COM` が Windows 2000 ドメインに追加済み。
- システム A は完全修飾ホスト名 `systema.ordept.myco.com` を持つ。

Windows 2000 サーバー

- レルム ORDEPT.MYCO.COM の Kerberos サーバーとしての役割を果たす。
- DNS ホスト名は `kdc1.ordept.myco.com`。
- 受注部門内の各ユーザーは、プリンシパル名とパスワードで Windows 2000 サーバー上の Microsoft Active Directory に定義済み。

クライアント PC

- Windows 2000 オペレーティング・システムを稼働させている。
- ネットワーク認証サービスを管理するのに使用される PC には、以下の製品がインストールされている。
 - System i Access for Windows (5722-XE1 または 5761-XE1)

- System i ナビゲーターおよび以下のサブコンポーネント:
 - セキュリティー
 - ネットワーク

出荷部門

システム B

- 次のオプションおよびライセンス・プログラムがインストールされている i5/OS V5R3 を実行します。
 - i5/OS PASE (5722-SS1 オプション 33)
 - Cryptographic Access Provider (5722-AC3)
 - System i Access for Windows (5722-XE1)
- i5/OS PASE 内にレルム SHIPDEPT.MYCO.COM で Kerberos サーバーが構成済み。
- レルム SHIPDEPT.MYCO.COM に参加するために、ネットワーク認証サービスが構成済み。i5/OS プリンシパル krsrv400/systemb.shipdept.myco.com@SHIPDEPT.MYCO.COM が i5/OS PASE Kerberos サーバーに追加済み。
- システム B と i5/OS PASE Kerberos サーバーの両方は、完全修飾ホスト名 systemb.shipdept.myco.com を共用。
- 出荷部門内の各ユーザーは、プリンシパル名とパスワードで i5/OS PASE Kerberos サーバーに定義済み。

クライアント PC

- Windows 2000 オペレーティング・システムを稼働させている。
- ネットワーク認証サービスを管理するのに使用される PC には、以下の製品がインストールされている。
 - System i Access for Windows (5722-XE1 または 5761-XE1)
 - System i ナビゲーターおよび以下のサブコンポーネント:
 - セキュリティー
 - ネットワーク

前提条件および前提事項

このシナリオでは、2 つの既存の Kerberos レルム間の信頼関係の確立に関与するタスクに焦点を当てるために、以下の前提事項を設定しています。

システム A 前提条件

1. ソフトウェアおよびオペレーティング・システムのインストールを含むすべてのシステム要件は、検証済みである。

必要なライセンス・プログラムがインストール済みであることを検証するには、以下の手順に従います。

- a. System i ナビゲーターで、「システム」→「構成およびサービス」→「ソフトウェア」→「インストール済みプロダクト」を展開する。
 - b. すべてのライセンス・プログラムがインストール済みであることを確認する。
2. 必要なハードウェアの計画とセットアップはすべて完了している。
 3. システム A で、TCP/IP および基本的なシステム・セキュリティが構成されており、テスト済みである。

- ネットワーク認証サービスが構成されており、テスト済みである。
- 単一の DNS サーバーが、ネットワークのホスト名解決に使用される。ホスト・テーブルは、ホスト名解決には使用されません。

注: Kerberos 認証でホスト・テーブルを使用すると、名前解決エラーまたはその他の問題が生じることがあります。Kerberos 認証でホスト名解決がどのように行われるかの詳細については、93 ページの『ホスト名解決の考慮事項』を参照してください。

システム B 前提条件

- ソフトウェアおよびオペレーティング・システムのインストールを含むすべてのシステム要件は、検証済みである。

必要なライセンス・プログラムがインストール済みであることを検証するには、以下の手順に従います。

- System i ナビゲーターで、「システム」 → 「構成およびサービス」 → 「ソフトウェア」 → 「インストール済みプロダクト」を展開する。
 - すべてのライセンス・プログラムがインストール済みであることを確認する。
- 必要なハードウェアの計画とセットアップはすべて完了している。
 - システムで、TCP/IP および基本的なシステム・セキュリティーが構成されており、テスト済みである。
 - ネットワーク認証サービスが構成されており、テスト済みである。

Windows 2000 サーバー前提条件

- 必要なハードウェアの計画とセットアップはすべて完了している。
- TCP/IP がサーバー上で構成されており、テスト済みである。
- Microsoft Active Directory が構成されており、テスト済みである。
- 受注部門内の各ユーザーは、プリンシパル名とパスワードで Microsoft Active Directory に定義済みである。

構成手順

2 つのレルム間の信頼関係をセットアップするには、以下の手順を完了します。

計画ワークシートの完成


レルム間での信頼性を設定する前に、以下のプランニング用ワークシートに記入してください。

レルム間での信頼性の設定を進める前に、前提条件ワークシートのすべての回答が「はい」になっている必要があります。

表 6. 前提条件計画ワークシート

質問	回答
ご使用の i5/OS は、V5R3、またはそれ以降 (5722-SS1)、あるいは V6R1 (5761-SS1) であるか ?	はい

表 6. 前提条件計画ワークシート (続き)

質問	回答
以下のオプションおよびライセンス・プログラムがシステム A にインストールされているか？ <ul style="list-style-type: none"> • i5/OS Host Servers (5722-SS1 オプション 12 または 5761-SS1 オプション 12) • System i Access for Windows (5722-XE1 または 5761-XE1) • Network Authentication Enablement (5722-NAE または 5761-NAE) (i5/OS V5R4 以降を使用している場合) • Cryptographic Access Provider (5722-AC3) (i5/OS V5R3 を実行している場合) 	はい
以下のライセンス・プログラムがシステム B にインストールされているか？ <ul style="list-style-type: none"> • System i Access for Windows (5722-XE1 または 5761-XE1) • Network Authentication Enablement (5722-NAE または 5761-NAE) (i5/OS V5R4 以降を使用している場合) • Cryptographic Access Provider (5722-AC3) (i5/OS V5R3 を実行している場合) • i5/OS PASE (5722-SS1 オプション 33 または 5761-SS1 オプション 33) 	はい
ご使用のすべての PC に、Windows 2000 がインストールされているか？	はい
ネットワーク認証サービスを管理するために使用される PC に、System i Access for Windows (5722-XE1 または 5761-XE1) がインストールされているか？	はい
ネットワーク認証サービスを管理するために使用される PC に、System i ナビゲーター および以下のサブコンポーネントがインストールされているか？ <ul style="list-style-type: none"> • セキュリティー • ネットワーク 	はい
最新の System i Access for Windows サービス・パックをインストール済みですか？ 最新の Service Pack については、System i Access  を参照してください。	はい
システムで *ALLOBJ 特殊権限を持っているか？	はい
Windows 2000 サーバーで管理権限を持っているか？	はい
DNS を構成してあり、System i プラットフォームと Kerberos サーバーに正しいホスト名があるか？	はい
Kerberos サーバーをどのオペレーティング・システム上に構成したいか？ <ol style="list-style-type: none"> 1. Windows 2000 サーバー 2. Windows サーバー 2003 3. AIX サーバー 4. i5/OS PASE (V5R3 以降) 5. z/OS 	i5/OS PASE
最新のプログラム一時修正 (PTF) を適用してあるか？	はい
System i システム時刻と Kerberos サーバーのシステム時刻との差が 5 分以内か？ そうでない場合は、114 ページの『システム時刻の同期化』を参照。	はい

以下の計画ワークシートは、レルム間の信頼関係のセットアップを開始する前に必要な情報のタイプを示しています。

表7. レルム間の信頼関係用の計画ワークシート

レルム間の信頼関係用の計画ワークシート	回答
信頼関係を確立したいレルムの名前は？ ・ Kerberos サーバーとして Windows 2000 サーバーを使用する Kerberos レルム ・ Kerberos サーバー (i5/OS PASE 内に構成されている) としてシステム B を使用する Kerberos レルム	ORDEPT.MYCO.COM SHIPDEPT.MYCO.COM
すべての i5/OS サービス・プリンシパルおよびユーザー・プリンシパルがそれぞれの Kerberos サーバーに追加されているか？	はい
i5/OS PASE 管理者のデフォルト・ユーザー名は？ i5/OS PASE 管理者に指定したいパスワードは？ 注: これは、i5/OS PASE 内に Kerberos サーバーを作成した時に使用したのと同じパスワードである必要があります。	ユーザー名: admin/admin パスワード : secret
レルム間の信頼関係をセットアップするために使用されるプリンシパルの名前は？ これらの各プリンシパルのそれぞれのパスワードは？	プリンシパル: krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM パスワード: shipord1 プリンシパル: krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO.COM パスワード: shipord2
これらのレルムの Kerberos サーバーのそれぞれの完全修飾ホスト名は？ ・ ORDEPT.MYCO.COM ・ SHIPDEPT.MYCO.COM	kdc1.ordept.myco.comsystemb.shipdept.myco.com
すべてのシステムのシステム時刻の互いの差が 5 分以内か？ そうでない場合は、114 ページの『システム時刻の同期化』を参照。	はい

システム B 上の i5/OS PASE 内で Kerberos サーバーが開始済みであることの確認

レルム間の信頼関係を構成する前に、i5/OS PASE Kerberos サーバーが開始済みであることを確認する必要があります。

i5/OS PASE Kerberos サーバーが開始済みかどうかを判別するためにプロセス統計コマンドを使用します。

1. システム B の文字ベース・インターフェースで `call QP2TERM` と入力する。このコマンドは、ユーザーが i5/OS PASE アプリケーションを処理できる対話式シェル環境をオープンします。
2. コマンド行で `ps -ef | grep krb5` と入力する。このコマンドは、ストリング `krb5` を含むシステム上のプロセスのすべての処理統計を表示することを示します。Kerberos サーバーが実行中であれば、以下の例と同様な結果が表示されるはずです。

```
> 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
$
```

Kerberos サーバーが開始されていない場合は、以下のような結果が表示されるはずです。

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

3. Kerberos サーバーが開始されていない場合は、以下の手順を行います。
 - a. コマンド行で `export PATH=$PATH:/usr/krb5/sbin` と入力し、Enter キーを押す。
 - b. `start.krb5` と入力し、Enter キーを押す。

```
> start.krb5
krb5kdc を始動中 ...
krb5kdc は正常に始動しました。
kadmind を始動中 ...
kadmind は正常に始動しました。
コマンドは正常に完了しました。
$
```

i5/OS PASE Kerberos サーバー上でレルム間の信頼のプリンシパルを作成

i5/OS PASE Kerberos サーバー上でレルム間の信頼のプリンシパルを作成するには、以下のステップを実行します。

1. 文字ベース・インターフェースで `call QP2TERM` と入力する。このコマンドは、ユーザーが i5/OS PASE アプリケーションを処理できるようにする対話式シェル環境をオープンします。
2. コマンド行で `export PATH=$PATH:/usr/krb5/sbin` と入力する。このコマンドは、実行可能ファイルを実行するために必要な Kerberos スクリプトを指します。
3. コマンド行で `kadmin -p admin/admin` と入力し、Enter キーを押す。
4. 管理者のパスワードを使ってサインインする。例えば、`secret`。
5. `kadmin` プロンプトで、`addprinc krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM` と入力する。プリンシパル「`krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM`」のパスワードを入力するよう求めるプロンプトが出される。パスワードとして `shipord1` を入力する。Enter キーを押します。このパスワードを再入力するよう求めるプロンプトが出され、以下のように表現されたメッセージを受け取ります。

```
プリンシパル "krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM" が作成されました。(Principal "krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM" created.)
```

6. `kadmin` プロンプトで、`addprinc krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO.COM` と入力する。プリンシパル「`krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO.COM`」のパスワードを入力するよう求めるプロンプトが出される。パスワードとして `shipord2` を入力する。Enter キーを押します。このパスワードを再入力するよう求めるプロンプトが出され、以下のように表現されたメッセージを受け取ります。

```
プリンシパル "krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO.COM" が作成されました。(Principal "krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO.COM" created.)
```

7. `quit` と入力して `kadmin` インターフェースを終了し、F3 (終了) を押して PASE 環境を終了する。

i5/OS PASE Kerberos サーバーでの暗号化値の変更

Windows ワークステーションとともに作動するためには、Kerberos サーバー・デフォルト暗号化設定値は、クライアントが i5/OS PASE Kerberos サーバーに認証されるように変更する必要があります。

デフォルト暗号化設定値を変更するには、/var/krb5/krb5kdc ディレクトリーにある kdc.conf ファイルを、次の手順を行って編集する必要があります。

1. 文字ベース・インターフェースで `edtf '/var/krb5/krb5kdc/kdc.conf'` と入力して kdc.conf ファイルにアクセスする。
2. kdc.conf ファイルの以下の行を

```
supported_enctypes = des3-cbc-sha1:normal  
arcfour-hmac:normal aes256-cts:normal  
des-cbc-md5:normal des-cbc-crc:normal
```

次のように変更する。

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

SHIPDEPT.MYCO.COM を信頼するように Windows 2000 サーバーを構成

システム B は ORDEPT.MYCO.COM レルムを信頼するように構成されたので、Windows 2000 サーバーが SHIPDEPT.MYCO.COM レルムを信頼するように構成する必要があります。

Windows 2000 サーバーを構成するには、次のステップを実行します。

1. 管理者アカウントを使用して Windows 2000 サーバーにログオンする。
2. 「スタート」メニューから「プログラム」→「管理ツール」→「Active Directory ドメインと信頼」と展開する。
3. 「Active Directory ドメインと信頼」ページで **ORDEPT.MYCO.COM** レルム (場合により Windows インターフェースの中では Windows ドメインとも呼ばれる) を右クリックし、「プロパティ」を選択する。
4. 「信頼」タブで「このドメインが信頼するドメイン」テーブル上の「追加」をクリックする。
5. 「信頼するドメインの追加」ページで、「信頼するドメイン」フィールドに SHIPDEPT.MYCO.COM と入力する。パスワードとして shipord1 を入力する。
6. MYCO.COM ドメインとの連絡が取れないことを示す「Active Directory」ダイアログ・ボックスが表示される。MYCO.COM ドメインは相互運用可能な Windows 以外のドメインであり、このドメイン側から信頼をセットアップしたいので、「OK」をクリックしてダイアログ・ボックスをクローズします。
7. 「信頼」タブで「このドメインを信頼するドメイン」テーブル上の「追加」をクリックする。
8. 「信頼するドメインの追加」ページで、「信頼するドメイン」フィールドに SHIPDEPT.MYCO.COM と入力する。パスワードとして shipord2 を入力する。
9. MYCO.COM ドメインとの連絡が取れないことを示す「Active Directory」ダイアログ・ボックスが表示される。MYCO.COM ドメインは相互運用可能な Windows 以外のドメインであり、このドメイン側から信頼をセットアップしたいので、「OK」をクリックしてダイアログ・ボックスをクローズします。
10. 「OK」をクリックします。

SHIPDEPT.MYCO.COM レルムのシステム A への追加

システム A が、SHIPDEPT.MYCO.COM レルムの中で i5/OS PASE Kerberos サーバーを見つけられる場所を判別できるように、SHIPDEPT.MYCO.COM レルムをシステム A 上で定義する必要があります。

SHIPDEPT.MYCO.COM レalmを定義するには、次のステップを実行します。

1. System i ナビゲーター で、「システム A」 → 「セキュリティー」 → 「ネットワーク認証サービス」と展開する。
2. 「レalm」を右クリックして、「レalmの追加」を選択する。
3. 「レalmの追加」ダイアログ・ボックスで、以下の情報を指定し、「OK」をクリックする。
 - a. 「追加するレalm (Realm to add)」: SHIPDEPT.MYCO.COM
 - b. KDC: systemb.shipdept.myco.com
 - c. 「ポート (Port)」: 88
4. 「レalm」をクリックして、右方のペインにあるレalmのリストを表示する。 SHIPDEPT.MYCO.COM レalmがリストに表示されていることを検証します。

これで、ORDEPT.MYCO.COM レalmと SHIPDEPT.MYCO.COM レalmの間のレalm間信頼関係を構成する手順が完了しました。

シナリオ: 複数システムにわたるネットワーク認証サービス構成の伝搬

複数のシステムにわたってネットワーク認証サービス構成を伝搬させる場合の前提条件と目的を、以下で説明します。

状況

貴方は、大規模な自動車部品メーカーのシステム管理者です。現在、System i ナビゲーター 付きの System i プラットフォームを 5 つ管理しています。1 つのシステムがセントラル・システムとして作動し、データを保管して他のシステムを管理しています。貴方の会社のセキュリティー管理者は、ユーザーをエンタープライズに対して認証するネットワーク認証サービスを、Windows 2000 ドメインに参加する新しいシステム上で構成したばかりです。セキュリティー管理者はこのシステム上でネットワーク認証サービスをテストし、この System i プラットフォーム用のサービス・チケットを正常に入手しました。貴方が管理するこれらのシステム間で、ネットワーク認証サービスの構成を単純化したいものとします。

「機能の同期化」ウィザードを使用して、モデル・システムからネットワーク認証サービス構成を取得し、これを他のシステムに適用します。「機能の同期化」ウィザードにより、各システムを別々に構成する必要がなくなるので、ご使用のネットワーク全体にわたってネットワーク認証サービスの構成がより迅速かつ容易になります。

システムのうち 1 つは OS/400® バージョン 5 リリース 2 (V5R2) を稼働させており、このリリースは「機能の同期化」ウィザードをサポートしないため、V5R2 システムは「ネットワーク認証サービス」ウィザードを使用して構成する必要があります。このシステムは、モデル・システム上の現行のネットワーク認証サービス構成と一致するように構成する必要があります。

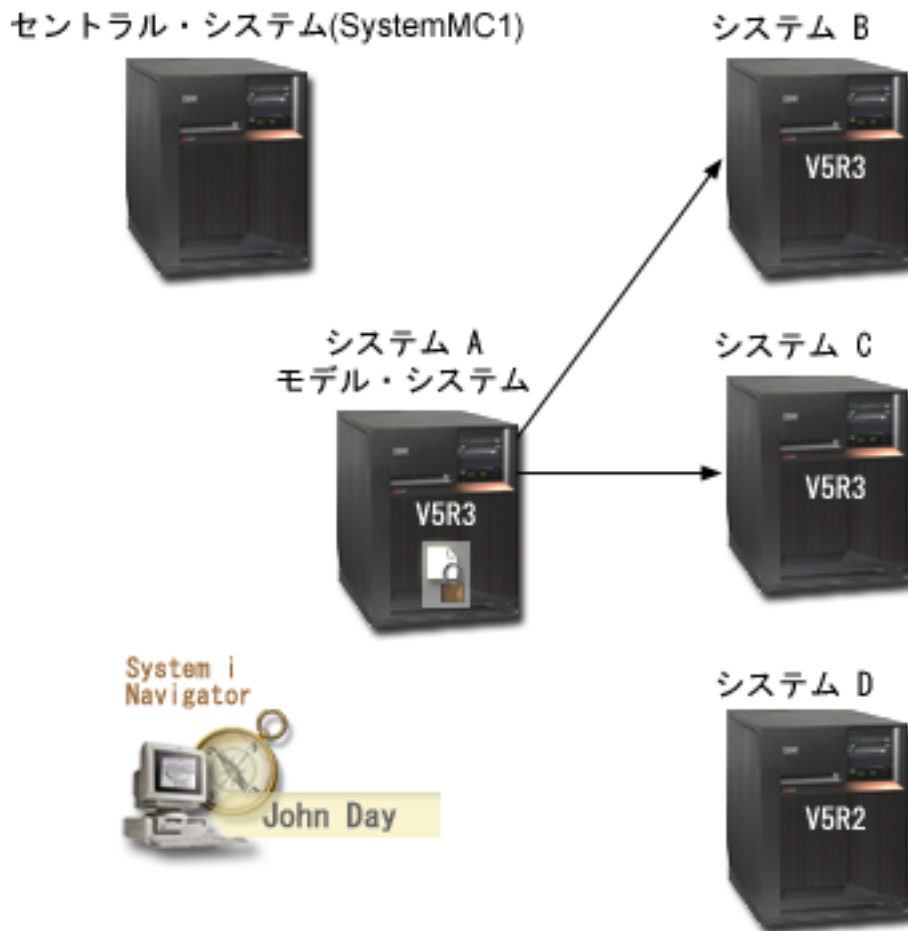
目的

このシナリオでは、MyCo, Inc には次の明確なゴールがあります。

1. ネットワーク内のネットワーク認証サービスの構成を単純化する。
2. すべての System i プラットフォームが同一の Kerberos サーバーを指すようにする。
3. V5R2 システムも同様に Kerberos レalmに参加するよう構成する。

詳細

以下の図は、このシナリオの詳細を示しています。



SystemMC1: セントラル・システム

- 次のオプションおよびライセンス・プログラムがインストールされている i5/OS V5R3 またはそれ以降を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12 または 5761-SS1 オプション 12)
 - System i Access for Windows (5722-XE1 または 5761-XE1)
 - Network Authentication Enablement (5722-NAE または 5761-NAE) (i5/OS V5R4 以降を使用している場合)
 - Cryptographic Access Provider (5722-AC3) (i5/OS V5R3 を実行している場合)
- 各エンドポイント・システムの同期化設定タスクを保管し、スケジュールし、実行する。

システム A: モデル・システム

- 次のオプションおよびライセンス・プログラムがインストールされている i5/OS V5R3 またはそれ以降を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12 または 5761-SS1 オプション 12)
 - System i Access for Windows (5722-XE1 または 5761-XE1)

- Network Authentication Enablement (5722-NAE または 5761-NAE) (i5/OS V5R4 以降を使用している場合)
- Cryptographic Access Provider (5722-AC3) (i5/OS V5R3 を実行している場合)
- エンドポイント・システムに対してネットワーク認証サービス構成を伝搬するモデル・システム。

システム B: エンドポイント・システム

- 次のオプションおよびライセンス・プログラムがインストールされている i5/OS V5R3 またはそれ以降を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12 または 5761-SS1 オプション 12)
 - System i Access for Windows (5722-XE1 または 5761-XE1)
 - Network Authentication Enablement (5722-NAE または 5761-NAE) (i5/OS V5R4 以降を使用している場合)
 - Cryptographic Access Provider (5722-AC3) (i5/OS V5R3 を実行している場合)
- ネットワーク認証サービス構成が伝搬されるエンドポイント・システムの 1 つ

システム C エンドポイント・システム

- 次のオプションおよびライセンス・プログラムがインストールされている i5/OS V5R3 を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12)
 - System i Access for Windows (5722-XE1)
 - Cryptographic Access Provider (5722-AC3)
- ネットワーク認証サービス構成が伝搬されるエンドポイント・システムの 1 つ

システム D エンドポイント・システム

- 次のオプションおよびライセンス・プログラムがインストールされている OS/400 V5R2 を実行します。
 - i5/OS ホスト・サーバー (5722-SS1 オプション 12)
 - iSeries™ Access for Windows (5722-XE1)
 - Cryptographic Access Provider (5722-AC3)
- 以下の V5R2 PTF (プログラム一時修正) が適用済み。
 - SI08977
 - SI08979
- iSeries ナビゲーターの「ネットワーク認証サービス」ウィザードを使用した、個別のネットワーク認証サービスの構成を必要とする。

クライアント PC

- System i Access for Windows (5722-XE1 または 5761-XE1) を実行します。
- 次のサブコンポーネントを備えた System i ナビゲーター を実行します。

注: これらのサブコンポーネントは、ネットワーク認証サービスを管理するのに使用される PC の場合にのみ必要です。

- ネットワーク
- セキュリティ

Windows 2000 サーバー (図には示されていない)

- ネットワーク (kdc1.myco.com) の Kerberos サーバーとして作動する。
- すべてのユーザーが Microsoft Active Directory に追加済み。

注: このシナリオでは、KDC サーバー名 **kdc1.myco.com** という架空の名前を使用しています。

前提条件および前提事項

SystemMC1: セントラル・システムの前提条件

1. ソフトウェアおよびオペレーティング・システムのインストールを含むすべてのシステム要件は、検証済みである。

これらのライセンス・プログラムがインストール済みであることを検証するには、以下の手順に従います。

- a. System i ナビゲーターで、「システム」 → 「構成およびサービス」 → 「ソフトウェア」 → 「インストール済みプロダクト」を展開する。
 - b. すべてのライセンス・プログラムがインストール済みであることを確認する。
2. 必要なハードウェアの計画とセットアップはすべて完了している。
 3. システム A で、TCP/IP および基本的なシステム・セキュリティーが構成されており、テスト済みである。
 4. タスク開始時に「タスク状況」ウィンドウをオープンすることができないように System i ナビゲーター内のデフォルトの設定値が変更されていない。デフォルトの設定値が変更されていないことを検証するには、以下の手順を行います。
 - a. System i ナビゲーターで、「ユーザーのセントラル・システム (*your central system*)」を右クリックし、「ユーザー・プリファレンス (User Preferences)」を選択する。
 - b. 「一般」ページで、「タスクのいずれかが開始する時にタスク状況ウィンドウを自動的にオープンする (Automatically open a task status window when one of my tasks starts)」が選択されていることを検証する。
 5. これらのシステム間のデータ伝送を保護するために Secure Sockets Layer (SSL) が構成されている。

注: ネットワーク認証サービス構成をシステム間で伝搬する場合、パスワードのような機密情報がネットワークを介して送信されます。この情報を保護するために SSL を使用する必要があります。特に、ローカル・エリア・ネットワーク (LAN) の外部へ送られる場合にはそれが必要です。詳細については、『シナリオ: マネージメント・セントラル・サーバーへのすべての接続を SSL で保護 (Scenario: Securing all connections to your Management Central server with SSL)』を参照してください。

システム A: モデル・システムの前提条件

1. このシナリオは、ネットワーク認証サービスがモデル・システム (システム A) 上で正しく構成されていることを前提とする。
2. ソフトウェアおよびオペレーティング・システムのインストールを含むすべてのシステム要件は、検証済みである。

これらのライセンス・プログラムがインストール済みであることを検証するには、以下の手順に従います。

- a. System i ナビゲーターで、「システム」 → 「構成およびサービス」 → 「ソフトウェア」 → 「インストール済みプロダクト」を展開する。
- b. すべてのライセンス・プログラムがインストール済みであることを確認する。

3. 必要なハードウェアの計画とセットアップはすべて完了している。
4. システムで、TCP/IP および基本的なシステム・セキュリティが構成されており、テスト済みである。
5. これらのシステム間のデータ伝送を保護するために Secure Sockets Layer (SSL) が構成されている。

注: ネットワーク認証サービス構成をシステム間で伝搬する場合、パスワードのような機密情報がネットワークを介して送信されます。この情報を保護するために SSL を使用する必要があります。特に、ローカル・エリア・ネットワーク (LAN) の外部へ送られる場合にはそれが必要です。詳細については、『シナリオ: マネージメント・セントラル・サーバーへのすべての接続を SSL で保護 (Scenario: Securing all connections to your Management Central server with SSL)』を参照してください。

システム B、システム C、システム D: エンドポイント・システムの前提条件

1. ソフトウェアおよびオペレーティング・システムのインストールを含むすべてのシステム要件は、検証済みである。

これらのライセンス・プログラムがインストール済みであることを検証するには、以下の手順に従います。

- a. System i ナビゲーターで、「システム」→「構成およびサービス」→「ソフトウェア」→「インストール済みプロダクト」を展開する。
 - b. すべてのライセンス・プログラムがインストール済みであることを確認する。
2. 必要なハードウェアの計画とセットアップはすべて完了している。
 3. システムで、TCP/IP および基本的なシステム・セキュリティが構成されており、テスト済みである。
 4. これらのシステム間のデータ伝送を保護するために Secure Sockets Layer (SSL) が構成されている。

注: ネットワーク認証サービス構成をシステム間で伝搬する場合、パスワードのような機密情報がネットワークを介して送信されます。この情報を保護するために SSL を使用する必要があります。特に、ローカル・エリア・ネットワーク (LAN) の外部へ送られる場合にはそれが必要です。詳細については、『シナリオ: マネージメント・セントラル・サーバーへのすべての接続を SSL で保護 (Scenario: Securing all connections to your Management Central server with SSL)』を参照してください。

Windows 2000 サーバー (図には示されていない)

1. 必要なハードウェアの計画とセットアップはすべて完了している。
2. TCP/IP がサーバー上で構成されており、テスト済みである。
3. Windows ドメインが構成されており、テスト済みである。
4. ネットワーク内のすべてのユーザーが、Active Directory を使用して Windows ドメインに追加済みである。

構成手順

「機能の同期化」ウィザードを使用してネットワーク認証サービス構成をエンドポイント・システムに伝搬するには、以下の手順を実行する必要があります。

計画ワークシートの完成

モデル・システム上の構成を受動システムに伝搬するために System i ナビゲーターの使用を開始するときは、その前に計画ワークシートに記入します。

すべての回答が「はい」になってから、ネットワーク認証サービスの伝搬を進めてください。

表 8. ネットワーク認証サービスの伝搬 - 前提条件ワークシート


前提条件ワークシート	回答
<p>以下のシステムにおいて、i5/OS V5R3 またはそれ以降 (5722-SS1)、または V6R1 (5761-SS1) を使用しているか ?</p> <ul style="list-style-type: none"> • セントラル・システム • システム A • システム B • システム C 	はい
<p>最新のプログラム一時修正 (PTF) を適用してあるか ?</p>	はい
<p>OS/400 V5R2、i5/OS V5R3、またはそれ以降がシステム D で実行されているか ?</p>	はい
<p>システム D について、次のものを含めて最新のプログラム一時修正 (PTF) が適用されているか ?</p> <ul style="list-style-type: none"> • SI08977 • SI08979 	
<p>以下のオプションとライセンス・プログラムが、すべての System i モデルにインストール済みですか?</p> <ul style="list-style-type: none"> • i5/OS Host Servers (5722-SS1 オプション 12 または 5761-SS1 オプション 12) • System i Access for Windows (5722-XE1 または 5761-XE1) • Network Authentication Enablement (5722-NAE または 5761-NAE) (i5/OS V5R4 以降を使用している場合) • Cryptographic Access Provider (5722-AC3) (i5/OS V5R3 を実行している場合) 	はい
<p>管理者の PC に System i Access for Windows (5722-XE1 または 5761-XE1) はインストール済みですか?</p>	はい
<p>管理者の PC に System i ナビゲーター はインストール済みですか?</p> <ul style="list-style-type: none"> • 管理者の PC に System i ナビゲーター のネットワーク・サブコンポーネントはインストール済みですか? • 管理者の PC に System i ナビゲーター のセキュリティー・サブコンポーネントはインストール済みですか? 	はい
<p>最新の IBM System i Access for Windows サービス・パックをインストール済みですか? 最新の Service Pack については、System i Access  を参照してください。</p>	はい
<p>*SECADM、*ALLOBJ、および *IOSYSCFG の特殊権限を持っているか ?</p>	はい

表 8. ネットワーク認証サービスの伝搬 - 前提条件ワークシート (続き)

前提条件ワークシート	回答
<p>Kerberos サーバーとしての役割を果たす以下のいずれかのシステムを持っているか？「はい」の場合、どのシステムか？</p> <ol style="list-style-type: none"> Microsoft Windows 2000 サーバー 注： Microsoft Windows 2000 サーバーは、Kerberos 認証をデフォルトのセキュリティー・メカニズムとして使用します。 Windows サーバー 2003 i5/OS PASE (V5R3 以降) AIX サーバー z/OS 	はい、Windows 2000 サーバー
Windows 2000 サーバーおよび Windows サーバー 2003 の場合、Windows サポート・ツール (ktpass ツールを提供する) がインストールされているか？	はい
System i システム時刻と Kerberos サーバー上のシステム時刻とのずれは 5 分以内ですか？ そうでない場合は、『システム時刻の同期』を参照。	はい

表 9. 同期化機能計画ワークシート

質問	回答
システム・グループの名前は？	MyCo システム・グループ
このシステム・グループに組み込まれるシステムは？	システム B、システム C、システム D
このシステム・グループに伝搬しようと計画している機能は？	ネットワーク認証サービス
<p>どのサービス用に keytab エントリーを作成したいか？</p> <ul style="list-style-type: none"> i5/OS Kerberos 認証 LDAP IBM HTTP Server i5/OS NetServer ネットワーク・ファイルシステムのサーバー 	i5/OS Kerberos 認証
構成を伝搬する対象となるシステムのサービス・プリンシパル名は？	krbsvr400/systema.myco.com@MYCO.COM krbsvr400/systemb.myco.com@MYCO.COM krbsvr400/systemc.myco.com@MYCO.COM krbsvr400/systemd.myco.com@MYCO.COM
これらの各プリンシパルのそれぞれに関連したパスワードは？	システム A、B、C のプリンシパルのパスワードは、systema123 です。システム D 用のプリンシパルのパスワードは systemd123 です。
各 System i プラットフォームそれぞれの完全修飾ホスト名は？	systema.myco.com systemb.myco.com systemc.myco.com systemd.myco.com
<p>Windows 2000 ドメインの名前は？</p> <p>注： Windows 2000 ドメインは、Kerberos レルムと同様です。Microsoft Active Directory は、Kerberos 認証をデフォルトのセキュリティー・メカニズムとして使用します。</p>	MYCO.COM

表 10. システム D 用のネットワーク認証サービス計画ワークシート

質問	回答
<p>ご使用の System i プラットフォームが属する Kerberos のデフォルト・レルムの名前は何か？</p> <p>注: Windows 2000 ドメインは、Kerberos レルムと同様です。Microsoft Active Directory は、Kerberos 認証をデフォルトのセキュリティー・メカニズムとして使用します。</p>	MYCO.COM
Microsoft Active Directory を使用しているか？	はい
<p>Kerberos デフォルト・レルムの Kerberos サーバーは？ Kerberos サーバーが listen するポートは？</p>	<p>KDC: kdc1.myco.com</p> <p>ポート: 88</p> <p>注: これは、Kerberos サーバーのデフォルト・ポートです。</p>
<p>このデフォルト・レルムにパスワード・サーバーを構成したいか？ 「はい」であれば、以下の質問に回答してください。</p> <p>この Kerberos サーバーのパスワード・サーバーの名前は？</p> <p>パスワード・サーバーが listen するポートは？</p>	<p>はい</p> <p>パスワード・サーバー: kdc1.myco.com</p> <p>ポート: 464</p> <p>注: これは、パスワード・サーバーのデフォルト・ポートです。</p>
<p>どのサービス用に keytab エントリーを作成したいか？</p> <ul style="list-style-type: none"> • i5/OS Kerberos 認証 • LDAP • IBM HTTP Server • i5/OS NetServer 	i5/OS Kerberos 認証
ご使用の i5/OS サービス・プリンシパルのパスワードは何ですか？	systemd123

システム・グループの作成

ネットワーク認証サービス構成を受動システムに伝搬する前に、すべてのエンドポイント・システム用のシステム・グループを作成する必要があります。

システム・グループとは、ユーザーが管理でき、同様な設定値と属性 (ネットワーク認証サービス構成など) を適用することができるシステムの集まりです。システム・グループを作成するには、次のステップを実行します。

1. System i ナビゲーターで、「**マネージメント・セントラル (SystemMC1)**」を展開します。
2. 「**システム・グループ**」を右クリックし、新しいシステム・グループを作成するために「**新規システム・グループ**」を選択する。
3. 「一般」ページで、名前のフィールドに MyCo system group と入力し、このシステム・グループの説明を指定する。
4. 「**選択可能なシステム**」リストから、「**システム B**」、「**システム C**」、および「**システム D**」を選択し、「**追加**」をクリックする。これらのシステムが「**選択されたシステム**」リストに追加されます。「**OK**」をクリックします。
5. 「**システム・グループ**」を展開して、ご使用のシステム・グループが追加されたことを検証する。

モデル・システム (システム A) からシステム B およびシステム C へのシステム設定値の伝搬

System i ナビゲーターの機能同期化ウィザードを使用して、複数のエンドポイント・システムにシステム設定を反映させてください。このウィザードは、ネットワーク認証サービス構成などの、システム設定を伝搬することができます。

ネットワーク認証サービス構成を受動システムに伝搬するために、以下のタスクを実行してください。

1. System i ナビゲーターで、「**マネージメント・セントラル (SystemMC1)**」 → 「**システム・グループ**」と展開する。
2. 「**MyCo system group**」を右クリックし、「**システム値**」 → 「**機能の同期化**」を選択する。これにより「**機能の同期化**」ウィザードが立ち上がります。
3. 「ようこそ」ページで、「**機能の同期化**」ウィザードに関する情報を検討し、「**次へ**」をクリックする。「ようこそ」ページには、ウィザード内で後に同期化させるために選択できる機能がリストされません。

注: ネットワーク認証サービス構成をシステム間で伝搬する場合、パスワードのような機密情報がネットワークを介して送信されます。この情報を保護するために SSL を使用する必要があります。特に、ローカル・エリア・ネットワーク (LAN) の外部へ送られる場合にはそれが必要です。詳細については、『シナリオ: マネージメント・セントラル・サーバーへのすべての接続を SSL で保護 (Scenario: Securing all connections to your Management Central server with SSL)』を参照してください。

4. 「モデル・システム」ページで、システム A をモデル・システムとして選択して「**次へ**」をクリックする。このモデル・システムが、他のシステムにネットワーク認証サービス構成を同期化させる際の基本として使用されます。
5. 「受動システムおよびグループ」ページで、「**MyCo system group**」を選択する。「**次へ**」をクリックします。
6. 「更新する内容 (What to Update)」ページで、「**ネットワーク認証サービス (Kerberos)**」を選択する。「**構成を検証する (Verify configuration)**」をクリックします。構成が検証されたら、「**次へ**」をクリックします。

注: ネットワーク認証サービスの検証が正常に終了しなかった場合は、モデル・システムのネットワーク認証サービスの構成に問題がある可能性があります。このエラーをリカバリーするには、モデル・システムで構成を検査し、構成を修正してからこの説明のステップ 2 に戻る必要があります。

7. 「ネットワーク認証サービス」ページで、「**i5/OS Kerberos 認証**」を選択し、「**パスワード (Password)**」フィールドと「**パスワードの確認 (Confirm password)**」フィールドに systema123 と入力する。「**次へ**」をクリックします。

注: このパスワードは、各受動システム上で keytab エントリーに使用されます。セキュリティ・ポリシー上、各システムで異なるパスワードが必要な場合は、このステップをスキップすることができます。その代わりに、このウィザードを完了した後に、手動で keytab エントリーを個々のシステムに追加し、各システムごとに異なるパスワードを入力します。

8. 「要約」ページで、適切な設定値がこのページにリストされていることを検証する。「**終了**」をクリックします。
9. デフォルトでは、「**機能の同期化**」タスクが開始されたことを示すダイアログ・ボックスが表示されます。ただし、デフォルトの設定値を変更した場合は、このダイアログ・ボックスは表示されません。「**OK**」をクリックします。

10. 「機能の同期化状況 (Synchronize Functions Status)」ダイアログ・ボックスが表示される。タスクが正常に完了したことを検証します。システム D 以外のすべてのエンドポイント・システムでタスクが正常に完了したとします。システム D は、OS/400 V5R2 で実行されているため、機能同期化ウィザードをサポートしません。

このエラーをリカバリーするには、モデル・システム (システム A) 上の構成と一致するように、システム D 上のネットワーク認証サービスを手動で構成する必要があります。

システム D 上でのネットワーク認証サービスの構成

システム D 上で、システム A 上の構成設定値と一致するようにネットワーク認証サービスを構成する必要があります。

ネットワーク認証サービスを構成するには、以下の手順に従います。

1. System i ナビゲーターで、「システム D」→「セキュリティ」と展開する。
2. 「ネットワーク認証サービス」を右クリックし、「構成」を選択して構成ウィザードを開始する。

注: ネットワーク認証サービスを構成した後では、このオプションは「再構成」になります。

3. ウィザードが作成するオブジェクトに関する情報について、「ようこそ」ページを検討する。「次へ」をクリックします。
4. 「レルム情報の指定 (Specify realm information)」ページで、「デフォルト・レルム」フィールドに MYCO.COM を入力し、「Microsoft Active Directory を Kerberos 認証に使用する (Microsoft Active Directory is used for Kerberos authentication)」を選択する。「次へ」をクリックします。
5. 「KDC 情報の指定 (Specify KDC information)」ページで、「KDC」フィールドにこのレルムの Kerberos サーバーの名前として kdc1.myco.com を入力し、「ポート」フィールドに 88 を入力する。「次へ」をクリックします。
6. 「パスワード情報の指定 (Specify password information)」ページで、システム D を構成して、デフォルト・レルムに構成されたパスワード・サーバーを指すように「はい (Yes)」を選択する。パスワード・サーバーは既に構成済みです。プリンシパルが Kerberos サーバー上のパスワードを変更できるようにします。「パスワード・サーバー (Password server)」フィールドに kdc1.myco.com を入力します。パスワード・サーバーはデフォルト・ポート 464 をもっています。「次へ」をクリックします。
7. 「keytab エントリーの選択」ページで、「i5/OS Kerberos 認証」を選択する。「次へ」をクリックします。
8. 「i5/OS keytab エントリーの作成 (Create i5/OS keytab entry)」ページで、パスワードを入力して確認する。例えば、systemd123。「次へ」をクリックします。
9. オプション: 「バッチ・ファイルの作成 (Create batch file)」ページで、「いいえ」を選択する。
10. 「要約」ページで、ネットワーク認証サービスの構成の詳細を検討する。「終了」をクリックします。

エンドポイント・システム用のプリンシパルを Windows 2000 ドメインに追加

エンドポイント・システム用のプリンシパル追加のステップは、次のとおりです。

1. システム B の手順

- a. Windows 2000 サーバー上で、「管理ツール (Administrative Tools)」→「Active Directory ユーザーとコンピューター (Active Directory Users and Computers)」と展開する。
- b. ドメインとして MYCO.COM を選択し、「アクション (Action)」→「新規 (New)」→「ユーザー (User)」と展開する。

注: この Windows ドメインは、ネットワーク認証サービス構成に指定したデフォルト・レルム名と同じでなければなりません。

- c. 「名前」フィールドに、この Windows ドメインに対して System i プラットフォームを識別する `systemb` を入力する。これによりシステム B 用の新しいユーザー・アカウントが追加されます。
- d. Active Directory ユーザー `systemb` でプロパティにアクセスする。「アカウント」タブから、「アカウントの委任は承認されています (Account is trusted for delegation)」を選択します。これにより、i5/OS サービス・プリンシパルは、サインイン・ユーザーに代わって他のサービスにアクセスすることができるようになります。
- e. Windows 2000 サーバー上で、作成したばかりのユーザー・アカウントを、`ktpass` コマンドを使用することにより i5/OS サービス・プリンシパルにマップする必要があります。 `ktpass` ツールは、Windows 2000 サーバーのインストール CD の「サービス・ツール (Service Tools)」フォルダーに入っています。 Windows コマンド・プロンプトで、次のコマンドを入力します。

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

2. システム C の手順

- a. Windows 2000 サーバー上で、「管理ツール (Administrative Tools)」 → 「Active Directory ユーザーとコンピューター (Active Directory Users and Computers)」と展開する。
- b. ドメインとして **MYCO.COM** を選択し、「アクション (Action)」 → 「新規 (New)」 → 「ユーザー (User)」と展開する。

注: この Windows ドメインは、ネットワーク認証サービス構成に指定したデフォルト・レルム名と同じでなければなりません。

- c. 「名前」フィールドに、この Windows ドメインに対して System i プラットフォームを識別する `systemc` を入力する。これによりシステム C 用の新しいユーザー・アカウントが追加されます。
- d. Active Directory ユーザー `systemc` でプロパティにアクセスする。「アカウント」タブから、「アカウントの委任は承認されています (Account is trusted for delegation)」を選択します。これにより、i5/OS サービス・プリンシパルは、サインイン・ユーザーに代わって他のサービスにアクセスすることができるようになります。
- e. Windows 2000 サーバー上で、作成したばかりのユーザー・アカウントを、`ktpass` コマンドを使用することにより i5/OS サービス・プリンシパルにマップする必要があります。 `ktpass` ツールは、Windows 2000 サーバーのインストール CD の「サービス・ツール (Service Tools)」フォルダーに入っています。 Windows コマンド・プロンプトで、次のコマンドを入力します。

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

3. システム D の手順

- a. Windows 2000 サーバー上で、「管理ツール (Administrative Tools)」 → 「Active Directory ユーザーとコンピューター (Active Directory Users and Computers)」と展開する。
- b. ドメインとして **MYCO.COM** を選択し、「アクション (Action)」 → 「新規 (New)」 → 「ユーザー (User)」と展開する。

注: この Windows ドメインは、ネットワーク認証サービス構成に指定したデフォルト・レルム名と同じでなければなりません。

- c. 「名前」フィールドに、この Windows ドメインに対して System i プラットフォームを識別する `systemd` を入力する。これによりシステム D 用の新しいユーザー・アカウントが追加されます。

- d. Active Directory ユーザー systemd でプロパティにアクセスする。「アカウント」タブから、「アカウントの委任は承認されています (Account is trusted for delegation)」を選択します。これにより、i5/OS サービス・プリンシパルは、サインイン・ユーザーに代わって他のサービスにアクセスすることができるようになります。
- e. Windows 2000 サーバー上で、作成したばかりのユーザー・アカウントを、ktpass コマンドを使用することにより i5/OS サービス・プリンシパルにマップする必要があります。ktpass ツールは、Windows 2000 サーバーのインストール CD の「サービス・ツール (Service Tools)」フォルダーに入っています。Windows コマンド・プロンプトで、次のコマンドを入力します。

```
ktpass -mapuser systemd -pass systemd123 -princ krbsvr400/systemd.myco.com@MYCO.COM -mapop set
```

複数システムへのネットワーク認証サービス構成の伝搬は完了しました。ネットワーク認証サービスを活用するためにマネージメント・セントラルを構成するには、いくつかの追加のタスクを実行する必要があります。詳細については、『シナリオ: マネージメント・セントラル・サーバー間での Kerberos 認証の使用』を参照してください。

シナリオ: マネージメント・セントラル・サーバー間での Kerberos 認証の使用

マネージメント・セントラル・サーバー間で Kerberos 認証を使用する場合の前提条件と目的を、以下で説明します。

状況

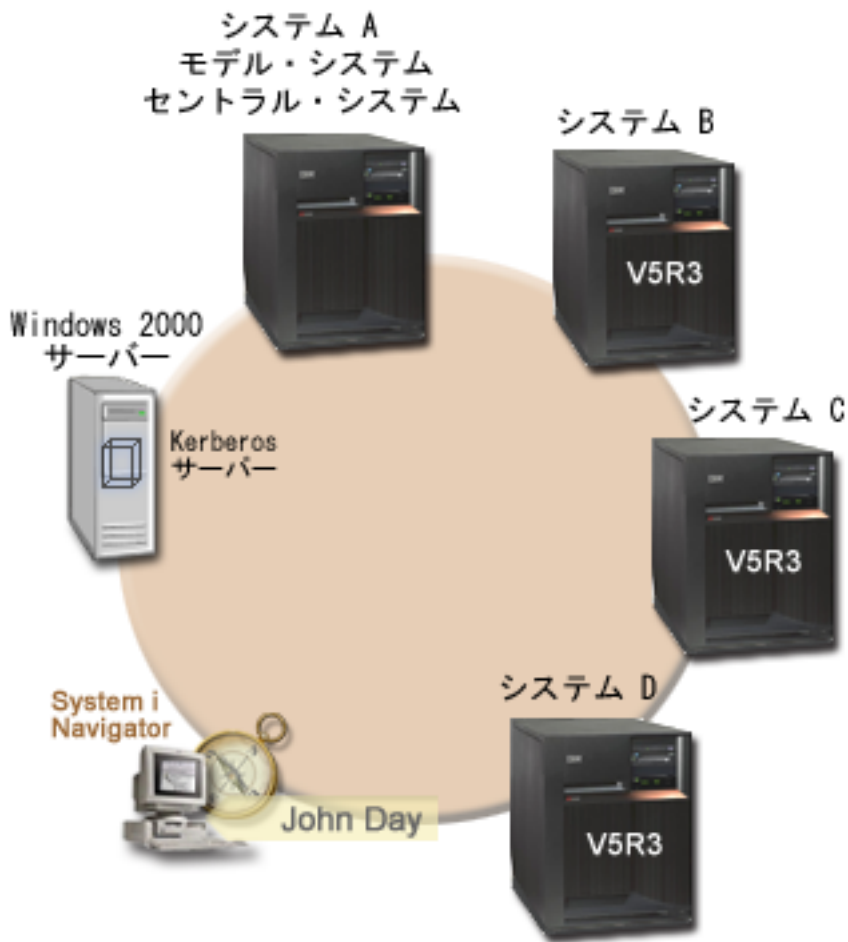
貴方は、中規模の部品メーカーのネットワーク管理者です。現在、System i ナビゲーター をクライアント PC で使用する 4 つの System i 製品を管理しています。マネージメント・セントラル・サーバー・ジョブが、過去に使用していた他の認証メソッド、すなわちパスワード同期ではなく、Kerberos 認証を使用したものとなります。

目的

このシナリオでは、MyCo, Inc. のゴールは、マネージメント・セントラル・サーバー間で Kerberos 認証を使用することです。

詳細

以下の図は、このシナリオの詳細を示しています。



システム A: モデル・システムであり同時にセントラル・システム

- 次のオプションおよびライセンス・プログラムがインストールされている i5/OS V5R3 またはそれ以降を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12 または 5761-SS1 オプション 12)
 - System i Access for Windows (5722-XE1 または 5761-XE1)
 - Network Authentication Enablement (5722-NAE または 5761-NAE) (i5/OS V5R4 以降を使用している場合)
 - Cryptographic Access Provider (5722-AC3) (i5/OS V5R3 を実行している場合)
- i5/OS サービス・プリンシパル `krbsvr400/systema.myco.com@MYCO.COM` および関連するパスワードが、`keytab` ファイルに追加済み。
- 各エンドポイント・システムの同期化設定タスクを保管し、スケジュールし、実行する。

システム B: エンドポイント・システム

- 次のオプションおよびライセンス・プログラムがインストールされている i5/OS V5R3 またはそれ以降を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12 または 5761-SS1 オプション 12)

- System i Access for Windows (5722-XE1 または 5761-XE1)
- Network Authentication Enablement (5722-NAE または 5761-NAE) (i5/OS V5R4 以降を使用している場合)
- Cryptographic Access Provider (5722-AC3) (i5/OS V5R3 を実行している場合)
- i5/OS サービス・プリンシパル krbsvr400/systemb.myco.com@MYCO.COM および関連するパスワードが、keytab ファイルに追加済み。

システム C エンドポイント・システム

- 次のオプションおよびライセンス・プログラムがインストールされている i5/OS V5R4 を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12 または 5761-SS1 オプション 12)
 - System i Access for Windows (5722-XE1 または 5761-XE1)
 - Network Authentication Enablement (5722-NAE または 5761-NAE)
- i5/OS サービス・プリンシパル krbsvr400/systemc.myco.com@MYCO.COM および関連するパスワードが、keytab ファイルに追加済み。

システム D エンドポイント・システム

- 次のオプションおよびライセンス・プログラムがインストールされている i5/OS V5R3 またはそれ以降を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12 または 5761-SS1 オプション 12)
 - System i Access for Windows (5722-XE1 または 5761-XE1)
 - Cryptographic Access Provider (5722-AC3)
- i5/OS サービス・プリンシパル krbsvr400/systemd.myco.com@MYCO.COM および関連するパスワードが、keytab ファイルに追加済み。

Windows 2000 サーバー

- これらのシステムの Kerberos サーバーとして作動する。
- 以下の i5/OS サービス・プリンシパルが、Windows 2000 サーバーに追加済み。
 - krbsvr400/systema.myco.com@MYCO.COM
 - krbsvr400/systemb.myco.com@MYCO.COM
 - krbsvr400/systemc.myco.com@MYCO.COM
 - krbsvr400/systemd.myco.com@MYCO.COM

クライアント PC

- System i Access for Windows (5722-XE1 または 5761-XE1) を実行します。
- 次のサブコンポーネントを備えた System i ナビゲーター を実行します。

注: ネットワーク認証サービスを管理するのに使用される PC のみに必要です。

- ネットワーク
- セキュリティー

前提条件および前提事項

1. ソフトウェアおよびオペレーティング・システムのインストールを含むすべてのシステム要件は、検証済みである。

ライセンス・プログラムがインストール済みであることを検証するには、以下の手順に従います。

- a. System i ナビゲーターで、「システム」 → 「構成およびサービス」 → 「ソフトウェア」 → 「インストール済みプロダクト」を展開する。
- b. すべてのライセンス・プログラムがインストール済みであることを確認する。
2. 必要なハードウェアの計画とセットアップはすべて完了している。
3. これらのシステムのそれぞれにおいて、TCP/IP および基本的なシステム・セキュリティーが構成されており、テスト済みである。
4. タスク開始時に「タスク状況」ウィンドウをオープンするのを止めるように System i ナビゲーター 内のデフォルトの設定値が変更されていない。デフォルトの設定値が変更されていないことを検証するには、以下の手順を行います。
 - a. System i ナビゲーター で、「ユーザーのセントラル・システム (*your central system*)」を右クリックし、「ユーザー・プリファレンス (*User Preferences*)」を選択する。
 - b. 「一般」 ページで、「タスクのいずれかが開始する時にタスク状況ウィンドウを自動的にオープンする (*Automatically open a task status window when one of my tasks starts*)」が選択されていることを検証する。
5. このシナリオでは、ネットワーク認証サービスが System i ナビゲーター の「機能の同期化」ウィザードを使用して各システム上に構成済みであることを前提事項とします。このウィザードは、モデル・システムから複数の受動システムへ、ネットワーク認証サービス構成を伝搬します。「機能の同期化」ウィザードの使用法の詳細については、39 ページの『シナリオ: 複数システムにわたるネットワーク認証サービス構成の伝搬』を参照してください。

構成手順

マネージメント・セントラル・サーバー間で Kerberos 認証を構成するには、以下の手順を実行します。

計画ワークシートの完成

以下の計画ワークシートは、ご使用のシステムが Kerberos 認証を使用できるようにする前に必要な情報のタイプを示しています。

表 II. マネージメント・セントラル・サーバー間での Kerberos 認証の使用 - 前提条件ワークシート

前提条件ワークシート	回答
ご使用のすべての System i プラットフォームにおいて、i5/OS V5R3 またはそれ以降 (5722-SS1)、または V6R1 (5761-SS1) を、使用していますか？	はい
最新のプログラム一時修正 (PTF) を適用していますか？	はい
以下のオプションとライセンス・プログラムが、すべての System i モデルにインストール済みですか? <ul style="list-style-type: none"> • i5/OS Host Servers (5722-SS1 オプション 12 または 5761-SS1 オプション 12) • System i Access for Windows (5722-XE1 または 5761-XE1) • Network Authentication Enablement (5722-NAE または 5761-NAE) (i5/OS V5R4 以降を使用している場合) • Cryptographic Access Provider (5722-AC3) (i5/OS V5R3 を実行している場合) 	はい
管理者の PC に System i Access for Windows (5722-XE1 または 5761-XE1) はインストール済みですか?	はい

表 11. マネージメント・セントラル・サーバー間での Kerberos 認証の使用 - 前提条件ワークシート (続き)

前提条件ワークシート	回答
管理者の PC に System i ナビゲーター はインストール済みですか? ・ 管理者の PC に System i ナビゲーター のネットワーク・サブコンポーネントはインストール済みですか? ・ 管理者の PC に System i ナビゲーター のセキュリティー・サブコンポーネントはインストール済みですか?	はい
最新の IBM System i Access for Windows サービス・パックをインストール済みですか? 最新の Service Pack については、System i Access  を参照してください。	はい
*SECADM、*ALLOBJ、および *IOSYSCFG の特殊権限を持っているか?	はい
Kerberos サーバーとしての役割を果たす以下のいずれかのシステムを持っているか? 「はい」の場合、どのシステムか? 1. Microsoft Windows 2000 サーバー 注: Microsoft Windows 2000 サーバーは、Kerberos 認証をデフォルトのセキュリティー・メカニズムとして使用します。 2. Windows サーバー 2003 3. i5/OS PASE (V5R3 以降) 4. AIX サーバー 5. z/OS	はい、Windows 2000 サーバー
Windows 2000 サーバーおよび Windows サーバー 2003 の場合、Windows サポート・ツール (ktpass ツールを提供する) がインストールされているか?	はい
System i システム時刻と Kerberos サーバー上のシステム時刻とのずれは 5 分以内ですか? そうでない場合は、114 ページの『システム時刻の同期化』を参照。	はい

表 12. マネージメント・セントラル・サーバー間での Kerberos 認証の使用 - 計画ワークシート

質問	回答
システム・グループの名前は?	MyCo2 システム・グループ
このシステム・グループに組み込まれるシステムは?	システム A、システム B、システム C、システム D
System i プラットフォームのサービス・プリンシパル名は?	krbsvr400/systema.myco.com@MYCO.COM krbsvr400/systemb.myco.com@MYCO.COM krbsvr400/systemc.myco.com@MYCO.COM krbsvr400/systemd.myco.com@MYCO.COM

Kerberos 認証を使用するセントラル・システムの設定

システム A は、他の受動システムのモデル・システムでありセントラル・システムです。

Kerberos 認証をセントラル・システムで設定するには、以下の手順を完了します。

- System i ナビゲーター で、「マネージメント・セントラル (システム A)」を右クリックして「プロパティ」を選択します。
- 「セキュリティー」タブで「Kerberos 認証を使用」を選択し、認証レベルを「トラステッド・グループに追加」に設定する。

3. 「ID マッピング」フィールドの「使用しない」を選択し、「OK」をクリックする。この設定値は、ご使用のエンドポイント・システム用のシングル・サインオン環境を使用可能にするために、マネージメント・セントラル・サーバーによる EIM (エンタープライズ識別マッピング) の使用を可能にするか不可能にすることをユーザーが行えるようにします。エンドポイント・システムでシングル・サインオンを使用可能にしたい場合は、この構成を示しているシナリオを『シナリオ: シングル・サインオン環境でマネージメント・セントラル・サーバーを構成する (Scenario: Configuring the Management Central server for a single sign-on environment)』で参照してください。

注: 「セキュリティ」ページの下部の注が、マネージメント・セントラル・サーバーが次回開始されるときに設定値が有効になることを示しています。この時点でサーバーを再始動してはなりません。このシナリオでは、後続のステップの中で、再始動すべき適切な時点を指示します。

4. これらの設定値に対する変更がこのセントラル・システムにのみ反映されること、およびこれらの設定値をマネージメント・セントラル・サーバー・ジョブで使用できるようにするには、まず Kerberos を正しく構成する必要があることを示すダイアログ・ボックスが表示される。「OK」をクリックします。セントラル・システムで使用する Kerberos 認証が使用可能となりました。

MyCo2 システム・グループの作成

システム・グループとは、ユーザーが管理でき、同様な設定値と属性 (ネットワーク認証サービス構成など) を適用することができるシステムの集まりです。

該当する設定値をネットワーク内の他のシステムに適用することができるようにするには、まず、すべてのエンドポイント・システム用のシステム・グループを作成しておく必要があります。

1. System i ナビゲーター で、「マネージメント・セントラル (システム A)」を展開します。
2. 「システム・グループ」を右クリックし、新しいシステム・グループを作成するために「新規システム・グループ」を選択する。
3. 「一般」ページで、名前のフィールドに MyCo2 system group と入力する。このシステム・グループの説明を指定する。
4. 「選択可能なシステム」リストから、システム A、システム B、システム C、およびシステム D を選択して「追加」をクリックする。これらのシステムが「選択されたシステム」リストに追加されます。「OK」をクリックします。
5. 「システム・グループ」を展開して、ご使用のシステム・グループが追加されたことを検証する。

システム値インベントリーの収集

MyCo2 システム・グループ内の受動システム用のインベントリーに対して Kerberos 認証設定値を追加するには、System i ナビゲーター で「インベントリー収集」機能を使用する必要があります。

MyCo2 システム・グループ用のインベントリーを収集するには、以下の手順を完了します。

1. System i ナビゲーター で、「マネージメント・セントラル (システム A)」 → 「システム・グループ」と展開する。
2. 「MyCo2 system group」を右クリックし、「インベントリー」 → 「収集」を選択する。
3. 「インベントリーの収集 - MyCo2 system group」ページで、「システム値」を選択する。「OK」をクリックします。デフォルトでは、「同期化機能インベントリー収集 (Synchronize Functions Collect Inventory)」タスクが開始されたことを示すダイアログ・ボックスが表示される。ただし、デフォルトの設定値を変更した場合は、このダイアログ・ボックスは表示されません。「OK」をクリックします。
4. 「インベントリーの収集状況」ページで、遭遇する可能性のある問題を表示し修正するすべての状況値を読む。このページに表示される、インベントリー収集に関連した特定の状況値の詳細については、

「ヘルプ」 → 「タスク状況のヘルプ」を選択してください。「タスク状況」ヘルプ・ページから、「インベントリー」を選択します。このページは、ユーザーが遭遇する可能性のあるすべての状況値を、詳細な説明とリカバリー情報付きで表示します。

5. インベントリー収集が正常に終了したら、状況ウィンドウをクローズする。

System i ナビゲーターにおける Kerberos 設定の比較と更新

システム値インベントリーを収集した後で、セントラル・システム上で選択された Kerberos 設定値を取得し、MyCo2 システム・グループ内の各受動システムに適用する必要があります。

MyCo2 システム・グループ内受動システムを更新するには、以下の手順を完了します。

1. System i ナビゲーターで、「マネージメント・セントラル (システム A)」 → 「システム・グループ」と展開する。
2. 「MyCo2 system group」を右クリックし、「システム値」 → 「比較および更新」を選択する。
3. 「比較および更新 - MyCo2 system group」ダイアログ・ボックスで以下のようにフィールドを完成する。
 - a. 「モデル・システム」フィールドには「システム A」を選択する。
 - b. 「カテゴリー」フィールドには「マネージメント・セントラル」を選択する。
 - c. 「比較する項目 (Items to compare)」のリストから、「Kerberos 認証を使用して要求を検証する (Use Kerberos authentication to verify requests)」と「Kerberos 認証信頼レベル (Kerberos authentication trust level)」を選択する。
4. MyCo2 システム・グループ内の受動システムが受動システムのリストの中に表示されていることを検証した上で、更新を開始するために「OK」をクリックする。これにより MyCo2 システム・グループ内の受動システムのそれぞれが、モデル・システム上で選択された Kerberos 認証設定値を使用して更新されます。
5. デフォルトでは、「比較および更新」タスクが開始されたことを示すダイアログ・ボックスが表示される。ただし、デフォルトの設定値を変更した場合は、このダイアログ・ボックスは表示されません。「OK」をクリックします。
6. 「値の更新の状況 (Update Values Status)」ダイアログ・ボックスで、各システム上の更新が完了したことを検証し、ダイアログ・ボックスをクローズする。

セントラル・システムおよび受動システムでのマネージメント・セントラル・サーバーの再始動

MyCo2 システム・グループ内の各受動システムごとに更新が完了した後に、セントラル・システムおよび受動システム上のすべてのマネージメント・セントラル・サーバーを再始動する必要があります。

マネージメント・セントラル・サーバーを再始動するには、以下の手順を完了します。

1. System i ナビゲーターで、「接続 (My connections)」 → 「システム A」 → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」と展開する。
2. 「マネージメント・セントラル」を右クリックし、「停止」を選択する。マネージメント・セントラルが停止するまで待ちます。F5 を押して画面を最新表示し、右方の画面区画に状況を表示します。サーバーが停止すると、状況は「停止」と表示されるはずですが。
3. 「マネージメント・セントラル」を右クリックし、「開始」を選択する。これにより、セントラル・システム上でマネージメント・セントラル・サーバーが再始動されます。
4. ステップ 1 から 3 までを次の受動システム: システム B、システム C、およびシステム D 上で繰り返す。

エンドポイントごとにトラステッド・グループ・ファイルに Kerberos サービス・プリンシパルを追加

マネージメント・セントラル・サーバーすべてが再始動された後に、各エンドポイント・システムごとにトラステッド・グループ・ファイルに対して、セントラル・システムの Kerberos サービス・プリンシパルを追加する必要があります。

セントラル・システムから、ライブラリー・リスト表示 (DSPLIBL) などのリモート・コマンドを、すべてのエンドポイント・システムに対して実行します。各エンドポイント・システム上の認証レベルとして「**トラステッド・グループに追加**」が選択されているために、各エンドポイント・システムは自動的にセントラル・システムの Kerberos サービス・プリンシパルを、自身の個別のトラステッド・グループ・ファイルに追加します。セントラル・システムからエンドポイント・システムに任意のリモート・コマンドを実行して、エンドポイント・システム上のマネージメント・セントラル・サーバー・ジョブが、必要な Kerberos サービス・プリンシパルをトラステッド・グループ・ファイルに記録させることができます。DSPLIBL コマンドは、例として使用しているにすぎません。

注: モデル・システムまたは起動システムを使用してタスク (修正プログラムの送信、ユーザーの送信、時刻の同期化など) を実行している場合、正しい Kerberos サービス・プリンシパルが正しいトラステッド・グループ・ファイルに追加されるように、これらのタスクを実行する必要があります。

このシナリオでは、各エンドポイント・システム上のトラステッド・グループ・ファイルに Kerberos サービス・プリンシパルを追加するために、すべてのエンドポイント・システムに対してリモート・コマンドを実行することを決めます。リモート・コマンドを実行するには、以下の手順を完了してください。

1. System i ナビゲーターで、「マネージメント・セントラル (システム A)」 → 「システム・グループ」と展開する。
2. 「MyCo2 system group」を右クリックし、「コマンドの実行」を選択する。
3. 「コマンドの実行 - MyCo2 system group」ページで、「実行するコマンド」フィールドに dsplibl と入力し、即時にコマンド・タスクを開始するために「OK」をクリックする。「前のコマンド」をクリックして以前に実行したコマンドのリストから選択することもでき、あるいは「プロンプト」をクリックして i5/OS コマンドを入力あるいは選択する時に援助を得ることもできます。
4. デフォルトでは、「コマンドの実行」タスクが開始されたことを示すダイアログ・ボックスが表示される。ただし、デフォルトの設定値を変更した場合は、このダイアログ・ボックスは表示されません。「OK」をクリックします。
5. 「コマンドの実行状況」ダイアログ・ボックスで、各システム上でコマンドが完了したことを検証し、ダイアログ・ボックスをクローズする。

Kerberos プリンシパルがトラステッド・グループ・ファイルに追加されたことの検証

リモート・コマンドを実行した後に、各受動システム上のトラステッド・グループ・ファイルにセントラル・システムの Kerberos サービス・プリンシパルがあることを検証することができます。

1. System i ナビゲーターで、「システム B」 → 「ファイル・システム」 → 「統合ファイル・システム」 → 「ルート」 → 「QIBM」 → 「UserData」 → 「OS400」 → 「MGTC」 → 「config」と展開する。
2. 「McTrustedGroup.conf」を右クリックし、ファイルの内容を表示するために「編集」を選択する。
 - a. 「統合ファイル・システム」を右クリックして「プロパティ」を選択する。
 - b. 「統合ファイル・システム・プロパティ」ダイアログ・ボックスで、「編集可能メニュー・オプション」で「すべてのファイル」を選択し、「OK」をクリックする。

3. セントラル・システムの Kerberos サービス・プリンシパルが、マネージメント・セントラル・トラステッド・グループ・メンバーの 1 つとしてリストされていることを検証する。
4. これらの手順をシステム C およびシステム D にも繰り返し、セントラル・システムの Kerberos サービス・プリンシパルが受動システムのそれぞれに追加されることを検証する。

セントラル・システムへの信頼された接続を可能にする

リモート・コマンドがエンドポイント・システムに対して正常に実行された後に、マネージメント・セントラル・サーバー間で信頼された接続を可能にする必要があります。

信頼された接続を可能にするために、以下のステップを実行してください。これにより、MyCo2 システム・グループのセントラル・システム (システム A) のみが、受動システムに対してタスクを実行できることが確認されます。

1. System i ナビゲーターで、「マネージメント・セントラル (システム A)」を右クリックして「プロパティ」を選択します。
2. 「セキュリティ」タブで「Kerberos 認証を使用」を選択し、認証レベルを「トラステッド接続のみを許可」に設定する。
3. 「ID マッピング」フィールドの「使用しない」を選択する。
4. これらの設定値に対する変更がこのセントラル・システムにのみ反映されること、およびこれらの設定値をマネージメント・セントラル・サーバー・ジョブで使用できるようにするには、まず Kerberos を正しく構成する必要があることを示すダイアログ・ボックスが表示される。「OK」をクリックします。

受動システムごとのステップ 4 から 6 の繰り返し

セントラル・システムへの信頼された接続を可能にした後、このシナリオのステップ 4 から 6 を繰り返し、MyCo2 システム・グループ内の受動システムに対してこれらの変更を適用する必要があります。これにより、受動システムが信頼された接続を可能にするよう構成されていることが確認されます。

以下の手順を参照してください。

1. ステップ 4: システム値インベントリーの収集
2. ステップ 5: System i ナビゲーターで Kerberos 設定を比較および更新
3. ステップ 6: セントラル・システムおよび受動システム上でマネージメント・セントラル・サーバーを再始動

エンドポイント・システムでの認証のテスト

サーバーが再始動されると、システムは、認証には Kerberos を、権限付与にはトラステッド・グループを使用します。トラステッド・グループ・リストにあるプリンシパルであることを検査した上でその Kerberos プリンシパルを信頼していることを検証します。要求を受け入れて実行するシステムの場合、そのシステムは、要求しているシステムが有効な Kerberos プリンシパルを持っていることを検証するだけでなく、トラステッド・グループ・リストにあるプリンシパルであることを検査した上でその Kerberos プリンシパルを信頼していることを検証します。

注: これらのステップを、以下の i5/OS サービス・プリンシパルを使用して、各受動システム上で繰り返す必要があります。

- krbsvr400/systema.myco.com@MYCO.COM
- krbsvr400/systemb.myco.com@MYCO.COM
- krbsvr400/systemc.myco.com@MYCO.COM

- krbsvr400/systemd.myco.com@MYCO.COM

Kerberos 認証がエンドポイント・システムで作動していることを検証するには、以下のタスクを完了します。

注: これらのテストを行う前に、必ず i5/OS ユーザー・プロファイル用のホーム・ディレクトリーを作成しておいてください。

1. System i ナビゲーター のセッションをすべてクローズする。
2. コマンド行で QSH と入力して、Qshell インタープリターを開始する。
3. keytab list と入力して、keytab ファイルに登録されているプリンシパルのリストを表示する。以下の表示と同様な結果が表示されるはずでず。

```
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. kinit -k krbsvr400/systema.myco.com@MYCO.COM と入力して、Kerberos サーバーからチケット許可チケットを要求する。このコマンドは、ご使用のシステムが正しく構成されており、keytab ファイル内のパスワードが Kerberos サーバーに保管されているパスワードと一致することを検証します。正しく入力されれば、QSH コマンドがエラーなしに表示されます。
5. klist と入力し、デフォルト・プリンシパルが krbsvr400/systema.myco.com@MYCO.COM であることを検証する。このコマンドにより、Kerberos 信任状キャッシュの内容が表示され、i5/OS サービス・プリンシパルに有効な許可証が作成され、かつシステムの信任状キャッシュに入れられていることが検査されます。

```
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
$
```

これで、エンドポイント・システム間で Kerberos 認証を使用するためにマネージメント・セントラル・サーバー・ジョブを構成するのに必要なタスクを完了しました。

シナリオ: i5/OS 用のシングル・サインオンを使用可能にする。

i5/OS オペレーティング・システムで、シングル・サインオンを使用可能にする場合の前提条件と目的を以下で説明します。

状況

貴方は、受注部門を含む自社のネットワークおよびネットワーク・セキュリティーを管理するネットワーク管理者です。電話でカスタマー・オーダーを取る多数の従業員の IT 操作を監督します。また、貴方がネットワークを維持管理するのを助ける、他の 2 名のネットワーク管理者も監視します。

受注部門の従業員は、Windows 2000 および i5/OS を使用し、毎日使用するさまざまなアプリケーションに複数のパスワードを必要としています。その結果、貴方は、忘れたパスワードのリセットなど、パスワードとユーザー ID に関連する問題の管理とトラブルシューティングに多くの時間を費やしています。

会社のネットワーク管理者として、貴方は、業務を改善する方法を常に模索しており、受注部門からそれを始めます。貴方は、多くの従業員が在庫状況の照会で使用するアプリケーションにアクセスするために、同一タイプの権限を必要としていることを知っています。このような状況で必要な個別のユーザー・プロファイルおよび多数のパスワードを維持することは、冗長であり時間の無駄であると考えられます。さらに、より少ないユーザー ID とパスワードを使用することがすべての従業員のためにもなることを貴方は知っています。そのため以下のことを行いたいものとします。

- 受注部門用のパスワード管理のタスクを単純化する。特に、従業員がカスタマー・オーダーのために日常的に使用するアプリケーションへのユーザー・アクセスを効果的に管理したいものとします。
- 受注部門の従業員だけでなくネットワーク管理者も、複数のユーザー ID とパスワードの使用を削減する。しかし、Windows 2000 ID と i5/OS ユーザー・プロファイルを同じにしたり、あるいはパスワード・キャッシングまたは同期化も使用したくありません。

研究の結果、通常はいくつものユーザー ID およびパスワードを使用してログオンしなければならない、複数のアプリケーションやサービスへのアクセスを、ユーザーが 1 回ログオンするだけで行えるソリューション、シングル・サインオンを i5/OS がサポートしていることがわかります。ユーザーがジョブを行うために多数のユーザー ID とパスワードを与える必要はないため、貴方は彼らのために解決すべきパスワードの問題は少なくなります。シングル・サインオンは、以下の点で、パスワード管理を単純化できるようにするため、理想的なソリューションであると考えられます。

- アプリケーションへの同一の権限を必要とする典型的ユーザーの場合、ポリシー・アソシエーションを作成することができます。例えば、受注部門の注文担当者が一度 Windows ユーザー名とパスワードでログオンしたら、再度の認証の必要なしに製造部門の新規在庫照会アプリケーションにアクセスできるようにしたいものとします。ただし、注文担当者がこのアプリケーションを使用する時に持つ権限のレベルは、必ず適切であるようにもしたいのです。この目標を達成するために、このグループのユーザーの Windows 2000 ユーザー ID を、単一の i5/OS ユーザー・プロファイル (在庫照会アプリケーションを実行するための適切なレベルの権限を持つ) にマップする、ポリシー関連を作成することにしました。これは照会のみアプリケーションであり、ユーザーはデータを変更することはできないため、このアプリケーションの詳細な監査について心配する必要はありません。したがって貴方は、この状態でポリシー関連を使用することはセキュリティー・ポリシーに合致すると確信します。

権限要件が類似しているオーダー・クレークのグループを、在庫照会アプリケーションに対してしかるべき権限レベルを持つ単一の i5/OS ユーザー・プロファイルにマップする、ポリシー関連を作成します。覚えていなければならないパスワードが 1 つ減り、実行しなければならないログオンが 1 回減ることが、ユーザーの利益になります。管理者としては、グループ内の各人に対する複数のユーザー・プロファイルに代わり、アプリケーションへのユーザー・アクセス用のただ 1 つのユーザー・プロファイルだけを維持するだけで済むという利益があります。

- *ALLOBJ や *SECADM などの特殊権限を持つユーザー・プロファイルを所有する各ネットワーク管理者の場合、ID アソシエーションを作成することができます。例えば、管理者は高水準な権限を持つため、単一のネットワーク管理者用のユーザー ID のすべてが互いに正確にかつ個別にマップされるようにしたいものとします。

会社のセキュリティー・ポリシーに基づいて、各ネットワーク管理者の Windows ID からその管理者の i5/OS ユーザー・プロファイルに明確にマップする ID アソシエーションを作成することを決めます。ID アソシエーションが提供する 1 対 1 マッピングのために、管理者のアクティビティーをより容易にモニターし、トレースすることができます。例えば、特定のユーザー ID を対象に、システム上で実行するジョブおよびオブジェクトをモニターすることができます。覚えていなければならないパスワードが 1 つ減り、実行しなければならないログオンが 1 回減ることは、ネットワーク管理者の利益になります。ネットワーク管理者として、すべての管理者のユーザー ID の関係をより厳重に制御することが、貴方の利益となります。

このシナリオには、以下の利点があります。

- ユーザーの認証プロセスを単純化する。
- アプリケーションへのアクセス管理を単純化する。
- ネットワーク内のシステムへのアクセス管理のオーバーヘッドを軽減する。
- パスワードが盗まれる危険性を最小に抑える。
- 複数回サインオンする必要がない。
- ネットワーク間のユーザー ID 管理を単純化する。

目的

このシナリオでは、貴方は MyCo, Inc. の管理者で、受注部門のユーザーがシングル・サインオンを使用できるようにしたいものとします。

このシナリオの目的は、次のとおりです。

- システム A およびシステム B は、MYCO.COM レルムに参加して、このシングル・サインオン環境に参加するユーザーおよびサービスを認証する必要があります。システムが Kerberos を使用できるようにするには、システム A およびシステム B をネットワーク認証サービス用に構成する必要があります。
- システム A 上の IBM Directory Server for i5/OS (LDAP) は、新規 EIM ドメインのドメイン・コントローラーとして機能する必要があります。

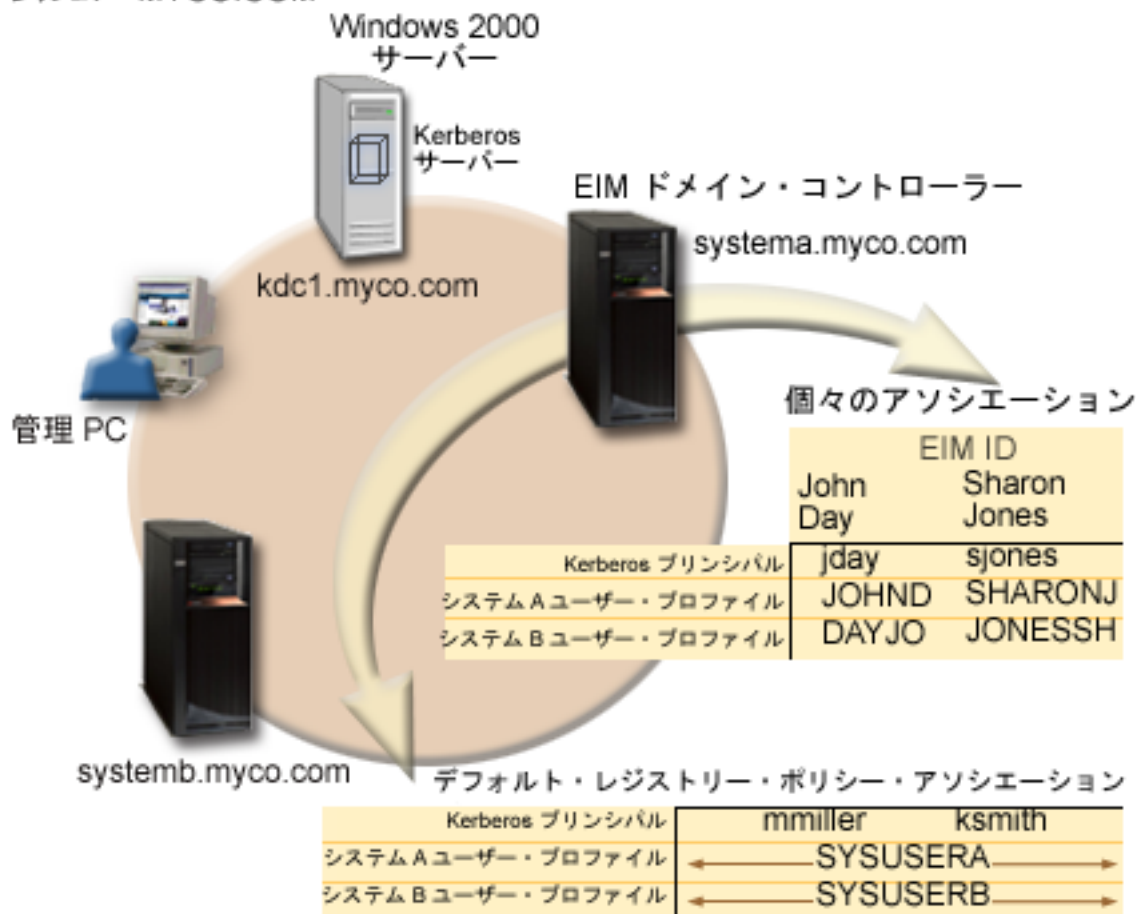
注: EIM ドメインおよび Windows 2000 ドメインという 2 つの異なるタイプのドメインが、どのようにシングル・サインオン環境に組み込まれるかについて学習するには、『ドメイン』トピックを参照してください。

- Kerberos レジストリー内のすべてのユーザー ID は、在庫照会アプリケーションへのユーザー・アクセスに関するしかるべき権限で、単一の i5/OS ユーザー・プロファイルに正常にマップする必要があります。
- セキュリティー・ポリシーに基づいて、同じく Kerberos レジストリーにユーザー ID を持つ 2 人の管理者、John Day と Sharon Jones は、これらの ID を、*SECADM 特殊権限を持つその i5/OS ユーザー・プロファイルにマップする ID アソシエーションを持つ必要があります。これらの 1 対 1 マッピングにより、貴方はこれらのユーザー ID を対象に、システム上で実行するジョブおよびオブジェクトを厳密にモニターすることができます。
- ユーザーを、System i ナビゲーターを含む IBM System i Access for Windows アプリケーションに認証させるには、Kerberos サービス・プリンシパルを使用する必要があります。

詳細

次の図は、このシナリオのネットワーク環境を示します。

レルム = MYCO.COM



図は、このシナリオに関連する以下の点を示します。

エンタープライズ用に定義される EIM ドメイン・データ

- 以下の 3 つのレジストリー定義名:
 - Windows 2000 サーバー・レジストリー用のレジストリー定義名 MYCO.COM。システム A 上で EIM 構成ウィザードを使用するときは、これを定義します。
 - システム A 上の i5/OS レジストリーのレジストリー定義名の SYSTEMA.MYCO.COM。システム A 上で EIM 構成ウィザードを使用するときは、これを定義します。
 - システム B 上の i5/OS レジストリーのレジストリー定義名の SYSTEMB.MYCO.COM。システム B 上で EIM 構成ウィザードを使用するときは、これを定義します。
- 以下の 2 つのデフォルト・レジストリー・ポリシー関連:

注: EIM 探索操作処理は、ID アソシエーションに対して高い優先順位を割り当てます。したがって、ポリシー関連と ID アソシエーションの両方でユーザー ID がソースとして定義されている時は、ID アソシエーションのみがそのユーザー ID とマップします。このシナリオにおいては、2 名のネットワーク管理者 John Day と Sharon Jones は、デフォルト・レジストリー・ポリシー関連のソースで

ある MYCO.COM 用のレジストリーにユーザー ID を持っています。ただし、以下に示すとおり、これらの管理者は MYCO.COM レジストリー内に自分のユーザー ID 用に定義された ID アソシエーションも持っています。ID アソシエーションは、MYCO.COM ユーザー ID がポリシー関連によってはマップされないことを確実にします。代わりに、ID アソシエーションにより、MYCO.COM レジストリー内のユーザー ID が他の特定の個別ユーザー ID へ別々に確実にマップされます。

- 1 つのデフォルト・レジストリー・ポリシー関連は、MYCO.COM と呼ばれる Windows 2000 サーバー・レジストリー内のすべてのユーザー ID を、システム A 上の SYSTEMA.MYCO.COM レジストリー内の SYSUSERA と呼ばれる単一の i5/OS ユーザー・プロファイルにマップする。このシナリオでは、mmiller と ksmith がこれらのユーザー ID のうちの 2 つを表します。
- 1 つのデフォルト・レジストリー・ポリシー関連は、MYCO.COM と呼ばれる Windows 2000 サーバー・レジストリー内のすべてのユーザー ID を、システム B 上の SYSTEMB.MYCO.COM レジストリー内の SYSUSERB と呼ばれる単一の i5/OS ユーザー・プロファイルにマップする。このシナリオでは、mmiller と ksmith がこれらのユーザー ID のうちの 2 つを表します。
- John Day と Sharon Jones という社内の 2 名のネットワーク管理者を表す、同じ名前の 2 つの EIM ID。
 - John Day EIM ID について、以下の ID アソシエーションが定義されている。
 - Windows 2000 サーバー・レジストリー内の Kerberos プリンシパルである、jday ユーザー ID 用のソース・アソシエーション。
 - システム A 上の i5/OS レジストリー内のユーザー・プロファイルである、JOHND ユーザー ID のターゲット関連。
 - システム B 上の i5/OS レジストリー内のユーザー・プロファイルである、DAYJO ユーザー ID のターゲット関連。
 - Sharon Jones EIM ID について、以下の ID アソシエーションが定義されている。
 - Windows 2000 サーバー・レジストリー内の Kerberos プリンシパルである、sjones ユーザー ID 用のソース・アソシエーション。
 - システム A 上の i5/OS レジストリー内のユーザー・プロファイルである、SHARONJ ユーザー ID のターゲット関連。
 - システム B 上の i5/OS レジストリー内のユーザー・プロファイルである、JONESSH ユーザー ID のターゲット関連。

Windows 2000 サーバー

- ネットワークの Kerberos サーバー (鍵配布センター (KDC) と呼ばれる) としての役割を果たす (kdc1.myco.com)。
- Kerberos サーバーのデフォルト・レルムは MYCO.COM。
- ID アソシエーションを持たないすべての Microsoft Active Directory ユーザーは、各 System i プラットフォームの単一の i5/OS ユーザー・プロファイルにマップされます。

システム A

- 次のオプションおよびライセンス・プログラムがインストールされている i5/OS V5R3 またはそれ以降を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12 または 5761-SS1 オプション 12)
 - Qshell インタープリター (5722-SS1 オプション 30 または 5761-SS1 オプション 30)
 - System i Access for Windows (5722-XE1 または 5761-XE1)
 - Network Authentication Enablement (5722-NAE または 5761-NAE) (i5/OS V5R4 を使用している場合)

- Cryptographic Access Provider (5722-AC3) (i5/OS V5R3 を使用している場合)

注: このシナリオは、OS/400 V5R2 を稼働させているシステムでもインプリメントできます。ただし、一部の構成手順はわずかに異なります。さらにこのシナリオは、ポリシー関連など、i5/OS V5R3 以降でのみ使用可能な一部のシングル・サインオン機能を示しています。

- システム A 上のディレクトリー・サーバーは、新規 EIM ドメイン、MyCoEimDomain の EIM ドメイン・コントローラーとして構成されます。
- EIM ドメイン MyCoEimDomain に参加する。
- krbsvr400/systema.myco.com@MYCO.COM という名前のサービス・プリンシパルを持つ。
- 完全修飾ホスト名 systema.myco.com をもつ。この名前は、ネットワーク内のすべての PC およびサーバーが指す単一の DNS 内に登録されています。
- システム A 上のホーム・ディレクトリーが、i5/OS ユーザー・プロファイルの Kerberos 信任状キャッシュを保管します。

システム B

- 次のオプションおよびライセンス・プログラムがインストールされている i5/OS V5R3 またはそれ以降を実行します。
 - i5/OS ホスト・サーバー (5722-SS1 オプション 12 または 5761-SS1 オプション 12)
 - Qshell インタープリター (5722-SS1 オプション 30 または 5761-SS1 オプション 30)
 - System i Access for Windows (5722-XE1 または 5761-XE1)
 - Network Authentication Enablement (5722-NAE または 5761-NAE) (i5/OS V5R4 以降を使用している場合)
 - Cryptographic Access Provider (5722-AC3) (i5/OS V5R3 を実行している場合)
- 完全修飾ホスト名 systemb.myco.com をもつ。この名前は、ネットワーク内のすべての PC およびサーバーが指す単一の DNS 内に登録されています。
- システム B のプリンシパル名は krbsvr400/systemb.myco.com@MYCO.COM です。
- EIM ドメイン MyCoEimDomain に参加する。
- システム B 上のホーム・ディレクトリーが、i5/OS ユーザー・プロファイルの Kerberos 信任状キャッシュを保管します。

管理 PC

- Microsoft Windows 2000 オペレーティング・システムを稼働させている。
- System i Access for Windows (5722-XE1 または 5761-XE1) を実行します。
- 次のサブコンポーネントをインストールした System i ナビゲーター を実行します。
 - ネットワーク
 - セキュリティー
 - ユーザーおよびグループ
- 管理者用の 1 次ログオン・システムとしての役割を果たす。
- MYCO.COM レルム (Windows ドメイン) の一部として構成される。

前提条件および前提事項

このシナリオの正常なインプリメンテーションのために、以下の前提事項および前提条件が満たされていることが必要です。

1. ソフトウェアおよびオペレーティング・システムのインストールを含むすべてのシステム要件は、検証済みである。

これらのライセンス・プログラムがインストール済みであることを検証するには、以下の手順に従います。

- a. System i ナビゲーターで、「システム」 → 「構成およびサービス」 → 「ソフトウェア」 → 「インストール済みプロダクト」を展開する。
- b. すべてのライセンス・プログラムがインストール済みであることを確認する。

注: ネットワーク認証サービス API は、ほとんどの EBCDIC CCSID のジョブ環境をサポートします。ただし、CCSID 290 および 5026 は、小文字 a から z の符号位置が異なるので、サポートされません。

2. 必要なハードウェアの計画とセットアップはすべて完了している。
3. 各システムにおいて、TCP/IP および基本的なシステム・セキュリティーが構成され、テスト済みである。
4. これまでにシステム A で、ディレクトリー・サーバーおよび EIM が構成されてはならない。

注: このシナリオの説明は、以前にシステム A 上でディレクトリー・サーバーが構成されたことがないという前提に基づいています。ただし、既にディレクトリー・サーバーを構成していたとしても、わずかな相違点があるのみでこれらの説明を使用することができます。これらの相違点については、構成の手順の該当する個所で注記します。

5. 単一の DNS サーバーが、ネットワークのホスト名解決に使用される。ホスト・テーブルは、ホスト名解決には使用されません。

注: Kerberos 認証でホスト・テーブルを使用すると、名前解決エラーまたはその他の問題が生じることがあります。Kerberos 認証でホスト名解決がどのように行われるかの詳細については、93 ページの『ホスト名解決の考慮事項』を参照してください。

構成手順

このシナリオをインプリメントする前に、ネットワーク認証サービスおよび EIM (エンタープライズ識別マッピング) を含む、シングル・サインオンに関連する概念を完全に理解する必要があります。シングル・サインオンに関連する用語および概念を学習するための情報については、以下の情報を参照してください。

- EIM (エンタープライズ識別マッピング) の概念
- ネットワーク認証サービスの概念

ご使用のシステム上でシングル・サインオンを構成するには、以下の手順を実行します。

関連概念

シングル・サインオンの概説

ドメイン

計画ワークシートの完成

これらの計画ワークシートは、このシナリオで説明されているシングル・サインオン機能を構成する準備の際に、集めるべき情報および行うべき判断を示すものです。

以下の計画ワークシートは、一般的なシングル・サインオン計画ワークシートに基づき、このシナリオに合わせてあります。正しいインプリメンテーションを確実に行うために、ワークシート内のすべての前提条件に「はい」と答えられなければなりません。また、構成タスクを実行する前に、ワークシートを完成するために必要なすべての情報を集める必要があります。

注: ネットワーク認証サービス API は、ほとんどの EBCDIC CCSID のジョブ環境をサポートします。ただし、CCSID 290 および 5026 は、小文字 a から z の符号位置が異なるので、サポートされません。

表 13. シングル・サインオン前提条件ワークシート


前提条件ワークシート	回答
ご使用の i5/OS は、V5R3、またはそれ以降 (5722-SS1)、あるいは V6R1 (5761-SS1) であるか ?	はい
以下のオプションおよびライセンス・プログラムがシステム A とシステム B にインストールされているか ? <ul style="list-style-type: none"> • i5/OS Host Servers (5722-SS1 オプション 12 または 5761-SS1 オプション 12) • Qshell インタープリター (5722-SS1 オプション 30 または 5761-SS1 オプション 30) • System i Access for Windows (5722-XE1 または 5761-XE1) • Network Authentication Enablement (5722-NAE または 5761-NAE) (i5/OS V5R4 以降を使用している場合) • Cryptographic Access Provider (5722-AC3) (i5/OS V5R3 を実行している場合) 	はい
シングル・サインオン環境に参加する各 PC 上に、シングル・サインオンを使用可能にするアプリケーションをインストールしてあるか ? 注: このシナリオの場合、参加 PCs のすべてに System i Access for Windows (5722-XE1 または 5761-XE1) がインストール済みです。	はい
管理者の PC に System i ナビゲーター はインストール済みですか? <ul style="list-style-type: none"> • シングル・サインオンの管理に使用する PC に System i ナビゲーターのネットワーク・サブコンポーネントはインストール済みですか? • シングル・サインオンの管理に使用する PC に System i ナビゲーターのセキュリティ・サブコンポーネントはインストール済みですか? • シングル・サインオンの管理に使用する PC に System i ナビゲーターのユーザーおよびグループ・サブコンポーネントはインストール済みですか? 	はい
最新の System i Access for Windows サービス・パックをインストール済みですか? 最新の Service Pack については、System i Access  を参照してください。	はい
シングル・サインオン管理者は *SECADM、*ALLOBJ、および *IOSYSCFG の特殊権限を持っているか ?	はい

表 13. シングル・サインオン前提条件ワークシート (続き)

前提条件ワークシート	回答
<p>Kerberos サーバー (KDC と呼ばれる) としての役割を果たす以下のいずれかのシステムを持っているか? 「はい」の場合、どのシステムか?</p> <p>1. Microsoft Windows 2000 サーバー 注: Microsoft Windows 2000 サーバーは、Kerberos 認証をデフォルトのセキュリティー・メカニズムとして使用します。</p> <p>2. Windows サーバー 2003</p> <p>3. i5/OS PASE (V5R3 以降)</p> <p>4. AIX サーバー</p> <p>5. z/OS</p>	はい、Windows 2000 サーバー
ネットワーク内のすべての PC が Windows 2000 ドメインに構成されているか?	はい
最新のプログラム一時修正 (PTF) を適用してあるか?	はい
System i システム時刻と Kerberos サーバー上のシステム時刻とのずれは 5 分以内ですか? そうでない場合は、114 ページの『システム時刻の同期化』を参照。	はい

システム A に EIM およびネットワーク認証サービスを構成する場合は、この情報が必要です。

表 14. システム A のシングル・サインオン構成計画ワークシート

システム A の構成計画ワークシート	回答
以下の情報を使用して、「EIM 構成」ウィザードを完成します。このワークシートの情報は、ウィザードの各ページに提供する必要のある情報と関連しています。	
<p>ご使用のシステムで EIM をどのように構成したいか?</p> <ul style="list-style-type: none"> • 既存のドメインを結合する • 新しいドメインを作成して結合する 	新しいドメインを作成して結合する
EIM ドメインをどこに構成したいか?	ローカル・ディレクトリー・サーバー 注: これは、現在 EIM を構成しているのと同じシステム上にあるディレクトリー・サーバーを構成します。
<p>ネットワーク認証サービスを構成したいか?</p> <p>注: シングル・サインオンを構成するには、ネットワーク認証サービスを構成する必要があります。</p>	はい
「ネットワーク認証サービス」ウィザードは、「EIM 構成」ウィザードから開始します。以下の情報を使用して、「ネットワーク認証サービス」ウィザードを完成します。	
<p>ご使用の System i 製品が属する Kerberos のデフォルト・レルムの名前は何か?</p> <p>注: Windows 2000 ドメインは、Kerberos レルムと同様です。Microsoft Active Directory は、Kerberos 認証をデフォルトのセキュリティー・メカニズムとして使用します。</p>	MYCO.COM
Microsoft Active Directory を使用しているか?	はい

表 14. システム A のシングル・サインオン構成計画ワークシート (続き)

システム A の構成計画ワークシート	回答
この Kerberos デフォルト・レルムの Kerberos サーバー (鍵配布センター (KDC) と呼ばれる) は ? Kerberos サーバーが listen するポートは ?	KDC: kdc1.myco.com ポート: 88 注: これは、Kerberos サーバーのデフォルト・ポートです。
このデフォルト・レルムにパスワード・サーバーを構成したいか ? 「はい」であれば、以下の質問に回答してください。 この Kerberos サーバーのパスワード・サーバーの名前は ? パスワード・サーバーが listen するポートは ?	はい パスワード・サーバー: kdc1.myco.com ポート: 464 注: これは、パスワード・サーバーのデフォルト・ポートです。
どのサービス用に keytab エントリーを作成したいか ? <ul style="list-style-type: none"> • i5/OS Kerberos 認証 • LDAP • IBM HTTP Server • i5/OS NetServer • ネットワーク・ファイルシステムのサーバー 	i5/OS Kerberos 認証
サービス・プリンシパル (単数または複数) のパスワードは ?	systema123
バッチ・ファイルを作成して、システム A のサービス・プリンシパルの Kerberos レジストリーへの追加を自動化しますか?	はい
パスワードを、バッチ・ファイルの i5/OS サービス・プリンシパルに組み込みますか?	はい
「ネットワーク認証サービス」ウィザードを終了すると、「EIM 構成」ウィザードに戻ります。以下の情報を使用して、「EIM 構成」ウィザードを完成します。	
ディレクトリー・サーバーの構成時にウィザードが使用すべきユーザー情報を指定する。これは、接続ユーザーです。ポート番号、管理者識別名、および管理者のパスワードを指定する必要があります。 注: ウィザードが EIM ドメインとその中のオブジェクトを管理するのに十分な権限を必ず持つように、LDAP 管理者の識別名 (DN) とパスワードを指定します。	ポート (Port): 389 識別名: cn=administrator パスワード: mycopwd
作成する EIM ドメインの名前は ?	MyCoEimDomain
EIM ドメインの親 DN を指定したいか ?	いいえ
EIM ドメインに追加したいユーザー・レジストリーはどれか ?	ローカル i5/OS--SYSTEMA.MYCO.COM Kerberos--KDC1.MYCO.COM 注: ウィザードが「 Kerberos ユーザー ID の大/小文字の区別あり (Kerberos user identities are case sensitive) 」のオプションを表示した場合は、これを選択してはなりません。
EIM 操作を行うときに、どの EIM ユーザーをシステム A に使用させますか?これは、システム・ユーザーです。 注: シングル・サインオンを構成する前にディレクトリー・サーバーを構成していなかった場合、システム・ユーザー用に提供できる唯一の識別名 (DN) は、LDAP 管理者の DN およびパスワードです。	ユーザー・タイプ: 識別名 識別名: cn=administrator パスワード: mycopwd

この情報は、システム B を EIM ドメインに参加させ、システム B 上にネットワーク認証サービスを構成する場合に必要です。

表 15. システム B のシングル・サインオン構成計画ワークシート

システム B の構成計画ワークシート	回答
次の情報は、システム B 用の EIM 構成ウィザードを完了する場合に使用します。	
ご使用のシステムで EIM をどのように構成したいか？	既存のドメインを結合する
ネットワーク認証サービスを構成したいか？ 注：シングル・サインオンを構成するには、ネットワーク認証サービスを構成する必要があります。	はい
「ネットワーク認証サービス」ウィザードは、「EIM 構成」ウィザードから開始します。以下の情報を使用して、「ネットワーク認証サービス」ウィザードを完成します。 注：「ネットワーク認証サービス」ウィザードは、「EIM 構成」ウィザードとは無関係に開始することができます。	
ご使用の System i 製品が属する Kerberos のデフォルト・レルムの名前は何か？ 注：Windows 2000 ドメインは、Kerberos レルムと同等です。Microsoft Active Directory は、Kerberos 認証をデフォルトのセキュリティ・メカニズムとして使用します。	MYCO.COM
Microsoft Active Directory を使用しているか？	はい
Kerberos デフォルト・レルムの Kerberos サーバーは？ Kerberos サーバーが listen するポートは？	KDC: kdc1.myco.com ポート: 88 注：これは、Kerberos サーバーのデフォルト・ポートです。
このデフォルト・レルムにパスワード・サーバーを構成したいか？ 「はい」であれば、以下の質問に回答してください。 この Kerberos サーバーのパスワード・サーバーの名前は？ パスワード・サーバーが listen するポートは？	はい パスワード・サーバー: kdc1.myco.com ポート: 464 注：これは、パスワード・サーバーのデフォルト・ポートです。
どのサービス用に keytab エントリーを作成したいか？ • i5/OS Kerberos 認証 • LDAP • IBM HTTP Server • i5/OS NetServer • ネットワーク・ファイルシステムのサーバー	i5/OS Kerberos 認証
ご使用の i5/OS サービス・プリンシパルのパスワードは何ですか？	systemb123
バッチ・ファイルを作成して、システム B のサービス・プリンシパルの Kerberos レジストリーへの追加を自動化しますか？	はい
パスワードを、バッチ・ファイルの i5/OS サービス・プリンシパルに組み込みますか？	はい
「ネットワーク認証サービス」ウィザードを終了すると、「EIM 構成」ウィザードに戻ります。次の情報は、システム B 用の EIM 構成ウィザードを完了する場合に使用します。	
結合したい EIM ドメインの EIM ドメイン・コントローラーの名前は？	systema.myco.com
接続を SSL または TLS で保護する計画があるか？	いいえ
EIM ドメイン・コントローラーが listen するポートは？	389

表 15. システム B のシングル・サインオン構成計画ワークシート (続き)

システム B の構成計画ワークシート	回答
ドメイン・コントローラーへの接続を使用したいユーザーは？これは、接続ユーザーです。 注: ウィザードが EIM ドメインとその中のオブジェクトを管理するのに十分な権限を必ず持つように、LDAP 管理者の識別名 (DN) とパスワードを指定します。	ユーザー・タイプ: 識別名およびパスワード 識別名: cn=administrator パスワード: mycopwd
結合したい EIM ドメインの名前は？	MyCoEimDomain
EIM ドメインの親 DN を指定したいか？	いいえ
EIM ドメインに追加したいユーザー・レジストリーの名前は？	ローカル i5/OS--SYSTEMB.MYCO.COM
EIM 操作を行うときに、どの EIM ユーザーをシステム B に使用させますか?これは、システム・ユーザーです。 注: このシナリオの前の方で、EIM 構成ウィザードを使用してシステム A 上にディレクトリー・サーバーを構成しました。その際に、LDAP 管理者の識別名 (DN) およびパスワードを作成しました。現在のところ、これがディレクトリー・サーバーに定義された唯一の DN です。したがってこれが、ここで提供しなければならない DN およびパスワードです。	ユーザー・タイプ: 識別名およびパスワード 識別名: cn=administrator パスワード: mycopwd

表 16. シングル・サインオン構成計画ワークシート - ユーザー・プロファイル

i5/OS ユーザー・プロファイル名	パスワードが指定されている	特殊権限 (特権クラス)	システム
SYSUSERA	いいえ	ユーザー	システム A
SYSUSERB	いいえ	ユーザー	システム B

表 17. シングル・サインオン構成計画ワークシート - EIM ドメイン・データ

ID 名	ユーザー・レジストリー	ユーザー ID	アソシエーション・タイプ	ID の説明
John Day	MYCO.COM	jday	ソース	Kerberos (Windows 2000) ログイン・ユーザー ID
John Day	SYSTEMA.MYCO.COM	JOHND	ターゲット	システム A 上の i5/OS ユーザー・プロファイル
John Day	SYSTEMB.MYCO.COM	DAYJO	ターゲット	システム B 上の i5/OS ユーザー・プロファイル
Sharon Jones	MYCO.COM	sjones	ソース	Kerberos (Windows 2000) ログイン・ユーザー ID
Sharon Jones	SYSTEMA.MYCO.COM	SHARONJ	ターゲット	システム A 上の i5/OS ユーザー・プロファイル
Sharon Jones	SYSTEMB.MYCO.COM	JONESSH	ターゲット	システム B 上の i5/OS ユーザー・プロファイル

表 18. シングル・サインオン構成計画ワークシート - EIM ドメイン・データ - ポリシー関連

ポリシー関連タイプ	ソース・ユーザー・レジストリー	ターゲット・ユーザー・レジストリー	ユーザー ID	説明
デフォルト・レジストリー	MYCO.COM	SYSTEMA.MYCO.COM	SYSUSERA	認証済み Kerberos ユーザーを該当する i5/OS ユーザー・プロファイルへマップする
デフォルト・レジストリー	MYCO.COM	SYSTEMB.MYCO.COM	SYSUSERB	認証済み Kerberos ユーザーを該当する i5/OS ユーザー・プロファイルへマップする

システム A の基本シングル・サインオン構成の作成

「EIM 構成 (EIM Configuration)」ウィザードは、基本的な EIM 構成を作成する援助となります。これはまた、基本的なネットワーク認証サービスの構成を作成するのに使用する「ネットワーク認証サービス」ウィザードもオープンします。

注: このシナリオの説明は、これまでにシステム A にディレクトリー・サーバーが構成されていないという前提事項に基づいています。しかし、既にディレクトリー・サーバーを構成している場合でも、これらの説明は、若干の相違点はあっても使用できます。これらの相違点については、構成の手順の該当する個所で注記します。

システム A に EIM およびネットワーク認証サービスを構成する場合は、ご使用の計画ワークシートの情報を使用します。このステップが完了したら、次のタスクを行ってください。

- 新しい EIM ドメインを作成する。
- システム A 上のディレクトリー・サーバーを EIM ドメイン・コントローラーとして構成する
- ネットワーク認証サービスを構成する。
- システム A 上の i5/OS レジストリーおよび Kerberos レジストリーに EIM レジストリー定義を作成する。
- システム A を構成して、EIM ドメインに参加する。
 1. System i ナビゲーターで、「システム A」 → 「ネットワーク」 → 「エンタープライズ識別マッピング」と展開します。
 2. 「構成 (Configuration)」を右クリックし、「構成」を選択して「EIM 構成」ウィザードを開始する。
 3. 「ようこそ」ページで、「新規ドメインの作成および結合 (Create and join a new domain)」を選択する。「次へ」をクリックします。
 4. 「EIM ドメイン・ロケーションの指定 (Specify EIM Domain Location)」ページで、「ローカル・ディレクトリー・サーバー上 (On the local Directory server)」を選択する。「次へ」をクリックします。
 5. 以下のタスクを完了してネットワーク認証サービスを構成する。
 - a. 「ネットワーク認証サービスを構成する (Configure Network Authentication Service)」ページで、「はい」を選択する。

注: これにより「ネットワーク認証サービス」ウィザードが開始します。このウィザードを用いて、いくつかの i5/OS インターフェースおよびサービスを構成し、Kerberos レルムに参加できます。

- b. 「レルム情報の指定 (Specify Realm Information)」 ページで、「デフォルト・レルム」フィールドに MYCO.COM を入力し、「**Microsoft Active Directory を Kerberos 認証に使用する (Microsoft Active Directory is used for Kerberos authentication)**」を選択する。「次へ」をクリックします。
 - c. 「KDC 情報の指定 (Specify KDC Information)」 ページで、「**KDC**」フィールドに Kerberos サーバーの名前として kdc1.myco.com を入力し、「**ポート**」フィールドに 88 を入力する。「次へ」をクリックします。
 - d. 「パスワード・サーバー情報の指定 (Specify Password Server Information)」 ページで、「はい」を選択する。「**パスワード・サーバー**」フィールドに kdc1.myco.com を入力し、「**ポート**」フィールドに 464 を入力します。「次へ」をクリックします。
 - e. 「keytab エントリーの選択」 ページで、「**i5/OS Kerberos 認証**」を選択する。「次へ」をクリックします。
 - f. 「i5/OS keytab エントリーの作成 (Create i5/OS Keytab Entry)」 ページで、パスワードを入力して確認してから、「次へ」をクリックする。例えば、systema123。このパスワードは、システム A サービス・プリンシパルが Kerberos サーバーに追加されるときに使用されます。
 - g. 「バッチ・ファイルの作成 (Create batch file)」 ページで、「はい」を選択し、以下の情報を指定してから「次へ」をクリックする。
 - 「**バッチ・ファイル (Batch file)**」: テキスト systema を、デフォルトのバッチ・ファイル名の終わりに追加する。例えば、C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystema.bat。
 - 「**パスワードの組み込み (Include password)**」を選択する。この結果、i5/OS サービス・プリンシパルに関連するパスワードは、すべてバッチ・ファイルに組み込まれます。パスワードは平文で表示され、バッチ・ファイルに対する読み取りアクセスを持っていれば誰でも読み取れる、ということに注意することが重要です。したがって、バッチ・ファイルは、使用した後に Kerberos サーバーと PC から削除することをお勧めします。

注: パスワードを組み込まない場合、パスワードを求めるプロンプトが、バッチ・ファイルが実行される時に出されます。
 - h. 「要約」 ページで、ネットワーク認証サービスの構成の詳細を検討する。「終了」をクリックします。
6. 「Directory Server の構成 (Configure Directory Server)」 ページで、以下の情報を入力してから「次へ」をクリックする。

注:

- このシナリオを開始する以前にディレクトリー・サーバーが構成済みだった場合は、「Directory Server の構成 (Configure Directory Server)」 ページの代わりに「接続用のユーザーの指定 (Specify User for Connection)」 ページが表示されます。この場合は LDAP 管理者用の識別名とパスワードを指定する必要があります。

| • i5/OS V6R1 が実行されているシステムに、複数のディレクトリー・サーバーを構成した場合は、
| 「ディレクトリー・サーバー・インスタンスの指定 (Specify Directory Server Instance)」 および
| 「接続用のユーザーの指定 (Specify User for Connection)」 ページが表示されます。この場
| 合は LDAP 管理者用の識別名とパスワードを指定する必要があります。

- **ポート (Port):** 389
- **識別名:** cn=administrator
- **パスワード:** mycopwd

7. 「ドメインの指定 (Specify Domain)」 ページで、「ドメイン」フィールドにドメインの名前を入力する。例えば、MyCoEimDomain。
8. 「ドメインの親 DN の指定 (Specify Parent DN for Domain)」 ページで、「いいえ」を選択する。「次へ」をクリックします。

注: ディレクトリー・サーバーがアクティブな場合、変更を有効にするためにはディレクトリー・サーバーを終了して再始動する必要があることを示すメッセージが表示されます。「はい」をクリックして、ディレクトリー・サーバーを再始動してください。

9. 「レジストリー情報 (Registry Information)」 ページで、「ローカル i5/OS」および「Kerberos」を選択する。「次へ」をクリックします。レジストリー名を書き留めます。このレジストリー名は、EIM ID へのアソシエーションの作成時に必要です。

注:

- レジストリー名は、ドメイン内で固有である必要があります。
- 特定のレジストリー定義命名計画を使用したい場合には、ユーザー・レジストリー用の特定のレジストリー定義名を入力することができます。ただし、このシナリオではデフォルト値を受け入れることができます。

10. 「EIM システム・ユーザーの指定 (Specify EIM System User)」 ページで、オペレーティング・システム機能の代わりに EIM 操作を実行している場合は、オペレーティング・システムが使用するユーザーを選択し、「次へ」をクリックする。

注: このシナリオの手順を実行する前にディレクトリー・サーバーを構成していなかった場合、選択できる唯一の識別名 (DN) は、LDAP 管理者の DN です。

- ユーザー・タイプ: 識別名およびパスワード
- 識別名: cn=administrator
- パスワード: mycopwd

11. 「要約」 ページで、EIM 構成情報を確認する。「終了」をクリックします。

システム B を EIM ドメインに参加するよう構成し、さらにネットワーク認証サービス用としてシステム B を構成

システム A 上に新規ドメインを作成し、ネットワーク認証サービスを構成した後は、システム B を構成して、EIM ドメインに参加し、システム B 上にネットワーク認証サービスを構成する必要があります。

ワークシートの情報を使用して、このステップを完了します。

1. System i ナビゲーターで、「システム B」 → 「ネットワーク」 → 「エンタープライズ識別マッピング」と展開します。
2. 「構成 (Configuration)」 を右クリックし、「構成 (Configure)」 を選択して構成ウィザードを開始します。
3. 「ようこそ」 ページで、「既存のドメインの結合 (Join an existing domain)」 を選択する。「次へ」 をクリックします。
4. 以下のタスクを完了してネットワーク認証サービスを構成する。
 - a. 「ネットワーク認証サービスを構成する (Configure Network Authentication Service)」 ページで、「はい」 を選択する。

注: これにより「ネットワーク認証サービス」ウィザードが開始します。このウィザードを使用すると、いくつかの i5/OS インターフェースおよびサービスを構成して、Kerberos ネットワークに参加できます。

- b. 「レルム情報の指定 (Specify Realm Information)」 ページで、「デフォルト・レルム」フィールドに MYCO.COM を入力し、「**Microsoft Active Directory を Kerberos 認証に使用する (Microsoft Active Directory is used for Kerberos authentication)**」を選択する。「次へ」をクリックします。
 - c. 「KDC 情報の指定 (Specify KDC Information)」 ページで、「**KDC**」フィールドに Kerberos サーバーの名前として kdc1.myco.com を入力し、「**ポート**」フィールドに 88 を入力する。「次へ」をクリックします。
 - d. 「パスワード・サーバー情報の指定 (Specify Password Server Information)」 ページで、「はい」を選択する。「**パスワード・サーバー**」フィールドに kdc1.myco.com を入力し、「**ポート**」フィールドに 464 を入力します。「次へ」をクリックします。
 - e. 「keytab エントリーの選択」 ページで、「**i5/OS Kerberos 認証**」を選択する。「次へ」をクリックします。
 - f. 「i5/OS Keytab エントリーの作成 (Create i5/OS Keytab Entry)」 ページでパスワードを入力して確認した上で、「次へ」をクリックし、例えば、「systema123」とタイプする。このパスワードは、システム A サービス・プリンシパルが Kerberos サーバーに追加されるときに使用されます。
 - g. オプション: 「バッチ・ファイルの作成 (Create batch file)」 ページで、「はい」を選択し、以下の情報を指定してから「次へ」をクリックする。
 - 「**バッチ・ファイル (Batch file)**」: テキスト systemb を、デフォルトのバッチ・ファイル名の終わりに追加する。例えば、C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystemb.bat。
 - 「**パスワードの組み込み (Include password)**」を選択する。これにより、i5/OS サービス・プリンシパルに関連付けられるすべてのパスワードが、バッチ・ファイルに必ず組み込まれます。パスワードは平文で表示され、バッチ・ファイルに対する読み取りアクセスを持っていれば誰でも読み取れる、ということに注意することが重要です。したがって、バッチ・ファイルは、使用した後に Kerberos サーバーと PC から削除することをお勧めします。
- 注:** パスワードを組み込まない場合、パスワードを求めるプロンプトが、バッチ・ファイルが実行される時に出されます。
- h. 「要約」 ページで、ネットワーク認証サービスの構成の詳細を検討する。「終了」をクリックします。
5. 「ドメイン・コントローラーの指定 (Specify Domain Controller)」 ページで、以下の情報を入力してから、「次へ」をクリックする。
 - **ドメイン・コントローラー名:** systema.myco.com
 - **ポート (Port):** 389
 6. 「接続のユーザーの指定 (Specify User for Connection)」 ページで、以下の情報を入力してから、「次へ」をクリックする。

注: システム A 上に、このシナリオで前に作成した LDAP 管理者の DN およびパスワードを指定します。

- a. **ユーザー・タイプ:** 識別名およびパスワード
- b. **識別名:** cn=administrator
- c. **パスワード:** mycopwd

7. 「ドメインの指定 (Specify Domain)」 ページで、参加したいドメインの名前を選択する。「次へ」をクリックします。例えば、MyCoEimDomain。
8. 「レジストリー情報 (Registry Information)」 ページで、「ローカル i5/OS」を選択し、「Kerberos レジストリー」を選択解除する。(Kerberos レジストリーは、MyCoEimDomain ドメインを作成した時に作成されました。) 「次へ」をクリックします。レジストリー名を書き留めます。このレジストリー名は、EIM ID へのアソシエーションの作成時に必要です。

注:

- レジストリー名は、ドメイン内で固有である必要があります。
- 特定のレジストリー定義命名計画を使用したい場合には、ユーザー・レジストリー用の特定のレジストリー定義名を入力することができます。ただし、このシナリオではデフォルト値を受け入れることができます。

9. 「EIM システム・ユーザーの指定 (Specify EIM System User)」 ページで、オペレーティング・システム機能の代わりに EIM 操作を実行している場合は、オペレーティング・システムが使用するユーザーを選択し、「次へ」をクリックする。

注: システム A 上に、このシナリオで前に作成した LDAP 管理者の DN およびパスワードを指定します。

- a. ユーザー・タイプ: 識別名およびパスワード
- b. 識別名: cn=administrator
- c. パスワード: mycopwd

10. 「要約」 ページで、EIM 構成を確認する。「終了」をクリックします。

Kerberos サーバーへの両方の i5/OS サービス・プリンシパルの追加

必要な i5/OS サービス・プリンシパルを Kerberos サーバーに手動で追加できます。このシナリオで説明するようにバッチ・ファイルを使用して追加することもできます。

このバッチ・ファイルはステップ 2 で作成しました。このファイルを使用するには、ファイル転送プロトコル (FTP) を使用してファイルを Kerberos サーバーにコピーして実行することができます。

バッチ・ファイルを使用して Kerberos サーバーにプリンシパル名を追加するには、以下の手順を行います。

1. FTP バッチ・ファイルの作成

- a. 管理者がネットワーク認証サービスを構成するために使用した Windows 2000 ワークステーション上で、コマンド・プロンプトをオープンし、ftp kdc1.myco.com と入力する。これにより FTP セッションが PC 上で開始されます。管理者のユーザー名とパスワードを求めるプロンプトが出されます。
- b. FTP プロンプトで lcd "C:¥Documents and Settings¥All Users¥Documents¥IBM¥Client Access" と入力する。Enter キーを押します。ユーザーは、メッセージ「現在のローカル・ディレクトリーは C:¥Documents and Settings¥All Users¥Documents¥IBM¥Client Access」を受け取るはずですが。
- c. FTP プロンプトで cd ¥mydirectory と入力する。ここで mydirectory は、kdc1.myco.com 上にあるディレクトリーです。
- d. FTP プロンプトで put NASConfigsystema.bat と入力する。メッセージ「226 転送が完了しました (226 Transfer complete)」を受け取るはずですが。
- e. quit と入力して FTP セッションを終了する。

2. kdc1.myco.com 上で両方のバッチ・ファイルを実行する

- a. Windows 2000 サーバー上で、バッチ・ファイルを転送したディレクトリーをオープンする。
- b. NASConfigsystema.bat ファイルを見つけ、それをダブルクリックして、実行します。
- c. NASConfigsystemb.bat について、1a (75 ページ) から 2b までのステップを繰り返す。
- d. 各ファイルの実行後、次の手順を行って、i5/OS プリンシパルが Kerberos サーバーに追加されたことを検査します。
 - 1) Windows 2000 サーバー上で、「管理ツール (Administrative Tools)」 → 「Active Directory ユーザーとコンピューター (Active Directory Users and Computers)」 → 「ユーザー」と展開する。
 - 2) 該当する Windows 2000 ドメインを選択して、System i プラットフォームにユーザー・アカウントがあることを検査します。

注: この Windows 2000 ドメインは、ネットワーク認証サービス構成で指定したデフォルト・レルム名と同じでなければなりません。

- 3) 表示されるユーザーのリストで、**systema_1_krbsvr400** および **systemb_1_krbsvr400** を探す。これらは、i5/OS プリンシパル名用に生成されたユーザー・アカウントです。
- 4) Active Directory ユーザーに関するプロパティにアクセスする。「アカウント」タブから、「アカウントの委任は承認されています (Account is trusted for delegation)」を選択します。

注: このオプションのステップは、ご使用のシステムがユーザーの信任状を他のシステムに委任または転送することができるようにします。その結果、i5/OS サービス・プリンシパルは、ユーザーに代わって複数のシステムのサービスにアクセスすることができます。これは、多重階層ネットワークにおいて役立ちます。

システム A およびシステム B 上でユーザー・プロファイルを作成

MYCO.COM Kerberos レジストリー内のすべてのユーザーを、ご使用の各 System i プラットフォームの単一の i5/OS ユーザー・プロファイルにマップする必要があります。したがって、システム A およびシステム B に i5/OS ユーザー・プロファイルを作成する必要があります。

ワークシートからの情報を使用して、これらのユーザー用のユーザー・プロファイルを以下のように作成します。

1. System i ナビゲーターで、「システム A」 → 「ユーザーとグループ」と展開します。
2. 「すべてのユーザー (All Users)」を右クリックして、「新しいユーザー (New User)」を選択する。
3. 「新規ユーザー (New User)」ダイアログ・ボックスで、「ユーザー名 (User name)」フィールドに SYSUSERA と入力する。
4. 「パスワード」フィールドで、「パスワードなし (サインオンは許可されない) (No password (sign-on not allowed))」を選択する。
5. 「機能 (Capabilities)」をクリックする。
6. 「特権 (Privileges)」ページの「特権クラス (Privilege class)」フィールドで「ユーザー」を選択する。「OK」をクリックし、「追加 (Add)」をクリックします。
7. システム B でステップ 1 から 6 を繰り返しますが、「ユーザー名」フィールドには、SYSUSERB と入力します。

システム A およびシステム B 上でホーム・ディレクトリーを作成

i5/OS および i5/OS アプリケーションに接続する各ユーザーには、/ホーム・ディレクトリーのディレクトリーが必要です。このディレクトリーは、ユーザーの Kerberos 信任状キャッシュを保管します。

ユーザーのホーム・ディレクトリーを作成するには、以下の手順を実行してください。

1. システム A コマンド行で、CRTDIR '/home/user profile' と入力します。ここで、user profile は、ユーザーの i5/OS ユーザー・プロファイル名です。例えば、CRTDIR '/home/SYSUSERA'。
2. システム B でこのコマンドを繰り返しますが、SYSUSERB を指定して、システム B 上のユーザー・プロファイル用のホーム・ディレクトリーを作成します。

システム A および B 上でのネットワーク認証サービスのテスト

両システムのネットワーク認証サービス構成作業が完了した後は、システム A とシステム B の両方の構成が正しく働くか検査する必要があります。

このテストは、システム A およびシステム B プリンシパル用のチケット許可チケットを要求するためのステップを実行することによって、行うことができます。

注: この手順を行う前に、i5/OS ユーザー・プロファイルのホーム・ディレクトリーを作成しているか確認してください。

1. コマンド行で QSH と入力して、Qshell インタープリターを開始する。
2. keytab list と入力して、keytab ファイルに登録されているプリンシパルのリストを表示する。このシナリオでは、システム A のプリンシパル名として、krbsvr400/systema.myco.com@MYCO.COM が表示されるはずです。
3. kinit -k krbsvr400/systema.myco.com@MYCO.COM と入力して、Kerberos サーバーからチケット許可チケットを要求する。このコマンドを実行すると、ご使用のシステムが正しく構成され、しかもキータブ・ファイル内のパスワードが、Kerberos サーバーに保管されているパスワードと一致しているか検査できます。正しく入力されれば、kinit コマンドがエラーなしに表示されます。
4. klist と入力し、デフォルト・プリンシパルが krbsvr400/systema.myco.com@MYCO.COM であることを検証する。このコマンドにより、Kerberos 信任状キャッシュの内容が表示され、i5/OS サービス・プリンシパルに有効な許可証が作成され、かつシステムの信任状キャッシュに入れられていることが検査されます。

```
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
$
```

2 名の管理者 John Day と Sharon Jones 用の EIM ID の作成

シングル・サインオンのテスト環境をセットアップする一環として、2 人の管理者の EIM ID を作成して、2 人ともその Windows ユーザー ID を使用して、i5/OS にログオンできるようにする必要があります。

このシナリオでは、一方は John Day という名前で、他方は Sharon Jones という名前の、2 つの EIM ID を作成します。EIM ID を作成するには、以下の手順を行ってください。

1. System i ナビゲーターで、「システム A」→「ネットワーク」→「エンタープライズ識別マッピング」→「ドメイン管理」→「MyCoEimDomain」と展開します。

注: ドメイン・コントローラーに接続するよう求めるプロンプトが出される場合があります。その場合、「EIM ドメイン・コントローラーへの接続」ダイアログ・ボックスが表示されます。ドメイン内でアクションを実行できるためには、まずドメインに接続する必要があります。ドメイン・コントローラーに接続するには、以下の情報を入力して「OK」をクリックします。

- a. ユーザー・タイプ: 識別名
 - b. 識別名: cn=administrator
 - c. パスワード: mycopwd
2. 「ID」を右クリックして、「新規 ID」を選択する。
 3. 「新規 EIM ID」ダイアログ・ボックスで、「ID」フィールドに John Day と入力する。「OK」をクリックします。
 4. ステップ 2 から 4 までを繰り返しますが、「ID」フィールドには Sharon Jones と入力します。

John Day 用の ID アソシエーションの作成

John Day という EIM ID と、その ID によって表される個人が使用するユーザー ID との間に、適切なアソシエーションを作成する必要があります。これらの ID アソシエーションは、正しく構成されていれば、ユーザーがシングル・サインオン環境に参加できるようにします。

このシナリオでは、John Day という ID 用に、以下のように 1 つのソース・アソシエーションと 2 つのターゲット関連を作成する必要があります。

- John Day が Windows およびネットワークに対してログオンするユーザー ID である Kerberos プリンシパル jday 用のソース・アソシエーション。ソース・アソシエーションにより、Kerberos プリンシパルは、対応するターゲット関連に定義されている別のユーザー ID にマップできます。
- JOHND i5/OS ユーザー・プロファイルのターゲット関連。これは、John Day が、System i ナビゲーター およびシステム A 上の他の i5/OS アプリケーションにログインする際に使用するユーザー ID です。ターゲット関連は、探索操作のマッピングが、同じ ID のソース・アソシエーションで定義された別の ID からこのユーザー ID にマップできることを指定します。
- DAYJO i5/OS ユーザー・プロファイルのターゲット関連。これは、John Day が、System i ナビゲーター およびシステム B 上の他の i5/OS アプリケーションにログインする際に使用するユーザー ID です。ターゲット関連は、探索操作のマッピングが、同じ ID のソース・アソシエーションで定義された別の ID からこのユーザー ID にマップできることを指定します。

計画ワークシートからの情報を使用して、アソシエーションを作成します。

John Day の Kerberos プリンシパル用のソース・アソシエーションを作成するには、以下の手順を行います。

1. システム A 上で、「ネットワーク」 → 「エンタープライズ識別マッピング」 → 「ドメイン管理」 → 「MyCoEimDomain」 → 「ID」と展開する。
2. 「John Day」を右クリックして「プロパティ」を選択する。
3. 「関連」ページで、「追加」をクリックする。
4. 「関連の追加」ダイアログ・ボックスで、以下の情報を、指定するかあるいはクリックするために「参照...」してから、「OK」をクリックする。
 - a. レジストリー: MYCO.COM
 - b. ユーザー: jday
 - c. 関連タイプ: Source
5. 「OK」をクリックし、「関連の追加」ダイアログ・ボックスをクローズする。

システム A 上に、John Day の i5/OS ユーザー・プロファイルのターゲット関連を作成するには、以下のステップに従います。

6. 「関連」ページで、「追加」をクリックする。

7. 「**関連の追加**」ダイアログ・ボックスで、以下の情報を、指定するかあるいはクリックするために「参照...」してから、「**OK**」をクリックする。
 - a. レジストリー: SYSTEMA.MYCO.COM
 - b. ユーザー: JOHND
 - c. 関連タイプ: Target
8. 「**OK**」をクリックし、「**関連の追加**」ダイアログ・ボックスをクローズする。

システム B 上に、John Day の i5/OS ユーザー・プロファイルのターゲット関連を作成するには、以下のステップに従います。
9. 「**関連**」ページで、「**追加**」をクリックする。
10. 「**関連の追加**」ダイアログ・ボックスで、以下の情報を、指定するかあるいはクリックするために「参照...」してから、「**OK**」をクリックする。
 - a. レジストリー: SYSTEMB.MYCO.COM
 - b. ユーザー: DAYJO
 - c. 関連タイプ: Target
11. 「**OK**」をクリックし、「**関連の追加**」ダイアログ・ボックスをクローズする。
12. 「**OK**」をクリックし、「**プロパティ**」ダイアログ・ボックスをクローズする。

Sharon Jones 用の ID アソシエーションの作成

Sharon Jones という EIM ID と、その ID によって表される個人が使用するユーザー ID との間に、適切なアソシエーションを作成する必要があります。これらのアソシエーションは、正しく構成されていれば、ユーザーがシングル・サインオン環境に参加できるようにします。

このシナリオでは、Sharon Jones という ID 用に、以下のように 1 つのソース・アソシエーションと 2 つのターゲット関連を作成する必要があります。

- Sharon Jones が Windows およびネットワークに対してログオンするユーザー ID である Kerberos プリンシパル sjones 用のソース・アソシエーション。ソース・アソシエーションにより、Kerberos プリンシパルは、対応するターゲット関連に定義されている別のユーザー ID にマップできます。
- SHARONJ i5/OS ユーザー・プロファイルのターゲット関連。これは、Sharon Jones が、System i ナビゲーター およびシステム A 上の他の i5/OS アプリケーションにログインする際に使用するユーザー ID です。ターゲット関連は、探索操作のマッピングが、同じ ID のソース・アソシエーションで定義された別の ID からこのユーザー ID にマップできることを指定します。
- JONESSH i5/OS ユーザー・プロファイルのターゲット関連。これは、Sharon Jones が、System i ナビゲーター およびシステム B 上の他の i5/OS アプリケーションにログインする際に使用するユーザー ID です。ターゲット関連は、探索操作のマッピングが、同じ ID のソース・アソシエーションで定義された別の ID からこのユーザー ID にマップできることを指定します。

計画ワークシートからの情報を使用して、アソシエーションを作成します。

Sharon Jones の Kerberos プリンシパル用のソース・アソシエーションを作成するには、以下の手順を行います。

1. システム A 上で、「**ネットワーク**」 → 「**エンタープライズ識別マッピング**」 → 「**ドメイン管理**」 → 「**MyCoEimDomain**」 → 「**ID**」と展開する。
2. 「**Sharon Jones**」を右クリックして「**プロパティ**」を選択する。
3. 「**関連**」ページで、「**追加**」をクリックする。

4. 「**関連の追加**」ダイアログ・ボックスで、以下の情報を、指定するかあるいは選択するために「**参照...**」してから、「**OK**」をクリックする。
 - a. **レジストリー**: MYCO.COM
 - b. **ユーザー**: sjones
 - c. **関連タイプ**: Source
5. 「**OK**」をクリックし、「**関連の追加**」ダイアログ・ボックスをクローズする。

システム A 上に、Sharon Jones の i5/OS ユーザー・プロファイルへのターゲット関連を作成するには、以下のステップに従います。

6. 「**関連**」ページで、「**追加**」をクリックする。
7. 「**関連の追加**」ダイアログ・ボックスで、以下の情報を、指定するかあるいは選択するために「**参照...**」してから、「**OK**」をクリックする。
 - a. **レジストリー**: SYSTEMA.MYCO.COM
 - b. **ユーザー**: SHARONJ
 - c. **関連タイプ**: Target
8. 「**OK**」をクリックし、「**関連の追加**」ダイアログ・ボックスをクローズする。

システム B 上に、Sharon Jones の i5/OS ユーザー・プロファイルへのターゲット関連を作成するには、以下のステップに従います。

9. 「**関連**」ページで、「**追加**」をクリックする。
10. 「**関連の追加**」ダイアログ・ボックスで、以下の情報を、指定するかあるいは選択するために「**参照...**」してから、「**OK**」をクリックする。
 - a. **レジストリー**: SYSTEMB.MYCO.COM
 - b. **ユーザー**: JONESSH
 - c. **関連タイプ**: Target
11. 「**OK**」をクリックし、「**関連の追加**」ダイアログ・ボックスをクローズする。
12. 「**OK**」をクリックし、「**プロパティ**」ダイアログ・ボックスをクローズする。

デフォルト・レジストリー・ポリシー関連の作成

ポリシー関連を使用して、ユーザーのグループと単一のターゲット・ユーザー ID を直接マッピングすることができます。

Windows 2000 サーバー上のすべての Microsoft Active Directory のユーザーを、システム A のユーザー・プロファイル SYSUSERA およびシステム B のユーザー・プロファイル SYSUSERB にマップしたいものとして。この場合は、MYCO.COM Kerberos レジストリー内のすべてのユーザー ID (ID アソシエーションが存在しない) をシステム A 上の単一の i5/OS ユーザー・プロファイルにマップする、デフォルトのレジストリー・ポリシー関連を作成することができます。

このゴールを達成するには、2 つのポリシー関連が必要です。各ポリシー関連は、アソシエーションのソースとして MYCO.COM ユーザー・レジストリー定義を使用します。しかし、各ポリシー関連は、Kerberos ユーザーがアクセスする System i プラットフォームによっては、このレジストリー内のユーザー ID を異なるターゲット・ユーザー ID にマップします。

- あるポリシー関連は MYCO.COM ユーザー・レジストリー内の Kerberos プリンシパルを、SYSTEMA.MYCO.COM のターゲット・レジストリー内のターゲット・ユーザー SYSUSERA に対してマップします。

- 他のポリシー関連は MYCO.COM ユーザー・レジストリー内の Kerberos プリンシパルを、SYSTEMB.MYCO.COM のターゲット・レジストリー内のターゲット・ユーザー SYSUSERB に対してマップします。

計画ワークシートからの情報を使用して、2 つのデフォルト・レジストリー・ポリシー関連を作成します。

ポリシー関連を使用する前に、まず、ドメインがマッピング探索操作にポリシー関連を使用できるようにする必要があります。

該当のドメインがポリシー関連を使用してマッピング探索操作ができるようにするには、以下のステップを実行しておく必要があります。

1. System i ナビゲーター で、「システム A」 → 「ネットワーク」 → 「エンタープライズ識別マッピング」 → 「ドメイン管理」と展開します。
2. 「MyCoEimDomain」を右クリックして、「マッピング・ポリシー」を選択する。
3. 「一般」ページで、「ドメイン MyCoEimDomain のポリシー関連を使用してマッピング・ルックアップを使用可能にする」を選択する。

システム A 上の SYSUSERA ユーザー・プロファイルにマップするユーザー用に、デフォルトのレジストリー・ポリシー関連を作成するには、以下のステップを実行します。

1. 「レジストリー」ページで、「追加」をクリックする。
2. 「デフォルト・レジストリー・ポリシー関連の追加」ダイアログ・ボックスで、以下の情報を、指定するかあるいは選択するために「参照...」してから、「OK」をクリックする。
 - a. ソース・レジストリー: MYCO.COM
 - b. ターゲット・レジストリー: SYSTEMA.MYCO.COM
 - c. ターゲット・ユーザー: SYSUSERB
3. 「OK」をクリックし、「マッピング・ポリシー」ダイアログ・ボックスをクローズする。

システム B 上の SYSUSERB ユーザー・プロファイルにマップするユーザー用に、デフォルトのレジストリー・ポリシー関連を作成するには、以下のステップを実行します。

1. 「レジストリー」ページで、「追加」をクリックする。
2. 「デフォルト・レジストリー・ポリシー関連の追加」ダイアログ・ボックスで、以下の情報を、指定するかあるいは選択するために「参照...」してから、「OK」をクリックする。
 - a. ソース・レジストリー: MYCO.COM
 - b. ターゲット・レジストリー: SYSTEMB.MYCO.COM
 - c. ターゲット・ユーザー: SYSUSERB
3. 「OK」をクリックし、「マッピング・ポリシー」ダイアログ・ボックスをクローズする。

レジストリーの探索操作への参加とポリシー関連の使用可能化

レジストリーにポリシー関連を使用するには、そのレジストリーにポリシー関連を使用できるようにするだけでなく、レジストリーが探索操作に参加できるようにする必要があります。

EIM によって、各レジストリーが EIM に参加する方法をユーザーが制御することができるようになります。ポリシー関連はエンタープライズの中で大きな影響を与えることがあるため、ユーザーは、レジストリーがポリシー関連によって影響されてよいかをどうかを制御することができます。また、レジストリーがマッピング探索操作に参加できるかどうかを制御することもできます。

レジストリーが、ポリシー関連を使用して探索操作に参加できるようにするために、以下の手順を実行します。

MYCO.COM レジストリーがマッピング探索操作に参加できるようにするには、以下の手順を行います。

1. System i ナビゲーター で、「システム A」 → 「ネットワーク」 → 「エンタープライズ識別マッピング」 → 「ドメイン管理」 → 「MyCoEimDomain」 → 「ユーザー・レジストリー」と展開します。
2. 「MYCO.COM」レジストリーを右クリックして、「マッピング・ポリシー」を選択する。
3. 「一般」ページで、「マッピング探索をレジストリー MYCO.COM で使用可能にする (Enable mapping lookups for registry MYCO.COM)」を選択し、「OK」をクリックする。

SYSTEMA.MYCO.COM レジストリーがマッピング探索操作に参加でき、かつポリシー関連を使用できるようにするには、以下の手順を行います。

4. System i ナビゲーター で、「システム A」 → 「ネットワーク」 → 「エンタープライズ識別マッピング」 → 「ドメイン管理」 → 「MyCoEimDomain」 → 「ユーザー・レジストリー」と展開します。
5. 「SYSTEMA.MYCO.COM」レジストリーを右クリックして、「マッピング・ポリシー」を選択する。
6. 「一般」ページで、「レジストリー SYSTEMA.MYCO.COM のマッピング・ルックアップを使用可能にする」を選択し、「ポリシー関連を使用」を選択し、「OK」をクリックする。
7. ステップ 1 から 6 を繰り返して、SYSTEMB.MYCO.COM レジストリーがマッピング探索操作に参加して、ポリシー関連を使用できるようにします。ただし、「一般」ページでは、「レジストリー SYSTEMB.MYCO.COM のマッピング・ルックアップを使用可能にする」を選択し、「ポリシー関連を使用」を選択して、「OK」をクリックします。

EIM ID マッピングのテスト

これで、必要なアソシエーションはすべて作成されたので、EIM マッピング探索操作が、構成されたアソシエーションに基づいた正しい結果を戻すことを検証する必要があります。

このシナリオの場合、各管理者用の ID アソシエーションで使用されるマッピングと、デフォルト・レジストリー・ポリシー関連用で使用されるマッピングをテストする必要があります。EIM マッピングをテストするには、以下の手順を行います。

John Day 用のマッピングをテストする

John Day 用の ID マッピングが期待どおりに機能するかをテストするために、以下の手順を行います。

1. System i ナビゲーター で、「システム A」 → 「ネットワーク」 → 「エンタープライズ識別マッピング」 → 「ドメイン管理」 → 「MyCoEimDomain」と展開します。

注: ドメイン・コントローラーに接続するよう求めるプロンプトが出される場合があります。その場合、「EIM ドメイン・コントローラーへの接続」ダイアログ・ボックスが表示されます。ドメイン内でアクションを実行できるためには、まずドメインに接続する必要があります。ドメイン・コントローラーに接続するには、以下の情報を入力して「OK」をクリックします。

- a. ユーザー・タイプ: 識別名
 - b. 識別名: cn=administrator
 - c. パスワード: mycopwd
2. 「MyCoEimDomain」を右クリックして、「マッピングをテスト」を選択する。
 3. 「マッピングのテスト」ダイアログ・ボックスで、以下の情報を選択するために「参照...」を指定またはクリックしてから、「テスト」をクリックする。
 - a. ソース・レジストリー: MYCO.COM

- b. ソース・ユーザー: jday
- c. ターゲット・レジストリー: SYSTEMA.MYCO.COM

結果は、以下のようにページの「検索されたマッピング」という部分に表示されます。

これらのフィールド	表示される結果
ターゲット・ユーザー	JOHND
発信元	EIM ID: John Day

4. 「クローズ」をクリックします。
5. これらのステップを繰り返しますが、「ターゲット・レジストリー」ページでは SYSTEMB.MYCO.COM を選択します。結果は、以下のようにページの「検索されたマッピング」という部分に表示されます。

これらのフィールド	表示される結果
ターゲット・ユーザー	DAYJO
発信元	EIM ID: John Day

Sharon Jones 用のマッピングをテストする

Sharon Jones 用の 個別のアソシエーションに使用されるマッピングをテストするには、以下の手順を行います。

6. System i ナビゲーター で、「システム A」 → 「ネットワーク」 → 「エンタープライズ識別マッピング」 → 「ドメイン管理」 → 「MyCoEimDomain」と展開します。

注: ドメイン・コントローラーに接続するよう求めるプロンプトが出される場合があります。その場合、「EIM ドメイン・コントローラーへの接続 (Connect to EIM Domain Controller)」ダイアログ・ボックスが表示されます。ドメイン内でアクションを実行できるためには、まずドメインに接続する必要があります。ドメイン・コントローラーに接続するには、以下の情報を入力して「OK」をクリックします。

- a. ユーザー・タイプ: 識別名
 - b. 識別名: cn=administrator
 - c. パスワード: mycopwd
7. 「MyCoEimDomain」を右クリックして、「マッピングのテスト」を選択する。
 8. 「マッピングのテスト」ダイアログ・ボックスで、以下の情報を選択するために「参照...」を指定またはクリックしてから、「テスト」をクリックする。
 - a. ソース・レジストリー: MYCO.COM
 - b. ソース・ユーザー: sjones
 - c. ターゲット・レジストリー: SYSTEMA.MYCO.COM

結果は、以下のようにページの「検索されたマッピング」という部分に表示されます。

これらのフィールド	表示される結果
ターゲット・ユーザー	SHARONJ
発信元	EIM ID: Sharon Jones

9. 「クローズ」をクリックします。

10. ステップ 1 (82 ページ) から 9 (83 ページ) を選択しますが、「ターゲット・レジストリー」フィールドでは SYSTEMB.MYCO.COM を選択します。結果は、以下のようにページの「検索されたマッピング」という部分に表示されます。

これらのフィールド	表示される結果
ターゲット・ユーザー	JONESSH
発信元	EIM ID: Sharon Jones

デフォルト・レジストリー・ポリシー関連用に使されるマッピングをテストする

受注部門内のユーザーの場合に、定義したポリシー関連に基づいてマッピングが期待どおりに機能するかをテストするには、以下の手順を行います。

11. System i ナビゲーター で、「システム A」 → 「ネットワーク」 → 「エンタープライズ識別マッピング」 → 「ドメイン管理」 → 「MyCoEimDomain」と展開します。

注: ドメイン・コントローラーに接続するよう求めるプロンプトが出される場合があります。その場合、「EIM ドメイン・コントローラーへの接続 (Connect to EIM Domain Controller)」ダイアログ・ボックスが表示されます。ドメイン内でアクションを実行できるためには、まずドメインに接続する必要があります。ドメイン・コントローラーに接続するには、以下の情報を入力して「OK」をクリックします。

- a. ユーザー・タイプ: 識別名
 - b. 識別名: cn=administrator
 - c. パスワード: mycopwd
12. 「MyCoEimDomain」を右クリックして、「マッピングをテスト」を選択する。
13. 「マッピングのテスト」ダイアログ・ボックスで、以下の情報を選択するために「参照...」を指定またはクリックしてから、「テスト」をクリックする。
- a. ソース・レジストリー: MYCO.COM
 - b. ソース・ユーザー: mmiller
 - c. ターゲット・レジストリー: SYSTEMA.MYCO.COM

結果は、以下のようにページの「検索されたマッピング」という部分に表示されます。

これらのフィールド	表示される結果
ターゲット・ユーザー	SYSUSERA
発信元	レジストリー・ポリシー関連

14. 「クローズ」をクリックします。

ユーザーをシステム B 上の SYSUSERB プロファイルにマップする、デフォルト・レジストリー・ポリシー関連用に使されるマッピングをテストするには、以下の手順を行います。

1. System i ナビゲーター で、「システム A」 → 「ネットワーク」 → 「エンタープライズ識別マッピング」 → 「ドメイン管理」 → 「MyCoEimDomain」と展開します。

注: ドメイン・コントローラーに接続するよう求めるプロンプトが出される場合があります。その場合、「EIM ドメイン・コントローラーへの接続」ダイアログ・ボックスが表示されます。ドメイン内でアクションを実行できるためには、まずドメインに接続する必要があります。ドメイン・コントローラーに接続するには、以下の情報を入力して「OK」をクリックします。

- a. ユーザー・タイプ: 識別名
 - b. 識別名: cn=administrator
 - c. パスワード: mycopwd
2. 「MyCoEimDomain」を右クリックして、「マッピングをテスト」を選択する。
 3. 「マッピングのテスト」ダイアログ・ボックスで、以下の情報を選択するために「参照...」を指定またはクリックしてから、「テスト」をクリックする。
 - a. ソース・レジストリー: MYCO.COM
 - b. ソース・ユーザー: ksmith
 - c. ターゲット・レジストリー: SYSTEMB.MYCO.COM

結果は、以下のようにページの「検索されたマッピング」という部分に表示されます。

これらのフィールド	表示される結果
ターゲット・ユーザー	SYSUSERB
発信元	レジストリー・ポリシー関連

4. 「クローズ」をクリックします。マッピングまたは通信に関する問題を示すメッセージまたはエラーを受け取った場合は、『EIM のトラブルシューティング (Troubleshooting EIM)』を参照し、これらの問題の解決策を見つける補助としてください。

Kerberos 認証を使用するよう System i Access for Windows アプリケーションを構成

シングル・サインオンという目的に基づいて、受注部門のすべてのユーザーは、System i ナビゲーターを用いてシステム A および B にアクセスする前に、Kerberos を使用して認証を受けておく必要があります。したがって、Kerberos 認証を使用するために System i Access for Windows を構成しておかなければなりません。

Kerberos 認証を使用する System i Access for Windows アプリケーションを構成するには、次の手順に従ってください。

注: 全ユーザーは、これらのすべての手順を自身の PC 上で実行する必要があります。

1. PC にサインインして、Windows ドメインにログオンします。
2. PC の System i ナビゲーターで、「システム A」を右マウス・ボタン・クリックして、「プロパティ」を選択します。
3. 「接続」ページで、「Kerberos プリンシパル名の使用 (プロンプトなし) (Use Kerberos principal name, no prompting)」を選択する。これで、System i Access for Windows 接続は、Kerberos プリンシパル名とパスワードを認証に使用できます。
4. 接続設定値に対する変更を有効にするために現在実行中のすべてのアプリケーションをクローズして再始動する必要があることを示すメッセージが表示される。「OK」をクリックします。次に、System i ナビゲーターを終了して、再始動します。
5. システム B についてこの手順を繰り返す。

ネットワーク認証サービスおよび EIM 構成の検証

これで、シングル・サインオン構成の個々の部分は検証済みとなり、すべてのセットアップが完了したことを確認したので、エンタープライズ識別マッピング (EIM) およびネットワーク認証サービスが正しく構成されたこと、およびシングル・サインオンが期待どおりに機能することを検証する必要があります。

シングル・サインオン環境が正しく働くことを検証するには、John Day に以下の手順を行わせます。

1. System i ナビゲーター で、「システム A」を展開して、システム A への接続を開きます。
2. F5 を押して画面を最新表示する。
3. 右側のペインの「名前」欄で、システム A を探し、John Day の i5/OS ユーザー・プロファイル JOHND が「サインオン・ユーザー (Signed On User)」欄に対応する項目として表示されていることを確認します。EIM ID、John Day に定義されたアソシエーションのため、System i ナビゲーター は正常に EIM を使用して、jday Kerberos プリンシパルを JOHND システム A ユーザー・プロファイルにマップしました。システム A の System i ナビゲーター セッションは、これで JOHND として接続されています。
4. これらのステップを、Sharon Jones について、また SYSUSERA ユーザー・プロファイルまたは SYSUSERB ユーザー・プロファイルに対してマップされるユーザー ID の、少なくとも 1 つについて繰り返す。

構成終了後の考慮事項

定義する追加の EIM ユーザーの数は、セキュリティの義務と責任の分離に関する、セキュリティ・ポリシーの重点が何であるかにより決まります。

これで、このシナリオは完了したので、EIM が使用できるように定義された EIM ユーザーは、LDAP 管理者の DN のみです。システム A と B のシステム・ユーザーに指定した LDAP 管理者 DN には、ディレクトリー・サーバー上のすべてのデータに対する高水準の権限があります。したがって、EIM データに対するより適切で限定されたアクセス制御を持つ追加のユーザーとして、1 つ以上の DN の作成を考慮することができます。通常、少なくとも以下のような 2 つのタイプの DN を作成することができます。

• EIM 管理者アクセス制御を持つ 1 人のユーザー

この EIM 管理者 DN により、EIM ドメインの管理を担当する管理者用の権限として適切なレベルが提供されます。この EIM 管理者 DN は、System i ナビゲーター によって EIM ドメインのすべての局面を管理する際、ドメイン・コントローラーに接続する場合に使用できます。

• 以下のアクセス制御をすべて持つ、少なくとも 1 人のユーザー:

- ID 管理者
- レジストリー管理者
- EIM マッピング操作

このユーザーにより、オペレーティング・システムに代わって EIM 操作を実行するシステム・ユーザーに必要とされる、適切なレベルのアクセス制御が提供されます。

注: システム・ユーザー用のこの新しい DN を LDAP 管理者 DN の代わりに使用するには、各システムの EIM 構成プロパティを変更する必要があります。このシナリオの場合、システム A および B の両方の EIM 構成プロパティを変更する必要があります。システム・ユーザー DN を変更する方法を学習するには、EIM 構成プロパティの管理に関する情報を参照してください。

関連概念

EIM のアクセス制御

IBM Directory Server for i5/OS (LDAP)

関連タスク


EIM 構成プロパティの管理

ネットワーク認証サービスの計画

ネットワーク認証サービスまたは Kerberos ソリューションをご使用のネットワーク上でインプリメントする前に、必要な計画タスクを完了することが必須です。

ネットワーク認証サービスおよび Kerberos インプリメンテーションを計画するには、ご使用のネットワーク上のシステムおよびユーザーに関する適切な情報を集める必要があります。ご使用のネットワーク上でネットワーク認証サービスを構成する援助となる計画ワークシートがいくつか提供されています。

注: 数多くのいろいろな Kerberos 認証ソリューションがあり、これらをエンタープライズで使用することができます。ここでの情報は、i5/OS インプリメンテーションを計画すること、および Microsoft Active Directory または i5/OS PASE において構成された Kerberos サーバーでネットワーク認証サービスを使用する時の考慮事項に焦点をあてます。

Microsoft Active Directory 内での Kerberos サーバーのセットアップに関する情報については、Windows 2000 サーバー  を参照してください。

次の IBM システムでは、Kerberos 認証がサポートされます。プラットフォーム固有の Kerberos インプリメンテーションに関する情報については、以下の情報源を参照してください。

- **System p™**

- *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*

注: この資料は、AIX 5L Expansion Pack and Bonus Pack CD  に収録されています。

- **System z™**

- z/OS Security Server Network Authentication Service Administration 

以下のタスクを、ネットワーク認証サービスを計画する援助として使用してください。

Kerberos サーバーの計画

ご使用のオペレーティング・システムに基づいて Kerberos サーバーを計画します。

Kerberos サーバーまたは鍵配布センター (KDC) は、プリンシパルおよび関連するパスワードのデータベースを維持管理します。これは、認証サーバーとチケット許可サーバーから構成されます。プリンシパルが Kerberos ネットワークにログインすると、認証サーバーはプリンシパルを検証し、プリンシパルにチケット許可チケットを送信します。Kerberos 認証を計画する時は、どのシステムを Kerberos サーバーとして構成するか、決める必要があります。


注: ネットワーク認証サービスの情報は、i5/OS PASE または Windows 2000 サーバー上で稼働する Kerberos サーバーに焦点をあてます。ほとんどのシナリオおよび例は、明示的にそうでないことが言及されている場合を除き、Windows 2000 サーバーが Kerberos サーバーとして構成されていることを前提にしています。これら他のオペレーティング・システムまたはサード・パーティー・アプリケーションのいずれかを Kerberos 認証に使用している場合は、対応する資料を参照してください。

以下のリストでは、3 つの重要なオペレーティング・システム上での Kerberos サーバー・サポートに関する詳細を提供します。

Microsoft Windows 2000 および Windows Server 2003

Microsoft Windows 2000 オペレーティング・システムおよび Windows Server 2003 オペレーティ

ング・システムは、ともにデフォルト・セキュリティ・メカニズムとして Kerberos 認証をサポートします。管理者が Microsoft Active Directory を通じてユーザーおよびサービスを追加する時、管理者は実際にはこれらのユーザーおよびサービス用の Kerberos プリンシパルを作成しています。ご使用のネットワーク内に Windows 2000 サーバーまたは 2003 サーバーがある場合、これらのオペレーティング・システムに組み込まれた Kerberos サーバーがあることになります。

Microsoft Windows サーバーで Kerberos 認証が使用される方法に関する情報については、Windows 2000 サーバー  を参照してください。


AIX および i5/OS PASE

AIX および i5/OS PASE は、ともに kadmin コマンドを通じて Kerberos サーバーをサポートします。管理者は、PASE Kerberos サーバーを構成し管理するには、PASE 環境に入る (call QP2TERM と入力することにより) 必要があります。i5/OS PASE は、Kerberos サーバーなどの AIX アプリケーション用のランタイム環境を提供します。以下の資料は、AIX 内で Kerberos サーバーを構成し管理する援助となります。

- *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*

注: この資料は、AIX 5L Expansion Pack and Bonus Pack CD  に収録されています。

z/OS Security Server Network Authentication Service for z/OS は、Kerberos バージョン 5 に基づく IBM z/OS プログラムです。z/OS 用のネットワーク認証サービスでは、ミドルウェア・プログラムの購入あるいは使用を必要とせず、Kerberos セキュリティ・サービスを提供します。これらのサービスは、ネイティブの Kerberos サーバーをサポートします。z/OS Kerberos サーバーの構成と

管理についての詳細は、z/OS Security Server Network Authentication Service Administration  を参照してください。

オペレーティング・システムが Kerberos サーバーを提供していても、ユーザーは、Kerberos サーバー用のサーバー・ポートを判別し、Kerberos サーバーへのアクセスを保護し、クライアントと Kerberos サーバーとの間で必ず時刻を同期させることが必要です。

サーバー・ポートの判別

ネットワーク認証サービスは、Kerberos サーバー用のデフォルトとしてポート 88 を使用します。ただし、他のポートを Kerberos サーバーの構成ファイル内で指定することもできます。Kerberos サーバー上にある Kerberos 構成ファイル内のポート番号を検証する必要があります。

Kerberos サーバーへのアクセスの保護

Kerberos サーバーは、プリンシパルとパスワードのデータベースが危険にさらされないようにするための援助となるよう、セキュアで専用のシステム上に置かなければなりません。ユーザーは、Kerberos サーバーに対するアクセスを限定される必要があります。Kerberos サーバーが存在するシステムが、Web サーバーあるいは FTP サーバーといった何らかの他の目的にも使用される場合、だれかがこれらのアプリケーションの中のセキュリティの欠陥を利用して、Kerberos サーバー上に保管されているデータベースへのアクセスを入手するおそれがあります。Microsoft Active Directory 内の Kerberos サーバーの場合、オプションで、プリンシパルが Kerberos サーバー上に保管されている自分のパスワードを管理し変更することができるようにパスワード・サーバーを構成することができます。Kerberos サーバーを i5/OS PASE 内で構成した場合で、System i プラットフォームを Kerberos 認証専用に行えない時は、必ず管理者だけが Kerberos 構成へアクセスできるようにする必要があります。

システム時刻を同期する

Kerberos 認証では、システム時刻が同期していることが必要です。Kerberos は、指定された Kerberos サーバーの最大クロック・スキューの範囲外の時刻を持つシステムまたはクライアントからの認証要求をリジェクトします。各チケットには、そのチケットがプリンシパルに送信された時刻が組み込まれているため、ハッカーが後で同じチケットを再送してネットワークに対して認証されるように試みることはできません。System i プラットフォームも、ネットワーク認証サービスの構成時に設定された最大クロック・スキューの範囲外のクロックを Kerberos サーバーが持っている場合は、その Kerberos サーバーからのチケットをリジェクトします。最大クロック・スキューのデフォルト値は 300 秒 (5 分) です。ネットワーク認証サービスの構成時に、最大クロック・スキューはこの値に設定されます。ただし、必要があればこの値を変更することができます。この値は、300 秒以下にされるようお勧めします。システム時刻を処理する方法の詳細については、114 ページの『システム時刻の同期化』を参照してください。

表 19. Kerberos サーバーの計画ワークシートの例： この計画ワークシートは、管理者がネットワークの Kerberos サーバーを計画する方法の例を提供します。

質問	回答
Kerberos サーバーをどのオペレーティング・システム上に構成するよう計画するか？ <ul style="list-style-type: none">• Windows 2000 サーバー• Windows サーバー 2003• AIX サーバー• i5/OS PASE (V5R3 以降)• z/OS	i5/OS ポータブル・アプリケーション・ソリューション環境 (PASE)
Kerberos サーバーの完全修飾ドメイン名は？	systema.myco.com
Kerberos サーバーに接続されている PC およびシステムの間で、時刻が同期しているか？最大のクロック・スキューは？	はい、300 秒
Network Authentication Enablement (5722-NAE または 5761-NAE) 製品をインストールする必要があるか？	V5R4 システムで i5/OS PASE に Kerberos サーバーを構成する計画がある場合は、必要です。V5R4 以降では、ネットワーク認証サーバーは別個の製品 <i>Network Authentication Enablement (5722-NAE または 5761-NAE)</i> として出荷されます。 i5/OS V5R3 を使用する場合は、i5/OS PASE で Kerberos サーバーを構成するために、代わりに <i>Cryptographic Access Provider (5722-AC3)</i> をインストールする必要があります。

レルムの計画

お客様自身のエンタープライズを理解すると、ご使用の環境でレルムを計画するのに役立ちます。

Kerberos プロトコルにおいて、レルムは、Kerberos サーバーまたは鍵配布センター (KDC) と呼ばれる単一の認証サーバーを使用するマシンおよびサービスの集まりで構成されます。レルムは、個別に管理されません。レルム内のアプリケーションおよびサービスは、一般に何らかの共通の用途または目的を共有しています。以下の一般的な質問は、エンタープライズにおいてレルムを計画する援助となります。

現在の環境の大きさは？

ご使用の環境の大きさによって、必要となるレルムの数が決まります。大規模なエンタープライズ

においては、組織境界に基づいたいくつかのレルム、あるいはエンタープライズの中で特定のシステムが使用される方法を考慮することができます。例えば、人事部門、顧客サービス部門、または出荷部門用のそれぞれのレルムなど、自社のいろいろな組織を表すレルムを確立します。同様な機能を実行するシステムまたはサービスの集まり用に、レルムを作成することもできます。一般に、小規模エンタープライズでは、1 つか 2 つのレルムしか必要としないこともあります。

環境が拡大していく速度の予想は？

エンタープライズの急速な拡大が計画される場合は、エンタープライズ内で比較的小さい組織単位を表すレルムをいくつかセットアップすることをお勧めします。エンタープライズが成長する速度は比較的緩やかであると予想する場合は、現在の組織に基づいて 1 つか 2 つのレルムのみをセットアップしてください。

これらのレルムを管理するために管理者は何人必要か？

エンタープライズが大規模でも小規模でも、必要とされるレルムのセットアップと管理は必ず知識を持った人が行う必要があります。

レルムの命名

Kerberos プロトコルの規則にしたがい、レルム名は一般には MYCO.COM などのようにドメイン名の大文字版にします。複数のレルムを持つネットワークでは、大文字の記述名とドメイン名を組み込んだレルム名を作成することができます。例えば、それぞれが、組織の中の特定の部門を表す、一方は HR.MYCO.COM、他方は SHIPPING.MYCO.COM という名前の 2 つのレルムがあるものとします。

必ず大文字を使用しなければならないわけではありませんが、Kerberos のインプリメンテーションの一部においては、この規則は強制されます。例えば、Microsoft Active Directory においては、レルム名は厳格に大文字です。Microsoft Active Directory に構成された Kerberos レルムに参加するために System i プラットフォーム上にネットワーク認証サービスを構成している場合は、レルム名は大文字で入力しなければなりません。

i5/OS PASE に構成される Kerberos サーバーの場合、大文字かまたは小文字のいずれでもレルム名を作成できます。ただし、Microsoft Active Directory で構成されている Kerberos サーバーと、i5/OS PASE に構成されている Kerberos サーバーとの間に信頼関係を作成する計画がある場合は、レルム名は大文字であることが必要です。

表 20. Kerberos レルム用の計画ワークシートの例

質問	回答
必要なレルムの数は？	2 つ。
レルムをどのように編成する計画か？	現在、自社には、受注部門のユーザーを認証する Windows 2000 サーバーがあります。出荷部門は、i5/OS PASE 内の Kerberos サーバーを使用します。これらの部門はいずれも、自分のレルムを持つことになります。
レルムに使用する命名規則は？	部門を表す大文字の短縮名に、Windows 2000 ドメイン名の太文字版を続けたものを使用します。例えば、ORDEPT.MYCO.COM が受注部門で、SHIPDEPT.MYCO.COM は出荷部門を表します。

プリンシパル名の計画

プリンシパルとは、Kerberos ネットワークにおけるユーザーまたはサービスの名前です。プリンシパルは、ユーザー名またはサービス名、およびそのユーザーまたはサービスが属するレルムの名前からなります。

Mary Jones がレルム MYCO.COM を使用する場合は、そのプリンシパル名は jonesm@MYCO.COM になります。Mary Jones は、このプリンシパル名とこれに関連するパスワードを使用して、中央の Kerberos サーバーによって認証されます。すべてのプリンシパルは Kerberos サーバーに追加され、Kerberos サーバーはレルム内のすべてのユーザーおよびサービスのデータベースを維持管理します。

プリンシパルの命名用のシステムを開発する場合は、現行ユーザーと将来のユーザーが共存できるように一貫性のある命名規則を使用して、プリンシパル名を割り当てる必要があります。以下の提案を使用してプリンシパルの命名規則を確立します。

- 姓、およびファーストネームのイニシャルを使用する
- ファーストネームのイニシャルと完全な姓を使用する
- ファーストネームにラストネームのイニシャルを加える
- database1 などのように、アプリケーション名またはサービス名に識別番号を付けて使用する

i5/OS プリンシパル名

System i プラットフォーム上でネットワーク認証サービスを構成する時は、プリンシパル名をオプションで作成することができます。これらのプリンシパルはそれぞれ、i5/OS オペレーティング・システム上にあるサービスを表します。ネットワーク認証サービスの構成中に、作成することを選択したサービス・プリンシパルのそれぞれに対して、システム上にキー・テーブル・エントリーが作成されます。このキー・テーブル・エントリーには、サービス・プリンシパル名および構成中に指定した暗号化されたパスワードが保管されます。ネットワーク認証サービスが構成された後に、すべての i5/OS サービス・プリンシパルが Kerberos サーバーに追加される必要があることに注意することが重要です。i5/OS プリンシパルを Kerberos サーバーに追加する方法は、エンタープライズで構成した Kerberos サーバーに基づいて変わります。i5/OS プリンシパル名を Windows 2000 ドメインまたは i5/OS PASE 内の Kerberos サーバーに追加する方法の説明については、110 ページの『Kerberos サーバーへの i5/OS プリンシパルの追加』を参照してください。以下の情報は、ネットワーク認証サービスの構成中に構成される i5/OS サービス・プリンシパルのそれぞれについて、説明しています。

i5/OS Kerberos 認証

i5/OS Kerberos 認証用の keytab エントリーを作成するよう選択すると、サービス・プリンシパルは次のいずれかの形式で keytab ファイル内に生成されます。すなわち、krbsvr400/System i fully qualified domain name@REALM NAME または krbsvr400/System i host name@REALM NAME です。例えば、i5/OS Kerberos 認証の有効なサービス・プリンシパルは、krbsvr400/systema.myco.com@MYCO.COM または krbsvr400/systema@MYCO.COM となります。i5/OS は、System i プラットフォームがホスト名を解決するためにどのように構成されたかに応じて、DNs サーバー上または System i プラットフォーム上のいずれかで検出したホスト名に基づき、プリンシパルを生成します。

サービス・プリンシパルは、いくつかの i5/OS インターフェース、例えば、QFileSrv.400、Telnet、分散リレーショナル・データベース体系 (DRDA[®])、i5/OS NetServer、および IBM System i Access for Windows (System i ナビゲーターなども含む) で使用されます。これらの各アプリケーションは、Kerberos 認証を使用可能にするために、追加の構成を必要とする場合があります。

LDAP i5/OS サービス・プリンシパル名に加えて、ネットワーク認証サービスの構成中に、オプションにより IBM Directory Server for i5/OS (LDAP) への追加のサービス・プリンシパルを構成することができます。LDAP プリンシパル名は、ldap/System i fully qualified domain name@REALM NAME です。例えば、有効な LDAP プリンシパル名は、ldap/systema.myco.com@MYCO.COM です。このプリンシパル名は、その System i プラットフォーム上にあるディレクトリー・サーバーを識別します。

注: 過去のリリースにおいては、「ネットワーク認証サービス」ウィザードは LDAP サービス用に大文字の `keytab` エントリーを作成しました。ネットワーク認証サービスを再構成する時、またはそのウィザードに EIM (エンタープライズ識別マッピング) インターフェースを通じてアクセスする時、それ以前に LDAP プリンシパルが構成済みだった場合は、このプリンシパル名を小文字版に変更するよう指示するプロンプトが出されます。

ディレクトリー・サーバーで Kerberos 認証を使用する計画がある場合は、ネットワーク認証サービスを構成する必要があるばかりでなく、ディレクトリー・サーバーのプロパティーを、Kerberos 認証を受け入れるように変更する必要があります。Kerberos 認証が使用される時は、ディレクトリー・サーバーはサーバー識別名 (DN) を Kerberos プリンシパル名と関連付けます。ユーザーは、以下のいずれかの方法を使用してサーバー DN を関連付けさせるよう選択できます。

- サーバーは Kerberos プリンシパル名に基づいて DN を作成することができる。このオプションを選択する場合、`principal@realm` の形式の Kerberos ID は、`ibm-kn=principal@realm` の形式の DN を生成します。`ibm-kn=` は、`ibm-kerberosName=` と同等です。
- サーバーは、ディレクトリーで、Kerberos プリンシパルおよびレルム用のエントリーを含む識別名 (DN) を検索することができる。このオプションを選択する場合、サーバーは、ディレクトリーで、この Kerberos ID を指定するエントリーを検索します。

ディレクトリー・サーバー用の Kerberos 認証の構成に関する詳細については、『IBM Tivoli® Directory Server for i5/OS (LDAP)』を参照してください。

HTTP Server

i5/OS サービス・プリンシパル名に加えて、オプションで、Apache で機能する HTTP Server (HTTP) 用の追加のサービス・プリンシパルを、ネットワーク認証サービスの構成中に作成することができます。HTTP プリンシパル名は、`HTTP/System i fully qualified domain name@REALM NAME` です。このプリンシパル名は、Web ユーザーの認証に Kerberos を使用する System i プラットフォーム上の ワークシート サーバー・インスタンスを識別します。HTTP Server インスタンスで Kerberos 認証を使用するときは、同時に HTTP Server に関する追加の構成手順も完了する必要があります。

HTTP Server での Kerberos 認証の使用に関する情報を検索するには、HTTP Server for i5/OS:

documentation  ホーム・ページを参照してください。

i5/OS NetServer

i5/OS NetServer の場合、System i プラットフォーム上の `keytab` ファイルに自動的に追加されるいくつかの NetServer プリンシパルを作成することを選択することもできます。これらの NetServer プリンシパルはそれぞれ、NetServer に接続するために使用する可能性のあるすべてのクライアントを表します。以下の表は、NetServer プリンシパル名、およびそれらが表すクライアントを示しています。

表 21. i5/OS NetServer プリンシパル名

クライアント接続	i5/OS NetServer プリンシパル名
Windows XP と Windows Vista	cifs/System i の完全修飾ドメイン名 cifs/System i ホスト名 cifs/QSystem i ホスト名 cifs/qSystem i ホスト名 cifs/IP アドレス

表 21. i5/OS NetServer プリンシパル名 (続き)

クライアント接続	i5/OS NetServer プリンシパル名
Windows 2000	HOST/System i の完全修飾ドメイン名 HOST/System i ホスト名 HOST/QSystem i ホスト名 HOST/qSystem i ホスト名 HOST/IP アドレス

このアプリケーションで Kerberos 認証を使用する詳細については、『i5/OS NetServer』を参照してください。

ネットワーク・ファイルシステムのサーバー

ネットワーク認証サービスの構成中に i5/OS サービス・プリンシパル名に加えて、ネットワーク・ファイル・システム (NFS) サーバーをオプションにより構成することができます。NFS プリンシパル名は `nfs/System i fully qualified domain name@REALM NAME` です。例えば、NFS サーバーの有効なプリンシパル名は、`nfs/systema.myco.com@MYCO.COM` です。

計画ワークシートの例

表 22. プリンシパル計画ワークシートの例

質問	回答
ネットワーク内のユーザーを表す、Kerberos プリンシパルに使用する予定の命名規則は ?	小文字で、ファーストネームのイニシャルの後に姓の最初の 5 文字を付ける。例: mjjones
ネットワーク上のアプリケーションの命名規則は ?	記述名の後に番号を付ける。例: database123
Kerberos 認証を使用する計画のある i5/OS サービスは ?	i5/OS Kerberos 認証は、以下のサービスで使用されます。 1. System i Access for Windows、System i ナビゲーター、i5/OS NetServer、および Telnet 2. Apache で機能する HTTP Server 3. LDAP 4. ネットワーク・ファイルシステム (NFS) のサーバー
これらの i5/OS サービスのそれぞれに対する i5/OS プリンシパル名は ?	1. <code>krbsvr400/systema.myco.com@MYCO.COM</code> 2. <code>HTTP/systema.myco.com@MYCO.COM</code> 3. <code>ldap/systema.myco.com@MYCO.COM</code> 4. <code>nfs/systema.myco.com/MYCO.COM</code>

ホスト名解決の考慮事項

Kerberos を使用できるアプリケーションで Kerberos-enabled 認証およびホスト名解決を確実に正しく機能させるためには、ご使用の PC および System i プラットフォームが、サービス・アプリケーションが置かれているシステムに対して同じホスト名を解決することを検証します。

Kerberos 環境では、クライアントもサーバーも、特定のアプリケーションまたはサービスが置かれているシステムのホスト名を判別するために、なんらかのホスト名解決の方法を使用します。System i プラットフォームと PC が DNS サーバーを使用する場合は、サーバーと PC が同じ DNS サーバーを使用してホスト名解決を実行することが重要です。複数の DNS サーバーを使用する場合は、両方の DNS サーバーに同じホスト名があることが重要です。System i プラットフォームまたは PC がホスト名をローカルに (ロ

ーカル・ホスト・テーブルまたはファイルから) 解決する場合は、DNS サーバー上に記録されている対応するホスト名とは異なるホスト名を解決する可能性があります。このことが、ネットワーク認証サービスを失敗させる場合があります。

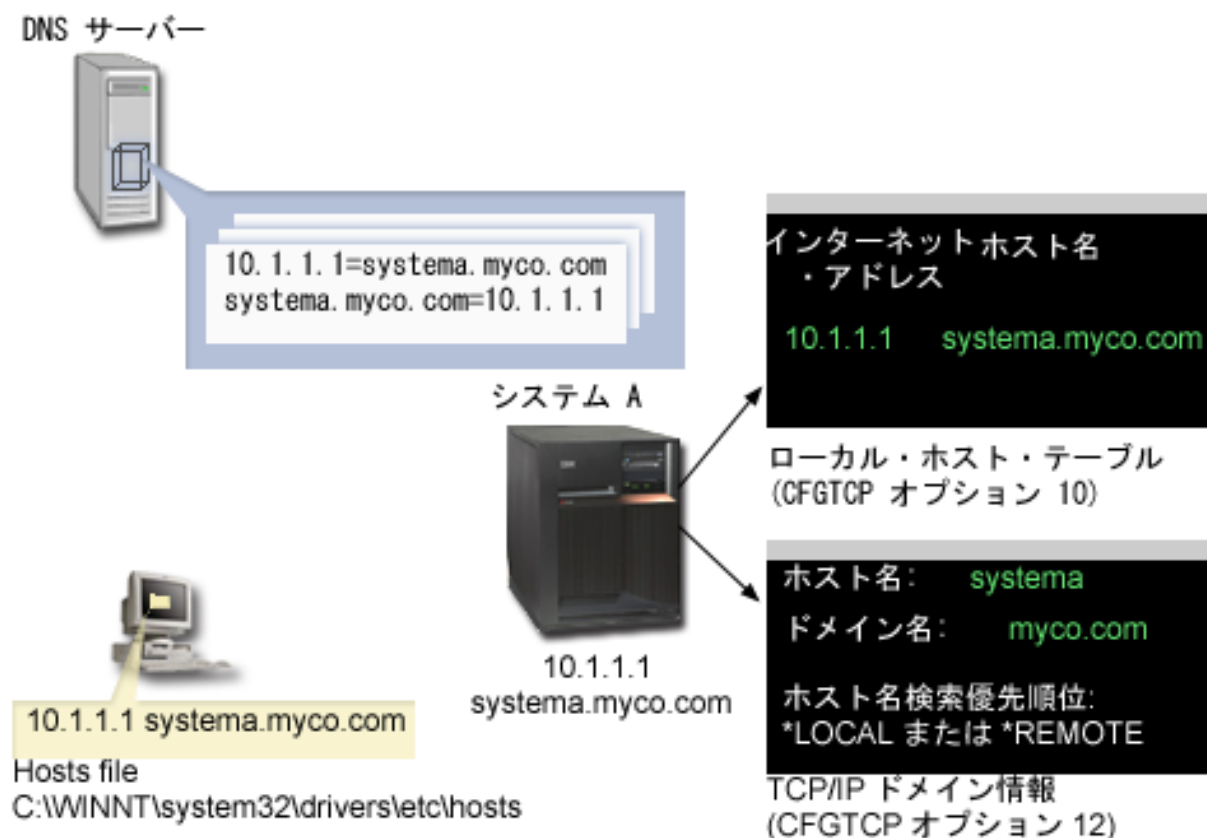
Kerberos を使用できるアプリケーションで Kerberos-enabled 認証およびホスト名解決を確実に正しく機能させるためには、ご使用の PC および System i プラットフォームが、サービス・アプリケーションが置かれているシステムに対して同じホスト名を解決することを検証する必要があります。以下の例では、このシステムをシステム A と呼びます。

以下の説明で、PC と System i プラットフォームが、システム A に対して同じ名前を解決するかどうかの判別方法を示します。指示にしたがって例のワークシートを参照してください。

ご使用の Kerberos レルムでこれらのステップを実行する時は、ブランクのワークシートにご自身の情報を記入することができます。

この図は、以下の例でホスト名情報を含むシステム・ファイルおよびレコードを示しています。

注: IP アドレス 10.1.1.1 は、共通 IP アドレスを表します。このアドレスは、例としてのみ使用されます。



詳細

DNS サーバー

- システム A 用の IP アドレスおよびホスト名である、IP アドレス 10.1.1.1 とホスト名 systema.myco.com が関連していることを示すデータ・リソース・レコードが入っている。

- PC、システム A、あるいはその両方によってホスト解決に使用される可能性がある。

注: この例では 1 つの DNS サーバーを示しています。ただし、ご使用のネットワークでは複数の DNS サーバーを使用する場合があります。例えば、PC は一方の DNS サーバーを使用してホスト名を解決し、System i プラットフォームは別の DNS サーバーを使用する可能性があります。ご使用のレールムでホスト解決に使用される DNS サーバーの数を判別し、ご使用になる状況にこの情報を適合させる必要があります。

PC

- Windows 2000 オペレーティング・システムを稼働させている。
- ネットワーク認証サービスを管理するために使用される PC、およびユーザーが自分の日常タスク用に特殊権限なしに使用する PC の両方を表す。
- IP アドレス 10.1.1.1 とホスト名 systema.myco.com が関連していることを示す hosts ファイルを含む。

注: これらのフォルダーで、以下のホスト・ファイルを検出することができます。

- Windows 2000 オペレーティング・システム: C:\WINNT\system32\drivers\etc\hosts
- Windows XP および Windows Vista オペレーティング・システム: C:\WINDOWS\system32\drivers\etc\hosts

システム A

- i5/OS V5R3 を実行する。
- ネットワーク認証サービス (Kerberos 認証) を使用してアクセスする必要のあるサービス・アプリケーションを含む。
- 「TCP (CFGTCP) の構成 (CFGTCP)」メニューの中で、オプション 10 とオプション 12 が、システム A に関する以下の情報を示す。
 - オプション 10 (TCP/IP ホスト・テーブル・エントリーの処理)
 - インターネット・アドレス: 10.1.1.1
 - ホスト名: systema.myco.com
 - オプション 12 (TCP/IP ドメイン情報の変更)
 - ホスト名: systema
 - ドメイン名: myco.com
 - ホスト名検索優先順位: *LOCAL または *REMOTE

注: ホスト名検索優先順位パラメーターは、ネットワーク管理者が、システム上でホスト解決を実行するために TCP/IP を構成する方法に応じて、*LOCAL または *REMOTE のいずれかを指示します。

表 23. 例: PC ホスト名解決ワークシート

PC 上でシステム A のホスト名を判別する。		
ステップ	ソース	ホスト名
1.a.1	PC hosts ファイル	systema.myco.com
1.b.1	DNS サーバー	systema.myco.com

表 24. 例: i5/OS ホスト名解決ワークシート

システム A 上でシステム A のホスト名を判別する。		
ステップ	ソース	ホスト名
2.a.2	システム A CFGTCP メニュー、オプション 12	ホスト名: systema ドメイン名: myco.com
注: ホスト名検索優先順位 の値: *LOCAL または *REMOTE		
2.b.2	システム A CFGTCP メニュー、オプション 10	systema.myco.com
2.c.1	DNS サーバー	systema.myco.com

表 25. 例: ホスト名突き合わせワークシート

これらの 3 つのホスト名は、正確に一致する必要がある。	
ステップ	ホスト名
ステップ 1	systema.myco.com
ステップ 2.a.2	systema myco.com
2d	systema.myco.com

ユーザーは、以下の 3 つのワークシートを使用して、ご使用の PC および System i プラットフォームが、サービス・アプリケーションが置かれているシステムについて同じホスト名を解決できることを検証できます。

表 26. PC ホスト名解決ワークシート

PC 上で System i プラットフォームのホスト名を判別する。		
ステップ	ソース	ホスト名
1.a.1	PC hosts ファイル	
1.b.1	DNS サーバー	

表 27. i5/OS ホスト名解決ワークシート

System i プラットフォーム上で System i プラットフォームのホスト名を判別する。		
ステップ	ソース	ホスト名
2.a.2	System i CFGTCP メニュー、オプション 12	ホスト名: ドメイン名:
注: ホスト名検索優先順位 の値: *LOCAL または *REMOTE		
2.b.2	System i CFGTCP メニュー、オプション 10	
2.c.1	DNS サーバー	

表 28. ホスト名突き合わせワークシート

これらの 3 つのホスト名は、正確に一致する必要がある。	
ステップ	ホスト名
ステップ 1	
ステップ 2.a.2	
2d	

ホスト名の解決

ご使用の PC および System i プラットフォームが同じホスト名を解決することを確認します。

ホスト名を解決するための参照として、直前のワークシート例を使用します。PC と System i プラットフォームがシステム A に対して同じホスト名を解決していることを検証するには、以下の手順を行います。

1. PC から、システム A の完全修飾 TCP/IP ホスト名を判別する。

注: ご使用のネットワークの管理方法によっては、これをシングル・サインオン環境を結合している他の PC から行いたい場合があります。

- a. PC の Windows Explorer で、以下のロケーションのいずれかから hosts ファイルをオープンする。
 - Windows 2000 オペレーティング・システム: C:\WINNT\system32\drivers\etc\hosts
 - Windows XP オペレーティング・システム: C:\WINDOWS\system32\drivers\etc\hosts

注: hosts ファイルが PC 上に存在しない場合、ご使用の PC はホスト名解決に DNS サーバーを使用している可能性があります。この場合はステップ 1b にスキップしてください。

ワークシート上に、大文字か小文字か注意しながらシステム A 用の最初のホスト名項目を書き込む。例えば、systema.myco.com。

注: hosts ファイルにシステム A 用の項目がない場合、ご使用の PC はホスト名解決に DNS サーバーを使用している可能性があります。その場合はステップ 1b を参照してください。

- b. NSLOOKUP を使用して DNS サーバーを照会する。

注: PC の hosts ファイル内にホスト名項目が見つかった場合は、このステップをスキップしてステップ 2 に進みます。(オペレーティング・システムが PC のホスト名を解決する時は、hosts ファイルが DNS サーバーより高い優先順位になります。)

- 1) コマンド・プロンプトで NSLOOKUP と入力し、Enter キーを押す。NSLOOKUP プロンプトで、10.1.1.1 と入力してシステム A の DNS サーバーを照会します。DNS サーバーが戻すホスト名を、大文字か小文字か注意しながら書き留めます。例えば、systema.myco.com です。
- 2) NSLOOKUP プロンプトで、systema.myco.com と入力する。これは、直前のステップで DNS サーバーが戻したホスト名でなければなりません。DNS サーバーが、予想通りの IP アドレスを戻すことを検証します。例えば、10.1.1.1 です。

注: NSLOOKUP が予想通りの結果を戻さない場合は、DNS 構成に不備があります。例えば、ステップ 1.b.1 で入力したアドレスとは異なる IP アドレスを NSLOOKUP が戻した場合、次の手順を続けられるためには、まず DNS 管理者に連絡してこの問題を解決する必要があります。

2. システム A から、自身の完全修飾 TCP/IP ホスト名を判別する。

a. TCP/IP ドメイン情報

- 1) コマンド・プロンプトで、CFGTCP と入力しオプション 12 (TCP/IP ドメインの変更) を選択する。
- 2) ホスト名 パラメーターおよび ドメイン名 パラメーターを、大文字か小文字か注意しながら書き留める。例えば、次のとおりです。
 - ホスト名: systema
 - ドメイン名: myco.com
- 3) ホスト名検索優先順位 パラメーターの値を書き留める。
 - *LOCAL - オペレーティング・システムは、最初にローカル・ホスト・テーブル (PC 上の hosts ファイル) を検索する。ホスト・テーブル内に一致する項目がなく、DNS サーバーが構成済みである場合は、オペレーティング・システムは DNS サーバーを検索します。
 - *REMOTE - オペレーティング・システムは最初に DNS サーバーを検索する。DNS サーバーに一致する項目がない場合は、オペレーティング・システムはローカル・ホスト・テーブルを検索します。

b. TCP/IP ホスト・テーブル

- 1) コマンド・プロンプトで、CFGTCP と入力しオプション 10 (TCP/IP ホスト・テーブル・エントリーの処理) を選択する。
- 2) システム A (IP アドレス 10.1.1.1) に対応するホスト名 欄の値を、大文字か小文字か注意しながら書き留める。例えば、systema.myco.com。

注: ホスト・テーブルにシステム A の項目がない場合、次のステップに進みます。

c. DNS サーバー

- 1) コマンド・プロンプトで NSLOOKUP と入力し、Enter キーを押す。NSLOOKUP プロンプトで、10.1.1.1 と入力してシステム A の DNS サーバーを照会します。DNS サーバーが戻すホスト名を、大文字か小文字か注意しながら書き留めます。例えば、systema.myco.com です。
- 2) NSLOOKUP プロンプトで、systema.myco.com と入力する。これは、直前のステップで DNS サーバーが戻したホスト名でなければなりません。DNS サーバーが、予想通りの IP アドレスを戻すことを検証します。例えば、10.1.1.1 です。

注: NSLOOKUP が予想通りの結果を戻さない場合は、DNS 構成に不備があります。例えば、ステップ 2.c.1 で入力したアドレスとは異なる IP アドレスを NSLOOKUP が戻した場合、次の手順を続けられるためには、まず DNS 管理者に連絡してこの問題を解決する必要があります。

d. TCP/IP 構成を基にして、どのホスト名の値をシステム A に対して保持すべきか判別する。

- ホスト名検索優先順位 パラメーターが *LOCAL であれば、ローカル・ホスト・テーブルからメモした項目を保持する (ステップ 2.b.2)。
- ホスト名検索優先順位 パラメーターが *REMOTE であれば、DNS サーバーからメモした項目を保持する (ステップ 2.c.1)。
- これらのソースのいずれか 1 つにのみシステム A 用の項目がある場合は、その項目を保持する。

3. これらのステップの結果を以下のようにして比較する。

a. ステップ 1: PC がシステム A に対して使用する名前。

注: PC の hosts ファイルでシステム A 用の項目が見つかった場合は、その項目を使用します。見つからない場合は、DNS サーバーからの項目を使用します。

- b. ステップ 2.a.2: システム A 中の TCP/IP 構成において iSeries が自身を呼ぶ名前。
- c. ステップ 2d: ホスト名解決に基づいてシステム A が自身を呼ぶ名前。

これらの 3 つの項目のすべてが、大文字か小文字かを含めて正確に一致する必要があります。結果が正確に一致しない場合は、keytab エントリーが見つからないことを示すエラー・メッセージを受け取りません。

ネットワーク認証サービス計画ワークシート

ネットワーク認証サービスを正しく構成するには、要件について理解し、必要な計画の手順を完了する必要があります。

このトピックでは、必要なすべての手順を完了するための前提条件ワークシートおよび計画ワークシートについて説明します。以下のワークシートを使用して、Kerberos インプリメンテーションおよびネットワーク認証サービスの構成を計画する援助とします。

前提条件ワークシート

この計画ワークシートを使用して、必要な前提条件を必ずすべて完了するようにしてください。任意の構成タスクを実行できるためには、まず、すべての前提条件項目に「はい」と答えることができる必要があります。

表 29. 前提条件ワークシート


質問	回答
ご使用の i5/OS は、V5R3、またはそれ以降 (5722-SS1)、あるいは V6R1 (5761-SS1) であるか ?	
i5/OS V5R3 を使用している場合、システムに Cryptographic Access Provider (5722-AC3) がインストールされているか ? i5/OS V5R4 以降を使用している場合、システムに Network Authentication Enablement (5722-NAE または 5761-NAE) がインストールされているか ?	
管理者の PC とご使用のシステムに System i Access for Windows (5722-XE1 または 5761-XE1) はインストール済みですか?	
管理者の PC に System i ナビゲーター のセキュリティー・サブコンポーネントはインストール済みですか?	
管理者の PC に System i ナビゲーター のネットワーク・サブコンポーネントはインストール済みですか?	
最新の IBM System i Access for Windows サービス・パックをインストール済みですか? 最新の Service Pack については、System i Access  を参照してください。	
*SECADM、*ALLOBJ、および *IOSYSCFG の特殊権限を持っているか ?	
以下のいずれかを、Kerberos サーバーとしての役割を果たすセキュア・システムにインストールしてあるか ? インストールされていれば、どれか ? 1. Windows 2000 サーバー 2. Windows サーバー 2003 3. AIX サーバー 4. i5/OS PASE (V5R3 以降) 5. z/OS	

表 29. 前提条件ワークシート (続き)

質問	回答
Windows 2000 サーバーおよび Windows サーバー 2003 の場合、Windows サポート・ツール (ktpass ツールを提供する) が、鍵配布センターとして使用されるシステムにインストールされているか ?	
Kerberos サーバーが Windows 2000 サーバーまたは 2003 サーバーにある場合、ネットワーク内のすべての PC が Windows 2000 ドメイン内に構成されているか ?	
最新のプログラム一時修正 (PTF) を適用してあるか ?	
System i システム時刻と Kerberos サーバーのシステム時刻との差が 5 分以内か ? そうでない場合は、114 ページの『システム時刻の同期化』を参照。	

表 30. Kerberos サーバー計画ワークシート

質問	回答
Kerberos サーバーをどのオペレーティング・システム上に構成するよう計画するか ? <ul style="list-style-type: none"> • Windows 2000 サーバー • Windows サーバー 2003 • AIX サーバー • i5/OS PASE (V5R3 以降) • z/OS 	
Kerberos サーバーの完全修飾ドメイン名は ?	
Kerberos サーバーに接続されている PC およびシステムの間で、時刻が同期しているか ? 最大のクロック・スキューは ?	

表 31. Kerberos レルム計画ワークシート

質問	回答
必要なレルムの数は ?	
レルムをどのように編成する計画か ?	
レルムに使用する命名規則は ?	

表 32. プリンシパル計画ワークシート

質問	回答
ネットワーク内のユーザーを表す、Kerberos プリンシパルに使用する予定の命名規則は ?	
ネットワーク上のアプリケーションの命名規則は ?	
Kerberos 認証を使用する計画のある i5/OS サービスは ?	
これらの i5/OS サービスのそれぞれに対する i5/OS プリンシパル名は ?	

表 33. ホスト名解決の考慮事項ワークシート

質問	回答
PC および System i プラットフォームは、ホスト名の解決に同じ DNS サーバーを使用しているか ?	

表 33. ホスト名解決の考慮事項ワークシート (続き)

質問	回答
ホスト名の解決に System i プラットフォーム上のローカル・ホスト・テーブルを使用しているか？	
ご使用の PC および System i プラットフォームは System i プラットフォームに対して同じホスト名を解決するか？ 援助として 93 ページの『ホスト名解決の考慮事項』を参照してください。	

以下の計画ワークシートは、i5/OS PASE における Kerberos サーバー、およびネットワーク認証サービスの構成を開始する前に必要な情報のタイプを示しています。i5/OS PASE において Kerberos サーバーの構成を進める前に、前提条件ワークシート上のすべての回答を答える必要があります。

表 34. i5/OS PASE 計画ワークシート

質問	回答
PASE はインストールしてあるか？	
デフォルト・レルムの名前は？	
Kerberos デフォルト・レルムの Kerberos サーバーは？ Kerberos サーバーが listen するポートは？	
ネットワーク内のユーザーを表す、ご使用になるプリンシパルの命名規則は？	
ネットワーク内のユーザーのプリンシパル名は？	

ネットワーク認証サービスの構成を開始する前に、以下の計画ワークシートを使用して必要な情報を集めます。ネットワーク認証サービスの構成を進める前に、前提条件ワークシートのすべての回答を答える必要があります。

表 35. ネットワーク認証サービス計画ワークシート

質問	回答
ご使用のシステムが属する Kerberos のデフォルト・レルムの名前は何か？ 注: Windows 2000 ドメインは、Kerberos レルムと同様です。Microsoft Active Directory は、Kerberos 認証をデフォルトのセキュリティー・メカニズムとして使用します。	
Microsoft Active Directory を使用しているか？	
Kerberos デフォルト・レルムの Kerberos サーバーは？ Kerberos サーバーが listen するポートは？	
このデフォルト・レルムにパスワード・サーバーを構成したいか？ 「はい」であれば、以下の質問に回答してください。	
この Kerberos サーバーのパスワード・サーバーの名前は？ パスワード・サーバーが listen するポートは？	
どのサービス用に keytab エントリーを作成したいか？	
<ul style="list-style-type: none"> • i5/OS Kerberos 認証 • LDAP • IBM HTTP Server • i5/OS NetServer • ネットワーク・ファイルシステムのサーバー 	

表 35. ネットワーク認証サービス計画ワークシート (続き)



質問	回答
i5/OS Kerberos 認証用のサービス・プリンシパルを作成する予定がある場合、そのパスワードは ?	
LDAP 用のサービス・プリンシパルを作成する予定がある場合、そのパスワードは ?	
HTTP Server 用のサービス・プリンシパルを作成する予定がある場合、そのパスワードは ?	
i5/OS NetServer 用のサービス・プリンシパルを作成する予定がある場合、そのパスワードは ? 注: 「ネットワーク認証サービス」ウィザードで、いくつかのプリンシパルが i5/OS NetServer 用に作成されます。これをウィザードで表示された通りにここに書き留めてください。これらのプリンシパルを Kerberos サーバーに追加する際に必要になります。	
ネットワーク・ファイル・システム・サーバー用のサービス・プリンシパルを作成する予定がある場合、そのパスワードは ?	
Microsoft Active Directory へのサービス・プリンシパルの追加を自動化するバッチ・ファイルを作成したいか ?	
パスワードを、バッチ・ファイルの i5/OS サービス・プリンシパルに組み込みますか?	

ネットワーク認証サービスの構成

ネットワーク認証サービスによって、System i 製品が、既存の Kerberos ネットワークに参加できるようになります。ネットワーク認証サービスは Kerberos サーバーがネットワーク内のセキュア・システム上に構成されていることを前提としています。

Kerberos サーバーの構成

i5/OS ポータブル・アプリケーション・ソリューション環境 (i5/OS PASE) 内で Kerberos サーバーを構成することができます。この i5/OS サポートに加えて、System i プラットフォームは、Microsoft Windows 2000、Windows 2003、AIX サーバー、および z/OS と相互運用されます。これらのプラットフォーム上で Kerberos サーバーを構成する方法を学習するには、以下の情報を使用します。

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

注: この資料は、AIX 5L Expansion Pack and Bonus Pack CD  に収録されています。

i5/OS PASE で Kerberos サーバーを構成する

1. 103 ページの『i5/OS PASE で Kerberos サーバーを構成する』
2. 104 ページの『Kerberos サーバー上での暗号化値の変更』
3. 104 ページの『Kerberos サーバーの停止と再始動』
4. 104 ページの『ホスト、ユーザー、およびサービスのプリンシパルの作成』
5. 105 ページの『Windows 2000、Windows XP、および Windows Vista ワークステーションの構成』
6. 106 ページの『2 次 Kerberos サーバーの構成』

System i プラットフォームでネットワーク認証サービスを構成する

1. 108 ページの『ネットワーク認証サービスの構成』
2. 110 ページの『Kerberos サーバーへの i5/OS プリンシパルの追加』
3. 112 ページの『ホーム・ディレクトリーの作成』
4. 112 ページの『ネットワーク認証サービス構成のテスト』

i5/OS PASE で Kerberos サーバーを構成する

AIX アプリケーション用の統合されたランタイム環境を提供するために、ご使用の System i プラットフォームから Kerberos サーバーを構成し、管理することができます。

i5/OS は、i5/OS ポータブル・アプリケーション・ソリューション環境 (PASE) で Kerberos サーバーをサポートします。i5/OS PASE は、AIX アプリケーション用の統合されたランタイム環境を提供します。System i プラットフォームから Kerberos サーバーを構成して管理することができます。i5/OS PASE で Kerberos サーバーを構成するには、以下の手順を完了します。

1. 文字ベース・インターフェースにおいて、コマンド・プロンプトで `call QP2TERM` と入力する。このコマンドは、ユーザーが i5/OS PASE アプリケーションを処理できる対話式シェル環境をオープンします。
2. コマンド行で `export PATH=$PATH:/usr/krb5/sbin` と入力する。このコマンドは、実行可能ファイルを実行するために必要な Kerberos スクリプトを指します。
3. コマンド行で `config.krb5 -S -d systema.myco.com -r MYCO.COM` と入力する。ここで、`-d` は、ご使用のネットワークの DNS であり、`-r` は、レルム名です。(この例では、`myco.com` は、DNS 名であり、`MYCO.COM` は、レルム名です。) このコマンドは、Kerberos サーバーのドメイン名とレルムを使用して `krb5.config` ファイルを更新し、統合ファイル・システムの中に Kerberos データベースを作成し、i5/OS PASE 内で Kerberos サーバーを構成します。データベース・マスター・パスワードおよび Kerberos サーバーの管理に使用される `admin/admin` プリンシパル用のパスワードを求めるプロンプトが出されます。

注: V5R3 および V5R4 では、Kerberos プリンシパルの保管は既存のデータベースのみについてサポートされます。LDAP ディレクトリー・プラグインは、現在はサポートされていません。

4. オプション: Kerberos サーバーおよび管理サーバーが、初期プログラム・ロード (IPL) 時に自動的に開始されるようにしたい場合は、2 つの追加ステップを行う必要があります。ジョブ記述を作成し、自動開始ジョブ項目を追加します。Kerberos サーバーおよび管理サーバーが IPL 時に自動的に開始されるように i5/OS を構成するには、以下の手順を行います。

- a. ジョブ記述を作成する

i5/OS コマンド行で、以下のコマンドを入力します。ここで、`xxxxxx` は `*ALLOBJ` ユーザー権限を持つ i5/OS ユーザー・プロファイルです。

```
CRTJOB JOB(QGPL/KRB5PASE) JOBQ(QSYS/QSYSNOMAX) TEXT('Start KDC and admin server in PASE') USER(xxxxxx) RQSDTA('QSYS/CALL PGM(QSYS/QP2SHELL) PARM('/usr/krb5/sbin/start.krb5')') SYNTAX(*NOCHK) INLLIBL(*SYSVAL) ENDSEV( 30)
```

- b. 自動開始ジョブ項目を追加するコマンド行で次のコマンドを入力します。

```
ADDAJE SBS(D(QSYS/QSYSWRK) JOB(KRB5PASE) JOBQ(QGPL/KRB5PASE).
```

注: IPL 時にサーバーを開始する代わりに、以下の手順を行うことにより IPL 後に手動でサーバーを開始することができます。

- a. 文字ベース・インターフェースで `call QP2TERM` と入力して i5/OS PASE 対話式シェル環境をオープンする。
- b. コマンド行で `/usr/krb5/sbin/start.krb5` と入力してサーバーを開始する。

次に行うことは？

Windows 2000 Active Directory を通じて構成されていない Kerberos サーバー (i5/OS PASE 内の Kerberos サーバーなど) とともに Windows 2000、Windows XP、または Windows Vista ワークステーションを使用している場合、Kerberos 認証が確実に正しく作動するために、Kerberos サーバーとワークステーションの両方でいくつかの追加の構成手順を行う必要があります。

Kerberos サーバー上での暗号化値の変更

Windows ワークステーションとともに作動するためには、Kerberos サーバー・デフォルト暗号化設定値は、クライアントが i5/OS PASE Kerberos サーバーに認証されるように変更される必要があります。

デフォルト暗号化設定値を変更するには、`/etc/krb5` ディレクトリーにある `kdc.conf` ファイルを、次の手順を行って編集する必要があります。

1. 文字ベース・インターフェースで `edtf '/var/krb5/krb5kdc/kdc.conf'` と入力して `kdc.conf` ファイルにアクセスする。
2. `kdc.conf` ファイルの以下の行を

```
supported_encetypes = des3-cbc-sha1:normal  
arcfour-hmac:normal aes256-cts:normal  
des-cbc-md5:normal des-cbc-crc:normal
```

次のように変更する。

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

Kerberos サーバーの停止と再始動

変更したばかりの暗号化値を更新するには、i5/OS PASE において Kerberos サーバーを停止してから再始動する必要があります。

以下の手順を完了してください。

1. 文字ベース・インターフェースにおいて、コマンド行で `call QP2TERM` と入力する。このコマンドは、ユーザーが i5/OS PASE アプリケーションを処理できるようにする対話式シェル環境をオープンします。
2. コマンド行で `export PATH=$PATH:/usr/krb5/sbin` と入力する。このコマンドは、実行可能ファイルを実行するために必要な Kerberos スクリプトを指します。
3. コマンド行で、`stop.krb5` と入力します。このコマンドは、Kerberos サーバーを停止します。
4. コマンド行で、`start.krb5` と入力します。このコマンドは、Kerberos サーバーを開始します。

ホスト、ユーザー、およびサービスのプリンシパルの作成

以下に示すプロシージャーは、Windows 2000、Windows XP、および Windows Vista のワークステーション用としてホスト・プリンシパルを作成、および Kerberos サーバー上にユーザーおよびサービス用としてプリンシパルを作成するためのものです。

Windows 2000、Windows XP、または Windows Vista ワークステーションと i5/OS PASE 内の Kerberos サーバーとの間に相互運用性を提供するには、Kerberos レベルに対してワークステーション用のホスト・プリンシパルを追加する必要があります。ご使用のネットワーク内のサービスに対してユーザーを認証する

- | 必要がある場合、それらのユーザーをプリンシパルとして Kerberos サーバーに追加する必要があります。
- | これらのユーザー・プリンシパルは Kerberos サーバー上に保管され、ネットワーク上のユーザーの検証を
- | 行うために使用されます。 Kerberos チケットを受信する i5/OS ごとに、それらを Kerberos サーバーに対
- | してプリンシパルとして追加する必要があります。以下のタスクを完了してください。

注: ユーザー名、ホスト名、およびパスワードは、例としてのみ使用されます。

1. 文字ベース・インターフェースにおいて、コマンド行で `call QP2TERM` と入力する。このコマンドは、ユーザーが i5/OS PASE アプリケーションを処理できる対話式シェル環境をオープンします。
2. コマンド行で `export PATH=$PATH:/usr/krb5/sbin` と入力する。このコマンドは、実行可能ファイルを実行するために必要な Kerberos スクリプトを指します。
3. コマンド行で `kadmin -p admin/admin` と入力し、Enter キーを押す。
4. 管理者のパスワードを使ってサインインする。
5. `kadmin` プロンプトで、`addprinc -pw secret1 host/pc1.myco.com` と入力する。このコマンドは、ネットワーク内に PC 用のホスト・プリンシパルを作成します。このステップを、ネットワーク内のすべての PC について繰り返します。
6. `addprinc -pw secret jonesm` と入力する。このコマンドは、ユーザー Mary Jones 用のプリンシパルを作成します。このステップを、すべてのユーザーについて繰り返します。
7. `kadmin` プロンプトで、`addprinc -pw systema123 krbsvr400/systema.myco.com` と入力する。このコマンドは、Kerberos サーバー用のサービス・プリンシパルを作成します。
8. `quit` と入力して `kadmin` インターフェースを終了し、F3 (終了) を押して PASE 環境を終了する。

Windows 2000、Windows XP、および Windows Vista ワークステーションの構成

Kerberos レalmと Kerberos サーバーを設定して、クライアント・ワークステーションを構成します。

i5/OS PASE 内で、Kerberos サーバーに Windows 2000 ワークステーション用の ホスト・プリンシパルを作成した後、クライアント・ワークステーションを構成する必要があります。Kerberos レalmおよび Kerberos サーバーをワークステーション上で設定することにより、このクライアントをワークグループの一部にする必要があります。このワークステーションに関連づけられるパスワードも、設定する必要があります。ワークステーションを構成するには、以下の手順を完了してください。

注: ユーザー名、ホスト名、およびパスワードは、例としてのみ使用されます。

1. Windows 2000 ワークステーションのコマンド・プロンプトから、以下のように入力する。

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

例えば、MyCo, Inc の管理者の場合、次のように入力します。

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

2. Windows 2000 ワークステーションのコマンド・プロンプトで以下のように入力することにより、ローカル・マシン・アカウント・パスワードを設定する。

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

このパスワードは、ホスト・プリンシパル `pc1.myco.com` を作成した時に使用したパスワードと一致する必要があります。例えば、MyCo, Inc のユーザーの場合、次のように入力します。

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

- Windows 2000 ワークステーションのコマンド・プロンプトで以下のように入力することにより、Kerberos ユーザーをローカル・ユーザーに対してマップする。

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

- 変更を有効にするために、コンピューターを再始動します。

オプションで、1 次 Kerberos サーバーがダウンしたり要求を処理しきれないほどビジーな場合にバックアップ・サーバーとして使用できる、2 次 Kerberos サーバーを構成することができます。詳細な指示については、『2 次 Kerberos サーバーの構成』を参照してください。

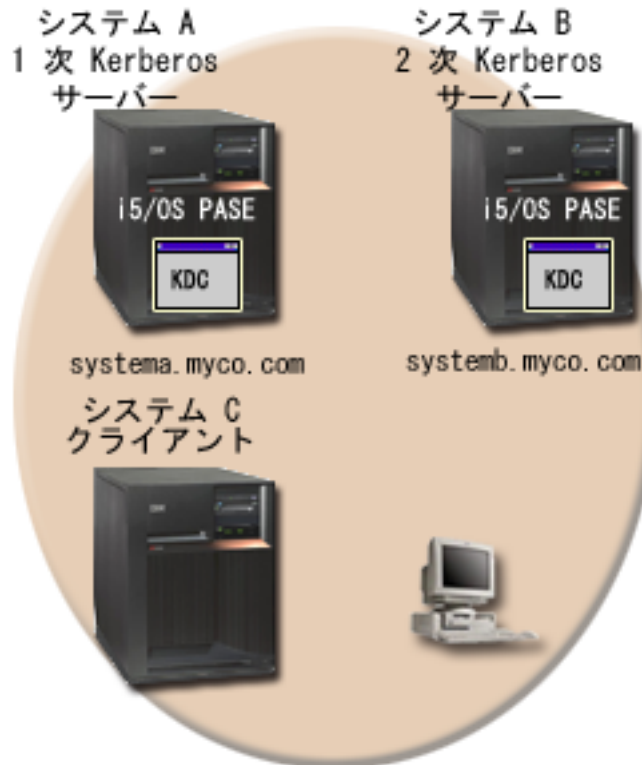
2 次 Kerberos サーバーの構成

1 次 Kerberos サーバーを i5/OS PASE で構成した後、オプションで、1 次 Kerberos サーバーがダウンしたり要求を処理しきれないほどビジーな場合にバックアップ・サーバーとして使用できる、2 次 Kerberos サーバーを構成することができます。

例えば、現在システム A を Kerberos サーバーとして使用しているものとします。ここで、システム B が 2 次 (バックアップ) Kerberos サーバーになるよう構成したいものとします。

注: Kerberos サーバーは、鍵配布センター (KDC) とも呼ばれます。

次の図は、以下の手順で説明されている System i 製品を示したものです。



詳細

- 図は、2 次 Kerberos サーバーの構成の手順を完了した後の、System i 製品の様子を示す。

- システム A は、i5/OS PASE に構成された 1 次 Kerberos サーバーとしての役割を果たす。
- システム B は、i5/OS PASE に構成された 2 次 Kerberos サーバーとしての役割を果たす。
- システム C は、システム B を Kerberos サーバーとして使用できるクライアントとしての役割を果たす。

システム B が i5/OS PASE において 2 次 Kerberos サーバーになるように構成するには、以下の手順を行います。

1. システム B をクライアントとして構成する。

- a. システム B の文字ベース・インターフェースで call QP2TERM と入力する。このコマンドは、ユーザーが i5/OS PASE アプリケーションを処理できる対話式シェル環境をオープンします。
- b. コマンド行で次のコマンドを入力します。

```
export PATH=$PATH:/usr/krb5/sbin
```

このコマンドは、実行可能ファイルを実行するために必要な Kerberos スクリプトを指します。

- c. コマンド行で次のように入力する。

```
config.krb5 -E -d rchland.ibm.com -r MYCO.COM -s lp16b1b.rchland.ibm.com
```

- d. 管理者パスワード (例えば、secret) を入力する。

config.krb5 コマンドは、クライアント、1 次サーバー、および 2 次サーバーを構成します。-C フラグは、システム C 上のクライアントを構成します。-s フラグはシステム A 上の 1 次 Kerberos サーバーを構成します。-E フラグは、システム B 上の 2 次 Kerberos サーバーを構成します。

2. システム A 上の Kerberos サーバーに対して、システム A 用およびシステム B 用に、i5/OS プリンシパルを追加する。

- a. システム A の文字ベース・インターフェースで call QP2TERM と入力する。このコマンドは、ユーザーが i5/OS PASE アプリケーションを処理できる対話式シェル環境をオープンします。
- b. コマンド行で次のように入力する。

```
export PATH=$PATH:/usr/krb5/sbin
```

このコマンドは、実行可能ファイルを実行するために必要な Kerberos スクリプトを指します。

- c. コマンド行で kadmin -p admin/admin と入力する。
- d. 管理者のパスワードを使ってサインインする。例えば、secret。
- e. コマンド行で次のコマンドを入力します。

```
addprinc -randkey -clearpolicy host/systema.myco.com
```

- f. コマンド行で次のコマンドを入力します。

```
addprinc -randkey -clearpolicy host/systemb.myco.com
```

3. 1 次 Kerberos サーバーから 2 次 Kerberos サーバーに、マスター・データベースを伝搬する。

- a. システム A の文字ベース・インターフェースで call QP2TERM と入力する。このコマンドは、ユーザーが i5/OS PASE アプリケーションを処理できる対話式シェル環境をオープンします。
- b. コマンド行で次のコマンドを入力します。

```
export PATH=$PATH:/usr/krb5/sbin
```

このコマンドは、実行可能ファイルを実行するために必要な Kerberos スクリプトを指します。

c. コマンド行で次のように入力する。

```
/usr/krb5/sbin/config.krb5 -P -r MYCO.COM -d rchland.ibm.com -e rchsrc2.rchland.ibm.com
```

ヒント: 1 次 Kerberos システム上のメッセージ内のコマンドをカット・アンド・ペーストすることができます。

-P フラグは、1 次 Kerberos サーバーから 2 次 Kerberos サーバーに、マスター・データベースを伝搬します。**-r** フラグは、レルム名を指定します。**-d** フラグは、DNS ドメインの名前を指定します。**-e** フラグは、2 次 Kerberos サーバーのホスト名を指定します。

4. 2 次 Kerberos サーバーで、マスター・データベースが正常に伝搬されたことを確認する。
 - a. 2 次 Kerberos サーバーで、「Have you successfully run the above command?」というプロンプトが表示されたら、Y と応答する。
 - b. データベース・マスター・パスワード (例えば、pasepwd) を入力する。このコマンドはマスター・キーを取り出します。

ネットワーク認証サービスの構成

以下に、システム上にネットワーク認証サービスを構成するための前提条件と手順を示します。

ネットワーク認証サービスを構成する前に、以下のタスクを実行する必要があります。

- すべての必要な計画ワークシートを完成する。
- PC および System i プラットフォームがホスト名を解決するときに、該当の System i 製品についても同じホスト名を解決することを検証する。このタスクについては、93 ページの『ホスト名解決の考慮事項』を参照してください。
- ネットワーク内のセキュア・システム上に Kerberos サーバーを構成する。i5/OS PASE 内に Kerberos サーバーを構成済みの場合、System i プラットフォーム上でネットワーク認証を構成する前に、必要なすべてのサーバーおよびクライアント・ワークステーションの構成が完了したことを確認してください。i5/OS PASE 内で Kerberos サーバーを構成する詳細については、103 ページの『i5/OS PASE で Kerberos サーバーを構成する』を参照してください。

Microsoft Windows 2000、Windows サーバー 2003、および z/OS 上でも、Kerberos サーバーを構成することができます。Kerberos サーバーとして使用されるシステムに対応した Kerberos 構成の資料を参照してください。

ネットワーク認証サービスを System i プラットフォーム上に構成する前に、Kerberos サーバーを構成します。

ネットワーク認証サービスを構成するには、以下の手順を完了してください。

1. System i ナビゲーターで、「システム」 → 「セキュリティ」を展開する。
2. 「ネットワーク認証サービス」を右クリックし、「構成」を選択して構成ウィザードを開始する。

注: ネットワーク認証サービスを構成した後では、このオプションは「再構成」になります。

3. ウィザードが作成するオブジェクトに関する情報について、「ようこそ」ページを検討する。「次へ」をクリックします。
4. 「レルム情報の指定 (Specify realm information)」ページで、「デフォルト・レルム」フィールドにデフォルト・レルムの名前を入力する。Microsoft Active Directory を Kerberos 認証に使用している場合は、「**Microsoft Active Directory を Kerberos 認証に使用する (Microsoft Active Directory is used for Kerberos authentication)**」を選択する。「次へ」をクリックします。

5. 「KDC 情報の指定 (Specify KDC information)」 ページで、「**KDC**」フィールドにこのレルムの Kerberos サーバーの名前を入力し、「**ポート**」フィールドに 88 を入力します。「**次へ**」をクリックします。
6. 「パスワード情報の指定 (Specify password information)」 ページで、「**はい**」または「**いいえ**」を選択してパスワード・サーバーをセットアップする。パスワード・サーバーは、プリンシパルが Kerberos サーバー上のパスワードを変更できるようにします。「**はい**」を選択したら、「**パスワード・サーバー**」フィールドにパスワード・サーバー名を入力します。パスワード・サーバーはデフォルト・ポート 464 をもっています。「**次へ**」をクリックします。
7. 「keytab エントリーの選択」 ページで、「**i5/OS Kerberos 認証**」を選択する。さらに、これらのサービスに Kerberos 認証を使用させたい場合には、ディレクトリー・サーバー (LDAP)、i5/OS NetServer、HTTP Server、および Network File System (NFS) サーバー用の keytab エントリーを作成することもできます。

注: これらのサービスの中には、Kerberos 認証を使用するために追加の構成が必要になるものもあります。

「**次へ**」をクリックします。

8. 「i5/OS keytab エントリーの作成」 ページで、パスワードを入力して確認する。「**次へ**」をクリックします。

注: このパスワードは、Kerberos サーバーに i5/OS プリンシパルを追加するとき使用するパスワードと同じです。

9. 「バッチ・ファイルの作成」 ページで、このファイルを作成するために「**はい**」を選択する。

注: このページは、ステップ 4 (上記) で「**Microsoft Active Directory を Kerberos 認証に使用する (Microsoft Active Directory is used for Kerberos authentication)**」を選択した場合にのみ、表示されます。

10. 「バッチ・ファイル」フィールドで、ディレクトリー・パスを更新する。適切なディレクトリーを見つけるには、「**参照...**」をクリックして、フィールド内のパスを編集することができます。
11. 「パスワードを組み込む (Include password)」フィールドで、「**はい**」を選択する。この結果、i5/OS サービス・プリンシパルに関連するパスワードは、すべてバッチ・ファイルに組み込まれます。パスワードは平文で表示され、バッチ・ファイルに対する読み取りアクセスを持っていれば誰でも読み取れる、ということに注意することが重要です。

注: ウィザードにより生成されるサービス・プリンシパルを、Microsoft Active Directory に手動で追加することもできます。i5/OS サービス・プリンシパルを Microsoft Active Directory に手動で追加する方法を知りたい場合は、110 ページの『Kerberos サーバーへの i5/OS プリンシパルの追加』を参照してください。

12. 「要約」 ページで、ネットワーク認証サービスの構成の詳細を検討する。「**終了**」をクリックします。

これで、ネットワーク認証サービスが構成されました。

関連概念

114 ページの『ネットワーク認証サービスの管理』

ネットワーク認証サービスを構成した後、チケットを要求し、キー・テーブル・ファイルを処理し、ホスト名解決を管理することができます。信任状ファイルを処理することも構成ファイルのバックアップをとることもできます。

Kerberos サーバーへの i5/OS プリンシパルの追加

System i プラットフォーム上でネットワーク認証サービスを構成した後、Kerberos サーバーに対して i5/OS プリンシパルを追加する必要があります。

ネットワーク認証サービスは、システムおよび i5/OS アプリケーションに i5/OS プリンシパル名 **krbsvr400** を提供します。i5/OS を表すプリンシパルの名前は「krbsrv400/System i ホスト名@大文字のレルム名」です。ここで、System i ホスト名は、System i プラットフォームの、完全修飾ホスト名または短縮ホスト名のいずれかです。このプリンシパル名は、Kerberos クライアント・アプリケーションがサービス・チケットを要求して受け取ることができるように、Kerberos サーバーに追加される必要があります。例えばこの構成シナリオでは、MyCo の管理者は、会社の Kerberos サーバーに対してサービス・プリンシパル `krbsvr400/systema.myco.com@MYCO.COM` を追加しました。

1 Kerberos サーバーが構成されているオペレーティング・システムに応じて、i5/OS プリンシパルを追加する方法は異なります。本書は、i5/OS プリンシパルを i5/OS PASE 内の Kerberos サーバーまたは Windows 2000 ドメインに追加する説明を記載しています。IBM Directory Server for i5/OS (LDAP)、i5/OS NetServer、Network File System (NFS) サーバー、または HTTP Server のサービス・プリンシパルをオプションで作成した場合は、これらのサービス・プリンシパルも Kerberos サーバーに追加する必要があります。

1. i5/OS PASE Kerberos サーバーが i5/OS PASE にある場合は、QP2TERM コマンドを使用して i5/OS サービス・プリンシパルを追加することができます。QP2TERM コマンドは、i5/OS PASE アプリケーションを処理できるようにする対話式シェル環境をオープンします。i5/OS サービス・プリンシパルを i5/OS PASE 内の Kerberos サーバーに追加するには、以下の手順を完了します。
 - a. 文字ベース・インターフェースで `call QP2TERM` と入力する。
 - b. コマンド行で `export PATH=$PATH:/usr/krb5/sbin` と入力する。このコマンドは、実行可能ファイルを実行するために必要な Kerberos スクリプトを指します。
 - c. コマンド行で `kadmin -p admin/admin` と入力する。
 - d. ユーザーのユーザー名とパスワードでログオンする。
 - e. `kadmin` コマンド行で、`addprinc -pw secret krbsvr400/System i fully qualified host name@REALM` と入力する。ここで、`secret` は i5/OS サービス・プリンシパル用のパスワードです。例えば、`krbsvr400/systema.myco.com@MYCO.COM` は、有効な i5/OS サービス・プリンシパル名です。

2. Microsoft Active Directory

i5/OS サービス・プリンシパルを Kerberos サーバーに追加するには、2 つのオプションがあります。すなわち、「ネットワーク認証サービス」ウィザードにプリンシパルを追加させるか、あるいは手動で追加するかです。

「ネットワーク認証サービス」ウィザードを使用すれば、オプションで `NASConfig.bat` という名前のバッチ・ファイルを作成することができます。このバッチ・ファイルには、構成中にユーザーが選択したサービスのプリンシパル名がすべて含まれます。プリンシパルに関連したパスワードをこのバッチ・ファイルに追加することも選択できます。

注: パスワードを組み込むと、バッチ・ファイルに読み取りアクセスを持っているだれかがパスワードを表示する可能性があります。したがって、パスワードを組み込む場合は、バッチ・ファイルを使用した直後に、これを Kerberos サーバーと PC から削除することをお勧めします。パスワードをバッチ・ファイルに組み込まない場合、バッチ・ファイルが Windows サーバー上で実行される時に、パスワードを求めるプロンプトが出されます。

「ネットワーク認証サービス」ウィザードが生成するバッチ・ファイルの使用

- a. 管理者がネットワーク認証サービスを構成するのに使用した Windows 2000 ワークステーションで FTP を使用して、コマンド・プロンプトをオープンし、`ftp server` と入力する。ここで、`server` は Kerberos サーバーのホスト名です。これにより FTP セッションが PC 上で開始されます。管理者のユーザー名とパスワードを求めるプロンプトが出されます。
- b. FTP プロンプトで `lcd "C:¥Documents and Settings¥All Users¥Documents¥IBM¥Client Access"` と入力する。 **Enter** キーを押します。

注: これは、バッチ・ファイルを入れることのできるディレクトリーの例です。

メッセージ「現在のローカル・ディレクトリーは C:¥Documents and Settings¥All Users¥Documents¥IBM¥Client Access (Local directory now C:¥Documents and Settings¥All Users¥Documents¥IBM¥Client Access)」を受け取るはずです。

- c. FTP プロンプトで `binary` と入力する。これは、転送されるファイルがバイナリーであることを示します。
- d. FTP プロンプトで `cd \mydirectory` と入力する。ここで、`mydirectory` は、バッチ・ファイルを配置したい Windows サーバー上のディレクトリーです。
- e. FTP プロンプトで `put NASConfig.bat` と入力する。メッセージ「226 転送が完了しました (226 Transfer complete)」を受け取るはずです。
- f. Windows 2000 サーバー上で、バッチ・ファイルを転送したディレクトリーをオープンする。
- g. `NASConfig.bat` ファイルを見つけ、それをダブルクリックして、実行します。
- h. ファイルを実行したあとで次の手順を行って、i5/OS プリンシパル名が Microsoft のアクティブ・ディレクトリーに追加されたことを検査します。
 - 1) Windows 2000 サーバー上で、「スタート」 → 「プログラム」 → 「管理ツール」 → 「Active Directory ユーザーとコンピュータ」 → 「ユーザー」と展開する。
 - 2) 該当する Windows 2000 ドメインを選択して、System i プラットフォームにユーザー・アカウントがあることを検査します。

注: この Windows ドメインは、ネットワーク認証サービス構成に指定したデフォルト・レルム名と同じでなければなりません。

- 3) 表示されるユーザーのリストで、追加したばかりのサービス・プリンシパルに対応する名前を探す。
- 4) Active Directory ユーザーに関するプロパティーにアクセスする。「アカウント」タブから、「アカウントの委任は承認されています (Account is trusted for delegation)」を選択します。

注: このオプションのステップは、ご使用のシステムがユーザーの信任状を他のシステムに委任または転送することができるようにします。その結果、i5/OS サービス・プリンシパルは、ユーザーに代わって複数のシステムのサービスにアクセスすることができます。これは、多重階層ネットワークにおいて役立ちます。

サービス・プリンシパルを手動で Microsoft Active Directory に追加する `ktpass` コマンドを使用することにより、i5/OS プリンシパルを Microsoft Active Directory に手動で追加することができます。このコマンドは、Windows サポート・ツールで出荷され、Kerberos サーバーとして使用されるシステムには必ずインストールする必要があります。

- a. Windows 2000 サーバー上で、「スタート」 → 「プログラム」 → 「管理ツール」 → 「Active Directory ユーザーとコンピュータ」と展開する。
- b. i5/OS ユーザー・アカウントを追加する Windows 2000 ドメインを選択し、「アクション (Action)」 → 「新規 (New)」 → 「ユーザー」と展開する。

注: この Windows 2000 ドメインは、ネットワーク認証サービス構成に指定したデフォルト・レルム名と同じでなければなりません。

- c. 「名前」フィールドに、この Windows 2000 ドメインに対して System i プラットフォームを識別する名前を入力する。これにより System i プラットフォーム用の新しいユーザー・アカウントが追加されます。例えば、有効なユーザー・アカウント名として `krbsvr400systema` または `httpssystema` を入力できます。
- d. ステップ 3 で作成した Active Directory ユーザーのプロパティにアクセスする。「アカウント」タブから、「アカウントの委任は承認されています (Account is trusted for delegation)」を選択します。これにより、i5/OS サービス・プリンシパルは、サインイン・ユーザーに代わって他のサービスにアクセスすることができるようになります。
- e. 作成したばかりのユーザー・アカウントを、`ktpass` コマンドを使用することにより i5/OS サービス・プリンシパルにマップする必要があります。`ktpass` ツールは、Windows 2000 サーバーのインストール CD の「サービス・ツール (Service Tools)」フォルダーに入っています。ユーザー・アカウントをマップするには、以下のタスクを完了します。
 - 1) コマンド・プロンプトで次のように入力する。

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

注: コマンドの中で、`krbsvr400systema` はステップ 3 で作成したユーザー・アカウント名を表し、`secret` は、ネットワーク認証サービスの構成中に i5/OS プリンシパル用として入力したパスワードです。

関連概念

136 ページの『ネットワーク認証サービスのトラブルシューティング』

このトラブルシューティング情報には、Kerberos 認証をサポートする、ネットワーク認証サービス、エンタープライズ識別マッピング (EIM)、および IBM 提供のアプリケーションに共通する問題が含まれています。

ホーム・ディレクトリーの作成

Kerberos サーバーに対して i5/OS プリンシパルを追加した後、i5/OS アプリケーションに接続する各ユーザー用に `/home` ディレクトリーを作成する必要があります。

このディレクトリーには、ユーザーの Kerberos 信任状キャッシュの名前が含まれているファイルが入ります。各ユーザーは、このディレクトリーの所有者になるか、またはこのディレクトリー内にファイルを作成できる適切な権限を持つ必要があります。

ユーザーのホーム・ディレクトリーを作成するには、以下の手順を実行してください。

1. i5/OS コマンド行で `CRTDIR '/home/user profile'` と入力します。ここで、`user profile` は、ユーザーの i5/OS ユーザー・プロファイルです。

注: このユーザー・プロファイルをターゲット EIM アソシエーションとして使用することを計画している場合は、ユーザー・プロファイルが存在していなければならず、パスワードは `*NONE` に設定することができます。

ネットワーク認証サービス構成のテスト

i5/OS プリンシパル用のチケット許可チケットを要求することによって、ネットワーク認証サービス構成をテストします。

i5/OS アプリケーションに接続予定の各ユーザーのホーム・ディレクトリーを作成したあとで、i5/OS プリンシパルのチケット許可チケットを要求することによって、ユーザーは、ネットワーク認証サービスの構成をテストすることができます。チケットを要求する前に、次のような一般的なエラーが修正済みであることを確認する必要があります。

- ネットワーク認証サービスのすべての前提条件を満たしているか？
- チケット要求を出そうとしているユーザー用のホーム・ディレクトリーが、i5/OS オペレーティング・システム上に存在するか？詳細については、112 ページの『ホーム・ディレクトリーの作成』を参照してください。
- i5/OS プリンシパルの正しいパスワードがあるか？このパスワードは、ネットワーク認証の構成中に作成されたもので、計画ワークシートに明記されているはずです。
- i5/OS プリンシパルを Kerberos サーバーに追加したか？詳細については、110 ページの『Kerberos サーバーへの i5/OS プリンシパルの追加』を参照してください。

ネットワーク認証サービスをテストするには、以下の手順を完了してください。

1. コマンド行で QSH と入力して、Qshell インタープリターを開始する。
2. `keytab list` と入力して、`keytab` ファイルに登録されているプリンシパルのリストを表示する。次の結果が表示されるはずです。

```
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. `kinit -k krbsvr400/fully qualified host name@REALM NAME` と入力して、Kerberos サーバーからチケット許可チケットを要求する。例えば、`krbsvr400/systema.myco.com@MYCO.COM` は、システムの有効なプリンシパル名です。このコマンドは、ご使用のシステムが正しく構成されており、`keytab` ファイル内のパスワードが Kerberos サーバーに保管されているパスワードと一致することを検証します。正しく入力されれば、QSH コマンドがエラーなしに表示されます。
4. `klist` と入力し、デフォルト・プリンシパルが「`krbsvr400/完全修飾ホスト名@REALM NAME`」であることを検証する。このコマンドにより、Kerberos 信任状キャッシュの内容が表示され、i5/OS サービス・プリンシパルに有効な許可証が作成され、かつシステムの信任状キャッシュに入れられていることが検査されます。

```
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
$
```

次に行うこと:

エンタープライズ識別マッピングの構成

このタスクは、ネットワーク認証サービスをユーザー独自のアプリケーションで使用している場合には、オプションになります。ただし、シングル・サインオン環境を作成する場合には、このタスクは IBM 提供のアプリケーションを使用することをお勧めします。

ネットワーク認証サービスの管理

ネットワーク認証サービスを構成した後、チケットを要求し、キー・テーブル・ファイル进行处理し、ホスト名解決を管理することができます。信任状ファイル进行处理することも構成ファイルのバックアップをとることもできます。

System i ユーザーのタスク

System i プラットフォームは、Kerberos を使用できるネットワークでクライアントとしても作動できます。ユーザーは、システムにサインオンして、Qshell インタープリターを通じて Kerberos 関連タスクを実行できます。以下のタスクは、ユーザーの一般的なタスクを実行するために、いくつかの Qshell コマンドを使用します。

- 112 ページの『ホーム・ディレクトリーの作成』
- 118 ページの『チケット許可チケットの取得または更新』
- 125 ページの『Kerberos パスワードの変更』
- 123 ページの『keytab ファイルの管理』
- 127 ページの『有効期限が切れた信任状キャッシュ・ファイルの削除』
- 121 ページの『信任状キャッシュの表示』
- 130 ページの『LDAP ディレクトリー内の Kerberos サービス・エントリーの管理』

注: System i ナビゲーター で PC5250 エミュレーターを使用している場合、サインオンをバイパスできるようにリモート・サインオン・システム値を変更する必要があります。リモート・サインオン・システム値を変更するには、以下の手順を行います。

1. System i ナビゲーターで、「システム」 → 「構成およびサービス」 → 「システム値」 → 「サインオン」を展開する。
2. 「リモート」ページで、「サインオンのバイパスを許容する (Allow sign-on to be bypassed)」と「ソースとターゲットのユーザー ID は一致することが必要 (Source and target user IDs must match)」を選択し、「OK」をクリックする。

ネットワーク認証サービス管理タスク

以下に、System i ナビゲーター で管理者が実行できるタスクを示します。タスク・ベースの詳細な情報については、ネットワーク認証サービスに関する System i ナビゲーター のヘルプを参照してください。

関連タスク

108 ページの『ネットワーク認証サービスの構成』

以下に、システム上にネットワーク認証サービスを構成するための前提条件と手順を示します。

システム時刻の同期化

ネットワーク認証サービスは、システム時刻の差の最大数のデフォルトとして 5 分 (300 秒) を使用します。時刻が違っている場合は、ネットワーク認証サービスのプロパティ进行处理して変更できます。

システム時刻を同期する前に、QTIMZON システム値を使用してユーザーの時間帯に合ったシステム時刻を設定してください。Kerberos サーバーに設定されている時刻を変更してこれらシステム時刻を同期するか、あるいは QTIME システム値を使用して System i システム時刻を変更することができます。ただし、システム時刻をネットワーク内で同期させておくには、Simple Network Time Protocol (SNTP) を構成する必要があります。SNTP によって、複数のシステムが単一のタイム・サーバーに時刻を合わせられるようになります。

SNTP を構成するには、以下のステップを実行してください。

- SNTP を System i プラットフォーム上に構成するために、コマンド行で CHGNTPA と入力します。
- Windows システム上で SNTP を構成するために、**NET HELP TIME** を使用して SNTP サーバーの構成情報を表示します。

関連概念

Simple Network Time Protocol

レルムの追加

レルムを i5/OS 構成に追加する前に、新しいレルムの Kerberos サーバーを構成する必要があります。レルムを i5/OS ネットワーク認証サービス・タスクに追加するには、レルム名、Kerberos サーバーの名前、および Kerberos サーバーが listen するポートが必要です。

ネットワーク認証サービスにレルムを追加するには、以下の手順に従ってください。

1. System i ナビゲーターで、「システム」 → 「セキュリティー」 → 「ネットワーク認証サービス」と展開する。
2. 「レルム」を右クリックして、「レルムの追加」を選択する。
3. 「追加レルム (Realm to add)」フィールドに、追加したいレルムのホスト名を入力する。例えば、有効なレルム名は MYCO.COM のようになります。
4. 追加するレルムの Kerberos サーバーの名前を、「KDC」フィールドに入力する。例えば、有効なレルム名は kdc1.myco.com のようになります。
5. Kerberos サーバーが要求を listen するポート番号を入力する。有効なポート番号は 1 から 65535 です。Kerberos サーバーのデフォルト・ポートは 88 です。
6. 「OK」をクリックします。

レルムの削除

ネットワーク管理者として、ネットワーク認証サービス構成から不要のレルムまたは未使用のレルムを削除することができます。またシステムに組み込まれたアプリケーションに関するある種のアプリケーション問題からリカバリーするために、デフォルトのレルムを除去しなければならない場合もあります。

例えば、ネットワーク内に Kerberos サーバーをセットアップせずにネットワーク認証サービスを構成した場合、QFileSvr.400 および分散データ管理 (DDM) は Kerberos 認証を使用していると想定します。これらの製品に認証をセットアップする前に、ネットワーク認証サービスの構成時に指定したデフォルト・レルムを削除する必要があります。

ネットワーク認証サービスのレルムを削除するには、以下の手順を完了してください。

1. System i ナビゲーターで、「システム」 → 「セキュリティー」 → 「ネットワーク認証サービス」 → 「レルム」と展開する。
2. 削除したいレルムの名前を右クリックして、「削除」を選択する。
3. 「OK」をクリックして削除を確認する。

レルムへの Kerberos サーバーの追加

ネットワーク認証サービスを使用してレルムに Kerberos サーバーを追加できます。Kerberos サーバーをレルムに追加する前に、Kerberos サーバーの名前および listen するポートを調べておく必要があります。

鍵配布センターをレルムに追加するには、以下の手順を完了してください。

1. System i ナビゲーターで、「システム」 → 「セキュリティー」 → 「ネットワーク認証サービス」 → 「レルム」と展開する。
2. 右側の画面区画にあるレルムの名前を右クリックして、「プロパティ」を選択する。
3. 「一般」タブで、このレルムに追加したい Kerberos サーバーの名前を「KDC」フィールドに入力する。すべてのレルムに Kerberos サーバーが必要です。例えば、kdc2.myco.com は有効な入力です。
4. Kerberos サーバーが要求を listen するポート番号を入力する。有効なポート番号は 1 から 65535 です。Kerberos サーバーのデフォルト・ポートは 88 です。
5. 「追加」をクリックする。新しい Kerberos サーバーが「このレルムの鍵配布センター (KDC)」リストに表示されます。
6. 「OK」をクリックします。

パスワード・サーバーの追加

パスワード・サーバーを使用すれば、Kerberos プリンシパルは自分のパスワードを変更できます。

現在、i5/OS PASE はパスワード・サーバーのオプション構成をサポートしません。i5/OS PASE Kerberos サーバー上のプリンシパルのパスワードを変更するには、PASE 環境に入って (call QP2TERM)、kpasswd コマンドを出す必要があります。以下の指示に従うことによって、ユーザーは、ネットワーク認証サービス構成がデフォルト・レルム用の追加の、あるいは新規のパスワード・サーバーを指すように、ネットワーク認証サービス構成を更新することができます。パスワード・サーバーをレルムに追加するには、以下の手順を完了してください。

1. System i ナビゲーターで、「システム」 → 「セキュリティー」 → 「ネットワーク認証サービス」 → 「レルム」と展開する。
2. 右側の画面区画にあるレルムの名前を右クリックして、「プロパティ」を選択する。
3. 「パスワード・サーバー」タブで、パスワード・サーバーの名前を入力する。例えば、有効なパスワード・サーバーの名前は psvr.myco.com になります。
4. パスワード・サーバーに対応するポート番号を入力する。有効なポート番号は 1 から 65535 です。パスワード・サーバーのデフォルト・ポートは 464 です。
5. 「追加」をクリックする。新しいパスワード・サーバーがリストに追加されます。
6. 「OK」をクリックします。

関連資料

127 ページの『kpasswd』

Qshell コマンド kpasswd は Kerberos プリンシパルのパスワードを変更します。

レルム間の信頼関係の作成

レルム間の信頼関係を設定することによって、認証へのショートカットが作成されます。

この機能は、デフォルトにより Kerberos プロトコルがレルム階層で信頼を検索しているため、オプションとなっています。この機能は、レルムが別々のドメインにあり、このプロセスをより速く実行したい場合には有効です。レルムの信頼をセットアップするには、それぞれのレルムの各 Kerberos サーバーがキーを共有する必要があります。ネットワーク認証サービス内で信頼関係を作成する前に、各 Kerberos サーバーを、相互に信頼関係を結ぶようにセットアップしなければなりません。レルム間の信頼関係を作成するには、以下の手順を実行してください。

1. In System i ナビゲーターで、「システム」 → 「セキュリティー」 → 「ネットワーク認証サービス」 → 「レルム」と展開する。
2. 右側の画面区画にあるレルムの名前を右クリックして、「プロパティ」を選択する。

3. 「トラステッド・レルム」タブで、信頼を設定したいレルムの名前を入力する。例えば、信頼関係の有効な名前は ORDEPT.MYCO.COM および SHIPDEPT.MYCO.COM のようになります。
4. 「追加」をクリックする。これで、テーブルにトラスト・アソシエーションが追加されます。
5. 「OK」をクリックします。

ホスト解決の変更

ホスト名およびレルム名を解決するために、LDAP サーバー、ドメイン・ネーム・システム (DNS)、および静的マッピングを指定します。

ネットワーク認証サービスでは、ホスト名およびレルム名を解決するために、LDAP サーバー、DNS、および構成ファイルに追加される静的マッピングを指定することができます。また、これらの 3 つの方式すべてをホスト名の解決に選択できます。これらの 3 つの方式すべてを選択すると、ネットワーク認証サービスは最初にディレクトリー・サーバーを調べ、次に DNS 項目、そして最後に静的マッピングを調べてホスト名を解決します。

ホスト解決を変更するには、以下の手順を完了してください。

1. System i ナビゲーターで、「システム」→「セキュリティー」を展開する。
2. 「ネットワーク認証サービス」を右クリックして、「プロパティ」を選択する。
3. 「ホスト解決」ページで、「LDAP 探索の使用 (Use LDAP lookup)」、「DNS 探索の使用 (Use DNS lookup)」または「静的マッピングの使用 (Use static mappings)」を選択する。
4. ホスト解決タイプとして「LDAP 探索の使用」を選択した場合には、ディレクトリー・サーバーの名前および対応するポートを入力する。例えば、ディレクトリー・サーバーに有効な名前は `ldapsrv.myco.com` になります。有効なポート番号は 1 から 65535 です。ディレクトリー・サーバーのデフォルト・ポートは 389 です。LDAP サーバーを使用してホスト名の解決を処理することを指示したならば、レルムが適切に LDAP サーバーに定義されていることを確認する必要があります。詳細については、133 ページの『LDAP サーバーでのレルムの定義』を参照してください。
5. ホスト解決タイプとして「DNS 探索の使用」を選択した場合には、レルム名にマップするように DNS を構成する必要があります。ホスト名の解決に DNS サーバーを使用して処理することを指定した後、レルムが適切に DNS サーバーに定義されているのを確認する必要があります。詳細については、132 ページの『DNS データベースでのレルムの定義』を参照してください。
6. ホスト解決タイプとして「静的マッピングの使用」を選択した場合には、レルム名および対応する DNS 名を入力する。例えば、ホスト名は `mypc.mycompanylan.com`、レルム名は `MYCO.COM` のようになります。特定のレルムに総称ホスト名をマップすることもできます。例えば、`myco.lan.com` で終わるすべてのマシンが `MYCO.COM` の一部である場合、DNS 名として `myco.lan.com` と入力し、レルムとして `MYCO.COM` と入力します。これで、レルム名と DNS 名の間のアソシエーションが構成ファイルに作成されます。「追加」をクリックして、DNS 名とレルム名間の静的マッピングを構成ファイルに作成します。
7. 選択したホスト解決タイプに関連する情報を入力したら、「OK」をクリックする。

暗号化設定の追加

チケット許可チケット (TGT) およびチケット許可サービス (TGS) の暗号化タイプを選択することができます。

暗号化は、識別不能にすることによってネットワーク間を流れるデータを隠します。クライアントがデータを暗号化し、サーバーが暗号化を解除します。暗号化が正しく機能するようにするには、Kerberos サーバ

ーまたは他の通信先アプリケーションで指定された暗号化タイプと同じものを使用する必要があります。この暗号化タイプが一致しないと、暗号化は失敗します。暗号化値は、TGT と TGS の両方に追加できます。

注: TGT および TGS のデフォルトの暗号化値は、des-cbc-crc および des-cbc-md5 です。構成時に、デフォルトの暗号化値が設定されます。以下の手順を完了すると、チケットの他の暗号化値を構成に追加できます。

1. System i ナビゲーターで、「システム」 → 「セキュリティー」を展開する。
2. 「ネットワーク認証サービス」を右クリックして、「プロパティ」を選択する。
3. 「チケット」ページで、使用可能な暗号化タイプのチケット許可チケットまたはチケット許可サービスのいずれかのリストから暗号化値を選択する。
4. 「前に追加」または「後に追加」のいずれかを選択して、選択した暗号化タイプのリストに暗号化タイプを追加する。これらの選択された暗号化タイプはそれぞれ、リストされた順序で試行されます。ある暗号化タイプが失敗すると、リストにある次のタイプが試行されます。
5. 「OK」をクリックします。

チケット許可チケットの取得または更新

- | kinit コマンドは、Kerberos チケット許可チケットを取得または更新します。Kerberos チケット追加 (Add Kerberos Ticket (ADDKRBTKT)) CL コマンドを使用して、チケット許可チケットを取得し、キャッシュに入れることができます。

kinit コマンド

kinit コマンドにチケット・オプションを指定しないと、Kerberos 構成ファイルに指定された Kerberos サーバー用のオプションが使用されます。

既存のチケットを更新するのではない場合、信任状キャッシュが再度初期化され、Kerberos サーバーから受け取った新しいチケット許可チケットがキャッシュに入ります。コマンド行でプリンシパル名を指定しない場合、プリンシパル名は信任状キャッシュから取得されます。-c オプションでキャッシュ名が指定されていない限り、新しい信任状キャッシュがデフォルトの信任状キャッシュになります。

チケットの時間値は *nw d n h m s* の形式で指定します。*n* は数字、*w* は週、*d* は日、*h* は時間、*m* は分、*s* は秒をそれぞれ表します。各時間要素はこの順に指定しなければなりません。ただし、任意の要素を省略することは可能です (例えば *4h5m* は 4 時間 5 分、*1w2h* は 1 週間と 2 時間をそれぞれ表します)。数字だけを指定した場合、デフォルトの単位は時間になります。

jday というプリンシパルのために存続時間が 5 時間のチケット許可チケットを取得するには、次のオプションのどちらかを選択します。

- Qshell コマンド行で、`kinit -l 5h Jday` と入力します。
- i5/OS 制御言語 (CL) コマンド行で、`call qsys/qkrbkinit parm('-l' '5h' 'jday')` と入力します。

この Qshell コマンドの使用法および制約事項に関する詳細については、**kinit** の使用上の注意を参照してください。

I Kerberos チケット追加 (Add Kerberos Ticket (ADDKRBTKT)) コマンド

I i5/OS コマンド行で、CL コマンド ADDKRBTKT を使用して、チケット許可チケットを取得することができます。例えば、プリンシパル `krbsrv400/jday.myco.com` およびデフォルトのレルムを使用して、転送可能
I チケットを追加するには、以下のコマンドを入力します。

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

関連資料

Kerberos チケット追加 (Add Kerberos Ticket (ADDKRBTKT)) コマンド

kinit

Qshell コマンド `kinit` は、Kerberos チケット許可チケットを取得または更新します。

構文

```
kinit [-r time] [-R] [-p] [-f] [-A] [-l time] [-c cache] [-k] [-t keytab] [principal]
```

デフォルトの共通権限: *USE

オプション

-r time

チケットを更新する時間間隔。この間隔が期限切れになると、チケットを更新できなくなります。更新時間は終了時間より大きくなっていなければなりません。このオプションを指定しないと、チケットは更新不可能になります (ただし、要求したチケットの存続時間がチケットの最大存続時間より長ければ、更新可能なチケットの作成は可能です)。

-R 既存のチケットを更新します。既存のチケットを更新する場合、他のチケット・オプションを指定できません。

-p チケットはプロキシであってもかまいません。このオプションを指定しなければ、チケットはプロキシにはなれません。

-f チケットを転送できます。このオプションを指定しなければ、チケットを転送できません。

-A チケットにはクライアント・アドレスのリストは含められません。このオプションを指定しなければ、チケットにはローカル・ホストのアドレス・リストが含まれます。初期チケットにアドレス・リストが含まれていると、アドレス・リストに示されたいずれかのアドレスからのみ、その初期チケットを使用できます。

-l time

チケットの終了時間間隔。この間隔が期限切れになると、更新しない限りチケットを使用できなくなります。このオプションを指定しなければ、終了時間間隔は 10 時間に設定されます。

-c cache

`kinit` コマンドが使用する信任状キャッシュの名前。このオプションを指定しなければ、このコマンドはデフォルトの信任状キャッシュを使います。

-k チケット・プリンシパルのキーをキー・テーブルから取得します。このオプションが指定されていないと、システムは、ユーザーにチケット・プリンシパルのパスワードを入力するよう指示するプロンプトを出します。

-t keytab

キー・テーブルの名前。このオプションは指定しないが -k オプションを指定している場合には、システムはデフォルトのキー・テーブルを使用します。 -t オプションを指定すると、-k オプションが暗黙指定されます。

principal

チケット・プリンシパル。コマンド行でプリンシパルを指定しない場合、システムはプリンシパルを信任状キャッシュから取得します。

権限

参照されるオブジェクト	必要な権限
-t オプションが指定されている場合にキー・テーブル・ファイルに先行するパス名の中の各ディレクトリー	*X
-t を指定したときのキー・テーブル・ファイル	*R
使用する信任状キャッシュ・ファイルに先行するパス名の中にある各ディレクトリー	*X
KRB5CCNAME 環境変数で指定している場合に使用されるキャッシュ・ファイルの親ディレクトリー、および作成されるファイル	*WX
信任状キャッシュ・ファイル	*RW
構成ファイルに至るパス内の各ディレクトリー	*X
構成ファイル	*R

Kerberos ランタイムが任意の実行中プロセスから信任状キャッシュ・ファイルを見つけられるように、キャッシュ・ファイルの名前は通常ホーム・ディレクトリーの **krb5ccname** という名前のファイルに保管されています。キャッシュ・ファイル名の保管場所は **_EUV_SEC_KRB5CCNAME_FILE** 環境変数を設定することによってオーバーライドすることができます。このファイルにアクセスするユーザー・プロファイルは、パス内の各ディレクトリーに対して ***X** 権限を持ち、キャッシュ・ファイル名を保管するファイルに対して ***R** 権限を持っていない限りなりません。信任状キャッシュをはじめて作成するときには、ユーザー・プロファイルは親ディレクトリーに対して ***WX** 権限を必要とします。

メッセージ

- option_name オプションには値が必要です。
- command_option は有効なコマンド・オプションではありません。
- チケットの更新または検証のときにはオプションを指定できません。
- デフォルトの信任状キャッシュの名前を取得できません。
- 信任状キャッシュ file_name を解決できません。
- 初期チケットが使用可能ではありません。
- プリンシパル名を指定する必要があります。
- 信任状キャッシュ file_name からチケットを取り出せません。
- 初期チケットが更新不可能です。
- option_value オプションは request_name 要求に対しては無効です。
- 初期信任状を取得できません。
- プリンシパル名を解析できません。
- キー・テーブル file_name を解決できません。

- principal_name のパスワードが正しくありません。
- パスワードを読み取れません。
- 初期信任状を信任状キャッシュ file_name に保管できません。
- 時間差分値が無効です。

このコマンドの使用例については、『チケット許可チケットの取得または更新』を参照してください。

信任状キャッシュの表示

- | klist コマンドは Kerberos 信任状キャッシュの内容を表示します。信任状キャッシュ・ファイルの表示 (Display Credentials Cache File (DSPKRBCCF)) CL コマンドを使用して、ローカル信任状キャッシュでエントリーを表示することができます。

klist コマンド

デフォルトの信任状キャッシュのエントリーをすべてリストし、チケット・フラグを表示するには、次のオプションのどちらかを選択します。

- Qshell コマンド行で次のように入力します。 `klist -f -a`
- i5/OS 制御言語 (CL) コマンド行で、次のように入力します。 `call qsys/qkrbklist parm('-f' '-a')`

この Qshell コマンドの使用法および制約事項に関する詳細については、**klist** の使用上の注意を参照してください。

| Kerberos 信任状キャッシュ・ファイルの表示 (Display Kerberos Credentials Cache File (DSPKRBCCF)) コマンド

- | i5/OS CL コマンド行で、Kerberos 信任状キャッシュ・ファイルの表示 (Display Kerberos Credentials Cache File (DSPKRBCCF)) コマンドを使用して、信任状を表示することもできます。例えば、デフォルトの信任状のキャッシュ・ファイルを表示するには、次のコマンドを入力します。

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

関連資料

Kerberos 信任状キャッシュ・ファイルの表示 (Display Kerberos Credentials Cache File (DSPKRBCCF)) コマンド

klist

Qshell コマンド `klist` は Kerberos 信任状キャッシュまたはキー・テーブルの内容を表示します。

構文

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

デフォルトの共通権限: *USE

オプション

- a 有効期限が切れたチケットも含めて、信任状キャッシュ内のチケットをすべて表示します。このオプションを指定しなければ、有効期限が切れたチケットは表示されません。このオプションが有効なのは、信任状キャッシュをリストする場合だけです。

- e セッション・キーとチケットの暗号化タイプを表示します。このオプションが有効なのは、信任状キャッシュをリストする場合だけです。
- c 信任状キャッシュ内のチケットをリストします。-c と -k がどちらも指定されていなければ、これがデフォルトになります。このオプションは -k オプションと一緒に指定できません。
- f 次の省略形を使って、チケットのフラグを表示します。

省略形	意味
F	チケットを転送できる
f	転送されたチケット
P	チケットはプロキシーであってもよい
p	プロキシーのチケット
D	チケットの日付を遅らせることができる
d	日付を遅らせたチケット
R	更新可能なチケット
I	初期チケット
i	無効なチケット
A	使用された事前認証
O	サーバーを委任できる
C	Kerberos サーバーがチェックした通過リスト

このオプションが有効なのは、信任状キャッシュをリストする場合だけです。

- s コマンドの出力結果を表示せず、信任状キャッシュ内に有効なチケット許可チケットが見つかった場合には終了状況を 0 に設定します。このオプションが有効なのは、信任状キャッシュをリストする場合だけです。
- k キー・テーブルのエントリーをリストします。このオプションは -c オプションと一緒に指定できません。
- t キー・テーブルのエントリーのタイム・スタンプを表示します。このオプションが有効なのは、キー・テーブルをリストする場合だけです。
- K キー・テーブルの各エントリーの暗号鍵値を表示します。このオプションが有効なのは、キー・テーブルをリストする場合だけです。

filename

信任状キャッシュまたはキー・テーブルの名前を指定します。ファイル名が指定されていなければ、デフォルトの信任状キャッシュまたはキー・テーブルが使われます。

権限

参照されるオブジェクト	必要な権限
keytab として -k オプションが指定されている場合にファイルに先行するパス名の中の各ディレクトリー	*X
-k を指定したときの Keytab ファイル	*R
-k オプションが指定されていない場合に信任状キャッシュ・ファイルに先行するパス名の中の各ディレクトリー	*X
-k オプションが指定されていない場合の信任状キャッシュ・ファイル	*R

Kerberos ランタイムが任意の実行中プロセスから信任状キャッシュ・ファイルを見つけられるように、キャッシュ・ファイルの名前は通常ホーム・ディレクトリーの **krb5ccname** という名前のファイルに保管されています。キャッシュ・ファイル名の保管場所は **_EUV_SEC_KRB5CCNAME_FILE** 環境変数を設定す

ることによってオーバーライドすることができます。このファイルにアクセスするユーザー・プロファイルは、パス内の各ディレクトリーに対して ***X** 権限を持ち、キャッシュ・ファイル名を保管するファイルに対する ***R** 権限を持っていなければなりません。信任状キャッシュをはじめて作成するときには、ユーザー・プロファイルは親ディレクトリーに対して ***WX** 権限を必要とします。

メッセージ

- option_name オプションには値が必要です。
- command_option は有効なコマンド・オプションではありません。
- command_option_one と command_option_two を一緒に指定することはできません。
- デフォルトの信任状キャッシュが見つかりません。
- 信任状キャッシュ file_name を解決できません。
- 信任状キャッシュ file_name からプリンシパル名を取得できません。
- 信任状キャッシュ file_name からチケットを取り出せません。
- チケットをデコードできません。
- デフォルトのキー・テーブルが見つかりません。
- キー・テーブル file_name を解決できません。

このコマンドの使用例については、『信任状キャッシュの表示』を参照してください。

keytab ファイルの管理

文字ベース・インターフェースまたは System i ナビゲーター のどちらかを使用して、keytab ファイルを維持管理できます。

ネットワーク管理者として、keytab ファイル (キー・テーブルとも呼ばれる) およびその内容を i5/OS オペレーティング・システム上で維持管理する必要があります。文字ベース・インターフェースあるいは System i ナビゲーター のいずれかを使用して、以下のように keytab ファイルおよび関連する keytab エントリーを管理することができます。

文字ベース・インターフェース使用による keytab ファイルの管理

- ```
| • keytab コマンドは、キー・テーブルのキーを追加または削除したり、リストしたりするために使用でき
| ます。例えば、レルム MYCO.COM のホスト kdc1.myco.com 上のサービス・プリンシパル krbsvr400
| にキーを追加するには、次のいずれかの方法を使用します。
| - Qshell コマンド行で keytab add krbsvr400/kdc1.myco.com@MYCO.COM と入力します
| - i5/OS 制御言語 (CL) コマンド行で、call qsys/qkrbkeytab parm('add' 'krbsvr400/
| kdc1.myco.com@MYCO.COM') と入力します
```

Kerberos サーバーに対してサービスを定義したときに使ったパスワードの入力を求められます。

この Qshell コマンドの使用法および制約事項に関する詳細については、**keytab** の使用上の注意を参照してください。

- ```
| • CL コマンド行で、Kerberos Keytab エントリーの追加 (Add Kerberos Keytab Entry (ADDKRBKTE))、
| Kerberos Keytab エントリーの表示 (Display Kerberos Keytab Entries (DSPKRBKTE))、および Kerberos
| Keytab エントリーの除去 (Remove Kerberos Keytab Entry (RMVKRBKTE)) コマンドを使用して、keytab
| ファイルを管理することもできます。
```

System i ナビゲーターによる keytab ファイルの管理

System i ナビゲーター を使用してキー・テーブルに keytab エントリーを追加することができます。
System i ナビゲーター により、以下のサービス用の keytab エントリーを追加することができます。

- | • i5/OS Kerberos 認証
- | • LDAP
- | • IBM HTTP Server
- | • i5/OS NetServer
- | • ネットワーク・ファイルシステムのサーバー

keytab ファイルに keytab エントリーを追加するには、以下の手順を行います。

1. System i ナビゲーターで、「システム」 → 「セキュリティー」を展開する。
2. 「ネットワーク認証サービス」を右クリックして、「keytab の管理 (Manage Keytab)」を選択する。
これにより、keytab エントリーを追加できるようにする「ネットワーク認証サービス」ウィザードの部分が立ち上がります。
3. 「keytab エントリーの選択」ページで、keytab ファイルを追加したいサービスのタイプ (例えば i5/OS Kerberos 認証) を選択する。「次へ」をクリックします。
4. 「i5/OS keytab エントリーの作成」ページで、パスワードを入力して確認する。このパスワードは、関連するサービス・プリンシパルを Kerberos サーバーに追加する際に使用するパスワードと同じでなければなりません。ステップ 3 で、LDAP、HTTP Server、i5/OS NetServer、またはネットワーク・ファイル・システム・サーバーなど、他のタイプのサービスを選択した場合は、これらのサービスのそれぞれに対して keytab エントリーを作成できるようにするページも表示されます。
5. 「要約」ページで、keytab ファイルに対して keytab エントリーとして追加される i5/OS サービスおよびサービス・プリンシパルのリストを表示します。

関連資料

Kerberos Keytab エントリーの追加 (Add Kerberos Keytab Entry (ADDKRBKTE)) コマンド

Kerberos Keytab エントリーの表示 (Display Kerberos Keytab Entries (DSPKRBKTE)) コマンド

Kerberos Keytab エントリーの除去 (Remove Kerberos Keytab Entry (RMVKRBKTE)) コマンド

keytab

Qshell コマンド keytab はキー・テーブルを管理します。

構文

```
keytab add principal [-p password] [-v version] [-k keytab] keytab delete principal [-v version] [-k keytab] keytab list [principal] [-k keytab]
```

デフォルトの共通権限: *USE

オプション

- k キー・テーブルの名前。このオプションを指定しないと、デフォルトのキー・テーブルが使われます。
- p パスワードを指定します。このオプションを指定しないと、キー・テーブルにエントリーを追加するときにパスワードを入力するよう求めるプロンプトが出されます。
- v キーのバージョン番号。キーを追加するときに、このオプションを指定していないと、その次のバージョン番号が割り当てられます。キーを削除するときに、このオプションを指定していないと、該当プリンシパルのすべてのキーが削除されます。

principal

プリンシパル名。キー・テーブルをリストする場合、このオプションを指定していないと、すべてのプリンシパルが表示されます。

権限

参照されるオブジェクト	必要な権限
オープンされるターゲットの keytab ファイルに先行するパス名のなかにある各ディレクトリー	*X
keytab ファイルがまだ存在しない場合、add を指定したときのターゲットの keytab ファイルの親ディレクトリー	*WX
list を指定したときの Keytab ファイル	*R
add または delete を指定したときのターゲットの keytab ファイル	*RW
構成ファイルに至るパス内の各ディレクトリー	*X
構成ファイル	*R

メッセージ

- *add*、*delete*、*list*、または *merge* のいずれかを指定する必要があります。
- *command_option* は有効なコマンド・オプションではありません。
- *command_option_one* と *command_option_two* を一緒に指定することはできません。
- *option_value* オプションは *request_name* 要求に対しては無効です。
- *option_name* オプションには値が必要です。
- プリンシパル名を解析できません。
- プリンシパル名を指定する必要があります。
- パスワードを読み取れません。
- デフォルトのキー・テーブルが見つかりません。
- キー・テーブル *key_table* を解決できません。
- キー・テーブル *key_table* からエントリーを読み取れません。
- キー・テーブル *key_table* からエントリーを除去できません。
- キー・テーブル *key_table* にエントリーを追加できません。
- プリンシパル *principal_name* のエントリーが見つかりません。
- 値が無効な数字です。
- キー・バージョンは 1 から 255 までの間でなければなりません。
- プリンシパル *principal_name* についてキー・バージョン *key_version* が見つかりません。

このコマンドの使用例については、『Keytab ファイルの管理』を参照してください。

Kerberos パスワードの変更

- 1 kpasswd コマンドは、パスワード変更サービスを使用して、指定された Kerberos プリンシパルのパスワードを変更します。「Kerberos パスワードの変更 (Change Kerberos Password (CHGKRBPWD))」 CL コマンドを使用して、Kerberos パスワードを変更することもできます。

kpasswd コマンド

新規パスワードに加えて、プリンシパルの現行パスワードも提供する必要があります。パスワード・サーバーは、パスワードを変更する前に、適用できるパスワード・ポリシー規則を新規パスワードに適用します。パスワード・サーバーは、Kerberos サーバーのインストール時および構成時に構成されます。そのシステムに対応する資料を参照してください。

注: i5/OS PASE は、パスワード・サーバーをサポートしません。Kerberos サーバー上に保管されているプリンシパルのパスワードを変更するには、PASE 環境に入って (call QP2TERM)、kpasswd コマンドを出す必要があります。

ネットワーク認証サービスの構成時に、パスワード・サーバーの名前を指定できます。構成時にパスワード・サーバーを指定しなかった場合は、パスワード・サーバーを追加することができます。

チケット許可サービスのプリンシパル (krbtgt/realm) のパスワードは kpasswd を使用して変更することはできません。

デフォルト・プリンシパルのパスワードを変更する場合：

- Qshell コマンド行で、kpasswd と入力します
- コマンド行で、call qsys/qkrbkpasswd と入力します

別のプリンシパルのパスワードを変更する場合：

- Qshell コマンド行で、kpasswd jday@myco.com と入力します

i5/OS PASE 内の別のプリンシパルのパスワードを変更する場合:

文字ベース・インターフェースを使用

1. 文字ベース・インターフェースで call QP2TERM と入力する。このコマンドは、ユーザーが i5/OS PASE アプリケーションを処理できるようにする対話式シェル環境をオープンします。
2. コマンド行で export PATH=\$PATH:/usr/krb5/sbin と入力する。このコマンドは、実行可能ファイルを実行するために必要な Kerberos スクリプトを指します。
3. QSH プロンプトで kadmin -p admin/admin と入力する。Enter キーを押します。
4. 管理者のユーザー名およびパスワードを使ってサインインする。
5. kpasswd jday@myco.com と入力する。このプリンシパルのパスワードを変更するためのプロンプトが出されます。

コマンド行を使用

コマンド行で、call qsys/qkrbkpasswd parm ('jday@myco.com') と入力します

このコマンドの使用の詳細については、passwd の使用上の注意を参照してください。

1 Kerberos パスワード変更 (Change Kerberos Password (CHGKRBPWD)) コマンド

1 i5/OS コマンド行で、Kerberos パスワードの変更 (Change Kerberos Password (CHGKRBPWD)) コマンドを使用して Kerberos パスワードを変更することもできます。例えば、realm myco.com での Kerberos プリンシパル jday の場合、ユーザーは次のコマンドを使用して、パスワードを myoldpwd から mynewpwd に変更することができます:

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

関連資料

Kerberos パスワード変更 (Change Kerberos Password (CHGKRBPWD)) コマンド

kpasswd

Qshell コマンド kpasswd は Kerberos プリンシパルのパスワードを変更します。

構文

```
kpasswd [-A ] [principal]
```

デフォルトの共通権限: *USE

オプション

-A kpasswd コマンドで使用する初期チケットにはクライアント・アドレスのリストは含められません。このオプションを指定しなければ、チケットにはローカル・ホストのアドレス・リストが含まれます。初期チケットにアドレス・リストが含まれていると、アドレス・リストに示されたいずれかのアドレスからのみ、その初期チケットを使用できます。

principal

パスワードを変更するプリンシパル。コマンド行にプリンシパルを指定しなければ、プリンシパルはデフォルト信任状キャッシュから取得されます。

メッセージ

- プリンシパル %3\$s が無効です。
- デフォルトの信任状キャッシュ file_name を読み取れません。
- デフォルトの信任状キャッシュが見つかりません。
- 信任状キャッシュ file_name からチケットを取り出せません。
- パスワードを読み取れません。
- パスワードの変更が取り消されました。
- principal_name のパスワードが正しくありません。
- 初期チケットを取得できません。
- パスワードの変更要求が失敗しました。

このコマンドの使用例については、『Kerberos パスワードの変更』を参照してください。

有効期限が切れた信任状キャッシュ・ファイルの削除

- | kdestroy コマンドは Kerberos 信任状キャッシュ・ファイルを削除します。Kerberos 信任状キャッシュの
- | 削除 (Delete Kerberos Credentials Cache (DLTKRBCCF)) CL コマンドを使用して、信任状キャッシュを削
- | 除することができます。ユーザーは、定期的に古い信任状を削除する必要があります。

kdestroy コマンド

-e オプションを指定すると、kdestroy コマンドはデフォルトのディレクトリー (/QIBM/UserData/OS400/NetworkAuthentication/creds) に入っている信任状キャッシュ・ファイルをすべてチェックします。有効期限が過ぎて *time_delta* 値の時間が経過したチケットのみが入っているファイルは、すべて削除されます。*time_delta* オプションは *nwndnhnmns* の形式で表されます。*n* は数字、*w* は週、*d* は日、*h* は時間、*m* は分、*s* は秒をそれぞれ示します。各時間要素はこの順に指定しなければなりません。ただし、任意の要素を

省略することは可能です (例えば *4h5m* は 4 時間 5 分、*1w2h* は 1 週間と 2 時間をそれぞれ表します)。数字だけを指定した場合、デフォルトの単位は時間になります。

1. デフォルトの信任状キャッシュを削除するには:
 - Qshell コマンド行で、`kdestroy` と入力します
 - i5/OS 制御言語 (CL) コマンド行で、`call qsys/qkrbkdstry` と入力します
2. チケットの有効期限が切れてから 1 日以上が経過した信任状キャッシュ・ファイルをすべて削除するには
 - Qshell コマンド行で、`kdestroy -e 1d` と入力します
 - CL コマンド行で、`call qsys/qkrbkdstry parm ('-e' '1d')` と入力します

この Qshell コマンドの使用法および制約事項に関する詳細については、**kdestroy** の使用上の注意を参照してください。

1 Kerberos 信任状キャッシュの削除 (Delete Kerberos Credentials Cache (DLTKRBCCF)) コマンド

- 1 i5/OS コマンド行で、DLTKRBCCF コマンドを使用して、信任状キャッシュを削除することができます。
- 1 デフォルトの信任状キャッシュを削除するには、DLTKRBCCF CCF(*DFT) を入力します。
- 1 チケットの有効期限が切れてから 1 日以上が経過した信任状キャッシュ・ファイルをすべて削除するには、DLTKRBCCF CCF(*EXPIRED) EXPTIME(1440) を入力します。

関連資料

Kerberos 信任状キャッシュ・ファイルの削除 (Delete Kerberos Credentials Cache File (DLTKRBCCF)) コマンド

kdestroy

Qshell コマンド `kdestroy` は Kerberos 信任状キャッシュを破棄します。

構文

```
kdestroy [-c cache_name] [-e time_delta]
```

デフォルトの共通権限: *USE

オプション

-c *cache_name*

破棄すべき信任状キャッシュの名前。コマンドのオプションが指定されていなければ、デフォルトの信任状キャッシュが破棄されます。このオプションは `-e` オプションと一緒に指定できません。

-e *time_delta*

有効期限が切れてから少なくとも *time_delta* 値の間の時間が経過したチケットが入っている信任状キャッシュ・ファイルが、すべて破棄されます。

権限

信任状キャッシュのタイプが **FILE** である場合 (キャッシュ・タイプの詳細については `krb5_cc_resolve()` を参照)、デフォルトの動作では、信任状キャッシュは `/QIBM/UserData/OS400/NetworkAuthentication/creds` ディレクトリーに作成されます。信任状キャッシュ・ファイルの配置は `KRB5CCNAME` 環境変数を設定することによって変更することができます。

信任状キャッシュ・ファイルがデフォルトのディレクトリーにない場合、以下の権限が必要になります。

参照されるオブジェクト	必要なデータ権限	必要なオブジェクト権限
信任状キャッシュ・ファイルに先行するパス名の中にある各ディレクトリー	*X	なし
信任状キャッシュ・ファイルの親ディレクトリー	*WX	なし
信任状キャッシュ・ファイル	*RW	*OBJEXIST
構成ファイルに至るパス内の各ディレクトリー	*X	なし
構成ファイル	*R	なし

信任状キャッシュ・ファイルがデフォルトのディレクトリーにある場合は、以下の権限が必要になります。

参照されるオブジェクト	必要なデータ権限	必要なオブジェクト権限
パス名の中にあるすべてのディレクトリー	*X	なし
信任状キャッシュ・ファイル	*RW	なし
構成ファイルに至るパス内の各ディレクトリー	*X	なし
構成ファイル	*R	なし

Kerberos プロトコルが任意の実行中プロセスから信任状キャッシュ・ファイルを見つけられるように、キャッシュ・ファイルの名前は通常ホーム・ディレクトリーの `krb5ccname` という名前のファイルに保管されています。System i プラットフォーム上で Kerberos 認証を使用したいユーザーは、ホーム・ディレクトリーを定義しておく必要があります。デフォルトでは、ホーム・ディレクトリーは `/home/` です。コマンドのオプションが何も指定されていなければ、このファイルを使ってデフォルトの信任状キャッシュを見つけます。キャッシュ・ファイル名の保管場所は `_EUV_SEC_KRB5CCNAME_FILE` 環境変数を設定することによってオーバーライドすることができます。このファイルにアクセスするユーザー・プロファイルは、パス内の各ディレクトリーに対して *X 権限を持ち、キャッシュ・ファイル名を保管するファイルに対する *R 権限を持っていないければなりません。

メッセージ

- 信任状キャッシュ `cache_file_name` を解決できません。
- 信任状キャッシュ `cache_file_name` を破棄できません。
- `function_name` 関数がエラーを検出しました。
- 信任状キャッシュ `file_name` からチケットを取り出せません。
- `option_name` オプションには値が必要です。
- `command_option` は有効なコマンド・オプションではありません。
- `command_option_one` と `command_option_two` を一緒に指定することはできません。
- デフォルトの信任状キャッシュが見つかりません。
- 時間差分値 `value` が有効ではありません。

このコマンドの使用例については、『期限切れの信任状キャッシュ・ファイルの削除』を参照してください。

LDAP ディレクトリー内の Kerberos サービス・エントリーの管理

ksetup コマンドは LDAP サーバー・ディレクトリーの Kerberos サービス・エントリーを管理します。

目的

ksetup コマンドは LDAP サーバー・ディレクトリーの Kerberos サービス・エントリーを管理します。以下のサブコマンドがサポートされています。

addhost host-name realm-name

このサブコマンドは、指定したレルムのホスト・エントリーを追加します。Kerberos クライアントでどの DNS ドメインが有効になっていてもホスト名が正しく解決されるように、完全修飾ホスト名を指定してください。レルム名を指定しなければ、デフォルトのレルム名が使用されます。

addkdc host-name:port-number realm-name

このサブコマンドは、指定したレルムのエントリーを Kerberos サーバーに追加します。ホスト・エントリーがまだ存在していなければ、新たに作成されます。ポート番号が指定されていなければ、88 に設定されます。Kerberos クライアントでどの DNS ドメインが有効になっていても名前が正しく解決されるように、完全修飾ホスト名を指定してください。レルム名を指定しなければ、デフォルトのレルム名が使用されます。

delhost host-name realm-name

このサブコマンドは、指定したレルムから、ホスト・エントリーと、それに関連する Kerberos サーバーの指定を削除します。レルム名を指定しなければ、デフォルトのレルム名が使用されます。

delkdc host-name realm-name

このサブコマンドは、Kerberos サーバー内の指定したホストのエントリーを削除します。ホスト・エントリー自体は削除されません。レルム名を指定しなければ、デフォルトのレルム名が使用されます。

listhost realm-name

このサブコマンドは、レルムの Kerberos サーバー内のエントリーをリストします。レルム名を指定しなければ、デフォルトのレルム名が使用されます。

exit このサブコマンドは ksetup コマンドを終了します。

制約事項: System i 製品は、文字ベース・インターフェースでは LDAP クライアントをサポートしますが、i5/OS PASE ではサポートしません。

例

- 1 管理者のディレクトリー・サーバー (LDAP) 管理者 ID とパスワード verysecret を使用して、レルム MYCO.COM の Kerberos サーバーとしてホスト kdc1.myco.com をサーバー ldapserv.myco.com に追加するには、以下の手順を完了してください。

Qshell コマンド行で次のように入力します。 `ksetup -h ldapserv.myco.com -n CN=Administrator -p verysecret`

または

1. i5/OS 制御言語 (CL) コマンド行で、次のように入力します。

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

2. ディレクトリー・サーバー (LDAP) が正常に連絡されれば、サブコマンドのプロンプトが表示されません。次のように入力してください。


```
addkdc kdc1.myco.com MYCO.COM
```

この Qshell コマンドの使用法および制約事項に関する詳細については、**ksetup** の使用上の注意を参照してください。

ksetup

Qshell コマンド **ksetup** は、Kerberos レルムのディレクトリー・サーバーにある Kerberos サービス・エントリーを管理します。

構文

```
ksetup -h host-name -n bind-name -p bind-password -e
```

デフォルトの共通権限: *USE

オプション

- h** ディレクトリー・サーバーのホスト名。このオプションを指定しなければ、Kerberos 構成ファイルで指定したディレクトリー・サーバーが使われます。
- n** ディレクトリー・サーバーにバインドするときに使う識別名。このオプションを指定しなければ、LDAP_BINDDN 環境変数を使って名前を取得します。
- p** ディレクトリー・サーバーにバインドするときに使うパスワード。このオプションを指定しなければ、LDAP_BINDPW 環境変数を使ってパスワードを取得します。
- e** 各コマンド行を stdout (標準出力) にエコーします。このオプションが役に立つのは、stdin (標準入力) がファイルにリダイレクトされている場合です。

権限

参照されるオブジェクト	必要な権限
構成ファイルに至るパス内の各ディレクトリー	*X
構成ファイル	*R

メッセージ

- subcommand が有効なサブコマンドではありません。
- 有効なサブコマンドは addhost、addkdc、delhost、delkdc、listhost、listkdc、exit です。
- command_option_one と command_option_two を一緒に指定することはできません。
- LDAP クライアントを初期化できません。
- ディレクトリー・サーバーにバインドできません。
- レルム名を指定してください。
- ホスト名を指定してください。
- 定位置パラメーターが多すぎます。
- ホスト host は既に存在しています。
- ルート・ドメイン domain が定義されていません。
- レルム名 realm が無効です。
- LDAP function name 関数がエラーを検出しました。
- ストレージが不足しています。

- ホスト名 `host` が無効です。
- ポート番号 `port` が無効です。
- ホスト `host` が定義されていません。
- ホスト `host` の Kerberos サーバーが定義されていません。
- デフォルトのレルム名を取得できません。

このコマンドの使用例については、『LDAP ディレクトリーでの Kerberos サービス・エントリーの管理』を参照してください。

DNS データベースでのレルムの定義

ホスト名を解決するために DNS データベースにレルムを定義できます。

ネットワーク認証サービスでは DNS サーバーを使ってホスト名を解決できます。このためには、レルム内の各鍵配布センターにサーバー (SRV) レコードとテキスト (TXT) レコードを追加しなければなりません。Kerberos プロトコルは DNS 検索名としてレルム名を使って SRV レコードを検索します。

DNS でレルムを定義するには、以下の手順を完了してください。

1. DNS を使うように構成ファイルを設定する。
2. レルム内の各 KDC サーバーごとに、DNS サーバーに対して SRV レコードを追加します。Kerberos ランタイムは検索名としてレルム名を使って SRV レコードを検索します。DNS 検索では大/小文字の区別が行われないことに注意してください。したがって、大文字と小文字だけが異なる同名のレルムを 2 つ定義することはできません。Kerberos SRV レコードの一般的な形式は次のとおりです。

```
service.protocol.realm TTL class SRV priority weight port target
```

`_kerberos` サービス・エントリーは KDC インスタンスを定義し、`_kpasswd` サービス・エントリーはパスワード変更サービス・インスタンスを定義します。

エントリーは優先順位の順に試みられます (0 が最高の優先順位です)。同一の優先順位のエントリーはランダムに試みられます。`_kerberos` エントリーと `_kpasswd` エントリーには、`_udp` プロトコル・レコードが必要です。

3. TXT レコードを追加して、ホスト名をレルム名に関連付けます。Kerberos プロトコルはホスト名から始まる TXT レコードを探します。TXT レコードが見つからなければ、先頭のラベルが除去されて新しい名前前で再度検索が試みられます。このプロセスは TXT レコードが見つかるか、またはルートに到達するまで繰り返されます。TXT レコードではレルム名の大/小文字の区別が行われることに注意してください。TXT レコードの一般的な形式は次のとおりです。

```
service.name TTL class TXT realm
```

この構成例では、以下のレコードを追加することにより、2 つのレルム用の KDC の例を定義することができます。

```
_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
```

この構成例では、Kerberos の TXT レコードの一般的な形式に従って、deptxyz ドメインと deptabc ドメインのホストを、以下のステートメントを使用して、それぞれのレルムに関連付けることができます。

```
_kerberos.deptxyz.bogusname.com IN TXT DEPTXYZ.BOGUSNAME.COM  
_kerberos.deptabc.bogusname.com IN TXT DEPTABC.BOGUSNAME.COM
```

DNS 検索の使用を指定したサンプルの **krb5.conf** 構成ファイルは次のとおりです。

サンプルの **krb5.conf** 構成ファイル

```
; krb5.conf - Kerberos V5 configuration file DO NOT REMOVE THIS LINE  
;  
[libdefaults]  
; The default_realm value  
;-default_realm = REALM1.ROCHESTER.IBM.COM  
default_realm = DEPTXYZ.BOGUSNAME.COM  
;  
; define the system to use DNS lookup  
use_dns_lookup = 1  
[realms]  
;  
; We could configure the same realm information here, but it would  
; only be used if the DNS lookup failed.  
;  
[domain_realm]  
; Convert host names to realm names. Individual host names may be  
; specified. Domain suffixes may be specified with a leading period  
; and will apply to all host names ending in that suffix.  
;  
; We will use DNS to resolve what realm a given host name belongs to.  
;  
[capaths]  
; Configurable authentication paths define the trust relationships  
; between client and servers. Each entry represents a client realm  
; and consists of the trust relationships for each server that can  
; be accessed from that realm. A server may be listed multiple times  
; if multiple trust relationships are involved. Specify '.' for  
; a direct connection.  
;-REALM1.ROCHESTER.IBM.COM = {  
;   REALM2.ROCHESTER.IBM.COM = .  
; }  
;-DEPTXYZ.BOGUSNAME.COM = {  
;   DEPTABC.BOGUSNAME.COM = .  
; }  
}
```

LDAP サーバーでのレルムの定義

ネットワーク認証サービスでは、LDAP サーバーを使ってホスト名を Kerberos レルムに解決し、Kerberos レルム用の KDC を見つけることができます。

LDAP を使ってこの情報を探索する場合には、LDAP サーバーに情報を定義しておく必要があります。これを行うには、以下の 2 セットのタスクを完了させます。

1. LDAP を使うように構成ファイルを設定する。

System i ナビゲーター を使用して、ホスト名を解決するためにどのディレクトリー・サーバーを使用したいかを指定します。これで、**/QIBM/UserData/OS400/NetworkAuthentication/krb5.conf** にある

krb5.conf 構成ファイルが更新されます。ディレクトリー・サーバーの名前が、構成ファイルの [libdefaults] セクションに追加されます。次に示すのは、この構成ファイルのサンプルです。

サンプルの krb5.conf 構成ファイル

```
; krb5.conf - Kerberos V5 configuration file DO NOT REMOVE THIS LINE
;
[libdefaults]
; The default_realm value
;-default_realm = REALM1.ROCHESTER.IBM.COM
default_realm = DEPTXYZ.BOGUSNAME.COM
; define the system to use LDAP lookup
use_ldap_lookup = 1
ldap_server = dirserv.bogusname.com
[realms]
;
; We could configure the same realm information here, but it would
; only be used if the LDAP lookup failed.
;
[domain_realm]
; Convert host names to realm names. Individual host names may be
; specified. Domain suffixes may be specified with a leading period
; and will apply to all host names ending in that suffix.
;
; We will use LDAP to resolve what realm a given host name belongs to.
; We could define them here also, but they would only be used if the
; LDAP lookup fails.
;
[capaths]
; Configurable authentication paths define the trust relationships
; between client and servers. Each entry represents a client realm
; and consists of the trust relationships for each server that can
; be accessed from that realm. A server may be listed multiple times
; if multiple trust relationships are involved. Specify '.' for
; a direct connection.
;-REALM1.ROCHESTER.IBM.COM = {
;- REALM2.ROCHESTER.IBM.COM = .
;};
DEPTXYZ.BOGUSNAME.COM = {
  DEPTABC.BOGUSNAME.COM = .
}
```

2. LDAP サーバー用の Kerberos を定義する。LDAP サーバーは Kerberos レalm名に対応する名前を持つドメイン・オブジェクトを持つ必要があります。例えば、Kerberos レalm名が DEPTABC.BOGUSNAME.COM であるとする、ディレクトリー内に dc=DEPTABC,dc=BOGUSNAME,dc=com という名前のオブジェクトがあることが必要です。このオブジェクトが存在しない場合は、まず LDAP サーバー構成に対して接尾部を追加しなければならない可能性があります。このオブジェクト名について、有効な接尾部は dc=DEPTABC,dc=BOGUSNAME,dc=COM あるいは親エントリー (dc=BOGUSNAME,dc=COM または dc=COM) が含まれます。i5/OS LDAP サーバーの場合、System i ナビゲーターを使用して接尾部を追加できます。
 - a. 接尾部を追加する場合は、以下の手順を行います。
 - 1) System i ナビゲーターで、「システム」→「ネットワーク」→「サーバー」→「TCP/IP」と展開する。
 - 2) 「IBM Directory Server」を右クリックして「プロパティ」を選択する。
 - 3) 「データベース/接尾部 (Database/Suffix)」ページで、追加したい接尾部を指定する。

- b. LDAPADD コマンドを使って、LDAP ディレクトリーのレルムにドメイン・オブジェクトを追加する。
- c. この構成例の 2 つのレルム (DEPTABC.BOGUSNAME.COM と DEPTXYZ.BOGUSNAME.COM という名前) について構成を続けて、統合ファイル・システム・ファイルに以下の行を入れる。

```
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. この統合ファイル・システム・ファイルの名前が **/tmp/addRealms.ldif** である場合、前述の例と同じ前提を使用して、次のコマンドを入力する。

```
STRQSH
ldapadd -h dirserv.bogusname.com -D cn=Administrator
-w verysecret -c -f
/tmp/addRealms.ldif
```

- e. レルム用の KDC エントリーを定義し、(オプションとして) ホスト名のエントリーを定義して、ネットワーク内の各ホストを特定のレルム名に割り当てる。これは、**ksetup** コマンドを、**addkdc** サブコマンドおよび **addhost** サブコマンドと一緒に使用して行うことができます。この構成例を続けます。以下のコマンドを入力することができます。

```
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
```

必要に応じ、各レルムの各ホストについて同じ操作を繰り返します。

LDAP サーバーでのスキーマの定義

i5/OS LDAP サーバー (IBM Directory Server) は、あらかじめ LDAP スキーマが定義されて出荷されます。ただし、IBM Directory Server 以外の LDAP サーバーを使用している場合は、このサーバー上に自分のスキーマを定義することができます。

LDAP スキーマ

以下の情報は、LDAP サーバーに自分のスキーマを定義することを決定する場合に役立ちます。

ネットワーク認証サービスは以下の LDAP スキーマ定義を必要とします。ここで、

- 整数値は、符号付き数値文字列 (最大長 11 文字) で表される。
- ブール値は、文字列の「TRUE」と「FALSE」によって表される。
- 時間値は、「YYYYMMDDhhmmssZ」形式でエンコードされた 15 バイトの文字列によって表される。時間はすべて UTC 値として表される。

LDAP オブジェクト・クラス

オブジェクト	必要となるもの	可能となるもの
domain	dc	description seeAlso
ibmCom1986-Krb-KerberosService	serviceName ibmCom1986-Krb-KerberosRealm	ipServicePort description seeAlso
domain	dc objectClass	description seeAlso

LDAP 属性

属性	タイプ	サイズ	値
dc	caseIgnoreString	64	単一
description	caseIgnoreString	1024	複数
ibmCom1986-Krb-KerberosRealm	caseExactString	256	単一
ipServicePort	integer	11	単一
seeAlso	DN	1000	複数
serviceName	caseIgnoreString	256	単一

ネットワーク認証サービスのトラブルシューティング

このトラブルシューティング情報には、Kerberos 認証をサポートする、ネットワーク認証サービス、エンタープライズ識別マッピング (EIM)、および IBM 提供のアプリケーションに共通する問題が含まれています。

1. すべての前提条件を完成する。
2. ユーザーが System i プラットフォーム上にユーザー・プロファイルを持ち、Kerberos サーバー上にプリンシパルを持つことを確認する。System i プラットフォーム上で、System i ナビゲーターの「ユーザーおよびグループ」をオープンするか、またはコマンド行で WRKUSRPRF 「ユーザー・プロファイルの処理 (Work with User Profile)」 コマンドを入力することによって、ユーザーが存在することを確認する。Windows オペレーティング・システムで実行されているシステムでは、「Active Directory ユーザーとコンピュータ」フォルダーにアクセスしてユーザーが存在することを確認する。
3. Qshell インタープリターから kinit コマンドを使用して、System i プラットフォームが Kerberos サーバーに連絡しているかどうか、検査する。kinit コマンドが失敗した場合は、i5/OS サービス・プリンシパルが Kerberos サーバーに登録されているかどうか調べます。登録されていない場合は、Kerberos サーバーに i5/OS プリンシパルを追加することができます。

関連タスク

110 ページの『Kerberos サーバーへの i5/OS プリンシパルの追加』

System i プラットフォーム上でネットワーク認証サービスを構成した後、Kerberos サーバーに対して i5/OS プリンシパルを追加する必要があります。

ネットワーク認証サービスのエラーおよびリカバリー

これらのエラーは、「ネットワーク認証サービス」ウィザードの実行時、または System i ナビゲーターでネットワーク認証サービスのプロパティを管理しているときに発生します。以下にリストした中から対応するリカバリー方式を使用して、トラブルシューティングしてください。

表 36. ネットワーク認証サービスのエラーおよびリカバリー

エラー	リカバリー
KRBWIZ_CONFIG_FILE_FORMAT_ERROR: ネットワーク認証サービスの構成ファイルの形式にエラーがあります。	ネットワーク認証サービスを再構成します。詳細については、108 ページの『ネットワーク認証サービスの構成』を参照してください。
KRBWIZ_ERROR_READ_CONFIG_FILE: ネットワーク認証サービスの構成ファイルの読み取りエラー。	ネットワーク認証サービスを再構成します。詳細については、108 ページの『ネットワーク認証サービスの構成』を参照してください。
KRBWIZ_ERROR_WRITE_CONFIG_FILE: ネットワーク認証サービスの構成ファイルの書き込みエラー。	構成ファイルの書き込みに使用するサービスが使用不能です。後でもう一度試してください。
KRBWIZ_PASSWORD_MISMATCH: 新規パスワードと、新規パスワードの確認が、一致しません。	新規パスワードと新規パスワードの確認を再入力します。
KRBWIZ_PORT_ERROR: ポート番号は 1 から 65535 までの間でなければなりません。	1 から 65 535 までの間でポート番号を再入力します。
KRBWIZ_ERROR_WRITE_KEYTAB: キー・テーブル・ファイルの書き込みエラー。	keytab の書き込みに使用するサービスが一時的に使用不能です。後でもう一度試してください。
KRBWIZ_NOT_AUTHORIZED_CONFIGURE: ネットワーク認証サービスを構成する権限がありません。	*ALLOBJ および *SECADM の権限を持っていることを確認します。
KrbPropItemExists: 項目は既に存在します。	新しい項目を入力します。
KrbPropKDCInListRequired: リストには KDC が必要です。	指定された Kerberos サーバーがリストに存在しません。リストから Kerberos を選択してください。
KrbPropKDCValueRequired: KDC 名を入力しなければなりません。	Kerberos サーバーに有効な名前を入力します。Kerberos サーバーは、ネットワーク内のセキュア・システムで構成する必要があります。
KrbPropPwdServerRequired: パスワード・サーバー名を入力しなければなりません。	パスワード・サーバーに有効な名前を入力します。
KrbPropRealmRequired: レalm名を入力しなければなりません。	このシステムが属するレalmの名前を入力します。
KrbPropRealmToTrustRequired: 信頼するレalmの名前を入力しなければなりません。	信頼関係を設定するレalmの名前を入力します。
KrbPropRealmValueRequired: レalm名を入力しなければなりません。	レalmに有効な名前を入力します。
CPD3E3F: ネットワーク認証サービス・エラー &2 が起きました。	このメッセージに対応する固有のリカバリー情報を参照してください。

アプリケーション接続の問題およびリカバリー

Kerberos 使用可能な i5/OS のインターフェースおよびそれらのリカバリー方式に共通のエラーがいくつかあります。

表 37. Kerberos を使用できる i5/OS インターフェースに共通のエラー

問題	リカバリー
次のエラーを受け取ります: デフォルトの信任状キャッシュの名前を取得できません。	System i プラットフォームにサインオンしたユーザーの /home ディレクトリー内にディレクトリーがあるかどうかを判別します。ユーザーのディレクトリーが存在しない場合は、信任状キャッシュのホーム・ディレクトリーを作成します。

表 37. Kerberos を使用できる i5/OS インターフェースに共通のエラー (続き)

問題	リカバリー
<p>CPD3E3F: ネットワーク認証サービス・エラー &2 が起きました。</p>	<p>このメッセージに対応する固有のリカバリー情報を参照してください。</p>
<p>既に接続された System i プラットフォーム上で DRDA/DDM 接続が失敗しました。</p>	<p>ネットワーク認証サービスの構成時に指定されたデフォルトのレルムが存在するかどうかを調べます。デフォルトのレルムおよび Kerberos サーバーが構成されていなければ、ネットワーク認証サービスの構成が誤っており、DRDA/DDM 接続が失敗します。このエラーからリカバリーするには、以下のいずれかのタスクを行います。</p> <ol style="list-style-type: none"> 1. Kerberos 認証を使用していない場合は、以下の手順に従ってください。 <p style="margin-left: 40px;">ネットワーク認証サービスの構成で指定したデフォルトのレルムを削除します。</p> 2. Kerberos 認証を使用している場合は、以下の手順に従ってください。 <ol style="list-style-type: none"> a. ステップ 1 で作成したデフォルトのレルムおよび Kerberos サーバーを指定して、ネットワーク認証サービスを再構成します。 b. Kerberos 認証を使用するように System i Access for Windows アプリケーションを構成する。これで、DRDA/DDM を含めてすべての System i Access for Windows アプリケーションに Kerberos 認証が設定されます。(59 ページの『シナリオ: i5/OS 用のシングル・サインオンを使用可能にする。』を参照してください。)

表 37. Kerberos を使用できる i5/OS インターフェースに共通のエラー (続き)

問題	リカバリー
<p>既に接続された System i プラットフォーム上で QFileSvr.400 接続が失敗しました。</p>	<p>ネットワーク認証サービスの構成時に指定されたデフォルトのレルムが存在するかどうかを調べます。デフォルトのレルムおよび Kerberos サーバーが構成されていないければ、ネットワーク認証サービスの構成が誤っており、QFileSvr.400 接続が失敗します。このエラーからリカバリーするには、以下のいずれかのタスクを行います。</p> <ol style="list-style-type: none"> 1. Kerberos 認証を使用していない場合は、以下の手順に従ってください。 <ul style="list-style-type: none"> ネットワーク認証サービスの構成で指定したデフォルトのレルムを削除します。 2. Kerberos 認証を使用している場合は、以下の手順に従ってください。 <ol style="list-style-type: none"> a. ネットワーク上のセキュア・システムでデフォルトのレルムおよび Kerberos サーバーを構成します。そのシステムに対応する資料を参照してください。 b. ステップ 1 で作成したデフォルトのレルムおよび Kerberos サーバーを指定して、ネットワーク認証サービスを再構成します。 c. Kerberos 認証を使用するように System i Access for Windows アプリケーションを構成する。これで、DRDA/DDM を含むすべての System i Access for Windows アプリケーションに Kerberos 認証が設定されます。(59 ページの『シナリオ: i5/OS 用のシングル・サインオンを使用可能にする。』を参照してください。)
<p>CWBSY1011: Kerberos クライアントの信任状が見つかりません。</p>	<p>ユーザーにチケット許可チケット (TGT) がありません。この接続エラーは、ユーザーが Windows 2000 ドメインにログインしていないときにクライアント PC で起こります。このエラーからリカバリーするには、Windows 2000 ドメインにログインしてください。</p>
<p>接続設定の検証時にエラーが起きました。URL のホストがありません。 注: このエラーは、エンタープライズ識別マッピング (EIM) の使用時に起こります。</p>	<p>このエラーからリカバリーするには、以下の手順に従ってください。</p> <ol style="list-style-type: none"> 1. System i ナビゲーターで、「システム」 → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」と展開する。 2. 「Directory」を右クリックして「プロパティ」を選択する。 3. 「一般」ページで、管理者の識別名とパスワードが EIM 構成時に入力したものと一致することを検証します。

表 37. Kerberos を使用できる i5/OS インターフェースに共通のエラー (続き)

問題	リカバリー
<p>ローカル・ディレクトリー・サーバーの構成の変更時にエラーが起きました。 GLD0232: 重複する接尾部を構成に入れることはできません。</p> <p>注: このエラーは、エンタープライズ識別マッピング (EIM) の使用時に起きます。</p>	<p>このエラーからリカバリーするには、以下の手順に従ってください。</p> <ol style="list-style-type: none"> 1. System i ナビゲーターで、「システム」 → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」と展開する。 2. 「Directory」を右クリックして「プロパティー」を選択する。 3. 「データベース/接尾部」ページで、ibm-eimDomainName エントリーを除去して EIM を再構成します。
<p>接続設定の検証時にエラーが起きました。 i5/OS プログラムの呼び出し中に例外が起きました。呼び出し先プログラムは <code>eimConnect</code> です。詳細は <code>com.ibm.as400.data.PcmlException</code> です。</p> <p>注: このエラーは、エンタープライズ識別マッピング (EIM) の使用時に起きます。</p>	<p>このエラーからリカバリーするには、以下の手順に従ってください。</p> <ol style="list-style-type: none"> 1. System i ナビゲーターで、「システム」 → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」と展開する。 2. 「Directory」を右クリックして「プロパティー」を選択する。 3. 「データベース/接尾部」ページで、ibm-eimDomainName エントリーを除去して EIM を再構成します。
<p>リモート・システムからの Kerberos チケットが認証できません。</p> <p>注: このエラーは、Kerberos 認証を使用するためにマネージメント・セントラル・システムを構成している時に起きます。</p>	<p>ご使用のシステムすべてにおいて、Kerberos が正しく構成されていることを検証します。このエラーはセキュリティー違反を示している可能性があります。要求を再試行してください。問題が解決しない場合には、お客様サポート担当員に連絡してください。</p>
<p>Kerberos サービス・チケットを検索できません。</p> <p>注: このエラーは、Kerberos 認証を使用するためにマネージメント・セントラル・システムを構成している時に起きます。</p>	<p>Kerberos プリンシパル「<code>krbsvr400/System i fully qualified host name@REALM</code>」が、Kerberos サーバーだけでなく各システムの keytab ファイルにもあることを検証します。Kerberos プリンシパルが Kerberos サーバーに入力されているかどうかを検証するには、110 ページの『Kerberos サーバーへの i5/OS プリンシパルの追加』を参照してください。Kerberos サービス・プリンシパル名が keytab ファイルに入力されているかどうかを検証するには、123 ページの『keytab ファイルの管理』で詳細を参照してください。</p>

表 37. Kerberos を使用できる i5/OS インターフェースに共通のエラー (続き)

問題	リカバリー
<p>Kerberos プリンシパルがトラステッド・グループにありません。</p> <p>注: このエラーは、Kerberos 認証を使用するためにマネージメント・セントラル・システムを構成している時に起こります。</p>	<p>このシステムに接続しようとしているシステム用の Kerberos プリンシパルを、トラステッド・グループ・ファイルに追加します。このエラーからリカバリーするには、以下の手順に従ってください。</p> <ol style="list-style-type: none"> 1. Kerberos 認証を使用するためにセントラル・システムを設定する。 2. システム値インベントリーを収集する。 3. 比較および更新を行う。 4. セントラル・システムおよび受動システム上でマネージメント・セントラル・サーバーを再始動する。 5. すべてのエンドポイント・システム用にトラステッド・グループ・ファイルに Kerberos サービス・プリンシパルを追加する。 6. 信頼された接続を可能にする。 7. セントラル・システムおよび受動システム上でマネージメント・セントラル・サーバーを再始動する。 8. マネージメント・セントラル・サーバー上で認証をテストする。

API トレース・ツール

Kerberos および Generic Security Service API 呼び出しの問題をトラブルシューティングするために、API トレース・ツールをセットアップすることができます。

ネットワーク認証サービスは、すべての Kerberos および Generic Security Service (GSS) API 呼び出しが含まれているファイルを管理者が作成できるようにするための API トレース・ツールを提供します。このツールにより、ユーザー自身の Kerberos-enabled を使用できるアプリケーションに関係するより高度なエラー、ネットワーク認証サービスの構成時に発生する可能性のあるエラー、および Kerberos チケット要求時に発生する可能性のあるエラーを、トラブルシューティングすることができます。環境変数を使用してこのツールを作成し、ログ・ファイルをユーザーのホーム・ディレクトリーに生成させることができます。

注: これらの手順を完了する前に、ホーム・ディレクトリーが存在している必要があります。

API トレース・ツールのセットアップ

API トレース・ツールをファイルに書き込むには、ネットワーク認証サービスが構成されている System i プラットフォームで、以下の手順を実行します。

API トレース・ツールをセットアップする手順は、次のとおりです。

1. ホーム・ディレクトリーで、トレース対象の `envar` ファイルを作成する。例えば、`/home/user_profile_name/envar` を指定できます。
2. 文字ベース・インターフェースで、`edtf /home/user_profile_name/envar` を使用してファイルを編集する。
3. 列 1 から始まるように注意して、次の行を `envar` ファイルに追加する。

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

4. 失敗したコマンドを再試行する。
5. `_EUV_SVC_STDOUT_FILENAME` によって参照されるトレースを表示する。

失敗したコマンドのトレースを完了した後、`envvar` ファイルを削除または名前変更してください。そうしないと、ユーザーが入力したすべての Kerberos コマンドがトレースされます。

API トレース・ログ・ファイルへのアクセス

API トレース・ツールをセットアップしたら、このログ・ファイルにアクセスしてトラブルシューティングを開始できます。

このログ・ファイルにアクセスするには、以下の手順を完了してください。

1. 文字ベース・インターフェースで、`wrklnk ('home/user profile')` と入力する。ここで `user profile` はユーザー・プロファイルの名前です。
2. 「オブジェクト・リンクの処理 (Work with Object Link)」ダイアログ・ボックスで、オプション 5 を選択し、ディレクトリーに保管されている `trace.txt` ファイルの内容を表示する。

次に示すのは、ログ・ファイルの例の一部です。

```
Browse : /home/day/trace.txt
Record :      1  of   5430 by 14          Column :      1  140 by 79
Control :

*****Beginning of data*****
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=Exit F10=Display Hex F12=Exit F15=Services F16=Repeat find
F19=Left F20=Right

API トレースで発生する特定のエラー・メッセージに関する情報については、`information center` 中の対応する API を参照してください。

関連情報

API ファインダー

Generic Security Service Application Programming Interfaces (GSS API)

ネットワーク認証サービス・アプリケーション・プログラミング・インターフェース (API)

i5/OS PASE での Kerberos サーバーのトラブルシューティング

i5/OS PASE で、Kerberos サーバーをトラブルシューティングするために、状況および情報のログ・ファイルにアクセスすることができます。

i5/OS PASE で Kerberos サーバーを構成する時に、認証サーバーと管理サーバーが作成されます。これらのサーバーは、`/var/krb5/log` ディレクトリーにあるログ・ファイルに、状況メッセージと通知メッセージを書き込みます。このログ・ファイル `krb5kdc.log` には、管理者が構成要求および認証要求に関する問題をトラブルシューティングする援助となるメッセージが入っています。

i5/OS PASE の中でユーザーが Kerberos サーバーを構成した System i プラットフォームから、Kerberos サーバーのログ・ファイルにアクセスする必要があります。ログ・ファイルにアクセスするには、以下の手順を実行してください。

1. 文字ベース・インターフェースで `QP2TERM` と入力する。このコマンドは、ユーザーが i5/OS PASE アプリケーションを処理できるようにする対話式シェル環境をオープンします。
2. コマンド行で `cd /var/krb5/log` と入力する。
3. コマンド行で `cat /krb5kdc.log` と入力する。これにより、i5/OS PASE KDC に関するエラー・メッセージが入っている `krb5kdc.log` ファイルをオープンします。

サンプルの `krb5kdc.log` ファイル

次のサンプル・ログには、いくつかのメッセージが入っています。

```
$
AS_REQ (3 etypes {16 3 1}) 10.1.1.2(88): NEEDED_PREAUTH:
jday@SYSTEMA.MYCO.COM for kadmin/changepw@SYSTEMA.MYCO.COM,
Additional pre-authentication required

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,
Additional pre-authentication required

Apr 30 14:18:56 systema.myco.com /usr/krb5/sbin/krb5kdc[334](info):
DISPATCH: replay found and re-transmitted
$
```

ネットワーク認証サービスのコマンド

以下のコマンドを使用して、ネットワーク認証サービスを構成し、使用することができます。

表 38. ネットワーク認証サービスのコマンド

コマンド	説明
<code>config.krb</code>	ネットワーク認証サービスのサーバーとクライアントを構成します。
<code>kadmin</code>	ネットワーク認証サービスのデータベースを管理します。
<code>kadmind_daemon</code>	ネットワーク認証サービスの管理サーバーを始動します。
<code>kdb5_util</code>	管理者がネットワーク認証サービスのデータベース上で低レベルの保守手順を実行することを許可します。
<code>kdestroy</code>	信任状キャッシュ (キー・テーブルとも呼ばれます) を破棄します。

表 38. ネットワーク認証サービスのコマンド (続き)

コマンド	説明
kinit	チケット許可チケットを取得または更新します。
klist	信任状キャッシュまたはキー・テーブルの内容を表示します。
kpasswd	プリンシパルのパスワードを変更します。
krb5kdc	ネットワーク認証サービスのマルチスレッド化された鍵配布センター (KDC) を始動します。
ksetup	LDAP ディレクトリー内にあるネットワーク認証サービス・レルムのネットワーク認証サービス・エントリーを管理します。
ksu	別のユーザー ID に切り替えます。
ktutil	管理者が keytab ファイル内のエントリーの読み取り、書き込み、または編集を行うことを許可します。
kvno	プリンシパルの現行キー・バージョン番号を表示します。
start.krb5	ネットワーク認証サービスのサーバーを始動します。
stop.krb5	ネットワーク認証サービスのサーバーを停止します。
unconfig.krb5	ネットワーク認証サービスのクライアントとサービスを構成解除します。

これらのコマンドについての詳細は、「*IBM Network Authentication Service AIX, Linux, and Solaris Administrator's and User's Guide*」を参照してください。

ネットワーク認証サービスの関連情報

製品資料、Web サイト、およびその他の Information Center トピック・コレクションには、ネットワーク認証サービスのトピック集に関連する情報が収められています。PDF ファイルは、いずれも表示または印刷することができます。

資料

AIX Expansion Pack CD をご注文になると、ネットワーク認証サービスの資料を利用することができます。これらの資料は AIX、Solaris、および Linux® オペレーティング・システム用に作成されていますが、i5/OS オペレーティング・システムでもネットワーク認証サービス・コマンドの多くを使用できます。ご使用の AIX システムにネットワーク認証サービス製品をインストールすると、資料は /usr/lpp/krb5/doc/pdf/en_US ディレクトリーにインストールされます。

さらに、システムに Network Authentication Enablement 製品 (5722-NAE または 5761-NAE) をインストールすると、/usr/lpp/krb5/doc/ ディレクトリーから同じ資料 (PDF と HTML の両方の形式) を利用できます。

- *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*

注: この資料は、AIX 5L Expansion Pack and Bonus Pack CD に収録されています。🌐

Web サイト

以下の Web サイトおよび情報は、特定のオペレーティング・システムを使用した Kerberos サーバーのセットアップについて、より詳細な情報を提供します。

- Windows 2000 サーバー 

- z/OS Security Server Network Authentication Service Administration 

その他の information center トピック

- ネットワーク認証サービス・アプリケーション・プログラミング・インターフェース (API)
- Generic Security Service Application Programming Interfaces (GSS API)
- エンタープライズ識別マッピング (EIM)
- シングル・サインオン

Request for Comments (RFC)

Requests for Comments (RFC) は、インターネットで使用されるプロトコル規格および提案された規格の定義を書面にしたものです。以下の RFC は、Kerberos プロトコルおよび関連機能を理解する援助となります。

RFC 1509

RFC 1509 の内容: Generic Security Service API : C-bindings。 Internet Engineering Task Force (IETF) が GSS API を正式に定義する。

RFC 1510


RFC 1510 の内容: Kerberos ネットワーク認証サービス (V5)、 Internet Engineering Task Force (IETF) が Kerberos V5 プロトコルを正式に定義する。

RFC 1964

RFC 1964 の内容: Kerberos バージョン 5 GSS-API メカニズム。 Internet Engineering Task Force (IETF) が Kerberos バージョン 5 および GSS API の仕様を定義する。

RFC 2743

RFC 2743 の内容: Generic Security Service Application Program Interface バージョン 2、アップデート 1、 Internet Engineering Task Force (IETF) が GSS API を正式に定義する。

上記の RFC を表示するには、RFC editor  Web サイトにある RFC index search engine を参照してください。表示したい RFC の番号で検索します。この検索エンジンの結果として、対応する RFC のタイトル、作成者、日付、および状況が表示されます。

関連資料

3 ページの『ネットワーク認証サービスの PDF ファイル』
本書の PDF ファイルを表示し、印刷することができます。

第 2 章 特別な条件

ここには、ネットワーク認証サービスに適用される特別な条件および商標が記載されています。

本書は米国 IBM が提供する製品およびサービスについて作成したものです。本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-8711
東京都港区六本木 3-2-12
IBM World Trade Asia Corporation
Intellectual Property Law & Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性があります。その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確認できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者をお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があります、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。

このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年).このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. _年を入れる_. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

以下の著作権表示および許可通知は、この情報のうち、Massachusetts Institute of Technology から取得した部分に適用されます。

Copyright © 1985-1999 by the Massachusetts Institute of Technology.

暗号を利用するソフトウェアをアメリカ合衆国から輸出するには、アメリカ合衆国政府からそのための許可を得なければならない場合があります。輸出する前にそのような許可を得ることは、輸出を企画している個人または組織の責任となります。

その制約の範囲内で、このソフトウェアおよびその関連文書を、目的の如何を問わず、無料で使用し、複製し、変更、配布することが許可されます。ただし、上記の著作権表示がすべての複製に表示され、かつその

著作権表示とこの許可通知とが関連文書に記載されている場合、および事前の書面による許可なしに M.I.T という名称をソフトウェアの配布時に広告または宣伝に使用しない場合に限り、さらに、このソフトウェアを変更した場合は、それが変更されたソフトウェアであることを表示しなければならず、オリジナルの MIT ソフトウェアと混同されかねないような方法で配布してはなりません。M.I.T. は、このソフトウェアの適合性については、いかなる目的においても責任を負いません。それは、明示的または黙示的な保証なしに、現存するままの状態を提供されます。

以下の著作権表示および許可通知は、`kadmin/create`、`kadmin/dbutil`、`kadmin/passwd`、`kadmin/server`、`lib/kadm5`、および `lib/rpc` の一部に置かれている OpenVision Kerberos Administration システムに適用されます。

Copyright, OpenVision Technologies, Inc., 1996, All Rights Reserved 警告: OpenVision Kerberos Administration システムのソース・コードを取り出した場合は、以下に示す条項に同意したと見なされます。その条項に同意しない場合は、OpenVision Kerberos Administration システムを取り出さないでください。このソース・コードおよびソース・コードからのコンパイルによって得られるオブジェクト・コードは、変更して使用することも、変更しないで使用することも自由です。ただし、このソース・コードは、商品性の保証、特定目的適合性の保証または法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任または保証条件の適用なしに、現存するままの状態を提供されます。OpenVision は、このソース・コードの使用によって生じるものであれ、このソース・コードの実行の失敗によって生じるものであれ、他のいかなる理由によるものであれ、逸失利益、データの喪失、代替の製品またはサービスの調達経費、またはこの合意事項から発生する特別、間接的、結果的損害について、これらに限られることなく、一切の責任を負いません。

OpenVision は、この寄贈されたソース・コードに関する一切の著作権を保持するものとします。OpenVision はさらに、OpenVision が作成したものであるか、第三者が作成したものであるかに拘らず、このソース・コードの派生物に関する著作権も保持するものとします。この寄贈されたソース・コードに基づく派生物を作成した場合は、OpenVision の著作権表示を記載する必要があります。OpenVision Technologies, Inc. は、この Kerberos Administration システムを標準の Kerberos 5 配布に含める目的で MIT に寄贈しました。この寄贈は、Kerberos テクノロジーのさらなる発展に対する弊社の約束と、MIT および Kerberos コミュニティーの業績に対する弊社の感謝の表れです。

Kerberos V5 には、University of California at Berkeley で開発されたソフトウェアと関連資料が含まれており、この著作権表示もその一部です。

Copyright © 1983 Regents of the University of California. All rights reserved.

ソースおよびバイナリー形式での再配布および使用は、変更の有無に拘らず、次の条件を満たす場合に許可されます。

1. ソース・コードを再配布する場合には、上記の著作権表示、この使用条件および以下の免責表示を含める必要があります。
2. バイナリー形式で再配布する場合には、上記の著作権表示、以下の使用条件および免責表示を、配布に際して提供する関連文書および資料に記載する必要があります。
3. このソフトウェアの機能および使用についての広告には、以下の表示を行う必要があります。

この製品には、カリフォルニア大学バークレー校およびその寄稿者が開発したソフトウェアが含まれています。

4. なお、カリフォルニア大学および寄稿者の名称は、事前の書面による承諾がある場合を除き、このソフトウェアをもとに開発した製品を保証または推奨する目的で使用することはできません。

このマニュアルと一語一語まったく同じ複製の作成および配布は、すべての複製に著作権表示とこの許可通知を記載する場合に限り許可されます。

このマニュアルの修正バージョンの複製および配布は、完全複製の場合と同じ条件の下で許可されます。ただし、その派生物全体が、これと同じ許可通知の条項の下で配布されることも条件となります。このマニュアルを別の言語に翻訳したものの複製および配布は、修正バージョンの場合と同じ条件の下で許可されません。

商標

以下は、IBM Corporation の商標です。

- AIX
- IBM
- Tivoli
- VisualAge

Kerberos は、Massachusetts Institute of Technology (MIT) の商標です。

Microsoft、Windows、Windows NT、および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

他の会社名、製品名およびサービス名などはそれぞれ各社の商標または登録商標です。

付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-8711
東京都港区六本木 3-2-12
IBM World Trade Asia Corporation
Intellectual Property Law & Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとしします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

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

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、IBM 機械コードのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性があります。その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確認できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者をお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があります、単に目標を示しているものです。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. _年を入れる_. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

プログラミング・インターフェース情報

このネットワーク認証サービスの資料には、プログラムを作成するユーザーが、IBM i5/OS のサービスを使用するためのプログラミング・インターフェースが記述されています。

商標

以下は、IBM Corporation の商標です。

AIX
AIX 5L
Distributed Relational Database Architecture
DRDA
i5/OS
IBM
IBM (ロゴ)
iSeries
NetServer
OS/400
Redbooks
System i
System p
System z
Tivoli
VisualAge
z/OS

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

他の会社名、製品名およびサービス名などはそれぞれ各社の商標または登録商標です。

使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態を提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。



Printed in Japan