IBM

eserver

iSeries

ネットワーク認証サービス

(英文原典：RZAK-H000-02)

IBM

@server

iSeries

ネットワーク認証サービス

(英文原典：RZAK-H000-02)

本マニュアルに関するご意見やご感想は、次の URL からお送りください。今後の参考にさせていただきます。

http://www.ibm.com/jp/manuals/main/mail.html

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

http://www.ibm.com/jp/manuals/ の「ご注文について」をご覧ください。

(URL は、変更になる場合があります)

原　典： RZAK–H000–02
iSeries
Network authentication service

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 2002.10

目次

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って、 iSeries および iSeries Access for Windows などのさまざまな iSeries サービスは、ユーザーの認証用のユーザー名およびパスワードの代わりに Kerberos チケットを使用することができます。 Massachusetts Institute of Technology が開発した Kerberos プロトコルは、プリンシパル (ユーザーまたはサービス) が保護されていない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します。プリンシパルの認証は、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。 KDC は、 Kerberos チケットを使用してユーザーを認証します。このチケットは、プリンシパルの ID をネットワーク内の他のサービスに対して証明します。プリンシパルがこのチケットによって認証されたら、ターゲット・サービスと暗号化されたデータを交換できます。ネットワーク認証サービスは、ネットワーク内のユーザーまたはサービスの ID を検証します。アプリケーションはユーザーを確実に認証し、ネットワーク上の他のサービスに対してそのユーザーの ID を確実に渡します。まずユーザーがシステムにとって既知であるかどうかを判別し、続いて別の機能を使ってネットワーク・リソースに対するユーザーの権限を検査します。 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
- RFC 1509、1964、2743 に定義された Generic Security Service (GSS) API

iSeries でのネットワーク認証サービスはこれらの RFC に準拠する認証、委任、データ保護のサービスに対応することを目指し、たとえば Microsoft の Windows 2000 Security Service Provider Interface (SSPI) API を組み込んでいます。

さらに、ネットワーク認証サービスは、エンタープライズ識別マッピング (EIM) で使用して、単一サインオン環境を可能にします。単一サインオンは、ユーザー、管理者、およびアプリケーション開発者が、基礎となるセキュリティー・ポリシーを変更することなく、複数のプラットフォーム間でより簡単なパスワード管理システムを使用できるようにします。以下の項目に、ネットワーク認証サービスおよびエンタープライズ識別マッピング (EIM) を使用した単一サインオンの使用可能性に関する詳細を示します。

単一サインオンの使用可能性
この項目は、単一サインオンの利点に関する概念、およびネットワーク認証サービスとエンタープライズ識別マッピング (EIM) が相互に作用して単一サインオン環境を形成する方法の概要を示します。

シナリオ: 単一サインオンの使用可能性
この項目は、自社の受注部門の管理者が単一サインオン環境を使用可能にする方法の例を示します。管理者は、Windows (R) ドメイン ID およびパスワードを使用して、ユーザーを iSeries アプリケーションに対して認証させたいとします。また、自社の管理者が単一サインオンを使用可能にするようにネットワーク認証サービスと EIM を構成する方法を示す段階的な説明も記します。

ここではネットワーク認証サービスに関して以下のトピックを説明します。

V5R2 の新機能
このトピックは、今回のリリースでのネットワーク認証サービスの新機能に関する詳細情報について説明し、各情報へリンクします。

トピックの印刷
このトピックは、この情報の PDF バージョンをダウンロードして印刷する手順を記載します。

ネットワーク認証サービスの処理方法
このトピックは、ネットワーク認証サービスが、Kerberos プロトコルを使用してユーザーを認証するネットワーク内での処理方法に関する概要を記載します。

ネットワーク認証サービスの用語
このトピックは、ネットワーク認証サービスに関連する用語を定義します。

ネットワーク認証サービスのプロトコル
このトピックは、Kerberos プロトコルおよび Generic Security Services (GSS) API の基本的な説明を記載します。 RFC およびその他の関連情報へのリンクを示します。

ネットワーク認証サービスのシナリオ
このトピックは、ネットワーク認証サービスをインプリメントした業務のシナリオをいくつか記載します。

ネットワーク認証サービスを計画する
このトピックは、ネットワーク認証サービスで作業する前に行う必要があることについて記載します。

ネットワーク認証サービスを構成する
このトピックは、iSeries ナビゲーターでネットワーク認証サービスを構成する方法を記載します。

ネットワーク認証サービスを管理する
このトピックは、管理者およびユーザーがネットワーク認証サービスの管理に使用できるタスクを記載します。

ネットワーク認証サービスのトラブルシューティング
このトピックは、ネットワーク認証サービスおよび関連アプリケーションのメッセージおよび問題解決を記載します。

関連情報
このトピックは、Kerberos プロトコルおよび Generic Security Services (GSS) API に関するその他のトピックについて説明し、そのトピックへのリンクを示します。

リーガル情報
このトピックは、Kerberos プロトコルおよびそれに関連する API を使用する際の重要なリーガル情報を記載します。

V5R2 の新機能

» ネットワーク認証サービスは、 iSeries が、Kerberos プロトコルを使用するネットワークに参加して、ネットワーク上のユーザーを認証できるようにします。

iSeries ナビゲーターでのネットワーク認証サービス
ネットワーク認証サービス・ウィザードでは、 Kerberos ネットワークに参加するように iSeries を簡単に構成できます。このウィザードにより、Kerberos レルムに参加するように iSeries を構成できます。 Kerberos プロトコルを使用することで、ユーザーのためにチケットがサービスに渡されて、ネットワーク上のリソースに対してユーザーを認証できるようにします。以下のトピックを参照して、構成を完成させてください。

- ネットワーク認証サービスのシナリオ
  ネットワーク認証サービスを使用する 2 人の顧客の場合の概要について説明します。
-
- ネットワーク認証サービスを構成する
  ネットワーク認証サービスを構成するのに必要なすべてのステップの概要について説明します。
-
- ネットワーク認証サービスを管理する
  iSeries ナビゲーターを使用して完成させられるすべてのタスクの概要について説明します。

新規 Qshell コマンドをサポートする
ユーザーは、Qshell コマンドによってチケットを要求して処理できます。今回のリリースでは、**kpasswd** コマンドが追加され、ユーザーが鍵配布センター上のパスワードを変更できるようになりました。

- Kerberos パスワードを変更する
  kpasswd Qshell コマンドを使用する方法について説明します。

エンタープライズ識別マッピング (EIM)
エンタープライズ識別マッピング (EIM) は、人またはエンティティー (サービスなど) をエンタープライズ全体のさまざまなユーザー・レジストリー内の適切なユーザー ID にマッピングするメカニズムです。ネットワーク認証サービスで使用するときに、EIM では単一サインオン環境が使用可能です。 iSeries は、EIM を使用して iSeries インターフェースを使用可能にし、ネットワーク認証サービスを通じてユーザーを認証します。 iSeries およびアプリケーションは、 Kerberos チケットを受け入れて EIM を使用し、あるシステム上のユーザー ID を関連する Kerberos プリンシパルにマッピングできます。

- 単一サインオンの使用可能性
  単一サインオンの利点に関する概念、およびネットワーク認証サービスとエンタープライズ識別マッピング (EIM) が相互に作用して単一サインオン環境を形成する方法の概要を示します。
- シナリオ: 単一サインオンを使用可能にする
  ネットワーク認証サービスと EIM を一緒に使用して単一サインオン環境を可能にする場合の詳細な例を記載します。

数種の iSeries アプリケーションへの認証サポート

- **構造化照会言語 (SQL)/ 分散リレーショナル・データベース・アーキテクチャー (DRDA)**
  SQL/DRDA は、データベース機能にアクセスするユーザーを認証する Kerberos チケットの使用を

サポートするようになりました。DRDA は、特定のユーザーのチケット認可チケットがあるかどうかを検査します。チケットが存在する場合には、そのチケットはユーザーのサービス・チケットの取得に使用されます。

-
- **分散データ管理 (DDM)**
  DDM は、リモート・ファイルにアクセスするユーザーを認証する Kerberos チケットの使用をサポートするようになりました。 DDM は、特定のユーザーのチケット認可チケットがあるかどうかを検査します。チケットが存在する場合には、そのチケットはユーザーのサービス・チケットの取得に使用されます。**注:** Kerberos 構成ファイルにデフォルトのレルムが指定されているが、認証方式として Kerberos を使用していない場合には、 DDM に認証をセットアップする前にデフォルトのレルムを除去する必要があります。この問題の回復については、アプリケーション接続の問題および回復を参照してください。
-
- **iSeries Access for Windows および iSeries ホスト・サーバー**
  iSeries Access for Windows および iSeries ホスト・サーバーは、 Kerberos チケットを使用した認証をサポートします。クライアントから、ユーザーは、iSeries Access ホスト・サーバーにアクセスする際に Kerberos チケットを使用するように指定できます。
-
- **iSeries NetServer**
  iSeries NetServer クライアントは、ネットワーク内で Kerberos を構成してある場合に、 Kerberos チケットを使用してサーバーによる認証を可能にします。 Kerberos v5 をサポートするクライアントのみが、このサポートを使用可能にしたときに iSeries NetServer へ接続できます。 Kerberos の iSeries NetServer サポートの要件について詳しくは、 Kerberos v5 認証の iSeries NetServer サポートを参照してください。
-
- **QFileSvr.400**
  QFileSvr.400 は、現行ユーザーにチケット認可チケットがあるかどうかを判別します。チケット認可チケットがある場合には、ターゲット・システム上のユーザーを認証するためのサーバー・チケットが作成されます。チケットがない場合、現行のパスワード置換方式が使用されます。**注:** Kerberos 構成ファイルにデフォルトのレルムが指定されているが、認証方式として Kerberos を使用していない場合には、 QFileSvr.400 に認証をセットアップする前にデフォルトのレルムを除去する必要があります。この問題の回復については、アプリケーション接続の問題および回復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、以下の情報を使用します。

- » 新しい情報や変更された情報の開始を示す形
- « 新しい情報や変更された情報の終了を示す形

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検索するには、 ユーザーへのメモ

 を参照してください。

«

トピックの印刷

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 (199 KB または 57 ページ) を選択してください。

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. ブラウザーで PDF を開きます (上のリンクをクリックします)。
2. ブラウザーのメニューで「**ファイル**」をクリックします。
3. 「**リンクを名前を付けて保存**」(Netscape Navigator) または「**対象をファイルに保存**」(Internet Explorer) を選択します。
4. PDF の保管先となるディレクトリーを指定します。
5. 「**保存**」をクリックします。

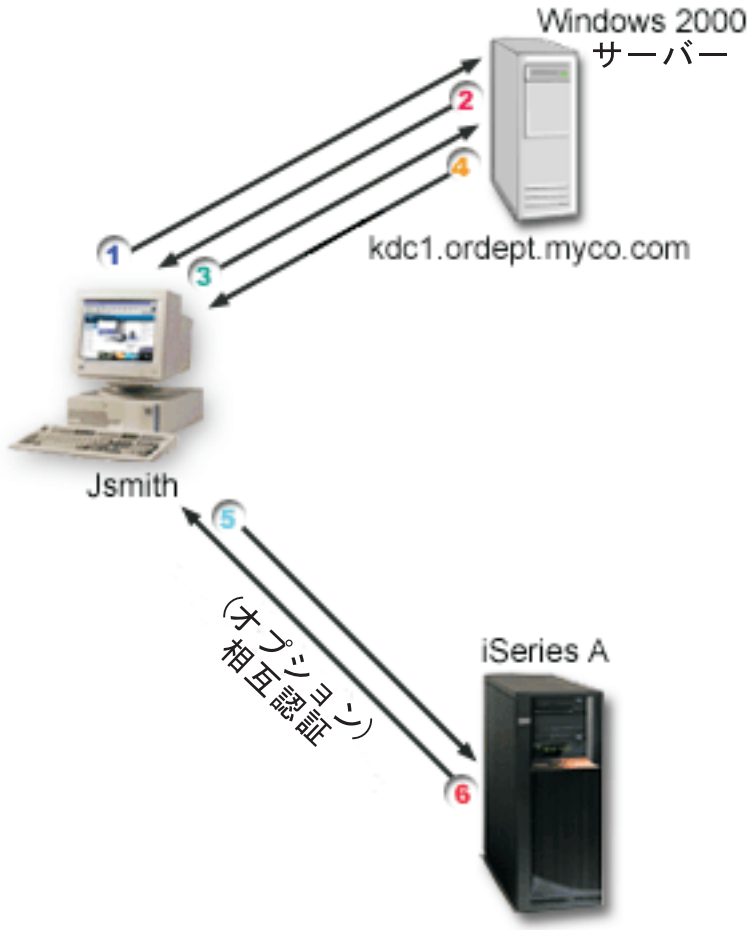
PDF の表示または印刷のために Adobe Acrobat Reader が必要な場合は、 Adobe Web サイト (www.adobe.com/product/acrobat/readstep.html) からコピーをダウンロードできます。

ネットワーク認証サービスの処理方法

ネットワーク管理者として、ネットワーク認証サービスを構成して、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保守する中央の鍵配布センター (KDC) で作成された Kerberos チケットを iSeries システムが受け入れるようにできます。 iSeries およびいくつかの iSeries 固有のアプリケーションは、 Kerberos ネットワーク内で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 / サーバーとして動作します。ユーザーが KDC からチケットを要求すると、ユーザーにはチケット認可チケット (TGT) と呼ばれる初期チケットが発行されます。そこで、ユーザーは、TGT を使用してサービス・チケットを要求することで、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できます。認証が正常に機能できるように、管理者はユーザー、iSeries サービス・プリンシパル、および KDC で Kerberos プロトコルを使用するアプリケーションを登録する必要があります。 iSeries は、プリンシパルがサービスへの認証を要求するサーバーとして動作するか、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動作することができます。次の図に、両方の状態でのチケットの流れを示します。

サーバーとしての iSeries

この図は、iSeries が Kerberos ネットワーク内でサーバーとして動作するときの認証方法を示しています。この図では、Windows (R) 2000 KDC はプリンシパル Jsmith にチケットを発行します。 Jsmith は、iSeries-A 上のアプリケーションにアクセスします。この場合、エンタープライズ識別マッピング (EIM) をサーバー上で使用して、Kerberos プリンシパルを iSeries ユーザー・プロファイルへマッピングします。これは、iSeries Access for Windows のような Kerberos が使用可能な iSeries サーバー機能で行われます。



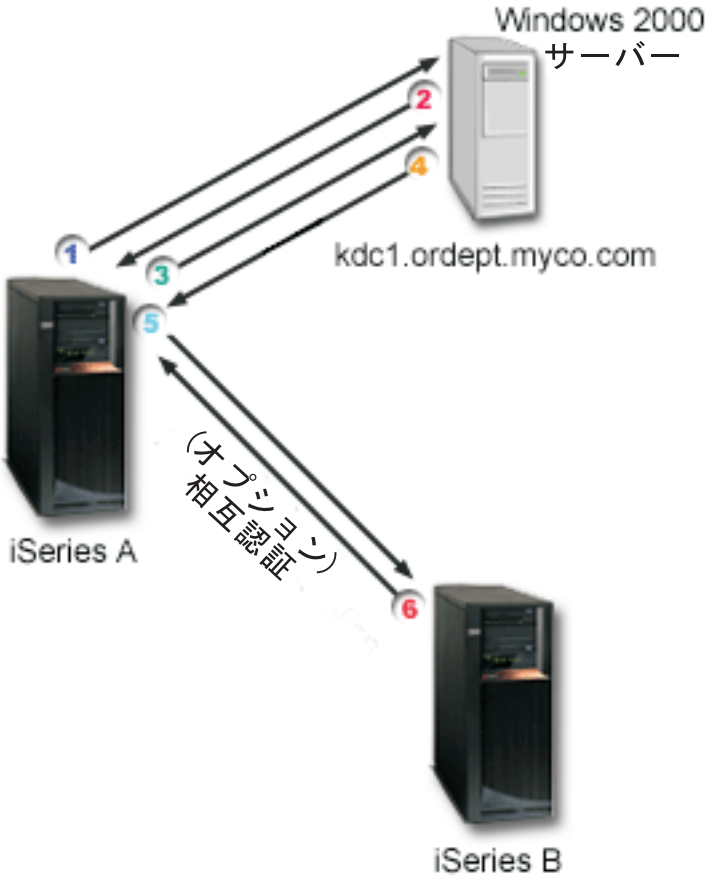
この説明では、ネットワーク内での認証処理方法の概要を記載します。

1. ユーザー Jsmith は、Kerberos ネットワークにサインインするときに KDC からチケットを要求します。これは、KDC へチケット認可チケットの要求を送信します。
2. KDC は、ユーザーのプリンシパル名およびパスワードの妥当性検査を行い、チケット認可チケットを Jsmith へ送信します。
3. Jsmith は、iSeries サーバー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 を呼び出すと、アプリケーションは Jsmith の TGT を KDC 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格納されます。このため、アプリケーションは自分で信任状を管理しなくてすみます。
4. KDC はサービス・チケットを付けて応答します。
5. アプリケーションは、サーバーのチケットを iSeries 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妥当性検査し、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すことができます。

クライアントとしての iSeries

この図は、iSeries が Kerberos ネットワーク内でクライアントとして動作するときの認証方法を示しています。この図では、Windows (R) 2000 KDC は iSeries-A プリンシパルにチケットを発行します。 iSeries-A

は他のサービスに対して認証できます。この例では、EIM を iSeries B 上で使用して、 Kerberos プリンシパルを iSeries ユーザー・プロファイルへマッピングします。これは、QFileSvr.400 のような Kerberos が使用可能な iSeries サーバー機能で行われます。



この説明では、ネットワーク内での認証処理方法の概要を記載します。

1. プリンシパル Jsmith は iSeries-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認可チケットを要求します。 iSeries は、KDC へこの要求を送信します。
2. KDC は、ユーザーのプリンシパル名およびパスワードの妥当性検査を行い、チケット認可チケットを Jsmith へ送信します。
3. Jsmith は、iSeries サーバー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 を呼び出すと、アプリケーションは Jsmith の TGT を KDC 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格納されます。このため、アプリケーションは自分で信任状を管理しなくてすみます。
4. KDC はサービス・チケットを付けて応答します。**注:** iSeries-B のサービス・プリンシパルを KDC に追加して、ネットワーク認証サービスも iSeries-B に構成する必要があります。
5. アプリケーションは、サーバーのチケットを iSeries 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妥当性検査し、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すことができます。

ネットワーク認証サービスの用語

ネットワーク認証サービスは、以下の Kerberos プロトコルの用語を使用します。

転送可能チケット
転送可能チケットは、サーバーが要求元の信任状を別のサービスへ渡すことができるようにします。これを行うために、初期 TGT に転送可能オプションを付けて要求し、サーバーが信任状を委任できるようにする必要があります。

鍵配布センター (KDC)
チケットと一時的なセッション・キーを提供するネットワーク・サービス。 KDC はプリンシパル（ユーザーとサービス）のデータベースとプリンシパルに関連付けられた機密鍵を維持管理します。KDC は認証サーバーとチケット認可チケット・サーバーから構成されます。 KDC として動作するには、保護マシンを使用することが重要になります。だれかが KDC へのアクセスを取得すると、レルム全体の暗号が漏えいする可能性があります。**注:** KDC は、iSeries システム上ではサポートされません。

キー・テーブル
サービスのホスト・システム上にあるファイル。ファイルの各エントリーには、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。 iSeries では、キー・テーブル・ファイルは、ネットワーク認証サービスの構成時に作成されます。サービスがネットワーク認証サービスを構成して iSeries への認証を要求すると、その iSeries 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を適切に認証させるには、ユーザーおよびサービスを KDC および iSeries に登録する必要があります。

パスワード・サーバー
クライアントがパスワードを KDC のリモート側で変更できるようにします。パスワード・サーバーは、一般的に KDC と同じマシンで稼働します。

プリンシパル
Kerberos ネットワーク内のユーザーまたはサービスの名前。ユーザーとは、サービスを使用して特定のアプリケーションまたはオペレーティング・システムのサービス・セットを識別する人を指します。 iSeries では、iSeries に対してクライアントから認証するときに、 **krbsvr400** サービスのプリンシパルを使用して iSeries 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します。

プロキシー可能チケット
プロキシー可能チケットは、チケット認可チケット (TGT) にあるもの以外の IP アドレス付きでサービスのチケットを取得できるようにする TGT です。転送可能チケットと異なり、新しい TGT は現行の TGT からプロキシーできません。プロキシーできるのはサービス・チケットのみです。転送可

能チケットでは、完全な識別 (TGT) を別のマシンに転送できます。プロキシー可能チケットは、特定のチケットのみを転送できます。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、元のチケット認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・アドレスに発行できることを KDC 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。

レルム
所定の鍵配布センター (KDC) の認証権限の対象となるユーザーとサーバーの集合。

レルム承認
Kerberos プロトコルは、構成ファイルを検索してレルム承認を判別するか、デフォルトによりレルム階層内の承認関係を検索します。ネットワーク認証サービス内で**承認レルム**を使用すれば、この処理をう回して認証へのショートカットを作成できるようになります。レルム承認は、レルムが異なるドメインにあるネットワーク内で使用できます。たとえば、ある企業で 1 つのレルムが NY.myco.com にあり、別のレルムが LA.myco.com にある場合に、この 2 レルムの間に承認を設定できます。2 つのレルムがお互いを承認すると、それらに関連付けられた KDC はキーを共用する必要があります。ショートカットを作成する前に、お互いを承認するように KDC をセットアップしなければなりません。

更新可能チケット
場合によっては、アプリケーションまたはサービスでチケットの有効期間を延長したいことがあります。しかし、期間を延長すると、チケットの期限内は有効である信任状が盗まれる可能性があります。交信可能チケットによって、アプリケーションは、盗まれる機会を少なくしながら延長期間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ンスタンスに適用され、 2 番目の有効期限はチケットの最新の許可期限に適用されます。

サービス・チケット
サービスに対してプリンシパルを認証するチケット。

チケット認可サービス (TGS)
サービス・チケットを発行する、KDC が提供するサービス。

チケット認可チケット (TGT)
KDC 上のチケット認可サービスへのアクセスを可能にするチケット。チケット認可チケットは、プリンシパルが正常に要求を完了した後で、KDC によってプリンシパルに渡されます。 Windows (R) 2000 環境では、ユーザーはネットワークにログオンし、 KDC はプリンシパルの名前および暗号化されたパスワードを検査してから、チケット認可チケットをユーザーに送信します。iSeries サーバーから、ユーザーは、文字ベース・インターフェースの Qshell インタープリター内で kinit コマンドを使用してチケットを要求できます。

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。以下のセクションでは、これらのプロトコルの概要および iSeries での使用方法について説明します。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 および他の外部情報源へのリンクを提供しています。

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発行する鍵配布センター (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。このチケットによって、異なるシステムに複数回サインオンしなくて済みます。 iSeries がサポートする Kerberos API は、マサチューセッツ工科大学 (MIT) が考案し、Kerberos プロトコルを使用するためのデファクト・スタンダードになっています。

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。侵入者は Kerberos プロトコルの一定の場所を利用して、アプリケーションが適切な認証ステップに実行できないようにすることができます。こうしたアタックを検出して防御する作業は、管理者とユーザーに任せられます。
- キーの共有や盗用を通じて、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み、該当のユーザーまたはサービスになりすます可能性があります。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有することを禁止し、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解読を防御できません。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行い成功する可能性があります。

Kerberos プロトコルの詳細については、以下の情報源を参照してください。

Kerberos ネットワーク認証サービス (V5) 。
Internet Engineering Task Force (IETF) は、Kerberos プロトコルを Request for Comment 1510 で正式に定義しています。

Kerberos: ネットワーク認証プロトコル (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記載しており、プロトコルの機能について説明しています。

ネットワーク認証サービスアプリケーション・プログラマブル・インターフェース (API)

この Information Center のトピックは、ネットワーク認証サービス API のリストと、その機能の概説を記載します。

Generic Security Service (GSS) API

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や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。この交信では、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 を確認します。
- 別のアプリケーションにアクセス権限を委任します。
- 機密保持や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します。

GSS API の詳細については、以下の情報源を参照してください。

Generic Security Service Application Program Interface Version 2, Update 1 。
Internet Engineering Task Force (IETF) は、GSS API を RFC 2743 で正式に定義しています。

Generic Security Service API : C-bindings 。
Internet Engineering Task Force (IETF) は、GSS API C-bindings を RFC 1509 で指定しています。

Kerberos バージョン 5 GSS-API メカニズム 。
Internet Engineering Task Force (IETF) は、Kerberos バージョン 5 および GSS API の仕様をこの RFC 1964 で定義しています。

Generic Security Service Application Programmable Interfaces (GSS API)
この Information Center のトピックは、GSS API のリストと、その機能の概説を記載します。

ネットワーク認証サービスのシナリオ

以下のシナリオは、ネットワーク認証サービスを使用して iSeries が Kerberos ネットワークに参加できる一般的な環境について説明します。以下のシナリオを参照して、ネットワーク認証サービスの構成に関する技術的な詳細および構成の詳細を確認しておいてください。

シナリオ : 既存の KDC によりネットワーク認証サービスを構成する
このトピックは、管理者が、鍵配布センターがインストールおよび構成されている Windows (R) 2000 環境にネットワーク認証を構成するお客様の場合について説明します。

シナリオ : 単一サインオンを使用可能にする
このシナリオは、エンタープライズ識別マッピング (EIM) でネットワーク認証サービスを使用して、単一サインオンを使用可能にする方法を示します。管理者は、ユーザーが Windows (R) 2000 サインオンを使用して、 iSeries システムおよび iSeries Access for Windows アプリケーションに対して認証できるようにします。

シナリオ : 既存の KDC によりネットワーク認証サービスを構成する

状態

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 iSeries を導入して、いくつかの必須アプリケーションを自分の部門に配置しました。現在、レルムの鍵配布センター (KDC) として動作する Windows (R) 2000 サーバーがあります。このネットワーク内のすべてのユーザーのプリンシパル名およびパスワードが KDC に格納されています。 iSeries を KDC に追加したいとします。iSeries をこのレルムに追加して、引き続き Windows (R) 2000 サーバーを認証サーバーとして使用しようと計画しています。 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します。
- ネットワーク内のサーバーへのアクセス管理のオーバーヘッドを減らします。
- パスワードが盗まれる危険性を最小に抑えます。

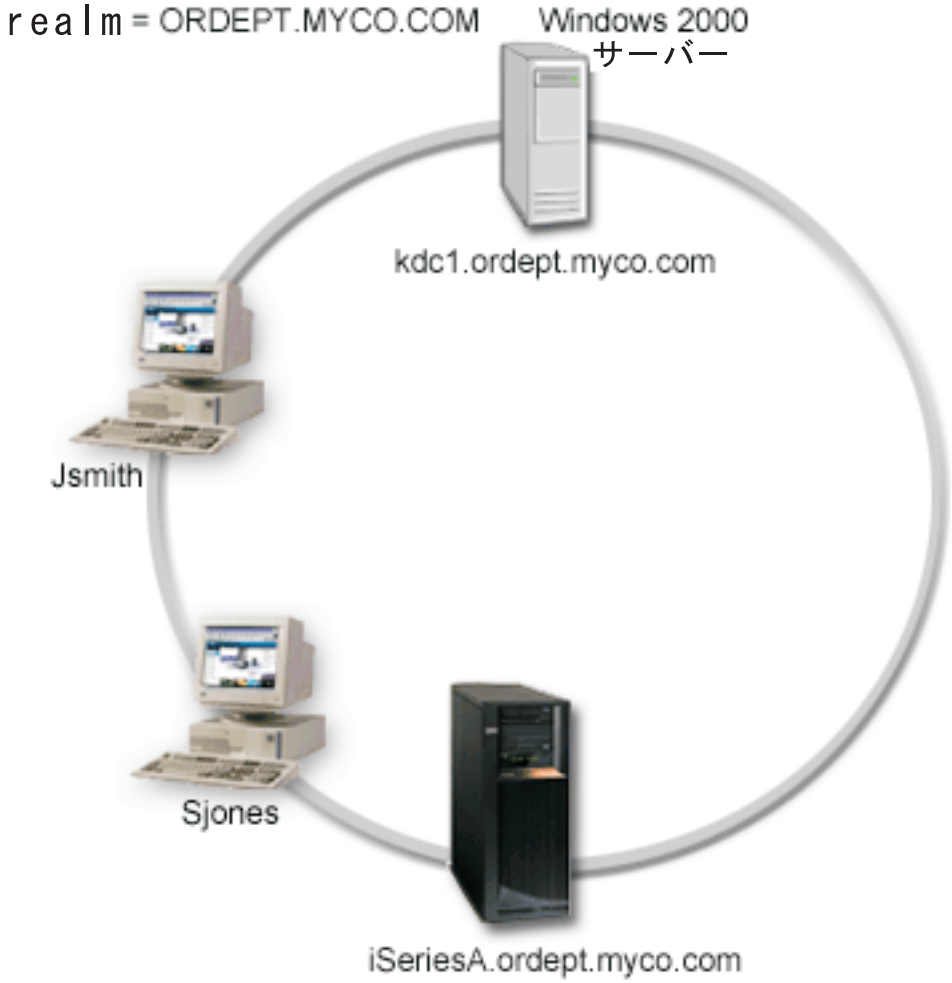
目的

このシナリオでは、MyCo, Inc. は、 Windows (R) 2000 サーバーが鍵配布センターとして動作する既存のレルムに iSeries システムを追加します。 iSeries には、適切なユーザーによってアクセスされるべきビジネスに欠くことのできないアプリケーションがいくつか含まれます。 KDC によって認証されるべきユーザーは、これらのアプリケーションへのアクセス権を取得する必要があります。 iSeries は、Windows (R) 2000 サーバーの KDC に追加する必要があります。

このシナリオの目的は、次のようになります。
- iSeries が既存の鍵配布センターによって参加できるようにします。
- 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します。
- Kerberos ユーザーが KDC 上の自分のパスワードを変更できるようにします。

シナリオの詳細

次の図は、MyCo ネットワークの特性を示します。



受注部門

- iSeries-A は、OS/400 バージョン 5 リリース 2 (V5R2) で稼働し、いくつかのビジネス・アプリケーションが入っています。
- KDC の DNS 名は kdc1.ordept.myco.com です。
- iSeries-A のプリンシパル名は krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM です。
- KDC のデフォルト・レルムは ORDEPT.MYCO.COM です。
- クライアント PC は Windows (R) 2000 を稼働します。

このシナリオの構成ステップ

1. ネットワーク認証サービスの計画ワークシートおよびチェックリストを完成 (14 ページを参照)させます。
2. iSeries-A でネットワーク認証サービスを構成 (15 ページを参照)します。
3. iSeries-A を KDC に追加 (16 ページを参照)します。

4. iSeries-A 上に各ユーザーのホーム・ディレクトリーを作成 (16 ページを参照)します。

5. 検査 (17 ページを参照) iSeries-A の TCP/IP ドメイン情報
6. iSeries-A でネットワーク認証サービスの構成をテスト (17 ページを参照)します。

構成の詳細

ステップ 1: 計画ワークシートの完成

以下の計画チェックリストは、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種類の情報を示しています。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、前提条件チェックリストのすべてに「はい」と回答する必要があります。

前提条件チェックリスト	回答
OS/400 V5R2 (5722-SS1) 以降か ?	はい
Cryptographic Access Provider (5722-AC3) が iSeries システムにインストールされているか ?	はい
iSeries Access for Windows (5722-XE1) がネットワーク内のすべての PC および iSeries システムにインストールされているか ?	はい
iSeries ナビゲーターのセキュリティー・サブコンポーネントがネットワーク内のすべての PC および iSeries システムにインストールされているか ?	はい
iSeries ナビゲーターのネットワーク・サブコンポーネントがネットワーク内のすべての PC および iSeries システムにインストールされているか ?	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、鍵配布センターとして動作するセキュア・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 (R) 2000 サーバー 2. Windows (R) XP サーバー 3. AIX サーバー 4. zSeries	はい Windows (R) 2000 サーバー
Windows (R) 2000 サーバーおよび Windows (R) XP サーバーの場合、ktpass ツールを装備する Windows (R) サポート・ツールが、鍵配布センターとして使用されるシステム上にインストールしてあるか ?	はい
ネットワーク内のすべての PC が Windows (R) 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
iSeries システム時刻と KDC のシステム時刻との差が 5 分以内か ? 超えている場合は、システム時刻を同期するを参照。	はい

ネットワーク認証サービスの構成には、以下の情報が必要	回答
iSeries-A が所属する Kerberos のデフォルト・レルムの名前は ?	ORDEPT.MYCO.COM

ネットワーク認証サービスの構成には、以下の情報が必要	回答
Kerberos デフォルト・レルムの KDC は ? KDC が listen するポートは ?	kdc1.ordept.myco.com 88 (**注 :** これは、KDC 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・サーバーを構成するか ? 構成する場合は、以下の質問に回答してください。 この KDC 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 kdc1.ordept.myco.com 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。)
iSeries サービス・プリンシパルのパスワードは ?	iseriesa123 **注 :** このシナリオ内で使用される任意およびすべてのパスワードは例として使用しているだけです。実際の構成には使用しないでください。
iSeries システムはほかにどのようなレルムと対話するか?	該当なし
各レルムについて、鍵配布センターのホスト名は ?	該当なし

ステップ 2: iSeries-A でのネットワーク認証サービスの構成

ワークシートからの情報を使用して、 、以下のように iSeries-A 上でネットワーク認証サービスを構成します。

1. iSeries ナビゲーターで、「**iSeries-A**」 **->「セキュリティー」**を展開します。
2. 「**ネットワーク認証サービス**」を右マウス・ボタン・クリックし、「**構成**」を選択して構成ウィザードを開始します。**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ついては、「**ウェルカム**」ページを参照してください。「**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 ORDEPT.MYCO.COM を入力します。「**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 kdc1.ordept.myco.com 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**」を選択します。「**パスワード・サーバー**」フィールドに kdc1.ordept.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 エントリーの作成 (Create keytab entry)**」ページで、「**iSeries Kerberos 認証**」を選択します。「**次へ**」をクリックします。
8. 「**iSeries keytab エントリーの作成 (Create iSeries keytab entry)**」ページで、 iSeries-A のキータブおよびプリンシパルを書き込みます。この KDC への追加には、プリンシパル名が必要です。パス

ワードを入力して確認します。たとえば、MyCo の管理者の場合、 iseriesa123 と入力します。**注 :** このシナリオ内で使用される任意およびすべてのパスワードは例として使用しているだけです。実際の構成には使用しないでください。

9. 「**次へ**」をクリックします。
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確認します。「**終了**」をクリックします。

これで、iSeries-A でのネットワーク認証サービスの構成が終わりました。次のステップは、 KDC へのプリンシパル名の追加です。

ステップ 3: KDC への iSeries-A プリンシパル名の追加

iSeries システムを Windows (R) 2000 KDC へ追加するには、 KDC へ追加するプリンシパルに対応した文書を使用します。規則では、 iSeries システム名をユーザー名として使用できます。以下のプリンシパル名を KDC に追加します。

```
krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM
```

Windows (R) 2000 サーバーでは、以下のステップを実行します。

1. Active Directory (R) の管理ツールを使って、 iSeries システム用のユーザー・アカウントを作成します (「**ユーザー**」フォルダーを選択して右マウス・ボタン・クリックし、「**新規作成**」を選択してから、「**ユーザー**」を選択します。) iSeriesA を Active Directory ユーザーとして指定します。
2. Active Directory ユーザー iSeriesA でプロパティーにアクセスします。「**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。これにより、iSeries-A サービス・プリンシパルはサインイン・ユーザーの代わりに他のサービスにアクセスできます。
3. **ktpass** コマンドを使い、ユーザー・アカウントをプリンシパルにマップします。 ktpass ツールは、Windows (R) 2000 サーバーのインストール CD の「**サービス・ツール**」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、次のように入力します。

   ```
   ktpass -princ krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM
   -mapuser iSeriesA -pass iseriesa123
   ```

   ここで iseriesa123 は、ネットワーク認証サービスを構成 (15 ページを参照)したときに指定したパスワードです。**注 :** このシナリオ内で使用される任意およびすべてのパスワードは例として使用しているだけです。実際の構成には使用しないでください。

ステップ 4: iSeries-A でのユーザーのホーム・ディレクトリーの作成

iSeries および iSeries 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、以下の処理を完了してください。

1. iSeries コマンド行で、次のように入力します。

   ```
   CRTDIR '/home/username'
   ```

   ここで username はユーザーの iSeries ユーザー名です。

たとえば、MyCo の管理者の場合、次のように入力します。
CRTDIR '/home/Johns' (ユーザー John Smith の場合。)
2. すべてのユーザーについて上記のステップを繰り返します。

ステップ 5: iSeries-A の TCP/IP ドメイン情報の検査

1. iSeries コマンド行で、次のように入力します。

   CFGTCP
2. オプション 10 を選択します。(TCP/IP ホスト・テーブル エントリーの作業。)
3. ホスト名フィールドで、iSeries-A の完全修飾ホスト名が小文字であることを検査します。さらに、複数のホスト名エントリーがある場合、完全修飾ホスト名が最初に表示されることを検査します。たとえば、iSeries A にはホスト名エントリー: iseriesa.ordept.myco.com.があります。
4. ホスト名エントリーを検査したら、F3 を押して「TCP メインメニューの構成(Configure TCP main menu)」に戻ります。
5. オプション 12を選択します。(TCP/IP ドメイン情報の変更。)
6. システム名がホスト名フィールドに表示されることを検査します。さらに、ドメイン名が正しいことを検査します。たとえば、ホスト名が、iseriesa であり、ドメイン名は、ordept.myco.com です。

ステップ 6: iSeries-A のネットワーク認証サービスのテスト

この時点で、iSeries-A プリンシパル名のチケット認可チケットを要求することで、ネットワーク認証サービスが正常に構成されたかどうかを検査できます。

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します。
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します。このシナリオでは、 krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM が iSeries-A のプリンシパル名として表示されます。**注 :** LDAP および iSeries NetServer のプリンシパルを構成するように選択した場合、 keytab ファイルには別のエントリーが入っています。このシナリオでは、管理者はこれらのサービスにプリンシパルを構成しないように選択しています。
3. kinit -k krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM と入力します。これが成功すると、QSH コマンドはエラーなしで表示されます。
4. klist と入力し、デフォルト・プリンシパルが krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM であるかどうかを検査します。

シナリオ : 単一サインオンを使用可能にする

状態

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。現在、貴社のユーザーは Windows (R) 2000 デスクトップを所有しています。 Windows ID およびパスワードと、その iSeries ユーザー名を管理する必要があります。 iSeries 認証に Windows (R) 2000 サインオンを使用できるようにしたいとします。これらのソリューションが示すセキュリティー上の問題のために、 Windows (R) 2000 ID と

iSeries ユーザー名を違うものにし、かつ、パスワードのキャッシュおよび同期化はしたくないものとします。サーバー上でネットワーク認証サービスおよびエンタープライズ識別マッピング (EIM) を構成することで、 iSeries サーバーで単一サインオンを使用できることが分かっています。ネットワーク認証サービスによって iSeries システムが Window (R) 2000 ドメインに参加できるようにしながら、 EIM は、エンタープライズ内のユーザーを表す単一の EIM ID に Windows (R) 2000 ID を関連付けるメカニズムを提供します。このアソシエーションによって、ネットワーク上の Kerberos プリンシパルは、 iSeries ユーザー名およびパスワードでサインインせずに一部の iSeries アプリケーションにアクセスできます。単一サインオンの使用の利点および EIM とネットワーク認証サービスが共同で作業する方法の詳細については、 単一サインオンの使用可能化のトピックを参照してください。

このシナリオの利点

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します。
- ネットワーク内のサーバーへのアクセス管理のオーバーヘッドを減らします。
- パスワードが盗まれる危険性を最小に抑えます。
- 複数回サインオンする必要がありません。
- ネットワーク間のユーザー ID 管理を単純化します。

目的

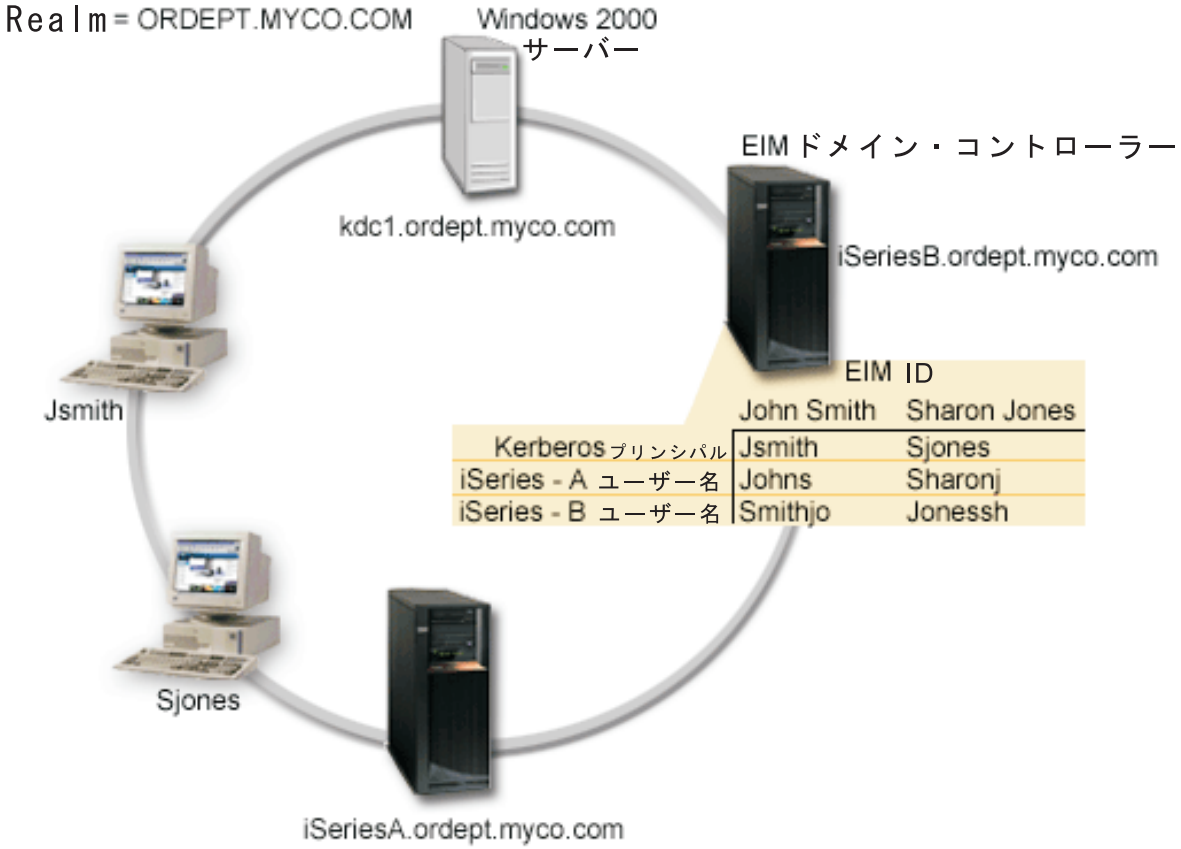
このシナリオでは、MyCo, Inc. は、認証の目的で既存の Windows (R) 2000 ドメインに iSeries システムを追加します。 iSeries システムには、ユーザーがアクセスする必要があるアプリケーションがいくつか入っています。 KDC によって認証されるべきユーザーは、これらのアプリケーションへのアクセス権を取得する必要があります。 iSeries サービスのプリンシパルを Windows (R) 2000 サーバーの KDC に追加して、プリンシパルがサービス・チケットを要求できるようにしなければなりません。さらに、EIM を構成してからアソシエーションを作成し、 iSeries ユーザー・プロファイルおよび Kerberos プリンシパルをエンタープライズ内の単一ユーザーを表す EIM ID にマップします。受注部門のユーザーは iSeries Access for Windows アプリケーションを使用するために、 iSeries Access for Windows および関連アプリケーションの優先認証方式として Kerberos プリンシパルを使用することを決定しています。

このシナリオの目的は、次のようになります。

- iSeries-A および iSeries-B が既存の鍵配布センターによって参加できるようにします。
- iSeries-B に Directory Server を構成して、ドメインの EIM ドメイン・コントローラーとして操作します。
- iSeries-A および iSeries-B のユーザー・プロファイルと、Kerberos プリンシパルを単一の EIM ID にマップできるようにします。
- Kerberos プリンシパルを使用して、iSeries Access for Windows アプリケーションに対して認証します。

シナリオの詳細

次の図は、MyCo ネットワークの特性を示します。



受注部門

- iSeries-A および iSeries-B は、OS/400 バージョン 5 リリース 2 (V5R2) で稼働し、いくつかのビジネス・アプリケーションが入っています。
- KDC の名前は `kdc1.ordept.myco.com` です。
- iSeries-A のプリンシパル名は `krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM` です。
- iSeries-A の DNS 名は `iSeriesA.ordept.myco.com` です。
- KDC のデフォルト・レルムは `ORDEPT.MYCO.COM` です。
- iSeries-B の Directory Server (LDAP) は、ネットワークの EIM ドメイン・コントローラーとして動作するように構成されます。**注：** LDAP 構成は、 EIM の構成前に行う必要がありますが、 EIM 構成ウィザードは LDAP がシステムに構成されていなければ構成できるようにします。このシナリオでは、iSeries-B は LDAP を構成しません。管理者は、 EIM 構成中に LDAP を構成するように計画しています。
- iSeries-B の DNS 名は `iSeriesB.ordept.myco.com` です。
- iSeries-B のプリンシパル名は `krbsvr400/iSeriesB.ordept.myco.com@ORDEPT.MYCO.COM` です。
- クライアント PC は Windows (R) 2000 を稼働します。
- Kerberos プリンシパルの Jsmith および Sjones は KDC に登録済みです。

このシナリオの構成ステップ

1. iSeries-A および iSeries-B の計画ワークシートを完成 (20 ページを参照)させます。
2. iSeries-A でネットワーク認証サービスを構成 (22 ページを参照)します。
3. iSeries-A サービス・プリンシパルを KDC に追加 (23 ページを参照)します。

4. iSeries-A 上に各ユーザーのホーム・ディレクトリーを作成 (23 ページを参照)します。
5. 検査 (23 ページを参照) iSeries-A の TCP/IP ドメイン情報
6. iSeries-A でネットワーク認証サービスの構成をテスト (24 ページを参照)します。
7. iSeries-B でのステップ 2-6 を繰り返します。
8. EIM ドメインを構成 (24 ページを参照)し、 EIM ドメイン・コントローラーとして iSeries-B にディレクトリー・サーバーを構成します。
9. EIM ドメインに参加するように iSeries-A を構成 (25 ページを参照)します。
10. エンタープライズのユーザーに EIM ID を作成 (26 ページを参照)します。
11. iSeries ユーザー・プロファイルおよびプリンシパル名の EIM アソシエーションを EIM ID に追加 (27 ページを参照)します。

12. 認証方式として Kerberos プリンシパルを使用するように iSeries Access for Windows 接続を構成 (28 ページを参照)します。
13. ネットワーク認証サービスおよび EIM セットアップを検査 (28 ページを参照)します。

構成の詳細

ステップ 1: 計画ワークシートの完成

以下の計画チェックリストは、ネットワーク認証サービスおよびエンタープライズ識別マッピング (EIM) の構成を開始する前に必要な種類の情報を示しています。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、前提条件チェックリストのすべてに「はい」と回答し、ネットワーク認証の構成情報を完成させる必要があります。

前提条件チェックリスト	回答
OS/400 V5R2 (5722-SS1) 以降か ?	はい
Cryptographic Access Provider (5722-AC3) が iSeries システムにインストールされているか ?	はい
iSeries Access for Windows (5722-XE1) がネットワーク内のすべての PC および iSeries システムにインストールされているか ?	はい
iSeries ナビゲーターのセキュリティー・サブコンポーネントがネットワーク内のすべての PC および iSeries システムにインストールされているか ?	はい
iSeries ナビゲーターのネットワーク・サブコンポーネントがネットワーク内のすべての PC および iSeries システムにインストールされているか ?	はい

*SECADM、*ALLOBJ、および *IOSYSCFG の特殊権限を持っているか ?	はい
以下のいずれかのシステムが、鍵配布センターとして動作しているか ? インストールされていれば、どれか ? 1. Windows (R) 2000 サーバー 2. Windows (R) XP サーバー 3. AIX サーバー 4. zSeries	はい Windows (R) 2000 サーバー
Windows (R) 2000 サーバーおよび Windows (R) XP サーバーの場合、ktpass ツールを装備する Windows サポート・ツールがインストールしてあるか ?	はい
ネットワーク内のすべての PC が Windows (R) 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
iSeries システム時刻と KDC のシステム時刻との差が 5 分以内か ? 超えている場合は、システム時刻を同期するを参照。	はい

ネットワーク認証サービスの構成には、以下の情報が必要	**回答**
iSeries が所属する Kerberos のデフォルト・レルムの名前は ?	ORDEPT.MYCO.COM
Kerberos デフォルト・レルムの KDC は ? KDC が listen するポートは ?	kdc1.ordept.myco.com 88 (**注 :** これは、KDC 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・サーバーを構成するか ? 構成する場合は、以下の質問に回答してください。 この KDC 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 kdc1.ordept.myco.com 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。)
iSeries サービス・プリンシパルのパスワードは ?	iseriesa123 iseriesb345 **注 :** このシナリオ内で使用される任意およびすべてのパスワードは例として使用しているだけです。実際の構成には使用しないでください。
iSeries はほかにどのようなレルムと対話するか?	該当なし
各レルムについて、鍵配布センターのホスト名は ?	該当なし

この情報は、エンタープライズ識別マッピング (EIM) を構成する際に必要	回答
LDAP 管理者の識別名およびパスワードは何か ?	識別名 : cn=administrator パスワード : mycopwd **注 :** このシナリオ内で使用される任意およびすべてのパスワードは例として使用しているだけです。実際の構成には使用しないでください。
ディレクトリー・サービス (LDAP) サーバーの名前は ?	iSeriesB.ordept.myco.com
ディレクトリー・サービス (LDAP) サーバーのポート番号は ?	389

ステップ 2: iSeries-A でのネットワーク認証サービスの構成

ワークシートからの情報を使用して、以下のタスクを完了して iSeries-A 上でネットワーク認証サービスを構成します。

1. iSeries ナビゲーターで、「**iSeries-A**」 **->「セキュリティー」**を展開します。
2. 「**ネットワーク認証サービス**」を右マウス・ボタン・クリックし、「**構成**」を選択して構成ウィザードを開始します。**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ついては、「**ウェルカム**」ページを参照してください。「**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 ORDEPT.MYCO.COM を入力します。「**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 kdc1.ordept.myco.com 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**」を選択します。「**パスワード・サーバー**」フィールドに kdc1.ordept.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。**注 :** このパスワードは、プリンシパルを KDC へ追加したときに入力したパスワードと同じにする必要があります。
7. 「**keytab エントリーの作成 (Create keytab entry)**」ページで、「**iSeries Kerberos 認証**」を選択します。「**次へ**」をクリックします。
8. 「**iSeries keytab エントリーの作成 (Create iSeries keytab entry)**」ページで、 iSeries-A のキータブおよびプリンシパルを書き込みます。この KDC への追加には、プリンシパル名が必要です。パスワードを入力して確認します。たとえば、MyCo の管理者はパスワード iseriesa123 を使用します。このパスワードは、iSeries-A が KDC に追加される時に使用されます。**注 :** このシナリオ内で使用される任意およびすべてのパスワードは例として使用しているだけです。実際の構成には使用しないでください。「**次へ**」をクリックします。
9. 「**要約 (Summary)**」ページで、ネットワーク認証サービスの構成の詳細を確認します。「**終了**」をクリックします。

これで、iSeries-A でのネットワーク認証サービスの構成が終わりました。次のステップは、 KDC へのプリンシパル名の追加です。

ステップ 3: KDC への iSeries-A プリンシパル名の追加

iSeries を Windows (R) 2000 KDC へ追加するには、 KDC へ追加するプリンシパルに対応した文書を使用します。規則では、 iSeries 名をユーザー名として使用できます。以下のプリンシパル名を KDC に追加します。

```
krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM
```

Windows (R) 2000 サーバーでは、以下のステップを実行します。

1. Active Directory (R) の管理ツールを使って、 iSeries-A 用のユーザー・アカウントを作成します (「**ユーザー**」フォルダーを選択して右マウス・ボタン・クリックし、「**新規作成**」を選択してから、「**ユーザー**」を選択します。) iSeriesA を Active Directory ユーザーとして指定します。
2. Active Directory ユーザー iSeriesA でプロパティーにアクセスします。「**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。これにより、iSeries-A サービス・プリンシパルはサインイン・ユーザーの代わりに他のサービスにアクセスできます。
3. **ktpass** コマンドを使い、ユーザー・アカウントをプリンシパルにマップします。 ktpass ツールは、Windows (R) 2000 サーバーのインストール CD の「**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、次のように入力します。

   ```
   ktpass -princ krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM
   -mapuser iSeriesA -pass iseriesa123
   ```

   ここで iseriesa123 は、ネットワーク認証サービスを構成 (22 ページを参照)したときにステップ 6 で指定したパスワードです。**注 :** このシナリオ内で使用される任意およびすべてのパスワードは例として使用しているだけです。実際の構成には使用しないでください。

ステップ 4: iSeries-A でのユーザーのホーム・ディレクトリーの作成

iSeries および iSeries 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、以下の処理を完了してください。

1. iSeries コマンド行で、次のように入力します。

   ```
   CRTDIR '/home/username'
   ```

   ここで username はユーザーの iSeries ユーザー名です。
   たとえば、MyCo の管理者の場合、次のように入力します。
   `CRTDIR '/home/Johns'` (ユーザー John Smith の場合。)
2. すべてのユーザーについて上記のステップを繰り返します。

ステップ 5: iSeries A の TCP/IP ドメイン情報の検査

1. iSeries コマンド行で、次のように入力します。

   ```
   CFGTCP
   ```

2. オプション 10 を選択します。(TCP/IP ホスト・テーブル エントリーの作業。)
3. ホスト名フィールドで、iSeries A の完全修飾ホスト名が小文字であることを検査します。さらに、複数のホスト名エントリーがある場合、完全修飾ホスト名は最初に表示されることを検査します。たとえば、iSeries A は、ホスト名エントリー: iseriesa.ordept.myco.com.です。
4. ホスト名エントリーを検査したら、F3 を押して「TCP メインメニューの構成(Configure TCP main menu)」に戻ります。
5. オプション 12 を選択します。(TCP/IP ドメイン情報の変更。)
6. ホスト名フィールドに、システム名が表示されることを検査します。さらにドメイン名が正しいことを検査します。たとえば、ホスト名は`iseriesa`であり、ドメイン名は、`ordept.myco.com` です。

ステップ 6: iSeries-A 上のネットワーク認証サービスのテスト

この時点で、iSeries-A プリンシパル名のチケット認可チケットを要求することで、ネットワーク認証サービスが正常に構成されたかどうかを検査できます。

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します。
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します。このシナリオでは、 krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM が iSeries-A のプリンシパル名として表示されます。
3. `kinit -k krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM` と入力します。これが成功すると、QSH コマンドはエラーなしで表示されます。
4. `klist` と入力し、デフォルト・プリンシパルが krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM であるかどうかを検査します。

ステップ 7: iSeries-B でのステップ 2 およびステップ 6 の繰り返し

ステップ 8: iSeries-B 上での EIM および EIM ドメイン・コントローラーの構成

ここで、ネットワークに EIM ドメインを構成する必要があります。また、新規 EIM ドメインの EIM ドメイン・コントローラーとして iSeries-B を構成する必要があります。このステップを終了したら、以下のタスクが完了します。

- 新規 EIM ドメインを作成しました。
- EIM ドメイン・コントローラーとして iSeries-B に Directory Server を構成しました。
- iSeries-B に EIM レジストリーおよびドメインに Kerberos ユーザー・レジストリーを作成しました。
- EIM ドメインに参加するように iSeries-B を構成しました。

1. iSeries ナビゲーターで、「**iSeries-B**」 —>「**ネットワーク**」 —>「**エンタープライズ識別マッピング (Enterprise Identity Mapping)**」を展開します。
2. 「**構成**」を右マウス・ボタン・クリックし、「**構成**」を選択して構成ウィザードを開始します。
3. 「**ウェルカム**」ページで、「**新規ドメインの作成および結合 (Create and join a new domain)**」を選択します。「**次へ**」をクリックします。

4. 「**Directory Server の構成**」ページの「**ポート**」フィールドでデフォルトの 389 を受け入れます。「**識別名 (Distinguished name)**」フィールドで、 cn=administrator と入力します。パスワードを入力して確認します。このパスワードは、 EIM ドメイン管理タスクにアクセスする際に使用されます。たとえば、MyCo の管理者の場合、パスワードに mycopwd と入力してパスワード・フィールドを確認します。**注 :** このシナリオ内で使用される任意およびすべてのパスワードは例として使用しているだけです。実際の構成には使用しないでください。「**次へ**」をクリックします。
5. 「**ドメインの指定 (Specify Domain)**」ページで、ドメインの名前を入力します。たとえば、MyCo の管理者の場合、「**ドメイン**」フィールドに mycoeimDomain と入力します。**注** : ドメイン・ネームには、 = + < > , # ; ¥ * の文字は含められません。「**説明**」フィールドはオプションです。このフィールドが必要であれば、ドメイン・コントローラーの簡単な説明を入力してください。「**次へ**」をクリックします。
6. 「**ドメインの親 DN の指定 (Specify Parent DN for Domain)**」ページで、「**いいえ**」を選択します。「**次へ**」をクリックします。
7. 「**レジストリー情報 (Registry Information)**」ページで、「**ローカル iSeries**」および「**Kerberos**」を選択します。「**Kerberos ユーザー ID の大文字小文字の区別あり (Kerberos user identities are case sensitive)**」を選択します。「**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、ドメイン内で固有のものにする必要があります。
8. 「**EIM システム・ユーザーの指定 (Specify EIM System User)**」ページで、システム EIM ユーザーを選択します。このページに表示されるデフォルトを受け入れます。たとえば、 MyCo の場合、このページには以下の情報があります。
   - 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
     注 : このシナリオ内で使用される任意およびすべてのパスワードは例として使用しているだけです。実際の構成には使用しないでください。

   「**次へ**」をクリックします。
9. 「**要約**」ページで、EIM 構成情報を確認します。「**終了**」をクリックします。

これで、ネットワーク内に新たに構成した EIM ドメインの EIM ドメイン・コントローラーとして Directory Server が iSeries-B に構成されました。ここで、iSeries-A をこの EIM ドメインの参加者として指定する必要があります。

ここで、EIM ドメインに参加するように iSeries-A を構成する必要があります。

1. iSeries ナビゲーターで、「**iSeries-A**」 **->「ネットワーク」 ->「エンタープライズ識別マッピング (Enterprise Identity Mapping)」**を展開します。
2. 「**構成**」を右マウス・ボタン・クリックし、「**構成**」を選択して構成ウィザードを開始します。
3. 「**ウェルカム**」ページで、「**既存のドメインの結合 (Join an existing domain)**」を選択します。「**次へ**」をクリックします。
4. 「**ドメイン・コントローラーの指定 (Specify Domain Controller)**」ページで、ドメイン・コントローラーの名前を入力します。たとえば、MyCo の管理者の場合、「**ドメイン・コントローラー名**」フィールドに iSeriesB.ordept.myco.com と入力します。「**次へ**」をクリックします。
5. 「**接続のユーザーの指定 (Specify User for Connection)**」ページで、そのユーザー・タイプに対して「**識別名およびパスワード (Distinguished name and password)**」を選択します。たとえば、MyCo の管理者の場合、「**識別名 (Distinguished name)**」フィールドに cn=administrator と入力し、パス

ワードに mycopwd と入力してパスワード・フィールドを確認します。**注 :** このシナリオ内で使用される任意およびすべてのパスワードは例として使用しているだけです。実際の構成には使用しないでください。「**次へ**」をクリックします。

6. 「**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します。「**次へ**」をクリックします。たとえば、MyCo の管理者の場合、 **mycoeimDomain** を選択します。
7. 「**レジストリー情報 (Registry Information)**」ページで、「**ローカル iSeries**」を選択します。「**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、ドメイン内で固有のものにする必要があります。
8. 「**EIM システム・ユーザーの指定 (Specify EIM System User)**」ページで、システム EIM ユーザーを選択します。このページに表示されるデフォルトを受け入れます。たとえば、 MyCo の場合、このページには以下の情報があります。
   - 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
     注 : このシナリオ内で使用される任意およびすべてのパスワードは例として使用しているだけです。実際の構成には使用しないでください。

   「**次へ**」をクリックします。
9. 「**要約**」ページで、EIM 構成を確認します。「**終了**」をクリックします。

これで、ドメインに参加するように iSeries-A が構成されました。

ここで、エンタープライズ内の各ユーザーに EIM ID を作成する必要があります。 EIM ID は、ネットワーク上のユーザーまたはエンティティーを表します。 MyCo の場合、管理者は John Smith と Sharon Jones の 2 つの EIM ID を作成します。

1. iSeries-B で、**「ネットワーク」 -> 「エンタープライズ識別マッピング (Enterprise Identity Mapping)」**を展開します。
2. 「**ドメイン管理**」を右マウス・ボタン・クリックして、「**ドメインの追加**」を選択します。
3. 「**ドメインの追加**」ダイアログで、以下のデフォルトが MyCo の EIM ドメインとして表示されます。
   - ポート : 389
   - ドメイン : mycoeimDomain
   - 親 DN: なし
   - ドメイン・コントローラー : iSeriesB.ordept.myco.com

   注 : これらのデフォルトは、EIM ドメイン・コントローラーの構成中に作成されます。
4. 「**OK**」をクリックします。
5. iSeries ナビゲーターの階層は、「**ドメイン管理**」の下に「**mycoeimDomain**」が最新表示されます。「**mycoeimDomain**」をクリックします。「**EIM ドメイン・コントローラーへの接続 (Connect to EIM Domain Controller)**」ダイアログにプロンプトが表示されます。ドメインを管理する前に、 EIM ドメイン・コントローラーへ接続する必要があります。

6. 「**EIM ドメイン・コントローラーへの接続 (Connect to EIM Domain Controller)**」ページで、ドメイン・コントローラーの管理者識別名およびパスワードを入力します。これは、EIM ドメイン・コントローラーの構成中に作成された識別名およびパスワードと同じです。 MyCo の場合、管理者は次のように入力します。
   - 識別名 : cn=administrator
   - パスワード : mycopwd **注 :** このシナリオ内で使用される任意およびすべてのパスワードは例として使用しているだけです。実際の構成には使用しないでください。
7. 「**OK**」をクリックします。
8. 新しいフォルダーが 2 つ表示されます。「**ID (Identifiers)**」を右マウス・ボタン・クリックして、「**新規 ID (New Identifier)**」を選択します。
9. 「**新規 EIM ID (New EIM Identifier)**」ページで、「**ID (Identifier)**」フィールドに ID を入力します。すべてのユーザーに ID を持たせるまでこのステップを繰り返します。 MyCo は、以下の ID を追加しました。
   - John Smith
   - Sharon Jones
10. 「**OK**」をクリックします。

これで、John Smith および Sharon Jones に固有の EIM ID が作成されました。ここで、iSeries-A および iSeries-B 上のそれぞれの iSeries ユーザー名と Kerberos プリンシパルをこれらの EIM ID に関連付けることができます。

ステップ 11: EIM ID へのOS/400のユーザー・プロファイルおよびプリンシパル名 の EIM アソシエーション追加

このタスクを完成させるには、MyCo の管理者は以下のステップを完了します。

1. iSeries-B で、「**ID (Identifiers)**」を展開して「**John Smith**」を右マウス・ボタン・クリックし、「**プロパティー**」を選択します。この ID には、 Kerberos プリンシパル、iSeries-A 上のユーザー・プロファイル、および iSeries-B のユーザー・プロファイルの 3 つのアソシエーションがあります。
2. Kerberos プリンシパルを ID に関連付けるには、John Smith について以下のことを行います。
   a. 「**アソシエーション (Associations)**」タブで、「**追加**」をクリックします。
   b. 「**アソシエーションの追加 (Add Association)**」ページで、「**レジストリー (Registry)**」フィールドの「**ブラウズ (Browse)**」をクリックし、「ORDEPT.MYCO.COM」を選択します。これは、 EIM 構成中に追加された Kerberos ユーザー・レジストリーです。
   c. 「**ユーザー**」フィールドに Jsmith と入力します。
   d. 「**アソシエーション・タイプ (Association type)**」フィールドで、「**ソース**」を選択します。
   e. 「**OK**」をクリックします。
3. iSeries-A 上のユーザー名を ID に関連付けるには、John Smith について以下のことを行います。
   a. 「**アソシエーション (Associations)**」タブで、「**追加**」をクリックします。
   b. 「**アソシエーションの追加 (Add Association)**」ページで、「**レジストリー (Registry)**」フィールドの「**ブラウズ (Browse)**」をクリックし、「iSeriesA.ordept.myco.com」を選択します。これは、iSeries-A の iSeries ユーザー・レジストリーです。
   c. 「**ユーザー**」フィールドに Johns と入力します。
   d. 「**アソシエーション・タイプ (Association type)**」フィールドで、「**ターゲット**」を選択します。

e. 「**OK**」をクリックします。

4. iSeries-B 上のユーザー名を ID に関連付けるには、John Smith について以下のことを行います。
   a. 「**アソシエーション (Associations)**」タブで、「**追加**」をクリックします。
   b. 「**アソシエーションの追加 (Add Association)**」ページで、「**レジストリー (Registry)**」フィールドの「**ブラウズ (Browse)**」をクリックし、「iSeriesB.ordept.myco.com」を選択します。これは、iSeries-B 上の iSeries ユーザー・レジストリーです。
   c. 「**ユーザー**」フィールドに Smithjo と入力します。
   d. 「**アソシエーション・タイプ (Association type)**」フィールドで、「**ターゲット**」を選択します。
   e. 「**OK**」をクリックします。
5. EIM ID Sharon Jones についてステップ 1 ～ 4 を繰り返します。

ここで、iSeries-A および iSeries-B への認証時に Kerberos を使用するように、 Jsmith および Sjones の PC 上で iSeries Access for Windows アプリケーションを構成する必要があります。

Jsmith の PC から、以下のステップを完了して、Kerberos 認証を使用するように iSeries-A およびそのアプリケーションを構成します。

1. iSeries ナビゲーターで、「**iSeries-A**」を右マウス・ボタン・クリックし、「**プロパティー**」を選択します。
2. 「**接続**」タブで、「**Kerberos プリンシパル名の使用 (プロンプトなし) (Use Kerberos principal name, no prompting)**」を選択します。これにより、認証に Kerberos プリンシパル名およびパスワードを使用した iSeries Access for Windows 接続が可能です。
3. iSeries-B について上記のステップを繰り返します。
4. Sjones の PC 上で上記のステップを繰り返します。

ステップ 13: ネットワーク認証サービスおよび EIM セットアップの検査

この時点で、すべての構成ステップが完了しました。ネットワーク認証サービスおよび EIM が正しくセットアップされたことを検査するには、管理者が Sharon Jones および John Smith をそれぞれの PC にサインインして Windows (R) 2000 ドメインにログオンさせます。そこで、管理者が iSeries-A 上で iSeries ナビゲーターを開きます。 iSeries サインオン・プロンプトが表示されなければ、 EIM は正常に Kerberos プリンシパルをドメイン上の ID にマップしました。 iSeries Access for Windows アプリケーションだけでなく、以下のような他のアプリケーションも Kerberos 認証をサポートします。

- Telnet サーバー
- iSeries NetServer
- QFileSrv.400
- 分散リレーショナル・データベース・アーキテクチャー (DRDA)

ネットワーク認証サービスを計画する

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、必要な計画のステップを完了する必要があります。このトピックは、必要なすべてのステップを完了するための前提条件チェックリストおよび計画ワークシートを記載します。以下のチェックリストおよびワークシートを使用して、ネットワーク認証サービスの構成に役立ててください。

前提条件チェックリスト	回答
OS/400 V5R2 (5722-SS1) 以降か ?	
Cryptographic Access Provider (5722-AC3) が iSeries システムにインストールされているか ?	
iSeries Access for Windows (5722-XE1) がネットワーク内のすべての PC および iSeries システムにインストールされているか ?	
iSeries ナビゲーターのセキュリティー・サブコンポーネントがネットワーク内のすべての PC および iSeries システムにインストールされているか ?	
iSeries ナビゲーターのネットワーク・サブコンポーネントがネットワーク内のすべての PC および iSeries システムにインストールされているか ?	
*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、鍵配布センターとして動作するセキュア・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 (R) 2000 サーバー 2. Windows (R) XP サーバー 3. AIX サーバー 4. zSeries	
Windows (R) 2000 サーバーおよび Windows (R) XP サーバーの場合、ktpass ツールを装備する Windows サポート・ツールが、鍵配布センターとして使用されるシステム上にインストールしてあるか ?	
ネットワーク内のすべての PC が Windows (R) 2000 ドメイン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 ?	
iSeries システム時刻の差が KDC のシステム時刻の 5 分以内か ? 超えている場合は、システム時刻を同期するを参照。	

ネットワーク認証サービスの構成には、以下の情報が必要	回答
iSeries-A が所属する Kerberos のデフォルト・レルムの名前は ?	
Kerberos デフォルト・レルムの KDC は ? KDC が listen するポートは ?	
このデフォルト・レルムにパスワード・サーバーを構成するか ? 構成する場合は、以下の質問に回答してください。 この KDC 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 ?	
iSeries サービス・プリンシパルのパスワードは ?	

ネットワーク認証サービスの構成には、以下の情報が必要	回答
iSeries はほかにどのようなレルムと対話するか？	
各レルムについて、鍵配布センターのホスト名は ？	
iSeries のアプリケーションはどのようなサービス・プリンシパル名を使うか？	

«

ネットワーク認証サービスを構成する

» ネットワーク認証サービスを構成する前に、必要な計画のステップをすべて完了しておく必要があります。さらに、ネットワーク認証サービスでは、鍵配布センター (KDC) 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。現在、KDC は iSeries 上ではサポートされません。Microsoft Windows (R) 2000、Windows (R) XP、および z/OS は、 KDC 機能をサポートします。KDC 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。

KDC を構成してからネットワーク認証サービスを iSeries 上に構成することをお勧めします。ネットワーク認証サービスを構成するには、以下のステップを完了してください。

1. iSeries ナビゲーターで、「**iSeries-A**」 ->「**セキュリティー**」を展開します。
2. 「**ネットワーク認証サービス**」を右マウス・ボタン・クリックし、「**構成**」を選択して構成ウィザードを開始します。**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ついては、「**ウェルカム**」ページを参照してください。「**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します。「**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鍵配布センターの名前を入力し、「**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します。パスワード・サーバーは、プリンシパルが KDC 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・サーバーのデフォルト・ポートは 464 です。「**次へ**」をクリックします。
7. 「**keytab エントリーの作成 (Create keytab entry)**」ページで、「**iSeries Kerberos 認証**」を選択します。さらに、 Kerberos 認証を使用する LDAP サーバーおよび iSeries NetServer の keytab エントリーを作成できます。「**次へ**」をクリックします。
8. 「**iSeries keytab エントリーの作成 (Create iSeries keytab entry)**」ページで、パスワードを入力して確認します。「**次へ**」をクリックします。**注 :** このパスワードは、 KDC に iSeries を定義するときに使用するパスワードと同じです。
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確認します。「**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。

次の処理

鍵配布センターに対して iSeries を定義する

iSeries のネットワーク認証サービスを構成したら、鍵配布センター (KDC) に対して iSeries を定義する必要があります。ネットワーク認証サービスは、サーバーおよびすべての固有な iSeries アプリケーションに iSeries プリンシパル名 **krbsvr400** を提供します。

たとえば、この構成のシナリオでは、 iSeries のホスト名は iSeriesA.ordept.myco.com としました。この iSeries に提示するサービス・チケットをクライアントが取得するためには、krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM というプリンシパルが KDC に定義されていなければなりません。

z/OS
Kadmin コマンドに関する資料を参照してください。

Windows (R) 2000 サーバー

1. Active Directory (R) の管理ツールを使って、 iSeries 用のユーザー・アカウントを作成します。Active Directory ユーザーとして iSeries の名前を指定します。たとえば、有効な名前は iSeriesA になります。
2. ステップ 1 で作成した Active Directory ユーザーのプロパティーにアクセスします。「**アカウント**」タブから、「**アカウントは委任に対して信頼されている (Account is trusted for delegation)**」を選択します。これにより、iSeries サービス・プリンシパルはサインイン・ユーザーの代わりに他のサービスにアクセスできます。
3. **ktpass** コマンドを使い、ユーザー・アカウントをプリンシパルにマップします。たとえば、次のように入力できます。
   ```
   ktpass -princ krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM -mapuser iSeriesA -pass xxxxxx
   ```
   ここで xxxxxx は、ネットワーク認証サービスの 構成時に指定したパスワードです。

次の処理

ホーム・ディレクトリーの作成

ホーム・ディレクトリーを作成する

鍵配布センターに対してiSeriesを定義 したら、 iSeries および iSeries アプリケーションに接続する各ユーザーのためのホーム・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入ります。ユーザーのホーム・ディレクトリーを作成するには、以下の処理を完了してください。

iSeries コマンド行で、次のように入力します。

```
CRTDIR '/home/username'
```
ここで username はユーザーの iSeries ユーザー名です。

次の処理

TCP/IP ドメイン情報の検査

TCP/IP ドメイン情報の検査

ホーム・ディレクトリーを作成後、サーバーに正しいホスト・テーブルのエントリーがあるか検査する必要があります。

1. iSeries コマンド行で、次のように入力します。

   ```
   CFGTCP
   ```

2. オプション 10を選択します。(TCP/IP ホスト・テーブル 項目の処理).
3. ホスト名フィールドで、iSeries A の完全修飾ホスト名が小文字であることを検査します。さらに、複数のホスト名エントリーがある場合、完全修飾ホスト名が最初に表示されることを検査します。 たとえば、iSeries A には、ホスト名 : iseriesa.ordept.myco.com.のエントリーがあります。
4. ホスト名エントリーを検査したら、F3を押して「TCP/IP の構成」に戻ります。
5. オプション 12 を選択します。(TCP/IP ドメイン情報の変更。)
6. システム名が、ホスト名フィールドに表示されることを検査します。さらに、ドメイン名が正しいことを検査します。たとえば、ホスト名は`iseriesa`であり、ドメイン名は`ordept.myco.com`です。

次の処理

ネットワーク認証サービス構成のテスト

ネットワーク認証サービス構成のテスト

正しいドメイン情報を 検査 したら、iSeries プリンシパル名のチケット許可証(ticket granting ticket)の要求によってネットワーク認証サービス構成をテストする必要があります。:

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します。
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します。たとえば、有効なプリンシパル名は、krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM です。
3. `kinit -k krbsvr400/system.domain@realm`を入力します。 たとえば、krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM は、iSeries の有効なプリンシパル名です。これが成功すると、QSH コマンドはエラーなしで表示されます。
4. デフォルト・プリンシパルが、krbsvr400/system.domain@realmであることを検査するために `klist`を入力します。

次の処理 :

エンタープライズ識別マッピング (EIM) を構成する
このステップは、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。しかし、ネットワーク間で複数のユーザー ID を管理する固有の iSeries アプリケーションでは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を管理する

ネットワーク認証サービスを構成した後で、チケットを要求し、キー・テーブル・ファイルを処理し、レルムの信頼関係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。以下のトピックはこれらのタスクの完了方法を説明しています。

管理者タスク

次に、iSeries ナビゲーターで管理者が実行できるタスクの簡略リストを示します。ネットワーク認証サービスのタスクについてのさらに詳しい情報は、 iSeries ナビゲーターのヘルプを参照してください。これらのタスクだけではなく、管理者は、ユーザーに kdestroy コマンドを使用して 古い信任状を削除させるようにする必要があります。

- システム時刻を同期する
  iSeries と KDC の間で交換されるチケットについては、システム時刻の差を 5 分以内にする必要があります。最大クロックの差は、ネットワーク認証サービスのプロパティーから構成できます。デフォルトの最大クロックの差は 5 分または 300 秒です。このトピックは、システム間で時刻を同期する方法について説明します。
-
- レルムを追加する
  このトピックは、新規レルムをネットワーク認証サービス構成に追加する方法について説明します。
-
- レルムを削除する
  このトピックは、レルムをネットワーク認証サービス構成から除去する方法について説明します。
-
- レルムへ鍵配布センターを追加する
  このトピックは、ネットワーク認証サービスの現行構成に鍵配布センターを追加する方法について説明します。
-
- パスワード・サーバーを追加する
  このトピックは、パスワード・サーバーをネットワーク認証サービス構成に追加し、ユーザーが自身の Kerberos パスワードを変更できるようにする方法について説明します。
-
- レルム間の信頼関係を作成する
  このトピックは、レルム間の信頼関係をセットアップする方法について説明します。この機能は、デフォルトで Kerberos プロトコルがレルム階層で信頼を検索しているためにオプションとなっています。ただし、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便利です。
-
- ホスト解決を変更する
  このトピックは、レルム名のホスト解決を変更する方法について説明します。
-

- 暗号化設定を追加する
  このトピックは、チケット認可チケット (TGT) およびチケット認可サービス (TGS) の暗号化タイプを追加する方法について説明します。

iSeries ユーザー・タスク

iSeries は、Kerberos 可能ネットワークでクライアントとしても運用できます。ユーザーは、iSeries にログオンして、 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、いくつかの Qshell コマンドを使用して iSeries ユーザーの共通タスクを実行します。

- ホーム・ディレクトリーを作成する
  このトピックは、ホーム・ディレクトリーを作成する方法について説明します。
-
- 新しいチケット認可チケットを取得する
  このトピックは、チケット認可チケットを Qshell コマンド **kinit** によって取得または更新する方法について説明します。
-
- Kerberos パスワードを変更する
  このトピックは、Qshell コマンド **kpasswd** によりパスワードを変更する方法について説明します。
-
- keytab ファイルを管理する
  このトピックは、Qshell コマンド **keytab** により keytab ファイルを管理する方法について説明します。
-
- 有効期限が切れた信任状キャッシュを削除する
  このトピックは、クライアントに格納されている有効期限が切れた信任状キャッシュを Qshell コマンド **kdestroy** により削除する方法について説明します。重要な点は、ユーザーが信任状キャッシュを定期的に削除することです。
-
- 信任状キャッシュまたは keytab ファイルを表示する
  このトピックは、ユーザーに関連付けられた信任状および keytab ファイルを Qshell コマンド **klist** によりリストする方法について説明します。
-
- LDAP ディレクトリー内の Kerberos サービス・エントリーを管理する
  このトピックは、ディレクトリー・サービス (LDAP) ディレクトリー内の Kerberos サービス・エントリーを Qshell コマンド **ksetup** コマンドにより管理する方法について説明します。

システム時刻を同期する

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。クロックの差は、ネットワーク認証サービスのプロパティーの設定によって変更できます。

システム時刻を同期する前に、 QUTCOFFSET 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。 KDC 時刻を変更してこのシステム時刻を同期するか、 QTIME システム値を

使用して iSeries システム時刻を変更できます。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します。 SNTP を構成するには、以下の項目を完了してください。

iSeries 上で SNTP を構成するには、コマンド行で CHGNTPA と入力します。

Windows (R) システム上で SNTP を構成するには、**NET HELP TIME** を使用して SNTP サーバーの構成情報を表示します。

レルムを追加する

 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に新しいレルムを追加することができます。レルムを iSeries 構成に追加する前に、新しいレルムのために KDC を構成する必要があります。レルムを iSeries ネットワーク認証サービス・タスクに追加する前に、レルム名、KDC 名、および KDC 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、以下のステップを完了してください。

1. iSeries ナビゲーターで、**「ユーザーの iSeries サーバー (your iSeries server)」** −> **「セキュリティー」** −> **「ネットワーク認証サービス」**を展開します。
2. 「**レルム**」を右マウス・ボタン・クリックして、「**レルムの追加**」を選択します。
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します。たとえば、有効なレルム名は ORDEPT.MYCO.COM のようになります。
4. 追加するレルムの KDC の名前を入力します。たとえば、有効な KDC 名は kdc1.ordept.myco.com のようになります。
5. KDC が要求を listen するポート番号を入力します。有効なポート番号は 1 〜 65535 です。 KDC のデフォルト・ポートは 88 です。
6. 「**OK**」をクリックします。

レルムを削除する

 ネットワーク管理者として、ネットワーク認証サービスからレルムを削除することができます。レルムが必要なくなったから、ネットワーク上で使用されなくなった場合です。また、iSeries 固有のアプリケーションの問題から回復するためにデフォルト・レルムを除去する必要があることもあります。

たとえば、ネットワーク内に鍵配布センター (KDC) 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、以下のステップを完了してください。

1. iSeries ナビゲーターで、**「ユーザーの iSeries サーバー (your iSeries server)」** −> **「セキュリティー」** −> **「ネットワーク認証サービス」** −> **「レルム」**を展開します。
2. 削除したいレルムの名前を右マウス・ボタン・クリックして、「**削除**」を選択します。

3. 「**OK**」をクリックして削除を確認します。

レルムへ鍵配布センターを追加する

 ネットワーク管理者として、ネットワーク認証サービスを使用してレルムに鍵配布センター (KDC) を追加できます。 KDC をレルムに追加する前に、KDC 名および 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、以下のステップを完了してください。

1. iSeries ナビゲーターで、**「ユーザーの iSeries サーバー (your iSeries server)」**—>**「セキュリティー」**—>**「ネットワーク認証サービス」**—>**「レルム」**を展開します。
2. 右側の画面区画にあるレルムの名前を右マウス・ボタン・クリックして、「**プロパティー**」を選択します。
3. 「**概要 (General)**」タブに、このレルムに追加したい KDC の名前を入力します。すべてのレルムに KDC が必要です。たとえば、kdc2.ordept.myco.com が有効な入力になります。
4. KDC が要求を listen するポート番号を入力します。有効なポート番号は 1 ～ 65535 です。 KDC のデフォルト・ポートは 88 です。
5. 「**追加**」をクリックします。新しい KDC が「**このレルムの鍵配布センター (KDC) (Key Distribution Center (KDC) for this realm)**」リスト表示されます。
6. 「**OK**」をクリックします。

パスワード・サーバーを追加する

パスワード・サーバーによって、Kerberos プリンシパルは自分のパスワードを変更できます。パスワード・サーバーをレルムに追加するには、以下のステップを完了してください。

1. iSeries ナビゲーターで、**「ユーザーの iSeries サーバー (your iSeries server)」**—>**「セキュリティー」**—>**「ネットワーク認証サービス」**—>**「レルム」**を展開します。
2. 右側の画面区画にあるレルムの名前を右マウス・ボタン・クリックして、「**プロパティー**」を選択します。
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します。たとえば、有効なパスワード・サーバーの名前は psvr.ordept.myco.com のようになります。
4. パスワード・サーバーに対応するポート番号を入力します。有効なポート番号は 1 ～ 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**」をクリックします。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。

レルム間の信頼関係を作成する

 レルム間の信頼関係を設定するためには、認証へのショートカットを作成します。この機能は、デフォルトで Kerberos プロトコルがレルム階層で信頼を検索しているために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 KDC がキーを共用する必要があります。信頼関係を作成する前に、お互いを承認するように KDC を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、以下のステップを完了してください。

1. iSeries ナビゲーターで、**「ユーザーの iSeries サーバー (your iSeries server)」** −>**「セキュリティー」** −>**「ネットワーク認証サービス」** −>**「レルム」**を展開します。
2. 右側の画面区画にあるレルムの名前を右マウス・ボタン・クリックして、「**プロパティー**」を選択します。
3. 「**トラステッド・レルム (Trusted Realms)**」タブで、信頼を設定したいレルムの名前を入力します。たとえば、信頼関係の有効な名前は NY.myco.com and LA.myco.com のようになります。
4. 「**追加**」をクリックします。これで、テーブルに信頼の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。

ホスト解決を変更する

ネットワーク認証サービスを使用して、ホスト名およびレルム名を解決できるように、ディレクトリー・サービス (LDAP) サーバー、ドメイン・ネーム・システム (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、以下のステップを完了してください。

1. iSeries ナビゲーターで、**「ユーザーの iSeries サーバー (your iSeries server)」** −> **「セキュリティー」**を展開します。
2. 「**ネットワーク認証サービス**」を右マウス・ボタン・クリックし、「**プロパティー**」を選択します。
3. 「**ホスト解決**」ページで、「**LDAP 検索の使用 (Use LDAP lookup)**」、「**DNS 検索の使用 (Use DNS lookup)**」または「**静的マッピングの使用 (Use static mappings)**」(あるいはこれらすべて) を選択します。
4. ホスト解決タイプとして「**LDAP 検索の使用**」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します。たとえば、ディレクトリー・サーバーに有効な名前は ldapsrv.ordept.myco.com のようになります。有効なポート番号は 1 〜 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。
5. ホスト解決タイプとして「**DNS 検索の使用**」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。
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、レルムの名前および対応する DNS 名を入力します。たとえば、ホスト名は mypc.mycompanylan.com、レルム名は ORDEPT.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。たとえば、myco.lan.com で終わるすべてのマシンが ORDEPT.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 ORDEPT.MYCO.COM と入力できます。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 とレルム名の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**」をクリックします。

暗号化設定を追加する

» チケット認可チケット (TGT) およびチケット認可サービス (TGS) の暗号化タイプを選択することができます。暗号化によって、識別不可にすることでネットワーク間を流れるデータを隠します。クライアントはデータを暗号化し、サーバーがそれを復号します。暗号化が正しく処理されるようにするには、 KDC 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。暗号化タイプは、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。以下のステップを完了すると、チケットの他の暗号化値を構成に追加できます。

1. iSeries ナビゲーターで、**「ユーザーの iSeries サーバー (your iSeries server)」** -> **「セキュリティー」**を展開します。
2. 「**ネットワーク認証サービス**」を右マウス・ボタン・クリックし、「**プロパティー**」を選択します。
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認可チケットまたはチケット認可サービスのいずれかのリストから暗号化値を選択します。
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します。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。

«

チケット認可チケットを取得または更新する

» **kinit** コマンドによって、Kerberos チケット認可チケットを取得または更新します。 **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鍵配布センター (KDC) 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ない場合、信任状キャッシュが再度初期化され、KDC から受け取った新しいチケット認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ければ、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 *nwndnhnmns* 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、いくつかの要素を省略することは可能です (たとえば *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。

Jsmith というプリンシパルのために存続時間が 5 時間のチケット認可チケットを取得するには、

Qshell コマンド行で次のように入力します。

```
kinit -l 5h Jsmith
```

または

iSeries コマンド行で、次のように入力します。

```
call qsys/qkrbkinit parm('-l' '5h' 'Jsmith')
```

使用法および制約事項については、この Qshell コマンドの使用法を参照してください。

kinit

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

Qshell コマンド **kinit** は、Kerberos のチケット認可チケットを取得または更新します。

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選択できません。

-p
チケットはプロキシー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、プロキシーのチケットは不可能です。

-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・アドレスのリストが記述されません。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・リストが記述されます。初期チケットにアドレス・リストが記述されていると、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、 kinit 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、チケット・プリンシパルのパスワードをユーザーが入力しなければなりません。

-t keytab
キー・テーブルの名前。 -k オプションが指定されているにもかかわらずこのオプションが指定されていないと、デフォルトのキー・テーブルが使われます。 -t オプションを指定すると、-k オプションも指定されたことになります。

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、プリンシパルは信任状キャッシュから取得されます。

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なか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なか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) 使用するキャッシュ・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

任意の実行中プロセスから Kerberos プロトコルが信任状キャッシュ・ファイルを見つけることができるように、ホーム・ディレクトリーの **krb5ccname** というファイルには信任状キャッシュ・ファイルの名前が記述されています。キャッシュ・ファイルの名前を記述したファイルの格納場所は **EUV_SEC_KRB5CCNAME_FILE** 環境変数を通じて変更できます。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する ***X** 権限を持ち、キャッシュ・ファイル名を格納したファイルに対する ***R** 権限を持っていなければなりません。信任状ファイル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する ***WX** 権限を必要とします。

メッセージ

- option_name オプションの値が必要です。
- 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査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 を取得できません。
- 初期チケットが用意されていません。
- プリンシパル名を指定してください。
- 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 を変換できません。
- principal_name のパスワードが間違っています。
- 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 に格納できません。
- 時間値が無効です。

このコマンドの使用例については、 チケット認可チケットを取得または更新するを参照してください。

信任状キャッシュまたは keytab ファイルを表示する

klist コマンドは 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。

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、

Qshell コマンド行で次のように入力します。

```
klist -f -a
```

または

iSeries コマンド行で、次のように入力します。

```
call qsys/krbklist parm('-f' '-a')
```

使用法および制約事項については、この Qshell コマンドの使用法を参照してください。

klist

構文

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

デフォルトの共通権限 : *USE

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。

オプション

-a
信任状キャッシュ内のチケットをすべて表示します。有効期限が切れたチケットも表示されます。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部分を表示します。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は指定できません。

-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	チケットが有効でない
A	使用された事前認証
O	サーバーを委任できる
C	KDC 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
コマンドの結果を表示せず、信任状キャッシュ内に有効なチケット認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は指定できません。

-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。filename 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

任意の実行中プロセスから Kerberos ランタイムが信任状キャッシュ・ファイルを見つけることができるように、ホーム・ディレクトリーの **krb5ccname** というファイルには信任状キャッシュ・ファイルの名前が記述されています。キャッシュ・ファイルの名前を記述したファイルの格納場所は **EUV_SEC_KRB5CCNAME_FILE** 環境変数を通じて変更できます。このファイルにアクセスするには、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する ***X** 権限を持ち、キャッシュ・ファイル名を格納したファイルに対する ***R** 権限を持っていなければなりません。信任状ファイル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する ***WX** 権限を必要とします。

メッセージ

- option_name オプションの値が必要です。
- 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 を取得できません。
- 信任状キャッシュ file_name からプリンシパル名を取り出せません。
- 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 を変換できません。

このコマンドの使用例については、 信任状キャッシュまたは keytab ファイルを表示するを参照してください。

keytab ファイルを管理する

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、キー・テーブルのエントリーを表示する際に使用されます。

たとえば、レルム ORDEPT.MYCO.COM のホスト kdc1.ordept.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、

Qshell コマンド行で次のように入力します。

```
keytab add krbsvr400/kdc1.ordept.myco.com@ORDEPT.MYCO.COM
```

または

iSeries コマンド行で次のように入力します。

```
call qsys/qkrbkeytab parm('add' 'krbsvr400/kdc1.ordept.myco.com@ORDEPT.MYCO.COM')
```

KDC 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。

使用法および制約事項については、この Qshell コマンドの使用法を参照してください。

keytab

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

Qshell コマンド **keytab** はキー・テーブルを管理します。

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しなければなりません。

-v
キーのバージョン番号。このオプションを指定しないと、次のバージョン番号が割り当てられます。キーを削除する場合、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・テーブルのリストを表示する場合、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
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* のいずれかを指定してください。
- *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* オプションの値が必要です。
- 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してください。
- 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 ファイルを管理するを参照してください。

Kerberos パスワードを変更する

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。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、 KDC をインストールして構成した時に構成されます。そのシステムに対応する資料を参照してください。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。

チケット認可サービスのプリンシパル (krbtgt/realm) のパスワードは **kpasswd** コマンドによって変更できません。

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 コマンド行で次のように入力します。

```
kpasswd
```

または

コマンド行で次のように入力します。

```
call qsys/qkrbkpsswd
```

別のプリンシパルのパスワードを変更する場合 :

Qshell コマンド行で次のように入力します。

```
kpasswd jsmith@ordept.myco.com
```

または

コマンド行で次のように入力します。

```
call qsys/qkrbkpsswd parm ('jsmith@ordept.myco.com')
```

このコマンドの使用時の詳細については、 kpasswd 使用法を参照してください。

kpasswd

構文

```
kpasswd [-A ] [principal]
```
デフォルトの共通権限 : *USE

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。

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・アドレスのリストが記述されません。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・リストが記述されます。初期チケットにアドレス・リストが記述されていると、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 のパスワードが間違っています。
- 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 パスワードを変更する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・ファイルを削除する

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。ユーザーは、 kdestroy コマンドを使用して定期的に古い信任状を削除する必要があります。

-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。有効期限から *time_delta* の時間を経過したチケットだけを格納しているファイルはすべて削除されます。 *time_delta* は *nwndnhnmns* 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、いくつかの要素を省略することは可能です (たとえば *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。

デフォルトの信任状キャッシュを削除するには、
Qshell コマンド行で次のように入力します。

```
kdestroy
```

または

iSeries コマンド行で、次のように入力します。

```
call qsys/qkrbkdstry
```

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 コマンド行で次のように入力します。

```
kdestroy -e 1d
```

または

iSeries コマンド行で、次のように入力します。

```
call qsys/qkrbkdstry parm ('e' '-1d')
```

使用法および制約事項については、この Qshell コマンドの使用法を参照してください。

kdestroy

構文

```
kdestroy [-c cache_name] [-e time_delta]
```
デフォルトの共通権限 : *USE

Qshell コマンド **kdestroy** は Kerberos 信任状キャッシュを破棄します。

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は指定できません。

-e time_delta
有効期限が切れてから少なくとも time_delta 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)、デフォルトの設定では、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・ファイルの格納場所は KRB5CCNAME 環境変数を通じて変更できます。

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格納されていない場合、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格納されている場合は、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

任意の実行中プロセスから Kerberos プロトコルが信任状キャッシュ・ファイルを見つけることができるように、ホーム・ディレクトリーの krb5ccname というファイルには信任状キャッシュ・ファイルの名前が記述されています。iSeries 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・ファイルの名前を記述したファイルの格納場所は _EUV_SEC_KRB5CCNAME_FILE 環境変数を通じて変更できます。このファイルにアクセスするには、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する ***X** 権限を持ち、キャッシュ・ファイル名を格納したファイルに対する ***R** 権限を持っていなければなりません。

メッセージ

- 信任状キャッシュ *cache_file_name* を変換できません。

- 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* オプションの値が必要です。
- *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、 有効期限が切れた信任状キャッシュ・ファイルを削除するを参照してください。

LDAP ディレクトリー内の Kerberos サービス・エントリーを管理する

ksetup コマンドはディレクトリー・サービス (LDAP) 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変換されるように、完全修飾の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われます。

addkdc host-name:port-number realm-name
このサブコマンドは、指定したレルム用の KDC エントリーを追加します。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変換されるように、完全修飾の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われます。

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 KDC 定義を削除します。レルム名を指定しなければ、デフォルトのレルム名が使われます。

delkdc host-name realm-name
このサブコマンドは、指定したホストの KDC 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われます。

listhost realm-name
このサブコマンドはレルムのホスト・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われます。

listkdc realm-name
このサブコマンドはレルムの KDC 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われます。

exit
このサブコマンドは ksetup コマンドを終了します。

例

管理者のディレクトリー・サービス (LDAP) 管理者 ID とパスワード verysecret を使用して、レルム ORDEPT.MYCO.COM の KDC としてホスト kdc1.ordept.myco.com をサーバー ldapserv.ordept.myco.com に追加するには、以下のステップ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.ordept.myco.com -n
CN=Administrator -p verysecret
```

または

1. iSeries コマンド行で、次のように入力します。

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

2. ディレクトリー・サービス (LDAP) サーバーに正常に到達したら、サムコマンドのプロンプトが表示されます。次のように入力してください。

```
addkdc kdc1.ordept.myco.com ORDEPT.MYCO.COM
```

使用法および制約事項については、この Qshell コマンドの使用法を参照してください。

ksetup

構文

```
ksetup -h host-name -n bind-name -p bind-password -e
```
デフォルトの共通権限 : *USE

Qshell コマンド **ksetup** は、Kerberos レルム用のディレクトリー・サービス (LDAP) ディレクトリーにある Kerberos サービス・エントリーを管理します。

オプション

-h
ディレクトリー・サービス (LDAP) 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・サービス (LDAP) サーバーが使われます。

-n
ディレクトリー・サービス (LDAP) 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、ディレクトリー・サービス (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・サービス (LDAP) 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、ディレクトリー・サービス (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・サービス (LDAP) サーバーを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 はすでに存在しています。
- 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 KDC 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 ディレクトリー内の Kerberos サービス・エントリーを管理するを参照してください。

ネットワーク認証サービスのトラブルシューティング

このセクションは、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 Kerberos 認証をサポートする iSeries 固有のアプリケーションに共通の問題に関するトラブルシューティングへのリンクを提供します。

1. 前提条件はすべて完了しています。
2. ユーザーが、iSeries 上にユーザー・プロファイルを持ち、 KDC 上にプリンシパル名を持つことを確認します。iSeries では、 iSeries ナビゲーターのユーザーおよびグループを開くか、コマンド行で WRKUSRPRF を使用してユーザーが存在することを確認します。 Windows (R) システムでは、Active Directory (R) のユーザーおよびコンピューター・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します。
3. iSeries が KDC に接続しているかどうかを、Qshell インタープリターから kinit コマンドを使用して調べます。 kinit が失敗したら、iSeries サービス・プリンシパルが KDC に登録されているかどうかを調べます。登録されていない場合は、KDC にiSeries プリンシパル名を追加できます。

特定のメッセージについては、以下のトピックを参照してください。

- ネットワーク認証サービスのエラーおよび回復
  これらのメッセージは、ネットワーク認証サービス・ウィザードの実行時、または iSeries 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ーを管理するときに出されます。
- アプリケーション接続のエラーおよび回復
  このトピックは、アプリケーションがネットワーク認証サービス、EIM、および一部の iSeries 固有アプリケーションを使用する際に、 iSeries、サービス、またはユーザーが KDC に接続しようとしたときに出される共通エラー・メッセージについて説明します。

ネットワーク認証サービスのエラーおよび回復

これらのメッセージは、ネットワーク認証サービス・ウィザードの実行時、または iSeries 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ーを管理するときに出されます。

メッセージ	回復
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様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、 ネットワーク認証サービスを構成するを参照してください。
KRBWIZ_CRYPTO_NOT_INSTALLED 必要な暗号化製品がシステムにインストールされていません。	Cryptographic Access Provider (572-AC3) をシステムにインストールします。
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、 ネットワーク認証サービスを構成する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 65535 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 項目はすでに存在します。	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 KDC がリストに存在しません。リストから KDC 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。	KDC に有効な名前を入力します。KDC 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 レルム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ルムの名前を入力します。
KrbPropRealmToTrustRequired 信頼するレルム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ルムの名前を入力します。
KrbPropRealmValueRequired レルム名を入力しなければなりません。	レルム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回復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回復

このメッセージは、アプリケーションがネットワーク認証サービスを使用するときに出されます。

問題	回復

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。

iSeries 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。

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回復情報を参照してください。

すでに接続されている iSeries システム上で DRDA/DDM 接続が失敗しました。

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鍵配布センター (KDC) 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。このエラーから回復するには、以下のいずれかのタスクを行います。

1. Kerberos 認証を使用していない場合には、以下の項目を完了してください。
   a. ネットワーク認証サービスの構成に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、以下のステップを完了してください。
   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 KDC 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。**注 :** 現在、iSeries は KDC をサポートしていません。
   b. ステップ 1 で作成したデフォルトのレルムおよび KDC 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 iSeries Access for Windows アプリケーションを構成 (28 ページを参照)します。これで、DRDA/DDM を含むすべての iSeries Access for Windows アプリケーションに Kerberos 認証が設定されます。

すでに接続されている iSeries システム上で QFileSvr.400 接続が失敗しました。

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鍵配布センター (KDC) 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、QFileSvr.400 接続が失敗します。このエラーから回復するには、以下のいずれかのタスクを行います。

1. Kerberos 認証を使用していない場合には、以下の項目を完了してください。
   a. ネットワーク認証サービスの構成に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、以下のステップを完了してください。
   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 KDC 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。**注 :** 現在、iSeries は KDC をサポートしていません。
   b. ステップ 1 で作成したデフォルトのレルムおよび KDC 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 iSeries Access for Windows アプリケーションを構成 (28 ページを参照)します。これで、DRDA/DDM を含むすべての iSeries Access for Windows アプリケーションに Kerberos 認証が設定されます。

CWBSY1011
Kerberos クライアントの信任状が見つかりません。

ユーザーにチケット認可チケット (TGT) がありません。この接続エラーは、ユーザーが Windows (R) 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。このエラーから回復するには、Windows (R) 2000 ドメインにログインしてください。

接続設定の検査時にエラーが起こりました。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。

このエラーから回復するには、以下の項目を完了してください。

1. iSeries ナビゲーターで、**「ユーザーの iSeries (your iSeries)」** －> **「ネットワーク」** －> **「サーバー」** －> **「TCP/IP」**を展開します。
2. 「**ディレクトリー**」を右マウス・ボタン・クリックし、「**プロパティー**」を選択します。
3. 「**概要 (General)**」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確認します。

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こりました。 GLD0232: 重複する接尾部を構成に入れることはできません。 **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。	このエラーから回復するには、以下の項目を完了してください。 1. iSeries ナビゲーターで、**「ユーザーの iSeries (your iSeries)」** −> **「ネットワーク」** −> **「サーバー」** −> **「TCP/IP」**を展開します。 2. 「**ディレクトリー**」を右マウス・ボタン・クリックし、「**プロパティー**」を選択します。 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。
接続設定の検査時にエラーが起こりました。iSeries プログラムの呼び出しで例外が起こりました。呼び出し先プログラムは eimConnect です。詳細は com.ibm.as400.data.PcmlException です。 **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。	このエラーから回復するには、以下の項目を完了してください。 1. iSeries ナビゲーターで、**「ユーザーの iSeries (your iSeries)」**−>**「ネットワーク」**−>**「サーバー」**−>**「TCP/IP」**を展開します。 2. 「**ディレクトリー**」を右マウス・ボタン・クリックし、「**プロパティー**」を選択します。 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。

«

関連情報

Kerberos プロトコルの仕様

Kerberos ネットワーク認証サービス (V5) 。
Internet Engineering Task Force (IETF) は、Kerberos プロトコルを Request for Comment 1510 で正式に定義しています。

Kerberos: ネットワーク認証プロトコル (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記載しており、プロトコルの機能について説明しています。

Generic Security Service (GSS) API の仕様

Kerberos および GSS API の詳細については、以下の情報源を参照してください。

Generic Security Service Application Program Interface Version 2, Update 1 。
Internet Engineering Task Force (IETF) は、GSS API を Request for Comments 2743 で正式に定義しています。

Generic Security Service API : C-bindings 。
Internet Engineering Task Force (IETF) は、GSS API C-bindings を Request for Comments 1509 で指定しています。

Kerberos バージョン 5 GSS-API メカニズム 。
Internet Engineering Task Force (IETF) は、Kerberos バージョン 5 および GSS API の仕様をこの Request for Comments 1964 で定義しています。

Information Center 関連トピック

ネットワーク認証サービスアプリケーション・プログラマブル・インターフェース (API)
この Information Center のトピックは、ネットワーク認証サービス API のリストと、その機能の概説を記載します。

Generic Security Service Application Programmable Interfaces (GSS API)
この Information Center のトピックは、GSS API のリストと、その機能の概説を記載します。

エンタープライズ識別マッピング (EIM)
エンタープライズ識別マッピング (EIM) は、人またはエンティティー (サービスなど) をエンタープライズ全体のさまざまなユーザー・レジストリー内の適切なユーザー ID にマッピングするメカニズムです。 iSeries は、EIM を使用して iSeries インターフェースを使用可能にし、ネットワーク認証サービスを通じてユーザーを認証します。 iSeries およびアプリケーションは、 Kerberos チケットを受け入れて、EIM を使用し、 Kerberos プリンシパルに関連付けられたこのシステム上のユーザー ID を検出することもできます。

特別な条項

» 以下に示す条項は、ネットワーク認証サービスのコードだけに適用されます。このコードは、ライブラリー QSYS 内のプログラム QKRBGSS、ライブラリー QSYSINC のファイル H 内のメンバー KRB5、ディレクトリー /QIBM/ProdData/OS400/NetworkAuthentication/ 内のメッセージ・カタログ skrbdll.cat と skrbkut.cat に入っています。

IBM はネットワーク認証サービスのオブジェクト・コードを現存するままの状態で使用許諾し、商品性の保証や特定の目的への適合性の保証を含む一切の明示もしくは暗黙の保証責任を負わないものとします。

IBM は、このコードの使用が著作権、商業上に秘密、特許権、その他の知的所有権、第三者の財産上または契約上の権利を侵害しないことを保証しません。

このコードの使用にあたっては以下の表記が必要になります。

この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、目的のいかんを問わず、無料で使用し、複製し、変更し、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ます。 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で提供されます。

Copyright 1994 by the Massachusetts Institute of Technology.
Copyright (c) 1994 CyberSAFE Corporation.
Copyright (c) 1993 Open Computing Security Group
Copyright (c) 1990, 1991 by the Massachusetts Institute of Technology.

All rights reserved.

この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、目的のいかんを問わず、無料で使用し、複製し、変更し、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ます。 M.I.T. も、Open Computing Security Group も、 CyberSAFE Corporation も、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で提供されます。

Copyright 1995, 1996 by Richard P. Basch. All Rights Reserved.
Copyright 1995, 1996 by Lehman Brothers, Inc. All Rights Reserved.

この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、目的のいかんを問わず、無料で使用し、複製し、変更し、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 Richard P. Basch、 Lehman Brothers、および 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ます。 Richard P. Basch、 Lehman Brothers、および 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で提供されます。

これらの特別な条項は上記に示したネットワーク認証サービスのコードにのみ適用され、 iSeries またはライセンス内部コードのその他の部分には適用されません。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12