



IBM Systems - iSeries

セキュリティー
シングル・サインオン

バージョン 5 リリース 4





IBM Systems - iSeries

**セキュリティー
シングル・サインオン**

バージョン 5 リリース 4

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、115 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 5722-SS1) のバージョン 5、リリース 4、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も適用されます。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。

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)

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： IBM Systems - iSeries
Security
Single signon
Version 5 Release 4

発 行： 日本アイ・ピー・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 2006.2

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 2004, 2006. All rights reserved.

© Copyright IBM Japan 2006

目次

シングル・サインオン	1	シナリオ: ISV アプリケーション用のシングル・サインオンを使用可能にする	72
I V5R4 の新機能	1	計画	83
印刷可能な PDF	1	シングル・サインオン環境の構成要件	84
概念	2	ネットワーク認証サービスの計画	85
シングル・サインオンの概説	2	EIM (エンタープライズ識別マッピング) (i5/OS 用) の計画	104
認証	3	シングル・サインオン計画ワークシート	104
権限	4	構成	107
ドメイン	5	管理	108
ID マッピング	6	トラブルシューティング	109
i5/OS の使用可能化	8	関連情報	112
ISV の使用可能化	9	付録. 特記事項	115
シナリオ	10	プログラミング・インターフェース情報	117
シナリオ: シングル・サインオンのテスト環境を作成する	10	商標	117
シナリオ: i5/OS のシングル・サインオンを使用できるようにする	26	使用条件	117
シナリオ: ネットワーク認証サービスおよび EIM を複数システムに反映させる	55		
シナリオ: シングル・サインオン用にマネージメント・セントラル・サーバーを構成する	64		

シングル・サインオン

ユーザーが使用し、管理者が管理しなければならないパスワードを削減する方法として、シングル・サインオン環境をインプリメントすることをお勧めします。この情報では、ネットワーク認証サービス (MIT の Kerberos V5 規格の IBM インプリメンテーション) を EIM (エンタープライズ識別マッピング) とのペアで使用する、i5/OS™ のシングル・サインオン・ソリューションをご紹介します。シングル・サインオン・ソリューションを使用すると、ユーザーが複数のアプリケーションおよびサーバーにアクセスする際に必要とするパスワード数だけでなく、ユーザーが実行しなければならないサインオン数も減少します。

注: 重要なリーガル情報については、113 ページの『コードに関するライセンス情報および特記事項』を参照してください。

V5R4 の新機能

このトピックでは、i5/OS V5R4 のシングル・サインオンの変更点に焦点をあてて説明します。

シングル・サインオンの新規または拡張機能

• EIM およびネットワーク認証サービスの機能拡張

シングル・サインオンの新規または拡張機能の多くは、i5/OS のシングル・サインオン・ソリューションを構成する 2 つのテクノロジーである、EIM およびネットワーク認証サービスの新規および拡張機能から提供されます。特定の機能拡張について詳しくは、次のトピックを参照してください。



- EIM の新機能
- ネットワーク認証サービスの新機能

このトピックの新規または拡張情報

これまででは、ネットワーク認証サービスと EIM の 2 つのテクノロジーが一緒に機能してシングル・サインオン環境を使用できるようにしていたため、シングル・サインオン機能に関する情報は、この両者のトピックで提供されました。この新しい Information Center のトピックでは、シングル・サインオンの構成と使用に関する集中した情報を提供します。この新しいトピックでは、このシングル・サインオン機能を使用する時点および方法を定めるのに役立つ、重要な概念、詳細な計画資料、およびシナリオなど、強化された詳細情報も提供します。

新機能または変更点の確認方法

技術的な変更が行われた箇所を探しやすくするために、本書では以下のマークを使用しています。

-  は、新しい情報または変更情報の始まりを示します。
-  は、新しい情報または変更情報の終わりを示します。

このリリースの新機能または変更に関するその他の情報を探す場合は、「プログラム資料解説書」を参照してください。

印刷可能な PDF

このトピックでは、本書の PDF バージョンをダウンロードし印刷する方法について説明します。

この資料の PDF バージョンを表示またはダウンロードするには、「シングル・サインオン」を選択します。

以下の関連トピックを表示またはダウンロードできます。


- 「EIM (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) は、個人またはエンティティ (サービスなど) を、企業全体のさまざまなユーザー・レジストリー内の該当するユーザー ID にマップするメカニズムです。
- ネットワーク認証サービス (約 2911 KB)。ネットワーク認証サービスにより、システムは既存の Kerberos ネットワークに参加できます。

PDF ファイルの保管

表示用または印刷用に PDF をワークステーションに保存するには、次のようにします。

1. ブラウザーで、PDF を右マウス・ボタンでクリックする (上記のリンクを右マウス・ボタンでクリックする)。
2. PDF をローカルで保管するオプションをクリックする。
3. PDF を保管するディレクトリーにナビゲートする。
4. 「保存」をクリックする。

Adobe Reader のダウンロード

- PDF を表示または印刷するには、システムに Adobe Reader がインストールされている必要があります。
- Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html)  から、無償コピーをダウンロードできます。

概念

シングル・サインオンの基礎概念を確認して、個々の企業でシングル・サインオンの使用を計画する方法の理解を深めてください。

シングル・サインオンでは、複数のサービスとテクノロジーを使用して、ID と権限の管理を単純化するソリューションを実現します。シングル・サインオンの利点、およびこのソリューションの作成に各種サービスを使用する方法を説明します。シングル・サインオンを使用する前に、これらの概念に目を通しておくとう便利です。

シングル・サインオンの概説

ここでは、シングル・サインオン・ソリューションによって障害の軽減を計画している問題点、および社内でのシングル・サインオンの使用によって達成される利点について説明します。

従来のネットワーク環境では、ユーザーがシステムまたはアプリケーションに対して認証されるには、そのシステムまたはアプリケーションによってそのシステムまたはアプリケーション上で定義されるユーザー信任状を提供します。ユーザーが、システムまたはアプリケーションによって管理されるリソースにアクセスしようとする場合は、従来、認証メカニズムと確認メカニズムはいずれも、同じユーザー・レジストリーを使用します。シングル・サインオン環境では、認証メカニズムと権限メカニズムは、システムまたはアプリケーションが管理するリソースにユーザーがアクセスできるようにするのに、同じユーザー・レジストリーを使用する必要はありません。シングル・サインオン環境は、ネットワーク認証サービス (Kerberos 認証) を認証メカニズムとして使用します。シングル・サインオン環境では、認証に使用されるユーザー・レジス

トリーは、システムまたはアプリケーションが定義するレジストリーである必要はありません。従来のネットワーク環境では、これが、権限の問題になりました。

シングル・サインオン・ネットワーク環境では、アプリケーションは、EIM (エンタープライズ識別マッピング) を使用してこの問題を解決します。EIM は、個人またはエンティティを、企業全体の各種レジストリー内の該当するユーザー ID にマッピングすなわち関連付けるメカニズムです。i5/OS のアプリケーション開発者は、EIM を使用して、認証と権限に別々のユーザー・レジストリーを使用するアプリケーションを作成します (ユーザーが別の信任状セットを提供する必要がありません)。シングル・サインオン環境の利点は多数あり、ユーザーにとっての利点だけではありません。管理者とアプリケーション開発者も、シングル・サインオン・ソリューションの恩恵を受けることができます。

ユーザーの利点

シングル・サインオン・ソリューションを使用すると、ユーザーが複数のアプリケーションやサーバーにアクセスする際に必要なサインオン回数が減少します。シングル・サインオンでは、ユーザーがネットワークにサインオンするときに 1 回だけ認証が行われます。EIM を使用すると、ネットワーク内の他のシステムにアクセスするために、ユーザーが複数のユーザー名とパスワードを追跡し、管理する必要が少なくなります。ネットワークに対してユーザーが認証された後、そのユーザーは、これらの別々のシステムに対して複数のパスワードを必要とすることなく、企業全体のサービスとアプリケーションにアクセスできます。

管理者の利点

管理者の場合、シングル・サインオンにより、企業の全体的なセキュリティ管理が単純化されます。シングル・サインオンを使用しない場合、ユーザーは異なるシステムに対して複数のパスワードをキャッシュに入れる場合があります。これは、ネットワーク全体のセキュリティを損なう恐れがあります。管理者は、これらのセキュリティの危険性を小さくするために、ソリューションに時間と費用を費やします。シングル・サインオンにより、認証を管理する際の管理オーバーヘッドを減らすと同時に、ネットワーク全体を保護することができます。さらに、シングル・サインオンにより、忘れてしまったパスワードをリセットする場合の管理コストも減少します。管理者がセットアップ可能なシングル・サインオン環境では、Windows® (Windows 2000 およびそれ以降のリリースの場合) のサインオンにより、ネットワーク全体へのアクセスが可能になり、認証と識別の管理が最小限に抑えられます。

アプリケーション開発者の利点

異機種混合ネットワークで実行する必要があるアプリケーションの開発者の場合、問題は、各層のプラットフォームのタイプが異なる可能性がある、複数層のアプリケーションを作成することです。EIM を利用すると、アプリケーション開発者は、認証に最も適した既存のユーザー・レジストリーを使用すると同時に、権限に異なるユーザー・レジストリーを使用するアプリケーションを自由に作成することができます。アプリケーション固有のユーザー・レジストリー、関連したセキュリティ・セマンティクス、およびアプリケーション・レベル・セキュリティを実現する必要がないので、複数層から成るクロスプラットフォーム・アプリケーションを実現するコストが大幅に減少します。

認証

認証プロセス、およびシングル・サインオン・ソリューションにおける認証の役割を説明します。

認証とは、通常、ユーザー名とパスワードに基づいて、自分自身がだれであるかを示し、それを証明するプロセスです。認証プロセスは、権限プロセスとは異なります。権限プロセスでは、ネットワークまたはシステム・リソースに対するアクセス権が、エンティティまたは個人に対して付与または拒否されます。

シングル・サインオン環境は、ユーザーと管理者の認証のプロセスと管理を簡素化します。ご使用のシステムでシングル・サインオンがインプリメントされている方法のために、ユーザーが入力しなければならない ID やパスワードの数を減らすことができるだけでなく、ユーザーがそう望めば、i5/OS パスワードを使用する必要さえなくなります。ユーザーは、使用するシステムへのアクセスのために覚えておく ID 数とパスワード数が少なくすむので、管理者は、ID とパスワードの問題のトラブルシューティングを行う回数が減ります。

シングル・サインオンが使用可能になっているインターフェースでは、認証方式として Kerberos を使用する必要があります。ネットワーク認証サービスは、Kerberos 認証機能を i5/OS に実装したものです。ネットワーク認証サービスは、鍵配布センター (KDC) と呼ばれる Kerberos サーバーを使用して分散認証メカニズムを提供します。このサーバーは、ネットワーク上のなんらかのサービスに対してユーザー (Kerberos の用語ではプリンシパル) を認証するのに使用されるサービス・チケットを作成します。このチケットは、ネットワーク内でプリンシパルが要求する他のサービスに対して、プリンシパルの ID 証明を提供します。

注: アプリケーション開発者である場合、アプリケーションがシングル・サインオン環境で機能できるようにするときに、他のタイプの認証方式を利用することが可能です。たとえば、アプリケーションがシングル・サインオン環境に参加できるようにする EIM API と連携して、デジタル証明書などの認証方式を使用するアプリケーションを作成できます。

権限

権限プロセス、いくつかの権限方式、およびシングル・サインオン・ソリューションにおける権限の役割を説明します。

権限とは、ネットワークまたはシステム・リソースへのアクセス権をユーザーに付与するプロセスです。大部分の企業では、ユーザーにネットワーク資産へのアクセスを許可するのに、2 段階のプロセスを使用します。このプロセスの最初の段階は、認証です。認証は、ユーザーが企業に対して自分自身を識別するプロセスです。通常、認証では、ユーザーが企業のセキュリティー・コンポーネントに対して ID とパスワードを提供する必要があります。このセキュリティー・コンポーネントは、受信する情報を検証します。認証に成功した後、使用できるプロセス、信任状、または企業に対してすでに認証済みであることの証明に使用するチケットが、ユーザーに発行されます。ユーザー認証の例は、iSeries™ ナビゲーター 接続時の ID とパスワードの要求です。認証が成功した後、ユーザーには、自分のユーザー ID で実行されるジョブが割り当てられます。2 番目の段階は、権限の許可です。認証と権限の違いを認識しておくことが重要です。

権限とは、企業内の資産にアクセスする権限がエンティティーまたは個人にあるかどうかを判別するプロセスです。権限検査が行われるのは、ユーザーが企業に対して認証された後です。これは、権限の許可では、誰がアクセスしようとしているかを企業が認識する必要があるからです。権限検査は必須であり、システムの一部として行われます。ユーザーは通常、アクセスが拒否された場合を除いて、権限検査が行われていることに気付きません。権限の例は、ユーザーが CRTSRCPF QGPL/MYFILE コマンドを使用する場合です。CRTSRCPF コマンドと QGPL ライブラリーで、システムは権限検査を実行します。このコマンドとライブラリーにアクセスする権限がユーザーにない場合、ユーザーの要求は失敗します。

i5/OS シングル・サインオン・ソリューションを実現している企業は、EIM (エンタープライズ識別マッピング) を使用して、企業資産へのユーザー・アクセスを管理します。EIM は権限検査を実行しませんが、ID マッピングにより、企業に対して正常に認証されたユーザーのローカル ID が確立されます。ソース (またはユーザー) は、ローカル ID を通じて受動システム上のアクセス権と権限を受け取ります。たとえば、次のような単純な企業環境であると想定します。

従業員名 (EIM ID)	ソース・ユーザー (EIM ソース)	システム A のターゲット・ユーザー (EIM ターゲット)	従業員の職責	システム A のユーザー・コメント
Susan Doe	SusanD	SecOfficer	IT 機密保護担当者	すべての特殊権限。すべてのファイルと情報にアクセスできる。
Fred Ray	FredR	PrimeAcnt	主任経理担当者	特殊権限なし。すべての給与計算情報にアクセスできる。
Nancy Me	NancyM	PrimePGM	IT アプリケーションのチーム・リーダー	特殊権限なし。企業のすべてのアプリケーション・ソース・ファイルにアクセスできる。
Brian Fa	BrianF	GenAcnt1	経理担当者	特殊権限なし。一部の給与計算情報にアクセスできる。
Tracy So	TracyS	ITPgm2	IT プログラマー	特殊権限なし。企業の一部のアプリケーション・ソース・ファイルにアクセスできる。
Daryl La	DarylL	ITPgm3	IT プログラマー	特殊権限なし。企業の一部のアプリケーション・ソース・ファイルにアクセスできる。
Sherry Te	SherryT	PrimeMKT	営業担当員	特殊権限なし。すべてのマーケティング・データにアクセスできる。

ユーザーとリソース間のすべてのアソシエーションが正しくセットアップされていることが重要です。アソシエーションに誤りがあると、ユーザーは職責の範囲を超えたデータにアクセスできます。大部分の企業では、これはセキュリティの問題です。システム管理者は、EIM マッピングを作成する際に注意し、正しいローカル・レジストリー ID にユーザーをマップしていることを確認する必要があります。たとえば、SecOfficer ID に Susan Doe ではなく、IT プログラマーの Daryl La をマップした場合、システムのセキュリティを損なう恐れがあります。このことから、セキュリティ管理者が企業内の受動システムの保護に引き続き注意しなければならないということが分かります。

ドメイン

ここでは、シングル・サインオン環境に含まれる EIM ドメインと Windows ドメインとの相違点を説明します。

シングル・サインオン環境では、2 つのタイプのドメイン (EIM ドメインと Windows 2000 ドメイン) が重要な役割を果たします。これらの用語のどちらにも、「ドメイン」という語が含まれていますが、これらのエンティティの定義は非常に異なっています。これらの 2 つのタイプのドメインの違いを理解するには、下記の説明を使用してください。

EIM ドメイン

EIM ドメインとは、EIM ID、EIM アソシエーション、およびそのドメインで定義されている EIM ユーザー・レジストリー定義を含む、データの集合です。このデータは、そのドメインで定義されるネットワーク内の任意のシステムで実行できる、IBM® Directory Server for iSeries などの Lightweight Directory Access Protocol (LDAP) サーバーに保管されます。管理者は、ドメインに加わるように、i5/OS などのシステム (EIM クライアント) を構成することができます。その結果、システムとアプリケーションは、EIM 探索操作と ID マッピングにドメイン・データを使用することができます。

Windows2000 ドメイン

シングル・サインオンでは、Windows 2000 ドメインは、クライアントとサーバーとして動作する複数のシステム、およびそれらのシステムが使用する各種サービスとアプリケーションを含む Windows ネットワークです。Windows 2000 ドメイン内にある、シングル・サインオンに関連したコンポーネントの一部は、次のとおりです。

レルム レルムは、マシンとサービスの集合です。レルムの主な目的は、クライアントとサービスを認証することです。各レルムは、1 つの Kerberos サーバーを使用して、その特定のレルムのプリンシパルを管理します。

Kerberos サーバー

鍵配布センター (KDC) と呼ばれる Kerberos サーバーは、Windows 2000 サーバーに常駐するネットワーク・サービスであり、ネットワーク認証サービス用のチケットと一時セッション鍵を提供します。Kerberos サーバーは、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した秘密鍵を保持します。このサーバーは、認証サーバーと発券サーバーで構成されます。Kerberos サーバーは、Microsoft® Windows Active Directory を使用して、Kerberos ユーザー・レジストリーに情報を保管し、管理します。

Microsoft Windows Active Directory

Microsoft Windows Active Directory は、Kerberos サーバーと一緒に、Windows 2000 サーバーに常駐する LDAP サーバーです。Active Directory は、Kerberos ユーザー・レジストリーに情報を保管し、管理するのに使用されます。Microsoft Windows Active Directory は、デフォルトのセキュリティー・メカニズムとして Kerberos 認証を使用します。したがって、Microsoft Active Directory を使用してユーザーを管理する場合、すでに Kerberos テクノロジーを使用していることとなります。

関連情報

EIM (エンタープライズ識別マッピング) の概要

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

ID マッピング

シングル・サインオン環境における ID マッピング・プロセスの働きについて説明します。

ID マッピングは、企業内のユーザー ID 間で定義された関係を使用して、アプリケーションとオペレーティング・システムが、1 つのユーザー ID を別の関連したユーザー ID にマップできるようにするプロセスです。ID 間でマップする機能は、認証プロセスと権限プロセスを区別できるようにするので、シングル・サインオンの使用可能化には非常に重要です。ID マッピングにより、ユーザーは、システムにログオンし、1 つのユーザー ID の信任状に基づいて認証され、新しい信任状を提供しなくてもそれ以降のシステムまたはリソースにアクセスできるようになります。代わりに、認証された ID は、要求されたシステムまたはリソースの該当する ID にマップされます。2 番目のシステムへのログオンに別の信任状を提示する必要がないので、ユーザーに便利であるだけでなく、2 番目のシステムに対するユーザーの権限が、適切な ID によって処理されます。

シングル・サインオンを実現するには、EIM ドメイン内で所定の EIM データを作成して、シングル・サインオン環境内で ID を適切にマップするのに必要な関係を定義する必要があります。これを行うと、EIM はそのデータを使用して、シングル・サインオンのマッピング探索操作を実行できることが確実になります。EIM を使用して、企業内のユーザー ID 間の関係を定義するアソシエーションを作成します。ID マッピングに求める機能に応じて、これらの関係を定義するのに、ID アソシエーションとポリシー・アソシエーションの両方を作成できます。

ID アソシエーション

ID アソシエーションにより、個人に対して定義される EIM ID を使用して、ユーザー ID 間の 1 対 1 の関係を定義できます。ID アソシエーションを使用すると、ユーザー ID の ID マッピングを制御することができます。特殊権限やその他の特権があるユーザー ID を個人が持っている場合は特に、ID アソシエーションが便利です。これらのアソシエーションは、ユーザー ID がマップされる方法を決定します。一般的な ID マッピング状況では、ユーザー ID を認証するためにソース・アソシエーションを作成します。また、認証するユーザー ID を、他のシステムやリソースへの許可アクセス用の適切なユーザー ID にマップするために、ターゲット・アソシエーションを作成します。たとえば、通常、EIM ID と対応するユーザー ID 間で次の ID アソシエーションを作成できます。

- ユーザーがネットワークにログインし、ネットワークに対して認証されるときに使用する ID である、ユーザーの Kerberos プリンシパルのソース・アソシエーション。
- ユーザーがアクセスする各種ユーザー・レジストリー内のユーザー ID ごとのターゲット・アソシエーション (たとえば、Windows 2000 ユーザー・プロファイル)。

次に、ID マッピング・プロセスが ID アソシエーションに対してどのような働きをするかの例を示します。Myco, Inc のセキュリティ管理者が、従業員の EIM ID (John Day) を作成するとします。この EIM ID は、この企業の John Day を一意的に識別します。管理者は、John Day ID と、社内で彼が日常使用する 2 つのユーザー ID と間の ID アソシエーションを作成します。これらのアソシエーションは、ユーザー ID がどのようにマップされるかを定義します。管理者は、Windows ID のソース・アソシエーション (Kerberos プリンシパル)、および Windows 2000 ユーザー・プロファイルのターゲット・アソシエーションを作成します。これらのアソシエーションにより、Windows ID を Windows 2000 ユーザー・プロファイルにマップすることができます。

John Day は、毎朝、適切なユーザー名とパスワードを使用して Windows 2000 ワークステーションにログオンします。John Day は、ログオンすると、iSeries Access for Windows を始動し、Windows 2000 を使用して Windows 2000 システムを操作します。シングル・サインオンが使用可能になっているので、ID マッピング・プロセスでは、彼の認証済み Windows ID を使用して、関連した Windows 2000 ユーザー・プロファイルを検出し、Windows 2000 に対して透過的に彼を認証し、許可します。

ポリシー・アソシエーション

ポリシー・アソシエーションにより、1 つ以上のユーザー・レジストリー内のユーザー ID のグループと、別のユーザー・レジストリー内の特定のターゲット・ユーザー ID との間に、多対 1 の関係を定義できます。一般に、アプリケーションに対する同じレベルの権限を必要とするユーザーのグループから、該当する権限を持つ 1 つのユーザー ID にマップするために、ポリシー・アソシエーションを使用します。

次に、ポリシー・アソシエーションを定義する場合の ID マッピングの働きの例を示します。Myco, Inc. の受注部門の複数の社員はすべて、サーバー上の Windows 2000 で実行される Web ベース・アプリケーションにアクセスするために、同じタイプの権限が必要です。これらのユーザーには、現在、Order_app という名前の 1 つのユーザー・レジストリーに、この目的のためのユーザー ID があります。管理者は、Order_app ユーザー・レジストリー内のすべてのユーザーを、1 つの Windows 2000 ユーザー・プロファイルにマップするために、デフォルトのレジストリー・ポリシー・アソシエーションを作成します。この Windows 2000 ユーザー・プロファイル SYSUSER は、このグループのユーザーに必要な最小限の権限を提供します。この単一構成ステップを実行すると、管理者は、Web ベース・アプリケーションのすべてのユーザーが、必要な権限レベルで、必要なアクセス権を持つことを保証できます。しかし、ユーザーごとに個別の Windows 2000 ユーザー・プロファイルを作成し、保持する必要がないので、管理者にも利点があります。

関連情報

EIM ID

EIM レジストリー定義

EIM アソシエーション

i5/OS の使用可能化

シングル・サインオンを使用可能にする場合の i5/OS の考慮事項、およびシングル・サインオン環境に加わることができる i5/OS アプリケーションとプログラムについて説明します。

i5/OS における EIM (エンタープライズ識別マッピング) と Kerberos (ネットワーク認証サービスとも呼ばれる) の実現により、真のマルチ層シングル・サインオン環境が得られます。ネットワーク認証サービスは、Kerberos および Generic Security Service (GSS) API を IBM が実現したものです。EIM を使用して、Kerberos プリンシパルと i5/OS ユーザー・プロファイル間のマッピングを提供するアソシエーションを定義できます。次に、このアソシエーションを使用して、どの EIM ID がローカル i5/OS ユーザー・プロファイルまたは Kerberos プリンシパルに対応するかを決定できます。これは、サーバー上の i5/OS でシングル・サインオンを使用可能にする利点の 1 つです。

i5/OS でのシングル・サインオンの使用可能化

シングル・サインオン環境を使用可能にするために、IBM は、連携して機能する 2 つのテクノロジーを利用します。すなわち、EIM とネットワーク認証サービスです。ネットワーク認証サービスは、IBM が Kerberos と GSS API を実現したものです。これらの 2 つのテクノロジーを構成すると、管理者はシングル・サインオン環境を使用可能にすることができます。Windows 2000、XP、AIX®、および zSeries® は、Kerberos プロトコルを使用して、ネットワークに対してユーザーを認証します。Kerberos には、ネットワークに対してプリンシパル (Kerberos ユーザー) を認証する、ネットワーク・ベースの安全な鍵配布センターを使用する必要があります。ユーザーが KDC に対して認証されたという事実は、Kerberos チケットによって表されます。チケットは、ユーザーから、チケットを受け入れるサービスに渡すことができます。チケットを受け入れるサービスは、チケットを使用して、(Kerberos ユーザー・レジストリーとレルム内で) ユーザーが主張する人物を判別し、実際に、主張する人物であるかどうかを判別します。

ネットワーク認証サービスにより、サーバーは Kerberos レルムに加わることができます。一方、EIM は、これらの Kerberos プリンシパルを、社内全体でそのユーザーを表す単一の EIM ID に関連付けるためのメカニズムを提供します。その他のユーザー ID (たとえば、i5/OS ユーザー名) をこの EIM ID に関連付けることもできます。これらのアソシエーションに基づいて、EIM は、どの i5/OS ユーザー・プロファイルが、Kerberos プリンシパルによって表される個人またはエンティティを表すかを、i5/OS とアプリケーションが判別するメカニズムを提供します。EIM 内の情報は、EIM ID をルートとするツリーと見なすことができます。また、EIM ID に関連したユーザー ID のリストは、分岐と見なすことができます。

サーバーのシングル・サインオンを使用可能にすると、i5/OS ユーザー・プロファイルを管理するタスクを単純化し、ユーザーが複数の i5/OS アプリケーションとサーバーにアクセスするのに必要なサインオン回数が減ります。さらに、各ユーザーがパスワード管理に要する時間が短くなります。シングル・サインオンにより、各ユーザーは、アプリケーションとサーバーにアクセスするために記憶し、使用するパスワードが少なくなり、それによって iSeries での作業が簡単になります。

シングル・サインオンが現在使用可能になっている i5/OS クライアント・アプリケーションとサーバー・アプリケーション

- i5/OS Host Servers (5722-SS1 オプション 12): iSeries Access for Windows と iSeries ナビゲーター によって現在使用されています。
- Telnet サーバー: 現在、PC5250 と IBM WebSphere® Host On-Demand Version 8: Web Express Logon 機能によって使用されています。

- Open DataBase Connectivity (ODBC): ODBC を通じた i5/OS データベースへのシングル・サインオン・アクセスを可能にします。
- Java™ Database Connectivity (JDBC): ODBC を通じた i5/OS データベースへのシングル・サインオン・アクセスを可能にします。
- 分散リレーショナル・データベース体系™ (DRDA®): ODBC を通じた i5/OS データベースへのシングル・サインオン・アクセスを可能にします。
- QFileSrv.400

ISV の使用可能化

ここでは、シングル・サインオンを使用可能にする場合の ISV に関する考慮事項、および、シングル・サインオン環境に加わることができるアプリケーションとプログラムを ISV が作成する方法を説明します。

独立ソフトウェア販売会社 (ISV) であれば、顧客の多くが、シングル・サインオン環境を実装して、シングル・サインオンが提供するコストと時間の利点を利用していることが分かっています。顧客が必要とするソリューションを引き続き提供できるようにするには、シングル・サインオン環境に加わるように自社のアプリケーション製品を設計する必要があります。

アプリケーションが i5/OS シングル・サインオン環境に加わることを可能にするには、次のタスクを実行する必要があります。

i5/OS サーバー・アプリケーションで EIM を使用可能にする

シングル・サインオン環境の基盤の 1 つは、EIM (エンタープライズ識別マッピング) です。EIM は、個人またはエンティティを、企業全体の各種レジストリー内の該当するユーザー ID にマッピングすなわち関連付けるメカニズムです。i5/OS のアプリケーション開発者は、EIM を使用して、認証と権限に別々のユーザー・レジストリーを使用するアプリケーションを作成します (ユーザーが別の信任状セットを提供する必要がありません)。EIM は、これらの ID マッピング関係を作成し、管理するための API とともに、アプリケーションがこの情報を照会するのに使用する API も提供します。EIM API を使用して社内のユーザー ID の探索操作を実行するアプリケーションを作成できます。

i5/OS サーバー・アプリケーションとクライアント・アプリケーションが共通の認証メカニズムを使用できるようにする

アプリケーションのシングル・サインオン環境に必要な共通の認証メカニズムを自由に選択できますが、i5/OS シングル・サインオン環境は、Windows 2000 ドメインを備えた統合シングル・サインオン環境を提供するネットワーク認証サービス (Kerberos) に基づきます。i5/OS と同じ安全な統合シングル・サインオン環境にアプリケーションを参加させたい場合、アプリケーションの認証メカニズムとしてネットワーク認証サービスを選択してください。アプリケーションに選択できる各種認証方式の例は、次のとおりです。

ネットワーク認証サービス

EIM アプリケーション・プログラミング・インターフェース (API) をネットワーク認証サービスと一緒に使用して、シングル・サインオン環境に完全に加わることができるアプリケーションを作成する方法を習得するには、『シナリオ: ISV アプリケーション用のシングル・サインオンを使用可能にする』を使用してください。このシナリオには、疑似コード (プログラムの完成に使用できる疑似コードとコードの断片のサンプル) を含めて、ISV コード例が含まれています。

デジタル証明書

認証方式としてデジタル証明書を使用するアプリケーションを、シングル・サインオン環

境用に開発することが可能です。デジタル証明書を使用した認証に必要なコードをプログラムに挿入するには、デジタル証明書管理 API を使用する必要があります。

Lightweight Directory Access Protocol (LDAP)

認証方式としてディレクトリー・サーバーを使用するアプリケーションを、シングル・サインオン環境用に開発することが可能です。ディレクトリー・サーバーを使用した認証に必要なコードをプログラムに挿入するには、Lightweight Directory Access Protocol (LDAP) API を使用する必要があります。

シナリオ

この情報は、代表的なシングル・サインオンのインプリメンテーション状況を説明するシナリオを検討するときに使用し、ご使用のサーバー・セキュリティー・ポリシーの一部としてユーザー独自の証明書のインプリメンテーションを計画する際に役立ててください。

これらのシナリオでは、企業内でのシングル・サインオンの構成および使用について、論理的に展開します。これらのシナリオはすべてネットワーク管理者のモデルですが、シングル・サインオン環境に参加できるアプリケーションを作成する際に開発者が行うべき作業を実証する、アプリケーション開発者用のシナリオもあります。

シナリオ: シングル・サインオンのテスト環境を作成する

このシナリオでは、ネットワーク認証サービスおよび EIM を構成して、基本的なシングル・サインオンのテスト環境を作成します。全社的なシングル・サインオンをインプリメントする前に、小規模のシングル・サインオン環境の構成から、問題の基本的な理解を得ることができます。

状況

John Day は、大型卸売り会社のネットワーク管理者です。現在、彼は、パスワードを忘れたなど、パスワードやユーザー ID 問題の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。このネットワークは、いくつかの iSeries システムとユーザーが Microsoft Windows Active Directory に登録される Windows 2000 サーバーから構成されます。調査によれば、Microsoft Active Directory は、Kerberos プロトコルを使用して Windows ユーザーを認証することが分かります。iSeries が、ネットワーク認証サービスという Kerberos 認証のインプリメンテーションを基に、EIM と組み合わせて、シングル・サインオン・ソリューションを提供していることも分かります。

シングル・サインオンを使用した場合の利点は刺激的です。しかし、これを全社的に使用する前に、シングル・サインオンの構成と使用方法を完全に理解する必要があります。したがって、まずテスト環境を構成することにします。

社内のいろいろなグループを考慮した後、受注部門のテスト環境を作成することに決めます。受注部門の従業員は、1 つの iSeries システム上の複数のアプリケーションを使用して、送られてくる顧客オーダーを処理しています。したがって、受注部門には、シングル・サインオンのテスト環境を作るのにふさわしい状況があり、これを利用すれば、シングル・サインオンの働き方と、シングル・サインオンの全社的なインプリメンテーションの計画方法の理解を深めることができます。

シナリオの利点

- 小規模のシングル・サインオンには、シングル・サインオン環境を大規模に作成する前に、その完全な利用方法の理解を深める上でいくつかの利点が認められます。
- シングル・サインオンの全社的なインプリメントを正常、かつ迅速に行う場合に、使用する必要がある計画プロセスの理解を深められます。

- シングル・サインオンの全社的なインプリメントの学習曲線を最小限に抑えます。

目的

MyCo, Inc. のネットワーク管理者として、少数のユーザーおよび単一 iSeries システムによるテスト用の小規模シングル・サインオン環境を作成する必要があります。ユーザー ID がテスト環境内で正しくマップされることを確認するために、完全なテストを行う必要があります。最終的には、この構成に基づいてテスト環境を拡張し、企業内の他のシステムおよびユーザーを組み込みます。

このシナリオの目的は次のとおりです。

- iSeries A として知られる iSeries システムは、MYCO.COM レルム内の Kerberos を使用して、このシングル・サインオンのテスト環境に参加するユーザーおよびサービスを認証できなければなりません。システムが Kerberos を使用できるようにするには、iSeries A 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。
- iSeries A 上のディレクトリー・サーバーは、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。

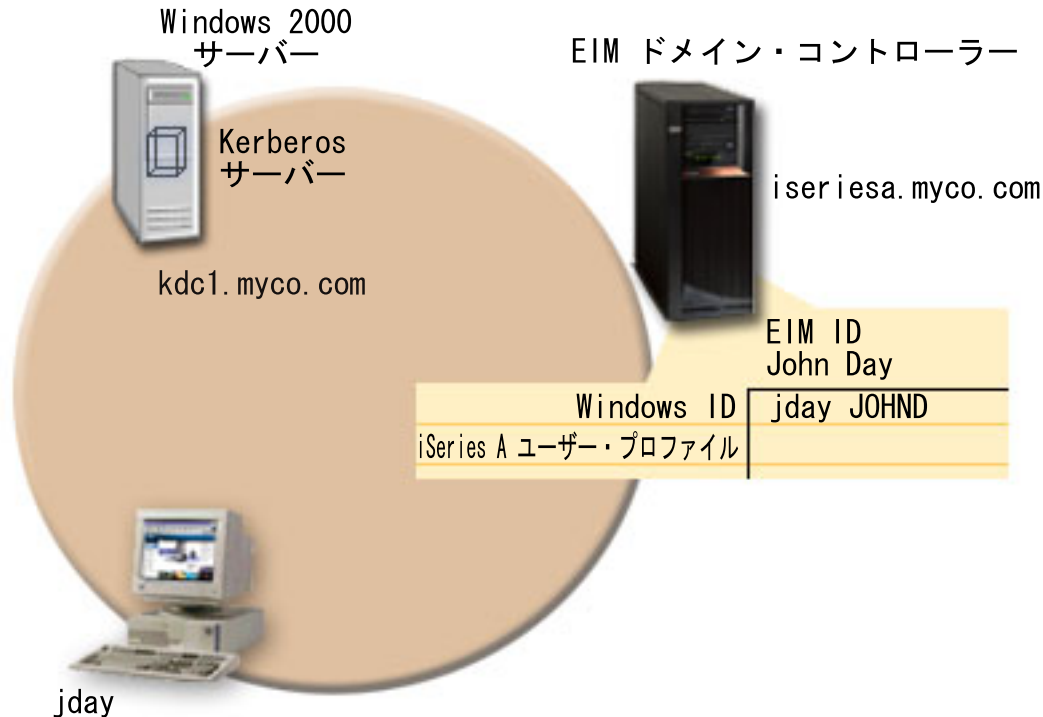
注: 5 ページの『ドメイン』を参照して、EIM ドメインおよび Windows 2000 ドメインが、ともにシングル・サインオン環境に適合する方法を確認してください。

- iSeries A のユーザー・プロファイル 1 つと Kerberos プリンシパル 1 つを、それぞれ単一 EIM ID にマップする必要があります。
- ユーザーを iSeries 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

以下の図で、このシナリオのネットワーク環境を説明します。

レルム = MYCO.COM



この図で、このシナリオに関連する以下の諸点を説明します。

企業に定義された EIM ドメイン・データ

- ISERIESA.MYCO.COM という iSeries A の EIM レジストリー定義。
- MYCO.COM という Kerberos レジストリーの EIM レジストリー定義。
- John Day という EIM ID。この ID で、MyCo. の管理者である、John Day を一意的に識別します。
- Windows 2000 サーバー上の jday Kerberos プリンシパルのソース・アソシエーション。
- iSeries A 上の JOHND ユーザー・プロファイルのターゲット・アソシエーション。

Windows 2000 サーバー

- ネットワークの鍵配布センター (KDC) としても知られている、Kerberos サーバー (kdc1.myco.com) として行動します。
- Kerberos サーバーのデフォルト・レルムは MYCO.COM です。
- jday の Kerberos プリンシパルは、Windows 2000 サーバーの Kerberos サーバーに登録されます。このプリンシパルは、EIM ID、John Day へのソース・アソシエーションの作成に使用されます。

iSeries A

- 次のオプションおよびライセンス製品をインストールした i5/OS バージョン 5 リリース 4 (V5R4) を実行します。

- i5/OS Host Servers (5722-SS1 オプション 12)
- Qshell Interpreter (5722-SS1 オプション 30)
- iSeries Access for Windows (5722-XE1)

注: このシナリオは、OS/400® V5R2 または i5/OS V5R3 を実行するサーバーを使用してインプリメントできます。しかし、i5/OS V5R4 機能拡張のために、構成ステップによって若干異なるものもあります。

- iSeries A の IBM Directory Server for iSeries (LDAP) 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。
- iSeries A は、EIM ドメイン、MyCoEimDomain に参加します。
- iSeries A のプリンシパル名は krbsvr400/iseriasa.myco.com@MYCO.COM です。
- JOHND のユーザー・プロファイルは iSeries A にあります。このユーザー・プロファイルと EIM ID、John Day の間にターゲット・アソシエーションを作成します。
- i5/OS ユーザー・プロファイル、JOHND、(/home/JOHND) のホーム・ディレクトリーは iSeries A 上に定義されます。

シングル・サインオン管理に使用するクライアント PC

- Microsoft Windows 2000 オペレーティング・システムを実行します。
- i5/OS V5R4 iSeries Access for Windows (5722-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 iSeries 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
- 管理者 John Day の 1 次ログオン・システムとして使用されます。
- MYCO.COM レルム (Windows ドメイン) の一部として構成されます。

前提条件および前提事項

このシナリオを正常にインプリメントするには、次の前提条件および前提事項が満たされる必要があります。

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など、すべてのシステム要件が検査されている。

ライセンス・プログラムがインストールされていることを検査するには、以下のことを行ってください。

- a. iSeries ナビゲーター で、「iSeries server」 → 「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」と展開する。
 - b. 必要なライセンス・プログラムがすべてインストールされていることを確認する。
2. 必要なハードウェア計画およびセットアップがすべて完了している。
 3. TCP/IP および基本的なシステム・セキュリティが、システムごとに構成されテストされている。
 4. これまでに iSeries 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、これまでに iSeries 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、すでにディレクトリー・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、構成ステップ内の該当する個所で注記されます。

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

注: Kerberos 認証にホスト・テーブルを使用すると、ネーム解決エラーまたはその他の問題を起こすことがあります。

構成ステップ

注: 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) の概念を含む、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。このシナリオを続ける準備ができている場合は、以下のステップを実行してください。

関連情報

ホスト名の解決に関する考慮事項

EIM (エンタープライズ識別マッピング)

ネットワーク認証サービス

計画ワークシートに記入する


次の計画ワークシートは、一般のシングル・サインオン計画ワークシートを基にして、このシナリオに合うように調整したものです。これらの計画ワークシートで、このシナリオで説明するシングル・サインオンのインプリメンテーションを準備する際に収集する必要がある情報、および行うべき判断を実証します。正常なインプリメンテーションを確保するには、構成作業を行う前に、ワークシートのすべての前提条件項目に「はい」で応答でき、かつワークシートの記入に必要なすべての情報を収集している必要があります。

注: 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) の概念を含む、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。

表 1. 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	応答
i5/OS は V5R4 (5722-SS1) ですか?	はい
以下のオプションおよびライセンス製品は iSeries A 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) • Qshell Interpreter (5722-SS1 オプション 30) • iSeries Access for Windows (5722-XE1) 	はい
シングル・サインオン環境に参加する各 PC に、シングル・サインオンが使用可能になっているアプリケーションがインストール済みですか? 注: このシナリオの場合、参加 PC のすべてに iSeries Access for Windows (5722-XE1) がインストール済みです。	はい
管理者の PC に iSeries ナビゲーター はインストール済みですか? <ul style="list-style-type: none"> • 管理者の PC に iSeries 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 iSeries 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

表1. 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	応答
最新の iSeries Access for Windows サービス・パックをインストール済みですか? 最新のサービス・パックについては、iSeries Access  を参照してください。	はい
管理者は *SECADM、*ALLOBJ、および *IOSYSCFG 特殊権限を持っていますか?	はい
Kerberos サーバー (KDC としても知られる) として働く、以下のいずれかのシステムを持っていますか? 持っている場合は、そのシステムを指定してください。 1. Windows ^(R) 2000 サーバー 注: Microsoft Windows 2000 サーバーは、デフォルトのセキュリティ・メカニズムとして Kerberos 認証を使用します。 2. Windows ^(R) Server 2003 3. i5/OS PASE (V5R3 以降) 4. AIX サーバー 5. zSeries	はい、Windows 2000 サーバー
ネットワーク内の PC はすべて、Windows 2000 ドメイン内で構成されていますか?	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
iSeries 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? 5 分以内でない場合は、『システム時刻を同期する』を参照してください。	はい

この情報は、EIM およびネットワーク認証サービスを構成して、シングル・サインオンのテスト環境を作成する場合に必要です。

表2. iSeries A のシングル・サインオン構成計画ワークシート

iSeries A の構成計画ワークシート	応答
次の情報は、EIM 構成ウィザードを完了する場合に使用します。このワークシートの情報は、ウィザードの各ページで記入する必要がある情報と相互関連します。	
ご使用システムにどのように EIM を構成しますか? • 既存のドメインを結合する • 新規ドメインを作成して結合する	新規ドメインを作成して結合する
ご使用の EIM ドメインを構成する必要がある場所は?	ローカル・ディレクトリー・サーバー上 注: これにより、現在 EIM を構成している同じシステム上にディレクトリー・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しますか? 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
EIM 構成ウィザードから、ネットワーク認証サービス・ウィザードが起動します。次の情報は、ネットワーク認証サービス・ウィザードを完了する場合に使用します。 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関係なく起動できます。	

表 2. iSeries A のシングル・サインオン構成計画ワークシート (続き)

iSeries A の構成計画ワークシート	応答
<p>ご使用の iSeries が属する Kerberos のデフォルト・レルムの名前は 何ですか?</p> <p>注: Windows 2000 ドメインは、Kerberos レルムに類似していま す。 Microsoft Windows Active Directory は、デフォルトのセキュ リティー・メカニズムとして Kerberos 認証を使用します。</p>	<p>MYCO.COM</p>
<p>Microsoft Active Directory を使用していますか?</p>	<p>はい</p>
<p>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) と呼ばれます) は何ですか? Kerberos サーバーが listen するポートは何ですか?</p>	<p>KDC: kdc1.myco.com ポート: 88 注: これは、Kerberos サーバーのデフォルトの ポートです。</p>
<p>このデフォルト・レルムにパスワード・サーバーを構成しますか? 「はい」の場合、次の質問に答えてください。</p> <p>この Kerberos サーバーのパスワード・サーバーの名前は 何ですか? パスワード・サーバーが listen するポートは何 ですか?</p>	<p>はい</p> <p>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 のポートです。</p>
<p>キータブ項目を作成する対象のサービスは?</p> <ul style="list-style-type: none"> • i5/OS Kerberos 認証 • LDAP • iSeries IBM HTTP サーバー • iSeries NetServer™ 	<p>i5/OS Kerberos 認証</p>
<p>ご使用のサービス・プリンシパルのパスワードは何ですか?</p>	<p>iseriesa123 注: このシナリオで指定されたパスワードは、 すべてサンプル目的専用です。ご使用のシステ ムまたはネットワーク・セキュリティを損な わないように、これらのパスワードはユーザー 独自の構成の一部として使用しないでくださ い。</p>
<p>バッチ・ファイルを作成して、iSeries 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?</p>	<p>はい</p>
<p>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?</p>	<p>はい</p>
<p>ネットワーク認証サービス・ウィザードを終了すると、EIM 構成ウィザードへ戻ります。次の情報は、EIM 構成ウィ ザードを完了する場合に使用します。</p>	
<p>ウィザードがディレクトリー・サーバーを構成する際に使用する 必要がある、ユーザー情報を指定します。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。</p> <p>注: ウィザードに EIM ドメインとその中のオブジェクトを管理す る十分な権限があることを確認するには、LDAP 管理者の識別名 (DN) とパスワードを指定してください。</p>	<p>ポート: 389 識別名: cn=administrator パスワード: mycopwd 注: このシナリオで指定されたパスワードは、 すべてサンプル目的専用です。ご使用のシステ ムまたはネットワーク・セキュリティを損な わないように、これらのパスワードはユーザー 独自の構成の一部として使用しないでくださ い。</p>
<p>作成する EIM ドメインの名前は 何ですか?</p>	<p>MyCoEimDomain</p>
<p>EIM ドメインの親 DN を指定 しますか?</p>	<p>いいえ</p>

表 2. iSeries A のシングル・サインオン構成計画ワークシート (続き)

iSeries A の構成計画ワークシート	応答
どのユーザー・レジストリーを EIM ドメインに追加しますか?	ローカル i5/OS--ISERIESA.MYCO.COM Kerberos--MYCO.COM 注: Windows 2000 サーバーに保管された Kerberos プリンシパルは大文字小文字を区別しません。したがって、「 Kerberos ユーザー ID は大文字小文字を区別する 」を選択しないでください。
EIM 操作を行うときに、どの EIM ユーザーを iSeries A に使用させますか? これはシステム・ユーザーです。 注: ディレクトリー・サーバーをシングル・サインオンの構成前に構成していなかった場合は、LDAP 管理者の DN とパスワードが、システム・ユーザーに指定できる唯一の識別名 (DN) です。	ユーザー・タイプ: Distinguished name and password ユーザー: cn=administrator パスワード: mycopwd 注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。
EIM 構成ウィザードが完了したら、次の情報を使用して、シングル・サインオンの構成に必要な残りのステップを完了してください。	
ユーザーの i5/OS ユーザー・プロファイル名は何ですか?	JOHND
作成する EIM ID の名前は何ですか?	John Day
どんな種類のアソシエーションを作成しますか?	ソース・アソシエーション: Kerberos プリンシパル jday ターゲット・アソシエーション: i5/OS ユーザー・プロファイル JOHND
ソース・アソシエーションを作成する Kerberos プリンシパルを含むユーザー・レジストリーの名前は何ですか?	MYCO.COM
ターゲット・アソシエーションを作成する i5/OS ユーザー・プロファイルを含むユーザー・レジストリーの名前は何ですか?	ISERIESA.MYCO.COM
EIM ID のマッピングをテストするのに、どんな情報を提供する必要がありますか?	ソース・レジストリー: MYCO.COM ソース・ユーザー: jday ターゲット・レジストリー: ISERIESA.MYCO.COM

関連情報

EIM (エンタープライズ識別マッピング)

ネットワーク認証サービス

iSeries A の基本シングル・サインオン構成を作成する

EIM 構成ウィザードは、基本的な EIM 構成を作成するのに役立ち、さらにネットワーク認証サービス・ウィザードを開き、基本的なネットワーク認証サービス構成を作成できるようになります。

注: このシナリオの説明は、これまでに iSeries 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、すでにディレクトリー・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、構成ステップ内の該当する個所で注記されます。

このステップを終了すれば、次の作業は完了します。

- 新規 EIM ドメインを作成する
- iSeries A 上のディレクトリー・サーバーを EIM ドメイン・コントローラーに構成する
- ネットワーク認証サービスを構成する
- 新しく作成された EIM ドメインに、iSeries A i5/OS レジストリーおよび Kerberos レジストリーの EIM レジストリー定義を作成する
- iSeries A を構成して、EIM ドメインに参加する
 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**」と展開します。
 2. 「**構成**」を右マウス・ボタン・クリックし、「**構成**」を選択して、EIM 構成ウィザードを開始します。
 3. 「**ウェルカム (Welcome)**」ページで、「**新規ドメインの作成と結合 (Create and join a new domain)**」を選択します。「**次へ**」をクリックします。
 4. 「**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)**」を選択します。「**次へ**」をクリックすると、ネットワーク認証サービス・ウィザードが表示されます。

注: シングル・サインオンのインプリメンテーション用のネットワーク認証サービスを構成するには追加情報の入力が必要であるとシステムが判断したときは、ネットワーク認証サービス・ウィザードのみが表示されます。

5. 以下の作業を行って、ネットワーク認証サービスを構成します。
 - a. 「**ネットワーク認証サービスの構成 (Configure Network Authentication Service)**」ページで、「**はい**」を選択します。

注: これで、ネットワーク認証サービス・ウィザードが起動します。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almに参加できます。

- b. 「**レalm情報の指定 (Specify Realm Information)**」ページで、「**デフォルト・レalm (Default realm)**」フィールドに「**MYCO.COM**」と入力し、「**Microsoft Active Directory を Kerberos 認証に使用 (Microsoft Active Directory is used for Kerberos authentication)**」を選択します。「**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「**kdc1.myco.com**」と入力し、「**ポート**」フィールドに「**88**」と入力します。「**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**」を選択します。「**パスワード・サーバー (Password server)**」フィールドに「**kdc1.myco.com**」と入力し、「**ポート**」フィールドに「**464**」と入力します。「**次へ**」をクリックします。
- e. 「**Keytab エントリーの選択 (Select Keytab Entries)**」ページで、「**i5/OS Kerberos 認証 (OS/400 Kerberos Authentication)**」を選択します。「**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の入力と確認を行い、「**次へ**」をクリックします。たとえば、**iseriesa123** です。このパスワードは、iSeries A が Kerberos サーバーに追加されるときに使用されます。

注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティーを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。

g. 任意: 「**バッチ・ファイルの作成 (Create Batch File)**」 ページで「はい」を選択し、次の情報を指定して、「次へ」をクリックします。

- **バッチ・ファイル:** デフォルトのバッチ・ファイル名の末尾に、テキスト `iseriesa` を追加します。たとえば、`C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigiseriesa.bat` です。
- 「**パスワードの組み込み (Include password)**」を選択します。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。重要なことは、パスワードを平文で表示すると、バッチ・ファイルへの読み取りアクセスによって、だれかに読まれるおそれがあることに注意することです。したがって、バッチ・ファイルは、使用后ただちに、Kerberos サーバーおよび 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と、バッチ・ファイルの実行時にプロンプトでパスワードの入力を求められます。

h. 「**サマリー**」 ページでネットワーク認証サービス構成の詳細を検討し、「終了」をクリックして、ネットワーク認証サービス・ウィザードを終了し、EIM 構成ウィザードに戻ります。

6. 「**ディレクトリー・サーバーの構成 (Configure Directory Server)**」 ページで次の情報を入力し、「次へ」をクリックします。

注: このシナリオを開始する前にディレクトリー・サーバーを構成した場合は、「**ディレクトリー・サーバーの構成 (Configure Directory Server)**」 ページではなく「**接続のためにユーザーを指定 (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:** 389
- **識別名:** `cn=admin`
- **パスワード:** `mycopwd`

注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。

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名を入力し、「次へ」をクリックします。たとえば、`MyCoEimDomain` です。

8. 「**ドメインの親 DN を指定 (Specify Parent DN for Domain)**」 ページで「いいえ」を選択して、「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の場合は、変更内容を有効にするために、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ます。

9. 「**レジストリー情報**」 ページで、「ローカル i5/OS」および「**Kerberos**」を選択して、「次へ」をクリックします。レジストリー名は書き留めておいてください。これらのレジストリー名は、EIM ID とのアソシエーションを作成する際に必要です。

注:

- レジストリー名は、ドメインに対して固有でなければなりません。
- 固有のレジストリー定義命名計画を使用する場合は、ユーザー・レジストリーに固有のレジストリー定義名を入力できます。しかし、このシナリオの場合は、デフォルト値を受け入れてもかまいません。

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・システム機能に代わって EIM 操作を実行する際にオペレーティング・システムが使用するユーザーを選択して、「次へ」をクリックします。

注: このシナリオでは、ステップの実行前に、ディレクトリー・サーバーを構成しなかったため、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: Distinguished name and password
- 識別名: cn=administrator
- パスワード: mycopwd

注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。

11. 「サマリー」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。

iSeries A での基本的な EIM およびネットワーク認証サービスの構成は終了したので、これで iSeries A のサービス・プリンシパルを Kerberos サーバーに追加できます。

iSeries A サービス・プリンシパルを Kerberos サーバーに追加する

必要な i5/OS サービス・プリンシパルを Kerberos サーバーに追加する場合は、2 つの方法のいずれかを使用できます。サービス・プリンシパルを手動で追加することもできれば、このシナリオの説明のように、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場合は、FTP (ファイル転送プロトコル) を使用してファイルを Kerberos サーバーにコピーして、実行できます。

バッチ・ファイルを使用してプリンシパルを Kerberos サーバーに追加するときは、以下のステップに従います。

ウィザードが作成する FTP バッチ・ファイル

1. ネットワーク認証サービスを構成する際に使用した Windows 2000 ワークステーション上でコマンド・プロンプトを開き、ftp kdc1.myco.com と入力して、PC 上に FTP セッションを開始します。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。
2. FTP プロンプトで、lcd "C:\Documents and Settings\All Users\Documents\IBM\Client Access" と入力します。Enter キーを押します。Local directory now C:\Documents and Settings\All Users\Documents\IBM\Client Access のメッセージを受け取るはずですが。
3. FTP プロンプトで、cd %mydirectory と入力します。ここで、mydirectory は kdc1.myco.com 上にあるディレクトリーです。
4. FTP プロンプトで、put NASConfigiseriesa.bat と入力します。226 転送は完了のメッセージを受け取るはずですが。
5. quit と入力して、FTP セッションを終了します。

kdc1.myco.com でバッチ・ファイルを実行する

1. ご使用の Windows 2000 サーバーで、バッチ・ファイルを転送したディレクトリーを開きます。
2. NASConfigiseriesa.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。
3. ファイルの実行後、次のことを行って、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。

- a. ご使用の Windows 2000 サーバーで、「管理ツール」 → 「Active Directory ユーザーとコンピュータ」 → 「ユーザー」と展開します。
- b. 該当する Windows 2000 ドメインを選択して、iSeries にユーザー・アカウントがあることをチェックします。

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のレルム名と同じでなければなりません。

- c. 表示されたユーザーのリストで、**iseriesa_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。
- d. (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、「アカウントは委任に対して信頼できる (Account is trusted for delegation)」を選択します。

注: このオプション・ステップによって、ご使用システムは、ユーザーの信任状を他のシステムに委譲あるいは転送することができます。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。これは多重層ネットワークでは便利です。

これで iSeries A サービス・プリンシパルが Kerberos サーバーに追加されたので、ここで John Day のホーム・ディレクトリーを作成できます。

iSeries A 上に John Day のホーム・ディレクトリーを作成する

ご使用の Kerberos 信任状キャッシュを保管するには、/home directory にディレクトリーを作成する必要があります。ホーム・ディレクトリーを作成するには、次のことを行ってください。

コマンド行で、CRTDIR '/home/user profile' と入力します。ここで user profile は、ご使用の i5/OS ユーザー・プロファイル名です。たとえば、CRTDIR '/home/JOHND' です。

これでホーム・ディレクトリーが作成されたので、ここで、ネットワーク認証サービスが正しく構成されているか検査できます。

iSeries A でネットワーク認証サービス構成をテストする

これで iSeries A のネットワーク認証サービス構成作業は終了したので、ここで、構成が正しく働くことをテストする必要があります。これは、iSeries A プリンシパル名の発券許可証を要求することで行えます。

ネットワーク認証サービス構成をテストするときは、以下のステップに従ってください。

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 Interpreter を開始します。
2. keytab list と入力して、キータブ・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、iSeries A のプリンシパル名として、krbsvr400/iseriesa.myco.com@MYCO.COM が表示されるはずですが。
3. kinit -k krbsvr400/iseriesa.myco.com@MYCO.COM と入力します。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 と入力して、デフォルトのプリンシパルが krbsvr400/iseriesa.myco.com@MYCO.COM であることを検査します。

これで、ネットワーク認証サービス構成はテストされたので、ここで John Day の EIM ID を作成できます。

John Day の EIM ID を作成する

これで、基本的なシングル・サインオン構成を作成する初期ステップは行われたので、ここで、シングル・サインオンのテスト環境を完了するためのこの構成への情報の追加を始めることができます。計画ワークシートで指定した EIM ID を作成する必要があります。このシナリオで、この EIM ID は、企業内で John Day を一意的に識別する名前です。

EIM ID を作成するには、以下のステップに従います。

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」 → 「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プロンプトが出される場合があります。この場合は、「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。ドメインでアクションを行うには、それに接続しておく必要があります。ドメイン・コントローラーに接続するには、次の情報を指定して、「OK」をクリックします。

- ユーザー・タイプ: Distinguished name
- 識別名: cn=administrator
- パスワード: mycopwd

注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティーを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。

2. 「ID」を右マウス・ボタン・クリックして、「新規 ID...」を選択します。
3. 「新規 EIM ID」ダイアログ・ボックスで、「ID」フィールドに新規 ID の名前を入力し、「OK」をクリックします。たとえば、John Day です。

ID を作成したので、ここで ID にアソシエーションを追加し、ID と対応する Kerberos プリンシパルおよび i5/OS ユーザー・プロファイル間の関係を定義することができます。

新しい EIM ID のソース・アソシエーションおよびターゲット・アソシエーションを作成する

EIM ID と、ID を表す人が使用するユーザー ID 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 アソシエーションが適切に構成されると、それによってユーザーはシングル・サインオン環境に参加できます。

このシナリオでは、John Day ID には、2 つの ID アソシエーションを作成する必要があります。

- jday Kerberos プリンシパルのソース・アソシエーション。これは、当の John Day が Windows およびネットワークにログインする際に使用するユーザー ID です。このソース・アソシエーションで、Kerberos プリンシパルを、対応するターゲット・アソシエーションで定義された別のユーザー ID にマップすることができます。
- JOHND i5/OS ユーザー・プロファイルのターゲット・アソシエーション。これは、当の John Day が、iSeries ナビゲーター および iSeries 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・アソシエーションは、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。

これで、John Day の ID が作成されたので、ここで、そのソース・アソシエーションとターゲット・アソシエーションの両方を作成する必要があります。

Kerberos プリンシパルと John Day の ID 間のソース・アソシエーションを作成するには、以下のステップに従います。

1. iSeries ナビゲーター で、「**iSeries A**」 → 「**エンタープライズ識別マッピング**」 → 「**ドメイン管理**」 → 「**MyCoEimDomain**」 → 「**ID**」と展開します。
2. 「**John Day**」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. 「**アソシエーション**」ページで、「**追加**」をクリックします。
4. 「**アソシエーションの追加**」ダイアログで、「**参照...**」を指定して次の情報を選択し、「**OK**」をクリックします。
 - レジストリー: MYCO.COM
 - ユーザー: jday
 - アソシエーション・タイプ: Source
5. 「**OK**」をクリックして、「**アソシエーションの追加**」ダイアログを閉じます。

i5/OS ユーザー・プロファイルと John Day の ID 間のターゲット・アソシエーションを作成するには、以下のステップに従います。

1. 「**OK**」をクリックして、「**アソシエーションの追加**」ダイアログを閉じます。
2. 「**アソシエーション**」ページで、「**追加**」をクリックします。
3. 「**アソシエーションの追加**」ダイアログで、「**参照...**」を指定して次の情報を選択し、「**OK**」をクリックします。
 - レジストリー: ISERIESA.MYCO.COM
 - ユーザー: JOHND
 - アソシエーション・タイプ: Target
4. 「**OK**」をクリックして、「**アソシエーションの追加**」ダイアログを閉じます。
5. 「**OK**」をクリックして、「**プロパティ**」ダイアログを閉じます。

これで、ID を作成し、ID に該当するアソシエーションが追加されたので、ここで、関連付けられたユーザー ID 間のマッピングが正しく働いているかテストする必要があります。

EIM ID マッピングをテストする

EIM マッピング探索操作が、構成された関連に基づいて正しい結果を戻すことを検査する必要があります。

EIM マッピング操作が正しく働いていることをテストするには、以下のステップに従います。

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**」 → 「**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プロンプトが出される場合があります。この場合は、「**EIM ドメイン・コントローラーへの接続 (Connect to EIM Domain Controller)**」ダイアログが表示されます。ドメインでアクションを行うには、それに接続しておく必要があります。ドメイン・コントローラーに接続するには、次の情報を指定して、「**OK**」をクリックします。

- ユーザー・タイプ: Distinguished name
- 識別名: cn=administrator

- パスワード: mycopwd

注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティーを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。

2. 「MyCoEimDomain」を右マウス・ボタン・クリックして、「マッピングのテスト...」を選択します。
3. 「マッピングのテスト」ダイアログで、「参照...」を指定して、次の情報を選択します。
 - ソース・レジストリー: MYCO.COM
 - ソース・ユーザー: jday
 - ターゲット・レジストリー: ISERIESA.MYCO.COM

注: 必要があれば、ダイアログの各フィールドに必要な情報について詳しくは、「ヘルプ」をクリックします。

「テスト」をクリックし、「クローズ」をクリックします。

EIM マッピングが正しく構成されていれば、ページの「検出されたマッピング (Mapping found)」の部分に次の結果が表示されます。

以下のフィールドの場合	以下の結果を参照
ターゲット・ユーザー	JOHND
オリジン (起点)	EIM ID: John Day

マッピング関係または通信関係の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』を参照して、問題の解決方法を見つけてください。

これで、EIM ID のマッピングがテストされたので、ここで、Kerberos 認証を使用する iSeries Access for Windows アプリケーションを構成することができます。

Kerberos 認証を使用する iSeries Access for Windows アプリケーションを構成する

iSeries ナビゲーター を使用してシステムにアクセスするには、Kerberos を使用して認証しておく必要があります。したがって、PC から、Kerberos 認証を使用する iSeries Access for Windows を構成する必要があります。

Kerberos 認証を使用する iSeries Access for Windows アプリケーションを構成するには、次のことを行ってください。

注: ユーザーのそれぞれが、自らの PC で以下のステップをすべて行う必要があります。

1. ご使用の PC にサインインして、Windows 2000 ドメインにログオンします。
2. ご使用の PC の iSeries ナビゲーター で、「iSeries 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 プリンシパル名を使用、プロンプトなし (Use Kerberos principal name, no prompting)」を選択します。これで、iSeries 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. 接続設定に加えられた変更を有効にするには、現在稼働中のすべてのアプリケーションを閉じて、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。「OK」をクリックします。次に、iSeries ナビゲーター を終了して、再始動します。

これで、Kerberos 認証を使用する iSeries Access for Windows アプリケーションが構成されたので、ここで、シングル・サインオン環境を検査することができます。

ネットワーク認証サービスと EIM 構成を検証する

これで、シングル・サインオン構成を個々に検査し、すべてのセットアップが完全であることが確認されたので、ここで、EIM およびネットワーク認証サービスを正しく構成したこと、かつシングル・サインオンが予想どおり働くことを検査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査するために、John Day に以下のステップを実行してもらいます。

1. iSeries ナビゲーター で、「**iSeries A**」を展開して、iSeries A への接続を開きます。
2. F5 を押して、画面を最新表示します。
3. 右側のペインの「名前」欄で iSeries 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、iSeries 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 iSeries A ユーザー・プロファイルにマップしました。iSeries A の iSeries 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。

(オプション) 構成後の考慮事項

ここで、このシナリオは終了したので、これで EIM が使用できると定義した EIM ユーザーのみが LDAP 管理者の DN です。iSeries A 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かつ限定されたアクセス制御権を持つ追加のユーザーとして、1 つ以上の DN を作成することを考慮することもできます。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対するセキュリティ・ポリシーの力点の置き方によって異なります。一般に、次のタイプの少なくとも 2 つの DN を作成します。

• EIM 管理者のアクセス制御権を持つユーザー

この EIM 管理者 DN には、EIM ドメインを管理する責任がある管理者のしかるべきレベルの権限があります。この EIM 管理者 DN は、iSeries 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権のすべてを持つ少なくとも 1 つのユーザー:

- ID 管理者
- レジストリー管理者
- EIM マッピング操作

このユーザーには、オペレーティング・システムに代わって EIM 操作を行うシステム・ユーザーに必要な、しかるべきレベルのアクセス制御権があります。

注: この新しい DN を LDAP 管理者 DN ではなくシステム・ユーザーに使用するには、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は、セットアップするすべての iSeries システムについて、EIM 構成プロパティの変更が必要です。システム・ユーザー DN の変更方法を確認するには『EIM 構成プロパティの管理』を参照してください。

シナリオ: i5/OS のシングル・サインオンを使用できるようにする

このシナリオでは、ネットワーク認証サービスおよび EIM を構成し、企業内の複数のシステム全体でシングル・サインオン環境を作成する方法を説明します。このシナリオでは、シングル・サインオンのテスト環境の作成方法を実証する前のシナリオで示した概念および作業を展開します。

状況

ネットワーク管理者は、受注部門を含む、会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します。ネットワーク管理者は、電話による顧客オーダーを受ける多数の従業員の IT 操作を監視します。さらには、ネットワーク管理者のネットワークの保守を助ける他の 2 人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。したがって、ネットワーク管理者は、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 に関連する管理やトラブルシューティングの問題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は、受注部門を始め事業改善の方策を常に模索しています。大部分の従業員が在庫状況の照会に使用するアプリケーションにアクセスするときは、同じタイプの権限を必要としていることを承知しています。この状況で必要とされる個々のユーザー・プロファイルと大量のパスワードの維持は、余分で時間浪費のように思えます。さらに、ユーザー ID およびパスワードの使用が減れば、すべての従業員の利益になることは分かっています。以下のことを行う必要があります。

- 受注部門のパスワード管理の作業を単純化する。特に、従業員が顧客オーダーで毎日使用するアプリケーションへのユーザー・アクセスを、効率的に管理する必要があります。
- ネットワーク管理者だけでなく、部門従業員による複数のユーザー ID およびパスワードの使用を減らす。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のに多くのユーザー ID とパスワードを用意する必要がないため、解決すべきパスワード問題も少なくなります。シングル・サインオンは、次のような方法でパスワード管理の単純化が可能になるため、理想的なソリューションと考えられます。

- アプリケーションに対して同じ権限を必要とする代表的ユーザーには、ポリシー・アソシエーションを作成することができます。たとえば、受注部門のオーダー・クレークが Windows ユーザー名およびパスワードを用いて 1 回ログオンできれば、もう一度認証を受ける必要なく、製造部門の新しい在庫照会アプリケーションにアクセスできます。しかし、このアプリケーションを使用する際のユーザーの権限レベルが適切かどうかの確認も必要です。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・アソシエーションを作成することにしました。これは、データを変更できない照会専用のアプリケーションであるため、このアプリケーションのための詳細な監査を心配する必要はありません。したがって、この状況では、ポリシー・アソシエーションの使用がセキュリティー・ポリシーに合っていることの確認が得られます。

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・アソシエーションを作成します。ユーザーには、覚えるパスワードが 1 つ少なく、行うログオンが 1 つ少ないという

利点があります。管理者としては、グループ内の全員について、アプリケーションへのユーザー・アクセスを行うユーザー・プロファイルを、複数ではなく 1 つだけ維持すれば済むという利点があります。

- *ALLOBJ や *SECADM などの特殊な権限のユーザー・プロファイルを持つ配下のネットワーク管理者のそれぞれに、ID アソシエーションを作成できます。たとえば、単一のネットワーク管理者のすべてのユーザー ID を、管理者の高いレベルの権限を利用して、正確に、一つ一つ相互にマップする必要があります。

会社のセキュリティ・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 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 アソシエーションは 1 対 1 のマッピングを行うので、管理者のアクティビティは、さらに容易にモニターおよびトレースできます。たとえば、システムで行われるジョブおよびオブジェクトを特定のユーザー ID についてモニターできます。配下のネットワーク管理者には、覚えるパスワードが 1 つ少なく、行うログオンが 1 つ少ないという利点があります。ネットワーク管理者本人としては、配下の管理者のすべてのユーザー ID 間の関係を綿密に制御するという利点があります。

このシナリオには、以下の利点があります。

- ユーザーの認証処理を単純化する。
- アプリケーションへのアクセス管理を単純化する。
- ネットワーク内サーバーへのアクセス管理のオーバーヘッドを緩和する。
- パスワード盗難の危険を最小限に抑える。
- 複数サインオンの必要を避ける。
- ネットワーク全体でのユーザー ID 管理の単純化。

目的

このシナリオでは、MyCo, Inc. の管理者として、受注部門のユーザーのシングル・サインオンを使用できるようにする必要があります。

このシナリオの目的は次のとおりです。

- iSeries A および iSeries 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、iSeries A および iSeries 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。
- iSeries A 上の IBM Directory Server for iSeries (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。

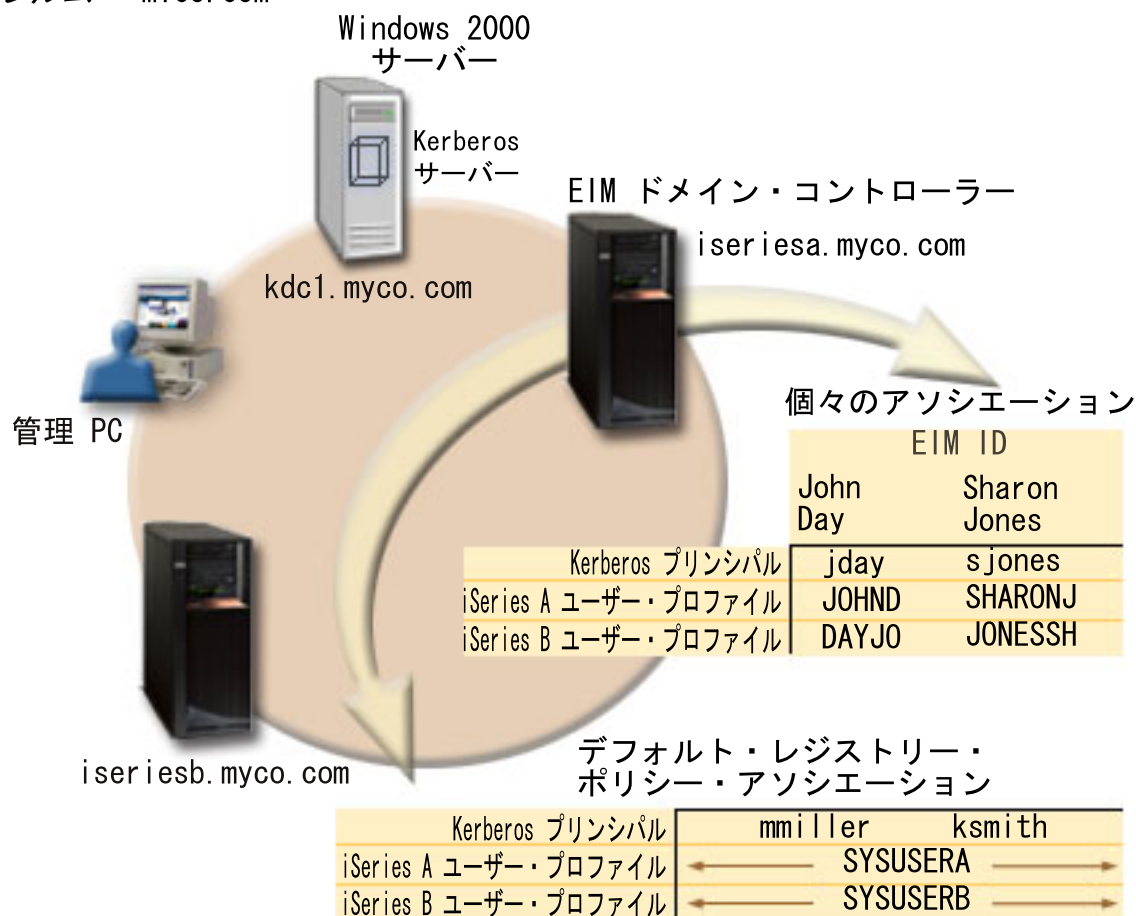
注: 異なるタイプの 2 つのドメインである、EIM ドメインおよび Windows 2000 ドメインが、シングル・サインオン環境に適合する方法を確認する場合は、『ドメイン』を参照してください。

- 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・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 のマッピングを使用すると、システムで行われるジョブおよびオブジェクトをこれらのユーザー ID について綿密にモニターできます。
- ユーザーを、iSeries ナビゲーターを含む iSeries 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

以下の図で、このシナリオのネットワーク環境を説明します。

レルム = MYCO.COM



この図で、このシナリオに関連する以下の諸点を説明します。

企業に定義された EIM ドメイン・データ

- 3 つのレジストリー定義名:
 - Windows 2000 サーバー・レジストリーのレジストリー定義名の MYCO.COM。iSeries 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。
 - iSeries A 上の i5/OS レジストリーのレジストリー定義名の ISERIESA.MYCO.COM。iSeries 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。
 - iSeries B 上の i5/OS レジストリーのレジストリー定義名の ISERIESB.MYCO.COM。iSeries 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。
- 2 つのデフォルト・レジストリー・ポリシー・アソシエーション:

注: EIM 探索操作処理では、ID アソシエーションに最高の優先順位が割り当てられます。したがって、ユーザー ID が、ポリシー・アソシエーションと ID アソシエーションの両方のソースとして定義される場合、そのユーザー ID をマップするのは ID アソシエーションのみです。このシナリオでは、John Day と Sharon Jones の 2 人のネットワーク管理者の両方が、デフォルト・レジストリ

- ー・ポリシー・アソシエーションのソースである、MYCO.COM レジストリーのユーザー ID を持っています。しかし、以下に示すように、これらの管理者も、ID アソシエーションを MYCO.COM レジストリーのそのユーザー ID に定義しています。この ID アソシエーションで、その MYCO.COM ユーザー ID がポリシー・アソシエーションによってマップされることはありません。代わりに、ID アソシエーションでは、MYCO.COM レジストリーのそのユーザー ID が、他の個々別々のユーザー ID に個別にマップされます。
- 1 つのデフォルト・レジストリー・ポリシー・アソシエーションが、MYCO.COM という Windows 2000 サーバー・レジストリー内のすべてのユーザー ID を、iSeries A 上の ISERIESA.MYCO.COM レジストリー内の SYSUSERA という単一の i5/OS ユーザー・プロファイルにマップします。このシナリオでは、mmiller と ksmith がこれら 2 つのユーザー ID を表しています。
 - 1 つのデフォルト・レジストリー・ポリシー・アソシエーションが、MYCO.COM という Windows 2000 サーバー・レジストリー内のすべてのユーザー ID を、iSeries B 上の ISERIESB.MYCO.COM レジストリー内の SYSUSERB という単一の i5/OS ユーザー・プロファイルにマップします。このシナリオでは、mmiller と ksmith がこれら 2 つのユーザー ID を表しています。
 - これらの名前の会社内の 2 人のネットワーク管理者を表す、John Day と Sharon Jones という 2 つの EIM ID。
 - John Day の EIM ID の場合、これらの ID アソシエーションは以下のように定義されます。
 - Windows 2000 サーバー・レジストリーの Kerberos プリンシパルである、jday ユーザー ID のソース・アソシエーション。
 - iSeries 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・アソシエーション。
 - iSeries 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・アソシエーション。
 - Sharon Jones の EIM ID の場合、これらの ID アソシエーションは以下のように定義されます。
 - Windows 2000 サーバー・レジストリーの Kerberos プリンシパルである、sjones ユーザー ID のソース・アソシエーション。
 - iSeries 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・アソシエーション。
 - iSeries 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・アソシエーション。

Windows 2000 サーバー

- ネットワークの鍵配布センター (KDC) としても知られている、Kerberos サーバー (kdc1.myco.com) として行動します。
- Kerberos サーバーのデフォルト・レルムは MYCO.COM です。
- ID アソシエーションを持たないすべての Microsoft Windows Active Directory ユーザーは、各 iSeries システムの単一の i5/OS ユーザー・プロファイルにマップされます。

iSeries A

- 次のオプションおよびライセンス製品をインストールした i5/OS バージョン 5 リリース 4 (V5R4) を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12)
 - Qshell Interpreter (5722-SS1 オプション 30)
 - iSeries Access for Windows (5722-XE1)

注: このシナリオは、V5R2 を実行するサーバーを使用して実現できます。構成ステップによっては若干異なるものもあります。さらに、このシナリオでは、ポリシー・アソシエーションのような、V5R3 以降でのみ使用可能なシングル・サインオン機能をいくつか実証します。

- iSeries 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 に参加します。
- krbsvr400/iseriesa.myco.com@MYCO.COM のサービス・プリンシパルを持っています。
- iseriesa.myco.com の完全修飾ホスト名を持っています。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ドメイン・ネーム・システム (DNS) に登録されています。
- iSeries 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。

iSeries B

- 次のオプションおよびライセンス製品をインストールした i5/OS バージョン 5 リリース 4 (V5R4) を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12)
 - Qshell Interpreter (5722-SS1 オプション 30)
 - iSeries Access for Windows (5722-XE1)
- iseriesb.myco.com の完全修飾ホスト名を持っています。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ドメイン・ネーム・システム (DNS) に登録されています。
- iSeries B のプリンシパル名は krbsvr400/seriesb.myco.com@MYCO.COM です。
- EIM ドメイン、MyCoEimDomain に参加します。
- iSeries 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・システムを実行します。
- i5/OS V5R4 iSeries Access for Windows (5722-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 iSeries 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
- 管理者の 1 次ログオン・システムとして使用されます。
- MYCO.COM レルム (Windows ドメイン) の一部として構成されます。

前提条件および前提事項

このシナリオを正常に完了するには、次の前提条件および前提事項が満たされる必要があります。

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など、すべてのシステム要件が検査されている。

これらのライセンス・プログラムがインストールされていることを検査するには、以下のことを行ってください。

- a. iSeries ナビゲーター で、「iSeries server」 → 「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」と展開する。

- b. 必要なライセンス・プログラムがすべてインストールされていることを確認する。
2. 必要なすべてのハードウェア計画およびセットアップが完了している。
3. TCP/IP および基本的なシステム・セキュリティが、システムごとに構成されテストされている。
4. これまでに iSeries 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、これまでに iSeries 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、すでにディレクトリー・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、構成ステップ内の該当する個所で注記されます。

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

注: Kerberos 認証にホスト・テーブルを使用すると、ネーム解決エラーまたはその他の問題を起こすことがあります。Kerberos 認証でのホスト・ネーム解決の働きについて詳しくは、『ホスト・ネーム解決に関する考慮事項』を参照してください。

構成ステップ

注: このシナリオを実行する前に、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) の概念を含む、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。このシナリオを続ける準備ができている場合は、以下のステップを実行してください。

関連情報

ホスト名の解決に関する考慮事項

EIM (エンタープライズ識別マッピング)

ネットワーク認証サービス

計画ワークシートに記入する

次の計画ワークシートは、一般のシングル・サインオン計画ワークシートを基にして、このシナリオに合うように調整したものです。これらの計画ワークシートで、このシナリオで説明するシングル・サインオンのインプリメンテーションの構成を準備する際に収集する必要がある情報、および行うべき判断を実証します。正常なインプリメンテーションを確保するには、構成作業を行う前に、ワークシートのすべての前提条件項目に「はい」で応答でき、かつワークシートの記入に必要なすべての情報を収集している必要があります。

注: 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) の概念を含む、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。

表 3. 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	応答
i5/OS は V5R4 (5722-SS1) ですか?	はい
以下のオプションおよびライセンス製品は iSeries A および iSeries B 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) • Qshell Interpreter (5722-SS1 オプション 30) • iSeries Access for Windows (5722-XE1) 	はい

表 3. 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	応答
<p>シングル・サインオン環境に参加する各 PC に、シングル・サインオンが使用可能になっているアプリケーションがインストール済みですか?</p> <p>注: このシナリオの場合、参加 PCs のすべてに iSeries Access for Windows (5722-XE1) がインストール済みです。</p>	はい
<p>管理者の PC に iSeries 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"> シングル・サインオンの管理に使用する PC に iSeries 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 iSeries 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? シングル・サインオンの管理に使用する PC に iSeries 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
<p>最新の IBM  server iSeries Access for Windows サービス・バックはインストール済みですか? 最新のサービス・バックについては、iSeries Access Web ページ  を参照してください。</p>	はい
<p>シングル・サインオンの管理者は、*SECADM、*ALLOBJ、および *IOSYSCFG 特殊権限を持っていますか?</p>	はい
<p>Kerberos サーバー (KDC としても知られる) として働く、以下のいずれかのシステムを持っていますか? 持っている場合は、そのシステムを指定してください。</p> <ol style="list-style-type: none"> Microsoft Windows 2000 サーバー 注: Microsoft Windows 2000 サーバーは、デフォルトのセキュリティー・メカニズムとして Kerberos 認証を使用します。 Windows ^(R) サーバー 2003 i5/OS PASE (V5R3 以降) AIX サーバー zSeries 	はい、Windows 2000 サーバー
<p>ネットワーク内の PC はすべて、Windows 2000 ドメイン内で構成されていますか?</p>	はい
<p>最新のプログラム一時修正 (PTF) を適用していますか?</p>	はい
<p>iSeries 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? 5 分以内でない場合は、『システム時刻を同期する』を参照してください。</p>	はい

iSeries 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 4. iSeries A のシングル・サインオン構成計画ワークシート

iSeries A の構成計画ワークシート	応答
<p>次の情報は、EIM 構成ウィザードを完了する場合に使用します。このワークシートの情報は、ウィザードの各ページで記入する必要がある情報と相互関連します。</p>	

表 4. iSeries A のシングル・サインオン構成計画ワークシート (続き)

iSeries A の構成計画ワークシート	応答
ご使用システムにどのように EIM を構成しますか? ・ 既存のドメインを結合する ・ 新規ドメインを作成して結合する	新規ドメインを作成して結合する
EIM ドメインを構成する必要がある場所は?	ローカル・ディレクトリー・サーバー上 注: これにより、現在 EIM を構成している同じシステム上にディレクトリー・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しますか? 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
EIM 構成ウィザードから、ネットワーク認証サービス・ウィザードが起動します。次の情報は、ネットワーク認証サービス・ウィザードを完了する場合に使用します。	
ご使用の iSeries 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 レルムに類似していません。Microsoft Windows Active Directory は、デフォルトのセキュリティ・メカニズムとして Kerberos 認証を使用します。	MYCO.COM
Microsoft Active Directory を使用していますか?	はい
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) と呼ばれます) は何ですか? Kerberos サーバーが listen するポートは何ですか?	KDC: kdc1.myco.com ポート: 88 注: これは、Kerberos サーバーのデフォルトのポートです。
このデフォルト・レルムにパスワード・サーバーを構成しますか? 「はい」の場合、次の質問に教えてください。 この Kerberos サーバーのパスワード・サーバーの名前は何か? パスワード・サーバーが listen するポートは何ですか?	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のポートです。
キータブ項目を作成する対象のサービスは? ・ i5/OS Kerberos 認証 ・ LDAP ・ iSeries IBM HTTP サーバー ・ iSeries NetServer	i5/OS Kerberos 認証
ご使用のサービス・プリンシパルのパスワードは何ですか?	iseriesa123 注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。
バッチ・ファイルを作成して、iSeries 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

表 4. iSeries A のシングル・サインオン構成計画ワークシート (続き)

iSeries A の構成計画ワークシート	応答
ネットワーク認証サービス・ウィザードを終了すると、EIM 構成ウィザードへ戻ります。次の情報は、EIM 構成ウィザードを完了する場合に使用します。	
<p>ウィザードがディレクトリー・サーバーを構成する際に使用する必要がある、ユーザー情報を指定します。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。</p> <p>注: ウィザードに EIM ドメインとその中のオブジェクトを管理する十分な権限があることを確認するには、LDAP 管理者の識別名 (DN) とパスワードを指定してください。</p>	<p>ポート: 389</p> <p>識別名: cn=administrator</p> <p>パスワード: mycopwd</p> <p>注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。</p>
作成する EIM ドメインの名前は何か?	MyCoEimDomain
EIM ドメインの親 DN を指定しますか?	いいえ
どのユーザー・レジストリーを EIM ドメインに追加しますか?	<p>ローカル i5/OS--ISERIESA.MYCO.COM</p> <p>Kerberos--KDC1.MYCO.COM</p> <p>注: ウィザードがこのオプションを表すときは、「Kerberos ユーザー ID は大文字小文字を区別する」を選択しないでください。</p>
<p>EIM 操作を行うときに、どの EIM ユーザーを iSeries A に使用させますか? これはシステム・ユーザーです。</p> <p>注: ディレクトリー・サーバーをシングル・サインオンの構成前に構成していなかった場合は、LDAP 管理者の DN とパスワードが、システム・ユーザーに指定できる唯一の識別名 (DN) です。</p>	<p>ユーザー・タイプ: Distinguished name</p> <p>識別名: cn=administrator</p> <p>パスワード: mycopwd</p> <p>注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。</p>

この情報は、iSeries B を EIM ドメインに参加させ、iSeries 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 5. iSeries B のシングル・サインオン構成計画ワークシート

iSeries B の構成計画ワークシート	応答
次の情報は、iSeries B 用の EIM 構成ウィザードを完了する場合に使用します。	
ご使用システムにどのように EIM を構成しますか?	既存のドメインを結合する
<p>ネットワーク認証サービスを構成しますか?</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
<p>EIM 構成ウィザードから、ネットワーク認証サービス・ウィザードが起動します。次の情報は、ネットワーク認証サービス・ウィザードを完了する場合に使用します。</p> <p>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関係なく起動できます。</p>	
<p>ご使用の iSeries 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 レルムと同等です。Microsoft Active Directory は、デフォルトのセキュリティ・メカニズムとして Kerberos 認証を使用します。</p>	MYCO.COM

表 5. iSeries B のシングル・サインオン構成計画ワークシート (続き)

iSeries B の構成計画ワークシート	応答
Microsoft Active Directory を使用していますか?	はい
この Kerberos のデフォルト・レルムの Kerberos サーバーは何ですか? Kerberos サーバーが listen するポートは何ですか?	KDC: kdc1.myco.com ポート: 88 注: これは、Kerberos サーバーのデフォルトのポートです。
このデフォルト・レルムにパスワード・サーバーを構成しますか? 「はい」の場合、次の質問に教えてください。 この Kerberos サーバーのパスワード・サーバーの名前は何ですか? パスワード・サーバーが listen するポートは何ですか?	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のポートです。
キータブ項目を作成する対象のサービスは? <ul style="list-style-type: none"> • i5/OS Kerberos 認証 • LDAP • iSeries IBM HTTP サーバー • iSeries 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?	iseriesb123 注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。
バッチ・ファイルを作成して、iSeries 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 構成ウィザードへ戻ります。次の情報は、iSeries B 用の EIM 構成ウィザードを完了する場合に使用します。	
結合する EIM ドメインの EIM ドメイン・コントローラーの名前は何ですか?	iseriesa.myco.com
SSL または TLS との接続を確保する計画ですか?	いいえ
EIM ドメイン・コントローラーが listen するポートは何ですか?	389
どのユーザーをドメイン・コントローラーへの接続に使用しますか? これは接続ユーザーです。 注: ウィザードに EIM ドメインとその中のオブジェクトを管理する十分な権限があることを確認するには、LDAP 管理者の識別名 (DN) とパスワードを指定してください。	ユーザー・タイプ: Distinguished name and password 識別名: cn=administrator パスワード: mycopwd 注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。
結合する EIM ドメインの名前は何ですか?	MyCoEimDomain
EIM ドメインの親 DN を指定しますか?	いいえ

表 5. iSeries B のシングル・サインオン構成計画ワークシート (続き)

iSeries B の構成計画ワークシート	応答
EIM ドメインに追加するユーザー・レジストリーの名前は何か?	ローカル i5/OS--ISERIESB.MYCO.COM
EIM 操作を行うときに、どの EIM ユーザーを iSeries B に使用させますか? これはシステム・ユーザーです。 注: このシナリオの前半では、EIM 構成ウィザードを使用して iSeries A 上にディレクトリー・サーバーを構成しました。そうする際、LDAP 管理者の DN およびパスワードを作成しました。これは、現在ディレクトリー・サーバーに定義された唯一の DN です。したがって、これは、ここで指定する必要がある DN およびパスワードです。	ユーザー・タイプ: Distinguished name and password 識別名: cn=administrator パスワード: mycopwd 注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティーを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。

表 6. 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る	特殊権限 (特権クラス)	システム
SYSUSERA	いいえ	ユーザー	iSeries A
SYSUSERB	いいえ	ユーザー	iSeries B

表 7. 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 記述
John Day	MYCO.COM	jday	ソース	Kerberos (Windows 2000) ログイン・ユーザー ID
John Day	ISERIESA.MYCO.COM	JOHND	ターゲット	iSeries A 上の i5/OS ユーザー・プロファイル
John Day	ISERIESB.MYCO.COM	DAYJO	ターゲット	iSeries 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	ISERIESA.MYCO.COM	SHARONJ	ターゲット	iSeries A 上の i5/OS ユーザー・プロファイル
Sharon Jones	ISERIESB.MYCO.COM	JONESSH	ターゲット	iSeries B 上の i5/OS ユーザー・プロファイル

表 8. 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・アソシエーション

ポリシー・アソシエーション・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	ISERIESA.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	ISERIESB.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

関連情報

EIM (エンタープライズ識別マッピング)
ネットワーク認証サービス

iSeries A の基本シングル・サインオン構成を作成する

EIM 構成ウィザードは、基本的な EIM 構成を作成するのに役立ち、さらにネットワーク認証サービス・ウィザードを開き、基本的なネットワーク認証サービス構成を作成できるようになります。

注: このシナリオの説明は、これまでに iSeries 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、すでにディレクトリー・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、構成ステップ内の該当する個所で注記されます。

iSeries 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、次のことを行ってください。

- 新しい EIM ドメインを作成する。
- iSeries 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。
- iSeries 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。
- iSeries A を構成して、EIM ドメインに参加する。
 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」と展開します。
 2. 「構成」を右マウス・ボタン・クリックし、「構成」を選択して、EIM 構成ウィザードを開始します。
 3. 「ウェルカム (Welcome)」ページで、「新規ドメインの作成と結合 (Create and join a new domain)」を選択します。「次へ」をクリックします。
 4. 「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)」を選択します。「次へ」をクリックします。
 5. 以下の作業を行って、ネットワーク認証サービスを構成します。

- a. 「ネットワーク認証サービスの構成 (Configure Network Authentication Service)」 ページで、「はい」を選択します。

注: これで、ネットワーク認証サービス・ウィザードが起動します。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almに参加できます。

- b. 「レalm情報の指定 (Specify Realm Information)」 ページで、「デフォルト・レalm (Default realm)」 フィールドに「MYCO.COM」と入力し、「Microsoft Active Directory を Kerberos 認証に使用 (Microsoft Active Directory is used for Kerberos authentication)」を選択します。「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」 フィールドの Kerberos サーバーの名前に「kdc1.myco.com」と入力し、「ポート」 フィールドに「88」と入力します。「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」を選択します。「パスワード・サーバー (Password server)」 フィールドに「kdc1.myco.com」と入力し、「ポート」 フィールドに「464」と入力します。「次へ」をクリックします。
- e. 「Keytab エントリーの選択 (Select Keytab Entries)」 ページで、「i5/OS Kerberos 認証 (OS/400 Kerberos Authentication)」を選択します。「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の入力と確認を行い、「次へ」をクリックします。たとえば、iseriesa123 です。このパスワードは、iSeries 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。

注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティーを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。

- g. 「バッチ・ファイルの作成 (Create Batch File)」 ページで「はい」を選択し、次の情報を指定して、「次へ」をクリックします。
 - バッチ・ファイル: デフォルトのバッチ・ファイル名の末尾に、テキスト iseriesa を追加します。たとえば、C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigiseriesa.bat です。
 - 「パスワードの組み込み (Include password)」を選択します。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。重要なことは、パスワードを平文で表示すると、バッチ・ファイルへの読み取りアクセスによって、だれかに読まれるおそれがあることに注意することです。したがって、バッチ・ファイルは、使用后ただちに、Kerberos サーバーおよび 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と、バッチ・ファイルの実行時にプロンプトでパスワードの入力を求められます。

- h. 「サマリー」 ページで、ネットワーク認証サービス構成の詳細を検討します。「終了」をクリックします。
6. 「ディレクトリー・サーバーの構成 (Configure Directory Server)」 ページで次の情報を入力し、「次へ」をクリックします。

注: このシナリオを開始する前にディレクトリー・サーバーを構成した場合は、「ディレクトリー・サーバーの構成 (Configure Directory Server)」 ページではなく「接続のためにユーザーを指定 (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: 389

- 識別名: cn=administrator
- パスワード: mycopwd

注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。

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します。たとえば、MyCoEimDomain です。
8. 「ドメインの親 DN を指定 (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。

注: ディレクトリー・サーバーがアクティブの場合は、変更内容を有効にするために、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ます。

9. 「レジストリー情報」 ページで、「ローカル i5/OS」 および「Kerberos」 を選択します。「次へ」 をクリックします。レジストリー名は書き留めておいてください。これらのレジストリー名は、EIM ID とのアソシエーションを作成する際に必要です。

注:

- レジストリー名は、ドメインに対して固有でなければなりません。
- 固有のレジストリー定義命名計画を使用する場合は、ユーザー・レジストリーに固有のレジストリー定義名を入力できます。しかし、このシナリオの場合は、デフォルト値を受け入れてもかまいません。

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・システム機能に代わって EIM 操作を実行する際にオペレーティング・システムが使用するユーザーを選択して、「次へ」 をクリックします。

注: このシナリオでは、ステップの実行前に、ディレクトリー・サーバーを構成しなかったため、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: Distinguished name and password
- 識別名: cn=administrator
- パスワード: mycopwd

注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。

11. 「サマリー」 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。

iSeries A での基本的な EIM およびネットワーク認証サービスの構成は終了しました。次のステップは、iSeries B を構成して、作成したばかりの EIM ドメインに参加することです。

iSeries B を構成して、EIM ドメインに参加し、ネットワーク認証サービス用に iSeries B を構成する

iSeries 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、iSeries B を構成して、EIM ドメインに参加し、iSeries 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. 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」と展開します。
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 (Welcome)」ページで、「既存ドメインの結合 (Join an existing domain)」を選択します。「次へ」をクリックします。
4. 以下の作業を行って、ネットワーク認証サービスを構成します。

- a. 「ネットワーク認証サービスの構成 (Configure Network Authentication Service)」ページで、「はい」を選択します。

注: これで、ネットワーク認証サービス・ウィザードが起動します。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 (Default realm)」フィールドに「MYCO.COM」と入力し、「Microsoft Active Directory を Kerberos 認証に使用 (Microsoft Active Directory is used for Kerberos authentication)」を選択します。「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」フィールドの Kerberos サーバーの名前に「kdc1.myco.com」と入力し、「ポート」フィールドに「88」と入力します。「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」を選択します。「パスワード・サーバー (Password server)」フィールドに「kdc1.myco.com」と入力し、「ポート」フィールドに「464」と入力します。「次へ」をクリックします。
- e. 「Keytab エントリーの選択 (Select Keytab Entries)」ページで、「i5/OS Kerberos 認証 (OS/400 Kerberos Authentication)」を選択します。「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の入力と確認を行い、「次へ」をクリックします。たとえば、iseriesa123 です。このパスワードは、iSeries 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。

注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。

- g. 「バッチ・ファイルの作成 (Create Batch File)」ページで「はい」を選択し、次の情報を指定して、「次へ」をクリックします。
 - **バッチ・ファイル:** デフォルトのバッチ・ファイル名の末尾に、テキスト iseriesb を追加します。たとえば、C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigiseriesb.bat です。
 - 「パスワードの組み込み (Include password)」を選択します。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。重要なことは、パスワードを平文で表示すると、バッチ・ファイルへの読み取りアクセスによって、だれかに読まれるおそれがあることに注意することです。したがって、バッチ・ファイルは、使用后ただちに、Kerberos サーバーおよび 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と、バッチ・ファイルの実行時にプロンプトでパスワードの入力を求められます。

- h. 「サマリー」ページで、ネットワーク認証サービス構成の詳細を検討します。「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、次の情報を入力し、「次へ」をクリックします。
 - ドメイン・コントローラー名: iseriesa.myco.com
 - ポート: 389
6. 「接続のためにユーザーを指定 (Specify User for Connection)」 ページで、次の情報を入力し、「次へ」をクリックします。

注: iSeries 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。

- ユーザー・タイプ: Distinguished name and password
- 識別名: cn=administrator
- パスワード: mycopwd

注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティーを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。

7. 「ドメインの指定 (Specify Domain)」 ページで、結合する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、MyCoEimDomain です。
8. 「レジストリー情報」 ページで、「ローカル i5/OS」を選択し、「Kerberos レジストリー」を選択解除します。(Kerberos レジストリーは、MyCoEimDomain ドメインを作成したときに作成されました。)「次へ」をクリックします。レジストリー名は書き留めておいてください。これらのレジストリー名は、EIM ID とのアソシエーションを作成する際に必要です。

注:

- レジストリー名は、ドメインに対して固有でなければなりません。
- 固有のレジストリー定義命名計画を使用する場合は、ユーザー・レジストリーに固有のレジストリー定義名を入力できます。しかし、このシナリオの場合は、デフォルト値を受け入れてもかまいません。

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・システム機能に代わって EIM 操作を実行する際にオペレーティング・システムが使用するユーザーを選択して、「次へ」をクリックします。

注: iSeries 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。

- ユーザー・タイプ: Distinguished name and password
- 識別名: cn=administrator
- パスワード: mycopwd

注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティーを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。

10. 「サマリー」 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、ドメインに参加し、ネットワーク認証サービスを使用する iSeries B を構成しました。

両方の i5/OS サービス・プリンシパルを Kerberos サーバーに追加する

必要な i5/OS サービス・プリンシパルを Kerberos サーバーに追加する場合は、2 つの方法のいずれかを使用できます。サービス・プリンシパルを手動で追加することもできれば、このシナリオの説明のように、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場合は、FTP (ファイル転送プロトコル) を使用してファイルを Kerberos サーバーにコピーして、実行できます。

バッチ・ファイルを使用してプリンシパル名を Kerberos サーバーに追加するときは、以下のステップに従います。

ウィザードが作成する FTP バッチ・ファイル

1. 管理者がネットワーク認証サービスを構成する際に使用した Windows 2000 ワークステーション上でコマンド・プロンプトを開き、`ftp kdc1.myco.com` と入力します。これで、ご使用の PC 上に FTP セッションを開始します。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。
2. FTP プロンプトで、`lcd "C:\Documents and Settings\All Users\Documents\IBM\Client Access"` と入力します。Enter キーを押します。Local directory now C:\Documents and Settings\All Users\Documents\IBM\Client Access のメッセージを受け取るはずですが、
3. FTP プロンプトで、`cd %mydirectory` と入力します。ここで、*mydirectory* は kdc1.myco.com 上にあるディレクトリーです。
4. FTP プロンプトで、`put NASConfigiseriesa.bat` と入力します。226 転送は完了のメッセージを受け取るはずですが、
5. `quit` と入力して、FTP セッションを終了します。

注: 以下のステップを繰り返して、NASConfigiseriesb.bat ファイルを Windows 2000 サーバーに転送します。

kdc1.myco.com で両方のバッチ・ファイルを実行する

1. ご使用の Windows 2000 サーバーで、バッチ・ファイルを転送したディレクトリーを開きます。
2. NASConfigiseriesa.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。
3. NASConfigiseriesb.bat に以下のステップを繰り返します。
4. 各ファイルの実行後、次のことを行って、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。
 - a. ご使用の Windows 2000 サーバーで、「管理ツール」 → 「Active Directory ユーザーとコンピュータ」 → 「ユーザー」と展開します。
 - b. 該当する Windows 2000 ドメインを選択して、iSeries 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のレルム名と同じでなければなりません。

- c. 表示されたユーザーのリストで、**iseriesa_1_krbsvr400** および **iseriesb_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。
- d. (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、「アカウントは委任に対して信頼できる (Account is trusted for delegation)」を選択します。

注: このオプション・ステップによって、ご使用システムは、ユーザーの信任状を他のシステムに委譲あるいは転送することができます。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。これは多重層ネットワークでは便利です。

これで、i5/OS サービス・プリンシパルが Kerberos サーバーに追加されたので、ここで iSeries システムにユーザー・プロファイルを作成できます。

ユーザー・プロファイルを iSeries A および iSeries B 上に作成する

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 iSeries システムの単一の 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、iSeries A および iSeries 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。

これらのユーザーのユーザー・プロファイルを作成する場合は、ご使用の計画ワークシートの情報を使用します。

1. iSeries ナビゲーター で、「**iSeries 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**」を右マウス・ボタン・クリックして、「**新規ユーザー...**」を選択します。
3. 「**新規ユーザー**」ダイアログで、「**ユーザー名**」フィールドに SYSUSERA と入力します。
4. 「**パスワード**」フィールドで、「**パスワードなし (サインオンが許可されていない) (No password (sign-on not allowed))**」を選択します。
5. 「**機能**」をクリックします。
6. 「**特権**」ページで、「**特権クラス**」フィールドの「**ユーザー**」を選択します。「**OK**」をクリックして、「**追加**」をクリックします。

iSeries B 上でこれらのステップを繰り返しますが、「**ユーザー名**」フィールドには SYSUSERB と入力します。

これで、iSeries A および iSeries B 上にユーザー・プロファイルを作成されたので、ここで i5/OS ユーザー・プロファイルのすべてにホーム・ディレクトリーを作成できます。

ホーム・ディレクトリーを、iSeries A および iSeries B 上に作成する

iSeries および iSeries 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、次のことを行ってください。

iSeries 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 iSeries ユーザー・プロファイル名です。たとえば、CRTDIR '/home/SYSUSERA' です。これで、すべての Active Directory ユーザーを表す iSeries A 上のユーザー・プロファイルのホーム・ディレクトリーが作成されます。

このコマンドを iSeries B で繰り返し (ただし SYSUSERB を指定して)、iSeries B 上にユーザー・プロファイルのホーム・ディレクトリーを作成します。

これで、ホーム・ディレクトリーが作成されたので、iSeries システム上のネットワーク認証サービス構成をテストできます。

iSeries A および iSeries B 上のネットワーク認証サービスをテストする

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、iSeries A および iSeries 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、以下のステップを行って、iSeries A および iSeries B プリンシパルの発券許可証を要求すると、行うことができます。

注: この手順を行う前に、iSeries 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 Interpreter を開始します。
2. `keytab list` と入力して、キータブ・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、iSeries A のプリンシパル名として、`krbsvr400/iseriasa.myco.com@MYCO.COM` が表示されるはずです。
3. `kinit -k krbsvr400/iseriasa.myco.com@MYCO.COM` と入力して、Kerberos サーバーの発券許可証を要求します。このコマンドを実行すると、ご使用の iSeries 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。これが正常ならば、`kinit` コマンドがエラーなしに表示されます。
4. `klist` と入力して、デフォルトのプリンシパルが `krbsvr400/iseriasa.myco.com@MYCO.COM` であることを検査します。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、iSeries サービス・プリンシパルに有効な許可証が作成され、かつ iSeries 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/iseriasa.myco.com@MYCO.COM
Server: krbtgt/MYCO.COM@MYCO.COM
Valid 200X/06/09-12:08:45 to 20XX/11/05-03:08:45
$
```

iSeries B のサービス・プリンシパル名を使用して、これらのステップを繰り返します:
`krbsvr400/iseriasb.myco.com@MYCO.COM`

これで、iSeries A および iSeries B 上のネットワーク認証サービスはテストされたので、ここで、管理者のそれぞれに EIM ID を作成できます。

2 人の管理者、John Day と Sharon Jones の EIM ID を作成する

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で、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、iSeries 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、1 つは John Day、もう 1 つは Sharon Jones という、2 つの EIM ID を作成します。

EIM ID を作成するには、以下のステップに従います。

1. iSeries で、「iSeries 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プロンプトが出される場合があります。この場合は、「EIM ドメイン・コントローラーへの接続 (Connect to EIM Domain Controller)」ダイアログが表示されます。ドメインでアクションを行うには、それに接続しておく必要があります。ドメイン・コントローラーに接続するには、次の情報を指定して、「OK」をクリックします。

- ユーザー・タイプ: Distinguished name

- 識別名: cn=administrator
- パスワード: mycopwd

注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。

2. 「ID」を右マウス・ボタン・クリックして、「新規 ID...」を選択します。
3. 「新規 EIM ID」ダイアログで、「ID」フィールドに John Day と入力します。
4. 「OK」をクリックします。

ステップ 2 から 4 を繰り返しますが、ID フィールドに Sharon Jones と入力します。

これで、各管理者の EIM ID が作成されたので、ユーザー ID をこの ID にマップする ID アソシエーションを作成する必要があります。まず、John Day の ID アソシエーションを作成します。

John Day の ID アソシエーションを作成する

EIM ID、John Day と、その ID によって表わされる人が使用するユーザー ID 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 アソシエーションが適切に構成されると、それによってユーザーはシングル・サインオン環境に参加できます。

このシナリオでは、John Day ID に、1 つのソース・アソシエーションと 2 つのターゲット・アソシエーションを作成する必要があります。

- jday Kerberos プリンシパルのソース・アソシエーション。これは、当の John Day が Windows およびネットワークにログインする際に使用するユーザー ID です。このソース・アソシエーションで、Kerberos プリンシパルを、対応するターゲット・アソシエーションで定義された別のユーザー ID にマップすることができます。
- JOHND iSeries ユーザー・プロファイルのターゲット・アソシエーション。これは、当の John Day が、iSeries および iSeries A 上の他の iSeries 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・アソシエーションは、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 iSeries ユーザー・プロファイルのターゲット・アソシエーション。これは、当の John Day が、iSeries ナビゲーター および iSeries B 上の他の iSeries 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・アソシエーションは、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。

アソシエーションの作成には、ご使用の計画ワークシートの情報を使用します。

John Day の Kerberos プリンシパルのソース・アソシエーションを作成する場合は、以下のステップに従います。

1. iSeries 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」と展開します。
2. 「John Day」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. 「アソシエーション」ページで、「追加」をクリックします。
4. 「アソシエーションの追加」ダイアログで、「参照...」を指定して次の情報を選択し、「OK」をクリックします。

- レジストリー: MYCO.COM

- ユーザー: jday
 - アソシエーション・タイプ: Source
5. 「OK」をクリックして、「アソシエーションの追加」ダイアログを閉じます。

iSeries A 上に、John Day の iSeries ユーザー・プロファイルのターゲット・アソシエーションを作成するには、以下のステップに従います。

1. 「アソシエーション」ページで、「追加」をクリックします。
2. 「アソシエーションの追加」ダイアログで、「参照...」を指定して次の情報を選択し、「OK」をクリックします。
 - レジストリー: ISERIESA.MYCO.COM
 - ユーザー: JOHND
 - アソシエーション・タイプ: Target
3. 「OK」をクリックして、「アソシエーションの追加」ダイアログを閉じます。

iSeries B 上に、John Day の iSeries ユーザー・プロファイルのターゲット・アソシエーションを作成するには、以下のステップに従います。

4. 「アソシエーション」ページで、「追加」をクリックします。
5. 「アソシエーションの追加」ダイアログで、「参照...」を指定して次の情報を選択し、「OK」をクリックします。
 - レジストリー: ISERIESB.MYCO.COM
 - ユーザー: DAYJO
 - アソシエーション・タイプ: Target
6. 「OK」をクリックして、「アソシエーションの追加」ダイアログを閉じます。
7. 「OK」をクリックして、「プロパティ」ダイアログを閉じます。

これで、John Day のユーザー ID を彼の EIM ID にマップする ID アソシエーションが作成されたので、同様のアソシエーションを Sharon Jones に作成することができます。

Sharon Jones の ID アソシエーションを作成する

EIM ID、Sharon Jones と、その ID によって表わされる人が使用するユーザー ID 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が適切に構成されると、それによってユーザーはシングル・サインオン環境に参加できます。

このシナリオでは、Sharon Jones ID に、1 つのソース・アソシエーションと 2 つのターゲット・アソシエーションを作成する必要があります。

- sjones Kerberos プリンシパルのソース・アソシエーション。これは、当の Sharon Jones が Windows およびネットワークにログインする際に使用するユーザー ID です。このソース・アソシエーションで、Kerberos プリンシパルを、対応するターゲット・アソシエーションで定義された別のユーザー ID にマップすることができます。
- SHARONJ i5/OS ユーザー・プロファイルのターゲット・アソシエーション。これは、当の Sharon Jones が、iSeries ナビゲーター および iSeries 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・アソシエーションは、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・アソシエーション。これは、当の Sharon Jones が、iSeries ナビゲーター および i5/OS B 上の他の iSeries 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・アソシエーションは、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。

アソシエーションの作成には、ご使用の計画ワークシートの情報を使用します。

Sharon Jones の Kerberos プリンシパルのソース・アソシエーションを作成する場合は、以下のステップに従います。

1. iSeries 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」と展開します。
2. 「Sharon Jones」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. 「アソシエーション」ページで、「追加」をクリックします。
4. 「アソシエーションの追加」ダイアログで、「参照...」を指定して次の情報を選択し、「OK」をクリックします。
 - レジストリー: MYCO.COM
 - ユーザー: sjones
 - アソシエーション・タイプ: Source
5. 「OK」をクリックして、「アソシエーションの追加」ダイアログを閉じます。

iSeries 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・アソシエーションを作成するには、以下のステップに従います。

1. 「アソシエーション」ページで、「追加」をクリックします。
2. 「アソシエーションの追加」ダイアログで、「参照...」を指定して次の情報を選択し、「OK」をクリックします。
 - レジストリー: ISERIESA.MYCO.COM
 - ユーザー: SHARONJ
 - アソシエーション・タイプ: Target
3. 「OK」をクリックして、「アソシエーションの追加」ダイアログを閉じます。

iSeries 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・アソシエーションを作成するには、以下のステップに従います。

4. 「アソシエーション」ページで、「追加」をクリックします。
5. 「アソシエーションの追加」ダイアログで、「参照...」を指定して次の情報を選択し、「OK」をクリックします。
 - レジストリー: ISERIESB.MYCO.COM
 - ユーザー: JONESSH
 - アソシエーション・タイプ: Target
6. 「OK」をクリックして、「アソシエーションの追加」ダイアログを閉じます。
7. 「OK」をクリックして、「プロパティ」ダイアログを閉じます。

これで、Sharon Jones のユーザー ID を彼女の EIM ID にマップする ID アソシエーションが作成されたので、ここで、Kerberos レジストリー・ユーザーのすべてを各 iSeries ユーザー・レジストリーの特定のユーザー・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・アソシエーションを作成できます。

デフォルト・レジストリー・ポリシー・アソシエーションを作成する

Windows 2000 サーバー上の Microsoft Active Directory ユーザーのすべてを、iSeries A 上のユーザー・プロファイル、SYSUSERA、ならびに iSeries B 上のユーザー・プロファイル、SYSUSERB にマップする必要があります。

幸いにも、ポリシー・アソシエーションを使用すると、ユーザーのグループと単一のターゲット・ユーザー ID 間の直接マッピングを作成できます。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 iSeries 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・レジストリー・ポリシー・アソシエーションを作成できます。

これを行うには、2 つのポリシー・アソシエーションが必要です。各ポリシー・アソシエーションは、MYCO.COM ユーザー・レジストリー定義をアソシエーションのソースとして使用します。しかし、各ポリシー・アソシエーションは、Kerberos ユーザーがアクセスする iSeries システムによっては、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。

- MYCO.COM ユーザー・レジストリー内の Kerberos プリンシパルを、ISERIESA.MYCO.COM のターゲット・レジストリー内の SYSUSERA のターゲット・ユーザーにマップするポリシー・アソシエーションもあります。
- また、MYCO.COM ユーザー・レジストリー内の Kerberos プリンシパルを、ISERIESB.MYCO.COM のターゲット・レジストリー内の SYSUSERB のターゲット・ユーザーにマップするポリシー・アソシエーションもあります。

2 つのデフォルト・レジストリー・ポリシー・アソシエーションを作成するには、ご使用の計画ワークシートの情報を使用します。

注: しかし、ポリシー・アソシエーションを使用するには、まず必ずドメインがポリシー・アソシエーションをマッピング探索操作に使用できるようにしておく必要があります。これは、以下のように、ポリシー・アソシエーションを作成するプロセスの一環で行うことができます。

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**」 → 「**ドメイン管理**」と展開します。
2. 「**MyCoEimDomain**」を右マウス・ボタン・クリックして、「**マッピング・ポリシー...**」を選択します。
3. 「**一般**」ページで、「**ドメイン MyCoEimDomain のポリシー・アソシエーションを使用してマッピング探索を使用可能にする (Enable mapping lookups using policy associations for domain MyCoEimDomain)**」を選択します。

以下のステップに従って、ユーザーのデフォルト・レジストリー・ポリシー・アソシエーションを作成し、iSeries A 上の SYSUSERA ユーザー・プロファイルにマップします。

1. 「**レジストリー**」ページで、「**追加**」をクリックします。
2. 「**デフォルト・レジストリー・ポリシー・アソシエーションの追加 (Add Default Registry Policy Association)**」ダイアログで、「**参照...**」を指定して次の情報を選択し、「**OK**」をクリックします。
 - ソース・レジストリー: MYCO.COM
 - ターゲット・レジストリー: ISERIESA.MYCO.COM
 - ターゲット・ユーザー: SYSUSERA
3. 「**OK**」をクリックして、「**マッピング・ポリシー**」ダイアログを閉じます。

以下のステップに従って、ユーザーのデフォルト・レジストリー・ポリシー・アソシエーションを作成し、iSeries B 上の SYSUSERB ユーザー・プロファイルにマップします。

4. 「レジストリー」ページで、「追加」をクリックします。
5. 「デフォルト・レジストリー・ポリシー・アソシエーションの追加 (Add Default Registry Policy Association)」ダイアログで、「参照...」を指定して次の情報を選択し、「OK」をクリックします。
 - ソース・レジストリー: MYCO.COM
 - ターゲット・レジストリー: ISERIESB.MYCO.COM
 - ターゲット・ユーザー: SYSUSERB
6. 「OK」をクリックして、「マッピング・ポリシー」ダイアログを閉じます。

これで、デフォルト・レジストリー・ポリシー・アソシエーションが作成されたので、レジストリーに探索操作に参加させたり、ポリシー・アソシエーションを使用させたりできます。

レジストリーを使用できるようにして、探索操作に参加し、ポリシー・アソシエーションを使用する

EIM を使用すると、各レジストリーの EIM への参加方法を制御できます。ポリシー・アソシエーションの企業内での効力を大規模にすることができるので、ポリシー・アソシエーションによるレジストリーへの影響を制御できます。また、レジストリーがマッピング探索操作に少しでも参加できるかどうかを制御できます。ポリシー・アソシエーションをレジストリーに使用するには、そのレジストリーが探索操作に参加できるようにするだけでなく、ポリシー・アソシエーションがそのレジストリーを使用できる必要があります。

レジストリーがポリシー・アソシエーションを使用し、かつ探索操作に参加できるようにするには、以下のステップを行います。

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、以下のステップに従います。

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」 → 「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」レジストリーを右マウス・ボタン・クリックして、「マッピング・ポリシー...」を選択します。
3. 「一般」ページで、「レジストリー MYCO.COM のマッピング探索を使用可能にする (Enable mapping lookups for registry MYCO.COM)」を選択して、「OK」をクリックします。

ISERIESA.MYCO.COM レジストリーがマッピング探索操作に参加し、ポリシー・アソシエーションを使用できるようにするには、以下のステップに従います。

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」 → 「ドメイン管理」 → 「MyCoEimDomain」 → 「ユーザー・レジストリー」と展開します。
2. 「ISERIESA.MYCO.COM」レジストリーを右マウス・ボタン・クリックして、「マッピング・ポリシー...」を選択します。
3. 「一般」ページで、「レジストリー ISERIESA.MYCO.COM のマッピング探索を使用可能にする (Enable mapping lookups for registry ISERIESA.MYCO.COM)」を選択し、「ポリシー・アソシエーションを使用 (Use policy associations)」を選択して、「OK」をクリックします。

これらのステップを繰り返して、ISERIESB.MYCO.COM レジストリーをマッピング探索操作に参加し、ポリシー・アソシエーションを使用できるようにしますが、「一般」ページでは、「レジストリー

ISERIESB.MYCO.COM のマッピング探索を使用可能にする (Enable mapping lookups for registry ISERIESB.MYCO.COM)」を選択し、「ポリシー・アソシエーションを使用 (Use policy associations)」を選択して、「OK」をクリックします。

これで、レジストリーおよびユーザーの EIM 構成は完了したので、その結果のマッピングをテストし、計画どおり働くかどうかを確認する必要があります。

EIM ID マッピングをテストする

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て正しい結果を戻すかどうかを検査する必要があります。このシナリオでは、管理者ごとに ID アソシエーションに使用するマッピングをテストし、かつデフォルト・レジストリー・ポリシー・アソシエーションに使用す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、以下のステップに従います。

John Day のマッピングをテストする

John Day の ID マッピングが予想どおり働くことをテストするには、以下のステップに従います。

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」→「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プロンプトが出される場合があります。この場合は、「EIM ドメイン・コントローラーへの接続 (Connect to EIM Domain Controller)」ダイアログが表示されます。ドメインでアクションを行うには、それに接続しておく必要があります。ドメイン・コントローラーに接続するには、次の情報を指定して、「OK」をクリックします。

- ユーザー・タイプ: Distinguished name
- 識別名: cn=administrator
- パスワード: mycopwd

注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティーを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。

2. 「MyCoEimDomain」を右マウス・ボタン・クリックして、「マッピングのテスト...」を選択します。
3. 「マッピングのテスト」ダイアログで、「参照...」を指定して次の情報を選択し、「テスト」をクリックします。
 - ソース・レジストリー: MYCO.COM
 - ソース・ユーザー: jday
 - ターゲット・レジストリー: ISERIESA.MYCO.COM
4. ページの「検出されたマッピング」の部分に、以下のように結果が表示されます。

以下のフィールドの場合	以下の結果を参照
ターゲット・ユーザー	JOHND
オリジン (起点)	EIM ID: John Day

5. 「クローズ」をクリックします。

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」フィールドでは「ISERIESB.MYCO.COM」を選択します。ページの「検出されたマッピング」の部分に、以下のように結果

が表示されます。

以下のフィールドの場合	以下の結果を参照
ターゲット・ユーザー	DAYJO
オリジン (起点)	EIM ID: John Day

Sharon Jones のマッピングをテストする

Sharon Jones の個々のアソシエーションに使用するマッピングをテストするには、以下のステップに従います。

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」 → 「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プロンプトが出される場合があります。この場合は、「EIM ドメイン・コントローラーへの接続 (Connect to EIM Domain Controller)」ダイアログが表示されます。ドメインでアクションを行うには、それに接続しておく必要があります。ドメイン・コントローラーに接続するには、次の情報を指定して、「OK」をクリックします。

- ユーザー・タイプ: Distinguished name
- 識別名: cn=administrator
- パスワード: mycopwd

注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティーを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。

2. 「MyCoEimDomain」を右マウス・ボタン・クリックして、「マッピングのテスト...」を選択します。
3. 「マッピングのテスト」ダイアログで、「参照...」を指定して次の情報を選択し、「テスト」をクリックします。
 - ソース・レジストリー: MYCO.COM
 - ソース・ユーザー: sjones
 - ターゲット・レジストリー: ISERIESA.MYCO.COM
4. ページの「検出されたマッピング」の部分に、以下のように結果が表示されます。

以下のフィールドの場合	以下の結果を参照
ターゲット・ユーザー	SHARONJ
オリジン (起点)	EIM ID: Sharon Jones

5. 「クローズ」をクリックします。

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」フィールドでは「ISERIESB.MYCO.COM」を選択します。ページの「検出されたマッピング」の部分に、以下のように結果が表示されます。

以下のフィールドの場合	以下の結果を参照
ターゲット・ユーザー	JONESSH
オリジン (起点)	EIM ID: Sharon Jones

デフォルト・レジストリー・ポリシー・アソシエーションに使用するマッピングをテストする

受注部門のユーザーのマッピングが、定義したポリシー・アソシエーションに基づいて期待どおり働いているかをテストするには、以下のステップに従います。

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**」 → 「**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プロンプトが出される場合があります。この場合は、「**EIM ドメイン・コントローラーへの接続 (Connect to EIM Domain Controller)**」ダイアログが表示されます。ドメインでアクションを行うには、それに接続しておく必要があります。ドメイン・コントローラーに接続するには、次の情報を指定して、「**OK**」をクリックします。

- **ユーザー・タイプ:** Distinguished name
- **識別名:** cn=administrator
- **パスワード:** mycopwd

注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティーを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。

2. 「**MyCoEimDomain**」を右マウス・ボタン・クリックして、「**マッピングのテスト...**」を選択します。
3. 「**マッピングのテスト**」ダイアログで、「**参照...**」を指定して次の情報を選択し、「**テスト**」をクリックします。
 - **ソース・レジストリー:** MYCO.COM
 - **ソース・ユーザー:** mmiller
 - **ターゲット・レジストリー:** ISERIESA.MYCO.COM
4. ページの「**検出されたマッピング**」の部分に、以下のように結果が表示されます。

以下のフィールドの場合	以下の結果を参照
ターゲット・ユーザー	SYSUSERA
オリジン (起点)	レジストリー・ポリシー・アソシエーション

5. 「**クローズ**」をクリックします。

ユーザーを iSeries B 上の SYSUSERB プロファイルへマップするデフォルト・レジストリー・ポリシー・アソシエーションに使用するマッピングをテストするには、以下のステップに従います。

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**」 → 「**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プロンプトが出される場合があります。この場合は、「**EIM ドメイン・コントローラーへの接続 (Connect to EIM Domain Controller)**」ダイアログが表示されます。ドメインでアクションを行うには、それに接続しておく必要があります。ドメイン・コントローラーに接続するには、次の情報を指定して、「**OK**」をクリックします。

- **ユーザー・タイプ:** Distinguished name
- **識別名:** cn=administrator
- **パスワード:** mycopwd

注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティーを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。

2. 「MyCoEimDomain」を右マウス・ボタン・クリックして、「マッピングのテスト...」を選択します。
3. 「マッピングのテスト」ダイアログで、「参照...」を指定して次の情報を選択し、「テスト」をクリックします。
 - ソース・レジストリー: MYCO.COM
 - ソース・ユーザー: ksmith
 - ターゲット・レジストリー: ISERIESB.MYCO.COM
4. ページの「検出されたマッピング」の部分に、以下のように結果が表示されます。

以下のフィールドの場合	以下の結果を参照
ターゲット・ユーザー	SYSUSERB
オリジン (起点)	レジストリー・ポリシー・アソシエーション

5. 「クローズ」をクリックします。

マッピング関係または通信関係の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』を参照して、これらの問題の解決方法を見つけてください。

これで、EIM ID のマッピングがテストされたので、ここで、Kerberos 認証を使用する iSeries Access for Windows アプリケーションを構成することができます。

Kerberos 認証を使用する iSeries Access for Windows アプリケーションを構成する

iSeries ナビゲーター を使用してシステムにアクセスするには、Kerberos を使用して認証しておく必要があります。したがって、PC から、Kerberos 認証を使用する iSeries Access for Windows を構成する必要があります。

Kerberos 認証を使用する iSeries Access for Windows アプリケーションを構成するには、次のことを行ってください。

注: ユーザーのそれぞれが、自らの PC で以下のステップをすべて行う必要があります。

1. ご使用の PC にサインインして、Windows 2000 ドメインにログオンします。
2. ご使用の PC の iSeries ナビゲーター で、「iSeries 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 プリンシパル名を使用、プロンプトなし (Use Kerberos principal name, no prompting)」を選択します。これで、iSeries 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. 接続設定に加えられた変更を有効にするには、現在稼働中のすべてのアプリケーションを閉じて、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。「OK」をクリックします。次に、iSeries ナビゲーター を終了して、再始動します。

これで、Kerberos 認証を使用する iSeries Access for Windows アプリケーションが構成されたので、ここで、シングル・サインオン環境を検査することができます。

ネットワーク認証サービスと EIM 構成を検証する

これで、シングル・サインオン構成を個々に検査し、すべてのセットアップが完全であることが確認されたので、ここで、EIM およびネットワーク認証サービスを正しく構成したこと、かつシングル・サインオンが予想どおり働くことを検査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査するために、John Day に以下のステップを実行してもらいます。

1. iSeries ナビゲーター で、「iSeries A」を展開して、iSeries A への接続を開きます。
2. F5 を押して、画面を最新表示します。
3. 右側のペインの「名前」欄で、iSeries 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、iSeries 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 iSeries A ユーザー・プロファイルにマップしました。iSeries A の iSeries 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。

Sharon Jones および、SYSUSERA または SYSUSERB ユーザー・プロファイルにマップされるユーザー ID のうち少なくとも 1 つについて、これらのステップを繰り返します。

(オプション) 構成後の考慮事項

ここで、このシナリオは終了したので、これで EIM が使用できると定義した EIM ユーザーのみが LDAP 管理者の DN です。iSeries A 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かつ限定されたアクセス制御権を持つ追加のユーザーとして、1 つ以上の DN を作成することを考慮することもできます。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対するセキュリティ・ポリシーの力点の置き方によって異なります。一般に、次のタイプの少なくとも 2 つの DN を作成します。

• EIM 管理者のアクセス制御権を持つユーザー

この EIM 管理者 DN には、EIM ドメインを管理する責任がある管理者のしかるべきレベルの権限があります。この EIM 管理者 DN は、iSeries 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権のすべてを持つ少なくとも 1 つのユーザー:

- ID 管理者
- レジストリー管理者
- EIM マッピング操作

このユーザーには、オペレーティング・システムに代わって EIM 操作を行うシステム・ユーザーに必要な、しかるべきレベルのアクセス制御権があります。

注: この新しい DN を LDAP 管理者 DN ではなくシステム・ユーザーに使用するには、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は、セットアップするすべての iSeries システムについて、EIM 構成プロパティの変更が必要です。システム・ユーザー DN の変更方法を確認するには『EIM 構成プロパティの管理』を参照してください。

シナリオ: ネットワーク認証サービスおよび EIM を複数システムに反映させる

このシナリオでは、iSeries™ ナビゲーターで機能同期化ウィザードを使用して、OS/400® リリース混合環境の複数のシステム全体にシングル・サインオン構成を反映させる方法を実証します。管理者は、各システムを個々に構成するのではなく、シングル・サインオンを一度構成すると、その構成をそのシステムのすべてに反映させることで、時間を節約できます。

状況

大規模な自動車部品メーカーのネットワーク管理者であるとして、iSeries ナビゲーターを備えたシステムを 5 台管理します。1 台のシステムがセントラル・システムとして動作し、データの保管とエンドポイント・システムの管理を行います。シングル・サインオンの利点について資料を読み、自社用のシングル・サインオン環境を構成したいものとして、現在、1 台のシステムでテスト環境のセットアップ・プロセスを完了したところであり、今後、社内全体にシングル・サインオン環境を拡大したいと考えています。他に構成が必要なサーバーが 4 台あります。それらのサーバーをできるだけ効率よく構成する方法を探しています。

iSeries ナビゲーター が提供する機能同期化ウィザードを使用すると、1 台のシステムのシングル・サインオン構成をコピーし、他の i5/OS V5R3 以降のシステムに適用できます。この方法を採用すると、各システムを別々に構成する必要がなくなります。

しかし、システムの 1 つが、OS/400 バージョン 5 リリース 2 (V5R2) を実行しています。OS/400 V5R2 は、機能同期化ウィザードをサポートしません。つまり、このシステムを別途構成して、モデル・システムの現在のネットワーク認証サービスと EIM の構成と一致させる必要があります。

このシナリオには、以下の利点があります。

- シングル・サインオン環境を作成するためにネットワーク認証サービスと EIM を複数のシステムで構成する作業を単純化する。
- 1 つのウィザードを使用して 1 つの手動構成を他の複数のサーバーにコピーし、適用するので、時間と労力を節約する。

目的

MyCo, Inc. のネットワーク管理者として、すべてのサーバーが関わる自社用のシングル・サインオン環境を作成し、できるだけ迅速かつ簡単にサーバーを構成したいものとして、

このシナリオの目的は次のとおりです。

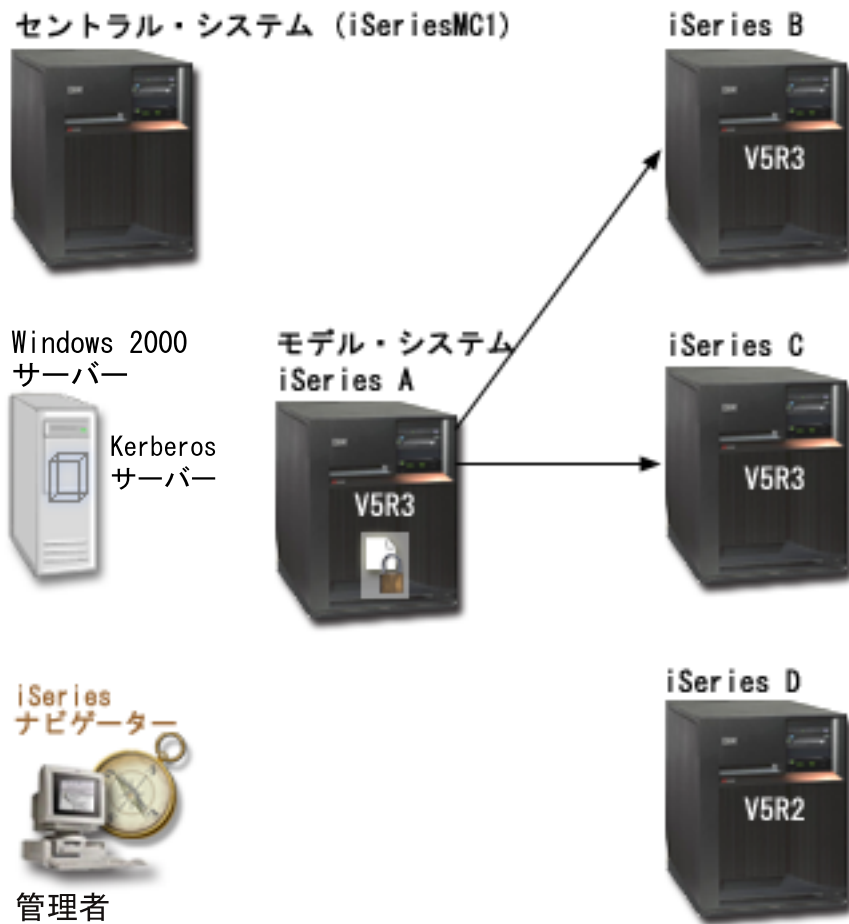
- iSeries A には、テスト環境を作成するためにセットアップされたときから、既存のネットワーク認証サービスと EIM の構成があります。したがって、iSeries B および iSeries C のエンドポイントにこれらの構成を反映させるためのモデル・システムとして、iSeries A を使用する必要があります。
- すべてのシステムが同じ EIM ドメインに加わるように構成され、同じ Kerberos サーバーと同じドメイン・コントローラーを使用する必要があります。

注: 2 つのタイプのドメイン (EIM ドメインと Windows 2000 ドメイン) がシングル・サインオン環境に適合する方法を確認するには、『ドメイン』を参照してください。

- iSeries D である OS/400 V5R2 システムは、ネットワーク認証サービスと EIM 用に手作業で構成されなければなりません。

詳細

以下の図で、このシナリオのネットワーク環境を説明します。



この図で、このシナリオに関連する以下の諸点を説明します。

Windows 2000 サーバー

- ネットワークの鍵配布センター (KDC) としても知られている、Kerberos サーバーの役目をします。
- すべてのユーザーは、Windows 2000 サーバー上の Kerberos サーバーに登録されます。

iSeries MC1 - セントラル・システム

- 次のオプションおよびライセンス製品をインストールした i5/OS バージョン 5 リリース 4 (V5R4) 以降を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12)
 - iSeries Access for Windows (5722-XE1)
- エンドポイント・システムごとに機能同期化タスクを保管し、スケジュールし、実行します。
- ネットワーク認証サービスと EIM 用に構成されます。

iSeries A - モデル・システム

注: モデル・システムは、10 ページの『シナリオ: シングル・サインオンのテスト環境を作成する』のシナリオで iSeries A として識別されたシステムと同様に構成する必要があります。このシナリオを参照して、モデル・システム上のすべてのシングル・サインオン構成タスクが完了し、検証されていることを確認してください。

- 次のオプションおよびライセンス製品をインストールした i5/OS バージョン 5 リリース 4 (V5R4) を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12)
 - iSeries Access for Windows (5722-XE1)
- ネットワーク認証サービスと EIM 用に構成されます。
- ネットワーク認証サービスと EIM の構成を受動システムに反映させる元のモデル・システムです。

iSeries B

- 次のオプションおよびライセンス製品をインストールした i5/OS バージョン 5 リリース 4 (V5R4) を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12)
 - iSeries Access for Windows (5722-XE1)
- ネットワーク認証サービスと EIM の構成を伝搬させる宛先の受動システムの 1 つです。

iSeries C

- 次のオプションおよびライセンス製品をインストールした i5/OS バージョン 5 リリース 4 (V5R4) を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12)
 - iSeries Access for Windows (5722-XE1)
- ネットワーク認証サービスと EIM の構成を伝搬させる宛先の受動システムの 1 つです。

iSeries D

- 次のオプションおよびライセンス製品をインストールした OS/400 バージョン 5 リリース 2 (V5R2) を実行します。
 - OS/400 Host Servers (5722-SS1 オプション 12)
 - iSeries Access for Windows (5722-XE1)
 - Cryptographic Access Provider (5722-AC3)
- 次の V5R2 PTF (プログラム一時修正) が適用されます。
 - SI08977
 - SI08979
- iSeries ナビゲーター の該当するウィザードを使用して、ネットワーク認証サービスと EIM を手動で別々に構成する必要があります。

管理者の PC

- i5/OS V5R4 iSeries Access for Windows (5722-XE1) を実行します。
- 次のサブコンポーネントを備えた i5/OS V5R4 iSeries 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の管理に使用される 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

このシナリオを正常にインプリメントするには、次の前提条件および前提事項が満たされる必要があります。

iSeries MC1 - 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など、すべてのシステム要件が検査されている。

これらのライセンス・プログラムがインストールされていることを検査するには、以下のことを行ってください。

- a. iSeries ナビゲーター で、「iSeries server」 → 「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」と展開する。
 - b. 必要なライセンス・プログラムがすべてインストールされていることを確認する。
2. 必要なハードウェア計画およびセットアップがすべて完了している。
 3. TCP/IP および基本的なシステム・セキュリティが構成され、テスト済みである。
 4. これらのサーバー間のデータ送信を保護するために、Secure Sockets Layer (SSL) が構成されている。

注: サーバー間でネットワーク構成サービスの構成を反映させる際に、パスワードなどの機密情報がネットワークを經由して送信されます。ローカル・エリア・ネットワーク (LAN) 外に送信する場合は特に、SSL を使用してこの情報を保護する必要があります。詳しくは、『シナリオ: SSL を使用してマネージメント・セントラル・サーバーとのすべての接続を保護する』を参照してください。

iSeries A - モデル・システムの前提条件

注: このシナリオでは、iSeries A がシングル・サインオン用に適切に構成されていることを前提とします。10 ページの『シナリオ: シングル・サインオンのテスト環境を作成する』シナリオを参照して、モデル・システム上のすべてのシングル・サインオン構成タスクが完了し、検証されていることを確認してください。

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など、すべてのシステム要件が検査されている。

これらのライセンス・プログラムがインストールされていることを検査するには、以下のことを行ってください。

- a. iSeries ナビゲーター で、「iSeries server」 → 「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」と展開する。
 - b. 必要なライセンス・プログラムがすべてインストールされていることを確認する。
2. 必要なハードウェア計画およびセットアップがすべて完了している。
 3. TCP/IP および基本的なシステム・セキュリティが構成され、テスト済みである。
 4. これらのサーバー間のデータ送信を保護するために、Secure Sockets Layer (SSL) が構成されている。

注: サーバー間でネットワーク構成サービスの構成を反映させる際に、パスワードなどの機密情報がネットワークを經由して送信されます。ローカル・エリア・ネットワーク (LAN) 外に送信する場合は特に、SSL を使用してこの情報を保護する必要があります。詳しくは、『シナリオ: SSL を使用してマネージメント・セントラル・サーバーとのすべての接続を保護する』を参照してください。

iSeries B, iSeries C, および iSeries 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など、すべてのシステム要件が検査されている。

これらのライセンス・プログラムがインストールされていることを検査するには、以下のことを行ってください。

- a. iSeries ナビゲーター で、「iSeries server」 → 「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」と展開する。
 - b. 必要なライセンス・プログラムがすべてインストールされていることを確認する。
2. 必要なハードウェア計画およびセットアップがすべて完了している。
 3. TCP/IP および基本的なシステム・セキュリティが構成され、テスト済みである。
 4. これらのサーバー間のデータ送信を保護するために、Secure Sockets Layer (SSL) が構成されている。

注: サーバー間でネットワーク構成サービスの構成を反映させる際に、パスワードなどの機密情報がネットワークを経由して送信されます。ローカル・エリア・ネットワーク (LAN) 外に送信する場合は特に、SSL を使用してこの情報を保護する必要があります。詳しくは、『シナリオ: SSL を使用してマネージメント・セントラル・サーバーとのすべての接続を保護する』を参照してください。

Windows 2000 サーバー前提条件

1. 必要なすべてのハードウェア計画およびセットアップが完了している。
2. サーバー上で TCP/IP が構成され、テスト済みである。
3. Windows 2000 ドメインが構成され、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 Kerberos サーバーに追加されている。

構成ステップ

ネットワーク認証サービスと EIM の構成を、モデル・システムである iSeries A から、エンドポイント・システムである iSeries B および iSeries C に反映させるためには、次のタスクを実行する必要があります。

注: 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) の概念を含む、シングル・サインオンに関連する概念を理解しておく必要があります。シングル・サインオンに関連する用語と概念を確認する場合は、以下の情報を参照してください。

関連情報

EIM (エンタープライズ識別マッピング)

ネットワーク認証サービス

計画ワークシートに記入する

次の計画ワークシートは、一般のシングル・サインオン計画ワークシートを基にして、このシナリオに合うように調整したものです。これらの計画ワークシートでは、このシナリオの準備をするために収集する必要がある情報、および必要な決定を示します。正常なインプリメンテーションを確保するには、構成作業を行う前に、ワークシートのすべての前提条件項目に「はい」で応答でき、かつワークシートの記入に必要なすべての情報を収集している必要があります。

表9. ネットワーク認証サービスおよび EIM を反映させる - 前提条件ワークシート



前提条件ワークシート	応答
次のシステムの iSeries は、V5R3 (5722-SS1) 以降ですか? <ul style="list-style-type: none"> • iSeries MC1 • iSeries A • iSeries B • iSeries C 	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
iSeries D の iSeries は、V5R2 (5722-SS1) 以降ですか?	はい
iSeries 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) を適用済みですか? <ul style="list-style-type: none"> • SI08977 • SI08979 	はい
以下のオプションとライセンス製品が、すべての iSeries システムにインストール済みですか? <ul style="list-style-type: none"> • iSeries Host Servers (5722-SS1 オプション 12) • iSeries (5722-XE1) • Cryptographic Access Provider (5722-AC3) (V5R2 システム用または V5R3 システム用) 	はい
管理者の PC に i5/OS V5R3 以降の iSeries (5722-XE1) がインストール済みですか?	はい
管理者の PC に i5/OS V5R3 以降の iSeries ナビゲーターがインストール済みですか? <ul style="list-style-type: none"> • 管理者の PC に iSeries 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 iSeries 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  server iSeries Access for Windows サービス・パックはインストール済みですか? 最新のサービス・パックについては、iSeries Access  を参照してください。	はい
*SECADM、*ALLOBJ、および *IOSYSCFG 特殊権限を持っていますか?	はい
Kerberos サーバーの役目をする、以下のいずれかのシステムがありますか? 持っている場合は、そのシステムを指定してください。 <ol style="list-style-type: none"> 1. Microsoft Windows 2000 サーバー 注: Microsoft Windows 2000 サーバーは、デフォルトのセキュリティー・メカニズムとして Kerberos 認証を使用します。 2. Windows ^(R) サーバー 2003 3. i5/OS PASE (V5R3 以降) 4. AIX サーバー 5. zSeries 	はい、Windows 2000 サーバー
Windows 2000 サーバーと Windows ^(R) Server 2003 の場合、Windows Support Tools (ktpass ツールを提供) がインストールされていますか?	はい

表9. ネットワーク認証サービスおよび EIM を反映させる - 前提条件ワークシート (続き)

前提条件ワークシート	応答
iSeries 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? 5 分以内でない場合は、『システム時刻を同期する』を参照してください。	はい

表10. ネットワーク認証サービスおよび EIM を反映させる - 計画ワークシート

iSeries A から iSeries B および iSeries C にネットワーク認証サービスと EIM の構成を反映させるための計画ワークシート	応答
システム・グループの名前は何ですか?	MyCo システム・グループ
このシステム・グループには、どのシステムが含まれていますか?	iSeries B、iSeries C
どのシステムがモデル・システムですか?	iSeries A
このシステム・グループにどの機能を反映させる計画ですか?	ネットワーク認証サービスと EIM (エンタープライズ識別マッピング)
受動システムのキータブ・ファイルに追加するのは、どのタイプのキータブ項目ですか?	i5/OS Kerberos 認証
モデル・システムと受動システムの各サービス・プリンシパルに関連したパスワードは何ですか? 注: このシナリオで指定されたパスワードは、すべてサンプル目的専用です。ご使用のシステムまたはネットワーク・セキュリティを損なわないように、これらのパスワードはユーザー独自の構成の一部として使用しないでください。	iSeries A、B、および C のプリンシパルのパスワード: iseriesa123 iSeries D のプリンシパルのパスワード: iseriesd123
どのユーザーをドメイン・コントローラーへの接続に使用しますか?	ユーザー・タイプ: Distinguished name and password 識別名: cn=administrator パスワード: mycopwd

システム・グループを作成する

ネットワーク認証サービスと EIM の構成を受動システムに反映させる前に、すべてのエンドポイント・システム用に 1 つのシステム・グループを作成しておく必要があります。システム・グループとは、同様な設定と属性 (たとえば、ネットワーク認証サービスの構成) を適用できる、管理可能な複数のシステムの集合です。

1. iSeries ナビゲーター で、「**マネージメント・セントラル (iSeriesMC1)**」を展開します。
2. 「**システム・グループ**」を右マウス・ボタンでクリックし、「**新規システム・グループ...**」を選択して新しいシステム・グループを作成します。
3. 「**一般**」ページで、名前フィールドに **MyCo system group** と入力します。
4. このシステム・グループの説明を指定します。
5. 「**使用可能なシステム**」リストから、iSeries B と iSeries C を選択し、「**追加**」をクリックします。これで、システムが「**選択済みのシステム**」リストに追加されます。
6. 「**OK**」をクリックします。
7. 「**システム・グループ**」を展開して、システム・グループが追加されたことを確認します。

これでご使用のエンドポイント・システム用のシステム・グループを作成したので、ネットワーク認証サービスと EIM の構成をこれらのシステムに反映させられようになりました。

モデル・システム (iSeries A) から iSeries B と iSeries C にシステム設定を反映させる

ここには、簡略説明を入れます。最初の段落と要約に使用されます。

iSeries ナビゲーター の機能同期化ウィザードを使用すると、同じシステム・グループ内の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られます。ネットワーク認証サービスと EIM の構成を受動システムに反映させるための手順は、次のとおりです。

1. iSeries ナビゲーター で、「**マネージメント・セントラル (iSeriesMC1)**」 → 「**システム・グループ**」と展開します。
2. 「**MyCo システム・グループ**」を右マウス・ボタンでクリックし、「**システム値**」 → 「**機能の同期化...**」の順に選択し、「**次へ**」をクリックします。**機能同期化ウィザード**が開きます。
3. 「**ウェルカム (Welcome)**」ページで、機能同期化ウィザードについての情報を検討します。「**ウェルカム (Welcome)**」ページは、このウィザードで後で同期することを選択できる機能をリストします。

注: サーバー間でネットワーク構成サービスと EIM の構成を反映させる際に、パスワードなどの機密情報がネットワークを経由して送信されます。ローカル・エリア・ネットワーク (LAN) 外に送信する場合は特に、SSL を使用してこの情報を保護する必要があります。詳しくは、『シナリオ: SSL を使用してマネージメント・セントラル・サーバーとのすべての接続を保護する』を参照してください。

4. 「**モデル・システム**」ページで、モデル・システムとして **iSeries A** を選択し、「**次へ**」をクリックします。このモデル・システムは、ネットワーク認証サービスと EIM の構成を他のシステムに同期化するベースとして使用されます。
5. 「**ターゲット・システムとグループ (Target Systems and Groups)**」ページで、**MyCo system group** を選択します。「**次へ**」をクリックします。
6. 「**更新する対象 (What to Update)**」ページで、「**ネットワーク認証サービス (Kerberos) (Network Authentication Service (Kerberos))**」および「**エンタープライズ識別マッピング**」を選択します。「**構成の検査 (Verify configuration)**」をクリックします。構成を確認した後、「**次へ**」をクリックします。

注: EIM の検証が正常に完了しなかった場合、モデル・システム上の EIM 構成に問題がある可能性があります。ネットワーク認証サービスの構成が失敗する場合、モデル・システム上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。

これらのエラーから回復するには、モデル・システム上の EIM とネットワーク認証サービスの構成を調べ、修正してから、このシナリオの先頭に戻る必要があります。10 ページの『シナリオ: シングル・サインオンテスト環境を作成する』を参照して、モデル・システム上のすべてのシングル・サインオン構成タスクが完了し、検証されていることを確認してください。

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**」フィールドと「**パスワードの確認**」フィールドに **iseriesa123** と入力してから、「**次へ**」をクリックします。

注: このパスワードは、各受動システム上のキータブ項目に使用されます。ご使用のセキュリティー・ポリシーで各システムに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。代わりに、このウィザードの完了後、個々のシステムにキータブ項目を手作業で追加し、システムごとに別々のパスワードを入力することができます。

8. 「エンタープライズ識別マッピング」 ページで、EIM 操作の実行時にオペレーティング・システムが使用するユーザーを選択します。
 - ユーザー・タイプ: Distinguished name and password
 - 識別名: cn=administrator
 - パスワード: mycopwd
9. 「サマリー」 ページで、このページに適切な設定値がリストされていることを確認します。「終了」をクリックします。
10. iSeries ナビゲーター で、「マネージメント・セントラル (iSeriesMC1)」 → 「タスク・アクティビティ」 → 「システム値」 と展開します。
11. タスクが正常に完了したことを確認します。

iSeries B および iSeries C でネットワーク認証サービスと EIM の構成を完了する

機能同期化ウィザードがシングル・サインオン環境に必要な大部分の構成を反映させますが、iSeries ナビゲーター B および iSeries ナビゲーター C でシングル・サインオン構成を完了するには、追加のタスクを実行する必要があります。

シングル・サインオン環境の設計内容に応じて、iSeries B と iSeries C で実行する必要があるタスクは次のとおりです。

1. i5/OS サービス・プリンシパルを Kerberos サーバーに追加する。
2. 各ユーザーのホーム・ディレクトリーを作成する
3. ネットワーク認証サービスをテストする
4. ユーザーごとの EIM ID を作成する
5. EIM ID に対してソース・アソシエーションとターゲット・アソシエーションを作成する
6. (オプション) ポリシー・アソシエーションを作成する
7. (オプション) レジストリーが探索操作に加わり、ポリシー・アソシエーションを使用できるようにする
8. EIM マッピングをテストする
9. (オプション) Kerberos を使用するように iSeries Access for Windows アプリケーションを構成する
10. ネットワーク認証サービスと EIM の構成を検証する

iSeries B と iSeries C で構成を行うガイドとして、『i5/OS のシングル・サインオンを使用できるようにする』シナリオを使用してください。このシナリオは、シングル・サインオンに必要なすべてのタスクを実行するための手順を段階ごとに説明します。

これで、iSeries A から iSeries B および iSeries C に EIM とネットワーク認証サービスの構成を反映させるために必要なタスクを完了しました。

V5R2 以降のシステムである iSeries D でネットワーク認証サービスと EIM を構成する

iSeries D は、OS/400 V5R2 を実行しています。このリリースは機能同期化ウィザードをサポートしません。したがって、iSeries A の構成を iSeries D に反映させられません。その代わりに、EIM 構成ウィザードとネットワーク認証サービス・ウィザードを使用して、このシステムを手作業で構成する必要があります。また、iSeries D がシングル・サインオン環境に加わるために必要な追加のステップを実行する必要があります。

iSeries A でのシングル・サインオンの構成内容に応じて、実行する必要があるタスクは次のとおりです。

1. EIM 構成ウィザードとネットワーク認証サービス・ウィザードを使用して、EIM ドメインに加わるように iSeries D を構成し、ネットワーク認証サービス用に iSeries D を構成する
2. i5/OS サービス・プリンシパルを Kerberos サーバーに追加する。
3. 各ユーザーのホーム・ディレクトリーを作成する
4. ネットワーク認証サービスをテストする
5. ユーザーごとの EIM ID を作成する
6. EIM ID に対してソース・アソシエーションとターゲット・アソシエーションを作成する
7. (オプション) ポリシー・アソシエーションを作成する
8. (オプション) レジストリーが探索操作に加わり、ポリシー・アソシエーションを使用できるようにする
9. EIM マッピングをテストする
10. (オプション) Kerberos を使用するように iSeries Access for Windows アプリケーションを構成する
11. ネットワーク認証サービスと EIM の構成を検証する

iSeries A 上のシングル・サインオン構成と一致するように iSeries D を構成するガイドとして、『i5/OS のシングル・サインオンを使用できるようにする』シナリオを使用できます。このシナリオは、シングル・サインオンに必要なすべてのタスクを実行するための手順を段階ごとに説明します。『i5/OS のシングル・サインオンを使用できるようにする』シナリオでは、iSeries B として識別されるシステムの手順に従う必要があります。これは、このシステムが既存の EIM ドメインに加わる方法が、iSeries D がこのシナリオで既存の EIM ドメインに加わるのに必要な手順と同じであるからです。

これで、ネットワーク認証サービスと EIM の構成を複数のシステムに伝搬させました。シングル・サインオン環境を利用するようにマネージメント・セントラル・サーバーを構成するには、追加のタスクを実行する必要があります。詳しくは、『シナリオ: シングル・サインオン環境用にマネージメント・セントラル・サーバーを構成する』を参照してください。

シナリオ: シングル・サインオン用にマネージメント・セントラル・サーバーを構成する

このシナリオでは、マネージメント・セントラル・サーバーを構成してシングル・サインオン環境に参加する方法について説明します。管理者は、シングル・サインオン構成を複数システム全体に反映させるこのシナリオを完了すれば、そのマネージメント・セントラル・サーバーがシングル・サインオン環境に参加できるよう必要な構成を行うことができます。

状況

中規模部品メーカーのシステム管理者であるとしします。この 3 年間、セントラル・サーバーと 3 台のエンドポイント・サーバーの管理に、iSeries ナビゲーター マネージメント・セントラル・サーバーを使用してきました。職責には、PTF の適用、ネットワーク上の新規ユーザーの作成などの管理業務があります。常に、セントラル・サーバーから複数のシステムに PTF を送信し、インストールできるようにしてきました。これで時間が節約できます。このたび、自社のシステムが V5R4 にアップグレードされ、セキュリティー管理者が新しいセキュリティー・ポリシーを設定しました。このポリシーでは、ネットワーク内の各システムでユーザー・パスワードが異ならなければなりません。以前、マネージメント・セントラル・サーバーは、ネットワーク全体でユーザー・プロファイルとパスワードが同一であることを要求しました。i5/OS V5R4 では、マネージメント・セントラル・サーバーのシングル・サインオンを可能にすると、マネ

ージメント・セントラル・サーバーの機能を使用するために、各エンドポイント・システムでユーザー・プロファイルとパスワードが一致する必要がなくなりました。これにより、i5/OS システム上でパスワードを管理する必要性が限定されます。

現在、『シナリオ: i5/OS のシングル・サインオンを使用できるようにする』を新規システムのいずれかに対して完了し、『ネットワーク認証サービスと EIM を複数システムに反映させる』を完了しました。次に、すべてのマネージメント・セントラル・サーバーがこのシングル・サインオン環境に加わるように構成しようとしています。

このシナリオには、以下の利点があります。

- セントラル・システムとエンドポイント・システム上で、ユーザー・プロファイルの管理作業を削減する
- セントラル・システムとエンドポイント・システム上で、ユーザーに対するパスワード管理作業を削減する
- 新しい企業セキュリティー・ポリシーに従い、各システムでユーザー・パスワードが固有であることを要求する

目的

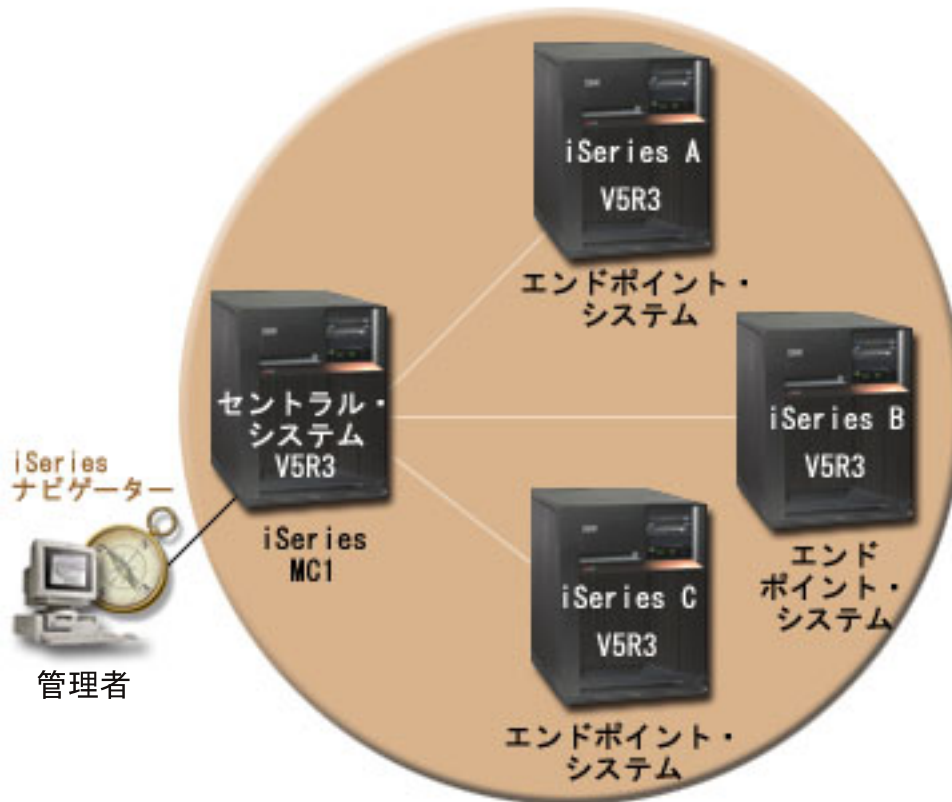
会社の 3 人のシステム管理者の 1 人であるとします。自分と、他の 2 人の管理者 (アマンダとジョージ) は、管理費用を削減し、中央管理アプリケーションとネットワーク資産へのアクセスを単純化する、小規模なシングル・サインオン環境を作成しようとしています。

このシナリオの目的は次のとおりです。

- i5/OS V5R4 マネージメント・セントラル・サーバーのシングル・サインオンを可能にして、社内の新しいセキュリティー・ポリシーに従う。
- マネージメント・セントラル・サーバーが管理するすべてのエンドポイント・システムで、同じユーザー・プロファイルとパスワードを使用する必要をなくして、パスワード管理を単純化する。
- マネージメント・セントラル・サーバーが管理するすべてのエンドポイント・システムが、シングル・サインオン環境に加わることを可能にする。
- ポリシー・アソシエーションを使用するのではなく、ユーザーを EIM ID にマップすることによって、社内の資産セキュリティーを確保する。

詳細

以下の図で、このシナリオのネットワーク環境を説明します。



この図で、このシナリオに関連する以下の諸点を説明します。

- セントラル・システム iSeriesMC1 (モデル・システムとしても指定)

- 次のオプションおよびライセンス製品をインストールした i5/OS バージョン 5 リリース 4 (V5R4) を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12)
 - i5/OS Access for Windows (5722-XE1)
- エンドポイント・システムごとに設定同期化タスクを保管し、スケジュールし、実行します。
- ネットワーク認証サービスと EIM 用に構成されます。
- ネットワーク認証サービスと EIM の構成を受動システムに反映させる元のモデル・システムとして選択されます。

注: モデル・システムは、『シナリオ:シングル・サインオンのテスト環境を作成する』で iSeries A として識別されるシステムと同様に構成する必要があります。このシナリオを参照して、モデル・システム上のすべてのシングル・サインオン構成タスクが完了し、検証されていることを確認してください。

- エンドポイント・システム iSeries A、iSeries B、および iSeries C

- 次のオプションおよびライセンス製品をインストールした i5/OS バージョン 5 リリース 4 (V5R4) を実行します。
 - i5/OS Host Servers (5722-SS1 オプション 12)

- iSeries Access for Windows (5722-XE1)
- ネットワーク認証サービスと EIM 用に構成されます。
- 管理者の PC
 - iSeries Access for Windows (5722-XE1) を実行します。
 - 次のサブコンポーネントを備えた iSeries 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

注: ネットワーク認証サービスの管理に使用される PC のみに必要です。

前提条件および前提事項

このシナリオを正常にインプリメントするには、次の前提条件および前提事項が満たされる必要があります。

• セントラル・システム iSeriesMC1 (モデル・システムとしても指定)

注: このシナリオでは、セントラル・システムがシングル・サインオン用に適切に構成されていることを前提とします。『シナリオ: シングル・サインオンのテスト環境を作成する』を参照して、セントラル・システム上のすべてのシングル・サインオン構成タスクが完了し、検証されていることを確認してください。

- 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など、すべてのシステム要件が検査されている。これらのライセンス・プログラムがインストールされていることを検査するには、以下のことを行ってください。
 - iSeries ナビゲーター で、「iSeries server」 → 「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」と展開する。
 - 必要なライセンス・プログラムがすべてインストールされていることを確認する。
- 必要なハードウェア計画およびセットアップがすべて完了している。
- 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。
- これらのサーバー間のデータ送信を保護するために、Secure Sockets Layer (SSL) が構成されている。

注: サーバー間でネットワーク構成サービスの構成を反映させる際に、パスワードなどの機密情報がネットワークを経由して送信されます。ローカル・エリア・ネットワーク (LAN) 外に送信する場合は特に、SSL を使用してこの情報を保護する必要があります。詳しくは、『シナリオ: SSL を使用してマネージメント・セントラル・サーバーとのすべての接続を保護する』を参照してください。

• エンドポイント・システム iSeries A、iSeries B、および iSeries C

- 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など、すべてのシステム要件が検査されている。これらのライセンス・プログラムがインストールされていることを検査するには、以下のことを行ってください。
 - iSeries ナビゲーター で、「iSeries server」 → 「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」と展開する。
 - 必要なライセンス・プログラムがすべてインストールされていることを確認する。
- 必要なハードウェア計画およびセットアップがすべて完了している。
- 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。
- これらのサーバー間のデータ送信を保護するために、Secure Sockets Layer (SSL) が構成されている。

注: サーバー間でネットワーク構成サービスの構成を反映させる際に、パスワードなどの機密情報がネットワークを経由して送信されます。ローカル・エリア・ネットワーク (LAN) 外に送信する場合は特に、SSL を使用してこの情報を保護する必要があります。詳しくは、『シナリオ: SSL を使用してマネージメント・セントラル・サーバーとのすべての接続を保護する』を参照してください。

- セントラル・システムとエンドポイント・システムでネットワーク認証サービスと EIM をすでに構成しています (『シナリオ: i5/OS のシングル・サインオンを使用できるようにする』と『シナリオ: ネットワーク認証サービスと EIM を複数システムに反映させる』を参照)。
- Kerberos サーバーとして Microsoft Windows Active Directory を使用しています。
- i5/OS サービス・プリンシパル名を Kerberos サーバーにすでに追加しています (このタスクは、『シナリオ: i5/OS のシングル・サインオンを使用できるようにする』で実行します)。
- ネットワーク認証サービスの構成をすでにテスト済みです (このタスクは、『シナリオ: ネットワーク認証サービスと EIM を複数システムに反映させる』で実行します)。

構成ステップ

マネージメント・セントラル・サーバーのユーザーに対してシングル・サインオンを使用可能にする手順は、次のとおりです。

ドメインが Domain Management に表示されていることを確認する

EIM ID を作成する前に、使用する EIM ドメインを「ドメイン管理」に追加したことを確認する必要があります。EIM ドメインを「ドメイン管理」にすでに追加してある場合は、EIM ドメインを「ドメイン管理」に追加するのに必要なこのステップをスキップし、新しい EIM ID の作成に必要な手順に進むことができます。

次の手順で EIM ドメインを「ドメイン管理」に追加します。

1. PC 上の iSeries ナビゲーター を使用して、**My Connections** の下にあるセントラル・システム **iSeriesMC1** を展開し、「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」の順に選択する。
2. 「ドメイン管理」を右マウス・ボタンでクリックし、「ドメインの追加」を選択する。
3. 「ドメインの追加」ページで、「ドメイン・コントローラー」フィールドに、追加したいドメイン用のドメイン・コントローラーの完全修飾名が入っていることを確認する。この例の場合、ドメイン・コントローラーの名前は `iSeriesMC1.myco.com` であり、追加したい EIM ドメインは `MyCoEimDomain` です。
4. 「OK」をクリックする。
5. 「ドメイン管理」の下で、`MyCoEimDomain` を展開する。「**EIM ドメイン・コントローラーへの接続 (Connect to EIM Domain Controller)**」ダイアログが表示されます。

注: ドメインを管理しようとする前に、EIM ドメイン・コントローラーに接続してください。

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、その EIM ドメイン・コントローラーの構成時に作成した識別名とパスワードを入力し、「OK」をクリックする。たとえば、『シナリオ: i5/OS のシングル・サインオンを使用できるようにする』を完了した場合、識別名 `cn=administrator` とパスワード `mycopwd` を入力します。

EIM ID を作成する

シングル・サインオン環境のセットアップの一環として、個人を表す EIM ID を作成する必要があります。このタスクは、マネージメント・セントラル・サーバーの機能にアクセスできるようにしたいすべてのユーザーに対して実行する必要があります。新しい EIM ID を作成する手順は、次のとおりです。

1. MyCoEimDomain の下で「ID」を右マウス・ボタンでクリックし、「新規 ID」を選択します。
2. 「新規 EIM ID」ページで、「ID」フィールドに新規 ID の名前を指定し、「OK」をクリックします。この例の場合、同僚のシステム管理者の一人である Amanda Jones 用の EIM ID を作成します。「ID」フィールドに指定する名前は Amanda Jones です。

EIM ID を必要とする個人ごとに、ステップ 1 から 3 を繰り返してください。

ID アソシエーションを作成する

各エンドポイント・システムとセントラル・システム (iSeriesMC1) で、各 EIM ID とユーザー・プロファイル間のソース・アソシエーションとターゲット・アソシエーションを作成する必要があります。セントラル・システムを通じてリソースにアクセスできるようにしたいユーザーごとに、このステップを実行する必要があります。ポリシー・アソシエーションを使用できますが、意図せず誤ってユーザーに資産権限を付与する危険を回避するために、ここではポリシー・アソシエーションの使用を選択しないものとします。このステップの完了後、各ユーザーには、エンドポイント・システム上の各ユーザー・プロファイルに関連した 1 つの EIM ID があります。これらのアソシエーションにより、ユーザーはシングル・サインオン環境に加わることができます。これらのアソシエーションを作成する手順は、次のとおりです。

1. 次の手順でソース・アソシエーションを作成します。
 - a. PC 上の iSeries ナビゲーター を使用して、セントラル・システム、iSeriesMC1 を選択し、「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」と展開する。
 - b. MyCoEimDomain を展開し、「ID」を選択する。右側のペインに ID のリストが表示されます。
 - c. Amanda Jones を右マウス・ボタンでクリックし、「プロパティ」を選択する。
 - d. 「アソシエーション」タブで、「追加」をクリックする。
 - e. 「アソシエーションの追加」ページで、「レジストリー」フィールドの横にある「参照...」をクリックし、Amanda Jones ID に関連付けたいユーザー・プロファイルを含むエンドポイント・システム・レジストリーのレジストリー定義を選択する。この例の場合、EIM ID Amanda Jones と、エンドポイント・システム iSeries A のユーザー・プロファイル AMJONES とのアソシエーションを作成します。
 - f. 「ユーザー」フィールドに、ユーザー・プロファイル AMJONES を入力する。
 - g. 「アソシエーション・タイプ」フィールドで、「ソース」を選択し、「OK」をクリックする。「アソシエーション」タブ上のアソシエーションのリストに、そのアソシエーションが追加されます。
2. 次の手順でターゲット・アソシエーションを作成します。
 - a. 「EIM ID」ページの「アソシエーション」タブで、「追加」をクリックする。
 - b. 「アソシエーションの追加」ページで、「参照...」をクリックし、iSeries A のレジストリー名を選択する。
 - c. 「ユーザー」フィールドに、ユーザー・プロファイル AMJONES を入力する。
 - d.

アソシエーションを作成したい各エンドポイント・システムと各 EIM ID に対して、上記のステップを繰り返してください。終了したら、「EIM ID プロパティ」ダイアログで「OK」をクリックします。

ネットワーク認証サービスを使用するようにマネージメント・セントラル・サーバーを構成する

ネットワーク認証サービス (Kerberos) を使用するようにセントラル・システムとすべてのエンドポイント・システムを構成するには、iSeries Information Center のネットワーク認証サービス・トピックにある『シナリオ: エンドポイント・システム間で Kerberos 認証を使用する』を実行してください。このシナリオを完了した後、このシナリオの次のステップに進んで、EIM を使用するようにセントラル・システムとすべてのエンドポイント・システムを構成する必要があります。

EIM を使用するようにマネージメント・セントラル・サーバーを構成する

EIM を使用するようにセントラル・システムとすべてのエンドポイント・システムを構成する手順は、次のとおりです。

1. 次の手順で、EIM を使用するようにセントラル・システムを設定します。
 - a. PC 上の iSeries ナビゲーター を使用して、セントラル・システム **iSeriesMC1** を右マウス・ボタンでクリックし、「プロパティ」を選択する。
 - b. 「セキュリティ」タブをクリックし、「**Kerberos 認証の使用 (Use Kerberos authentication)**」が選択されていることを確認する。
 - c. ID マッピングに対して「**ID があれば使用する (なければプロファイルを使用) (Use if identity exists (otherwise use profile))**」オプションを選択する。

注: 「**ID マッピングが必要 (Require identity mapping)**」オプションを選択できます。しかし、これを選択する場合、EIM アソシエーションを作成していない EIM ID について、マネージメント・セントラル・サーバーを使用するエンドポイント・システムに対する iSeries ナビゲーター タスクが失敗します。

- d. 「**OK**」をクリックし、**iSeriesMC1** でこの値を設定する。ネットワーク認証サービスと EIM を使用するようにマネージメント・セントラル・サーバーを構成するための前提条件に注意を促す、メッセージが表示されます。
 - e. 「**OK**」をクリックして、前提条件を理解していることを確認します。
2. 次の手順でシステム・グループを作成します。
 - a. iSeries ナビゲーター で、**iSeriesMC1** を展開する。
 - b. 「システム・グループ」を右マウス・ボタンでクリックし、「**新規システム・グループ**」を選択する。
 - c. 「一般」ページで、「名前」フィールドにシステム・グループを指定する。このシステム・グループの説明を作成してください。この例の場合、**group1** という名前でシステム・グループを指定し、**iSeriesMC1** が管理するエンドポイント・システムのグループという説明を指定します。
 - d. 「使用可能なシステム」リストから、セントラル・システム **iSeriesMC1**、およびすべてのエンドポイント・システム **iSeries A**、**iSeries B**、および **iSeries C** を選択し、「追加」をクリックする。これで、これらのシステムが「**選択済みのシステム**」リストに追加されます。
 - e. 「**OK**」をクリックする。
 - f. 「システム・グループ」を展開して、システム・グループ **group1** が追加されたことを確認する。
 3. 次の手順でシステム・グループのインベントリーを収集します。
 - a. iSeries ナビゲーター で、**iSeriesMC1** を展開し、「システム・グループ」を選択する。
 - b. **group1** を右クリックし、「インベントリー」 → 「収集」の順に選択する。

- c. **group1** の「インベントリーの収集」ページで、「システム値」を選択し、「OK」をクリックする。

注: デフォルトで、**Collect Inventory** タスクが開始したことを知らせるダイアログが表示されます。ただし、デフォルトの設定を変更した場合、このダイアログは表示されません。
 - d. 「OK」をクリックする。
 - e. 「インベントリーの収集状況」ページで、表示される状況値をすべて読みとり、検出される問題を修正する。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。
 - f. 「タスク状況」ヘルプ・ページで、「インベントリー」を選択する。このページには、検出されるすべての状況値が、詳細な説明とリカバリー情報と一緒に表示されます。
 - g. インベントリー収集が正常に完了した後、状況ウィンドウを閉じる。
4. 次の手順で EIM 設定を比較し、更新します。
 - a. iSeries ナビゲーターで、セントラル・システム **iSeriesMC1** を展開し、「システム・グループ」を選択する。
 - b. システム・グループ「**group1**」を右クリックし、「システム値」→「比較と更新」の順に選択する。
 - c. 「比較と更新」システム・グループ・ダイアログのフィールドに入力する。
 - 1) 「モデル・システム」フィールドに、セントラル・システム **iSeriesMC1** を選択する。
 - 2) 「カテゴリ」フィールドに、「マネージメント・セントラル」を選択する。
 - 3) 比較対象の項目のリストから、「ユーザー・マッピングに EIM を使用する (Use EIM for user mapping)」と「ID マッピングが必要 (Require identity mapping)」を選択する。
 - d. 受動システムがご使用のシステム・グループであることを確認し、「OK」をクリックして更新を開始する。これにより、システム・グループ内の各受動システムが、モデル・システムで選択した EIM 設定値で更新されます。

注: デフォルトで、**Compare and Update** タスクが開始したことを知らせるダイアログが表示されます。ただし、デフォルトの設定を変更した場合、このダイアログは表示されません。
 - e. 「OK」をクリックする。
 - f. 「値の更新の状況 (Update Values Status)」ダイアログで、各システムで更新が完了したことを確認し、このダイアログを閉じる。
 5. 次の手順で、セントラル・システムとすべてのエンドポイント・システム上のマネージメント・セントラル・サーバーを再始動します。
 - a. iSeries ナビゲーター で、**My Connections** を展開する。
 - b. 再始動したい iSeries ナビゲーター システムを展開する。
 - c. 「ネットワーク」→「サーバー」と展開し、「TCP/IP」を選択する。
 - d. 「マネージメント・セントラル」を右マウス・ボタンでクリックし、「停止」を選択する。サーバー・ビューが縮小され、サーバーとの接続が切断されたことを説明するメッセージが表示されます。
 - e. マネージメント・セントラル・サーバーの停止後、「始動」をクリックして再始動する。
 6. 各エンドポイント・システム (iSeries ナビゲーター A、iSeries ナビゲーター B、および iSeries ナビゲーター C) で上記のステップを繰り返します。

シナリオ: ISV アプリケーション用のシングル・サインオンを使用可能にする

この情報は、代表的なシングル・サインオンのインプリメンテーション状況を説明するシナリオを検討するときに使用し、ご使用のサーバー・セキュリティー・ポリシーの一部としてユーザー独自の証明書のインプリメンテーションを計画する際に参照してください。

状況

独立ソフトウェア販売会社 (ISV) の主任アプリケーション開発者であり、自社が開発し、iSeries ナビゲーター ユーザーに提供するアプリケーションを監督する立場にあるとします。iSeries ナビゲーターにより、ユーザーはシングル・サインオン環境を作成し、この環境に加わることができます。これらのシングル・サインオン機能を有効利用するためのアプリケーションがあれば、製品の販売に役立つので、こうしたアプリケーションを必要としています。そこで、ネットワーク認証サービスと EIM (エンタープライズ識別マッピング) を使用してシングル・サインオン環境を作成する iSeries ナビゲーター ユーザーに、**Calendar** という名前のアプリケーションを販売することを決定しました。**Calendar** アプリケーションを使用すると、ユーザーは平日のスケジュールを表示し、管理できるようになります。シングル・サインオン用に **Calendar** アプリケーションを使用できるようにするには、シングル・サインオン環境に加わることを可能にするサーバー固有のコードをアプリケーションに組み込む必要があります。以前、EIM API を呼び出すアプリケーションを作成した経験がありますが、ネットワーク認証サービス API も呼び出すアプリケーションを扱うのは初めてです。

注: また、異なる認証方式を使用するアプリケーションをシングル・サインオン環境用に開発することも可能です。たとえば、ネットワーク認証サービスで認証するのに必要なコードを挿入するのではなく、デジタル証明書で認証するか、ディレクトリー・サーバーをバインドするのに必要なコードを挿入することができます。

目的

シングル・サインオン環境に加わることが可能なアプリケーションに関心がある iSeries ナビゲーター ユーザーに、**Calendar** アプリケーションを販売しようとしています。**Calendar** アプリケーションのサーバー・サイドが、シングル・サインオン環境に参加できるようにします。このシナリオを実行する際の目標は次のとおりです。

- 既存の **Calendar** アプリケーションのサーバー固有の部分を変更するか、EIM とネットワーク認証サービスを使用するシングル・サインオン環境に加わる新しい **Calendar** アプリケーションを開発する。
- アプリケーションをテストできるシングル・サインオン環境を作成する。
- **Calendar** アプリケーションをテストし、シングル・サインオン環境に正常に加わることを保証する。

前提条件および前提事項

このシナリオが実現するかどうかは、次の前提事項と前提条件によって決まります。

- Kerberos と EIM を使用するように構成されるシングル・サインオン環境に加わるための **Calendar** アプリケーションが必要である。
- すでに、iSeries ナビゲーター システム用のアプリケーションを作成した実績がある。iSeries ナビゲーター システムのプログラミングについては、iSeries ナビゲーター のプログラミング・トピックを参照してください。
- 次のオプションおよびライセンス製品をインストールしたバージョン 5 リリース 4 (V5R4) iSeries ナビゲーター システムがある。
 - iSeries ナビゲーター Host Servers (5722-SS1 オプション 12)

- iSeries ナビゲーター (5722-XE1)
- Kerberos レルムに加わるように iSeries ナビゲーター システムを構成した。
- 次の言語のいずれかでアプリケーションを作成する。
 - C などの ILE プログラム言語を使用してアプリケーションを作成し、GSS API セットについて十分理解している (『Generic Security Service API』を参照)。
 - Java を使用してアプリケーションを作成し、JGSS API セットについて十分理解している (『IBM Java Generic Security Service (JGSS)』を参照)。

注: また、使用する JGSS API のセットに応じて、Java ツールボックスが必要な場合もあります。


- アプリケーションのクライアント固有の部分をすでに完了し、アプリケーションが Kerberos 認証を使用できるようにしている。

構成ステップ

計画前提条件ワークシートに記入する

次の計画ワークシートに記入して、アプリケーションをテストできる正常なシングル・サインオン環境の前提条件を満たしていることを確認してください。

前提条件ワークシート	応答
iSeries ナビゲーターは V5R4 (5722-SS1) ですか?	はい
iSeries Access for Windows (5722-XE1) が、管理を行う PC 上にインストールされていますか?	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、管理を行う PC 上にインストールされていますか?	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、管理を行う PC 上にインストールされていますか?	はい
*SECADM、*ALLOBJ、および *IOSYSCFG 特殊権限を持っていますか?	はい
Kerberos サーバーの役目をする、以下のいずれかのサーバーがありますか? ある場合は、そのサーバーを指定してください。 1. iSeries ナビゲーター サーバー 注: Microsoft iSeries ナビゲーター サーバーは、デフォルトのセキュリティー・メカニズムとして Kerberos 認証を使用します。 2. Windows Server 2003 3. iSeries ナビゲーター PASE (V5R3 以降) 4. AIX サーバー 5. zSeriesサーバー	はい
Windows 2000 サーバーの場合、Windows Support Tools (ktpass ツールを提供) がインストールされていますか?	はい
ネットワークのシングル・サインオン環境に加わるようにしたいすべての PC が、iSeries ナビゲーター ドメイン内で構成されていますか?	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

前提条件ワークシート	応答
最新の iSeries ナビゲーター サービス・バックをインストール済みですか? 最新のサービス・バックについては、iSeries Access Web ページ  を参照してください。	はい
iSeries ナビゲーター 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? 5 分以内でない場合は、『システム時刻を同期する』を参照してください。	はい

新規アプリケーションを作成するか、既存のアプリケーションを変更する

Calendar アプリケーションがシングル・サインオン環境に加わることを可能にするサーバー固有のコードを組み込む用意ができました。以前の EIM API のプログラミング経験を使用して、次のようなプログラム・フローを作成します。

- アプリケーションの初期化
 - EIM Get Handle
 - EIM Connect
- ループ処理
 - ユーザー要求を待機する
 - Kerberos を使用してユーザーを認証する
 - EIM を呼び出して、ネットワーク認証サービス・ユーザーから、ローカル・ユーザーにマップする
 - ローカル・ユーザーにスワップする
 - タスクを実行する
 - オリジナルのユーザーに戻る
 - 「ユーザー要求を待機する」に進む

注: このシナリオでは、i5/OS シングル・サインオン環境用にアプリケーションを使用可能にするためのクライアント固有のコードをすでに作成したか、変更したことを前提としています。したがって、プログラムのサーバー固有の部分を完成するのに必要な手順だけを説明します。

- アプリケーションの終了
 - EIM ハンドルの破棄

プログラムのサーバー固有の部分の完成に使用できる疑似コードとコードの断片のサンプルについては、『ISV コード例』を参照してください。必要なクライアントとサーバー固有のコードを **Calendar** アプリケーションに追加したら、テスト用のシングル・サインオン・テスト環境を作成できます。

シングル・サインオンのテスト環境を作成する

『シナリオ: シングル・サインオンのテスト環境を作成する』を完了します。このシナリオでは、ネットワーク認証サービスおよび EIM を構成して、基本的なシングル・サインオンのテスト環境を作成する方法を実証します。このシナリオでは、単純なシングル・サインオン環境を構成し、使用するための次の手順を説明します。

1. 必要な計画ワークシートに記入する
2. iSeries システムの基本的なシングル・サインオン構成を作成する
3. iSeries サービス・プリンシパルを Kerberos サーバーに追加する

4. テスト・ユーザー (John Day) のホーム・ディレクトリーを iSeries システム上に作成する
5. iSeries システム上のネットワーク認証サービス構成をテストする
6. John Day の EIM ID を作成する
7. 新しい EIM ID 用のソース・アソシエーションとターゲット・アソシエーションを作成する
8. EIM ID マッピングをテストする
9. Kerberos を使用するように iSeries Access for Windows アプリケーションを構成する
10. ネットワーク認証サービスと EIM の構成を検証する

このシナリオで説明するシングル・サインオン・テスト環境を作成した後、**Calendar** アプリケーションをテストして、正常に機能することを確認できます。

アプリケーションをテストする

Calendar アプリケーションに対するクライアントとサーバーに固有の更新を両方とも開発し、このアプリケーションの i5/OS シングル・サインオン環境を使用できるようになりました。これで、アプリケーションをテストする準備ができました。

シングル・サインオン環境に正常に加わるアプリケーションを作成したことを確認する手順は、次のとおりです。

1. テスト・ユーザー jday (『シナリオ: シングル・サインオンのテスト環境を作成する』で作成) を PC にサインインすることによって、このユーザーを Windows 2000 ドメインのログに記録する。
2. テスト・ユーザーに、PC 上で **Calendar** アプリケーションを開かせる。予定表が開く場合、EIM ID John Day に対してアソシエーションが定義されているので、このアプリケーションは EIM を使用して、jday Kerberos プリンシパルを JOHND i5/OS ユーザー・プロファイルにマップしました。これで、iSeries 用の **Calendar** アプリケーション・セッションは、JOHND として接続されました。i5/OS シングル・サインオン環境用に ISV アプリケーションが正常に使用可能になりました。

ISV コード例

IBM は、お客様に、すべてのプログラム・コードのサンプルを使用することができる非独占的な著作権使用権を許諾します。お客様は、このサンプル・コードから、お客様独自の特別のニーズに合わせた類似のプログラムを作成することができます。

すべてのサンプル・コードは、例として示す目的でのみ、IBM により提供されます。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。

ここに含まれるすべてのプログラムは、現存するままの状態を提供され、いかなる保証も適用されません。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の保証の適用も一切ありません。

注: コーディング例を使用することにより、お客様は、113 ページの『コードに関するライセンス情報および特記事項』の条件に同意することになります。

```

/**** 仕様開始 *****/
/*                               */
/* モジュール名: Kerberos/EIM サーバー・サンプル */
/*                               */
/* 説明:      下記のコードは、Kerberos プリンシパルから */
/*           OS/400 ユーザー・プロファイルにマップするために、 */
/*           EIM API の呼び出しと一緒に Kerberos サーバーを */
/*           作成するためのサンプル・コードです。 */

```

```

/*          */
/*          注: エラー検査が除去されました。          */
/*          */
/*****/

/* #include ファイルがここで除去されます          */

//-----
// EIM の前提事項:
// このプログラムが実行されている OS400 で、EIM 構成情報が
// 設定されました。このプログラムが使用する情報は、
// 次のとおりです。
// - ldapURL
// - ローカル・レジストリー
// EIM ldap 探索接続
// - このプログラムでマッピング検索を行うのに必要な ldap 接続
// 情報は、妥当性検査リストまたはその他のユーザー保護スペース
// に保管できます。
// ここでは、仮の値のハードコーディングのみを行います。
// - この接続は、探索操作のみに使用されるので、
// ldap ユーザーは EIM マッピング探索権限だけが必要です。
// すべての EIM データ (ID、アソシエーションなど) が追加されました。
//-----

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

//-----
//
// 関数 : l_eimError
// 目的 : EIM エラーが発生しました。この関数は、
// EIM エラー・メッセージをプリントアウトします。
//
//-----
void l_eimError(char * function, EimRC * err)
{
    char * msg = NULL;
    printf("EIM ERROR for function = %s.%n", function);
    msg = eimErr2String(err);
    printf(" %s.%n",msg);
    free(msg);
}

//-----
//
// 関数 : l_eimConnect
// 目的 : EIM ハンドルを取得し、LDAP サーバーに接続します。
//
//-----
int l_eimConnect(EimHandle * handle)
{
    int rc = 0;
    char eimerr[150];
    EimRC *err = (EimRC *)&eimerr
    EimConnectInfo con;

    /* これは少なくとも 48 である必要があります。*/
    err->memoryProvidedByCaller = 150;

    //-----
    // ハンドルを作成します。URL に NULL を渡して、システムに対して
    // 構成された情報を使用することを示します。

```

```

//-----
eimCreateHandle(handle,
                NULL,
                err);

//-----
// 接続
//-----
// LDAP ユーザー ID とパスワードは、妥当性検査リストまたは
// その他のユーザー保護スペースに保管できます。
// ここでは、仮の値のハードコーディングのみを行います。
// また、LDAP との接続時に Kerberos 認証を使用することも選択できます。
// まず、Kerberos 認証を受け入れるように LDAP サーバーがセットアップ
// されていることを確認する必要があります。
//-----
// この接続は、探索操作のみに使用されるので、
// LDAP ユーザーは EIM マッピング探索権限だけが必要です。
//-----
con.type = EIM_SIMPLE;
con.creds.simpleCreds.protect = EIM_PROTECT_NO;
con.creds.simpleCreds.bindDn = LDAP_BINDDN;
con.creds.simpleCreds.bindPw = LDAP_BINDPW;
con.ssl = NULL;
eimConnect(handle,
           con,
           err);
return 0;
}

//-----
//-----
//
// 関数   : getOS400User
// 目的   : Kerberos ユーザーに関連した OS400 ユーザーを取得し、
//         そのユーザーにスワップします。
//
//-----
int getOS400User(EimHandle * handle,
                 char * OS400User,
                 gss_buffer_desc * client_name)
{
    char * principal;
    char * realm;
    char * atsign;

    //-----
    //
    // Kerberos client_name からプリンシパルとレルムを取得します。
    //
    //-----
    // client_name.value には、principal@realm の文字列が入ります。
    // 各部分へのポインターを取得します。
    //-----
    principal = client_name->value;
    atsign = strchr(principal, '@');
    *atsign = 0x00; // NULL terminate the principal
    realm = atsign + 1; // Advance pointer to the realm

    //-----
    //
    // EIM を呼び出して、Kerberos ソース・ユーザーに関連したターゲット・
    // ユーザーを取得します。このサンプル・アプリケーションは、
    // Kerberos レルム名が、このレルムを定義する EIM レジストリーの
    // 名前でもあることを前提とします。
    //
}

```

```

//-----
listPtr = (EimList *)listBuff;
for (i = 0; i < 2; i++)
{
    if (0 != (rc =
        eimGetTargetFromSource(handle,
                                realm,
                                principal,
                                NULL,          // use configured
                                                // local
                                                // registry.
                                NULL,
                                listSize,
                                listPtr,
                                err)))
    {
        ]_eimError("eimGetTargetFromSource", err);
        return -1;
    }

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

// マッピングが 0 の場合、検出される項目数を調べます。
// それ以外の場合は、バッファとクリーンアップ・ストレージ
// からユーザー・プロファイルを抽出します。
return 0;
}

/*****
/* 関数名:      get_kerberos_credentials_for_server      */
/*            */
/* 記述名      : 基本的に、この関数は、このサーバーのキータブ項目を */
/*            検出します。これを使用して、受信されるトークンを */
/*            検証します。 */
/*            */
/* 入力:      char * service_name - サービス名 */
/*            gss_buffer_t msg_buf - 入力メッセージ */
/* 出力:      gss_cred_id_t *server_creds - 出力信任状 */
/*            */
/* 正常終了  : 戻り値 == 0 */
/* エラー終了:  -1、エラーが検出されました。 */
/*****
int get_kerberos_credentials_for_server (
char *      service_name, /* サービス・プリンシパルの名前 */
gss_cred_id_t * server_creds) /* 獲得される信任状 */
{
    gss_buffer_desc name_buf; /* インポート名のバッファ */
    gss_name_t server_name; /* gss サービス名 */
    OM_uint32 maj_stat, /* GSS 状況コード */
              min_stat; /* メカニズム Kerberos 状況 */

    /* サービス名を GSS 内部形式に変換します */
    name_buf.value = service_name;
    name_buf.length = strlen((char *)name_buf.value) + 1;
    maj_stat = gss_import_name(
        &min_stat, /* Kerberos 状況 */
        &name_buf, /* 変換する名前 */

```

```

        (gss_OID) gss_nt_service_name, /* 名前のタイプ */
        &server_name); /* GSS 内部名 */

/* キータブからサービスの信任状を獲得します */
maj_stat = gss_acquire_cred(
    &min_stat, /* Kerberos 状況 */
    server_name, /* gss 内部名 */
    GSS_C_INDEFINITE, /* 信任状の最大寿命 */
    GSS_C_NULL_OID_SET, /* デフォルト・メカニズムを使用 */
    GSS_C_ACCEPT, /* 信任状の使用 */
    server_creds, /* 出力 cred ハンドル */
    NULL, /* 実際のメカニズムを無視 */
    NULL); /* 残りの時間を無視 */

/* gss 内部形式名をリリースします */
gss_release_name(&min_stat, &server_name);

return 0;
}

/*****
/* 関数名 : do_kerberos_authentication()
/* 目的 : 有効なクライアント要求をすべて受け入れます。コンテキスト*
/* が確立されると、そのハンドルがコンテキストで戻され、
/* クライアント名が戻されます。
/*
/* 正常終了 : 戻り値 == 0
/* エラー終了: -1、エラーが検出されました。
*****/
int do_kerberos_authentication (
    int s, /* ソケット接続 */
    gss_cred_id_t server_creds, /* サーバーの信任状 */
    gss_ctx_id_t * context, /* GSS コンテキスト */
    gss_buffer_t client_name) /* Kerberos プリンシパル */
{
    gss_buffer_desc send_tok, /* クライアントに送信するトークン */
    rcv_tok; /* クライアントから受信されるトークン */
    gss_name_t client; /* クライアント・プリンシパル */
    OM_uint32 maj_stat, /* GSS 状況コード */
    min_stat; /* メカニズム (kerberos) 状況 */
    msgDesc_t msgSend, /* 送信するメッセージ・バッファ */
    msgRecv; /* 受信されるメッセージ・バッファ */
    gss_OID doid;

    *context = GSS_C_NO_CONTEXT; /* コンテキストを初期化 */

    do {
        /* クライアントからメッセージを受信します */
        memset(&msgRecv, 0x00, sizeof(msgRecv));
        if (0 != rcvAmessage(s, &msgRecv))
            return -1;
        rcv_tok.length = msgRecv.dataLength;
        rcv_tok.value = msgRecv.buffer;

        /* セキュリティー・コンテキストを受け入れます */
        maj_stat = gss_accept_sec_context(
            &min_stat, /* Kerberos 状況 */
            context, /* コンテキスト・ハンドル */
            server_creds, /* 獲得されるサーバー信任状 */
            &rcv_tok, /* 受信されるトークン */
            GSS_C_NO_CHANNEL_BINDINGS, /* CB なし */
            &cClient, /* クライアント・リクエスター */
            NULL, /* メカニズムのタイプを無視 */
            &send_tok, /* 送信されるトークン */
            NULL, /* ctx フラグを無視 */
            NULL, /* time_rec を無視 */
            NULL); /* 代行信任状を無視 */
    }
}

```

```

        /* 受信されたトークンをリリースします */
        gss_release_buffer(&min_stat, &recv_tok);

        /* クライアントが相互の認証を求めるトークンがあるかどうか
        調べます。 */
        if (send_tok.length != 0)
        {
            /* 相手側にトークン・メッセージを送信します */
            /* 送信トークン・バッファをリリースします */
        }
    } while (maj_stat == GSS_S_CONTINUE_NEEDED);

    /* クライアント名が戻されます - チケットからクライアントを抽出します。
    この クライアント名は、OS400 ユーザー・プロファイルとの
    マップに使用されます*/
    maj_stat = gss_display_name(&min_stat, client, client_name, &doid);

    maj_stat = gss_release_name(&min_stat, &client);

    return 0;
}

/*****
/*
/* 関数名: getTestPort()
/*
/* 記述名: サーバーが listen するポートを取得します
/*
/* 入力: char * service - サービス名。ヌルの場合、
/*         kerb-test-server を探します。
/*
/* 出力: なし
/*
/* 正常終了: 戻り値 == ポート番号
/*
/* エラー終了: N/A
/*
*****/
CLINKAGE int getTestPort(char *name)
{
    struct servent service;
    struct servent_data servdata;
    char defaultName[] = "kerb-test-server", *servName;
    char tcp[] = "tcp";
    int retPort, rc;
    memset(&servdata, 0x00, sizeof(servdata));
    memset(&service, 0x00, sizeof(service));
    if (name == NULL)
        servName = defaultName;
    else
        servName = name;
    rc = getservbyname_r(servName, tcp, &service,
        &servdata);

    if (rc != 0)
        retPort = DEFAULT_KERB_SERVER_PORT;
    else
        retPort = service.s_port;

    return ntohs(retPort);
}

/*****
/*
/* 関数名: getListeningSocket()
*****/

```

```

/*
/* 記述名: 作成された listen ソケットを取得し、それを戻します。
/*
/* 入力: なし。
/*
/* 出力: 作成された listen ソケット。
/*
/* 正常終了: 戻り値 == listen ソケット。
/*
/* エラー終了: -1、エラーが検出されました。
/*
/* 注: エラー検査が除去されました
/*
/*****
CLINKAGE int getListeningSocket(void)
{
    int rc, sd, option;
    struct sockaddr_in sin;

    sd = socket(AF_INET, SOCK_STREAM, 0)

    option = 1;

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

    memset(&sin, 0x00, sizeof(sin));
    sin.sin_family = AF_INET;
    sin.sin_port = htons(getTestPort(NULL));

    bind(sd, (struct sockaddr *)&sin, sizeof(sin));

    listen(sd, SOMAXCONN);

    return sd;
}
/* getListeningSocket() を終了します */

/*****
/*
/* 関数名: getServerSocket()
/*
/* 記述名: クライアントに接続されているサーバー・ソケットを
/* 取得します。このルーチンは、クライアントの待機
/* をブロックします。
/*
/* 入力: int lsd - listen ソケット。
/*
/* 出力: 作成されたサーバー・ソケット。
/*
/* 正常終了: 戻り値 == サーバー・ソケット。
/*
/* エラー終了: -1、エラーが検出されました。
/*
/* 注: エラー検査が除去されました
/*
/*****
CLINKAGE int getServerSocket(int lsd)
{
    return accept(lsd, NULL, 0);
}
/* getServerSocket() を終了します */

/*****
/*
/* 関数名: main
/*

```

```

/* 記述名:      Kerberos 認証と EIM マッピングを実行する      */
/*              サーバー・プログラム用のドライバー。          */
/*              */
/* 入力:      char* service_name - 要求されたサービスの名前  */
/*              */
/* 正常終了:  0 = 成功                                          */
/*              */
/* エラー終了: -1、エラーが検出されました。                */
/*              */
/* 注: エラー検査が除去されました                          */
/*              */
/*              */
/*****/
int main(int argc, char **argv)
{
    int ssd,          /* サーバー・ソケット      */
        lsd;         /* listen ソケット        */
    char *service_name; /* サービスの名前 (入力) */
    gss_cred_id_t server_creds; /* 獲得するサーバー信任状 */
    gss_ctx_id_t context; /* GSS コンテキスト      */
    OM_uint32 maj_stat, /* GSS 状況コード        */
              min_stat; /* メカニズム (kerberos) 状況 */
    gss_buffer_desc client_name; /* コンテキストを確立する
                                   クライアント・プリンシパル */

char OS400User[10];
char save_handle[SY_PH_MAX_PRFHDL_LEN]; // *CURRENT プロファイル・ハンドル
char client_handle[SY_PH_MAX_PRFHDL_LEN]; // プロファイル・ハンドルにスワップ
EimHandle eimHandle;

    Qus_EC_t errorcode;
    memset(errorcode, 0x00, 256);
    errorcode->Bytes_Provided = 256;

    service_name = argv[1];

    /*-----
    // Kerberos セットアップ
    // サービスの信任状を獲得します
    //-----*/
    get_kerberos_credentials_for_server(service_name, &server_creds);

    /*-----
    // listen ソケットを取得します
    //-----*/
    lsd = getListeningSocket();

    /*-----
    // EIM セットアップ
    // EIM との接続
    // -----*/
    l_eimConnect(&eimHandle);

    /*-----
    // 現行ユーザーのコピーを保管して、各要求後に現行ユーザーに
    // 戻れるようにします。
    // -----*/
    QsyGetProfileHandleNoPwd(save_handle,
                             " *CURRENT ",
                             " *NOPWD ",
                             &errorcode);

    /*-----
    // ソケット上の要求の待機をループします
    //-----*/
    do { /* アプリケーションまたはシステムが終了するまでループします */
        /* 現行ユーザーのプロファイル・ハンドルを保管します */

```



```

        /* TCP 接続を受け入れます */
        ssd = getServerSocket(lsd);

        /* -----
        // クライアントとのコンテキストを確立し、クライアント名を取得します。
        //-----
        // クライアント名には、Kerberos プリンシパルとレルムが含まれます。
        // EIM では、ソース・ユーザーとソース・レジストリーに相当します。
        //----- */
        do_kerberos_authentication(ssd,
                                   server_creds,
                                   &context,
                                   &client_name);

/*-----
// EIM マッピング探索操作を実行して、関連した
// OS400 ユーザーを取得します。
//----- */
getOS400User(&eimHandle,
             OS400User,
             &client_name);

/* -----
// EIM 探索から戻されたユーザーにスワップします。
// ----- */
QsyGetProfileHandleNoPwd(client_handle,
                        client_name,
                        "*NOPWDCHK ",
                        &errorcode);
QsySetToProfileHandle(client_handle, &errorcode);

/* -----
// アプリケーションが該当するユーザー・プロファイルの下で現在実行
// されているので、ここでアプリケーションの実際の作業を行います
// ----- */
// ここで、アプリケーション固有の動作を呼び出すか、コード化します。

/* -----
// オリジナルのユーザー・プロファイルの下で実行されるようにプロセスを再設定します
// ----- */
QsySetToProfileHandle(save_handle, &errorcode);

} while (1)

eimDestroy_handle(&eimHandle);

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

```

計画

ここでは、ソフトウェアおよびハードウェアの前提条件ならびにその他の要件など、シングル・サインオンのインプリメントの計画に関する考慮事項および作業について確認します。また、シングル・サインオンの計画プロセスを検討して、個々の企業でシングル・サインオンをインプリメントする際の最善の立案に役立てます。

自社のニーズを満たすシングル・サインオン環境を作成するには、慎重な計画が必要です。i5/OS シングル・サインオンを計画する際に、いくつかの決定を行う必要があります。1つの決定は、ポリシー・アソシエーションを作成するかどうかです。企業のセキュリティーの問題が、この種類の決定に大きく影響します。

シングル・サインオン環境の計画段階を完了するのに使用できるリソースは、次のとおりです。

シングル・サインオン環境を十分に計画した後、シングル・サインオン環境を構成できます。

シングル・サインオン環境の構成要件

この情報により、シングル・サインオン環境を実現する前に、サーバーがハードウェアとソフトウェアの前提条件を満たしていることを確認してください。

V5R4 iSeries サーバーの要件

注: シングル・サインオンは、OS/400 バージョン 5 リリース 2 (V5R2) およびi5/OS V5R3 でも使用可能です。しかし、このトピックの詳細な構成情報は、i5/OS V5R4 以降でのみ使用可能な新しいシングル・サインオン機能 (ポリシー・アソシエーションなど) に基づいています。

正常なシングル・サインオン環境を作成するには、下記の要件がすべて満たされていることを確認してください。

- i5/OS バージョン 5 リリース 4 (5722-SS1) がインストールされていること。
- 最新の i5/OS プログラム一時修正 (PTF) が適用されていること。
- iSeries Access for Windows、バージョン 5 リリース 4(5722-XE1) がインストールされていること。
- 最新の i5/OS V5R4 iSeries Access for Windows サービス・パックがインストールされていること。

最新のサービス・パックについては、『iSeries Access』を参照してください。

- i5/OS Host Servers (5722-SS1 オプション 12) がインストールされていること。
- Qshell Interpreter (5722-SS1 オプション 30) がインストールされていること。
- 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いること。

注: iSeries ナビゲーター の機能同期化ウィザードを使用して、複数のシステムに既存のシングル・サインオン構成を反映させようとする場合は、パスワードなどの機密構成情報の送信を保護するために Secure Sockets Layer (SSL) を使用するよう、システムを構成する必要があります。

クライアント PC の要件

正常なシングル・サインオン環境を作成するには、下記の要件がすべて満たされていることを確認してください。

- Microsoft Windows 2000 または Microsoft Windows XP オペレーティング・システムが使用されていること。
- iSeries Access for Windows、バージョン 5 リリース 4(5722-XE1) がインストールされていること。
 - iSeries ナビゲーター のネットワーク・コンポーネントが、シングル・サインオンを管理する PC にインストールされていること。
 - iSeries ナビゲーター のセキュリティー・コンポーネントが、シングル・サインオンを管理する PC にインストールされていること。
- 最新の i5/OS V5R4 iSeries Access for Windows サービス・パックがインストールされていること。

最新のサービス・パックについては、『iSeries Access』を参照してください。

- TCP/IP が構成されていること。

Microsoft Windows サーバーの要件

正常なシングル・サインオン環境を作成するには、下記の要件がすべて満たされていることを確認してください。

- ハードウェアの計画とセットアップが完了していること。
- Windows 2000 Server または Windows Server 2003 が使用されていること。
- Windows Support Tools (ktpass ツールを提供) がインストールされていること。
- TCP/IP が構成されていること。
- Windows 2000 ドメインが構成されていること。
- ネットワーク内のユーザーが、Microsoft Windows Active Directory を使用して Windows 2000 ドメインに追加されていること。


提供されている計画ワークシートを使用すると、シングル・サインオンの実現についての情報収集と決定に役立ちます。各ワークシートには、実行する必要があるタスクのリストが含まれています。


ネットワーク認証サービスの計画

ネットワークでネットワーク認証サービスまたは Kerberos ソリューションをインプリメントする前に、必要な計画作業を完了しておく必要があります。

ネットワーク認証サービスまたは Kerberos インプリメンテーションを計画するには、ネットワーク上のシステムとユーザーについて、適切な情報を収集する必要があります。ネットワーク内にネットワーク認証サービスを構成するのに役立つ、数種類の計画ワークシートが用意されています。

注: 多くの、さまざまな Kerberos 認証ソリューションがあり、お客様の企業で使用できます。以下では、iSeries インプリメンテーションの計画、および、Microsoft Windows Active Directory または i5/OS PASE に構成された Kerberos サーバーでネットワーク認証サービスを使用する際の考慮事項に焦点をあてて説明します。

Microsoft Windows Active Directory 内での Kerberos サーバーのセットアップについては、Microsoft Windows 2000 のヘルプ  を参照してください。

以下の IBM  プラットフォームでは、Kerberos 認証をサポートしています。プラットフォーム固有の Kerberos インプリメンテーションについては、次のソースを参照してください。

- pSeries®
 - 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 にあります。 

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

ネットワーク認証サービスを計画するには、以下の作業を実行してください。

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 サーバーの計画を作成します。

Kerberos サーバーすなわち鍵配布センター (KDC) は、プリンシパルおよびその関連パスワードのデータを保守します。このサーバーは、認証サーバーと発券サーバーで構成されます。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、発券許可証を送信します。Kerberos 認証の使用を計画する際は、どのシステムを Kerberos サーバーとして構成するかを決定する必要があります。

注: ネットワーク認証サービスについては、i5/OS PASE または Windows 2000 サーバーで実行される Kerberos サーバーに焦点をあてて説明します。ほとんどのシナリオおよび例では、明示的に断りがない限り、Windows 2000 サーバーが Kerberos サーバーとして構成されていると想定しています。その他のオペレーティング・システムまたはサード・パーティーのアプリケーションを Kerberos 認証用に使用する場合は、該当する資料を参照してください。

以下に、3 つの主要なオペレーティング・システムでの Kerberos サーバーのサポートについて詳しく説明します。

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・システムが、それぞれのデフォルトのセキュリティ・メカニズムとして Kerberos 認証をサポートしています。管理者が、Microsoft Windows Active Directory を使用してユーザーおよびサービスを追加すると、管理者は、実際には、これらのユーザーおよびサービスに対して Kerberos プリンシパルを作成します。Windows 2000 または 2003 サーバーをネットワークで使用している場合は、そのオペレーティング・システムの中に Kerberos サーバーが作成されます。Kerberos 認証がどのように Microsoft Windows サーバーの中で使用されるかについては、Microsoft Windows


のヘルプ  を参照してください。

AIX および i5/OS PASE

AIX および i5/OS PASE は、kadmin コマンドを使用して Kerberos サーバーをサポートします。管理者は (call QP2TERM と入力して) PASE 環境に入り、PASE Kerberos サーバーを構成し、管理する必要があります。i5/OS PASE による Kerberos サーバーのサポートは、V5R3 が初めてです。i5/OS PASE は、Kerberos サーバーなどの AIX アプリケーションにランタイム環境を提供します。AIX での Kerberos サーバーの構成と管理については、次の資料を参照してください。

- *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 にあります。 

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。Network Authentication Service for z/OS は、ミドルウェア・プログラムを購入または使用しなくても、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 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詳しくは、「z/OS Security Server ネットワーク認証サービス 管理ガイド」  を参照してください。

どのオペレーティング・システムによって Kerberos サーバーが提供されている場合でも、Kerberos サーバー用のサーバー・ポートを決め、Kerberos サーバーへのアクセスを保護し、クライアントと Kerberos サーバーとの間の時刻が同期していることを確認する必要があります。

サーバー・ポートの決定

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、Kerberos サーバーの構成ファイルにはその他のポートを指定できます。Kerberos サーバーにある Kerberos 構成ファイルのポート番号を確認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の暗号漏えいが起こらないようにするために、機密保護機能のある専用システムに配置する必要があります。Kerberos サーバーへのユーザーのアクセスは限定する必要があります。Kerberos サーバーがあるシステムが、Web サーバーまたは FTP サーバーなどの他の目的にも使用されている場合、あるユーザーが、これらのアプリケーションの中のセキュリティ上の欠陥を利用して、Kerberos サーバーに保管されているデータベースにアクセスすることがあります。Microsoft Windows Active Directory に作成されている Kerberos サーバーの場合、Kerberos サーバーに保管されている自分自身のパスワードを管理し更新するためにプリンシパルが使用できる、パスワード・サーバーをオプションで構成できます。Kerberos サーバーを i5/OS PASE に構成して、iSeries を Kerberos 認証専用にはできない場合は、管理者のみが Kerberos 構成にアクセスできるようにする必要があります。

システム時刻の同期化

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、Kerberos サーバーの指定最大クロック・スキュー内に時刻がおさまっていない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、ハッカーは、後刻同じチケットをネットワークに再送信して認証を受けることはできません。また、iSeries システムは、Kerberos サーバーのクロックが、ネットワーク認証サービス構成時に設定された最大クロック・スキュー内にない場合、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・スキューはこのデフォルトに設定されます。ただし、必要な場合は、この値を変更できます。この値を 300 秒を超えた値に上げることはお勧めできません。システム時刻の処理について詳しくは、システム時刻の同期化を参照してください。

表 11. 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、管理者が計画したネットワーク用の Kerberos サーバーの例を示します。

質問	応答
どのオペレーティング・システムに Kerberos サーバーを構成することを計画しますか？ <ul style="list-style-type: none">• Windows 2000 サーバー• Windows Server 2003• AIX サーバー• i5/OS PASE (V5R3 以降)• zSeries	i5/OS Portable Application Solutions Environment (PASE)
Kerberos サーバーの完全修飾ドメイン名は何ですか？	iseriesa.myco.com
PC と、Kerberos サーバーに接続するシステムとの間の時刻は同期していますか？ 最大クロック・スキューは何秒ですか？	はい、300 秒です。

表 11. Kerberos サーバーの計画ワークシートの例 (続き) : この計画ワークシートは、管理者が計画したネットワーク用の Kerberos サーバーの例を示します。

質問	応答
Network Authentication Enablement (5722-NAE) プロダクトをインストールするべきですか?	はい。Kerberos サーバーを V5R4 システムで実行される i5/OS PASE 上に構成する予定がある場合はインストールするべきです。V5R4 では、ネットワーク認証サーバーは、別のプロダクト、Network Authentication Enablement (5722-NAE) として配送されます。 i5/OS V5R3 を使用している場合、Kerberos サーバーを i5/OS PASE に構成する場合は、代わりに Cryptographic Access Provider (5722-AC3) をインストールする必要があります。

レルムの計画

お客様のエンタープライズを理解することは、ご使用の環境のレルムの計画に役立ちます。

Kerberos プロトコルでは、レルムは、Kerberos サーバーまたは鍵配布センター (KDC) と呼ばれる単一認証サーバーを使用するマシンおよびサービスの集合で構成されます。レルムは個々に管理されます。レルム内のアプリケーションおよびサービスは、通常、ある種の共通使用あるいは共通目的を共有します。以下の一般質問が、エンタープライズ内のレルムの計画を作成する際に役立ちます。

現行の環境はどのような大きさか?

環境のサイズによって、必要なレルムの数が決まります。大規模なエンタープライズでは、組織上の境界、または、エンタープライズ内のシステムの使用方法に基づいた複数のレルムを考慮することができます。たとえば、会社の中の異なる組織 (人的資源、お客様サービス、配送を担当する各部門) をあらわすレルムを設定します。また、同様の機能を実行するマシンまたはサービスの集合を表すレルムを作成できます。通常、小規模のエンタープライズでは、1 つまたは 2 つのレルムで十分です。

環境が大きくなる速さはどのくらい速いか?

エンタープライズが速く大きくなるのが計画できる場合は、エンタープライズ内の小規模な組織単位を表す複数のレルムをセットアップする必要があります。エンタープライズがゆっくり大きくなるのが予想できる場合は、現行の組織を基にして、レルムを 1 つまたは 2 つだけセットアップします。

レルムを管理するのに何人の管理者が必要か?

エンタープライズの規模に関係なく、有能な人材を使用して、必要なレルムをセットアップし管理できることが必要です。

レルムの命名

Kerberos プロトコルの規則にしたがって、レルムの名前は、通常、たとえば MYCO.COM のようにドメイン名の太文字で構成されます。複数のレルムがあるネットワークでは、太文字の記述名とドメイン名を含むレルム名を作成できます。たとえば、2 つのレルムがある場合、それぞれが会社内の特定の部門を表すように、1 つには HR.MYCO.COM という名前、他方には SHIPPING.MYCO.COM という名前を付けることができます。

太文字の使用は必須ではありませんが、Kerberos のインプリメンテーションの一部ではこの規則が強制されます。たとえば、Microsoft Windows Active Directory では、レルム名は太文字でなければなりません。

Microsoft Windows Active Directory 内に構成された Kerberos レルムに参加するように iSeries 上でネットワーク認証サービスを構成する場合は、レルム名を大文字で入力する必要があります。

i5/OS PASE に構成された Kerberos サーバーの場合は、大文字のレルム名でも小文字のレルム名でも作成できます。ただし、Microsoft Window Active Directory を使用して構成された Kerberos サーバーと、i5/OS PASE 内に構成された Kerberos サーバーとの間にトラスト関係を作成する予定がある場合は、レルム名は大文字でなければなりません。

表 12. Kerberos レルムの計画ワークシートの例

質問	応答
レルムはいくつ必要ですか?	2 つ
レルムはどのように編成する予定ですか?	現在、会社では Windows 2000 サーバーを使用して、注文受理部門でユーザーを認証しています。配送部門では、i5/OS PASE 内に構成された Kerberos サーバーを使用しています。これらの部門ではそれぞれ自分のレルムを使用する予定です。
レルムにはどのような命名規則を使用しますか?	部門名の後に Windows 2000 の大文字のドメイン名を続けて部門を表す、大文字の短縮名を使用する予定です。たとえば、ORDEPT.MYCO.COM は注文受理部門を表し、SHIPDEPT.MYCO.COM は配送部門を表します。

プリンシパル名の計画

Kerberos ネットワーク内のプリンシパル名を計画します。

プリンシパルは、Kerberos ネットワーク内のユーザーまたはサービスの名前です。プリンシパル名は、ユーザー名またはサービス名と、ユーザーまたはサービスが属すレルムの名前で構成されます。Mary Jones が使用するレルムが MYCO.COM である場合、Mary Jones のプリンシパル名は jonesm@MYCO.COM のようになります。Mary Jones は、中央の Kerberos サーバーによって認証を受けるには、このプリンシパル名と関連パスワードを使用します。すべてのプリンシパルが Kerberos サーバーに追加され、Kerberos サーバーが、レルム内のすべてのユーザーとサービスのデータベースを維持します。

プリンシパルを命名する体系を作成する際は、現在と将来のユーザーを収容できる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。以下の提案を参考にしてプリンシパルの命名規則を設定してください。

- ファミリー名とファーストネームのイニシャルを使用する
- 最初のイニシャルとフル・ファミリー名を使用する
- ファーストネームと最後のイニシャルを使用する
- たとえば database1 のように、アプリケーション名またはサービス名と識別番号を使用する


i5/OS プリンシパル名

iSeries システム上にネットワーク認証サービスを構成する際に、オプションでプリンシパル名を作成できます。これらのプリンシパルのそれぞれは、iSeries サーバーにあるサービスを表します。ネットワーク認証サービスを構成する際に、ユーザーが作成するサービス・プリンシパルのそれぞれについて、キー・テーブル項目が iSeries システムに作成されます。このキー・テーブル項目には、サービス・プリンシパル名と、構成時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ら、すべての i5/OS サービス・プリンシパルを Kerberos サーバーに追加する必要があることに注意してください。Kerberos サーバーに i5/OS プリンシパルを追加する方式は、エンタープライズ内に構成した

Kerberos サーバーによって異なります。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、101 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。以下に、ネットワーク認証サービスの構成時に作成された i5/OS サービス・プリンシパルのそれぞれについて説明します。

i5/OS Kerberos 認証

i5/OS Kerberos 認証のキータブ項目を作成することを選択すると、キータブ・ファイルに、サービス・プリンシパルが、**krbsvr400/iSeries fully qualified domain name@REALM NAME** または **krbsvr400/iSeries host name@REALM NAME** のどちらかの形式で生成されます。たとえば、i5/OS Kerberos 認証の有効なサービス・プリンシパルは、krbsvr400/iseriasa.myco.com@MYCO.COM または krbsvr400/iseriasa@MYCO.COM になります。i5/OS は、ホスト名を解決するために iSeries がどのように構成されているかによって、DNS サーバーまたは iSeries サーバーのどちらかで検出したホスト名を基にして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、たとえば、QFileSrv.400、Telnet、Distributed Relational Database Architecture (DRDA)、iSeries NetServer、および IBM  iSeries Access for Windows (iSeries ナビゲーターを含む) 用に使用されます。これらのアプリケーションのそれぞれは、Kerberos 認証を使用可能にするには、追加の構成が必要です。

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時に、IBM Directory Server for iSeries (LDAP) 用にオプションで追加のサービス・プリンシパルを構成できます。LDAP のプリンシパル名は、**ldap/iSeries fully qualified domain name@REALM NAME** になります。たとえば、有効な LDAP プリンシパル名は ldap/iseriasa.myco.com@MYCO.COM になります。このプリンシパル名は、その iSeries システムにあるディレクトリー・サーバーを示します。

注：従来のリリースでは、ネットワーク認証サービス・ウィザードで、LDAP サービス用の大文字のキータブ項目が作成されていました。ネットワーク認証サービスを再構成する際にすでに LDAP プリンシパルを構成していた場合、または、EIM (エンタープライズ識別マッピング) を使用してウィザードを使用する場合に、このプリンシパル名を小文字バージョンに変更するようプロンプトが出されます。

ディレクトリー・サーバーで Kerberos 認証を使用する予定がある場合は、ネットワーク認証サービスを構成するだけでなく、Kerberos 認証を受け入れるようにディレクトリー・サーバーのプロパティーを変更する必要があります。Kerberos 認証が使用されると、ディレクトリー・サーバーは、サーバーの識別名 (DN) を Kerberos プリンシパル名に関連付けます。ユーザーは、サーバー DN を、以下の方式のいずれかに関連付けることを選択できます。

- サーバーは、Kerberos プリンシパル名を基にして DN を作成できます。このオプションを選択すると、principal@realm という形式の Kerberos ID が、ibm-kn=principal@realm という形式の DN を生成します。ibm-kn= は、ibm-kerberosName= に等価です。
- サーバーはディレクトリーをサーチして、Kerberos プリンシパルおよびレルム用の項目が入っている識別名 (DN) の有無を調べます。ユーザーがこのオプションを選択すると、サーバーはディレクトリーをサーチし、この Kerberos ID を指定した項目の有無を調べます。

ディレクトリー・サーバーの構成 Kerberos 認証について詳しくは、『IBM Directory Server for iSeries (LDAP)』を参照してください。

Apache で稼働する HTTP Server

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時に、オプションで、Apache で稼働する HTTP Server 用の追加のサービス・プリンシパルを構成できます。HTTP プリンシパル名は **HTTP/iSeries fully qualified domain name@REALM NAME** になります。こ

のプリンシパル名は、Kerberos を使用してウェブ・ユーザーを認証する iSeries 上の HTTP サーバー・インスタンスを示します。HTTP サーバー・インスタンスを使用して Kerberos 認証を使用するには、HTTP サーバーに関する追加の構成ステップを実行する必要があります。

HTTP サーバーを使用して Kerberos 認証を使用する方法については、HTTP Server:

documentation  ホーム・ページを参照してください。

iSeries NetServer

iSeries NetServer の場合、iSeries 上のキータブ・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できます。これらの NetServer プリンシパルのそれぞれは、iSeries NetServer に接続するために使用する潜在的なクライアントを表します。次の表は、iSeries NetServer プリンシパル名、およびプリンシパルが表すクライアントを示します。

表 13. iSeries NetServer プリンシパル名

クライアント接続	iSeries NetServer プリンシパル名
Windows XP	cifs/iSeries 完全修飾ドメイン名 cifs/iSeries ホスト名 cifs/QiSeries ホスト名 cifs/qiSeries ホスト名 cifs/IP アドレス
Windows 2000	HOST/iSeries 完全修飾ドメイン名 HOST/iSeries ホスト名 HOST/QiSeries ホスト名 HOST/qiSeries ホスト名 HOST/IP アドレス

このアプリケーションで Kerberos 認証を使用することについて詳しくは、iSeries NetServer を参照してください。

計画ワークシートの例

表 14. プリンシパルの計画ワークシートの例

質問	応答
ネットワーク内のユーザーを表す Kerberos プリンシパル用に使用する予定の命名規則は何ですか?	最初のイニシャルに続くファミリー名の小文字の最初の 5 文字。例: mjones
ネットワーク上のアプリケーションに使用する命名規則は何ですか?	後に数値が続く記述名。例: database123
どの i5/OS サービスに Kerberos 認証を使用する予定ですか?	1. i5/OS Kerberos 認証は次のサービスに使用する予定: iSeries Access for Windows、iSeries ナビゲーター、NetServer、および Telnet。 2. Apache で稼働する HTTP Server 3. LDAP
これらの i5/OS サービスのそれぞれの i5/OS プリンシパル名は何ですか?	1. krbsvr400/iseriasa.myco.com@MYCO.COM 2. HTTP/iseriasa.myco.com@MYCO.COM 3. ldap/iseriasa.myco.com@MYCO.COM

ホスト名の解決に関する考慮事項

Kerberos が使用できるアプリケーションで、Kerberos 認証とホスト名の解決が正しく機能できることを確認してください。これは、ご使用の PC と、ご使用の iSeries サーバーが、サービス・アプリケーションがあるシステムの同じホスト名を解決できることを確認することによって行います。

Kerberos 環境では、クライアントとサーバーの両方が、ある方式によるホスト名解決を使用して、特定のアプリケーションまたはサービスがあるシステムのホスト名を決定します。iSeries サーバーと PC がドメイン・ネーム・システム (DNS) サーバーを使用する場合は、ホスト名解決を実行するためにサーバーと PC が 1 つの DNS サーバーを使用する、または、複数の DNS サーバーを使用する場合は、ホスト名が両方のサーバーで同じであることが重要です。ご使用の iSeries システムまたは PC がホスト名をローカルで (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、DNS サーバーに記録されている対応するホスト名と異なるホスト名を解決する場合があります。これはネットワーク認証サービスが失敗する原因になります。

Kerberos 認証とホスト名解決が、Kerberos が使用できるアプリケーションで正しく機能できるようにするには、ご使用の PC と、ご使用の iSeries サーバーが、サービス・アプリケーションが存在しているシステムの同じホスト名を解決できることを確認しなければなりません。次の例では、このシステムは iSeries A と呼ばれます。

以下の説明では、PC と iSeries システムが iSeries A の同じ名前を解決するかどうかを判別する方法を示します。説明にしたがって進む際には、ワークシートの例を参照してください。

ユーザーの Kerberos レalmについて以下のステップを実行するときは、ブランクのワークシートにご自身の情報を入力してください。

次の図には、次の例で使用しているホスト名情報が入っているシステム・ファイルとレコードが示されています。

注: IP アドレス 10.1.1.1 は公用 IP アドレスを表します。このアドレスは例示目的のみに使用されています。

DNS サーバー



```
10.1.1.1=iseriesa.myco.com
iseriesa.myco.com=10.1.1.1
```



```
10.1.1.1 i seriesa.myco.com
```

ホスト・ファイル

C:\WINNT\system32\drivers\etc\hosts

iSeries A



```
10.1.1.1
```

```
iseriesa.myco.com
```

インターネット・アドレス	ホスト名
10.1.1.1	iseriesa.myco.com

ローカル・ホスト・テーブル
(CFGTCP オプション 10)

```
ホスト名: iseriesa
ドメイン名: myco.com
```

ホスト名検索優先順位:
*LOCAL または *REMOTE

TCP/IP ドメイン情報

(CFGTCP オプション 12)

詳細

DNS サーバー

- IP アドレス 10.1.1.1 が、iSeries A の IP アドレスおよびホスト名であるホスト名 iseriesa.myco.com に相互に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ます。
- ホストの解決のために、PC、iSeries A、あるいはその両方で使用できます。

注: この例では、DNS サーバーが 1 つ示されています。ただし、ご使用のネットワークでは複数の DNS サーバーを使用できます。たとえば、ホスト名を解決するためにご使用の PC が DNS サーバーを 1 つ使用し、さらにご使用の iSeries サーバーが別の DNS サーバーを使用できます。ホスト解決のためにご使用のレームが DNS サーバーをいくつ使用しているかを判別し、この情報をご使用の状態に当てはめる必要があります。

PC

- Windows 2000 オペレーティング・システムを実行します。
- ネットワーク認証サービスを管理するために使用されている PC、および、ユーザーがルーチン作業のために特殊権限なしに使用している PC の両方を表します。
- IP アドレス 10.1.1.1 がホスト名 iseriesa.myco.com に相互関連していることを示す hosts ファイルが入っています。

注: hosts ファイルは以下のフォルダーにあります。

- 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

iSeries A

- i5/OS バージョン 5 リリース 3 (V5R3) を実行します。
- 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があるサービス・アプリケーションが入っています。
- 「TCP の構成 (CFGTCP)」メニュー内で、オプション 10 および 12 は、iSeries A について以下の情報を示します。
 - オプション 10 (TCP/IP ホスト・テーブル項目の処理):
 - インターネット・アドレス: 10.1.1.1
 - ホスト名: iseriesa.myco.com
 - オプション 12 (TCP/IP ドメイン情報の変更):
 - ホスト名: iseriesa
 - 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、サーバーでホスト解決を実行するためにネットワーク管理者がどのように TCP/IP を構成したかによって、*LOCAL または *REMOTE を示します。

表 15. 例: PC ホスト名解決ワークシート

PC 上で、iSeries 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	iseriesa.myco.com
1.b.1	DNS サーバー	iseriesa.myco.com

表 16. 例: iSeries ホスト名解決ワークシート

iSeries A 上で、iSeries 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	iSeries A CFGTCP オプション 12	ホスト名: iseriesa 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	iSeries A CFGTCP オプション 10	iseriesa.myco.com
2.c.1	DNS サーバー	iseriesa.myco.com

表 17. 例: ホスト名のマッチング・ワークシート

これらの 3 つのホスト名は正確に一致しなければなりません	
ステップ	ホスト名
ステップ 1	iseriesa.myco.com

表 17. 例: ホスト名のマッチング・ワークシート (続き)

これらの 3 つのホスト名は正確に一致しなければなりません	
ステップ 2.a.2	iseriesa myco.com
2d	iseriesa.myco.com

表 18. PC ホスト名解決ワークシート

PC 上で、iSeries サーバー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 19. iSeries ホスト名解決ワークシート

ご使用の iSeries サーバーで、iSeries のホスト名を判別する		
ステップ	ソース	ホスト名
2.a.2	iSeries CFGTCP 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	iSeries CFGTCP オプション 10	
2.c.1	DNS サーバー	

表 20. ホスト名のマッチング・ワークシート

これらの 3 つのホスト名は正確に一致しなければなりません	
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 とご使用の iSeries サーバーが、同じホスト名を解決することを確認してください。

ホスト名を解決する、前のワークシートの例を参考に使用します。PC と iSeries システムが、iSeries A の同じホスト名を解決することを確認するには、以下のステップを実行します。

1. PC から、iSeries A の完全修飾 TCP/IP ホスト名を判別します。

注: ご使用のネットワークの管理方法によっては、上記のステップを、シングル・サインオン環境を結合するほかの PC で実行する必要があります。

a. PC 上の Windows エクスプローラーで、以下の場所のいずれかから hosts ファイルを開きます。

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

注: PC に hosts ファイルが存在しない場合は、ご使用の PC は、ホスト名を解決するために DNS サーバーを使用している場合があります。その場合は、ステップ 1b にスキップしてください。

1) ワークシート上に、大文字か小文字かを注意して、iSeries A の最初のホスト名項目を記入します。たとえば、iseriesa.myco.com と記入します。

注: 「hosts」ファイルに iSeries A 用の項目が入っていない場合は、ご使用の PC は、ホスト名を解決するために DNS サーバーを使用している場合があります。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 サーバーに照会します。

注: PC の hosts ファイルにホスト名項目があった場合は、このステップをスキップし、ステップ 2 に進んでください。(オペレーティング・システムが PC のホスト名を解決するときは、hosts ファイルが DNS サーバーよりも優先順位が高くなります。)

1) コマンド・プロンプトで NSLOOKUP と入力し、Enter キーを押します。NSLOOKUP プロンプトで、10.1.1.1 と入力し、DNS サーバーに照会して iSeries A の有無を調べます。大文字または小文字に注意して、DNS サーバーが戻したホスト名を書き留めます。たとえば、iseriesa.myco.com と書き留めます。

2) NSLOOKUP プロンプトで iseriesa.myco.com と入力します。これは、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、期待していた IP アドレスを戻したか確認します。たとえば、10.1.1.1 です。

注: NSLOOKUP が期待した結果を戻さない場合は、ご使用の DNS 構成が完全ではありません。たとえば、NSLOOKUP が、ステップ 1.b.1 でユーザーが入力したアドレスではない IP アドレスを戻した場合は、次のステップに進む前に、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. iSeries A から、その完全修飾 TCP/IP ホスト名を判別します。

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) を選択します。

2) 大文字または小文字に注意して、ホスト名 パラメーターおよび ドメイン名 パラメーターの値を書き留めます。たとえば、

- **ホスト名:** iseriesa
- **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ます。

- *LOCAL - オペレーティング・システムは、まず、ローカル・ホスト・テーブル (PC 上の hosts ファイルに等価) を検索します。ホスト・テーブルにマッチングする項目がなく、さらに DNS サーバーが構成されている場合、オペレーティング・システムは次にご使用の 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、まず、DNS サーバーを検索します。DNS サーバーにマッチングする項目がない場合は、オペレーティング・システムは次にローカル・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・テーブル項目の処理) を選択します。
- 2) 大文字または小文字に注意して、iSeries A に対応する ホスト名 欄の値を書き留めます (IP アドレス 10.1.1.1)。たとえば、iseriesa.myco.com と書き留めます。

注: ホスト・テーブルに iSeries A の項目がない場合は、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 キーを押します。NSLOOKUP プロンプトで、10.1.1.1 と入力し、DNS サーバーに照会して iSeries A の有無を調べます。大文字または小文字に注意して、DNS サーバーが戻したホスト名を書き留めます。たとえば、iseriesa.myco.com と書き留めます。
- 2) NSLOOKUP プロンプトで iseriesa.myco.com と入力します。これは、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、期待していた IP アドレスを戻したか確認します。たとえば、10.1.1.1 です。

注: NSLOOKUP が期待した結果を戻さない場合は、ご使用の DNS 構成が完全ではありません。たとえば、NSLOOKUP が、ステップ 2.b.1 でユーザーが入力したアドレスではない IP アドレスを戻した場合は、次のステップに進む前に、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 構成に基づいて、iSeries A が保持するホスト名の値を判別します。

- ホスト名検索優先順位 パラメーターの値が *LOCAL である場合は、ローカル・ホスト・テーブルから書き留めた (ステップ 2.b.2) 項目を保持します。
- ホスト名検索優先順位 パラメーターの値が *REMOTE である場合は、DNS サーバーから書き留めた (ステップ 2.c.1) 項目を保持します。
- これらのソースの 1 つだけに iSeries A の項目が入っていた場合は、この項目を保持します。

3. これらのステップの結果を比較します。

a. ステップ 1 - iSeries A 用に PC が使用する名前。

注: PC の hosts ファイルに iSeries A の項目がある場合は、その項目を使用します。そうでない場合は、DNS サーバーにある項目を使用します。

b. ステップ 2.a.2 - iSeries A がその TCP/IP 構成内で自身を呼び出す名前。

c. ステップ 2d - iSeries A がホスト名の解決に基づいて自身を呼び出す名前。

これらの項目は 3 つがすべて、大文字および小文字を含めて、正確に一致しなければなりません。結果が正確に一致しない場合は、キータブ項目が見つからなかったことを示すエラー・メッセージが出ます。

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常に構成するには、要件を理解し、必要な計画ステップを完了する必要があります。

このトピックでは、必要なステップをすべて完了できるようにするための、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の計画、および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、必要な前提条件がすべて完了したことを確認します。構成作業を実行する前に、すべての前提条件項目に「はい」と応答できなければなりません。

表 21. 前提条件ワークシート



質問	応答
ご使用の i5/OS は V5R3 (5722-SS1) 以降ですか?	
i5/OS V5R3 を使用する場合、Cryptographic Access Provider (5722-AC3) が iSeries システムにインストール済みですか?	
i5/OS V5R4 を使用する場合、Network Authentication Enablement (5722-NAE) がシステムにインストール済みですか?	
iSeries Access for Windows (5722-XE1) が、管理者の PC およびご使用の iSeries システムにインストール済みですか?	
iSeries ナビゲーターのセキュリティー・サブコンポーネントは、管理者の PC にインストール済みですか?	
iSeries のネットワーク・サブコンポーネントは、管理者の PC にインストール済みですか?	
最新の IBM  server iSeries Access for Window サービス・パックはインストール済みですか? 最新のサービス・パックについては、iSeries Access Web ページ  を参照してください。	
*SECADM、*ALLOBJ、および *IOSYSCFG 特殊権限を持っていますか?	
以下のいずれかが機密保護機能のあるシステムにインストールされていて、Kerberos サーバーの役目をしますか? どれがインストールされていますか? 1. Windows 2000 サーバー 2. Windows Server 2003 3. AIX サーバー 4. i5/OS PASE (V5R3 以降) 5. zSeries	
Windows 2000 サーバーおよび Windows Server 2003 の場合、Windows Support Tools (これは ktpass ツールを提供する) が、鍵配布センターとして使用されているシステムにインストールされていますか?	
ご使用の Kerberos サーバーが Windows 2000 または 2003 サーバー上にある場合、ご使用のネットワーク内の PC がすべて、Windows ドメイン内に構成されていますか?	
最新のプログラム一時修正 (PTF) を適用していますか?	
iSeries のシステム時刻と、Kerberos サーバーのシステム時刻とのずれは 5 分以内ですか? 5 分以内でない場合は、101 ページの『システム時刻の同期化』を参照してください。	

表 22. Kerberos サーバーの計画ワークシート

質問	応答
<p>どのオペレーティング・システムに Kerberos サーバーを構成する予定ですか?</p> <ul style="list-style-type: none"> • Windows 2000 サーバー • Windows Server 2003 • AIX サーバー • i5/OS PASE (V5R3 以降) • zSeries 	
Kerberos サーバーの完全修飾ドメイン名は何ですか?	
PC と、Kerberos サーバーに接続するシステムとの間の時刻は同期していますか? 最大クロック・スキューは何秒ですか?	

表 23. Kerberos レルムの計画ワークシート

質問	応答
レルムはいくつ必要ですか?	
レルムはどのように編成する予定ですか?	
レルムにはどのような命名規則を使用しますか?	

表 24. プリンシパルの計画ワークシート

質問	応答
ネットワーク内のユーザーを表す Kerberos プリンシパル用に使用する予定の命名規則は何ですか?	
ネットワーク上のアプリケーションに使用する命名規則は何ですか?	
どの i5/OS サービスに Kerberos 認証を使用する予定ですか?	
これらの i5/OS サービスのそれぞれの i5/OS プリンシパル名は何ですか?	

表 25. ホスト名の解決に関する考慮事項のワークシート

質問	応答
ホスト名を解決するために、PC と iSeries が同じ DNS サーバーを使用していますか?	
ホスト名を解決するために、iSeries 上のローカル・ホスト・テーブルを使用していますか?	
ご使用の PC と iSeries サーバーは、iSeries サーバーの同じホスト名を解決しますか? 詳しくは、92 ページの『ホスト名の解決に関する考慮事項』を参照してください。	

以下の計画ワークシートは、i5/OS PASE およびネットワーク認証サービス内に Kerberos サーバーを構成する作業を始める前に必要なタイプの情報を示しています。前提条件ワークシートにある質問はすべて、i5/OS PASE に Kerberos サーバーを構成する作業を始める前に解答しておく必要があります。

表 26. i5/OS PASE 計画ワークシート

質問	応答
PASE はインストール済みですか?	
デフォルト・レルムの名前は何ですか?	
この Kerberos のデフォルト・レルムの Kerberos サーバーは何ですか? Kerberos サーバーが listen するポートは何ですか?	
ネットワーク内のユーザーを表すプリンシパルに使用する命名規則は何ですか?	
ネットワーク内のユーザーのプリンシパル名は何ですか?	

以下の計画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作業を始める前に必要な情報を収集します。前提条件ワークシートにある質問はすべて、ネットワーク認証サービスの構成作業を始める前に解答しておく必要があります。

表 27. ネットワーク認証サービスの計画ワークシート

質問	応答
ご使用の iSeries が属する Kerberos のデフォルト・レルムの名前は何ですか? 注: Windows 2000 ドメインは、Kerberos レルムに似ています。Microsoft Active Directory は、デフォルトのセキュリティ・メカニズムとして Kerberos 認証を使用します。	
Microsoft Active Directory を使用していますか?	
この Kerberos のデフォルト・レルムの Kerberos サーバーは何ですか? Kerberos サーバーが listen するポートは何ですか?	
このデフォルト・レルムにパスワード・サーバーを構成しますか? 「はい」の場合、次の質問に答えてください。 この Kerberos サーバーのパスワード・サーバーの名前は何ですか? パスワード・サーバーが listen するポートは何ですか?	
キータブ項目を作成する対象のサービスは? <ul style="list-style-type: none"> • i5/OS Kerberos 認証 • LDAP • iSeries IBM HTTP サーバー • iSeries NetServer 	
i5/OS Kerberos 認証のサービス・プリンシパルを作成する予定がある場合、そのパスワードは何ですか?	
LDAP のサービス・プリンシパルを作成する予定がある場合、そのパスワードは何ですか?	
HTTP Server のサービス・プリンシパルを作成する予定がある場合、そのパスワードは何ですか?	

表 27. ネットワーク認証サービスの計画ワークシート (続き)

質問	応答
<p>NetServer のサービス・プリンシパルを作成する予定がある場合、そのパスワードは何ですか?</p> <p>注: ネットワーク認証サービス・ウィザードの実行中に、iSeries NetServer 用に複数のプリンシパルが作成されます。これらのプリンシパルがウィザードに表示されるときに、ここに書き留めておいてください。これらのプリンシパルを Kerberos サーバーに追加するときに必要になります。</p>	
<p>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・ファイルを作成しますか?</p>	
<p>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?</p>	

システム時刻の同期化

ネットワークのシステム時刻を同期します。

ネットワーク認証サービスは、システム時刻の差の最大時間のデフォルト値として 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・プロパティの処理を実行することによって変更できます。

システム時刻を同期する前に、QTIMZON システム値を使用し、タイム・ゾーンにしたがってご使用のシステム時刻を設定します。これらのシステム時刻は、Kerberos サーバーに設定されている時刻を変更することによって同期させるか、あるいは、QTIME システム値を使用して、iSeries システム値を変更します。ただし、ネットワーク内のシステム時刻を同期させて保持するには、Simple Network Time Protocol (SNTP) を構成する必要があります。SNTP を使用すると、複数のシステムがその時刻の基礎を 1 つのタイム・サーバーに置くことができます。

SNTP を構成するには、以下のようにします。

- iSeries で SNTP を構成するには、コマンド行で CHGNTPA と入力します。
- Windows システムで 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。

Kerberos サーバーへの i5/OS プリンシパルの追加

i5/OS PASE または Windows 2000 ドメインで、Kerberos サーバーに、i5/OS プリンシパルを追加します。

ご使用の iSeries にネットワーク認証サービスを構成した後で、Kerberos サーバーに、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、サーバーおよび i5/OS アプリケーションの 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/iSeries host name@REALM NAME** で、ここで、*iSeries host name* は iSeries サーバーの完全修飾ホスト名または短縮ホスト名です。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・チケットを要求し受信できるように、Kerberos サーバーに追加する必要があります。たとえば、例で使用している構成シナリオでは、MyCo の管理者は、サービス・プリンシパル **krbsvr400/iseriasa.myco.com@MYCO.COM** を会社の Kerberos サーバーに追加しています。

Kerberos サーバーを構成したオペレーティング・システムに応じて、i5/OS プリンシパルを追加するステップが異なります。ここでは、i5/OS PASE または Windows 2000 ドメインで、Kerberos サーバーに、i5/OS プリンシパルを追加する方法について説明します。また、オプションで、IBM Directory Server for

iSeries (LDAP)、iSeries NetServer、または HTTP Server のサービス・プリンシパルを作成している場合は、作成したサービス・プリンシパルを Kerberos サーバーに追加する必要があります。

1. i5/OS PASE。 ご使用の 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できます。これによって、対話式シェル環境が開き、ユーザーは i5/OS PASE アプリケーションを処理できるようになります。i5/OS PASE 内で、Kerberos サーバーに、i5/OS サービス・プリンシパルを追加するには、以下のステップを実行します。
 - a. 文字ベースのインターフェースで、call QP2TERM と入力します。
 - b. コマンド行で、export PATH=\$PATH:/usr/krb5/sbin と入力します。このコマンドは、実行可能ファイルを実行するのに必要な Kerberos スクリプトを指します。
 - c. コマンド行で、kadmin -p admin/admin と入力します。
 - d. ユーザー名とパスワードを使用してログオンします。
 - e. kadmin コマンド行で、addprinc -pw secret krbsvr400/iSeries fully qualified host name@REALM と入力します。ここで、secret は、i5/OS サービス・プリンシパルのパスワードです。たとえば、krbsvr400/iseriasa.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 Windows 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、ネットワーク認証サービス・ウィザードに追加させる、または、ユーザーが手動で追加する、の 2 つの方法があります。ネットワーク認証サービス・ウィザードを使用すると、NASConfig.bat という名前のバッチ・ファイルを、オプションで作成できます。このバッチ・ファイルには、構成時にユーザーが選択したサービスのすべてのプリンシパル名が入っています。また、プリンシパル名の関連パスワードを、バッチ・ファイルに追加することを選択できます。

注: パスワードを組み込んだ場合は、バッチ・ファイルに対する読み取りアクセスを持っているユーザーはだれでもパスワードを表示することができます。したがって、パスワードを組み込んだ場合は、バッチ・ファイルを使用したらただちに、バッチ・ファイルを Kerberos サーバーおよび PC から削除することをお勧めします。バッチ・ファイルにパスワードを組み込んでいない場合は、バッチ・ファイルが Windows サーバーで実行されると、パスワードの入力を求めるプロンプトが表示されます。

ネットワーク認証サービス・ウィザードによって生成されたバッチ・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ために使用した Windows 2000 ワークステーションで FTP を使用するには、コマンド・プロンプトを開いて ftp server と入力します (server は Kerberos サーバーのホスト名)。これで、ご使用の PC で FTP セッションが開始されます。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表示されます。
- b. FTP プロンプトで、lcd "C:¥Documents and Settings¥All Users¥Documents¥IBM¥Client Access" と入力します。「機能開始」を押します。

注: これは、バッチ・ファイルを入れることができるディレクトリーの例です。

Local directory now C:¥Documents and Settings¥All Users¥Documents¥IBM¥Client Access のメッセージを受け取るはずです。

- c. FTP プロンプトで、binary と入力します。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 と入力します。ここで mydirectory は、バッチ・ファイルを入れる 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 と入力します。226 転送は完了のメッセージを受け取るはずです。
- f. ご使用の Windows 2000 サーバーで、バッチ・ファイルを転送したディレクトリーを開きます。
- 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. ファイルが実行されたら、以下のことを行って、i5/OS プリンシパル名が、Microsoft Windows Active Directory に追加されたことを確認します。

- 1) ご使用の Windows 2000 サーバーで、「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」と展開します。
- 2) 該当する Windows 2000 ドメインを選択して、iSeries 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で指定したデフォルトの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します。
- 4) 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、「アカウントは委任に対して信頼できる (Account is trusted for delegation)」を選択します。

注: このオプション・ステップによって、ご使用のシステムは、ユーザーの信任状を他のシステムに委譲あるいは転送することができます。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。これは多重層ネットワークでは便利です。

Microsoft Windows Active Directory へのサービス・プリンシパルの手動による追加 また、Microsoft Windows Active Directory への i5/OS プリンシパルの追加は、ktpass コマンドを使用して手動で行うこともできます。このコマンドは、Windows のサポート・ツールと一緒に配送され、Kerberos サーバーとして使用されるシステムにインストールする必要があります。

- a. ご使用の Windows 2000 サーバーで、「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」と展開します。
- b. iSeries ユーザー・アカウントを追加する Windows 2000 ドメインを選択し、次に「アクション」 → 「新規」 → 「ユーザー」と展開します。

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の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 iSeries を識別させる名前を入力します。これによって、iSeries の新規ユーザー・アカウントが追加されます。たとえば、正当なユーザー・アカウント名として、krbsvr400iseriesa または httpiseriesa という名前を入力できます。
- 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できる (Account is trusted for delegation)」を選択します。これによって、i5/OS サービス・プリンシパルが、サインインしたユーザーに代わって他のサービスを使用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 コマンドを使用して、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「保守ツール」フォルダーで提供されています。ユーザー・アカウントをマップするには、以下の作業を実行します。

- 1) コマンド・プロンプトで、次のコマンドを入力します。

```
ktpass -mapuser krbsvr400iseriesa -pass secret -princ krbsvr400/iseriesa-domain-name@REALM -mapop set
```

注: このコマンドで、krbsvr400iseriesa は、ステップ 3 で作成されたユーザー・アカウント名を表し、また、secret は、i5/OS プリンシパルのネットワーク認証サービスの構成時にユーザーが入力したパスワードを表します。

EIM (エンタープライズ識別マッピング) (i5/OS 用) の計画

EIM (エンタープライズ識別マッピング) は、iSeries サーバー上で、複数のテクノロジーとサービスを提供できます。ご使用のサーバーで EIM を構成する前に、EIM およびシングル・サインオン機能を使用してインプリメントする機能を決定しておく必要があります。

EIM を実施する前に、ご使用のネットワークの基本的なセキュリティー要件を決め、そのセキュリティー手段をインプリメントしておく必要があります。EIM では、エンタープライズ全体に対して使用できる、使いやすい識別管理手段を管理者およびユーザーに提供します。EIM は、ネットワーク認証サービスと一緒に使用すると、エンタープライズ全体にシングル・サインオン機能を提供します。

シングル・サインオンのインプリメンテーションの一環として Kerberos を使用してユーザーを認証する予定がある場合は、ネットワーク認証サービスも構成する必要があります。ネットワーク認証サービスの計画については『ネットワーク認証サービスの計画』、および、シングル・サインオン環境の計画については『シングル・サインオンの計画』を参照してください。

さらに、ご使用の iSeries の EIM 構成の計画方法については、以下の説明を検討してください。

シングル・サインオン計画ワークシート

これらのワークシートを使用して、シングル・サインオンの前提条件をすべて満たしていること、および特定のシステムとそのセキュリティー要件のあらゆる面を検討済みであることを確認してください。

下記の構成計画ワークシートを使用する前に、全体的なシングル・サインオン実現を計画しておく必要があります。次の構成計画ワークシートを使用して、すべての前提条件が満たされていること、および特定の iSeries システムのあらゆる特徴を考慮に入れていることを確認してください。


シングル・サインオン前提条件ワークシート

この詳しいワークシートは、シングル・サインオンを実現するためのハードウェアとソフトウェアのあらゆる前提条件を満たしていることを確認するためのものです。正常なインプリメンテーションを確保するには、構成作業を行う前に、ワークシートのすべての前提条件項目に「はい」で応答でき、かつワークシートの記入に必要なすべての情報を収集している必要があります。

表 28. 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	応答
i5/OS は V5R4 (5722-SS1) ですか?	
以下のオプションおよびライセンス製品がサーバーにインストール済みですか? • i5/OS Host Servers (5722-SS1 オプション 12) • Qshell Interpreter (5722-SS1 オプション 30) • iSeries Access for Windows (5722-XE1)	
シングル・サインオン環境に参加する各 PC に、シングル・サインオンが使用可能になっているアプリケーションがインストール済みですか? 注: この情報のシナリオの場合、すべての PC に iSeries Access for Windows (5722-XE1) がインストールされています。	

表 28. シングル・サインオン前提条件ワークシート (続き)

管理者の PC に iSeries ナビゲーター はインストール済みですか? • 管理者の PC に iSeries 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 iSeries 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 iSeries Access for Windows サービス・パックをインストール済みですか? 最新のサービス・パックについては、iSeries Access  を参照してください。	
管理者は *SECADM、*ALLOBJ、および *IOSYSCFG 特殊権限を持っていますか?	
Kerberos サーバー (KDC としても知られる) として働く、以下のいずれかのシステムを持っていますか? 持っている場合は、そのシステムを指定してください。 1. Windows 2000 サーバー 注: Microsoft Windows 2000 は、デフォルトのセキュリティー・メカニズムとして Kerberos 認証を使用します。 2. Windows ^(R) サーバー 2003 3. i5/OS PASE (V5R3 以降) 4. AIX サーバー 5. zSeries	
ネットワーク内の PC はすべて、Windows 2000 ドメイン内で構成されていますか?	
最新のプログラム一時修正 (PTF) を適用していますか?	
iSeries 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? 5 分以内でない場合は、『システム時刻を同期する』を参照してください。	

シングル・サインオン構成計画ワークシート

この構成計画ワークシートは、シングル・サインオン用のハードウェアとソフトウェアの前提条件をすべて満たしていることを確認するためのものです。また、このワークシートは、正常なシングル・サインオン環境の作成に必要な EIM (エンタープライズ識別マッピング) およびネットワーク認証サービスの構成タスクを完了していることも確認します。

注: シングル・サインオン構成計画ワークシートは、EIM (エンタープライズ識別マッピング) とネットワーク認証サービスに基づくシングル・サインオン環境の実現に役立てるためのものです。IBM Directory Server for iSeries (LDAP) やデジタル証明書などの別の認証メカニズムを使用したい場合は、ニーズに合わせてこのワークシートの一部の変更が必要になる場合があります。

表 29. シングル・サインオン構成計画ワークシート

構成計画ワークシート	応答
次の情報は、EIM 構成ウィザードを完了する場合に使用します。	
ご使用システムにどのように EIM を構成しますか? • 既存のドメインを結合する • 新規ドメインを作成して結合する	

表 29. シングル・サインオン構成計画ワークシート (続き)

ご使用の EIM ドメインを構成する必要がある場所は?	
ネットワーク認証サービスを構成しますか?	
<p>EIM 構成ウィザードから、ネットワーク認証サービス・ウィザードが起動します。次の情報は、ネットワーク認証サービス・ウィザードを完了する場合に使用します。</p> <p>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起動することもできます。</p>	
ご使用の iSeries 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 レルムに類似しています。Microsoft Windows Active Directory は、デフォルトのセキュリティー・メカニズムとして Kerberos 認証を使用します。	
Microsoft Active Directory を使用していますか?	
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) と呼ばれます) は何ですか? Kerberos サーバーが listen するポートは何ですか?	
このデフォルト・レルムにパスワード・サーバーを構成しますか? 「はい」の場合、 この Kerberos サーバーのパスワード・サーバーの名前は何か? パスワード・サーバーが listen するポートは何ですか?	
キータブ項目を作成する対象のサービスは? <ul style="list-style-type: none"> • i5/OS Kerberos 認証 • LDAP • IBM HTTP Server for i5/OS • iSeries NetServer 	
ご使用のサービス・プリンシパルのパスワードは何ですか?	
バッチ・ファイルを作成して、iSeries 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?	
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?	
<p>ネットワーク認証サービス・ウィザードを終了すると、EIM 構成ウィザードへ戻ります。次の情報は、EIM 構成ウィザードを完了する場合に使用します。</p>	
ウィザードがディレクトリー・サーバーを構成する際に使用する必要がある、ユーザー情報を指定します。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。	
作成する EIM ドメインの名前は何か?	
EIM ドメインの親 DN を指定しますか?	
どのユーザー・レジストリーを EIM ドメインに追加しますか?	
EIM 操作を行うときに、どの EIM ユーザーを iSeries A に使用させますか? これはシステム・ユーザーです。	
<p>EIM 構成ウィザードが完了したら、次の情報を使用して、シングル・サインオンの構成に必要な残りのステップを完了してください。</p>	
ユーザーの i5/OS ユーザー・プロファイル名は何ですか?	
作成する EIM ID の名前は何か?	

表 29. シングル・サインオン構成計画ワークシート (続き)

どんな種類のアソシエーションを作成しますか?	
ソース・アソシエーションを作成する Kerberos プリンシパルを含むユーザー・レジストリーの名前は何かですか?	
ターゲット・アソシエーションを作成する i5/OS ユーザー・プロフィールを含むユーザー・レジストリーの名前は何かですか?	
EIM ID のマッピングをテストするのに、どんな情報を提供する必要がありますか?	

構成

ここでは、個々の企業でシングル・サインオン環境をインプリメントするのに必要なすべての構成方法を説明します。

シングル・サインオン環境の作成とは、EIM (エンタープライズ識別マッピング) および互換性のある認証方式と一緒に機能するように適切に構成することです。その結果、組み合わせた構成が真のシングル・サインオン環境を提供します。i5/OS シングル・サインオン・ソリューションの場合、認証方式はネットワーク認証サービス (Kerberos) です。

シングル・サインオン環境の構成は複雑になる場合があるので、企業全体でシングル・サインオンを実現する前に、テスト環境を作成すると便利です。『シナリオ: シングル・サインオンのテスト環境を作成する』では、このようなテスト環境の構成方法をわかりやすく説明しているため、シングル・サインオンを実現する計画ニーズの詳細を理解するだけでなく、シングル・サインオン環境の働きも理解することができます。

テスト環境を使用した後、テストの結果を使用して、社内でより大規模にシングル・サインオンを実現する方法を計画することができます。シングル・サインオン環境の実現時に使用できる拡張構成オプションを理解するには、『シナリオ:i5/OS のシングル・サインオンを使用できるようにする』が役立ちます。

上記のシナリオやその他のシングル・サインオン・シナリオを検討した後、シングル・サインオン計画ワークシートを使用して、自社のニーズに合う確実なシングル・サインオン実現計画を作成することができます。こうした計画ワークシートが用意できたので、構成プロセスに進む準備ができました。

この情報は、認証方式としてネットワーク認証サービスを使用し、ユーザー・プロフィールと ID マッピングの作成と管理に EIM を使用して、シングル・サインオン環境を構成するのに役立ちます。シングル・サインオンには複数の詳細な構成手順が含まれているので、この情報は、シングル・サインオンのハイレベルな構成タスクについて説明し、該当する場合、EIM とネットワーク認証サービスの両方について、もっと詳しい構成情報へのリンクを提供します。

シングル・サインオン環境を構成するには、次のタスクを実行します。

1. Windows 2000 ドメインを作成します。

- a. Active Directory (AD) サーバー上で KDC を構成する。

注: Windows ドメインを作成し、Windows サーバー上で KDC を実行するのではなく、i5/OS PASE で KDC を作成し、実行することを選択できます。

- b. i5/OS サービス・プリンシパルを Kerberos サーバーに追加する。
- c. シングル・サインオン環境に加わる Kerberos ユーザーごとに、ホーム・ディレクトリーを作成する。

- d. TCP/IP ドメイン情報を検証する。
2. サーバー上でネットワーク認証サービス・ウィザードと EIM 構成ウィザードの両方を実行して、EIM ドメインを作成します。これらのウィザードを実行したら、実際に次のタスクを完了したことになります。
 - a. Kerberos チケットを受け入れるように i5/OS インターフェースを構成する。
 - b. EIM ドメイン・コントローラーになるように、iSeries 上でディレクトリー・サーバーを構成する。
 - c. EIM ドメインを作成する。
 - d. i5/OS と i5/OS アプリケーションが EIM 操作の実行時に使用するユーザー ID を構成する。
 - e. ローカル i5/OS レジストリーとローカル Kerberos レジストリー (Kerberos が構成されている場合) のレジストリー定義を EIM に追加する。
3. i5/OS V5R3 以降を実行するサーバーの場合、iSeries ナビゲーター の機能同期化ウィザードを使用して、混合 i5/OS リリース環境で複数のサーバーにシングル・サインオン構成を反映させる方法の詳細なデモンストレーションについては、『シナリオ: ネットワーク認証サービスおよび EIM を複数システムに反映させる』を参照してください。管理者は、各システムを個々に構成するのではなく、シングル・サインオンを一度構成すると、その構成をすべてのシステムに反映させることで、時間を節約できます。
4. ネットワーク認証サービスの構成を終了します。シングル・サインオン実現計画に基づいて、サーバー上のユーザーのホーム・ディレクトリーを作成する。
5. 実現計画に基づいて、社内のユーザー ID のアソシエーションをセットアップして、EIM 環境をカスタマイズします。iSeries Information Center で、EIM 環境をカスタマイズする方法を確認してください。
 - a. EIM ドメインに加わるように他のサーバーを構成する。
 - b. 必要に応じて、EIM ID と ID アソシエーションを作成する。
 - c. 必要に応じて、レジストリー定義を追加する。
 - d. 必要に応じて、ポリシー・アソシエーションを作成する。
6. シングル・サインオン構成をテストします。

ネットワーク認証サービスと EIM を正しく構成していることを確認するには、ユーザー ID を使用してシステムにサインオンしてから、iSeries ナビゲーター を開きます。i5/OS サインオン・プロンプトが表示されない場合、EIM は Kerberos プリンシパルと、ドメイン上の ID とのマッピングに成功しました。

注: シングル・サインオン構成のテストが失敗した場合、構成に問題がある可能性があります。シングル・サインオンのトラブルシューティングを行い、シングル・サインオン構成でよくある問題を認識し、修正する方法が分かります。

管理

この情報は、ネットワーク認証サービスおよび EIM の管理タスクなど、シングル・サインオン環境を管理する場合に使用してください。

シングル・サインオン環境を実現した後、ネットワークの他の特徴の場合と同じように、セキュリティー・ポリシーにしたがってその環境を保持するために、各種管理タスクの実行が必要な場合があります。シングル・サインオン環境を管理するには、シングル・サインオン環境を作成するために構成した機能 (EIM (エンタープライズ識別マッピング) とネットワーク認証サービス) を管理します。

これらの機能を管理してシングル・サインオン環境を保持する詳しい方法については、次のものを参照してください。

- ネットワーク認証サービスの管理

システム時刻の同期化、レルムの追加と削除、Kerberos サーバーの追加などの、一般的なネットワーク認証サービスの管理タスクについて確認してください。

- EIM の管理

アソシエーション、ID、レジストリー定義の管理方法などの、一般的な EIM 管理タスクについて確認してください。

シングル・サインオン環境に問題がある場合、シングル・サインオンのトラブルシューティングを行うことができます。

トラブルシューティング

この情報は、シングル・サインオン環境の構成および使用の際に発生することがあるいくつかの共通エラーを解決する場合に使用してください。

i5/OS シングル・サインオン構成の問題を回避するために実行可能なアクションは、次のとおりです。

1. qshell kinit コマンドを実行すると、ネットワーク認証サービスの構成が正しいかどうかを確認できます。これを確認するには、qshell 環境に入り、`kinit -k <service name>` コマンドを実行します。このコマンドは、ネットワーク認証サービス・ウィザードで作成したキータブ項目を使用します。このコマンドは、このサービスの暗号化パスワードが、KDC に保管されているのと同じパスワードであるかどうかを確認します。このコマンドが正常に実行されない場合、『ネットワーク認証サービスの構成』を参照してください。
2. DNS サーバーを含めて、ホスト名解決の構成を検証します。
3. 次の手順で、マッピング探索操作を実行する各 i5/OS システム上で EIM システム構成情報を検証します。
 - a. iSeries ナビゲーター を使用して、システムにサインオンする。
 - b. システムを選択し、「ネットワーク」 → 「エンタープライズ識別マッピング」 → 「構成」と展開する。
 - c. 「構成」フォルダーを右マウス・ボタンでクリックし、「プロパティ」を選択する。
 - d. 「ドメイン」ページで、ドメイン接続の設定値を検証し、「構成の検査 (Verify Configuration)」をクリックする。これは、ドメイン・コントローラーがアクティブであること、およびドメイン・コントローラーの設定が正しいことを確認します。
 - e. 「システム・ユーザー」ページで、「接続の検査 (Verify Connection)」をクリックして、システム・ユーザーが正しく指定されていることを確認する。
4. EIM マッピングのテスト機能を使用して、定義された EIM アソシエーションを検証し、定義したアソシエーションが予想どおりのマッピングを行うことを確認します。
5. シングル・サインオン構成に複数層ネットワークが含まれている場合、中間層のサーバーのチケット代行が使用可能になっていることを確認します。これは、中間層のサーバーがユーザー信任状を次のサーバーに転送するのに必要です。チケット代行は、Active Directory または Kerberos サーバーで使用可能にすることができます。複数層ネットワークの一例は、1 つのサーバーで認証されてから、別のサーバーに接続する PC です。

上記のステップを検討したあとでもまだシングル・サインオンに問題がある場合は、次の表を使用して、構成の問題の症状に対する解決法を判別してください。

症状	考えられる解決方法
ホスト名解決の問題	
<p>シングル・サインオン環境内の i5/OS システムに接続できない。</p>	<ul style="list-style-type: none"> • この原因は、ホスト解決の問題である可能性があります。PC と iSeries が同じホスト名に解決されることを確認してください。DNS サーバーを含めて、ホスト名解決の構成を確認してください。 • この原因は、NAS 構成の問題である可能性があります。iSeries Information Center 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』を参照してください。
<p>iSeries システムとクライアント PC 間でホスト解決が一致していることを確認しようとするときに、IP アドレスを指定すると、NSLOOKUP ユーティリティがホスト名を解決できない。</p>	<p>NSLOOKUP ユーティリティは、現在構成されている DNS を使用して、ホスト名から IP アドレスを解決すると共に、IP アドレスからホスト名を解決します。IP アドレスからホスト名を解決できない場合、おそらく原因は、DNS に PTR レコードがないことです。この IP アドレスの PTR レコードを追加するように、DNS 管理者に依頼してください。</p>
EIM 構成の問題	

症状	考えられる解決方法
<p>EIM マッピングが予想どおりに機能しない。 Kerberos 認証の使用時に、iSeries ナビゲーター にサインインできない場合がある。</p>	<ul style="list-style-type: none"> • ドメイン・コントローラーが非アクティブです。ドメイン・コントローラーをアクティブにしてください。 • Kerberos 認証を使用するか、マッピングを取得しようとするシステム (単数または複数) で、EIM 構成に誤りがあります。EIM 構成を検証してください。認証に使用するシステムで、「ネットワーク」→「エンタープライズ識別マッピング」→「構成」と展開します。「構成」フォルダーを右マウス・ボタンでクリックし、「プロパティ」を選択して、次の項目を確認してください。 <ul style="list-style-type: none"> - 「ドメイン」 ページ <ul style="list-style-type: none"> - ドメイン・コントローラーの名前とポート番号が正しい。 - 「構成の検査 (Verify Configuration)」をクリックして、ドメイン・コントローラーがアクティブであることを確認する。 - ローカル・レジストリー名が正しく指定されている。 - Kerberos レジストリー名が正しく指定されている。 - 「このシステムの EIM 操作を使用可能にする (Enable EIM operations for this system)」が選択されていることを確認する。 - 「システム・ユーザー」 ページ <ul style="list-style-type: none"> - 指定されたユーザーには、マッピング検索を実行できる EIM アクセス制御権があり、パスワードがそのユーザーに有効である。さまざまなタイプのユーザー・信任状の詳細については、オンライン・ヘルプを参照してください。 注: ディレクトリー・サーバーでパスワードが更新されるたびに、システム構成でも更新されなければなりません。 - 「接続の検査 (Verify Connection)」をクリックして、指定されたユーザー情報が正しいことを確認する。 • EIM ドメイン構成に、次のような誤りがあります。 注: EIM マッピングをテストすると、EIM ドメインのアソシエーションが正しく構成されているかどうかを確認できます。 <ul style="list-style-type: none"> - EIM ID のターゲット・アソシエーションまたはソース・アソシエーションが正しくセットアップされていない。たとえば、Kerberos プリンシパル (または Windows ユーザー) のソース・アソシエーションがないか、正しくありません。もしくは、ターゲット・アソシエーションが誤ったユーザー ID を指定しています。EIM ID の ID アソシエーションをすべて表示して、特定の ID アソシエーションを検証してください。 - ポリシー・アソシエーションが正しくセットアップされていない。ドメインのすべてのポリシー・アソシエーションを表示して、ドメイン内で定義されているすべてのポリシー・アソシエーションのソース情報とターゲット情報を検証してください。 - マッピング探索が複数のターゲット ID を戻し、構成されているマッピングがあいまいであることを示す。EIM マッピングをテストして、誤りのあるマッピングを特定してください。 - 大文字小文字の区別があるので、レジストリー定義とユーザー ID が一致しない。レジストリーをいったん削除して再作成するか、またはアソシエーションをいったん削除して、大文字小文字を正しく区別するアソシエーションを再作成することができます。 • EIM サポートが使用可能になっていません。 <ul style="list-style-type: none"> - システムの EIM が使用不可になっている。「ドメイン」 ページで、システム EIM 構成プロパティに対して「このシステムの EIM 操作を使用可能にする (Enable EIM operations for this system)」が選択されていることを確認してください (「ネットワーク」→「エンタープライズ識別マッピング」→「構成フォルダー (Configuration folder)」→「プロパティ」) と展開します)。 - ポリシー・アソシエーション・サポートが、ドメイン・レベルで使用可能になっていない。ドメインに対してポリシー・アソシエーションを使用可能にする必要があります。 - マッピング探索サポートまたはポリシー・アソシエーション・サポートが、個々のレジストリー・レベルで使用可能になっていない。ターゲット・レジストリーに対してマッピング探索サポートおよびポリシー・アソシエーションの使用を可能にする必要があります。
	<p>ネットワーク認証サービス構成の問題</p>

症状	考えられる解決方法
keytab list の実行時に、keytab entry が検出されない。	<ul style="list-style-type: none"> この原因は、iSeries システム上のホスト解決の問題である可能性があります。ホスト・テーブルを使用する場合は、CFGTCP コマンド、オプション 10 を実行し、サーバーの IP アドレスについて、1 次ホスト名が先頭にリストされていることを確認してください。 DNS サーバーを含めて、ホスト名解決の構成を確認してください。
ユーザーがシステムに接続できない。	<p>Kerberos レジストリーの EIM レジストリー定義で、大文字小文字の区別が誤って指定されている場合、ユーザーはシステムに接続できない場合があります。その Kerberos レジストリーをいったん削除して、再作成してください。</p> <p>注: そのレジストリーに対して定義されているアソシエーションがすべて失われるので、それらを再作成する必要があります。</p>
ネットワーク認証サービス構成の検証時に、パスワードの誤りを指摘するメッセージをユーザーが受け取る。	<p>KDC のサービス用のパスワードが、キータブのサービス用のパスワードと一致しません。</p> <p>keytab add コマンドを使用してキータブ項目を更新し、KDC 上のサービス用のパスワードを更新してください。</p>
ユーザーが「デフォルトの証明書キャッシュの名前を取得できません」というメッセージを受け取る。	<p>kinit を実行するユーザー用に、ホーム・ディレクトリー (/home/<user profile>) が存在することを確認してください。</p>
ユーザーが「データグラムには大きすぎる応答です」というメッセージを受け取る。	<p>次の手順を使用して、データ通信プロトコルとして TCP を使用するよう、ネットワーク認証サービスの構成を更新してください。</p> <ol style="list-style-type: none"> iSeries ナビゲーター を使用して、そのメッセージを発行したシステムを選択する。 「セキュリティ」 → 「ネットワーク認証サービスのプロパティ」の順に選択する。 「一般」ページで、「TCP を使用する」を選択し、「OK」をクリックする。
一般的な問題	
シングル・サインオンの試行時に、エラー・メッセージ CWBSY10XX が表示される。	<ul style="list-style-type: none"> そのメッセージ本文に関連したヘルプを使用して、問題を解決してください。 iSeries Access 詳細トレース機能を使用して、該当する Kerberos チケットが検索されるかどうかを判別してください。 Microsoft kerbtray ユーティリティーをダウンロードして、ユーザーに Kerberos 信任状があることを確認してください。 iSeries ナビゲーター のシングル・サインオンが失敗する場合、QUSRWRK サブシステムの QZSOSIGN ジョブを調べてください。それらのジョブを調べて、CPD3E3F メッセージを見つけます。CPD3E3F メッセージを検出した場合、そのメッセージ内に表示されるリカバリー情報を使用してください。問題が起きた場所を示すために、診断メッセージには、メジャーとマイナーの両方の状況コードが含まれます。メッセージには、リカバリー方法と一緒に、最も一般的なエラーが記述されています。 PC5250 が失敗する場合は、次の検査を行ってください。 <ul style="list-style-type: none"> CPD3E3F メッセージがあるかどうか、QTVDEVICE ジョブを調べる。 QRMTSIGN システム値を調べ、*VERIFY または *SAMEPRF に設定されていることを確認する。

関連情報

ネットワーク認証サービスのトラブルシューティング

DNS デバッグのツール

EIM のトラブルシューティング

関連情報

この情報は、シングル・サインオン・ソリューションとその基本テクノロジーをサポートする情報にアクセスするとき使用してください。

シングル・サインオン、EIM (エンタープライズ識別マッピング)、ネットワーク認証サービス、IBM Directory Server、デジタル証明書マネージャー、およびその他の関連情報について学習するために他のリソースへのリンクを検索するには、このページを表示してください。シングル・サインオンの使用が増えるにしたがい、多くの情報源が使用可能になっています。

デジタル証明書、およびデジタル証明書を使用して iSeries™ のセキュリティー・ポリシーの強化方法について確認するために検討できる主要な情報源を以下にリストします。

- EIM (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) は、個人またはエンティティ (サービスなど) を、企業全体のさまざまなユーザー・レジストリー内の該当するユーザー ID にマップするメカニズムです。iSeries システムは EIM を使用して i5/OS インターフェースを使用可能にし、ユーザー認証サービスを使用してユーザーを認証します。また、iSeries およびアプリケーションは Kerberos チケットを受け入れ、EIM を使用して、Kerberos プリンシパルに関連付けられているユーザー ID を、このシステム上で検出することもできます。

- ネットワーク認証サービス

このトピックでは、iSeries 上でのネットワーク認証サービスの構成について説明します。ネットワーク認証サービスによって、iSeries システムが、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、EIM と一緒に使用すると、ネットワークのシングル・サインオンを提供します。

- IBM Directory Server for iSeries (LDAP)

このトピックは、ディレクトリー・サービスとも呼ばれる LDAP の構成と概念の情報を提供します。EIM は LDAP サーバーを使用して、EIM データとマッピングのアソシエーションを保管し、管理します。

- デジタル証明書マネージャー

このトピックは、デジタル証明書、および拡張ネットワーク・セキュリティー手段を提供するためにデジタル証明書の使用が増えていることについて説明します。

コードに関するライセンス情報および特記事項

IBM は、お客様に、すべてのプログラム・コードのサンプルを使用することができる非独占的な著作使用権を許諾します。お客様は、このサンプル・コードから、お客様独自の特別のニーズに合わせた類似のプログラムを作成することができます。

1 強行法規で除外を禁止されている場合を除き、IBM、そのプログラム開発者、および供給者は、「プログラム」および「プログラム」に対する技術的サポートがある場合にはその技術的サポートについて、第三者の権利の不侵害の保証、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。

1 IBM、そのプログラム開発者、または供給者は、いかなる場合においてもその予見の有無を問わず、以下に対する責任を負いません。

- 1 1. データの喪失、または損傷。
- 1 2. 特別損害、付随的損害、間接損害、または経済上の結果的損害
- 1 3. 逸失した利益、ビジネス上の収益、あるいは節約すべかりし費用

1 国または地域によっては、法律の強行規定により、上記の責任の制限が適用されない場合があります。

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。

〒106-0032
東京都港区六本木 3-2-31
IBM World Trade Asia Corporation
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。

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。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

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。

- | 強行法規で除外を禁止されている場合を除き、IBM、そのプログラム開発者および提供者は、「プログラ
- | ム」および「プログラム」に対する技術的サポートがある場合にはその技術的サポートについて、第三者の
- | 権利の不侵害の保証、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。

- | IBM、そのプログラム開発者、または供給者は、いかなる場合においてもその予見を問わず、以下に対する
- | 責任を負いません。

- | 1. データの喪失、または損傷
- | 2. 特別損害、付随的損害、間接損害、または経済上の結果的損害
- | 3. 逸失した利益、ビジネス上の収益、あるいは節約すべかりし費用

- | 国または地域によっては、法律の強行規定により、上記の責任の制限が適用されない場合があります。

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

本書「シングル・サインオン」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
- | Distributed Relational Database Architecture
- | DRDA
- | NetServer
- | OS/400
- | WebSphere
- | WordPro
- | i5/OS
- | IBM
- | iSeries
- | zSeries

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。

Java およびすべての Java 関連の商標およびロゴは、Sun Microsystems, Inc. の米国およびその他の国における商標または登録商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

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。この資料は、特定物として現存するままの状態を提供され、第三者の権利の不侵害の保証、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ています。



Printed in Japan