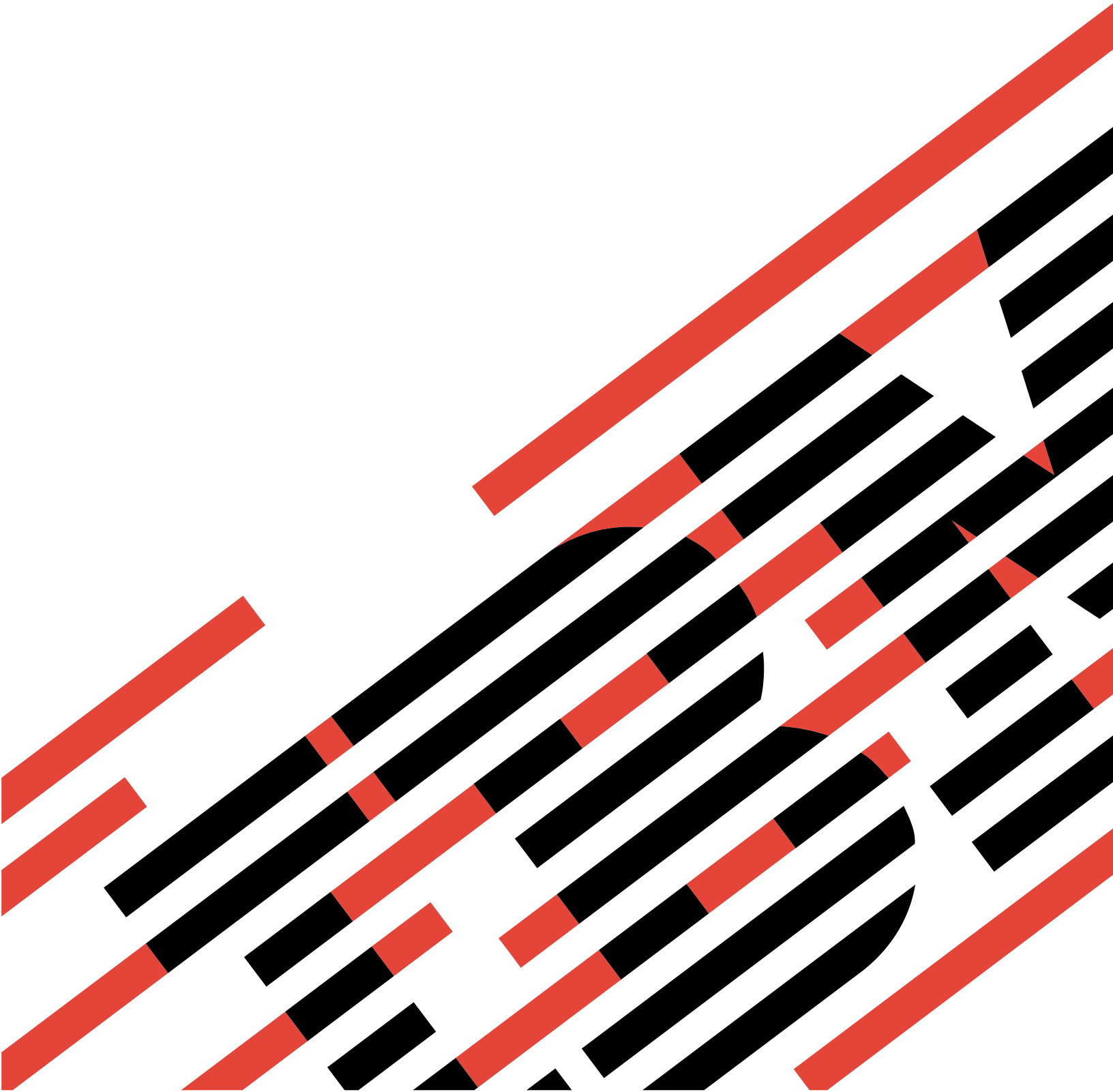
IBM

eserver

iSeries

網路鑑別服務



IBM

@server

iSeries

網路鑑別服務

目錄

網路鑑別服務

網路鑑別服務允許 iSeries 及若干 iSeries 服務程式 (如 iSeries Access for Windows) 使用 Kerberos 通行證作爲鑑別使用者的另一種選擇，取代使用者名稱和密碼。 Kerberos 通信協定是由 Massachusetts Institute of Technology 所開發，它允許主體 (使用者或服務程式) 向不安全網路內另一個服務程式證明其身份。主體的鑑別是透過一個稱爲「金鑰分送中心 (KDC)」的中央伺服器來完成。 KDC 使用 Kerberos 通行證來鑑別使用者。這些通行證可向網路內其它服務程式證明主體的身份。這些通行證鑑別主體之後，它們可與目標服務程式交換加密資料。網路鑑別服務可驗證網路內使用者或服務程式的身份。應用程式可安全地鑑別使用者並將其身份安全地遞送給網路上其它服務程式。一旦識別了使用者，則需要個別的功能來驗證使用者使用網路資源的授權。網路鑑別服務實作下列規格：

- Kerberos 版本 5 通信協定 Request for Comment (RFC) 1510
- 現行產業中普遍使用的許多實際標準 Kerberos 通信協定 API
- 由 RFC 1509、1964 及 2743 所定義的同屬安全服務 (GSS) API

iSeries 上的網路鑑別服務與遵循這些 RFC 的鑑別、代表及資料機密性服務交互作用，例如 Microsoft Windows 2000 安全服務提供者介面 (SSPI) API。

此外，網路鑑別服務可搭配使用「企業識別對映 (EIM)」來啓用單一登入環境。單一登入有益於使用者、管理者及應用程式開發者在多重平台之間啓用便利密碼管理系統，而不需要變更基本安全原則。下列文章提供有關使用網路鑑別服務及「企業識別對映 (EIM)」啓用單一登入的詳細資料：

啓用單一登入
本文章提供有關單一登入優點的概念資訊，以及如何共同使用網路鑑別服務和「企業識別對映 (EIM)」來建立單一登入環境的概觀。

實務範例：啓用單一登入
本文提供 MyCo 的「訂單接收部門」管理者如何啓用單一登入環境的範例。管理者想要利用使用者的 Windows (R) 網域 ID 及密碼來對 iSeries 應用程式鑑別使用者。併入了一些逐步指示來顯示 MyCo 管理者如何配置網路鑑別服務和 EIM 來啓用單一登入。

網路鑑別服務的討論包括下列主題：

V5R2 的新增功能
此主題說明並鏈結至有關本版次網路鑑別服務新功能的詳細資訊。

列印此主題
此主題提供下載及列印此資訊 PDF 版本的指示。

網路鑑別服務如何運作？
此主題提供有關如何在使用 Kerberos 通信協定來鑑別使用者的網路內使用網路鑑別服務的概觀。

網路鑑別服務術語
此主題定義與網路鑑別服務相關的術語。

網路鑑別服務通信協定
此主題提供 Kerberos 通信協定及「同屬安全服務 (GSS)」API 的基本討論。有提供對 RFC 及其它相關資訊的鏈結。

網路鑑別服務實務範例
此主題說明一些實作網路鑑別服務的不同商務實務範例。

規劃網路鑑別服務
此主題說明使用網路鑑別服務的前置作業。

配置網路鑑別服務
此主題說明如何在「iSeries 領航員」中配置網路鑑別服務。

管理網路鑑別服務
此主題說明管理者及使用者可用來管理網路鑑別服務的一些作業。

網路鑑別服務疑難排解
此主題說明網路鑑別服務及相關應用程式的訊息和問題解決方案。

相關資訊
此主題說明並提供與 Kerberos 通信協定及「同屬安全服務 (GSS)」API 相關的其它主題鏈結。

法律資訊
此主題提供與使用 Kerberos 通信協定及其相關 API 有關的重要法律資訊。

V5R2 的新增功能

網路鑑別服務可讓 iSeries 加入網路中，使用 Kerberos 通信協定來鑑別網路使用者。

「iSeries 領航員」中的網路鑑別服務
網路鑑別服務精靈提供 iSeries 加入 Kerberos 網路的簡易配置。此精靈可讓您配置 iSeries 來加入 Kerberos 領域。藉由使用 Kerberos 通信協定，可傳遞代表使用者的通行證給服務，讓網路資源能鑑別別。 請參閱下列這些主題來完成配置：

- 網路鑑別服務實務範例
  提供使用網路鑑別服務的兩個客戶狀況之簡要說明。
-
- 配置網路鑑別服務
  提供配置網路鑑別服務所需全部步驟的概觀。
-

- 管理網路鑑別服務
  提供可使用「iSeries 領航員」來完成的全部作業概觀。

支援新的 Qshell 指令

使用者可利用 Qshell 指令來要求及使用通行證。於此版次中，新增了 **kpasswd** 指令供使用者在金鑰分送中心上變更密碼。

- 變更 Kerberos 密碼
  提供如何使用 kpasswd Qshell 指令的資訊。

企業識別對映 (EIM)

EIM 是一種機制，可將某人或實體 (如服務) 對映到整個企業內不同使用者登錄中的適當使用者身份。當搭配網路鑑別服務使用時，EIM 可啓用單一登入環境。iSeries 使用 EIM 來啓用 OS/400 介面，透過網路鑑別服務來鑑別使用者。iSeries 及應用程式也可接受 Kerberos 通行證，使用 EIM 來將一個系統上的某個使用者 ID 對映到該系統相關的 Kerberos 主體。

- 啓用單一登入
  提供單一登入優點的概念資訊，以及如何共同使用網路鑑別服務和 EIM 來建立單一登入環境的概觀。
- 實務範例：啓用單一登入
  提供共同使用網路鑑別服務及 EIM 來啓用單一登入環境的詳細範例。

數個 iSeries 應用程式的鑑別支援：

- **結構化查詢語言 (SQL)/分散式關連資料庫架構 (DRDA)**
  SQL/DRDA 現在支援使用 Kerberos 通行證來鑑別存取資料庫功能的使用者。DRDA 檢查指定使用者的通行證授予通行證。若通行證存在，則使用該通行證來取得使用者的服務通行證。
-
- **分散式資料管理 (DDM)**
  DDM 現在支援使用 Kerberos 通行證來鑑別存取遠端檔案的使用者。DDM 檢查指定使用者的通行證授予通行證。若通行證存在，則使用該通行證來取得使用者的服務通行證。**註**：若您有指定於 Kerberos 配置檔中的預設領域，但未使用 Kerberos 作爲您的鑑別方法，則在對 DDM 設定鑑別之前，您必須移除預設領域。有關如何從此問題恢復的資訊，請參閱應用程式連線問題和回復。
-
- **iSeries Access for Windows 及 OS/400 主電腦伺服器**
  iSeries Access for Windows 及 OS/400 主電腦伺服器支援將透過 Kerberos 通行證的鑑別。在從屬站中，使用者可指定在存取 iSeries Access 主電腦伺服器時使用 Kerberos 通行證。
-
- **iSeries NetServer**
  如果您的網路中配置了 Kerberos，iSeries NetServer 從屬站可使用 Kerberos 通行證來鑑別伺服器。當啓用此支援時，僅支援 Kerberos v5 的從屬站可連接 iSeries NetServer。有關 Kerberos 的 iSeries NetServer 支援需求詳細資料，請參閱 iSeries NetServer support for Kerberos v5 authentication。
-
- **QFileSvr.400**
  QFileSvr.400 會判斷現行使用者的通行證授予通行證是否存在。如果通行證授予通行證存在的話，則會建立伺服器通行證來鑑別目標系統使用者。如果通行證不存在，則使用現行的密碼替代方法。**註**：如果您有指定於 Kerberos 配置檔中的預設領域，但未使用 Kerberos 作爲您的鑑別方法，則在對 QFileSvr.400 設定鑑別之前，您必須移除預設領域。有關如可從此問題恢復的資訊，請參閱應用程式連線問題和回復。

如何查看新增功能或變更內容

爲協助您了解技術變更之處，此資訊使用：

- » 影像標示了新增及變更資訊開始之處。
- « 影像標示了新增及變更資訊結束之處。

有關本版次新增或變更功能的相關資訊，請參閱 Memo to Users (使用者備忘錄) 。

«

列印此主題

欲檢視或下載 PDF 版本，請選取網路鑑別服務 (大約 199 KB 或 50 頁)。

若要在您的工作站儲存 PDF 以供檢視或列印：

1. 在您的瀏覽器中開啓 PDF（按一下上述的鏈結）。
2. 在瀏覽器功能表中，按一下**檔案**。
3. 按一下**另存新檔...**
4. 導覽至要儲存 PDF 的目錄。
5. 按一下**儲存**。

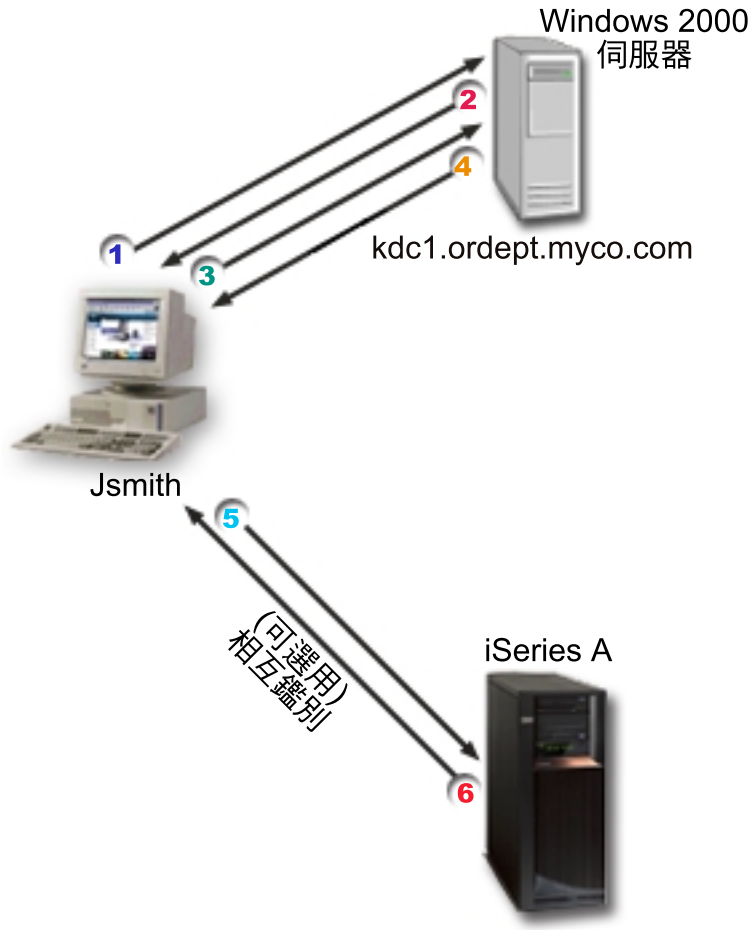
如果需要 Adobe Acrobat Reader 來檢視或列印 PDF，可從 Adobe 網站 (www.adobe.com/product/acrobat/readstep.html) 下載複本。

網路鑑別服務如何運作？

» 身爲網路管理者，您可以配置網路鑑別服務以使您的 iSeries 系統接受中央金鑰分送中心 (KDC) 所建立的 Kerberos 通行證，此 KDC 維護領域內所有使用者及服務的資料庫。iSeries 及數個 iSeries 特定應用程式充當 Kerberos 網路內的主從架構，要求使用者及服務的通行證。當使用者向 KDC 要求通行證時，使用者發出了一個起始通行證，稱爲通行證授予通行證 (TGT)。使用者則可使用 TGT 來要求服務通行證，以存取網路上其它服務及應用程式。要讓鑑別順利進行，管理者必須登錄使用者、iSeries 服務主體及將搭配使用 KDC 及 Kerberos 通信協定的應用程式。iSeries 可充當主體要求服務鑑別的伺服器，或充當要求網路上應用程式及服務通行證的從屬站。下列圖形顯示這些狀況中的通行證流程。

iSeries 作為伺服器

此圖顯示當 iSeries 充當 Kerberos 網路內的伺服器時鑑別如何運作。在此圖中，Windows (R) 2000 KDC 發出通行證給主體 Jsmith。Jsmith 想要存取 iSeries-A 上的應用程式。在此情形下，會在伺服器上使用「企業識別對映 (EIM)」來將 Kerberos 主體對映至 iSeries 使用者設定檔。可對任何已 kerberized 化的 iSeries 伺服器功能執行此動作，例如 iSeries-Access for Windows。

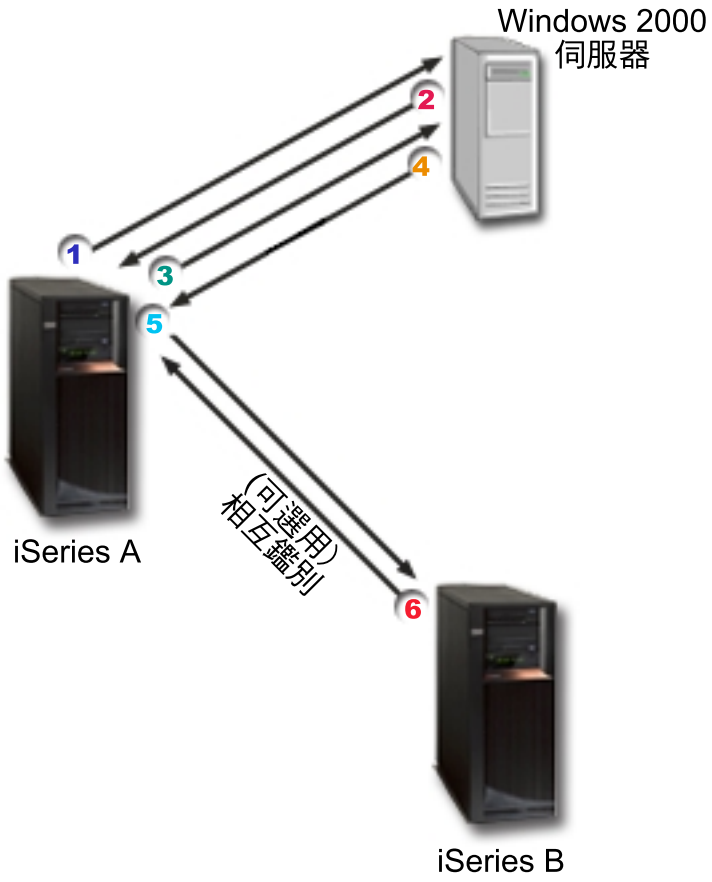


此說明提供此鑑別流程在網路內如何運作的概觀：

1. 使用者 Jsmith 登入 Kerberos 網路時向 KDC 要求通行證。這會傳送要求給 KDC 來取得通行證授予通行證。
2. KDC 會驗證 Jsmith 的主體名稱和密碼並傳送通行證授予通行證給他。
3. Jsmith 需要存取 iSeries 伺服器上的應用程式。藉由呼叫網路鑑別服務 API，應用程式會傳送 Jsmith 的 TGT 給 KDC，以要求特定應用程式或服務使用的服務通行證。主體的本端機器管理認證快取，其中保留通行證及其它使用者識別資訊。這些認證可在需要時從快取中讀取，而取得的新認證也儲存於快取中。這可減輕應用程式自己管理認證的責任。
4. KDC 以服務通行證作爲回應。
5. 應用程式傳送伺服器通行證給 iSeries 服務程式來鑑別使用者。
6. 伺服器應用程式藉由呼叫網路鑑別服務 API 來驗證通行證，並選用性地將回應傳回從屬站來相互鑑別。

iSeries 作為從屬站

此圖顯示當 iSeries 充當 Kerberos 網路內的從屬站時鑑別如何運作。在此圖中，Windows (R) 2000 KDC 發出通行證給 iSeries-A 主體。iSeries-A 可對其它服務鑑別。在此範例中，會在 iSeries B 上使用 EIM 以將 kerberos 主體對映至 iSeries 使用者設定檔。可對任何已 kerberized 化的 iSeries 伺服器功能執行此動作，例如 QFileSvr.400。



此說明提供此鑑別流程在網路內如何運作的概觀：

1. Jsmith 主體登入 iSeries-A，然後在 Qshell 直譯器中執行 kinit 指令來要求通行證授予通行證。iSeries 將此要求傳給 KDC。
2. KDC 會驗證 Jsmith 的主體名稱和密碼並傳送通行證授予通行證給他。
3. Jsmith 需要存取 iSeries 伺服器上的應用程式。藉由呼叫網路鑑別服務 API，應用程式會傳送 Jsmith 的 TGT 給 KDC，以要求特定應用程式或服務使用的服務通行證。主體的本端機器管理認證快取，其中保留通行證、階段作業金鑰及其它使用者識別資訊。這些認證可於需要時，由快取中讀取，而取得的新認證也儲存於快取中。這可減輕應用程式自己管理認證的責任。
4. KDC 以服務通行證作爲回應。**註**：iSeries-B 的服務主體必須新增至 KDC，而網路鑑別服務也必須配置於 iSeries-B 上。
5. 應用程式傳送伺服器通行證給 iSeries 服務程式來鑑別使用者。
6. 伺服器應用程式藉由呼叫網路鑑別服務 API 來驗證通行證，並選用性地將回應傳回從屬站來相互鑑別。

網路鑑別服務術語

網路鑑別服務使用下列 Kerberos 通信協定術語：

可轉遞通行證
可轉遞通行證允許伺服器將要求端認證傳遞給另一個服務。要讓這個情況發生的話，必須使用可轉遞選項來要求起始 TGT 並允許伺服器授權認證。

金鑰分送中心 (KDC)
提供通行證及暫時階段作業金鑰的網路服務。KDC 維護一個含有主體 (使用者和服務) 及其相關私密金鑰的資料庫。它是由鑑別伺服器與通行證授予通行證伺服器所組成。請務必使用安全機器充當您的 KDC。如果某人取得了 KDC 存取權，可能使您的整個領域受到威脅。**註**：iSeries 系統不支援 KDC。

金鑰表格
位於服務之主電腦系統上的檔案。此檔案中每一個登錄都含有服務主體的名稱及私密金鑰。在 iSeries 上，金鑰表格是在網路鑑別服務配置期間所建立。當某個服務要求以配置的「網路鑑別服務」鑑別 iSeries 時，iSeries 會檢查金鑰表格檔以取得該服務的認證。爲確定使用者及服務的鑑別無誤，您必須有列名於 KDC 和 iSeries 上的使用者及服務。

密碼伺服器
允許從屬站在遠端 KDC 變更它們的密碼。一般而言，密碼伺服器與 KDC 是在相同機器上執行。

主體
Kerberos 網路中使用者或服務的名稱。使用者就是使用服務來識別特定應用程式或一組作業系統服務的人。在 iSeries 上， **krbsvr400** 服務主體用來識別 iSeries Access for Windows、QFileSrv.400 及 Telnet 伺服器在從屬站與 iSeries 間鑑別時所使用的服務。

可 proxy 通行證
可 proxy 通行證就是「通行證授予通行證 (TGT)」，它可讓您使用 TGT 以外的 IP 位址來取得服務的通行證。與可轉遞通行證不同的是，您無法根據現行 TGT 來代 proxy 理新的 TGT；您只能 proxy 服務通行證。可轉遞通行證可讓您將完整識別資訊 (TGT) 轉送至另一台機器，而可 proxy 通行證只能讓您轉送特定的通行證。可 proxy 通行證允許服務代表主體執行作業。此服務必須能夠採用主體的識別資料作爲特定用途。可 proxy 通行證會根據原始通行證授予通行證來通知 KDC 以發出新通行證給不同的網址。可 proxy 通行證不需要密碼。

領域
以給定的金鑰分送中心 (KDC) 作爲鑑別中心的一組使用者及伺服器。

領域信任
Kerberos 通信協定搜尋配置檔來判定領域信任，或依預設尋找領域階層內的信任關係。網路鑑別服務中的**可靠的領域**可讓您略過這個程序並建立鑑別捷徑。領域信任可使用於其領域位於不同網域的網路。例如，如果公司有一個領域在 NY.myco.com，另一個在 LA.myco.com，那麼您可以建立這兩個領域之間的信任關係。如果兩個領域彼此信任，其相關的 KDC 必須共用一個金鑰。在建立捷徑之前，您必須設定 KDC 來彼此信任。

可更新通行證

在某些情況下，應用程式或服務可能想要可延長使用的通行證。不過，延長時間可能會讓某人竊取到通行證過期前有效的這些認證。可更新通行證可讓應用程式取得可延長使用的通行證，同時減少失竊的機會。可更新通行證含有兩個到期時間。第一個到期時間套用到現行通行證案例，第二個到期時間套用到通行證的最新許可到期日。

服務通行證
對服務鑑別主體的通行證。

通行證授予服務 (TGS)
由發出服務通行證的 KDC 所提供的一種服務。

通行證授予通行證 (TGT)
可在 KDC 存取通行證授予服務的通行證。在主體順利完成要求後，KDC 會將通行證授予通行證傳遞給主體。在 Windows (R) 2000 環境中，使用者登入網路，KDC 會驗證主體的名稱及加密密碼，然後將通行證授予通行證傳送給使用者。在 iSeries 伺服器上，使用者可在字元型介面中使用「Qshell 直譯器」的 kinit 指令來要求通行證。

網路鑑別服務通信協定

網路鑑別服務將 Kerberos 通信協定搭配「同屬安全服務 (GSS)」API 用於鑑別，以提供鑑別及安全服務。下列各節提供這些通信協定及如何在 iSeries 上使用它們的一般說明。有關這些標準的完整資訊，已提供一些相關 Request for Comment 及其它外部來源的鏈結。

Kerberos 通信協定

Kerberos 通信協定提供協力廠商鑑別，可供使用者向中央伺服器證明身份，所謂中央伺服器就是發出通行證給使用者的金鑰分送中心 (KDC)。使用者則可使用這些通行證在網路上證明自己的身份。有了通行證就不需要多次登入不同系統。iSeries 支援的 Kerberos API 源自 Massachusetts Institute of Technology，現已成爲使用 Kerberos 通信協定的實際標準。

安全性環境假設

Kerberos 通信協定假設所有資料交換發生於可任意插入、變更或截取封包的環境中。將 Kerberos 當作整體安全性規劃的一層。雖然 Kerberos 通信協定可讓您在網路中鑑別使用者及應用程式，但在定義您的網路安全目標時，有一些限制您應該要知道：

- Kerberos 通信協定沒有提供「拒絕服務」攻擊的保護。侵入者可利用這些通信協定的某些漏洞阻止應用程式參與適當的鑑別步驟。通常，這類攻擊的偵測及解決方案最好留給管理者及使用者來操作。
- 金鑰共用或金鑰失竊可能造成「冒充」攻擊。如果侵入者以某種方法取得主體的金鑰，他們就能夠僞裝成該使用者或服務。若要防止受到這種威脅，請禁止使用者共用金鑰並在您的安全規定內放入此原則。
- Kerberos 通信協定無法防止密碼遭受典型攻擊，例如密碼猜測。如果使用者密碼選得不好，侵入者便可藉由不斷嘗試將使用者密碼衍生出的金鑰所加密的訊息解密，順利發動「離線內碼轉換」攻擊。

有關 Kerberos 通信協定的詳細資訊，請參閱下列來源：

The Kerberos Network Authentication Service (V5)  。
Internet Engineering Task Force (IETF) 正式在 Request for Comments 1510 中定義 Kerberos 通信協定。

Kerberos: The Network Authentication Protocol (V5)  。
Massachusetts Institute of Technology 的 Kerberos 通信協定正式文件，提供程式設計資訊及說明通信協定特性。

Network Authentication Service Application Programmable Interfaces (APIs)

此「資訊中心」主題提供網路鑑別服務 API 報表及其功能的簡要說明。

同屬安全服務 (GSS) API

GSS API 提供一般性安全服務，由一些安全性技術支援，如 Kerberos 通信協定。這可讓 GSS 應用程式移轉到不同的環境。由於這個理由，建議您使用這些 API 來取代 Kerberos API。您可以撰寫使用 GSS API 的應用程式來與相同網路中的其它應用程式和從屬站通信。每一個通信應用程式在此交換都扮演一個角色。使用 GSS API，應用程式可以執行下列作業：

- 決定另一個應用程式的使用者 ID。
- 授予存取權給另一個應用程式。
- 對每一個訊息套用安全服務，例如機密性和整合性。

有關 GSS API 的詳細資訊，請參閱下列來源：

Generic Security Service Application Program Interface Version 2, Update 1  。
Internet Engineering Task Force (IETF) 正式在 RFC 2743 中定義 GSS API。

Generic Security Service API : C-bindings  。
Internet Engineering Task Force (IETF) 在 RFC 1509 中指定 GSS API C 連結。

The Kerberos Version 5 GSS-API Mechanism  .
Internet Engineering Task Force (IETF) 在這個 RFC 1964 中定義 Kerberos 版本 5 和 GSS API 規格。

Generic Security Service Application Programmable Interfaces (GSS APIs)
此「資訊中心」主題提供 GSS API 報表及其功能的簡要說明。

網路鑑別服務實務範例

» 正列實務範例提供可使用網路鑑別服務讓 iSeries 參與 Kerberos 網路之一般環境的說明。請複查下列實務範例來熟悉有關配置網路鑑別服務的技術及配置詳細資料：

實務範例：使用現有的 KDC 配置網路鑑別服務
此主題說明管理者在 Windows (R) 2000 環境 (已安裝及配置 KDC) 中配置網路鑑別的客戶狀況。

實務範例：啓用單一登入
此實務範例顯示如何搭配使用網路鑑別服務與「企業識別對映 (EIM)」來啓用單一登入。管理者想要讓使用者使用他們的 Windows (R) 2000 登入來鑑別 iSeries 系統及 iSeries Access for Windows 應用程式。

«

實務範例：使用現有的 KDC 配置網路鑑別服務

狀況

» 您是一個網路管理者，負責管理公司訂單接收部門的網路。您最近新增 iSeries 至網路來存放您部門的幾個必要之應用程式。目前您有一個 Windows (R) 2000 伺服器，它充當領域的金鑰分送中心 (KDC)。此網路內的使用者全部將主體名稱及密碼儲存在 KDC。您要將 iSeries 新增至 KDC。您打算將 iSeries 新增至這個領域，然後繼續將 Windows (R) 2000 伺服器當作鑑別伺服器使用。您有自己的可使用 Kerberos 的應用程式 (使用 GSS API)。

此實務範例具有下列優點：

- 簡化使用者的鑑別程序
- 減少在網路中管理伺服器存取的額外執行時間
- 將密碼失竊的威脅降至最低

目標

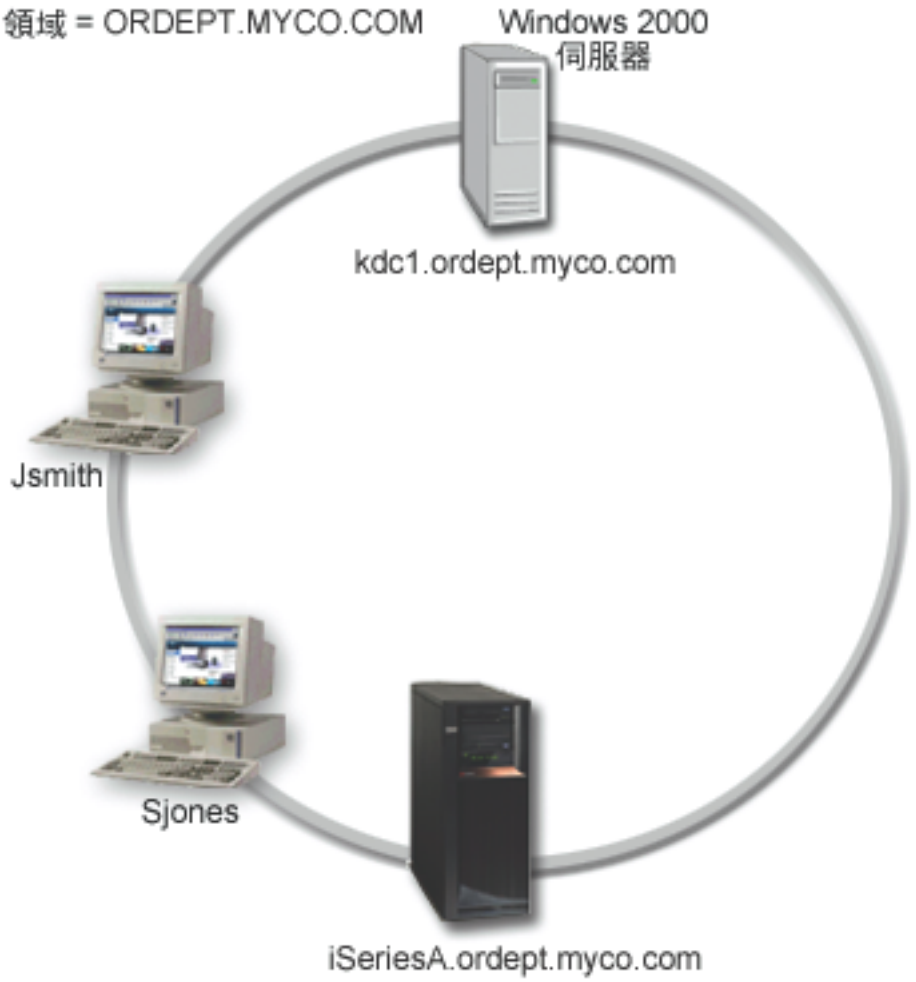
在此實務範例中，MyCo, Inc. 想要將 iSeries 系統新增至現有領域中，在該領域中 Windows (R) 2000 伺服器充當金鑰分送中心。iSeries 含有適當使用者才能存取的幾個重要業務應用程式。使用者需要經過 KDC 鑑別才能存取這些應用程式。iSeries 必須新增至 Windows (R) 2000 伺服器的 KDC 中。

此實務範例的目標如下：

- 使 iSeries 加入現有的金鑰分送中心
- 讓主體名稱及使用者名稱同時存在於網路中
- 讓 Kerberos 使用者在 KDC 變更自己的密碼

實務範例明細

下圖說明 MyCo 的網路性質。



訂單接收部門

- iSeries-A 執行於 OS/400 版本 5 版次 2 (V5R2) 上，且含有數個商務應用程式。
- KDC 的 DNS 名稱爲 kdc1.ordept.myco.com
- iSeries-A 的主體名稱爲 krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM
- KDC 的預設領域爲 ORDEPT.MYCO.COM
- 從屬站 PC 執行 Windows (R) 2000。

此實務範例的配置步驟

1. 完成 (12See)網路鑑別服務的規劃工作表及核對清單。
2. 在 iSeries-A 上配置 (13See)網路鑑別服務。
3. 新增 (13See) iSeries-A 至 KDC。

4. 爲 iSeries-A 的每一個使用者建立 (14See)起始目錄

5. 驗證 (14See) iSeries-A 的 TCP/IP 網域資訊
6. 測試 (14See) iSeries-A 上的網路鑑別服務配置。

配置明細

步驟 1：完成規劃工作表

下列規劃核對清單說明您於開始配置網路鑑別服務前所需的資訊類型。在您繼續進行網路鑑別服務設定之前，有關先決條件核對清單的所有回答應該全部爲「是」。

先決條件核對清單	回答
您的 OS/400 是 V5R2 (5722-SS1) 以上的版本？	是
您已於 iSeries 系統上安裝了「密碼存取提供者 (5722-AC3)」嗎？	是
您網路中所有 PC 及您的 iSeries 系統上已安裝了 iSeries Access for Windows (5722-XE1) 嗎？	是
您網路中所有 PC 及您的 iSeries 系統上已安裝了「iSeries 領航員」的「安全性」子元件嗎？	是
您網路中所有 PC 及您的 iSeries 系統上已安裝了「iSeries 領航員」的「網路」子元件嗎？	是
您有 *SECADM、*ALLOBJ 及 *IOSYSCFG 特殊權限嗎？	是
您的安全系統上有安裝將充當金鑰分送中心的下列之其中一項嗎？如果有的話，是哪一個？ 1. Windows (R) 2000 Server 2. Windows (R) XP Server 3. AIX Server 4. zSeries	是 Windows (R) 2000 Server
若爲 Windows (R) 2000 Server 和 Windows (R) XP Server，您是否於可作爲金鑰分送中心的系統上，安裝了提供 ktpass 工具的 Windows (R) 支援工具？	是
您網路中所有 PC 是否配置於 Windows (R) 2000 網域中？	是
您套用了最新的暫時修訂程式 (PTF) 嗎？	是
iSeries 系統時間與 KDC 系統時間相差於 5 分鐘內？如果不是，請參閱同步化系統時間。	是

您需要此資訊來配置網路鑑別服務	回答
iSeries-A 所屬的 Kerberos 預設領域名稱爲何？	ORDEPT.MYCO.COM
此 Kerberos 預設領域的 KDC 爲何？ KDC 接收埠爲何？	kdc1.ordept.myco.com 88 (**註**：此爲 KDC 的預設埠)。

您需要此資訊來配置網路鑑別服務	回答
您要爲這個預設領域配置密碼伺服器嗎？如果是，請回答下列問題： 此 KDC 的密碼伺服器名稱爲何？ 密碼伺服器的接收埠爲何？	是 kdc1.ordept.myco.com 464 (**註**：此爲密碼伺服器的預設埠)。
您的 iSeries 服務主體之密碼爲何？	iseriesa123 **註**：此實務範例內使用的任何及所有密碼只是舉例而已。於實際配置期間不應使用它們。
有無其他領域與您的 iSeries 系統相互作用？	N/A
每個領域之金鑰分送中心的主電腦名稱爲何？	N/A

步驟 2：在 iSeries-A 上配置網路鑑別服務

使用您工作表中的資訊以於 iSeries-A 上配置網路鑑別服務，如下所示：

1. 在「iSeries 領航員」中，展開 **iSeries-A —>安全性**。
2. 以滑鼠右鍵按一下**網路鑑別服務**，然後選取**配置**來啓動配置精靈。**註**：在您配置網路鑑別服務後，此選項將爲**重新配置**。
3. 有關精靈所建立物件的資訊，請複查**歡迎使用**頁。按一下**下一步**。
4. 在**指定領域資訊**頁上，將 ORDEPT.MYCO.COM 輸入於**預設領域**欄位中。按一下**下一步**。
5. 在**指定 KDC 資訊**頁上，將 kdc1.ordept.myco.com 輸入於 **KDC** 欄位中，並在**埠**欄位中輸入 88。按一下**下一步**。
6. 在**指定密碼資訊**頁上，選取**是**。將 kdc1.ordept.myco.com 輸入於**密碼伺服器**欄位中，以及在**埠**欄位中輸入 464。按一下**下一步**。
7. 在**建立 keytab 登錄**頁上，選取 **iSeries Kerberos 鑑別**。按一下**下一步**。
8. 在**建立 iSeries keytab 登錄**頁上，寫下 iSeries-A 的 keytab 和主體。當您將主體名稱新增至 KDC 時，您需要此名稱。輸入並確認密碼。例如，MyCo 管理者輸入 iseriesa123。**註**：此實務範例內使用的任何所有密碼只是舉例而已。於實際配置期間不應使用它們。
9. 按一下**下一步**。
10. 於**摘要**頁上，複查網路鑑別服務配置明細。按一下**完成**。

現在已完成 iSeries-A 上的網路鑑別服務配置。下一步是將主體名稱新增至 KDC。

步驟 3：將 iSeries-A 主體名稱新增至 KDC

若要新增 iSeries 系統至 Windows (R) 2000 KDC，請參考新增主體至 KDC 所對應的文件。依慣例，iSeries 系統名稱可作爲使用者名稱。請將下列主體名稱新增至 KDC：

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

在 Windows (R) 2000 Server 上，請遵循下列步驟：

1. 使用 Active Directory (R) 管理工具來建立 iSeries 系統使用者帳戶 (選取**使用者**資料夾，以滑鼠右鍵按一下，選取**新建**，然後選取**使用者**)。將 iSeriesA 指定爲 Active Directory 使用者。
2. 存取 Active Directory 使用者 iSeriesA 上的內容。從**帳戶**標籤中，選取**帳戶受信任可以委派**。這可使 iSeries-A 服務主體代表登入使用者存取其它服務。
3. 使用 **ktpass** 指令，將使用者帳戶對映至主體。Windows (R) 2000 Server 安裝 CD 上的 **Service Tools** 資料夾中提供 ktpass 工具。若要對映使用者帳戶，請輸入下列指令：

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

   其中 iseriesa123 是您剛於配置 (13See)網路鑑別服務時所指定的密碼。**註**：此實務範例內使用的任何及所有密碼只是舉例而已。於實際配置期間不應使用它們。

步驟 4：爲 iSeries-A 的使用者建立一個起始目錄

連接 iSeries 和 iSeries 應用程式的每一個使用者都需要一個位於 /home 目錄下的目錄。此目錄將包含使用者的 Kerberos 認證快取名稱。若要爲使用者建立起始目錄，請完成下列步驟：

1. 在 iSeries 指令行上，輸入：

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

   其中 username 爲使用者的 iSeries 使用者名稱。
   例如，MyCo 管理者輸入下列指令：
   CRTDIR '/home/Johns' 代表使用者 John Smith。
2. 對您的所有使用者重複這些步驟。

步驟 5：驗證 iSeries-A 的 TCP/IP 網域資訊

1. 在 iSeries 指令行上，輸入：

   ```
   CFGTCP
   ```

2. 選取「選項 10」(使用 TCP/IP 主電腦表格登錄)。
3. 在主電腦名稱欄位中，請驗證 iSeries-A 的完整主電腦名稱是小寫。若有多個主電腦名稱登錄，亦請驗證是否先出現完整主電腦名稱。例如，iSeries A 的主電腦名稱登錄應爲：iseriesa.ordept.myco.com。
4. 驗證主電腦名稱登錄之後，請按 F3 返回「配置 TCP」主功能表。
5. 選取「選項 12」(變更 TCP/IP 網域資訊)。
6. 驗證系統名稱是否出現在主電腦名稱欄位中。亦請驗證網域名稱是否正確。在本範例中， 主電腦名稱是 iseriesa，而網域名稱是 ordept.myco.com。

步驟 6：在 iSeries-A 上測試網路鑑別服務

此時，您可以藉由對 iSeries-A 主體名稱要求通行證授予通行證，來驗證網路鑑別服務的配置是否正確：

1. 在指令行上，輸入 QSH 來啓動 Qshell 直譯器。
2. 輸入 keytab list 來顯示 keytab 檔中登記的主體清單。於此實務範例中，krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM 應顯示爲 iSeries-A 的主體名稱。**註**：如果您選擇對 LDAP 和 iSeries NetServer 配置主體，keytab 檔中將有其它登錄。於此實務範例中，管理者選擇不爲這些服務配置主體。

3. 輸入 `kinit -k krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM`。若此順利完成，QSH 指令會顯示無誤。
4. 輸入 `klist` 來驗證預設主體是否爲 krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM。

實務範例：啓用單一登入

狀況

您是一個網路管理者，負責管理公司「訂單接收部門」的網路。目前您的使用者使用 Windows (R) 2000 桌面。他們需要管理自己的 Windows ID 和密碼及其 OS/400 使用者名稱。您想要將 Windows (R) 2000 登入用於 iSeries 鑑別。您不想要使 Windows (R) 2000 ID 與 OS/400 使用者名稱相同，也不想要使用密碼快取或同步，原因是這些解決方案有安全上的問題。您聽說 iSeries 伺服器可啓用單一登入，方法是在您的伺服器上配置網路鑑別服務及 EIM。網路鑑別服務允許 iSeries 系統加入 Window (R) 2000 網域，而 EIM 則提供一個機制使 Windows (R) 2000 ID 與在該企業中代表該使用者的單一 EIM ID 產生關聯。由於這些關聯，網路上的 Kerberos 主體便可存取一些 iSeries 應用程式，而不需要使用其 iSeries 使用者名稱及密碼登入。有關使用單一登入的好處及如何一起使用 EIM 和網路鑑別服務的詳細資料，請參閱啓用單一登入主題。

實務範例優點

此實務範例具有下列優點：

- 簡化使用者的鑑別程序
- 減少在網路中管理伺服器存取的額外執行時間
- 將密碼失竊的威脅降至最低
- 避免需要多重登入
- 簡化網路間的使用者識別管理

目標

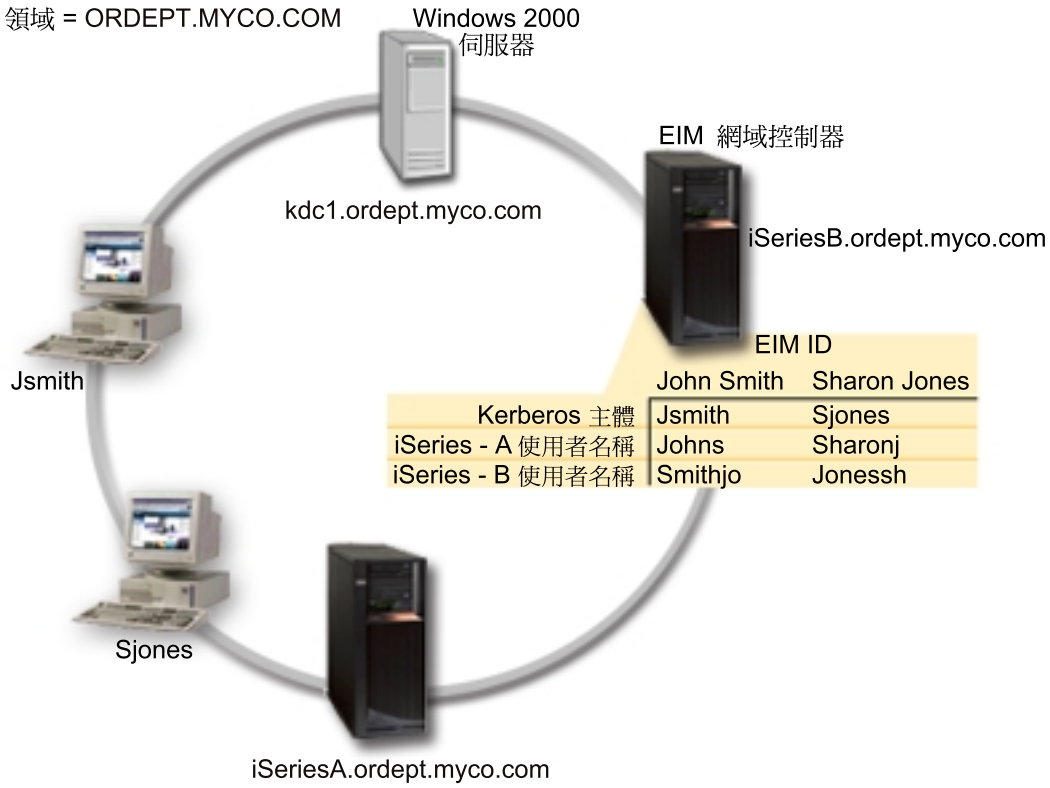
於此實務範例中，MyCo, Inc. 想要將 iSeries 系統新增至現有的 Windows (R) 2000 網域作爲鑑別之用。iSeries 系統含有數個必須由使用者存取的應用程式。使用者需要經過 KDC 鑑別才能存取這些應用程式。iSeries 服務主體必須新增至 Windows (R) 2000 伺服器的 KDC 中，才能讓主體要求服務通行證。此外，您將配置 EIM，然後建立關聯以將 OS/400 使用者設定檔及 Kerberos 主體對映至代表企業中單一使用者的 EIM ID。由於「訂單接收部門」中的使用者使用 iSeries Access for Windows 應用程式，所以您決定使用 Kerberos 主體作爲 iSeries Access for Windows 及其相關應用程式偏好的鑑別方法。

此實務範例的目標如下：

- 使 iSeries-A 和 iSeries-B 加入現有的金鑰分送中心
- 將 iSeries-B 上的「目錄伺服器」配置爲網域的 EIM 網域控制器
- 讓 iSeries-A 和 iSeries-B 上的使用者設定檔及 Kerberos 主體對映至單一 EIM ID
- 使用 Kerberos 主體來鑑別 iSeries Access for Windows 應用程式

實務範例明細

下圖說明 MyCo 的網路性質。



訂單接收部門

- iSeries-A 與 iSeries-B 執行於 OS/400 版本 5 版次 2 (V5R2) 上，且含有數個商務應用程式。
- KDC 的名稱爲 `kdc1.ordept.myco.com`。
- iSeries-A 的主體名稱爲 `krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM`。
- iSeries-A 的 DNS 名稱爲 `iSeriesA.ordept.myco.com`。
- KDC 的預設領域爲 `ORDEPT.MYCO.COM`。
- 配置 iSeries-B 上的 Directory Server (LDAP) 作爲網路的 EIM 網域控制器。**註**：LDAP 配置必須在配置 EIM 之前完成；不過，如果系統上沒有配置 LDAP，EIM 配置精靈提供了 LDAP 配置。在此實務範例中，iSeries-B 並沒有配置 LDAP。管理者計劃在 EIM 配置期間配置 LDAP。
- iSeries-B 的 DNS 名稱爲 `iSeriesB.ordept.myco.com`。
- iSeries-B 的主體名稱爲 `krbsvr400/iSeriesB.ordept.myco.com@ORDEPT.MYCO.COM`。
- 從屬站 PC 執行 Windows (R) 2000。
- Kerberos 的兩個主體 Jsmith 和 Sjones 已在 KDC 完成登記。

此實務範例的配置步驟

1. 完成 (17See) iSeries-A 和 iSeries-B 的規劃工作表
2. 在 iSeries-A 上配置 (18See)網路鑑別服務
3. 新增 (19See) iSeries-A 服務主體至 KDC

4. 爲 iSeries-A 的每一個使用者建立 (19See)起始目錄
5. 驗證 (20See) iSeries-A 的 TCP/IP 網域資訊
6. 測試 (20See) iSeries-A 上的網路鑑別服務配置
7. 對 iSeries-B 重複步驟 2-6
8. 配置 (20See) EIM 網域並將 iSeries-B 上的目錄伺服器配置爲 EIM 網域控制器
9. 配置 (21See) iSeries-A 以加入 EIM 網域
10. 爲企業中的使用者建立 (22See) EIM ID
11. 將 OS/400 使用者設定檔及主體名稱的 EIM 關聯新增 (22See)至 EIM ID

12. 配置 (23See) iSeries Access for Windows 連線來使用 Kerberos 主體作爲鑑別方法
13. 驗證 (23See)網路鑑別服務及 EIM 設定

配置明細

步驟 1：完成規劃工作表

下列規劃核對清單說明您開始配置網路鑑別服務及「企業識別對映 (EIM)」之前所需的資訊類型。在您繼續進行網路鑑別服務設定前，有關先決條件核對清單的所有回答應該全部爲「是」且配置網路鑑別的資訊應該完整。

先決條件核對清單	回答
您的 OS/400 是 V5R2 (5722-SS1) 以上的版本？	是
您的 iSeries 系統上已安裝了「密碼存取提供者 (5722-AC3)」嗎？	是
您網路中所有 PC 及您的 iSeries 系統上已安裝了 iSeries Access for Windows (5722-XE1) 嗎？	是
您網路中所有 PC 及您的 iSeries 系統上已安裝了「iSeries 領航員」的「安全性」子元件嗎？	是
您網路中所有 PC 及您的 iSeries 系統上已安裝了「iSeries 領航員」的「網路」子元件嗎？	是
您有 *SECADM、*ALLOBJ 及 *IOSYSCFG 特殊權限嗎？	是
您有下列其中一個充當金鑰分送中心的系統嗎？是哪一個？ 1. Windows (R) 2000 Server 2. Windows (R) XP Server 3. AIX Server 4. zSeries	是 Windows (R) 2000 Server

若是 Windows (R) 2000 Server 和 Windows (R) XP Server，您安裝了提供 ktpass 工具的 Windows 支援工具嗎？	是
您網路中所有 PC 配置於 Windows (R) 2000 網域中？	是
您套用了最新的暫時修訂程式 (PTF) 嗎？	是
iSeries 系統時間與 KDC 系統時間相差於 5 分鐘內？如果不是，請參閱同步化系統時間。	是

您需要此資訊來配置網路鑑別服務	**回答**
iSeries 所屬的 Kerberos 預設領域名稱爲何？	ORDEPT.MYCO.COM
此 Kerberos 預設領域的 KDC 爲何？ KDC 接收埠爲何？	kdc1.ordept.myco.com 88 (**註**：此爲 KDC 的預設埠)。
您要爲這個預設領域配置密碼伺服器嗎？如果是，請回答下列問題： 此 KDC 的密碼伺服器名稱爲何？ 密碼伺服器的接收埠爲何？	是 kdc1.ordept.myco.com 464 (**註**：此爲密碼伺服器的預設埠)。
您的 iSeries 服務主體之密碼爲何？	iseriesa123 iseriesb345 **註**：此實務範例內使用的任何及所有密碼只是舉例而已。於實際配置期間不應使用它們。
有無其它領域與您的 iSeries 相互作用？	N/A
每個領域之金鑰分送中心的主電腦名稱爲何？	N/A

您需要此資訊來配置「企業識別對映 (EIM)」	**回答**
LDAP 管理者的識別名稱及密碼爲何？	識別名稱：cn=administrator 密碼：mycopwd **註**：此實務範例內使用的任何及所有密碼只是舉例而已。 於實際配置期間不應使用它們。
「目錄服務 (LDAP)」伺服器名稱爲何？	iSeriesB.ordept.myco.com
「目錄服務 (LDAP)」伺服器的埠號爲何？	389

步驟 2：在 iSeries-A 上配置網路鑑別服務

若要使用您工作表中的資訊以於 iSeries-A 上配置網路鑑別服務，請完成下列作業：

1. 在「iSeries 領航員」中，展開 **iSeries-A —>安全性**。
2. 以滑鼠右鍵按一下**網路鑑別服務**，然後選取**配置**來啓動配置精靈。**註**：在您配置網路鑑別服務後，此選項將爲**重新配置**。
3. 有關精靈所建立物件的資訊，請複查**歡迎使用**頁。按一下**下一步**。
4. 在**指定領域資訊**頁上，將 ORDEPT.MYCO.COM 輸入於**預設領域**欄位中。按一下**下一步**。
5. 在**指定 KDC 資訊**頁上，將 kdc1.ordept.myco.com 輸入於 **KDC** 欄位中，並在**埠**欄位中輸入 88。按一下**下一步**。
6. 在**指定密碼資訊**頁上，選取**是**。將 kdc1.ordept.myco.com 輸入於**密碼伺服器**欄位中，以及在**埠**欄位中輸入 464。按一下**下一步**。**註**：此密碼必須與新增主體至 KDC 時所輸入的密碼相同。
7. 在**建立 keytab 登錄**頁上，選取 **iSeries Kerberos 鑑別**。按一下**下一步**。
8. 在**建立 iSeries keytab 登錄**頁上，寫下 iSeries-A 的 keytab 和主體。當您將主體名稱新增至 KDC 時，您需要此名稱。輸入並確認密碼。例如，MyCo 管理者使用密碼 iseriesa123。當 iSeries-A 新增至 KDC 時，將使用此密碼。**註**：此實務範例內使用的任何及所有密碼只是舉例而已。於實際配置期間不應使用它們。按一下**下一步**。
9. 於**摘要**頁上，複查網路鑑別服務配置明細。按一下**完成**。

現在已完成 iSeries-A 上的網路鑑別服務配置。下一步是將主體名稱新增至 KDC。

步驟 3：將 iSeries-A 主體名稱新增至 KDC

若要新增 iSeries 至 Windows (R) 2000 KDC，請參考新增主體至 KDC 所對應的文件。依慣例，iSeries 名稱可作爲使用者名稱。請將下列主體名稱新增至 KDC：

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

在 Windows (R) 2000 Server 上，請遵循下列步驟：

1. 使用 Active Directory (R) 管理工具來建立 iSeries-A 使用者帳戶 (選取**使用者**資料夾，以滑鼠右鍵按一下、選取**新建**，然後選取**使用者**)。將 iSeriesA 指定爲 Active Directory 使用者。
2. 存取 Active Directory 使用者 iSeriesA 上的內容。從**帳戶**標籤中，選取**帳戶受信任可以委派**。這可使 iSeries-A 服務主體代表登入使用者存取其它服務。
3. 使用 **ktpass** 指令，將使用者帳戶對映至主體。Windows (R) 2000 Server 安裝 CD 上的 **Service Tools** 資料夾中提供 ktpass 工具。若要對映使用者帳戶，請輸入下列指令：

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

   其中 iseriesa123 是您在步驟 6 中配置 (18See)網路鑑別服務時所指定的密碼。**註**：此實務範例內使用的任何及所有密碼只是舉例而已。於實際配置期間不應使用它們。

步驟 4：爲 iSeries-A 的使用者建立一個起始目錄

連接 iSeries 和 iSeries 應用程式的每一個使用者都需要一個位於 /home 目錄下的目錄。此目錄將包含使用者的 Kerberos 認證快取名稱。若要爲使用者建立起始目錄，請完成下列步驟：

1. 在 iSeries 指令行上，輸入：

CRTDIR '/home/username'
其中 username 是使用者的 iSeries 使用者名稱。
例如，MyCo 管理者輸入下列指令：
CRTDIR '/home/Johns' 代表使用者 John Smith。

2. 對您的所有使用者重複這些步驟。

步驟 5：驗證 iSeries A 的 TCP/IP 網域資訊

1. 在 iSeries 指令行上，輸入：

   CFGTCP

2. 選取「選項 10」(使用 TCP/IP 主電腦表格登錄)。
3. 在主電腦名稱欄位中，請驗證 iSeries A 的完整主電腦名稱是小寫。若有多個主電腦名稱登錄，亦請驗證是否先出現完整主電腦名稱。例如，iSeries A 的主電腦名稱登錄應爲：iseriesa.ordept.myco.com。
4. 驗證主電腦名稱登錄之後，請按 F3 返回「配置 TCP」主功能表。
5. 選取「選項 12」(變更 TCP/IP 網域資訊)。
6. 驗證系統名稱是否出現在主電腦名稱欄位中。亦請驗證網域名稱是否正確。在本範例中， 主電腦名稱是 iseriesa，而網域名稱是 ordept.myco.com。

步驟 6：在 iSeries-A 上測試網路鑑別服務

此時，您可以藉由對 iSeries-A 主體名稱要求通行證授予通行證，來驗證網路鑑別服務的配置是否正確：

1. 在指令行上，輸入 QSH 來啓動 Qshell 直譯器。
2. 輸入 keytab list 來顯示 keytab 檔中登記的主體清單。於此實務範例中，krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM 應顯示爲 iSeries-A 的主體名稱。
3. 輸入 kinit -k krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM。若此順利完成，QSH 指令會顯示無誤。
4. 輸入 klist 來驗證預設主體是否爲 krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM。

步驟 7：對 iSeries-B 重複步驟 2 及 6。

步驟 8：在 iSeries-B 上配置 EIM 和 EIM 網域控制器

現在您必須在網路中配置 EIM 網域。您也需要將 iSeries-B 配置成新 EIM 網域的 EIM 網域控制器。完成此步驟後，您就完成了下列作業：

- 建立了新的 EIM 網域。
- 將 iSeries-B 上的「目錄伺服器」配置爲 EIM 網域控制器。
- 在網域中建立 iSeries-B 的 EIM 登錄及 Kerberos 使用者登錄。
- 配置 iSeries-B 以加入 EIM 網域中。

1. 於「iSeries 領航員」中，展開 **iSeries-B —>網路—>企業識別對映**。
2. 以滑鼠右鍵按一下**配置**，然後選取**配置**以啓動配置精靈。
3. 在**歡迎使用**頁上，選取**建立並結合新網域**。按一下**下一步**。
4. 在**配置目錄伺服器**頁上，接受**埠**欄位的預設值 389。於**識別名稱**欄位中，輸入 cn=administrator。輸入並確認密碼。此密碼將使用於存取 EIM 網域管理作業時。例如，MyCo 管理者在密碼和確認密碼欄位中輸入 mycopwd。**註**：此實務範例內使用的任何及所有密碼只是舉例而已。於實際配置期間不應使用它們。按一下**下一步**。
5. 在**指定網域**頁上，輸入網域名稱。例如，MyCo 管理者在**網域**欄位中輸入 mycoeimDomain。**註**：網域名稱不可含有下列任何字元：= + < > , # ; \ 及 *。**說明**欄位爲可選用的。如果您要的話，可輸入網域控制器的簡要說明。按一下**下一步**。
6. 在**指定網域上層 DN** 頁上，選取**否**。按一下**下一步**。
7. 在**登錄資訊**頁上，選取**本端 OS/400** 及 **Kerberos**。選取 **Kerberos 使用者識別為區分大小寫**。按一下**下一步**。記下登錄名稱。當建立 EIM ID 連結時，您需要這些登錄名稱。**註**：登錄名稱在網域中必須是唯一的。
8. 在**指定 EIM 系統使用者**頁上，選取系統 EIM 使用者。接受此頁面所顯示的預設值。例如，MyCo 在此頁面中有下列資訊：
   - 使用者類型：識別名稱及密碼
   - 識別名稱：cn=administrator
   - 密碼：mycopwd
     註：此實務範例內使用的任何及所有密碼只是舉例而已。於實際配置期間不應使用它們。

   按一下**下一步**。
9. 於**摘要**頁上，確認 EIM 配置資訊。按一下**完成**。

現在，您已將 iSeries-B 的目錄伺服器配置爲網路中最近配置的 EIM 網域之 EIM 網域控制器。您必須將 iSeries-A 指定爲此 EIM 網域中的參與者。

現在，您需要配置 iSeries-A 來加入 EIM 網域中。

1. 於「iSeries 領航員」中，展開 **iSeries-A —>網路—>企業識別對映**。
2. 以滑鼠右鍵按一下**配置**，然後選取**配置**以啓動配置精靈。
3. 於**歡迎使用**頁上，選取**結合現有的網域**。按一下**下一步**。
4. 於**指定網域控制器**頁上，輸入網域控制器名稱。例如，MyCo 管理者在**網域控制器名稱**欄位中輸入 iSeriesB.ordept.myco.com。按一下**下一步**。
5. 於**指定連線使用者**頁上，針對使用者類型選取**識別名稱及密碼**。例如，MyCo 管理者在**識別名稱**欄位中輸入 cn=administrator，以及在密碼和確認密碼欄位中輸入 mycopwd。**註**：此實務範例內使用的任何及所有密碼只是舉例而已。於實際配置期間不應使用它們。 按一下**下一步**。
6. 於**指定網域**頁上，選取您要加入的網域名稱。按一下**下一步**。例如，MyCo 管理者選取 **mycoeimDomain**。
7. 於**登錄資訊**頁上，選取**本端 OS/400**。按一下**下一步**。記下登錄名稱。當建立 EIM ID 連結時，您需要這些登錄名稱。**註**：登錄名稱在網域中必須是唯一的。
8. 在**指定 EIM 系統使用者**頁上，選取系統 EIM 使用者。接受此頁面所顯示的預設值。例如，MyCo 在此頁面中有下列資訊：
   - 使用者類型：識別名稱及密碼
   - 識別名稱：cn=administrator
   - 密碼：mycopwd
     註：此實務範例內使用的任何及所有密碼只是舉例而已。於實際配置期間不應使用它們。

按一下**下一步**。

9. 於**摘要**頁上，確認 EIM 配置。按一下**完成**。

現在，您已配置 iSeries-A 以加入網域中。

現在，您需要爲企業中每一個使用者建立 EIM ID。EIM ID 代表網路上的使用者或實體。在 MyCo 案例中，管理者建立兩個 EIM ID：John Smith 和 Sharon Jones。

1. 在 iSeries-B 上，展開**網路**—> **企業識別對映**。
2. 以滑鼠右鍵按一下**網域管理**，然後選取**新增網域...**
3. 在**新增網域**對話框中，這些預設值應針對 MyCo 的 EIM 網域顯示：
   - 埠：389
   - 網域：mycoeimDomain
   - 上層 DN：無
   - 網域控制器：iSeriesB.ordept.myco.com

   註：這些預設值建立於 EIM 網域控制器配置期間。
4. 按一下**確定**。
5. 「iSeries 領航員」階層隨**網域管理**下的 **mycoeimDomain** 重新整理。按一下 **mycoeimDomain**。將出現**連接 EIM 網域控制器**對話框。您必須先連接 EIM 網域控制器，才能管理網域。
6. 於**連接 EIM 網域控制器**頁上，輸入「網域控制器」的管理者識別名稱及密碼。這些就是於 EIM 網域控制器配置期間所建立的相同識別名稱及密碼。就 MyCo 而言，管理者輸入下列項目：
   - 識別名稱：cn=administrator
   - 密碼：mycopwd **註**：此實務範例內使用的任何及所有密碼只是舉例而已。於實際配置期間不應使用它們。
7. 按一下**確定**。
8. 將顯示兩個新資料夾。以滑鼠右鍵按一下 **ID**，然後選取**新 ID**。
9. 於**新 EIM ID** 頁的 **ID** 欄位中輸入 ID。重複此步驟直到所有使用者都擁有 ID 爲止。MyCo 新增下列 ID：
   - John Smith
   - Sharon Jones
10. 按一下**確定**。

既然已爲 John Smith 和 Sharon Jones 建立了唯一的 EIM ID，所以現在我們可以使在 iSeries-A 和 iSeries-B 上的 OS/400 使用者名稱及其 Kerberos 主體與這些 EIM ID 產生關聯。

步驟 11：新增 OS/400 使用者設定檔及主體名稱的 EIM 關聯到 EIM ID

若要完成此作業，MyCo 管理者要完成下列步驟：

1. 在 iSeries-B 上，展開 **ID**，以滑鼠右鍵按一下 **John Smith**，然後選取**內容**。此 ID 有三個關聯：Kerberos 主體、iSeries-A 的使用者設定檔及 iSeries-B 的使用者設定檔。
2. 使 Kerberos 主體與 John Smith 這個 ID 產生關聯：
   a. 於**關聯**標籤上，按一下**新增**。

b. 在**新增關聯**頁上，按一下**登錄**欄位中的**瀏覽**，然後選取 ORDEPT.MYCO.COM。此爲於 EIM 配置期間所新增的 Kerberos 使用者登錄。
c. 於**使用者**欄位中，輸入 Jsmith。
d. 於**關聯類型**欄位中，選取**來源**。
e. 按一下**確定**。

3. 使 iSeries-A 的使用者名稱與 John Smith 這個 ID 產生關聯：
a. 於**關聯**標籤上，按一下**新增**。
b. 在**新增關聯**頁上，按一下**登錄**欄位中的**瀏覽**，然後選取 iSeriesA.ordept.myco.com。此爲 iSeries-A 的 OS/400 使用者登錄。
c. 於**使用者**欄位中，輸入 Johns。
d. 於**關聯類型**欄位中，選取**目標**。
e. 按一下**確定**。

4. 使 iSeries-B 的使用者名稱與 John Smith 這個 ID 產生關聯：
a. 於**關聯**標籤上，按一下**新增**。
b. 於**新增關聯**頁上，按一下**登錄**欄位中的**瀏覽**，然後選取 iSeriesB.ordept.myco.com。此爲 iSeries-B 的 OS/400 使用者登錄。
c. 於**使用者**欄位中，輸入 Smithjo。
d. 於**關聯類型**欄位中，選取**目標**。
e. 按一下**確定**。

5. 對 Sharon Jones 這個 EIM ID 重複步驟 1-4。

現在，您需要在 Jsmith 的 PC 和 Sjones 的 PC 上配置 iSeries Access for Windows 應用程式，以便在鑑別 iSeries-A 和 iSeries-B 時使用 Kerberos。

若要在 Jsmith 的 PC 上配置 iSeries-A 及其應用程式來使用 Kerberos 鑑別，請完成下列步驟：

1. 在「iSeries 領航員」中，以滑鼠右鍵按一下 **iSeries-A**，然後選取**內容**。
2. 在**連線**標籤上，選取**使用 Kerberos 主體名稱，不提示**。這可使 iSeries Access for Windows 連線使用 Kerberos 主體名稱及密碼來鑑別。
3. 對 iSeries-B 重複這些步驟。
4. 對 Sjones 的 PC 重複這些步驟。

步驟 13：驗證網路鑑別服務及 EIM 設定

此時，已完成所有配置步驟。若要驗證網路鑑別服務及 EIM 的設定是否正確，管理者必須藉由登入 Sharon Jones 和 John Smith 的 PC 來將他們登入至 Windows (R) 2000 網域。然後，使之於 iSeries-A 上開啓「iSeries 領航員」。若 iSeries 登入提示沒有顯示，表示 EIM 順利將 Kerberos 主體對映到網域上的 ID。除了 iSeries Access for Windows 應用程式以外，以下這些應用程式支援 Kerberos 鑑別：

- Telnet 伺服器
- iSeries NetServer
- QFileSrv.400

- 分散式關聯資料庫架構 (DRDA)

«

規劃網路鑑別服務

» 若要順利配置網路鑑別服務，您必須瞭解基本要求並完成必要的規劃步驟。此主題提供先決條件核對清單及規劃工作表來確保所有必要步驟順利完成。下列核對清單及工作表可協助您配置網路鑑別服務。

先決條件核對清單	回答
您的 OS/400 是 V5R2 (5722-SS1) 以上的版本？	
您已於 iSeries 系統上安裝了「密碼存取提供者 (5722-AC3)」嗎？	
您網路中所有 PC 及您的 iSeries 系統上已安裝了 iSeries Access for Windows (5722-XE1) 嗎？	
您網路中所有 PC 及您的 iSeries 系統上已安裝了「iSeries 領航員」的「安全性」子元件嗎？	
您網路中所有 PC 及您的 iSeries 系統上已安裝了「iSeries 領航員」的「網路」子元件嗎？	
您有 *SECADM、*ALLOBJ 及 *IOSYSCFG 特殊權限嗎？	
您的安全系統上有安裝將充當金鑰分送中心的下列其中一項？哪一個？ 1. Windows (R) 2000 Server 2. Windows (R) XP Server 3. AIX Server 4. zSeries	
若是 Windows (R) 2000 Server 和 Windows (R) XP Server，您是否於可作爲金鑰分送中心的系統上，安裝了提供 ktpass 工具的 Windows Support Tools？	
您網路中所有 PC 是否配置於 Windows (R) 2000 網域中？	
您套用了最新的暫時修訂程式 (PTF) 嗎？	
iSeries 系統時間與 KDC 系統時間相差於 5 分鐘內？如果不是，請參閱同步化系統時間。	

您需要此資訊來配置網路鑑別服務	回答
iSeries-A 所屬的 Kerberos 預設領域名稱爲何？	
此 Kerberos 預設領域的 KDC 爲何？ KDC 接收埠爲何？	
您要爲這個預設領域配置密碼伺服器嗎？如果是，請回答下列問題： 此 KDC 的密碼伺服器名稱爲何？ 密碼伺服器的接收埠爲何？	
您的 iSeries 服務主體之密碼爲何？	

您需要此資訊來配置網路鑑別服務	回答
有無其它領域與您的 iSeries 相互作用？	
每個領域之金鑰分送中心的主電腦名稱爲何？	
您 iSeries 上的應用程式使用的服務主體名稱爲何？	

«

配置網路鑑別服務

» 在配置網路鑑別服務之前，您應該先完成所有必要的規劃步驟。此外，網路鑑別服務假設您已在網路的安全系統上配置 KDC。目前，iSeries 不支援 KDC。Microsoft Windows (R) 2000 和 Windows (R) XP 及 z/OS 支援 KDC 功能。請參閱將作爲 KDC 的系統之 Kerberos 配置所對應的適當文件。

建議您在 iSeries 上配置網路鑑別服務之前先配置 KDC。若要配置網路鑑別服務，請完成下列步驟：

1. 在「iSeries 領航員」中，展開 **iSeries-A —>安全性**。
2. 以滑鼠右鍵按一下**網路鑑別服務**，然後選取**配置**來啓動配置精靈。**註**：在您配置網路鑑別服務之後，此選項將爲**重新配置**。
3. 有關精靈所建立物件的資訊，請複查**歡迎使用**頁。按一下**下一步**。
4. 在**指定領域資訊**頁上，將預設領域名稱輸入**預設領域**欄位中。按一下**下一步**。
5. 在**指定 KDC 資訊**頁上，將此領域的金鑰分送中心名稱輸入 **KDC** 欄位中，然後在**埠**欄位中輸入 88。按一下**下一步**。
6. 在**指定密碼資訊**頁上，選取**是**或**否**來設定密碼伺服器。密碼伺服器允許主體變更 KDC 上的密碼。如果您選取**是**，請在**密碼伺服器**欄位中輸入密碼伺服器名稱。密碼伺服器的預設埠爲 464。按一下**下一步**。
7. 在**建立 keytab 登錄**頁上，選取 **iSeries Kerberos 鑑別**。此外，如果您想要這些服務使用 Kerberos 鑑別，則也可對 LDAP 伺服器及 iSeries NetServer 建立 keytab 登錄。按一下**下一步**。
8. 在**建立 iSeries keytab 登錄**頁上，輸入並確認密碼。按一下**下一步**。**註**：這是您在定義 iSeries 給 KDC 時使用的相同密碼。
9. 於**摘要**頁上，複查網路鑑別服務配置明細。按一下**完成**。

現已完成網路鑑別服務配置。

下一個步驟？

定義 iSeries 給金鑰分送中心

«

定義 iSeries 給金鑰分送中心

» 在 iSeries 上配置網路鑑別服務之後，您必須將 iSeries 定義到金鑰分送中心 (KDC)。網路鑑別服務提供 iSeries 主體名稱 **krbsvr400** 給伺服器及所有原始 iSeries 應用程式。

例如，在我們的配置實務範例中，我們參照主電腦名稱爲 iSeriesA.ordept.myco.com 的 iSeries。爲了讓從屬站取得服務通行證來提出給此 iSeries，必須以 KDC 定義主體 krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM。

z/OS
請參考 **Kadmin** 指令的文件。

Windows (R) 2000 伺服器

1. 使用 Active Directory (R) 管理工具來建立 iSeries 使用者帳戶。將 iSeries 名稱指定爲 Active Directory 使用者。例如，有效的名稱可爲 iSeriesA。
2. 存取您在步驟 1 所建立 Active Directory 使用者的內容。從**帳戶**標籤上，選取 **帳戶受信任可以委派**。這可讓 iSeries 服務主體代表登入使用者以存取其它服務。
3. 使用 **ktpass** 指令，將使用者帳戶對映到主體。例如，您可以輸入下列指令：
   ```
   ktpass -princ krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM -mapuser iSeriesA -pass xxxxxx
   ```
   其中 xxxxxx 是您在網路鑑別服務配置期間所指定的密碼。

下一個步驟？

建立起始目錄 ≪

建立起始目錄

≫

已將 iSeries 定義到金鑰分送中心後，您必須爲每一個將連接至 iSeries 與 iSeries 應用程式的使用者建立 /home 目錄。此目錄將包含使用者的 Kerberos 認證快取名稱。若要爲使用者建立起始目錄，請完成下列步驟：

在 iSeries 指令行上，輸入：

```
CRTDIR '/home/username'
```
其中 username 爲使用者的 iSeries 使用者名稱。

下一個步驟：

驗證 TCP/IP 網域資訊

≪

驗證 TCP/IP 網域資訊

≫ 建立起始目錄之後，您應驗證伺服器已有正確的主電腦表格登錄。

1. 在 iSeries 指令行上，輸入：
   ```
   CFGTCP
   ```
2. 選取「選項 10」(使用 TCP/IP 主電腦表格登錄)。
3. 在主電腦名稱欄位中，請驗證 iSeries A 的完整主電腦名稱是小寫。若有多個主電腦名稱登錄，亦請驗證是否先出現完整主電腦名稱。例如，iSeries A 的主電腦名稱登錄應爲：iseriesa.ordept.myco.com。
4. 驗證主電腦名稱登錄之後，請按 F3 返回「配置 TCP」主功能表。
5. 選取「選項 12」(變更 TCP/IP 網域資訊)。
6. 驗證系統名稱是否出現在主電腦名稱欄位中。亦請驗證網域名稱是否正確。例如，主電腦名稱可以是 iseriesa，而網域名稱可以是 ordept.myco.com。

下一個步驟：

測試網路鑑別服務配置

測試網路鑑別服務配置

驗證正確的網域資訊之後，您可藉由要求授予 iSeries 主體名稱的通行證，測試網路鑑別服務配置：

1. 在指令行上，輸入 QSH 來啓動 Qshell 直譯器。
2. 輸入 keytab list 來顯示 keytab 檔中登記的主體清單。例如，有效的主體名稱可以是 krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM。
3. 輸入 kinit -k krbsvr400/system.domain@realm。例如，krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM 是 iSeries 的有效主體名稱。若此順利完成，QSH 指令會顯示無誤。
4. 輸入 klist，驗證預設主體是否爲 krbsvr400/system.domain@realm。

下一個步驟：

配置「企業識別對映 (EIM)」
若您搭配您自己的應用程式來使用網路鑑別服務，此步驟爲選用性。不過，建議搭配使用原有的 iSeries 應用程式來管理網路中的多重使用者 ID。

管理網路鑑別服務

於配置網路鑑別服務後，您可以要求通行證、使用金鑰表格檔以及管理領域信任關係。您也可以使用認證檔及備份配置檔。下列主題說明如何完成這些作業：

管理者作業

下列爲「iSeries 領航員」中管理者可執行的簡要作業清單。如需基本作業詳細資訊，請參閱網路鑑別服務的「iSeries 領航員」說明。除了這些作業之外，管理者需要確定使用者已使用 kdestroy 指令刪除舊認證。

- 同步化系統時間
  若要在 iSeries 和 KDC 之間交換通行證，系統時間彼此的差距必須在 5 分鐘內。您可以從網路鑑別服務「內容」中配置最大時鐘差值。預設的最大時鐘差值爲 5 分鐘或 300 秒。此主題說明如何同步化系統時間。
-
- 新增領域
  此主題說明如何新增領域至網路鑑別服務配置。
-
- 刪除領域
  此主題說明如何從網路鑑別服務配置中移除領域。
-
- 新增金鑰分送中心至領域
  此主題說明如何將金鑰分送中心新增至現行網路鑑別服務配置中。

- 新增密碼伺服器
  此主題說明如何新增密碼伺服器至網路鑑別服務配置中，讓使用者可變更他們的 Kerberos 密碼。
- 建立領域之間的信任關係
  此主題說明如何設定領域之間的信任關係。此功能是可選用的，因爲依預設，Kerberos 通信協定會在領域階層中尋找信任。不過，若您有不同網域中的領域且想要加快這個程序，此功能很有用。
- 變更主電腦解析
  此主題說明如何變更領域名稱的主電腦解析。
- 新增加密設定值
  此主題說明如何新增通行證授予通行證 (TGT) 及通行證授予服務 (TGS) 的加密類型。

iSeries 使用者作業

iSeries 也可作爲 Kerberos 型網路中的從屬站。使用者可登入 iSeries 並透過「Qshell 直譯器」執行 Kerberos 相關作業。下列作業使用數個 Qshell 指令來執行 iSeries 使用者的一般作業。

- 建立起始目錄
  此主題說明如何建立起始目錄。
- 取得新的通行證授予通行證
  此主題說明如何使用 **kinit** Qshell 指令來取得或更新通行證授予通行證。
- 變更 Kerberos 密碼
  此主題說明如何使用 Qshell 指令 **kpasswd** 來變更密碼。
- 管理 keytab 檔
  此主題說明如何使用 Qshell 指令 **keytab** 來管理 keytab 檔。
- 刪除已過期認證快取
  此主題說明如何使用 **kdestroy** Qshell 指令來刪除儲存於從屬站的已過期認證快取。使用者定期刪除他們的認證快取很重要。
- 顯示認證快取或 keytab 檔
  此主題說明如何使用 **klist** Qshell 指令來列出與使用者相關的認證及 keytab 檔。
- 管理 LDAP 目錄中的 Kerberos 服務登錄
  此主題說明如何使用 **ksetup** QSHELL 指令來管理 LDAP 目錄中的 Kerberos 服務登錄。

同步化系統時間

網路鑑別服務以 5 分鐘 (300 秒) 作爲系統時間最大時差預設值。您可以使用網路鑑別服務內容來變更時差。

在同步化系統時間之前，請根據您的時區使用 QUTCOFFSET 系統值來設定系統時間。您可以變更 KDC 時間或使用 QTIME 系統值來變更 iSeries 系統時間，藉以同步化這些系統時間。不過，若要保持網路中的系統時間同步，您應該配置「簡易網路時間通信協定 (NTP)」。SNTP 允許多重系統根據單一時間伺服器來設定它們的時間。若要配置 SNTP，請完成下列步驟：

若要在 iSeries 上配置 SNTP，請在指令行輸入 CHGNTPA。

若要在 Windows (R) 系統上配置 SNTP，請使用 **NET HELP TIME** 來顯示 SNTP 伺服器配置資訊。

新增領域

身爲網路管理者，您可能想要新增領域至網路鑑別服務配置中。在新增領域至 iSeries 配置之前，必須對新領域配置 KDC。在新增領域至 iSeries 網路鑑別服務作業之前，您需要領域名稱、KDC 名稱及 KDC 接收埠。

若要新增領域至網路鑑別服務，請完成下列步驟：

1. 在「iSeries 領航員」中，選取**您的 iSeries 伺服器** —> **安全性** —> **網路鑑別服務**。
2. 以滑鼠右鍵按一下**領域**，然後選取**新增領域**。
3. 在**要新增的領域**欄位中，輸入您要新增的領域之主電腦名稱。例如，有效的領域名稱可爲 ORDEPT.MYCO.COM。
4. 輸入您要新增領域的 KDC 名稱。例如，有效的 KDC 名稱可爲 kdc1.ordept.myco.com。
5. 輸入 KDC 接收要求的埠號。有效的埠號範圍是 1-65535。KDC 的預設埠號爲 88。
6. 按一下**確定**。

刪除領域

身爲網路管理者，您可能想要從網路鑑別服務配置中刪除領域。領域可能不再需要或使用於網路上。您可能也需要移除預設領域，才能夠從一些 iSeries 原有的應用程式問題中恢復。

例如，如果您已配置網路鑑別服務但未在網路中設定 KDC，QFileSvr.400 和「分散式資料管理 (DDM)」將假設您是使用 Kerberos 鑑別。在設定鑑別這些產品前，您應該刪除網路鑑別服務配置期間所指定的預設領域。

若要刪除網路鑑別服務的領域，請完成下列步驟：

1. 在「iSeries 領航員」中，展開**您的 iSeries 伺服器** —> **安全性** —> **網路鑑別服務** —> **領域**。
2. 以滑鼠右鍵按一下要刪除的領域名稱，然後選取**刪除**。
3. 按一下**確定**以確認刪除。

將金鑰分送中心新增至一個領域

» 身爲網路管理者，您可以利用網路鑑別服務來將金鑰分送中心 (KDC) 新增至領域。在將 KDC 新增至領域之前，您必須知道 KDC 名稱及其接收埠。

若要將金鑰分送中心新增至領域中，請完成下列步驟：

1. 在「iSeries 領航員」中，展開**您的 iSeries 伺服器** —> **安全性** —> **網路鑑別服務** —> **領域**。
2. 以滑鼠右鍵按一下右窗格中的領域名稱，然後選取**內容**。
3. 在**一般**標籤上，輸入要新增至此領域中的 KDC 名稱。所有領域都需要 KDC。例如，kdc2.ordept.myco.com 是一個有效的登錄。
4. 輸入 KDC 接收要求的埠號。有效的埠號範圍是 1-65535。KDC 的預設埠號爲 88。
5. 按一下**新增**。在**此領域的「金鑰分送中心 (KDC)」**清單中出現新的 KDC。
6. 按一下**確定**。

«

新增密碼伺服器

»

密碼伺服器允許 Kerberos 主體變更它們的密碼。若要將密碼伺服器新增至領域，請完成下列步驟：

1. 在「iSeries 領航員」中，展開**您的 iSeries 伺服器** —> **安全性** —> **網路鑑別服務** —> **領域**。
2. 以滑鼠右鍵按一下右窗格中的領域名稱，然後選取**內容**。
3. 在**密碼伺服器**標籤上，輸入密碼伺服器名稱。例如，密碼伺服器的有效名稱可爲 psvr.ordept.myco.com。
4. 輸入密碼伺服器對應的埠號。有效的埠號範圍是 1-65535。密碼伺服器的預設埠號爲 464。
5. 按一下**新增**。新密碼伺服器將新增至清單中。
6. 按一下**確定**。

«

建立領域之間的信任關係

» 建立領域之間的信任關係可產生鑑別捷徑。此功能是可選用的，因爲依預設，Kerberos 通信協定會在領域階層中尋找信任。如果您有不同網域中的領域且想要讓這個程序加快速度，此功能很有用。若要設定領域信任，每個領域的 KDC 必須共用金鑰。在建立信任關係之前，您必須設定 KDC 來彼此信任。若要建立領域之間的信任關係，請完成下列步驟：

1. 在「iSeries 領航員」中，展開**您的 iSeries 伺服器** —> **安全性** —> **網路鑑別服務** —> **領域**。
2. 以滑鼠右鍵按一下右窗格中的領域名稱，然後選取**內容**。
3. 在**信任的領域**標籤中，輸入要建立信任的領域名稱。例如，信任關係的有效名稱可爲 NY.myco.com 和 LA.myco.com。
4. 按一下**新增**。這會在表格中新增信任關係。
5. 按一下**確定**。

«

變更主電腦解析

» 透過網路鑑別服務，您可以指定將目錄服務 (LDAP) 伺服器、網域名稱系統 (DNS) 及靜態對映新增至配置檔中，來解析主電腦名稱和領域名稱。您也可以選取所有三個方法來解析主電腦名稱。如果您選取所有這些方法，網路鑑別服務會先檢查目錄伺服器，接著是 DNS 登錄，最後是靜態對映，來解析主電腦名稱。

若要變更主電腦解析，請完成下列步驟：

1. 在「iSeries 領航員」中，展開**您的 iSeries 伺服器** —> **安全性**。
2. 以滑鼠右鍵按一下**網路鑑別服務**，然後選取**內容**。
3. 在**主電腦解析**頁上，選取**使用 LDAP 查閱**、**使用 DNS 查閱**，及/或**使用靜態對映**。
4. 如果您選取**使用 LDAP 查閱**作爲主電腦解析類型，請輸入目錄伺服器名稱及其對應埠。例如，ldapsrv.ordept.myco.com 可爲目錄伺服器的有效名稱。有效的埠號範圍是 1-65535。目錄伺服器的預設埠號爲 389。
5. 如果您選取**使用 DNS 查閱**作爲主電腦解析類型，則必須配置 DNS 來對映至領域名稱。
6. 如果您選取**使用靜態對映**爲主電腦解析類型，請輸入領域名稱及其對應 DNS 名稱。例如，主電腦名稱可爲 mypc.mycompanylan.com，而領域名稱爲 ORDEPT.MYCO.COM。您也可以將同屬主電腦名稱對映至特定領域。例如，如果以 myco.lan.com 爲結尾的所有機器屬於 ORDEPT.MYCO.COM，您可以輸入 `myco.lan.com` 作爲 DNS 名稱，並輸入 ORDEPT.MYCO.COM 作爲領域。這會在配置檔中建立領域名稱與 DNS 名稱間的關聯。按一下**新增**，在配置檔中建立 DNS 與領域名稱間的靜態對映。
7. 輸入所選取主電腦解析類型的相關資訊後，按一下**確定**。

«

新增加密設定值

» 您可以對通行證授予通行證 (TGT) 及通行證授予服務 (TGS) 選取加密類型。加密使資料無法被識別，來隱藏網路中傳輸的資料。從屬站會加密資料，而伺服器會解密資料。爲確保加密正確運作，您必須使用 KDC 或其它通信應用程式上指定的相同加密類型。如果這些加密類型不符，加密將會失敗。您可以對 TGT 和 TGS 新增加密值。**註**：TGT 和 TGS 的預設加密值爲 des-cbc-crc 和 des-cbc-md5。在配置期間已設定預設加密值。若要將通行證的其它加密值新增至配置，請完成下列步驟：

1. 在「iSeries 領航員」中，展開**您的 iSeries 伺服器** —> **安全性**。
2. 以滑鼠右鍵按一下**網路鑑別服務**，然後選取**內容**。
3. 在**通行證**頁上，從可用的加密類型的「通行證授予通行證」或「通行證授予服務」清單中選取加密值。
4. 按一下**加在前面**或**加在後面**，將加密類型新增至所選取的加密類型清單中。將依列示的順序嘗試使用所選取的每一個這些加密類型。如果一個加密類型失敗，便會嘗試清單中的下一個加密類型。
5. 按一下**確定**。

«

取得或更新通行證授予通行證

» **kinit** 指令可取得或更新 Kerberos 通行證授予通行證。如果未對 **kinit** 指令指定任何通行證選項，則使用 Kerberos 配置檔中指定的 KDC 選項。

若未更新現有的通行證，則認證快取會重新起始設定並包含接收自 KDC 的新通行證授予通行證。如果未在指令行指定主體名稱，則從認證快取中取得主體名稱。除非以 `-c` 選項指定快取名稱，否則新認證快取會成爲預設認證快取。

通行證時間值以 *nwndnhnmns* 表示，其中 *n* 代表數字，*w* 表示週數，*d* 表示天數，*h* 表示時數，*m* 表示分鐘數，而 *s* 表示秒數。這些元件必須以此順序指定，但可省略任何元件 (例如，*4h5m* 代表 4 小時又 5 分鐘，而 *1w2h* 代表 1 週又 2 小時)。如果僅指定一個數字，則預設爲小時。

若要爲 Jsmith 這個主體取得具有 5 小時使用期限的通行證授予通行證：

在 Qshell 指令行上，輸入：

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

或

在 iSeries 指令行，輸入：

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

有關特定用法和限制，請參閱此 Qshell 指令的 用法注意事項。

kinit

語法

```
kinit [-r time] [-R] [-p] [-f] [-A] [-l time] [-c cache] [-k] [-t keytab] [principal]
```

預設公用權限：*USE

Qshell 指令 **kinit** 可取得或更新 Kerberos 通行證授予通行證。

選項

-r time
更新通行證的時間間隔。此間隔到期後即無法再更新通行證。更新時間必須大於結束時間。如果未指定此選項，則無法更新通行證 (如果所要求的通行證使用期限超出最大通行證使用期限，還是會產生可更新的通行證)。

-R
更新現有的通行證。當更新現有的通行證時，您無法指定其它任何通行證選項。

-p
通行證可爲 proxy。如果未指定此選項，則通行證不能爲 proxy。

-f
通行證可轉遞。如果未指定此選項，則無法轉遞通行證。

-A
通行證不含從屬站位址清單。如果未指定此選項，則通行證將含有本端主電腦位址清單。當起始通行證含有位址清單時，則只能從位址清單的其中一個位址使用它。

-l time
通行證終止時間間隔。此間隔到期後，通行證即無法使用，直到它更新爲止。如果未指定此選項，間隔設爲 10 小時。

-c cache
kinit 指令將使用的認證快取名稱。如果未指定此選項，此指令使用預設認證快取。

-k
會從金鑰表格取得通行證主體的金鑰。如果未指定此選項，系統會提示您輸入通行證主體的密碼。

-t keytab
金鑰表格名稱。如果未指定此選項但指定了 -k 選項，則系統使用預設金鑰表格。-t 選項暗指 -k 選項。

主體
通行證主體。如果沒有在指令行指定主體，系統會從認證快取中取得主體。

權限

參照到的物件	必要的權限
若指定了 -t 選項，則指路徑名稱中位於金鑰表格檔之前的每一個目錄	*X
當指定 -t 時，指金鑰表格檔	*R
路徑名稱中位於所要使用的認證快取檔之前的每一個目錄	*X
如果以 **KRB5CCNAME** 環境變數指定且檔案已建立，則指所要使用的快取檔的上層目錄	*WX
認證快取檔	*RW
配置檔路徑中的每一個目錄	*X
配置檔	*R

爲了讓 Kerberos 執行時間能夠從任何執行中程序尋找您的認證快取檔，快取檔名通常儲存於 **krb5ccname** 檔的起始目錄中。藉由設定環境變數 **_EUV_SEC_KRB5CCNAME_FILE** 可置換快取檔名的儲存體位置。若要存

取此檔案，使用者設定檔必須對路徑中的每個目錄擁有 ***X** 權限，以及對儲存快取檔名的檔案擁有 ***R** 權限。使用者首次建立認證快取時，使用者設定檔必須擁有上層目錄的 ***WX** 權限。

訊息

- option_name 選項需要一值。
- command_option 不是有效的指令選項。
- 更新或驗證通行證時不允許任何選項。
- 無法取得預設認證快取名稱。
- 無法解析認證快取 file_name。
- 沒有可用的起始通行證。
- 必須指定主體名稱。
- 無法從認證快取 file_name 中擷取通行證。
- 起始通行證無法更新。
- option_value 選項不適用 request_name 要求。
- 無法取得起始認證。
- 無法剖析主體名稱。
- 無法解析金鑰表格 file_name。
- principal_name 的密碼不正確。
- 無法讀取密碼。
- 無法將起始認證儲存於認證快取 file_name 中。
- 時間差異值無效。

有關如何使用此指令的範例，請參閱取得或更新通行證授予通行證。

顯示認證快取或 keytab 檔

klist 指令可顯示 Kerberos 認證快取或金鑰表格的內容。

若要列出預設認證快取中所有登錄及顯示通行證旗號：

在 Qshell 指令行上，輸入

```
klist -f -a
```

或

在 iSeries 指令行上，輸入

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

有關特定用法和限制，請參閱此 Qshell 指令的用法注意事項。

klist

語法

```
klist [-a] [-e] [-c] [-f] [-s] [-k] [-t] [-K] [filename]
```
預設公用權限：*USE

Qshell 指令 **klist** 可顯示 Kerberos 認證快取或金鑰表格的內容。

選項

-a
顯示認證快取中所有通行證，包括過期的通行證。如果未指定此選項，則不列出過期的通行證。此選項僅在列出認證快取時有效。

-e
顯示階段作業金鑰和通行證的加密類型。此選項僅在列出認證快取時有效。

-c
列出認證快取中的通行證。若尚未指定 `-c` 和 `-k` 選項，此爲預設值。此選項與 `-k` 選項互斥。

-f
以下列縮寫顯示通行證旗號：

縮寫	意義
F	可轉遞通行證
f	轉遞的通行證
P	通行證可爲 proxy
p	Proxy 通行證
D	可延期通行證
d	可延期的通行證
R	可更新通行證
I	起始通行證
i	通行證無效
A	使用事先鑑別
O	伺服器可爲代表
C	由 KDC 檢查轉移清單

此選項僅在列出認證快取時有效。

-s
抑制指令輸出，但如果在認證快取中找到有效通行證授予通行證，則跳出狀態設爲 0。 此選項僅在列出認證快取時有效。

-k
列出金鑰表格中的登錄。此選項與 **-c** 選項互斥。

-t
顯示金鑰表格登錄的時間戳記。此選項僅在列出金鑰表格時有效。

-K
顯示每個金鑰表格登錄的加密金鑰值。此選項僅在列出金鑰表格時有效。

檔名
指定認證快取或金鑰表格的名稱。如果未指定檔名，則使用預設認證快取或金鑰表格。

權限

參照到的物件	必要的權限
如果 -k 選項指定爲 keytab，則指路徑名稱中位於檔案之前的每一個目錄	*X
當指定 -k 時，指 keytab 檔	*R
若未指定 -k 選項，則指路徑名稱中位於認證快取檔之前的每一個目錄	*X
如果未指定 -k 選項，則指定認證快取檔	*R

爲了讓 Kerberos 執行時間能夠從任何執行中程序尋找您的認證快取檔，快取檔名通常儲存於 **krb5ccname** 檔的起始目錄中。藉由設定 **_EUV_SEC_KRB5CCNAME_FILE** 環境變數，可置換快取檔名的儲存體位置。若要存取此檔案，使用者設定檔必須對路徑中的每個目錄擁有 ***X** 權限，以及對儲存快取檔名的檔案擁有 ***R** 權限。使用者首次建立認證快取時，使用者設定檔必須擁有上層目錄的 ***WX** 權限。

訊息

- option_name 選項需要一值。
- command_option 不是有效的指令選項。
- command_option_one 和 command_option_two 無法一起指定。
- 找不到預設認證快取。
- 無法解析認證快取 file_name。
- 無法從認證快取 file_name 中擷取主體名稱。
- 無法從認證快取 file_name 中擷取通行證。
- 無法將通行證解碼。
- 找不到預設金鑰表格。
- 無法解析金鑰表格 file_name。

有關如何使用此指令的範例，請參閱顯示認證快取或 keytab 檔。

管理 keytab 檔

keytab 指令用來新增或刪除金鑰表格中的金鑰，或顯示金鑰表格中的登錄。

例如，要對 ORDEPT.MYCO.COM 領域中的 kdc1.ordept.myco.com 主電腦上的服務主體 krbsvr400 新增金鑰：

在 Qshell 指令行上，輸入

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

或

在 iSeries 指令行，輸入

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

將會提示您輸入服務定義給 KDC 時所使用的密碼。

有關特定用法和限制，請參閱此 Qshell 指令的用法注意事項。

keytab

語法

```
keytab add principal [-p password] [-v version] [-k keytab] keytab delete principal [-v version]
[-k keytab] keytab list [principal] [-k keytab]
```

預設公用權限：*USE

Qshell 指令 **keytab** 可管理金鑰表格。

選項

-k
金鑰表格名稱。如果未指定此選項，則使用預設金鑰表格。

-p
指定密碼。如果未指定此選項，則當使用者新增登錄至金鑰表格時，會被提示輸入密碼。

-v
金鑰版本號碼。當您新增金鑰時，如果未指定此選項，則指定下一個版本號碼。當您刪除金鑰時，如果未指定此選項，則主體的所有金鑰會被刪除。

主體
主體名稱。當您列出金鑰表格時，如果未指定此選項，則會顯示所有主體。

權限

參照到的物件	必要的權限
路徑名稱中位於所要開啓的目標 keytab 檔前的每一個目錄	*X
如果 keytab 檔尚未存在，則是指定新增時的目標 keytab 檔的上層目錄	*WX
指定清單時的 Keytab 檔	*R
指定新增或刪除時的目標 keytab 檔	*RW
配置檔路徑中的每一個目錄	*X
配置檔	*R

訊息

- 您必須指定*新增*、*刪除*、*列出*或*合併*。
- *command_option* 不是有效的指令選項。
- *command_option_one* 和 *command_option_two* 無法一起指定。
- *option_value* 選項不適用 *request_name* 要求。
- *option_name* 選項需要一值。
- 無法剖析主體名稱。
- 您必須指定主體名稱。
- 無法讀取密碼。
- 找不到預設金鑰表格。
- 無法解析金鑰表格 *key_table*。
- 無法從金鑰表格 *key_table* 中讀取登錄。
- 無法從金鑰表格 *key_table* 中移除登錄。
- 無法新增登錄至金鑰表格 *key_table*。
- 找不到主體 *principal_name* 的登錄。
- 值不是一個有效的號碼。
- 金鑰版本必須介於 1 和 255 之間。
- 找不到主體 *principal_name* 的金鑰版本 *key_version*。

有關如何使用此指令的範例，請參閱管理 keytab 檔。

變更 Kerberos 密碼

kpasswd 指令可利用密碼變更服務來變更指定 Kerberos 主體的密碼。您必須提供主體的現行密碼及新密碼。在變更密碼之前，密碼伺服器會將任何適用的密碼原則規則套用至新密碼。密碼伺服器是在 KDC 安裝與配置期間完成配置。請參閱該系統所對應的文件。在網路鑑別服務配置期間，您可以指定密碼伺服器的名稱。如果於配置期間未指定，您可以新增密碼伺服器。

您不可使用 **kpasswd** 指令來變更通行證授予服務主體 (krbtgt/realm) 的密碼。

變更預設主體的密碼：

在 Qshell 指令行上，輸入

```
kpasswd
```

或

在指令行上，輸入

```
call qsys/qkrbkpsswd
```

變更另一個主體的密碼：

在 Qshell 指令行上，輸入

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

或

在指令行上，輸入

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

有關使用此指令的詳細資訊，請參閱 kpasswd 用法注意事項。

kpasswd

語法

```
kpasswd [-A ] [principal]
```

預設公用權限：*USE

Qshell 指令 kpasswd 可變更 kerberos 主體的密碼。

選項

-A kpasswd 指令使用的起始通行證將不含從屬站位址清單。如果未指定此選項，則通行證將含有本端主電腦位址清單。當起始通行證含有位址清單時，則只能從位址清單的其中一個位址使用它。

主體 要變更密碼的主體。如果指令行上未指定主體，則會從預設認證快取中取得主體。

訊息

- 主體 %3$s 無效。
- 無法讀取預設認證快取 file_name。
- 無預設認證快取。
- 無法從認證快取 file_name 中擷取通行證。
- 無法讀取密碼。
- 已取消密碼變更。
- principal_name 的密碼不正確。
- 無法取得起始通行證。
- 密碼變更要求失敗。

有關如何使用此指令的範例，請參閱變更 Kerberos 密碼。

刪除已過期認證快取檔

kdestroy 指令可刪除 Kerberos 認證快取檔。使用者必須定期使用 kdestroy 指令來刪除舊認證。

-e 選項可讓 **kdestroy** 指令檢查預設快取目錄 (**/QIBM/UserData/OS400/NetworkAuthentication/creds**) 中所有認證快取檔。任何僅含有過期時間達 *time_delta* 之久的已過期通行證之檔案會被刪除。*time_delta* 表示爲 *nwndnhnmns*，其中 *n* 代表數字，*w* 表示週數，*d* 表示天數，*h* 表示時數，*m* 表示分鐘數，而 *s* 表示秒數。這些元件必須以此順序指定，但可省略任何元件 (例如，*4h5m* 代表 4 小時又 5 分鐘，而 *1w2h* 代表 1 週又 2 小時)。如果僅指定一個數字，則預設爲小時。

刪除預設認證快取：
在 Qshell 指令行上，輸入

```
kdestroy
```

或

在 iSeries 指令行上，輸入

```
call qsys/qkrbkdstry
```

刪除具有超過 1 天的過期通行證之所有認證快取檔：

在 Qshell 指令行上，輸入

```
kdestroy -e 1d
```

或

在 iSeries 指令行上，輸入

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

有關特定用法和限制，請參閱此 Qshell 指令的用法注意事項。

kdestroy

語法

```
kdestroy [-c cache_name] [-e time_delta]
```
預設公用權限：*USE

Qshell 指令 **kdestroy** 損毀 Kerberos 認證快取。

選項

-c cache_name
要損毀的認證快取名稱。如果未指定指令選項，則會損毀預設認證快取。此選項與 -e 選項互斥。

-e time_delta
如果通行證過期的時間至少像 time_delta 值那麼久，則含有過期通行證的所有認證快取檔會被刪除。

權限

當認證快取類型爲 **FILE** (有關快取類型的詳細資訊，請參閱 **krb5_cc_resolve()**) 時，預設行爲是在 /QIBM/UserData/OS400/NetworkAuthentication/creds 目錄下建立認證快取檔。藉由設定 KRB5CCNAME 環境變數可變更認證快取檔的位置。

如果認證快取檔不是位於預設目錄下，則需要下列權限：

參照到的物件	需要資料權限	需要物件權限
路徑名稱中位於認證快取檔前的每一個目錄	*X	無
認證快取檔的上層目錄	*WX	無
認證快取檔	*RW	*OBJEXIST

參照到的物件	需要資料權限	需要物件權限
配置檔路徑中的每一個目錄	*X	無
配置檔	*R	無

如果認證快取檔位於預設目錄下，則需要下列權限：

參照到的物件	需要資料權限	需要物件權限
路徑名稱中的所有目錄	*X	無
認證快取檔	*RW	無
配置檔路徑中的每一個目錄	*X	無
配置檔	*R	無

爲了讓 Kerberos 通信協定從任何執行中程序尋找您的認證快取檔，快取檔名稱通常儲存於 krb5ccname 檔的起始目錄中。想要對 iSeries 使用 Kerberos 鑑別的使用者必須有定義起始目錄。依預設，起始目錄爲 /home/。如果未指定任何指令選項，此檔案用來尋找預設認證快取。藉由設定 _EUV_SEC_KRB5CCNAME_FILE 環境變數可置換快取檔名的儲存體位置。若要存取此檔案，使用者設定檔必須對路徑中每個目錄擁有 ***X** 權限，以及對儲存快取檔名的檔案擁有 ***R** 權限。

訊息

- 無法解析認證快取 *cache_file_name*。
- 無法損毀認證快取 *cache_file_name*。
- *function_name* 功能偵測到錯誤。
- 無法從認證快取 *file_name* 中擷取通行證。
- *option_name* 選項需要一值。
- *command_option* 不是有效的指令選項。
- *command_option_one* 和 *command_option_two* 不可一起指定。
- 找不到預設認證快取。
- 時間差值 *value* 無效。

有關如何使用此指令的範例，請參閱刪除過期的認證快取檔。

管理 LDAP 目錄中的 Kerberos 服務登錄

ksetup 指令可管理 LDAP 目錄中的 Kerberos 服務登錄。下列爲支援的次指令：

addhost host-name realm-name
這個次指令可對指定的領域新增主電腦登錄。無論在 Kerberos 從屬站上哪一個預設 DNS 網域有效，應使用完整主電腦名稱才能正確解析。如果未指定領域名稱，則使用預設領域名稱。

addkdc host-name:port-number realm-name

這個次指令可對指定的領域新增 KDC 登錄。如果主電腦登錄尚不存在，則會建立它。如果未指定埠號，則預設爲 88。無論 Kerberos 從屬站上哪一個預設 DNS 網域有效，應使用完整主電腦名稱才能正確解析。如果未指定領域名稱，則使用預設領域名稱。

delhost host-name realm-name
這個次指令可從指定的領域刪除主電腦登錄及任何相關的 KDC 規格。如果未指定領域名稱，則使用預設領域名稱。

delkdc host-name realm-name
此次指令可刪除指定主電腦的 KDC 登錄。主電腦登錄本身不會被刪除。如果未指定領域名稱，則使用預設領域名稱。

listhost realm-name
此次指令可列出領域的主電腦登錄。如果未指定領域名稱，則使用預設領域名稱。

listkdc realm-name
此次指令可列出領域的 KDC 登錄。如果未指定領域名稱，則使用預設領域名稱。

exit
此次指令可結束 ksetup 指令。

範例

若要使用 Administrator 這個 Directory Services (LDAP) 管理者 ID 及 verysecret 這個密碼，將 kdc1.ordept.myco.com 主電腦新增至 ldapserv.ordept.myco.com 伺服器作爲 ORDEPT.MYCO.COM 領域的 KDC，請完成下列步驟：

在 Qshell 指令行，輸入： `ksetup -h ldapserv.ordept.myco.com -n CN=Administrator -p verysecret`

或

1. 在 iSeries 指令行，輸入：

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

2. 當順利聯絡上 Directory Services (LDAP) 伺服器時，會顯示次指令提示。輸入

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

有關特定用法和限制，請參閱此 Qshell 指令的用法注意事項。

ksetup

語法

```
ksetup -h host-name -n bind-name -p bind-password -e
```
預設公用權限：*USE

Qshell 指令 **ksetup** 可管理 Kerberos 領域中之「目錄服務 (LDAP)」目錄中的 Kerberos 服務登錄。

選項

-h
「目錄服務 (LDAP)」伺服器的主電腦名稱。如果未指定此選項，則使用 Kerberos 配置檔中指定的「目錄服務 (LDAP)」伺服器。

-n
連結至「目錄服務 (LDAP)」伺服器時使用的識別名稱。如果未指定此選項，則使用目錄服務 (LDAP)_BINDDN 環境變數來取得此名稱。

-p
連結至「目錄服務 (LDAP)」伺服器時使用的密碼。如果未指定此選項，則使用目錄服務 (LDAP)_BINDPW 環境變數來取得此密碼。

-e
使每一個指令行回應在 stdout 上。當將 stdin 重新導向至檔案時非常有用。

權限

參照到的物件	必要的權限
配置檔路徑中的每一個目錄	*X
配置檔	*R

訊息

- `subcommand` 不是有效的次指令。
- 有效的次指令爲 `addhost`、`addkdc`、`delhost`、`delkdc`、`listhost`、`listkdc`、`exit`。
- `command_option_one` 和 `command_option_two` 無法一起指定。
- 無法起始設定 LDAPclient。
- 無法連結至「目錄服務 (LDAP)」伺服器。
- 必須指定領域名稱。
- 必須指定主電腦名稱。
- 定位參數太多。

- 主電腦 host 已存在。
- 未定義根網域 domain。
- 領域名稱 realm 無效。
- LDAP function name 函數偵測到錯誤。
- 可用儲存體不足。
- 主電腦名稱 host 無效。
- 埠號 port 無效。
- 未定義主電腦 host。
- 未對主電腦 host 定義 KDC。
- 無法取得預設領域名稱。

有關如何使用此指令的範例，請參閱管理 LDAP 目錄中的 Kerberos 服務登錄。

網路鑑別服務疑難排解

本節提供網路鑑別服務、企業識別對映 (EIM) 及支援 Kerberos 鑑別的 iSeries 原始應用程式一般問題的疑難排解資訊鏈結。

1. 已完成所有先決條件。
2. 請確定使用者有 iSeries 上的使用者設定檔及 KDC 上的主體名稱。在 iSeries 上，開啓「iSeries 領航員」中的「使用者與群組」或在指令行使用 WRKUSRPRF，來驗證使用者是否存在。在 Windows (R) 系統上，存取 Active Directory (R) Users and Computers 資料夾來驗證使用者是否存在。
3. 從「Qshell 直譯器」中使用 kinit 指令，檢查 iSeries 是否在聯繫 KDC。如果 kinit 失敗，請檢查 iSeries 服務主體是否已在 KDC 上完成登記。如果尚未登記，您可以新增 iSeries 主體名稱至 KDC。

有關特定訊息的資訊，請參閱下列主題：

- 網路鑑別服務錯誤和回復
  在網路鑑別服務精靈期間或在「iSeries 領航員」中管理網路鑑別服務內容時，您可能會遇到這些訊息。
- 應用程式連線錯誤和回復
  此主題討論當應用程式使用網路鑑別服務、EIM 及一些 iSeries 原始應用程式時，可能在 iSeries、服務或使用者嘗試連接 KDC 時發生的一般錯誤訊息。

網路鑑別服務錯誤和回復

在網路鑑別服務精靈期間或在「iSeries 領航員」中管理網路鑑別服務內容時，您可能會遇到這些訊息。

訊息	回復
KRBWIZ_CONFIG_FILE_FORMAT_ERROR 「網路鑑別服務」配置檔「格式」錯誤。	重新配置網路鑑別服務。詳細資料，請參閱配置網路鑑別服務。

KRBWIZ_CRYPTO_NOT_INSTALLED
系統上未安裝必要的加密產品。

請在系統上安裝「密碼存取提供者 (572-AC3)」。

KRBWIZ_ERROR_READ_CONFIG_FILE
讀取網路鑑別服務配置檔發生錯誤。

重新配置網路鑑別服務。詳細資料，請參閱配置網路鑑別服務。

KRBWIZ_ERROR_WRITE_CONFIG_FILE
寫入網路鑑別服務配置檔發生錯誤。

用來撰寫配置檔的服務無法使用。請稍後重試。

KRBWIZ_PASSWORD_MISMATCH
新密碼和確認新密碼不同

請重新輸入新密碼並確認新密碼。

KRBWIZ_PORT_ERROR
埠號必須介於 1 和 65535 之間。

請重新輸入介於 1 和 65535 之間的埠號。

KRBWIZ_ERROR_WRITE_KEYTAB
寫入金鑰表格檔發生錯誤

用來撰寫 keytab 的服務暫時無法使用。請稍後重試。

KRBWIZ_NOT_AUTHORIZED_CONFIGURE
未授權配置「網路鑑別服務」。

請確定您擁有下列權限：*ALLOBJ 和 *SECADM。

KrbPropItemExists
項目已存在。

請輸入新項目。

KrbPropKDCInListRequired
清單中必須有 KDC。

指定的 KDC 不在清單中。請從清單中選取 KDC。

KrbPropKDCValueRequired
必須輸入 KDC 名稱。

請輸入有效的 KDC 名稱。網路的安全系統上必須配置 KDC。

KrbPropPwdServerRequired
必須輸入密碼伺服器名稱。

請輸入有效的密碼伺服器名稱。

KrbPropRealmRequired
必須輸入領域名稱。

請輸入此系統所屬的領域名稱。

KrbPropRealmToTrustRequired
必須輸入領域所信任的名稱。

請輸入正在建立信任關係的領域名稱。

KrbPropRealmValueRequired
必須輸入領域名稱。

請輸入有效的領域名稱。

CPD3E3F
發生「網路鑑別服務」錯誤 &2。

請參閱對應此訊息的特定回復資訊。

應用程式連線問題和回復

當應用程式使用網路鑑別服務時，您可能會遇到這些訊息。

問題	回復
您收到這個錯誤： 無法取得預設認證快取名稱。	決定登入 iSeries 的使用者是否有位於 /home 目錄下的目錄。若使用者的目錄不存在，請針對認證快取建立一個起始目錄。
CPD3E3F 發生「網路鑑別服務」錯誤 &2。	請參閱對應此訊息的特定回復資訊。
在先前連接的 iSeries 系統上，DRDA/DDM 連線失敗。	檢查網路鑑別服務配置期間所指定的預設領域是否存在。如果尚未配置預設領域和金鑰分送中心 (KDC)，則網路鑑別服務配置不正確且 DRDA/DDM 連線將會失敗。若要回復此錯誤，您可以執行下列其中一項作業： 1. 如果您不是使用 Kerberos 鑑別，請完成下列動作： a. 刪除網路鑑別服務配置中指定的預設領域。 2. 如果您正使用 Kerberos 鑑別，請完成下列步驟： a. 對網路的安全系統配置預設領域和 KDC。請參閱對應該系統的文件。**註**：iSeries 目前不支援 KDC。 b. 重新配置網路鑑別服務，指定您在步驟 1 建立的預設領域和 KDC。 c. 配置 (23See) iSeries Access for Windows 應用程式來使用 Kerberos 鑑別。這會對所有 iSeries Access for Windows 應用程式 (包括 DRDA/DDM) 設定 Kerberos 鑑別。
在先前連接的 iSeries 系統上的 QFileSvr.400 連線失敗。	檢查網路鑑別服務配置期間所指定的預設領域是否存在。如果尚未配置預設領域和金鑰分送中心 (KDC)，則網路鑑別服務配置不正確且 QFileSvr.400 連線將會失敗。若要回復此錯誤，您可以執行下列其中一項作業： 1. 如果您不是使用 Kerberos 鑑別，請完成下列動作： a. 刪除網路鑑別服務配置中指定的預設領域。 2. 如果您正使用 Kerberos 鑑別，請完成下列步驟： a. 對網路的安全系統配置預設領域和 KDC。請參閱對應該系統的文件。**註**：iSeries 目前不支援 KDC。 b. 重新配置網路鑑別服務，指定您於步驟 1 所建立的預設領域和 KDC。 c. 配置 (23See) iSeries Access for Windows 應用程式來使用 Kerberos 鑑別。這會對所有 iSeries Access for Windows 應用程式 (包括 DRDA/DDM) 設定 Kerberos 鑑別。
CWBSY1011 找不到 Kerberos 從屬站認證。	使用者沒有通行證授予通行證 (TGT)。當使用者未登入 Windows (R) 2000 領域時，從屬站 PC 上會發生此連線錯誤。若要回復此錯誤，請登入 Windows (R) 2000 網域。

驗證連線設定值時發生錯誤。URL 沒有主電腦。 **註**：當您使用「企業識別對映 (EIM)」時會發生此錯誤。	若要回復此錯誤，請完成下列步驟： 1. 在「iSeries 領航員」中，展開**您的 iSeries** —> **網路** —> **伺服器**—> **TCP/IP**。 2. 以滑鼠右鍵按一下**目錄**，然後選取**內容**。 3. 在**一般**頁上，驗證管理者的識別名稱和密碼是否符合您在 EIM 配置期間所輸入的值。
變更本端目錄伺服器配置時發生錯誤。GLD0232：配置不可含有重疊字尾。 **註**：當您使用「企業識別對映 (EIM)」時會發生此錯誤。	若要回復此錯誤，請完成下列步驟： 1. 在「iSeries 領航員」中，展開**您的 iSeries** —> **網路** —> **伺服器** —> **TCP/IP**。 2. 以滑鼠右鍵按一下**目錄**，然後選取**內容**。 3. 在**資料庫/字尾**頁上，移除任何 **ibm-eimDomainName** 登錄並重新配置 EIM。
驗證連線設定值時發生錯誤。呼叫 iSeries 程式時發生異常。被呼叫的程式爲 eimConnect。詳細資料爲：com.ibm.as400.data.PcmlException。 **註**：當您使用「企業識別對映 (EIM)」時會發生此錯誤。	若要回復此錯誤，請完成下列步驟： 1. 在「iSeries 領航員」中，展開**您的 iSeries**—> **網路**—>**伺服器**—> **TCP/IP**。 2. 以滑鼠右鍵按一下**目錄**，然後選取**內容**。 3. 在**資料庫/字尾**頁上，移除任何 **ibm-eimDomainName** 登錄並重新配置 EIM。

«

相關資訊

Kerberos 通信協定規格

The Kerberos Network Authentication Service (V5) 。
Internet Engineering Task Force (IETF) 正式在 Request for Comments 1510 中定義 Kerberos 通信協定。

Kerberos: The Network Authentication Protocol (V5) 。
Massachusetts Institute of Technology 的 Kerberos 通信協定正式文件，提供程式設計資訊及說明通信協定特性。

同屬安全服務 (GSS) API 規格

有關 Kerberos 及 GSS API 的詳細資訊，請參閱下列來源：

Generic Security Service Application Program Interface Version 2, Update 1 。
Internet Engineering Task Force (IETF) 正式在 Request for Comments 2743 中定義 GSS API。

Generic Security Service API : C-bindings 。
Internet Engineering Task Force (IETF) 在 Request for Comment 1509 中指定 GSS API C 連結。

The Kerberos Version 5 GSS-API Mechanism  。
Internet Engineering Task Force (IETF) 在這個 Request for Comments 1964 中定義 Kerberos 版本 5 和 GSS API 規格。

資訊中心相關主題

Network Authentication Service Application Programmable Interfaces (APIs)
此「資訊中心」主題提供網路鑑別服務 API 報表及其功能的簡要說明。

Generic Security Service Application Programmable Interfaces (GSS APIs)
此「資訊中心」主題提供 GSS API 報表及其功能的簡要說明。

Enterprise Identity Mapping (EIM)
EIM 是一種機制，可將某人或實體 (如服務) 對映到整個企業內不同使用者登錄中的適當使用者身份。iSeries 使用 EIM 來啓用 OS/400 介面，透過網路鑑別服務來鑑別使用者。iSeries 及應用程式也可接受 Kerberos 通行證，使用 EIM 來尋找此系統相關 Kerberos 主體之使用者 ID。

特殊條款

下列條款僅適用於網路鑑別服務程式碼，此網路鑑別服務程式碼包含於檔案庫 QSYS 之服務程式 QKRBGSS、檔案庫 QSYSINC 之檔案 H 之成員 KRB5 及包含於目錄 /QIBM/ProdData/OS400/NetworkAuthentication/ 之訊息型錄 skrbdll.cat 及 skrbkut.cat 中。

IBM 依網路鑑別服務程式目的碼的「現狀」來提供授權，不含任何明示或默示之保證，包括但不限於可售性或符合特定效用之保證。

IBM 不保證使用這些程式碼不會侵害任何著作權、商業機密、專利，或其他智慧財產權、所有權，或任何第三者的合約權利。

散佈者需要遵循下列注意事項：

Copyright 1985, 1986, 1987, 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995
by the Massachusetts Institute of Technology.
All Rights Reserved.

自美國輸出本軟體需取得美國政府的特別授權。任何人或組織欲輸出本軟體之前，需先取得該特別授權。

在該限制下，授予任何目的之免費使用、複製、修改與散布本軟體及其文件之許可權。且必需在所有拷貝中顯示上述著作權聲明，以及在支援文件中必須顯示上述著作權聲明及本許可聲明。若未先取得書面許可，不得將 M.I.T. 的名稱用來爲有關文件或軟體的散布做廣告或宣傳。不管任何目的，M.I.T. 的名稱不得代表本軟體之適用性。以現狀提供本軟體，而並不提供任何明示或默示之保證。

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

All rights reserved.

自美國輸出本軟體需取得美國政府的特別授權。任何人或組織欲輸出本軟體之前，需先取得該特別授權。

在該限制下，授予任何目的之免費使用、複製、修改與散布本軟體及其文件之許可權。且必需在所有拷貝中顯示上述著作權聲明，以及在支援文件中必須顯示上述著作權聲明及本許可聲明。若未先取得書面許可，不得將 M.I.T. 的名稱用來爲有關文件或軟體的散布做廣告或宣傳。不管任何目的，M.I.T.、Open Computing Security Group 或 CyberSAFE Corporation 的名稱均不得代表本軟體之適用性。以現狀提供本軟體，而並不提供任何明示或默示之保證。

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

自美國輸出本軟體需取得美國政府的特別授權。任何人或組織欲輸出本軟體之前，需先取得該特別授權。

在該限制下，授予任何目的之免費使用、複製、修改與散布本軟體及其文件之許可權。且必需在所有拷貝中顯示上述著作權聲明，以及在支援文件中必須顯示上述著作權聲明及本許可聲明。若未先取得書面許可，不得將 Richard P. Basch、Lehman Brothers 及 M.I.T. 的名稱用來爲有關文件或軟體的散布做廣告或宣傳。不管任何目的，Richard P. Basch、Lehman Brothers 及 M.I.T. 的名稱不得代表本軟體之適用性。以現狀提供本軟體，而並不提供任何明示或默示之保證。

這些特殊條款僅適用如上所述的網路鑑別服務程式碼，而不及於 OS/400 其他部份或授權內碼。