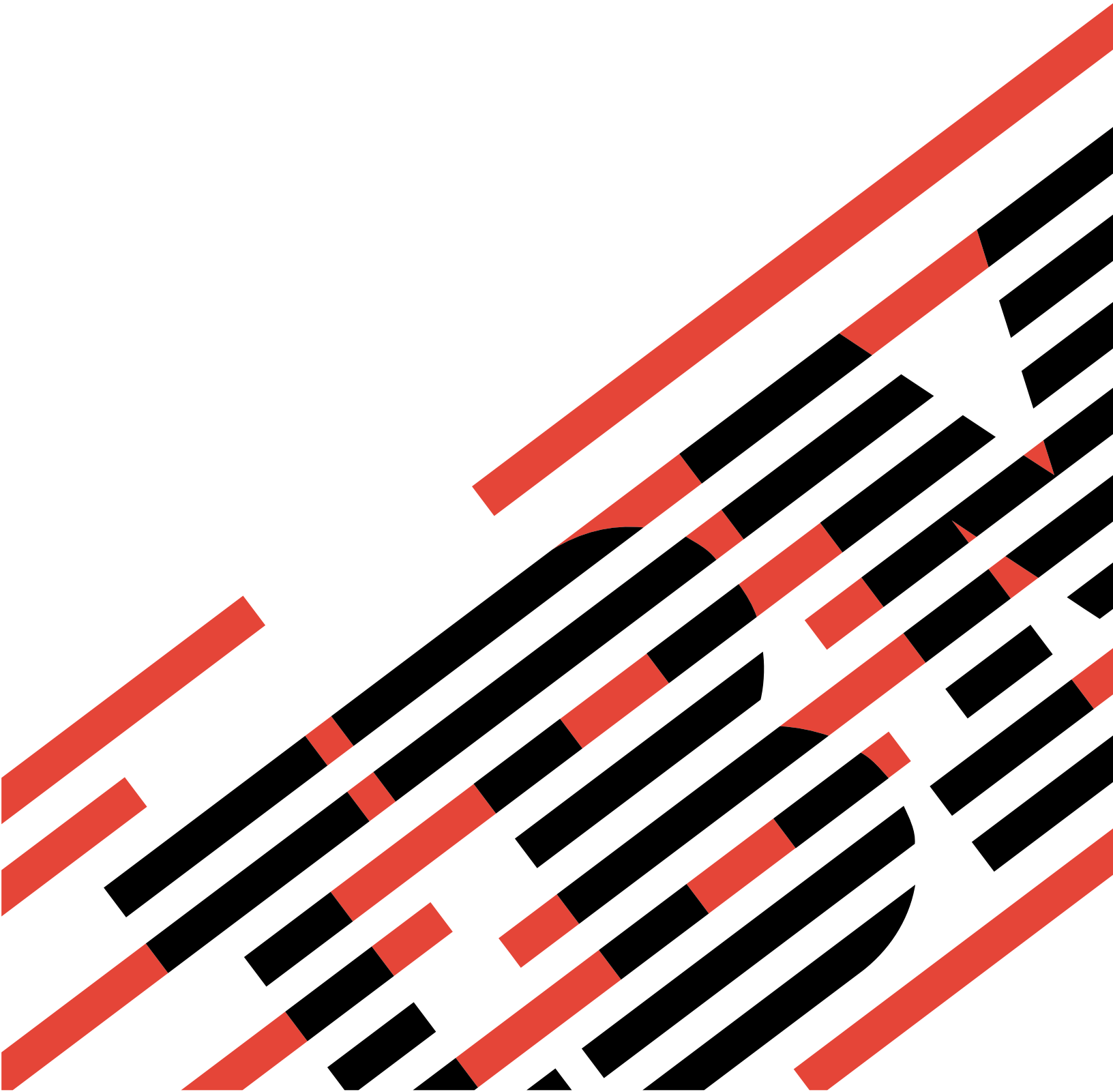
IBM

eserver

iSeries

네트워크 인증 서비스



IBM

@server

iSeries

네트워크 인증 서비스

목차

네트워크 인증 서비스

네트워크 인증 서비스를 사용하면 iSeries와 여러 가지 iSeries 서비스(예: Windows용 iSeries Access)에서 사용자 인증을 위한 사용자명과 암호에 대한 선택적 대체로 Kerberos 티켓을 사용할 수 있습니다. Massachusetts Institute of Technology에서 개발한 Kerberos 프로토콜을 사용하면 프린시펄(사용자 또는 서비스)이 보안이 갖춰지지 않은 네트워크 내의 또 다른 서비스에 대하여 자신의 ID를 증명할 수 있습니다. 프린시펄 인증은 KDC(Key Distribution Center)라고 하는 중앙 서버를 통해 이루어집니다. KDC에서는 Kerberos 티켓을 사용하여 사용자를 인증합니다. 이 티켓을 통해 네트워크의 다른 서비스에 대해 프린시펄 ID를 증명할 수 있습니다. 이 티켓으로 프린시펄이 인증되면 티켓은 목표 서비스와 암호화된 자료를 교환할 수 있습니다. 네트워크 인증 서비스에서 네트워크의 사용자 ID나 서비스를 확인합니다. 어플리케이션에서는 사용자를 인증하고 네트워크의 다른 서비스로 사용자 ID를 안전하게 전달할 수 있습니다. 일단 사용자가 알려지면, 사용자가 네트워크 자원을 사용할 수 있는 권한을 검증할 별도의 함수가 필요합니다. 네트워크 인증 서비스는 다음 스펙을 구현합니다.

- Kerberos 버전 5 프로토콜 RFC(Request for Comment) 1510
- 현재 업계 주류를 이루고 있는 실질적인 표준 Kerberos 프로토콜 API
- RFC 1509, 1964 및 2743에서 정의된 GSS(Generic Security Service) API

iSeries의 네트워크 인증 서비스는 인증 및 위임과 Microsoft의 Windows 2000 SSPI(Security Service Provider Interface) API와 같이 RFC를 따르는 자료 기밀성 서비스와 상호 작동합니다.

또한 네트워크 인증 서비스를 EIM(Enterprise Identity Mapping)과 함께 사용하여 단일 사인 온 환경을 활성화할 수 있습니다. 단일 사인 온의 경우, 기초 보안 정책을 변경할 필요없이 여러 플랫폼에서 더 쉬운 암호 관리 시스템을 사용할 수 있게 함으로써 사용자, 관리자, 어플리케이션 개발자 모두에게 혜택을 줍니다. 다음 항목에서는 네트워크 인증 서비스와 EIM(Enterprise Identity Mapping)을 사용한 단일 사인 온 작동에 대한 세부사항을 제공합니다.

단일 사인 온 작동

다음 항목에서는 단일 사인 온의 장점에 대한 개념 정보, 네트워크 인증 서비스와 EIM(Enterprise Identity Mapping)을 함께 작동하여 단일 사인 온 환경을 만드는 방법에 대한 개요를 제공합니다.

시나리오: 단일 사인 온 작동

이 항목은 MyCo 주문 수신 부서의 관리자가 단일 사인 온 환경을 작동하는 방법에 대한 예를 제공합니다. 관리자는 iSeries 어플리케이션의 Windows(R) 정의역 ID와 암호를 사용하여 사용자를 iSeries 어플리케이션에 인증하고자 합니다. MyCo의 관리자가 단일 사인 온을 활성화하기 위해 네트워크 인증 서비스와 EIM을 구성한 방법에 대한 단계별 지침이 포함되어 있습니다.

이러한 네트워크 인증 서비스에 관한 논의에는 다음과 같은 주제들이 포함됩니다.

V5R2의 새로운 사항
이 주제에서는 이 릴리스의 네트워크 인증 서비스의 새로운 기능에 대한 추가 정보를 설명하고 해당 정보로 링크합니다.

이 주제 인쇄
이 주제에서는 해당 정보의 PDF 버전을 다운로드하고 인쇄하기 위한 지침을 제공합니다.

네트워크 인증 서비스 작동 방법
이 주제에서는 Kerberos 프로토콜을 사용하여 사용자를 인증하는 네트워크 내에서 네트워크 인증 서비스가 작동하는 방법에 대한 개요를 제공합니다.

네트워크 인증 서비스 전문 용어
이 주제에서는 네트워크 인증 서비스와 관련된 전문 용어를 정의합니다.

네트워크 인증 서비스 프로토콜
이 주제에서는 Kerberos 프로토콜과 GSS(Generic Security Services) API의 기본 사항을 설명합니다. RFC와 기타 관련된 정보에 대한 링크가 제공됩니다.

네트워크 인증 서비스 시나리오
이 주제에서는 네트워크 인증 서비스를 구현하는 몇 가지의 업무 시나리오를 설명합니다.

네트워크 인증 서비스 계획
이 주제에서는 네트워크 인증 서비스에 대한 작업을 하기 전에 수행해야 할 사항에 대하여 설명합니다.

네트워크 인증 서비스 구성
이 주제에서는 iSeries Navigator에 네트워크 인증 서비스를 구성하는 방법을 설명합니다.

네트워크 인증 서비스 관리
이 주제에서는 관리자와 사용자가 네트워크 인증 서비스를 관리하기 위해 사용할 수 있는 타스크를 설명합니다.

네트워크 인증 서비스 문제 해결
이 주제에서는 네트워크 인증 서비스, 관련 어플리케이션에 대한 메세지 및 문제 해결에 대해 설명합니다.

관련 정보

이 주제에서는 Kerberos 프로토콜 및 GSS(Generic Security Services) API와 관련된 기타 주제를 설명하고 해당 주제에 대한 링크를 제공합니다.

법률 정보

이 주제에서는 Kerberos 프로토콜 및 연관된 API 사용에 대해 다루는 중요한 법률 정보를 제공합니다.

V5R2의 새로운 사항

네트워크 인증 서비스를 사용하면 Kerberos 프로토콜을 사용하여 네트워크의 사용자를 인증하는 네트워크에 iSeries가 참여할 수 있습니다.

iSeries Navigator의 네트워크 인증 서비스

네트워크 인증 서비스 마법사를 사용하면 iSeries가 Kerberos 네트워크에 참여할 수 있도록 쉽게 구성할 수 있습니다. 마법사를 사용하여 iSeries가 Kerberos 영역에 참여하도록 구성할 수 있습니다. 그에 따라 Kerberos 프로토콜을 사용하면 사용자를 위해 티켓을 서비스로 전달하여 네트워크의 자원에 사용자를 인증할 수 있습니다. 구성을 완료하려면 다음 주제를 참조하십시오.

- 네트워크 인증 서비스 시나리오
  네트워크 인증 서비스를 사용하는 두 가지 고객 상황에 대해 간략하게 설명합니다.
- 네트워크 인증 서비스 구성
  네트워크 인증 서비스를 구성하는 데 필요한 모든 단계에 대한 개요를 제공합니다.
- 네트워크 인증 서비스 관리
  iSeries Navigator를 사용하여 완료할 수 있는 모든 타스크에 대한 개요를 제공합니다.

새로운 Qshell 명령 지원

사용자는 Qshell 명령으로 티켓을 요구하고 티켓에 대한 작업을 할 수 있습니다. 이 릴리스에 **kpasswd** 명령이 추가되어 사용자는 키 분배 센터에서 자신의 암호를 변경할 수 있습니다.

- Kerberos 암호 변경
  kpasswd Qshell 명령 사용법에 대한 정보를 제공합니다.

EIM(Enterprise Identity Mapping)

EIM(Enterprise Identity Mapping)은 개인이나 엔티티(예: 서비스)를 기업망에서 다양한 사용자 레지스트리의 해당 사용자 ID로 맵핑하는 메카니즘입니다. 네트워크 인증 서비스에 사용할 경우, EIM은 단일 사인 온 환경을 작동할 수 있습니다. iSeries에서는 네트워크 인증 서비스를 통해 사용자를 인증할 수 있

도록 EIM을 사용하여 OS/400 인터페이스를 활성화합니다. iSeries와 어플리케이션에서는 또한 Kerberos 티켓을 허용하고 EIM을 사용하여 시스템의 사용자 ID를 연관된 Kerberos 프린시펄로 맵핑할 수 있습니다.

- 단일 사인 온 작동
  단일 사인 온의 장점에 대한 개념 정보과 네트워크 인증 서비스와 EIM(Enterprise Identity Mapping)을 함께 작동하여 단일 사인 온 환경을 만드는 방법에 대한 개요를 제공합니다.
- 시나리오: 단일 사인 온 작동
  네트워크 인증 서비스와 EIM을 함께 사용하여 단일 사인 온 환경을 작동하는 상황에 대한 자세한 예를 제공합니다.

여러 가지 iSeries 어플리케이션에 대한 인증 지원

- **SQL(구조화 조회 언어)/DRDA(분산 관계형 데이터베이스 구조)**
  이제 SQL/DRDA는 Kerberos 티켓 사용을 지원하여 데이터베이스 기능에 액세스하는 사용자를 인증할 수 있습니다. DRDA에서는 지정한 사용자의 티켓 부여 티켓을 검사합니다. 티켓이 있으면 이 티켓을 사용하여 사용자에 대한 서비스 티켓을 가져오게 됩니다.
- **DDM(분산 자료 관리)**
  이제 DDM에서는 리모트 파일에 액세스하는 사용자를 인증할 수 있도록 Kerberos 티켓 사용을 지원합니다. DDM에서는 지정된 사용자의 티켓 부여 티켓을 검사합니다. 티켓이 있으면 이 티켓을 사용하여 사용자에 대한 서비스 티켓을 가져오게 됩니다.
  주: Kerberos 구성 파일에 지정된 디폴트 영역이 있지만 Kerberos를 인증 방법으로 사용하지 않을 경우, DDM에 대한 인증을 설정하기 전에 디폴트 영역을 제거해야 합니다. 이 문제를 회복하기 위한 정보는 어플리케이션 연결 문제점 및 회복을 참조하십시오.
- **Windows용 iSeries Access 및 OS/400 호스트 서버**
  Windows용 iSeries Access 및 OS/400 호스트 서버에서는 Kerberos 티켓을 통하여 인증을 지원합니다. 클라이언트에서 사용자는 iSeries Access 호스트 서버에 액세스할 때 사용할 Kerberos 티켓을 지정할 수 있습니다.
- **iSeries NetServer**
  네트워크에 Kerberos를 구성한 경우, iSeries NetServer 클라이언트는 Kerberos 티켓을 사용하여 서버에 인증할 수 있습니다. 이 지원을 활성화하면 Kerberos v5를 지원하는 클라이언트만 iSeries NetServer에 연결할 수 있습니다. Kerberos의 iSeries NetServer 지원에 대한 요구사항과 관련한 자세한 내용은 Kerberos v5 인증에 대한 iSeries NetServer 지원을 참조하십시오.
- **QFileSvr.400**
  QFileSvr.400이 현재 사용자에 대한 티켓 부여 티켓이 있는지 판별합니다. 티켓 부여 티켓이 있으면 목표 시스템의 사용자를 인증하기 위해 서버 티켓이 작성됩니다. 티켓이 없으면 암호 대체의 현재 방법을 사용합니다.
  주: Kerberos 구성 파일에 지정된 디폴트 영역이 있지만 Kerberos를 인증 방법으로 사용하지 않을 경우, QFileSvr에 대한 인증을 설정하기 전에 디폴트 영역을 제거해야 합니다. 이 문제를 회복하기 위한 정보는 어플리케이션 연결 문제점 및 회복을 참조하십시오.

새로운 사항 및 변경 사항을 보는 방법

기술적으로 변경된 부분을 찾으려면 이 정보를 사용하십시오.

- 새로운 정보 또는 변경된 정보가 시작되는 곳에

  이미지가 표시됩니다.
- 새로운 정보 또는 변경된 정보가 끝나는 곳에

  이미지가 표시됩니다.

이 릴리스의 새로운 사항 및 변경 사항에 대한 기타 정보는 Memo to Users  를 참조하십시오.

이 주제 인쇄

PDF 버전을 보거나 다운로드하려면 네트워크 인증 서비스를 선택하십시오(약 199KB 또는 50 페이지).

보거나 인쇄하기 위해 워크스테이션에 PDF를 저장하려면 다음과 같이 하십시오.

1. 브라우저에서 PDF를 여십시오(위의 링크를 클릭하십시오).
2. 브라우저 메뉴에서 **파일**을 클릭하십시오.
3. **다른 이름으로 저장**을 클릭하십시오.
4. PDF를 저장할 디렉토리를 찾으십시오.
5. **저장**을 클릭하십시오

PDF를 보거나 인쇄하기 위해 Adobe Acrobat Reader가 필요한 경우, Adobe 웹 사이트 (www.adobe.com/product/acrobat/readstep.html)  에서 사본을 다운로드 받을 수 있습니다.

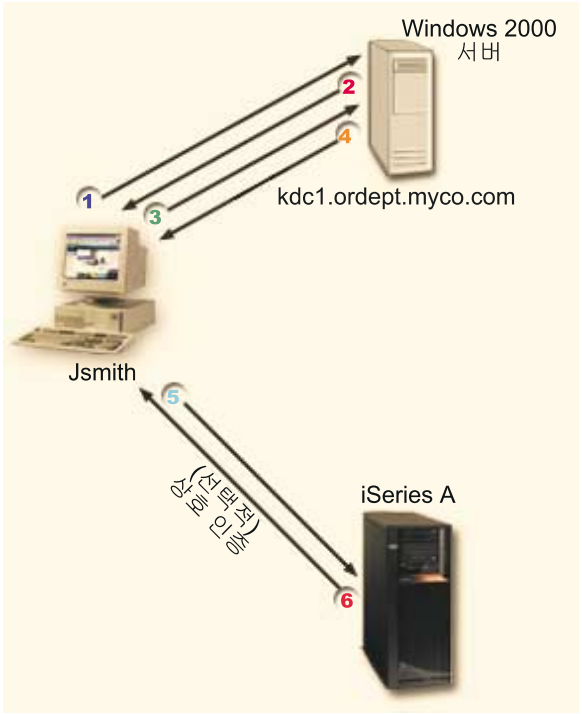
네트워크 인증 서비스 작동 방법

네트워크 관리자로서 iSeries 시스템이 중앙 KDC(Key Distribution Center)에서 작성한 Kerberos 티켓을 허용하도록 네트워크 인증 서비스를 구성할 수 있습니다. KDC는 모든 사용자와 서비스의 데이터베이스를 영역 내에서 유지보수합니다. iSeries와 여러 가지 iSeries 고유 어플리케이션은 Kerberos 네트워크 내에서 클라이언트/서버 역할을 하며 사용자와 서비스에 대한 티켓을 요구합니다. 사용자가 KDC에서 티켓을 요구하면 TGT(Ticket Granting Ticket)라는 최초 티켓이 발행됩니다. 그러면 사용자는 TGT를 사용하여 네트워크의 다른 서비스와 어플리케이션에 액세스하는 서비스 티켓을 요구할 수 있습니다. 인증이 제대로 이루어지려면 관리

자가 사용자, iSeries 서비스 프린시펄, Kerberos 프로토콜을 사용할 어플리케이션을 KDC에 등록해야 합니다. iSeries는 프린시펄이 서비스에 대한 인증을 요구하는 서버 역할을 하거나, 네트워크의 어플리케이션 및 서비스에 대한 티켓을 요구하는 클라이언트 역할을 할 수 있습니다. 다음 그래픽에서는 이 두 상황의 티켓 흐름 방식을 보여줍니다.

서버로서의 iSeries

이 그래픽은 iSeries가 Kerberos 네트워크에서 서버 역할을 할 경우 인증 작동 방법을 보여줍니다. 이 그래픽에서는 Windows (R) 2000 KDC가 프린시펄, Jsmith에게 티켓을 발행합니다. Jsmith는 iSeries-A의 어플리케이션에 액세스하고자 합니다. 이 경우 서버에서 EIM(Enterprise Identity Mapping)을 사용하여 Kerberos 프린시펄을 iSeries 사용자 프로파일에 맵핑합니다. Windows용 iSeries Access와 같이 Kerberos화한 iSeries 서버에 대하여 이 작업이 수행됩니다.



이 설명에서는 네트워크 내에서 인증 프로세스가 작동하는 방법에 대한 개요를 제공합니다.

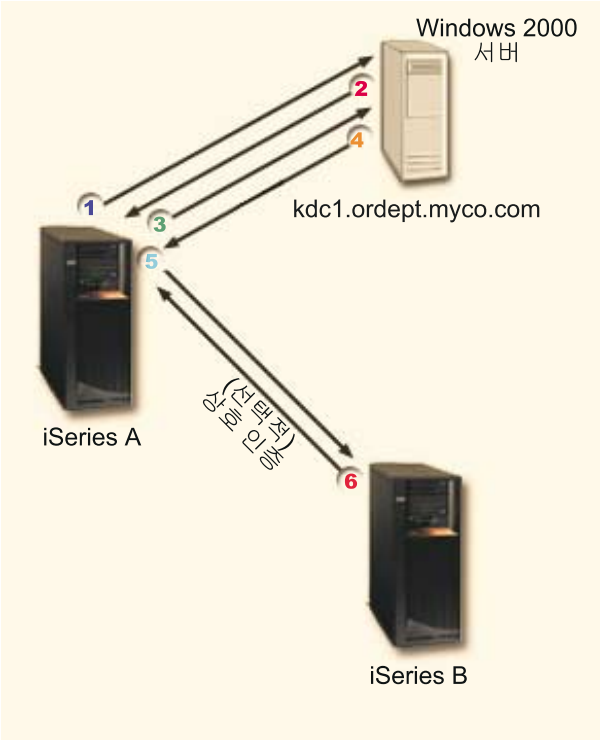
1. 사용자 Jsmith는 Kerberos 네트워크에 들어갈 때 KDC로부터 티켓을 요구합니다. 그러면 KDC에게 티켓 부여 티켓에 대한 요구를 송신합니다.
2. KDC에서는 사용자의 프린시펄명과 암호 유효성을 검사하고 Jsmith에게 티켓 부여 티켓을 송신합니다.
3. Jsmith는 iSeries 서버의 어플리케이션에 대한 액세스 권한이 필요합니다. 네트워크 인증 서비스 API를 호출하면 어플리케이션에서 Jsmith의 TGT를 KDC에게 송신하여 특정 어플리케이션이나 서비스에 대한 서비스 티켓을 요구합니다. 티켓과 사용자에 대한 기타 식별 정보를 보유하고 있는 증명서 캐시는

프린시펄의 로컬 기계에서 관리합니다. 필요에 따라 캐시에서 이 증명서를 읽고, 새 증명서를 획득하면 캐시에 저장합니다. 이것은 어플리케이션에서 증명서 자체를 관리할 책임을 덜어줍니다.

4. KDC에서 서비스 티켓으로 응답합니다.
5. 어플리케이션에서는 서버 티켓을 iSeries 서비스에 송신하여 사용자를 인증합니다.
6. 서버 어플리케이션에서는 네트워크 인증 서비스 API를 호출하여 티켓 유효성을 검사하고 선택적으로 응답을 다시 클라이언트에 송신하여 상호 인증할 수 있습니다.

클라이언트로서의 iSeries

이 그래픽은 iSeries가 Kerberos 네트워크에서 클라이언트 역할을 할 경우 인증 작동 방법을 보여줍니다. 이 그래픽에서는 Windows (R) 2000 KDC가 iSeries-A 프린시펄에게 티켓을 발행합니다. iSeries-A는 다른 서비스에 대해 인증을 받을 수 있습니다. 이 예에서는 iSeries-B에서 EIM을 사용하여 kerberos 프린시펄을 iSeries 사용자 프로파일에 맵핑합니다. QFileSvr.400과 같이 kerberos화한 iSeries 서버 기능에 대하여 이 작업이 수행됩니다.



이 설명에서는 네트워크 내에서 인증 프로세스가 작동하는 방법에 대한 개요를 제공합니다.

1. 프린시펄 Jsmith가 iSeries-A에 서명한 다음 Qshell 인터프리터에서 kinit 명령을 수행하여 티켓 부여 티켓을 요구합니다. iSeries는 이 요구를 KDC에 송신합니다.
2. KDC에서는 사용자의 프린시펄명과 암호 유효성을 검사하고 Jsmith에게 티켓 부여 티켓을 송신합니다.

3. Jsmith는 iSeries 서버의 어플리케이션에 대한 액세스가 필요합니다. 네트워크 인증 서비스 API를 호출함으로써 어플리케이션에서 Jsmith의 TGT를 KDC로 송신하여 특정 어플리케이션이나 서비스에 대한 서비스 티켓을 요구합니다. 티켓, 세션 키, 사용자에 대한 기타 식별 정보가 있는 증명서 캐시는 프린시펄의 로컬 기계에서 관리합니다. 필요에 따라 캐시에서 이 증명서를 읽고, 새 증명서를 새 증명서를 획득하면 캐시에 저장합니다. 이것은 어플리케이션에서 증명서 자체를 관리할 책임을 덜어줍니다.
4. KDC에서 서비스 티켓에 응답합니다.
   주: iSeries-B용 서비스 프린시펄을 KDC에 추가하고 iSeries-B에서도 네트워크 인증 서비스를 구성해야 합니다.
5. 어플리케이션에서는 서버 티켓을 iSeries 서비스에 송신하여 사용자를 인증합니다.
6. 서버 어플리케이션에서는 네트워크 인증 서비스 API를 호출하여 티켓 유효성을 검사하고 선택적으로 응답을 다시 클라이언트에 송신하여 상호 인증할 수도 있습니다.

네트워크 인증 서비스 전문 용어

네트워크 인증 서비스에서는 다음과 같은 Kerberos 프로토콜 전문 용어를 사용합니다.

이송 가능 티켓
이송 가능 티켓을 사용하면 서버에서 다른 서비스에 대한 리퀘스터의 증명서에 전달할 수 있습니다. 이럴 경우, 초기 TGT를 이송 가능 옵션으로 요구하고 서버에서 증명서를 위임할 수 있습니다.

KDC(Key Distribution Center)
티켓과 임시 세션 키를 제공하는 네트워크 서비스. KDC는 프린시펄(사용자 및 서비스)의 데이터베이스와 이와 연관된 비밀 키를 유지보수합니다. KDC는 인증 서버와 티켓 부여 티켓 서버로 구성됩니다. KDC로 역할하는 보안 기계를 사용해야 합니다. 사용자 이외의 개인이 KDC에 대한 액세스를 얻으면 전체 영역이 손상될 수 있습니다.
주: iSeries 시스템은 KDC를 지원하지 않습니다.

키 표
서비스 호스트 시스템 상의 파일. 파일의 각 항목에는 서비스 프린시펄의 이름과 비밀 키가 있습니다. iSeries의 경우, 네트워크 인증 서비스를 구성하는 동안 키 표 파일이 작성됩니다. 서비스에서 네트워크 인증 서비스가 구성된 iSeries에 대한 인증을 요구할 경우, iSeries는 해당 서비스의 증명서에 대한 키 표 파일을 검사합니다. 사용자와 서비스가 제대로 인증받도록 하려면 KDC와 iSeries에 사용자와 서비스를 등록해야 합니다.

암호 서버
클라이언트에서 리모트로 KDC에 대한 자신의 암호를 변경할 수 있습니다. 일반적으로 암호 서버는 KDC와 동일한 기계에서 실행됩니다.

프린시펄
Kerberos 네트워크에 있는 사용자명이나 서비스명. 사용자는 서비스를 사용하여 특정 어플리케이션이나 오퍼레이팅 시스템 서비스를 식별하는 개인으로 간주됩니다. iSeries에서는 클라이언트에서 iSeries로 인증할 경우, **krbsvr400** 서비스 프린시펄을 사용하여 Windows용 iSeries Access, QFileSrv.400 및 Telnet 서버를 식별합니다.

프록시 가능 티켓
프록시 가능 티켓은 TGT(Ticket Granting Ticket)에 있는 IP 주소 이외에 다른 IP 주소가 있는 서비스의 티켓을 가져올 수 있게 하는 TGT입니다. 이송 가능 티켓과는 달리 현재 TGT에서 새로운 TGT를 프록시할 수 없습니다. 서비스 티켓인 경우에만 프록시할 수 있습니다. 이송 가능 티켓을 사용하면 전체 ID(TGT)를 다른 기계에 전송할 수 있지만, 프록시 가능 티켓을 사용하면 특정 티켓만 전송할 수 있습니다. 프록시 가능 티켓을 사용하면 서비스가 프린시펄을 대신하여 타스크를 수행할 수 있습니다. 서비스는 특정 목적을 위해 프린시펄의 ID를 사용할 수 있어야 합니다. 프록시 가능 티켓은 원래의 티켓 부여 티켓을 기준으로 다른 네트워크 주소로 새 티켓을 발행할 수 있음을 KDC에게 알려줍니다. 프록시 가능 티켓을 사용할 경우, 암호가 필요없습니다.

영역
지정된 KDC(Key Distribution Center)가 인증 기관인 사용자와 서버 집합.

영역 신뢰
Kerberos 프로토콜은 구성 파일을 탐색하여 영역 신뢰를 판별하거나, 디폴트로 영역 계층 내에서 신뢰 관계를 찾습니다. 네트워크 인증 서비스에서 **신뢰할 수 있는 영역**을 사용하면 이 프로세스를 바이패스하고 인증에 대한 단축키를 작성할 수 있습니다. 영역이 서로 다른 정의역에 있는 네트워크에서 영역 신뢰를 사용할 수 있습니다. 예를 들어, NY.myco.com에 회사의 한 영역이 있고 LA.myco.com에 다른 영역이 있을 경우 이 두 영역 간에 신뢰를 설정할 수 있습니다. 두 영역이 서로 신뢰할 경우 영역의 연관된 KDC에서 키를 공유해야 합니다. 단축키를 작성하기 전에 서로 신뢰할 KDC를 설정해야 합니다.

갱신 가능 티켓
어플리케이션이나 서비스에서 기간을 확장하여 유효한 티켓을 가지려는 경우도 있습니다. 그러나 기간을 확장하면 티켓이 만기될 때까지 유효한 이 증명서를 다른 사람이 도용할 수 있습니다. 갱신 가능 티켓을 사용하면 어플리케이션에서는 도용의 위험을 줄이면서 확장 기간 동안 유효한 티켓을 가져올 수 있습니

다. 갱신 가능 티켓에는 두 가지 만기 시간이 있습니다. 첫 번째 만기는 티켓의 현재 인스턴스에 적용되고, 두 번째는 티켓에 대한 최종 허용 가능 만기에 적용됩니다.

서비스 티켓
프린시펄을 서비스에 인증하는 티켓.

TGS(Ticket Granting Service)
서비스 티켓을 발행하는 KDC에서 제공하는 서비스.

TGT(Ticket Granting Ticket)
KDC의 티켓 부여 서비스에 액세스를 허용하는 티켓. 프린시펄이 요구를 성공적으로 완료한 후 KDC에서 프린시펄로 티켓 부여 티켓을 전달합니다. Windows(R) 2000 환경에서는 사용자가 네트워크에 로그온하고, KDC에서 프린시펄의 이름과 암호화된 암호를 확인한 다음 사용자에게 티켓 부여 티켓을 송신합니다. iSeries 서버에서 사용자는 문자 기반 인터페이스의 Qshell 인터프리터 내에서 kinit 명령을 사용하여 티켓을 요구할 수 있습니다.

네트워크 인증 서비스 프로토콜

네트워크 인증 서비스는 인증을 위해 GSS(Generic Security Services) API와 Kerberos 프로토콜을 함께 사용하여 인증 및 보안 서비스를 제공합니다. 다음 섹션에서는 이 프로토콜의 일반적인 설명과 iSeries에서 이 프로토콜을 사용하는 방법을 제공합니다. 이 표준에 대한 자세한 정보를 위해 연관된 RFC(Request for Comment)와 다른 외부 소스로의 링크를 제공합니다.

Kerberos 프로토콜

Kerberos 프로토콜은 사용자에게 티켓을 발행하는 KDC(Key Distribution Center)라는 중앙 서버에 사용자 ID를 증명하는 경우, Kerberos 프로토콜은 제 3자 인증을 제공합니다. 그런 다음 사용자는 이 티켓을 사용하여 네트워크에서 자신의 ID를 증명할 수 있습니다. 티켓을 사용하면 다른 시스템에 여러 번 사인 온 할 필요가 없습니다. iSeries에서 지원하는 Kerberos API는 Massachusetts Institute of Technology에서 개발되었고 사실상 Kerberos 프로토콜 사용을 위한 표준이 되었습니다.

보안 환경 가정

Kerberos 프로토콜은 모든 자료 교환은 언제든지 패킷을 삽입, 변경 및 가로챌 수 있는 환경에서 발생한다고 가정합니다. Kerberos를 전체 보안 계획의 한 층으로 사용하십시오. Kerberos 프로토콜로 사용자와 네트워크 상의 어플리케이션을 인증할 수 있지만, 네트워크 보안 목표를 정의할 때는 일부 제한 사항을 숙지하고 있어야 합니다.

- Kerberos 프로토콜은 서비스 거부 공격으로부터 보호되지 않습니다. 이 프로토콜에는 어플리케이션이 적절한 인증 단계를 거치는 것을 침입자가 방해할 수 있는 부분이 있습니다. 그러한 공격을 감지하고 해결하는 것은 여전히 관리자와 사용자의 몫입니다.
- 키 공유 또는 키 절도가 의인화 공격을 불러올 수 있습니다. 침입자가 프린시펄 키를 가져간 경우, 이들은 사용자나 서비스로 가장할 수 있습니다. 이러한 위협을 막기 위해 사용자들의 키 공유를 금지하고 이러한 정책을 보안 규칙에 명시하십시오.
- Kerberos 프로토콜은 암호 추측과 같은 일반적인 암호의 취약성 부분에 대하여는 보호되지 않습니다. 사용자가 쉬운 암호를 선택하였다면, 공격자는 사용자의 암호로부터 나온 키 아래에서 암호화된 메세지 해독을 반복적으로 시도하여 오프라인 사전 공격을 마운트할 수도 있습니다.

Kerberos 프로토콜에 대한 자세한 정보는 다음 소스를 참조하십시오.

The Kerberos Network Authentication Service(V5)
IETF(Internet Engineering Task Force)는 RFC(Request for Comment) 1510에서 Kerberos 프로토콜을 정식으로 정의합니다.

Kerberos: The Network Authentication Protocol(V5)
Massachusetts Institute of Technology의 Kerberos 프로토콜에 대한 공식 문서에서 프로그래밍 정보를 제공하고 프로토콜 피처에 대해 설명합니다.

네트워크 인증 서비스 API(Application Programmable Interfaces)

이 Information Center 주제에서는 네트워크 인증 서비스 API 리스트와 해당 기능에 대한 간단한 설명을 제공합니다.

GSS(Generic Security Services) API

GSS API는 일반적으로 보안 서비스를 제공하고 Kerberos 프로토콜과 같은 보안 기술 범위에서 GSS API를 지원합니다. GSS API를 사용하면 GSS 어플리케이션을 다른 환경에 포트할 수 있습니다. 이러한 이유로 인해 Kerberos API 대신 GSS API를 사용할 것을 권장합니다. 같은 네트워크 내의 다른 어플리케이션 및 클라이언트와 통신하기 위해 GSS API를 사용하는 어플리케이션을 작성할 수 있습니다. 통신하는 각각의 어플리케이션들은 이러한 교환에서 일정한 역할을 수행합니다. GSS API를 사용하여 어플리케이션은 다음 조작을 수행할 수 있습니다.

- 다른 어플리케이션의 사용자 ID를 판별합니다.

- 다른 어플리케이션에 액세스 권한을 위임합니다.
- 하나의 메세지 단위로 기밀성 및 무결성 등의 보안 서비스를 적용합니다.

GSS API에 대한 자세한 정보는 다음 소스를 참조하십시오.

Generic Security Service Application Program Interface Version 2, Update 1
IETF(Internet Engineering Task Force)는 RFC 2743에 GSS API를 정식으로 정의합니다.

Generic Security Service API : C-bindings
IETF(Internet Engineering Task Force)는 RFC 1509에 GSS API C-바인딩을 지정합니다.

The Kerberos Version 5 GSS-API Mechanism
IETF(Internet Engineering Task Force)는 RFC 1964에 Kerveros 버전 5와 GSS API 스펙을 정의합니다.

GSS API(Generic Security Service Application Programmable Interface)
이 Information Center 주제에서는 GSS API 리스트와 해당 기능에 대한 간단한 설명을 제공합니다.

«

네트워크 인증 서비스 시나리오

»

다음 시나리오에서는 네트워크 인증 서비스를 사용하여 iSeries가 Kerberos 네트워크에 참여할 수 있는 일반적인 환경을 설명합니다. 다음 시나리오를 검토하여 네트워크 인증 서비스 구성에 관련된 기술 및 구성 세부사항을 익히십시오.

시나리오: 기존 KDC를 사용하여네트워크 인증 서비스 구성
이 주제에서는 키 분배 센터가 설치되고 구성된 Windows(R) 2000 환경에서 관리자가 네트워크 인증을 구성하는 고객의 상황을 설명합니다.

시나리오: 단일 사인 온 작동
이 시나리오에서는 EIM(Enterprise Identity Mapping)과 함께 네트워크 인증 서비스를 사용하여 단일 사인 온 작동 방법을 설명합니다. 사용자가 자신의 Windows(R) 2000 사인 온을 사용하여 iSeries 시스템과 Windows용 iSeries Access 어플리케이션을 인증하도록 관리자가 허용하고자 합니다.

시나리오: 기존 KDC를 사용하여 네트워크 인증 서비스 구성

상황

사용자는 회사에서 주문 수신 부서의 네트워크를 관리하는 네트워크 관리자입니다. 최근 부서에 필요한 여러 가지 어플리케이션이 있는 네트워크에 iSeries를 추가하였습니다. 영역에 대한 KDC(Key Distribution Center) 역할을 하는 Windows(R) 2000 서버가 갖추어져 있습니다. 이 네트워크 내의 사용자는 모두 KDC에 저장된 프린시펄명과 암호가 있습니다. iSeries를 KDC에 추가하고자 합니다. iSeries를 이 영역에 추가하고 계속해서 Windows(R) 2000 서버를 인증 서버로 사용할 계획입니다. GSS API를 사용하는 사용자 고유의 Kerberos 작동 어플리케이션이 있습니다.

이 시나리오에는 다음과 같은 장점이 있습니다.

- 사용자의 인증 프로세스를 단순화합니다.
- 네트워크에서 서버에 대한 액세스 관리 오버헤드를 덜어줍니다.
- 암호 노출 위험을 최소화합니다.

목적

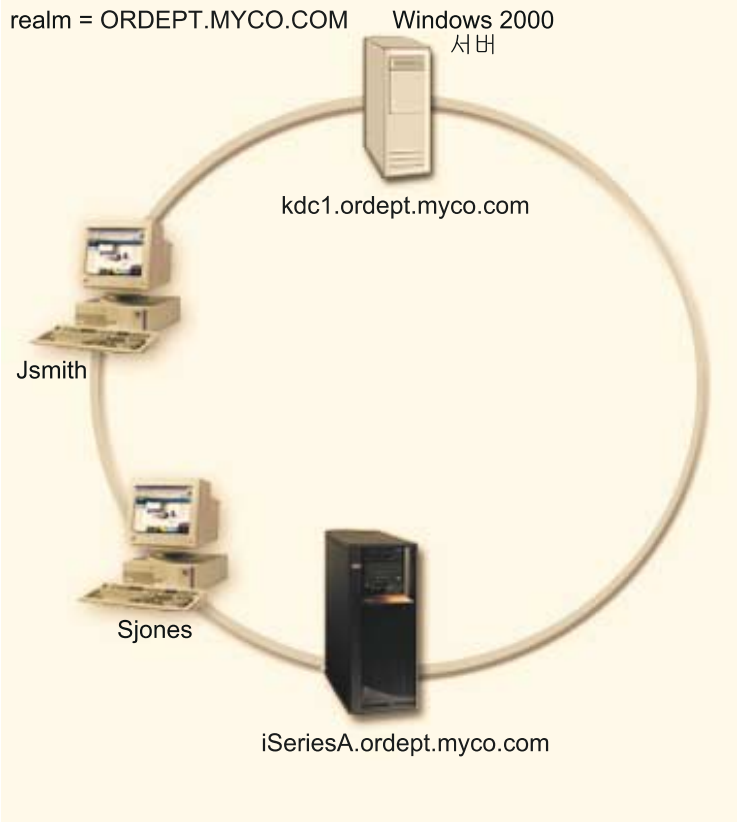
이 시나리오에서 MyCo Inc.는 Windows(R) 2000 서버가 키 분배 센터 역할을 하는 기존 영역에 iSeries 시스템을 추가하고자 합니다. iSeries에는 적절한 사용자가 액세스할 필요가 있는 업무에 중요한 여러 가지 어플리케이션이 있습니다. 사용자가 이 어플리케이션에 대한 액세스를 얻으려면 KDC가 사용자를 인증해야 합니다. iSeries를 Windows(R) 2000 서버의 KDC에 추가해야 합니다.

이 시나리오의 목적은 다음과 같습니다.

- iSeries가 기존의 키 분배 센터에 참여할 수 있게 합니다.
- 네트워크에 프린시펄명과 사용자명을 모두 허용합니다.
- Kerberos 사용자가 KDC에서 자신의 암호를 변경할 수 있습니다.

시나리오 세부사항

다음 그림에서는 MyCo의 네트워크 특성을 설명합니다.



주문 수신 부서

- iSeries-A는 OS/400 버전 5 릴리스 2(V5R2)에서 실행되며 여러 가지 업무 어플리케이션이 포함되어 있습니다.
- KDC의 DNS 이름은 kdc1.ordept.myco.com입니다.
- iSeries-A의 프린시펄명은 krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM입니다.
- KDC의 디폴트 영역은 ORDEPT.MYCO.COM입니다.
- 클라이언트 PC에서는 Windows(R) 2000을 실행합니다.

이 시나리오의 구성 단계

1. 네트워크 인증 서비스의 계획 작업용지와 체크 리스트를 완료(15 페이지 참조)하십시오.
2. iSeries-A에 네트워크 인증 서비스를 구성(16 페이지 참조)하십시오.
3. iSeries-A를 KDC에 추가(17 페이지 참조)하십시오.
4. iSeries-A의 각 사용자에 대한 홈 디렉토리를 작성(17 페이지 참조)하십시오.

5. iSeries-A에 대한 TCP/IP 정의역 정보를 확인(17 페이지 참조)하십시오.
6. iSeries-A의 네트워크 인증 서비스 구성을 테스트(18 페이지 참조)하십시오.

구성 세부사항

1단계: 계획 작업용지를 완료하십시오.

다음 계획 체크 리스트는 네트워크 인증 서비스 구성을 시작하기 전에 필요한 정보 유형을 설명합니다. 네트워크 인증 서비스 설정을 진행하려면 전제조건 체크 리스트의 모든 대답이 "예"이어야 합니다.

필수 체크 리스트	대답
OS/400이 V5R2(5722-SS1) 또는 그 이상입니까?	예
iSeries 시스템에 Cryptographic Access Provider(5722-AC3)가 설치되어 있습니까?	예
네트워크의 모든 PC와 iSeries 시스템에 Windows용 iSeries Access(5722-XE1)가 설치되어 있습니까?	예
네트워크의 모든 PC와 iSeries 시스템에 iSeries Navigator의 보안 부속 구성요소가 설치되어 있습니까?	예
네트워크의 모든 PC와 iSeries 시스템에 iSeries Navigator의 네트워크 부속 구성요소가 설치되어 있습니까?	예
*SECADM, *ALLOBJ, *IOSYSCFG 특수 권한이 있습니까?	예
키 분배 센터 역할을 하는 보안 시스템에 다음 중 하나를 설치했습니까? 그렇다면 어떤 종류를 설치했습니까? 1. Windows(R) 2000 서버 2. Windows(R) XP 서버 3. AIX 서버 4. zSeries	예 Windows(R) 2000 서버
Windows(R) 2000 서버 및 Windows (R) XP 서버의 경우, ktpass 툴을 제공하는 Windows(R) 지원 툴을 키 분배 센터로 사용하는 시스템에 설치했습니까?	예
Windows (R) 2000 정의역으로 구성된 네트워크에 모든 PC가 있습니까?	예
최신 프로그램 임시 수정(PTF)을 적용했습니까?	예
iSeries 시스템 시간과 KDC 시스템의 시간 차이가 5분 이내입니까? 그렇지 않으면 시스템 시간 동기화를 참조하십시오.	예

네트워크 인증 서비스를 구성하려면 이 정보가 필요합니다.	대답
iSeries-A가 속할 Kerberos 디폴트 영역의 이름은 무엇입니까?	ORDEPT.MYCO.COM

네트워크 인증 서비스를 구성하려면 이 정보가 필요합니다.	대답
이 Kerberos 디폴트 영역의 KDC는 무엇입니까? KDC가 청취하는 포트는 무엇입니까?	kdc1.ordept.myco.com 88(**주:** 이것은 KDC의 디폴트 포트입니다.)
이 디폴트 영역에 대한 암호 서버를 구성하시겠습니까? 구성할 경우, 다음 질문에 대답하십시오. 이 KDC에 대한 암호 서버명은 무엇입니까? 암호 서버가 청취하는 포트는 무엇입니까?	예 kdc1.ordept.myco.com 464(**주:** 이것은 암호 서버의 디폴트 포트입니다.)
iSeries 서비스 프린시펄의 암호는 무엇입니까?	iseriesa123 **주:** 이 시나리오에서 사용한 모든 암호는 단지 예를 들기 위한 암호입니다. 실제로 구성하는 동안에는 사용하지 마십시오.
iSeries 시스템은 어떤 추가 영역과 대화합니까?	해당 없음
각 영역에 대하여 키 분배 센터의 호스트명은 무엇입니까?	해당 없음

2단계: iSeries-A에 네트워크 인증 서비스를 구성하십시오.

작업용지의 정보를 사용하여 다음과 같이 iSeries-A에 네트워크 인증 서비스를 구성하십시오.

1. iSeries Navigator에서 **iSeries-A —> 보안**을 확장하십시오.
2. **네트워크 인증 서비스**를 마우스 오른쪽 버튼으로 클릭하고 **구성**을 선택하여 구성 마법사를 시작하십시오.
   주: 네트워크 인증 서비스를 구성한 후에 이 옵션은 **재구성**됩니다.
3. **시작** 페이지에서 마법사가 작성한 오브젝트에 대한 정보를 검토하십시오. **다음**을 클릭하십시오.
4. **영역 정보 지정** 페이지의 **디폴트 영역** 필드에 `ORDEPT.MYCO.COM`을 입력하십시오. **다음**을 클릭하십시오.
5. **KDC 정보 지정** 페이지의 **KDC** 필드에 `kdc1.ordept.myco.com`을 입력하고, **포트** 필드에 88을 입력하십시오. **다음**을 클릭하십시오.
6. **암호 정보 지정** 페이지에서 **예**를 선택하십시오. **암호 서버** 필드에 `kdc1.ordept.myco.com`을 입력하고, **포트** 필드에 464를 입력하십시오. **다음**을 클릭하십시오.
7. **키 표 항목 작성** 페이지에서 **iSeries Kerberos 인증**을 선택하십시오. **다음**을 클릭하십시오.
8. **iSeries 키 표 항목 작성** 페이지에서 iSeries-A용 키 표와 프린시펄을 기록해 두십시오. KDC에 추가할 때 프린시펄명이 필요합니다. 암호를 입력하고 확인하십시오. 예를 들어, Myco 관리자가 `iseriesa123`을 입력했습니다.
   주: 이 시나리오에서 사용한 모든 암호는 단지 예를 들기 위한 암호입니다. 실제로 구성하는 동안에는 사용하지 마십시오.
9. **다음**을 클릭하십시오.
10. **요약** 페이지에서 네트워크 인증 서비스 구성 세부사항을 검토하십시오. **완료**를 클릭하십시오.

이제 iSeries-A에서 네트워크 인증 서비스 구성을 완료했습니다. 다음 단계는 프린시펄명을 KDC에 추가하는 것입니다.

3단계: iSeries-A 프린시펄명을 KDC에 추가하십시오.

iSeries 시스템을 Windows(R) 2000 KDC에 추가하려면 KDC에 프린시펄 추가와 관련된 문서를 사용하십시오. 편의를 위해 iSeries 시스템명을 사용자명으로 사용할 수 있습니다. 다음 프린시펄명을 KDC에 추가하십시오.

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

Windows(R) 2000 서버에서 다음 단계를 수행하십시오.

1. Active Directory (R) Management 툴을 사용하여 iSeries 시스템용 사용자 계정을 작성하십시오. **사용자** 폴더를 선택한 후 마우스 오른쪽 버튼으로 클릭하고 **신규**를 선택한 다음, **사용자**를 선택하십시오. iSeriesA를 Active Directory 사용자로 지정하십시오.
2. Active Directory 사용자 iSeriesA의 등록 정보에 액세스하십시오. **계정** 탭에서 **계정이 위임에 대하여 신뢰됨**을 선택하십시오. 이렇게 하면 iSeries-A 서비스 프린시펄이 서명한 사용자를 대신해서 다른 서비스에 액세스할 수 있습니다.
3. **ktpass** 명령을 사용하여 사용자 계정을 프린시펄에 맵핑하십시오. Windows(R) 2000 서버 설치 CD의 **서비스 툴** 폴더에 ktpass 툴이 있습니다. 사용자 계정을 맵핑하려면 다음을 입력하십시오.

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

   여기에서 iseriesa123은 네트워크 인증 서비스를 구성(16 페이지 참조)할 때 지정한 암호입니다.
   주: 이 시나리오에서 사용한 모든 암호는 단지 예를 들기 위한 암호입니다. 실제로 구성하는 동안에는 사용하지 마십시오.

4단계: iSeries-A에 사용자를 위한 홈 디렉토리를 작성하십시오.

iSeries와 iSeries 어플리케이션에 연결하는 각 사용자는 /home 디렉토리에 디렉토리가 있어야 합니다. 이 디렉토리에는 사용자의 Kerberos 증명서 캐시명이 포함됩니다. 사용자의 홈 디렉토리를 작성하려면 다음을 완료하십시오.

1. iSeries 명령행에서 다음을 입력하십시오.
   ```
   CRTDIR '/home/username'
   ```
   여기에서 username은 사용자의 iSeries 사용자명입니다.
   예를 들어, MyCo의 관리자는 John Smith 사용자에 대하여
   `CRTDIR '/home/Johns'`를 입력했습니다.
2. 모든 사용자에 대하여 이 단계를 반복하십시오.

5단계: iSeries-A에 대한 TCP/IP 정의역 정보 확인

1. iSeries 명령행에서 다음을 입력하십시오.
   `CFGTCP`
2. 옵션 10을 선택하십시오(TCP/IP 호스트 표 항목에 대한 작업).
3. 호스트명 필드에 iSeries-A에 대한 완전 규정된 호스트명이 소문자인지 확인하십시오. 또한 복수 호스트명 항목이 있으면 완전 규정된 호스트명이 먼저 나타나는지 확인하십시오. 예를 들면, iSeries A는 다음 호스트명 항목을 가져야 합니다.
   iseriesa.ordept.myco.com.
4. 호스트명 항목을 확인한 후, F3을 눌러 TCP 구성 기본 메뉴로 리턴하십시오.
5. 옵션 12를 선택하십시오(TCP/IP 정의역 정보 변경).
6. 호스트명 필드에 사용자의 시스템명이 나타나는지 확인하십시오. 또한 사용자 정의역명이 올바른지 확인하십시오. 예를 들면, 호스트명은 `iseriesa`이고 정의역명은 `ordept.myco.com`이 됩니다.

6단계: iSeries-A에서 네트워크 인증 서비스 테스트

이 시점에서 iSeries-A 프린시펄명에 대한 티켓 부여 티켓을 요구하여 네트워크 인증 서비스를 올바르게 구성했는지 확인할 수 있습니다.

1. 명령행에서 `QSH`를 입력하여 Qshell 인터프리터를 시작하십시오.
2. `keytab list`를 입력하여 키 표 파일에 등록된 프린시펄 리스트를 표시하십시오. 이 시나리오에서는 iSeries-A의 프린시펄명으로 krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM이 표시됩니다.
   주: LDAP와 iSeries NetServer의 프린시펄을 구성하기로 선택한 경우, 키 표 파일에 다른 항목이 있습니다. 이 시나리오에서 관리자는 해당 서비스의 프린시펄을 구성하지 않기로 선택했습니다.
3. `kinit -k krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM`을 입력하십시오. 입력이 완료되면 QSH 명령이 오류없이 표시됩니다.
4. `klist`를 입력하여 디폴트 프린시펄이 krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM인지 확인하십시오.

시나리오: 단일 사인 온 작동

상황

사용자는 회사에서 주문 수신 부서의 네트워크를 관리하는 네트워크 관리자입니다. 현재 사용자에게 Windows(R) 2000 데스크탑이 있습니다. 사용자는 Windows ID 및 암호와 OS/400 사용자명을 관리해야 합니다. iSeries 인증을 위해 Windows(R) 2000 사인 온 사용을 허용하고자 합니다. Windows(R) 2000 ID와 OS/400 사용자명을 다르게 하거나 이 솔루션에서 제공하는 보안 문제 때문에 암호 캐싱이나 동기화를 사용하지 않으려고 합

니다. 서버에 네트워크 인증 서비스와 EIM(Enterprise Identity Mapping)을 구성하여 iSeries 서버에서 단일 사인 온을 작동할 수 있다는 사실을 알고 있습니다. 네트워크 인증 서비스를 사용하여 iSeries 시스템이 Window(R) 2000 정의역에 참여하는 동안 EIM이 Windows(R) 2000 ID를 기업망 내 사용자를 나타내는 단일 EIM ID에 연관시키는 메카니즘을 제공합니다. 이러한 연관으로 인해 네트워크의 Kerberos 프린시펄은 자신의 iSeries 사용자명과 암호를 사용하여 등록하지 않아도 일부 iSeries 어플리케이션에 액세스할 수 있습니다. 단일 사인 온 사용에 대한 장점 EIM과 네트워크 인증 서비스를 함께 작동하는 방법에 대한 자세한 내용은 단일 사인 온 작동을 참조하십시오.

시나리오 장점

이 시나리오에는 다음과 같은 장점이 있습니다.

- 사용자의 인증 프로세스를 단순화합니다.
- 네트워크에서 서버에 대한 액세스 관리 오버헤드를 덜어줍니다.
- 암호 노출 위험을 최소화합니다.
- 복수 사인 온을 사용할 필요가 없습니다.
- 네트워크에서 사용자 ID 관리를 단순화합니다.

목적

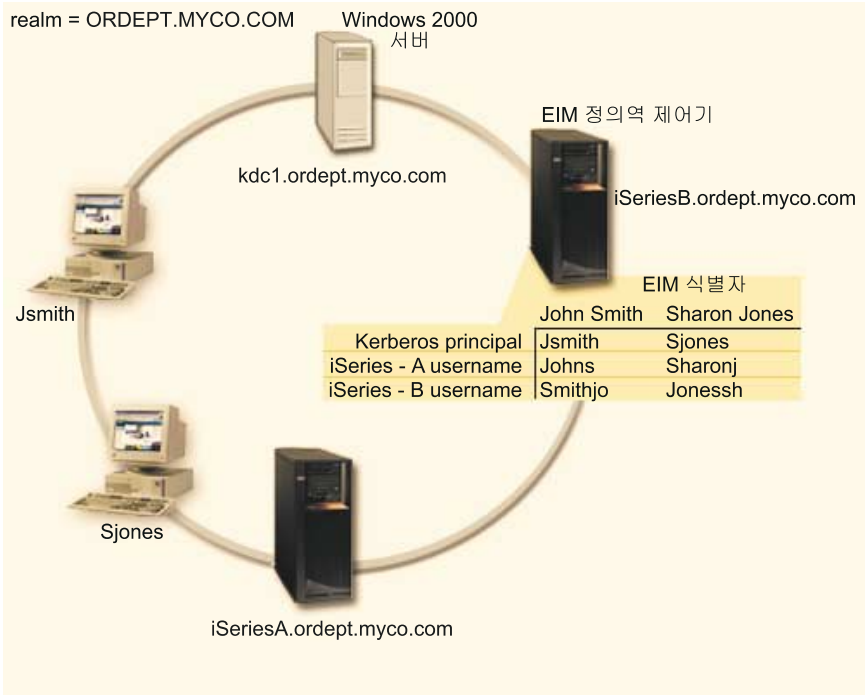
이 시나리오에서 MyCo Inc.는 인증을 목적으로 iSeries 시스템을 기존의 Windows(R) 2000 정의역에 추가하고자 합니다. iSeries 시스템에는 사용자가 액세스할 필요가 있는 여러 가지 어플리케이션이 포함되어 있습니다. 사용자가 이 어플리케이션에 대한 액세스를 얻으려면 KDC가 사용자를 인증해야 합니다. 프린시펄이 서비스 티켓을 요구하도록 허용하려면 iSeries 서비스 프린시펄을 Windows(R) 2000 서버의 KDC에 추가해야 합니다. 또한 EIM을 구성한 다음 연관을 작성하여 OS/400 사용자 프로파일과 Kerberos 프린시펄을 기업망의 단일 사용자를 나타내는 EIM ID에 맵핑합니다. 주문 수신 부서의 사용자가 Windows용 iSeries Access 어플리케이션을 사용하기 때문에 Windows용 iSeries Access 및 관련 어플리케이션에 대한 우선 인증 방법으로 Kerberos 프린시펄을 사용하기로 결정했습니다.

이 시나리오의 목적은 다음과 같습니다.

- iSeries-A와 iSeries-B가 기존의 키 분배 센터에 참여할 수 있게 합니다.
- iSeries-B의 디렉토리 서버를 정의역에 대한 EIM 정의역 제어기로 작동하도록 구성합니다.
- iSeries-A와 Series-B의 사용자 프로파일 및 Kerberos 프린시펄을 단일 EIM ID에 맵핑할 수 있게 합니다.
- Kerberos 프린시펄을 사용하여 Windows용 iSeries Access 어플리케이션에 인증합니다.

시나리오 세부사항

다음 그림에서는 MyCo의 네트워크 특성을 설명합니다.



주문 수신 부서

- iSeries-A와 iSeries-B는 OS/400 버전 5 릴리스 2(V5R2)에서 실행되며 여러 가지 업무 어플리케이션이 포함되어 있습니다.
- KDC 이름은 `kdc1.ordept.myco.com`입니다.
- iSeries-A의 프린시펄명은 `krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM`입니다.
- iSeries-A의 DNS 이름은 `iSeriesA.ordept.myco.com`입니다.
- KDC의 디폴트 영역은 `ORDEPT.MYCO.COM`입니다.
- iSeries-B의 디렉토리 서버(LDAP)는 네트워크의 EIM 정의역 제어기 역할을 하도록 구성됩니다.
  주: EIM을 구성하기 전에 LDAP 구성을 완료해야 합니다. LDAP를 시스템에 구성하지 않은 경우, EIM 구성 마법사에서 LDAP 구성을 제공합니다. 이 시나리오의 경우, iSeries-B에 LDAP가 구성되어 있지 않습니다. EIM을 구성하는 동안 관리자는 LDAP를 구성할 계획입니다.
- iSeries-B의 DNS 이름은 `iSeriesB.ordept.myco.com`입니다.
- iSeries-B의 프린시펄명은 `krbsvr400/iSeriesB.ordept.myco.com@ORDEPT.MYCO.COM`입니다.
- 클라이언트 PC에서는 Windows(R)2000을 실행합니다.
- Kerberos 프린시펄인 Jsmith와 Sjones가 KDC에 등록되어 있습니다.

이 시나리오의 구성 단계

1. iSeries-A와 iSeries-B에 대한 계획 작업용지를 완료(21 페이지 참조)하십시오.
2. iSeries-A에 네트워크 인증 서비스를 구성(23 페이지 참조)하십시오.
3. iSeries-A 서비스 프린시펄을 KDC에 추가(23 페이지 참조)하십시오.

4. iSeries-A의 각 사용자에 대한 홈 디렉토리를 작성(24 페이지 참조)하십시오.
5. iSeries-A에 대한 TCP/IP 정의역 정보를 확인(24 페이지 참조)하십시오.
6. iSeries-A의 네트워크 인증 서비스 구성을 테스트(25 페이지 참조)하십시오.
7. iSeries-B에서 2 - 6단계를 반복하십시오.
8. EIM 정의역을 구성(25 페이지 참조)하고 iSeries-B의 디렉토리 서버를 EIM 정의역 제어기로 구성하십시오.
9. iSeries-A가 EIM 정의역에 참여하도록 구성(26 페이지 참조)하십시오.
10. 기업망의 사용자에 대한 EIM ID를 작성(27 페이지 참조)하십시오.
11. OS/400 사용자 프로파일 및 프린시펄명에 대한 EIM 연관을 EIM ID에 추가(28 페이지 참조)하십시오.

12. 인증 방법으로 Kerberos 프린시펄을 사용하도록 Windows용 iSeries Access 연결을 구성(29 페이지 참조)하십시오.
13. 네트워크 인증 서비스와 EIM 설정을 확인(29 페이지 참조)하십시오.

구성 세부사항

1단계: 계획 작업용지를 완료하십시오.

다음 계획 체크 리스트는 네트워크 인증 서비스와 EIM(Enterprise Identity Mapping) 구성을 시작하기 전에 필요한 정보 유형을 설명합니다. 네트워크 인증 서비스 설정을 진행하려면 필수 체크 리스트의 모든 대답이 "예"이어야 하고 네트워크 인증 구성을 위한 정보가 완전해야 합니다.

필수 체크 리스트	대답
OS/400이 V5R2(5722-SS1) 또는 그 이상입니까?	예
iSeries 시스템에 Cryptographic Access Provider(5722-AC3)가 설치되어 있습니까?	예
네트워크의 모든 PC와 iSeries 시스템에 Windows용 iSeries Access(5722-XE1)가 설치되어 있습니까?	예
네트워크의 모든 PC와 iSeries 시스템에 iSeries Navigator의 보안 부속 구성 요소가 설치되어 있습니까?	예

네트워크의 모든 PC와 iSeries 시스템에 iSeries Navigator의 네트워크 부속 구성요소가 설치되어 있습니까?	예
*SECADM, *ALLOBJ, *IOSYSCFG 특수 권한이 있습니까?	예
키 분배 센터 역할을 하는 다음 시스템 중 하나가 있습니까? 어떤 종류입니까? 1. Windows(R) 2000 서버 2. Windows(R) XP 서버 3. AIX 서버 4. zSeries	예 Windows(R) 2000 서버
Windows(R) 2000 서버 및 Windows (R) XP 서버의 경우, ktpass 툴을 제공하는 Windows 지원 툴을 설치했습니까?	예
Windows (R) 2000 정의역으로 구성된 네트워크에 모든 PC가 있습니까?	예
최신 프로그램 임시 수정(PTF)을 적용했습니까?	예
iSeries 시스템 시간과 KDC 시스템의 시간 차이가 5분 이내입니까? 그렇지 않으면 시스템 시간 동기화를 참조하십시오.	예

네트워크 인증 서비스를 구성하려면 이 정보가 필요합니다.	**대답**
iSeries가 속할 Kerberos 디폴트 영역의 이름은 무엇입니까?	ORDEPT.MYCO.COM
이 Kerberos 디폴트 영역의 KDC는 무엇입니까? KDC가 청취하는 포트는 무엇입니까?	kdc1.ordept.myco.com 88(**주:** 이것은 KDC의 디폴트 포트입니다.)
이 디폴트 영역에 대한 암호 서버를 구성하시겠습니까? 구성할 경우, 다음 질문에 대답하십시오. 이 KDC에 대한 암호 서버명은 무엇입니까? 암호 서버가 청취하는 포트는 무엇입니까?	예 kdc1.ordept.myco.com 464(**주:** 이것은 암호 서버의 디폴트 포트입니다.)
iSeries 서비스 프린시펄의 암호는 무엇입니까?	iseriesa123 iseriesb345 **주:** 이 시나리오에서 사용한 모든 암호는 단지 예를 들기 위한 암호입니다. 실제로 구성하는 동안에는 사용하지 마십시오.
iSeries는 어떤 추가 영역과 대화합니까?	해당 없음
각 영역에 대하여 키 분배 센터의 호스트명은 무엇입니까?	해당 없음

EIM(Enterprise Identity Mapping)을 구성하려면 이 정보가 필요합니다.	**대답**
LDAP 관리자의 식별명과 암호는 무엇입니까?	식별명: cn=administrator 암호: mycopwd **주:** 이 시나리오에서 사용한 모든 암호는 단지 예를 들기 위한 암호입니다. 실제로 구성하는 동안에는 사용하지 마십시오.
디렉토리 서비스(LDAP) 서버의 이름은 무엇입니까?	iSeriesB.ordept.myco.com
디렉토리 서비스(LDAP) 서버의 포트 번호는 무엇입니까?	389

2단계: iSeries-A에 네트워크 인증 서비스를 구성하십시오.

다음 타스크를 완료하여 iSeries-A에 네트워크 인증 서비스를 구성하려면 작업용지의 정보를 사용하십시오.

1. iSeries Navigator에서 **iSeries-A —> 보안**을 확장하십시오.
2. **네트워크 인증 서비스**를 마우스 오른쪽 버튼으로 클릭하고 **구성**을 선택하여 구성 마법사를 시작하십시오.
   주: 네트워크 인증 서비스를 구성한 후에 이 옵션은 **재구성**됩니다.
3. **시작** 페이지에서 마법사가 작성한 오브젝트에 대한 정보를 검토하십시오. **다음**을 클릭하십시오.
4. **영역 정보 지정** 페이지의 **디폴트 영역** 필드에 ORDEPT.MYCO.COM을 입력하십시오. **다음**을 클릭하십시오.
5. **KDC 정보 지정** 페이지의 **KDC** 필드에 kdc1.ordept.myco.com을 입력하고, **포트** 필드에 88을 입력하십시오. **다음**을 클릭하십시오.
6. **암호 정보 지정** 페이지에서 **예**를 선택하십시오. **암호 서버** 필드에 kdc1.ordept.myco.com을 입력하고, **포트** 필드에 464를 입력하십시오. **다음**을 클릭하십시오.
   주: 암호는 프린시펄을 KDC에 추가할 때 입력한 암호와 같아야 합니다.
7. **키 표 항목 작성** 페이지에서 **iSeries Kerberos 인증**을 선택하십시오. **다음**을 클릭하십시오.
8. **iSeries 키 표 항목 작성** 페이지에서 iSeries-A용 키 표와 프린시펄을 기록해 두십시오. KDC에 추가할 때 프린시펄명이 필요합니다. 암호를 입력하고 확인하십시오. 예를 들어, Myco 관리자가 iseriesa123을 사용했습니다. iSeries-A를 KDC에 추가할 때 이 암호를 사용합니다.
   주: 이 시나리오에서 사용한 모든 암호는 단지 예를 들기 위한 암호입니다. 실제로 구성하는 동안에는 사용하지 마십시오. **다음**을 클릭하십시오.
9. **요약** 페이지에서 네트워크 인증 서비스 구성 세부사항을 검토하십시오. **완료**를 클릭하십시오.

이제 iSeries-A에서 네트워크 인증 서비스 구성을 완료했습니다. 다음 단계는 프린시펄명을 KDC에 추가하는 것입니다.

3단계: iSeries-A 프린시펄명을 KDC에 추가하십시오.

iSeries를 Windows(R) 2000 KDC에 추가하려면 KDC에 프린시펄 추가와 관련된 문서를 사용하십시오. 편의를 위해 iSeries 이름을 사용자명으로 사용할 수 있습니다. 다음 프린시펄명을 KDC에 추가하십시오.

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

Windows(R) 2000 서버에서 다음 단계를 수행하십시오.

1. Active Directory (R) Management 툴을 사용하여 iSeries-A용 사용자 계정을 작성하십시오. **사용자** 폴더를 선택하고, 마우스 오른쪽 버튼으로 클릭하고, **신규**를 선택한 다음 **사용자**를 선택하십시오. iSeriesA를 Active Directory 사용자로 지정하십시오.
2. Active Directory 사용자 iSeriesA의 등록 정보에 액세스하십시오. **계정** 탭에서 **계정이 위임에 대하여 신뢰됨**을 선택하십시오. 이렇게 하면 iSeries-A 서비스 프린시펄이 서명한 사용자를 대신해서 다른 서비스에 액세스할 수 있습니다.
3. **ktpass** 명령을 사용하여 사용자 계정을 프린시펄에 맵핑하십시오. Windows(R) 2000 서버 설치 CD의 **서비스 툴** 폴더에 ktpass 툴이 있습니다. 사용자 계정을 맵핑하려면 다음을 입력하십시오.

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

   여기에서 iseriesa123은 네트워크 인증 서비스를 구성(23 페이지 참조)할 때 6단계에서 지정한 암호입니다.

   주: 이 시나리오에서 사용한 모든 암호는 단지 예를 들기 위한 암호입니다. 실제로 구성하는 동안에는 사용하지 마십시오.

4단계: iSeries-A에 사용자를 위한 홈 디렉토리를 작성하십시오.

iSeries와 iSeries 어플리케이션에 연결하는 각 사용자는 /home 디렉토리에 디렉토리가 있어야 합니다. 이 디렉토리에는 사용자의 Kerberos 증명서 캐시명이 포함됩니다. 사용자의 홈 디렉토리를 작성하려면 다음을 완료하십시오.

1. iSeries 명령행에서 다음을 입력하십시오.

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

   여기에서 username은 사용자의 iSeries 사용자명입니다.
   예를 들어, MyCo의 관리자는 John Smith 사용자에 대하여
   `CRTDIR '/home/Johns'`를 입력했습니다.
2. 모든 사용자에 대하여 이 단계를 반복하십시오.

5단계: iSeries A에 대한 TCP/IP 정의역 정보를 확인하십시오

1. iSeries 명령행에서 다음을 입력하십시오.

   ```
   CFGTCP
   ```
2. 옵션 10을 선택하십시오(TCP/IP 호스트 표 항목에 대한 작업).

3. 호스트명 필드에 iSeries A에 대한 완전 규정된 호스트명이 소문자인지 확인하십시오. 또한 복수 호스트명 항목이 있으면 완전 규정된 호스트명이 먼저 나타나는지 확인하십시오. 예를 들면, iSeries A는 다음 호스트명 항목을 가져야 합니다.
   iseriesa.ordept.myco.com.
4. 호스트명 항목을 확인한 후, F3을 눌러 TCP 구성 기본 메뉴로 리턴하십시오.
5. 옵션 12를 선택하십시오(TCP/IP 정의역 정보 변경).
6. 호스트명 필드에 사용자의 시스템명이 나타나는지 확인하십시오. 또한 사용자 정의역명이 올바른지 확인하십시오. 예를 들면, 호스트명은 `iseriesa`이고 정의역명은 `ordept.myco.com`이 됩니다.

6단계: iSeries-A에서 네트워크 인증 서비스를 테스트하십시오.

이 시점에서 iSeries-A 프린시펄명에 대한 티켓 부여 티켓을 요구하여 네트워크 인증 서비스를 올바르게 구성했는지 확인할 수 있습니다.

1. 명령행에서 `QSH`를 입력하여 Qshell 인터프리터를 시작하십시오.
2. `keytab list`를 입력하여 키 표 파일에 등록된 프린시펄 리스트를 표시하십시오. 이 시나리오에서는 iSeries-A의 프린시펄명으로 krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM이 표시됩니다.
3. `kinit -k krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM`을 입력하십시오. 입력이 완료되면 QSH 명령이 오류없이 표시됩니다.
4. `klist`를 입력하여 디폴트 프린시펄이 krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM인지 확인하십시오.

7단계: iSeries-B에 대한 2와 6단계를 반복하십시오.

단계: iSeries-B에서 EIM 및 EIM 정의역 제어기를 구성하십시오.

이제 네트워크에 EIM 정의역을 구성해야 합니다. 또한 iSeries-B가 신규 EIM 정의역에 대한 EIM 정의역 제어기가 되도록 구성해야 합니다. 이 단계를 완료하면 다음 타스크가 완료됩니다.

- 새로운 EIM 정의역 작성
- iSeries-B의 디렉토리 서버를 EIM 정의역 제어기로 구성
- iSeries-B용 EIM 레지스트리와 Kerberos 사용자 레지스트리를 정의역에 작성
- iSeries-B가 EIM 정의역에 참여하도록 구성

1. iSeries Navigator에서 **iSeries-B —> 네트워크 —> EIM(Enterprise Identity Mapping)**을 확장하십시오.
2. **구성**을 마우스 오른쪽 버튼으로 클릭하고 **구성**을 선택하여 구성 마법사를 시작하십시오.
3. **시작** 페이지에서 **신규 정의역 작성 및 결합**을 선택하십시오. **다음**을 클릭하십시오.

4. **디렉토리 서버 구성** 페이지의 **포트** 필드에서 디폴트 389를 허용하십시오. **식별명** 필드에 cn=administrator를 입력하십시오. 암호를 입력하고 확인하십시오. EIM 정의역 관리 타스크에 액세스할 때 이 암호를 사용합니다. 예를 들어, MyCo 관리자가 암호 필드와 암호 확인 필드에 mycopwd를 입력했습니다.
   주: 이 시나리오에서 사용한 모든 암호는 단지 예를 들기 위한 암호입니다. 실제로 구성하는 동안에는 사용하지 마십시오. **다음**을 클릭하십시오.
5. **정의역 지정** 페이지에서 정의역명을 입력하십시오. 예를 들어, MyCo 관리자가 **정의역** 필드에 mycoeimDomain을 입력했습니다.
   주: 정의역명에는 = + < > , # ; \, *를 포함할 수 없습니다. **설명** 필드는 선택적입니다. 원할 경우, 정의역 제어기에 대한 간단한 설명을 입력하십시오. **다음**을 클릭하십시오.
6. **정의역의 상위 DN 지정** 페이지에서 **아니오**를 선택하십시오. **다음**을 클릭하십시오.
7. **레지스트리 정보** 페이지에서 **로컬 OS/400** 및 **Kerberos**를 선택하십시오. **Kerberos 사용자 ID는 대소문자를 구분함**을 선택하십시오. **다음**을 클릭하십시오. 레지스트리명을 기록해 두십시오. EIM ID에 대한 연관을 작성할 경우 이 레지스트리명이 필요합니다.
   주: 레지스트리명은 정의역에 대하여 고유해야 합니다.
8. **EIM 시스템 사용자 지정** 페이지에서 시스템 EIM 사용자를 선택하십시오. 이 페이지에 나타나는 디폴트를 허용하십시오. 예를 들어, 이 페이지에서 MyCo는 다음과 같은 정보를 가지고 있습니다.
   - 사용자 유형: 식별명 및 암호
   - 식별명: cn=administrator
   - 암호: mycopwd
     주: 이 시나리오에서 사용한 모든 암호는 단지 예를 들기 위한 암호입니다. 실제로 구성하는 동안에는 사용하지 마십시오.

   다음을 클릭하십시오.
9. **요약** 페이지에서 EIM 구성 정보를 확인하십시오. **완료**를 클릭하십시오.

iSeries-B의 디렉토리 서버를 네트워크에 새로 구성한 EIM 정의역에 대한 EIM 정의역 제어기로 구성했습니다. 이제 iSeries-A를 이 EIM 정의역의 참여자로 지정해야 합니다.

iSeries-A가 EIM 정의역에 참여하도록 구성해야 합니다.

1. iSeries Navigator에서 **iSeries-A —> 네트워크 —> 기업망 ID 맵핑**을 확장하십시오.
2. **구성**을 마우스 오른쪽 버튼으로 클릭하고 **구성**을 선택하여 구성 마법사를 시작하십시오.
3. **시작** 페이지에서 **기존 정의역 결합**을 선택하십시오. **다음**을 클릭하십시오.
4. **정의역 제어기 지정** 페이지에서 정의역 제어기명을 입력하십시오. 예를 들어, MyCo 관리자가 **정의역 제어기명** 필드에 iSeriesB.ordept.myco.com을 입력했습니다. **다음**을 클릭하십시오.
5. **연결을 위해 사용자 지정** 페이지에서 사용자 유형에 대하여 **식별명 및 암호**를 선택하십시오. 예를 들어, MyCo의 관리자가 **식별명** 필드에 cn=administrator를 입력하고 암호 필드와 암호 확인 필드에 mycopwd를 입력했습니다.
   주: 이 시나리오에서 사용한 모든 암호는 단지 예를 들기 위한 암호입니다. 실제로 구성하는 동안에는 사용하지 마십시오. **다음**을 클릭하십시오.

6. **정의역 지정** 페이지에서 참여할 정의역명을 선택하십시오. **다음**을 클릭하십시오. 예를 들어, MyCo 관리자가 **mycoeimDomain**을 선택했습니다.
7. **레지스트리 정보** 페이지에서 **로컬 OS/400**을 선택하십시오. **다음**을 클릭하십시오. 레지스트리명을 기록해 두십시오. EIM ID에 대한 연관을 작성할 경우 이 레지스트리명이 필요합니다.
   주: 레지스트리명은 정의역에 대하여 고유해야 합니다.
8. **EIM 시스템 사용자 지정** 페이지에서 시스템 EIM 사용자를 선택하십시오. 이 페이지에 나타나는 디폴트를 허용하십시오. 예를 들어, 이 페이지에서 MyCo는 다음과 같은 정보를 가지고 있습니다.
   - 사용자 유형: 식별명 및 암호
   - 식별명: cn=administrator
   - 암호: mycopwd
     주: 이 시나리오에서 사용한 모든 암호는 단지 예를 들기 위한 암호입니다. 실제로 구성하는 동안에는 사용하지 마십시오.

   다음을 클릭하십시오.
9. **요약** 페이지에서 EIM 구성을 확인하십시오. **완료**를 클릭하십시오.

이제 iSeries-A가 정의역에 참여하도록 구성되었습니다.

이제 기업망의 각 사용자에 대하여 EIM ID를 작성해야 합니다. EIM ID는 네트워크의 사용자나 엔티티를 나타냅니다. MyCo의 경우 관리자가 두 개의 EIM ID, John Smith와 Sharon Jones를 작성했습니다.

1. iSeries-B에서 **네트워크 —> 기업망 ID 맵핑**을 확장하십시오.
2. **정의역 관리**를 마우스 오른쪽 버튼으로 클릭하고 **정의역 추가...**를 선택하십시오.
3. **정의역 추가** 대화 상자에서 MyCo의 EIM 정의역에 대하여 다음 디폴트가 표시됩니다.
   - 포트: 389
   - 정의역: mycoeimDomain
   - 상위 DN: 없음
   - 정의역 제어기: iSeriesB.ordept.myco.com

   주: EIM 정의역 제어기를 구성하는 동안 이 디폴트가 작성되었습니다.
4. **확인**을 클릭하십시오.
5. iSeries Navigator 계층이 **정의역 관리**의 **mycoeimDomain**으로 화면정리됩니다. **mycoeimDomain**을 클릭하십시오. **EIM 정의역 제어기에 연결** 대화 상자가 프롬트됩니다. 정의역을 관리하려면 먼저 EIM 정의역 제어기에 연결해야 합니다.
6. **EIM 정의역 제어기에 연결** 페이지에서 정의역 제어기 관리자의 식별명과 암호를 입력하십시오. 이 이름과 암호는 EIM 정의역 제어기를 구성하는 동안 작성된 식별명 및 암호와 같습니다. MyCo의 경우 관리자가 다음을 입력했습니다.
   - 식별명: cn=administrator

- 암호: mycopwd
  주: 이 시나리오에서 사용한 모든 암호는 단지 예를 들기 위한 암호입니다. 실제로 구성하는 동안에는 사용하지 마십시오.

7. **확인**을 클릭하십시오.
8. 두 개의 새로운 폴더가 표시됩니다. **ID**를 마우스 오른쪽 버튼으로 클릭하고 **신규 ID**를 선택하십시오.
9. **신규 EIM ID** 페이지의 **ID** 필드에 ID를 입력하십시오. 모든 사용자가 ID를 가지게 될 때까지 이 단계를 반복하십시오. MyCo에서 다음 ID를 추가했습니다.
   - John Smith
   - Sharon Jones
10. **확인**을 클릭하십시오.

이제 John Smith와 Sharon Jones에 대하여 고유한 EIM ID가 작성되었습니다. iSeries-A와 iSeries-B에 있는 이들의 OS/400 사용자명과 Kerberos 프린시펄을 이 EIM ID에 연관시킬 수 있습니다.

11단계: OS/400 사용자 프로파일과 프린시펄명에 대한 EIM 연관성을 EIM ID에 추가하십시오.

이 타스크를 완료하기 위해 MyCo의 관리자는 다음 단계를 완료했습니다.

1. iSeries-B에서 **ID**를 확장하고 **John Smith**를 마우스 오른쪽 버튼으로 클릭한 후 **등록 정보**를 선택하십시오. 이 ID에 대한 세 개의 연관이 있는데, Kerberos 프린시펄, iSeries-A의 사용자 프로파일 및 iSeries-B의 사용자 프로파일입니다.
2. Kerberos 프린시펄을 ID, John Smith와 연관시키려면 다음을 수행하십시오.
   a. **연관** 탭에서 **추가**를 클릭하십시오.
   b. **연관 추가** 페이지의 **레지스트리** 필드에서 **찾아보기**를 클릭하고 ORDEPT.MYCO.COM을 선택하십시오. 이것은 EIM을 구성하는 동안 추가된 Kerberos 사용자 레지스트리입니다.
   c. **사용자** 필드에서 Jsmith를 입력하십시오.
   d. **연관 유형** 필드에서 **소스**를 선택하십시오.
   e. **확인**을 클릭하십시오.
3. iSeries-A의 사용자명을 ID, John Smith와 연관시키려면 다음을 수행하십시오.
   a. **연관** 탭에서 **추가**를 클릭하십시오.
   b. **연관 추가** 페이지의 **레지스트리** 필드에서 **찾아보기**를 클릭하고 iSeriesA.ordept.mycomcom을 선택하십시오. 이것은 iSeries-A용 OS/400 사용자 레지스트리입니다.
   c. **사용자** 필드에서 Johns를 입력하십시오.
   d. **연관 유형** 필드에서 **목표**를 선택하십시오.
   e. **확인**을 클릭하십시오.
4. iSeries-B의 사용자명을 ID, John Smith와 연관시키려면 다음을 수행하십시오.
   a. **연관** 탭에서 **추가**를 클릭하십시오.

b. **연관 추가** 페이지의 **레지스트리** 필드에서 **찾아보기**를 클릭하고 iSeriesB.ordept.mycomcom을 선택하십시오. 이것은 iSeries-B에서 OS/400 사용자 레지스트리입니다.

c. **사용자** 필드에서 Smithjo를 입력하십시오.

d. **연관 유형** 필드에서 **목표**를 선택하십시오.

e. **확인**을 클릭하십시오.

5. EIM ID, Sharon Jones에 대해 1 - 4단계를 반복하십시오.

이제 Jsmith와 Sjones PC의 Windows용 iSeries Access 어플리케이션에서 iSeries-A와 iSeries-B에 대해 인증할 경우, Kerberos를 사용하도록 구성해야 합니다.

Jsmith의 PC에서 iSeries-A와 iSeries-A의 어플리케이션에서 다음 단계를 완료하여 Kerberos 인증을 사용하도록 구성하십시오.

1. iSeries Navigator에서 **iSeries-A**를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
2. **연결** 탭에서 **프롬트없이 Kerberos 프린시펄명 사용**을 선택하십시오. 이렇게 하면 Windows용 iSeries Access 연결에서 인증을 위하여 Kerberos 프린시펄명과 암호를 사용할 수 있습니다.
3. iSeries-B에 대하여 이 단계를 반복하십시오.
4. Sjones의 PC에서 이 단계를 반복하십시오.

13단계: 네트워크 인증 서비스 및 EIM 설정을 확인하십시오.

이 시점에서 모든 구성 단계가 완료됩니다. 네트워크 인증 서비스와 EIM이 올바르게 설정되었는지 확인하기 위하여 관리자는 Sharon Jones와 John Smith가 자신들 PC에 등록함으로써 Windows(R) 2000 정의역에 로그온하도록 합니다. 그런 다음 iSeries-A에서 iSeries Navigator를 열도록 합니다. iSeries 사인 온 프롬트가 표시되지 않으면, EIM에서 Kerberos 프린시펄을 정의역의 ID에 성공적으로 맵핑한 것입니다. Windows용 iSeries Access 어플리케이션 외에 다음과 같은 어플리케이션에서도 Kerberos 인증을 지원합니다.

- Telnet 서버
- iSeries NetServer
- QFileSrv.400
- DRDA(분산 관계형 데이터베이스 구조)

네트워크 인증 서비스 계획

네트워크 인증 서비스를 제대로 구성하려면 요구사항을 이해하고 필요한 계획 단계를 완료해야 합니다. 이 주제에서는 필요한 모든 단계를 완료할 수 있도록 필수 체크 리스트와 계획 작업용지를 제공합니다. 다음 체크 리스트와 작업용지를 사용하여 네트워크 인증 서비스를 구성하는 데 도움을 받을 수 있습니다.

필수 체크 리스트	대답
OS/400이 V5R2(5722-SS1) 또는 그 이상입니까?	
iSeries 시스템에 Cryptographic Access Provider(5722-AC3)가 설치되어 있습니까?	
네트워크의 모든 PC와 iSeries 시스템에 Windows용 iSeries Access(5722-XE1)가 설치되어 있습니까?	
네트워크의 모든 PC와 iSeries 시스템에 iSeries Navigator의 보안 부속 구성요소가 설치되어 있습니까?	
네트워크의 모든 PC와 iSeries 시스템에 iSeries Navigator의 네트워크 부속 구성요소가 설치되어 있습니까?	
*SECADM, *ALLOBJ, *IOSYSCFG 특수 권한이 있습니까?	
키 분배 센터 역할을 하는 보안 시스템에 다음 중 하나를 설치했습니까? 어떤 종류입니까? 1. Windows(R) 2000 서버 2. Windows(R) XP 서버 3. AIX 서버 4. zSeries	
Windows(R) 2000 서버 및 Windows (R) XP 서버의 경우 ktpass 툴을 제공하는 Windows 지원 툴을 키 분배 센터로 사용할 시스템에 설치했습니까?	
Windows (R) 2000 정의역으로 구성된 네트워크에 모든 PC가 있습니까?	
최신 프로그램 임시 수정(PTF)을 적용했습니까?	
iSeries 시스템 시간과 KDC 시스템의 시간 차이가 5분 이내입니까? 그렇지 않으면 시스템 시간 동기화를 참조하십시오.	

네트워크 인증 서비스를 구성하려면 이 정보가 필요합니다.	대답
iSeries-A가 속할 Kerberos 디폴트 영역의 이름은 무엇입니까?	
이 Kerberos 디폴트 영역의 KDC는 무엇입니까? KDC가 청취하는 포트는 무엇입니까?	
이 디폴트 영역에 대한 암호 서버를 구성하시겠습니까? 구성할 경우 다음 질문에 대답하십시오. 이 KDC에 대한 암호 서버명은 무엇입니까? 암호 서버가 청취하는 포트는 무엇입니까?	
iSeries 서비스 프린시펄의 암호는 무엇입니까?	
iSeries는 어떤 추가 영역과 대화합니까?	
각 영역에 대하여 키 분배 센터의 호스트명은 무엇인가?	
iSeries의 어플리케이션이 사용할 서비스 프린시펄명은 무엇입니까?	

네트워크 인증 서비스 구성

네트워크 인증 서비스를 구성하기 전에 필요한 모든 계획 단계를 완료해야 합니다. 추가로 네트워크 인증 서비스에서는 사용자가 네트워크의 보안 시스템에 KDC(Key Distribution Center)를 구성했다고 가정합니다. 현재 iSeries에서는 KDC를 지원하지 않습니다. Microsoft Windows (R) 2000과 Windows(R) XP 및 z/OS에서는 KDC 기능을 지원합니다. KDC로 사용할 시스템의 Kerberos 구성에 해당하는 문서를 참조하십시오.

iSeries에 네트워크 인증 서비스를 구성하기 전에 KDC를 구성할 것을 권장합니다. 네트워크 인증 서비스를 구성하려면 다음 단계를 완료하십시오.

1. iSeries Navigator에서 **iSeries-A —> 보안**을 확장하십시오.
2. **네트워크 인증 서비스**를 마우스 오른쪽 버튼으로 클릭하고 **구성**을 선택하여 구성 마법사를 시작하십시오.
   주: 네트워크 인증 서비스를 구성한 후에 이 옵션은 **재구성**됩니다.
3. **시작** 페이지에서 마법사가 작성한 오브젝트에 대한 정보를 검토하십시오. **다음**을 클릭하십시오.
4. **영역 정보 지정** 페이지의 **디폴트 영역** 필드에서 디폴트 영역명을 입력하십시오. **다음**을 클릭하십시오.
5. **KDC 정보 지정** 페이지의 **KDC** 필드에 이 영역의 키 분배 센터명을 입력하고 **포트** 필드에 88을 입력하십시오. **다음**을 클릭하십시오.
6. **암호 정보 지정** 페이지에서 암호 서버를 설정하기 위해 **예** 또는 **아니오**를 선택하십시오. 암호 서버를 사용하면 프린시펄이 KDC의 암호를 변경할 수 있습니다. **예**를 선택한 경우 **암호 서버** 필드에서 암호 서버명을 입력하십시오. 암호 서버의 디폴트 포트는 464입니다. **다음**을 클릭하십시오.
7. **키 표 항목 작성** 페이지에서 **iSeries Kerberos 인증**을 선택하십시오. 또한 이 서비스에서 Kerberos 인증을 사용하도록 할 경우 LDAP 서버와 iSeries NetServer에 대한 키 표 항목을 작성할 수 있습니다. **다음**을 클릭하십시오.
8. **iSeries 키 표 항목 작성** 페이지에서 암호를 입력하고 확인하십시오. **다음**을 클릭하십시오.
   주: 이 암호는 iSeries를 KDC에 정의할 때 사용할 암호와 같습니다.
9. **요약** 페이지에서 네트워크 인증 서비스 구성 세부사항을 검토하십시오. **완료**를 클릭하십시오.

이제 네트워크 인증 서비스가 구성되었습니다.

다음에 할 작업

iSeries를 키 분배 센터에 정의

iSeries를 키 분배 센터에 정의

iSeries에 네트워크 인증 서비스를 구성한 후에, iSeries를 KDC(key distribution center)에 정의해야 합니다. 네트워크 인증 서비스에서는 서버와 모든 고유한 iSeries 어플리케이션에 대하여 iSeries 프린시펄명 **krbsvr400**을 제공합니다.

예를 들어, 구성 시나리오에서는 iSeriesA.ordept.myco.com이라는 호스트명으로 iSeries를 조회합니다. 클라이언트가 이 iSeries에 제공할 서비스 티켓을 가져오려면 KDC를 사용하여 프린시펄 krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM을 정의해야 합니다.

z/OS

Kadmin 명령은 문서를 참조하십시오.

Windows(R) 2000 서버

1. Active Directory (R) Management 툴을 사용하여 iSeries에 대한 사용자 계정을 만드십시오. iSeries의 이름은 Active Directory 사용자로 지정하십시오. 예를 들어, 유효한 이름은 iSeriesA가 될 수 있습니다.
2. 1단계에서 작성한 Active Directory 사용자의 등록 정보에 액세스하십시오. **계정** 탭에서 **계정이 위임에 대하여 신뢰됨**을 선택하십시오. 이렇게 하면 iSeries 서비스 프린시펄이 서명한 사용자를 대신해서 다른 서비스에 액세스할 수 있습니다.
3. **ktpass** 명령을 사용하여 사용자 계정을 프린시펄에 맵핑하십시오. 예를 들어, 다음을 입력할 수 있습니다.

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

   여기에서 xxxxxx는 네트워크 인증 서비스를 구성하는 동안 지정한 암호입니다.

다음에 할 작업

홈 디렉토리 작성

«

홈 디렉토리 작성

»

iSeries를 키 분배 센터에 정의한 후에, iSeries 및 iSeries 어플리케이션을 연결할 각 사용자에 대한 /home 디렉토리를 작성해야 합니다. 이 디렉토리에는 사용자의 Kerberos 증명서 캐시명이 포함됩니다. 사용자의 홈 디렉토리를 작성하려면 다음을 완료하십시오.

iSeries 명령행에서 다음을 입력하십시오.

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

여기에서 username은 사용자의 iSeries 사용자명입니다.

다음에 할 작업:

TCP/IP 정의역 정보 확인

TCP/IP 정의역 정보 확인

홈 디렉토리를 작성한 후에, 서버에 대한 올바른 호스트 표 항목이 있는지 확인해야 합니다.

1. iSeries 명령행에서 다음을 입력하십시오.
   `CFGTCP`
2. 옵션 10을 선택하십시오(TCP/IP 호스트 표 항목에 대한 작업).
3. 호스트명 필드에, iSeries A에 대한 완전 규정된 호스트명이 소문자인지 확인하십시오. 또한 복수 호스트명 항목이 있으면 완전 규정된 호스트명이 먼저 나타나는지 확인하십시오. 예를 들면, iSeries A는 다음 호스트명 항목을 가져야 합니다.
   iseriesa.ordept.myco.com.
4. 호스트명 항목을 확인한 후, F3을 눌러 TCP 구성 기본 메뉴로 리턴하십시오.
5. 옵션 12를 선택하십시오(TCP/IP 정의역 정보 변경).
6. 호스트명 필드에 사용자의 시스템명이 나타나는지 확인하십시오. 또한 사용자 정의역명이 올바른지 확인하십시오. 예를 들면, 호스트명은 `iseriesa`이고 정의역명은 `ordept.myco.com`이 될 수 있습니다.

다음에 할 작업:

네트워크 인증 서비스 구성 테스트

네트워크 인증 서비스 구성 테스트

올바른 정의역 정보를 확인한 후에, 사용자 iSeries 프린시펄명에 대해 부여된 티켓을 요청하여 네트워크 인증 서비스 구성을 테스트해야 합니다.

1. 명령행에서 `QSH`를 입력하여 Qshell 인터프리터를 시작하십시오.
2. `keytab list`를 입력하여 키 표 파일에 등록된 프린시펄 리스트를 표시하십시오. 예를 들면, 올바른 프린시펄명은 krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM이 될 수 있습니다.

3. `kinit -k krbsvr400/system.domain@realm`을 입력하십시오. 예를 들면, krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM이 iSeries에 대한 유효한 프린시펄명이 됩니다. 입력이 완료되면 QSH 명령이 오류없이 표시됩니다.
4. `klist`를 입력하여 디폴트 프린시펄이 krbsvr400/system.domain@realm임을 확인하십시오.

다음에 할 작업

EIM(Enterprise Identity Mapping) 구성
사용자 자신의 어플리케이션과 함께 네트워크 인증 서비스를 사용할 경우 이 단계는 선택적입니다. 그러나 네트워크에서 여러 사용자 ID를 관리하기 위하여 고유 iSeries 어플리케이션과 함께 사용할 것을 권장합니다.

네트워크 인증 서비스 관리

네트워크 인증 서비스를 구성하고 난 후 티켓을 요구하고, 키 표 파일에 대한 작업을 하고, 영역 신뢰 관계를 관리할 수 있습니다. 또한 증명서 파일에 대한 작업을 할 수도 있고 구성 파일을 백업할 수도 있습니다. 다음 주제에서는 이 타스크들을 완료하는 방법을 설명합니다.

관리자 타스크

다음은 iSeries Navigator에서 관리자가 수행할 수 있는 간단한 타스크 리스트입니다. 자세한 타스크 기반 정보를 보려면 네트워크 인증 서비스에 대한 iSeriesNavigator 도움말을 참조하십시오. 이 타스크 외에 관리자는 kdestory 명령을 사용하여 사용자가 오래된 증명서를 삭제했는지 확인해야 합니다.

- 시스템 시간 동기화
  iSeries와 KDC 사이에서 티켓을 교환하려면 시스템 간 시간 차이는 5분 이내여야 합니다. 네트워크 인증 서비스 등록 정보에서 최대 시계 차이를 구성할 수 있습니다. 디폴트 최대 시계 차이는 5분 또는 300초입니다. 이 주제에서는 시스템 간에 시간을 동기화하는 방법을 설명합니다.
- 영역 추가
  이 주제에서는 네트워크 인증 서비스 구성에 새 영역을 추가하는 방법을 설명합니다.
- 영역 삭제
  이 주제에서는 네트워크 인증 서비스 구성에서 영역을 제거하는 방법을 설명합니다.
- 키 분배 센터를 영역에 추가
  이 주제에서는 네트워크 인증 서비스의 현재 구성에 키 분배 센터를 추가하는 방법을 설명합니다.
- 암호 서버 추가
  이 주제에서는 네트워크 인증 서비스 구성에 암호 서버를 추가하여 사용자가 자신의 Kerberos 암호를 변경하는 방법을 설명합니다.

- 영역 간에 신뢰 관계 작성
  이 항목에서는 영역 간에 신뢰 관계를 설정하는 방법을 설명합니다. 디폴트로 Kerberos 프로토콜은 영역 계층을 탐색하여 신뢰를 찾기 때문에 이 기능은 선택적입니다. 그러나 다른 정의역에 영역이 있고 프로세스를 더 빨리 처리하고 싶은 경우에는 이 기능이 유용합니다.
- 호스트 분석 변경
  이 주제에서는 영역명의 호스트 분석을 변경하는 방법을 설명합니다.
- 암호화 설정 추가
  이 주제에서는 TGT(Ticket Granting Ticket)와 TGS(Ticket Granting Service)에 대한 암호화 유형을 추가하는 방법을 설명합니다.

iSeries 사용자 타스크

iSeries는 또한 Kerberos 작동 가능한 네트워크에서 클라이언트 역할을 할 수도 있습니다. 사용자는 iSeries에 로그온하고 Qshell 인터프리터를 통하여 Kerberos 관련 타스크를 수행할 수 있습니다. 다음 타스크에서는 여러 Qshell 명령을 사용하여 iSeries 사용자에 대한 공통 타스크를 수행합니다.

- 홈 디렉토리 작성
  이 주제에서는 홈 디렉토리를 작성하는 방법을 설명합니다.
- 새로운 티켓 부여 티켓 가져오기
  이 주제에서는 **kinit** Qshell 명령을 사용하여 티켓 부여 티켓을 가져오거나 갱신하는 방법을 설명합니다.
- Kerberos 암호 변경
  이 주제에서는 **kpasswd** Qshell 명령을 사용하여 암호를 변경하는 방법을 설명합니다.
- 키 표 파일 관리
  이 주제에서는 **keytab** Qshell 명령을 사용하여 키 표 파일을 관리하는 방법을 설명합니다.
- 만기된 증명서 캐시 삭제
  이 주제에서는 **kdestroy** Qshell 명령을 사용하여 클라이언트에 저장된 만기 증명서 캐시를 삭제하는 방법을 설명합니다. 사용자는 주기적으로 자신의 증명서 캐시를 삭제해야 합니다.
- 증명서 캐시 또는 키 표 파일 표시
  이 주제에서는 **klist** Qshell 명령을 사용하여 사용자와 연관된 증명서와 키 표 파일을 나열하는 방법을 설명합니다.
- LDAP 디렉토리의 Kerberos 서비스 항목 관리
  이 주제에서는 **ksetup** QSHELL 명령을 사용하여 디렉토리 서비스(LDAP) 디렉토리의 Kerberos 서비스 항목을 관리하는 방법을 설명합니다.

시스템 시간 동기화

네트워크 인증 서비스에서는 시스템 시간 차이가 날 수 있는 최대 시간은 디폴트로 5분(300초)을 사용합니다. 네트워크 인증 서비스 등록 정보를 사용하여 시계 차이를 변경할 수 있습니다.

시스템 시간을 동기화하기 전에 QUTCOFFSET 시스템 값을 사용하여 사용자의 시간대에 맞게 시스템 시간을 설정하십시오. KDC 시간을 변경하여 이 시스템 시간을 동기화하거나 QTIME 시스템 값을 사용하여 iSeries 시스템 시간을 변경할 수 있습니다. 그러나 네트워크의 시스템 시간을 동기화하려면 SNTP(Simple Network Time Protocol)를 구성해야 합니다. SNTP를 사용하면 단일 시간 서버를 여러 시스템의 시간 기준으로 삼을 수 있습니다. SNTP를 구성하려면 다음 단계를 완료하십시오.

iSeries에서 SNTP를 구성하려면 명령행에 `CHGNTPA`를 입력하십시오.

Windows(R) 시스템에 SNTP를 구성하려면 **NET HELP TIME**을 사용하여 SNTP 서버에 대한 구성 정보를 표시하십시오.

영역 추가

네트워크 관리자로서 네트워크 인증 서비스 구성에 새 영역을 추가하고자 할 수 있습니다. iSeries 구성에 영역을 추가하려면, 먼저 새 영역에 대하여 KDC를 구성해야 합니다. iSeries 네트워크 인증 서비스 타스크에 영역을 추가하려면 영역명, KDC 이름 및 KDC에서 청취하는 포트가 필요합니다.

네트워크 인증 서비스에 영역을 추가하려면 다음 단계를 완료하십시오.

1. iSeries Navigator에서 **iSeries 서버** —> **보안** —> **네트워크 인증 서비스**를 선택하십시오.
2. **영역**을 마우스 오른쪽 버튼으로 클릭하고 **영역 추가**를 선택하십시오.
3. **추가할 영역** 필드에서 추가할 영역의 호스트명을 입력하십시오. 예를 들어, 유효한 영역명은 ORDEPT.MYCO.COM이 될 수 있습니다.
4. 추가할 영역의 KDC 이름을 입력하십시오. 예를 들어, 유효한 KDC 이름은 kdc1.ordept.myco.com이 될 수 있습니다.
5. 요구에 대하여 KDC에서 청취하는 포트 번호를 입력하십시오. 유효한 포트 번호는 1-65535입니다. KDC의 디폴트 포트는 88입니다.
6. **확인**을 클릭하십시오.

영역 삭제

네트워크 관리자로서 네트워크 인증 서비스 구성에서 영역을 삭제할 수 있습니다. 영역이 더 이상 필요없거나 네트워크에서 사용되지 않을 수 있습니다. 또한 일부 iSeries 고유 어플리케이션 문제점을 회복하기 위하여 디폴트 영역을 제거해야 할 수도 있습니다.

예를 들어, 네트워크에 KDC(Key Distribution Center)를 설정하지 않고 네트워크 인증 서비스를 구성한 경우, QFileSvr.400과 DDM(Distributed Data Management)에서는 사용자가 Kerberos 인증을 사용하는 것으로 가정합니다. 이 제품에 대한 인증을 설정하기 전에 네트워크 인증 서비스 구성 중에 지정한 디폴트 영역을 삭제해야 합니다.

네트워크 인증 서비스에 대한 영역을 삭제하려면 다음 단계를 완료하십시오.

1. iSeries Navigator에서 **iSeries 서버** —> **보안** —> **네트워크 인증 서비스** —> **영역**을 확장하십시오.
2. 삭제할 영역명을 마우스 오른쪽 버튼으로 클릭하고 **삭제**를 선택하십시오.
3. **확인**을 클릭하여 삭제를 확인하십시오.

키 분배 센터를 영역에 추가

네트워크 관리자로서 네트워크 인증 서비스를 사용하여 KDC(Key Distribution Center)를 영역에 추가할 수 있습니다. KDC를 영역에 추가하려면 먼저 KDC 이름과 KDC에서 청취하는 포트를 알아야 합니다.

키 분배 센터를 영역에 추가하려면 다음 단계를 완료하십시오.

1. iSeries Navigator에서 **iSeries 서버** —> **보안** —> **네트워크 인증 서비스** —> **영역**을 확장하십시오.
2. 오른쪽 분할 창에서 영역명을 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
3. **일반** 탭에서 이 영역에 추가할 KDC 이름을 입력하십시오. 모든 영역에 KDC가 필요합니다. 예를 들어, kdc2.ordept.myco.com은 유효한 항목이 될 수 있습니다.
4. 요구에 대하여 KDC에서 청취하는 포트 번호를 입력하십시오. 유효한 포트 번호는 1-65535입니다. KDC의 디폴트 포트는 88입니다.
5. **추가**를 클릭하십시오. **이 영역의 KDC(Key Distribution Center)** 리스트에 신규 KDC가 나타납니다.
6. **확인**을 클릭하십시오.

암호 서버 추가

암호 서버를 사용하면 Kerberos 프린시펄이 자신의 암호를 변경할 수 있습니다. 암호 서버를 영역에 추가하려면 다음 단계를 완료하십시오.

1. iSeries Navigator에서 **iSeries 서버** —> **보안** —> **네트워크 인증 서비스** —> **영역**을 확장하십시오.
2. 오른쪽 분할 창에서 영역명을 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
3. **암호 서버** 탭에서 암호 서버명을 입력하십시오. 예를 들어, 암호 서버의 유효한 이름은 psvr.ordept.myco.com 이 될 수 있습니다.
4. 암호 서버에 해당하는 포트 번호를 입력하십시오. 유효한 포트 번호는 1-65535입니다. 암호 서버의 디폴트 포트는 464입니다.
5. **추가**를 클릭하십시오. 새 암호 서버가 리스트에 추가됩니다.
6. **확인**을 클릭하십시오.

영역 간에 신뢰 관계 작성

영역 간에 신뢰 관계를 설정하면 인증에 대한 단축키가 작성됩니다. Kerberos 프로토콜은 디폴트로 영역 계층을 탐색하여 신뢰를 찾기 때문에 이 기능은 선택적입니다. 그러나 다른 정의역에 영역이 있고 이 프로세스를 더 빨리 처리하고 싶은 경우에는 이 기능이 유용합니다. 영역 신뢰를 설정하려면, 각 영역에 대한 KDC에서 키를 공유해야 합니다. 신뢰 관계를 작성하려면 먼저 KDC가 서로 신뢰하도록 설정해야 합니다. 영역 간에 신뢰 관계를 작성하려면 다음 단계를 완료하십시오.

1. iSeries Navigator에서 **iSeries 서버** —> **보안** —> **네트워크 인증 서비스** —> **영역**을 확장하십시오.
2. 오른쪽 분할 창에서 영역명을 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
3. **신뢰할 수 있는 영역** 탭에서 신뢰를 설정할 영역명을 입력하십시오. 예를 들어, 유효한 신뢰 관계의 이름은 NY.myco.com 및 LA.myco.com이 될 수 있습니다.
4. **추가**를 클릭하십시오. 신뢰 연관이 표에 추가됩니다.
5. **확인**을 클릭하십시오.

호스트 분석 변경

네트워크 인증 서비스를 사용하면 구성 파일에 추가된 디렉토리 서비스(LDAP) 서버, DNS(Domain Name System) 및 정적 맵핑을 지정하여 호스트명과 영역명을 분석할 수 있습니다. 세 가지 방법을 모두 선택하여 호스트명을 분석할 수도 있습니다. 세 가지 방법을 모두 선택하면 네트워크 인증 서비스에서는 디렉토리 서버를 먼저 검사하고 DNS 항목을 검사한 다음, 마지막으로 정적 맵핑을 확인하여 호스트명을 분석합니다.

호스트 분석을 변경하려면 다음 단계를 완료하십시오.

1. iSeries Navigator에서 **iSeries 서버** —> **보안**을 확장하십시오.
2. **네트워크 인증 서비스**를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
3. **호스트 분석** 페이지에서 **LDAP 찾아보기 사용**, **DNS 찾아보기 사용** 및/또는 **정적 맵핑 사용**을 선택하십시오.
4. **LDAP 찾아보기 사용**을 호스트 분석 유형으로 선택한 경우, 디렉토리 서버명과 해당 포트를 입력하십시오. 예를 들어, ldapsrv.ordept.myco.com은 유효한 디렉토리 서버명이 될 수 있습니다. 유효한 포트 번호는 1-65535입니다. 디렉토리 서버의 디폴트 포트는 389입니다.
5. **DNS 찾아보기 사용**을 호스트 분석 유형으로 선택한 경우, 영역명으로 맵핑하도록 DNS를 구성해야 합니다.
6. **정적 맵핑 사용**을 호스트 분석 유형으로 선택한 경우, 영역명과 해당 DNS 이름을 입력하십시오. 예를 들어, 호스트명이 mypc.mycompanylan.com이 되고, 영역명이 ORDEPT.MYCO.COM이 될 수 있습니다. 총칭 호스트명을 특정 영역에 맵핑할 수도 있습니다. 예를 들어, myco.lan.com으로 끝나는 모든 기계가 ORDEPT.MYCO.COM의 일부인 경우, DNS 이름으로 `myco.lan.com`을 입력하고 영역으로 ORDEPT.MYCO.COM을 입력할 수 있습니다. 그러면 구성 파일에서 영역명과 DNS 이름 사이에 연관이 작성됩니다. **추가**를 클릭하여 구성 파일의 DNS 이름과 영역명 사이에 정적 맵핑을 작성하십시오.
7. 선택한 호스트 분석 유형에 적절한 정보를 입력한 다음 **확인**을 클릭하십시오.

암호화 설정 추가

TGT(Ticket Granting Ticket)와 TGS(Ticket Granting Service)에 대한 암호화 유형을 선택할 수 있습니다. 암호화는 네트워크에 흐르는 자료를 식별할 수 없게 만들어 숨깁니다. 클라이언트에서 자료를 암호화하고, 서버에서 자료를 해독합니다. 암호화 작업이 올바르게 이루어지게 하려면 KDC나 다른 통신 어플리케이션에서 지정한 것과 같은 암호화 유형을 사용해야 합니다. 이 암호화 유형이 일치하지 않으면 암호화는 실패합니다. TGT와 TGS에 대한 암호화 값을 추가할 수 있습니다.

주: TGT와 TGS의 디폴트 암호화 값은 des-cbc-crc와 des-cbc-md5입니다. 구성하는 동안 디폴트 암호화 값이 설정됩니다. 다음 단계를 완료하여 티켓에 대한 다른 암호화 값을 구성에 추가할 수 있습니다.

1. iSeries Navigator에서 **iSeries 서버** —> **보안**을 확장하십시오.
2. **네트워크 인증 서비스**를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.

3. **티켓** 페이지의 사용 가능한 암호화 유형의 티켓 부여 티켓 또는 티켓 부여 서비스 리스트에서 암호화 값을 선택하십시오.
4. 선택한 암호화 유형 리스트에 암호화 유형을 추가하려면 **앞에 추가** 또는 **뒤에 추가**를 클릭하십시오. 선택한 암호화 유형은 모두 나열된 순서대로 시도됩니다. 암호화 유형이 하나 실패하면 리스트의 다음 암호화 유형이 시도됩니다.
5. **확인**을 클릭하십시오.

티켓 부여 티켓 가져오기 또는 갱신

kinit 명령은 Kerberos 티켓 부여 티켓을 가져오거나 갱신합니다. **kinit** 명령에서 티켓 옵션을 지정하지 않으면, Kerberos 구성 파일에 지정된 KDC(Key Distribution Center) 옵션을 사용합니다.

기존 티켓을 갱신하지 않는 경우, 증명서 캐시는 다시 초기화되고 KDC로부터 수신한 새로운 티켓 부여 티켓이 포함됩니다. 명령행에서 프린시펄명을 지정하지 않으면 프린시펄명은 증명서 캐시로부터 구합니다. `-c` 옵션으로 캐시명을 지정하지 않으면 새로운 증명서 캐시가 디폴트 증명서 캐시가 됩니다.

티켓 시간 값은 *nwndnhnmns*로 표시되는데, 여기에서 *n*은 숫자, *w*는 주, *d*는 일, *h*는 시간, *m*은 분, *s*는 초를 나타냅니다. 구성요소들은 반드시 이 순서로 지정되어야 하지만, 어떤 구성요소든 생략할 수 있습니다(예를 들어 *4h5m*은 4시간 5분을 나타내고, *1w2h*는 1주와 2시간을 나타냅니다). 숫자만 지정되면, 디폴트는 시간입니다.

프린시펄 jsmith에 대하여 수명이 5시간인 티켓 부여 티켓을 가져오려면

Qshell 명령행에서 다음을 입력하십시오.

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

또는

iSeries 명령행에서 다음을 입력하십시오.

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

이 Qshell 명령 사용법 및 제한사항에 대한 구체적 내용은 사용법 주의사항을 참조하십시오.

kinit

구문

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

디폴트 공용 권한: *USE

kinit Qshell 명령은 Kerberos 티켓 부여 티켓을 가져오거나 갱신합니다.

옵션

-r time
티켓 갱신시 시간 간격. 이 간격이 만기가 되면 티켓은 더 이상 갱신되지 않습니다. 갱신 시간은 종료 시간보다 커야 합니다. 이 옵션을 지정하지 않으면, 티켓은 갱신할 수 없습니다(갱신 가능한 티켓은 요구된 티켓 수명이 최대 티켓 수명보다 큰 경우 생성될 수 있습니다).

-R
기존 티켓이 갱신됩니다. 기존 티켓을 갱신하는 경우, 다른 티켓 옵션을 지정할 수 없습니다.

-p
티켓이 프록시가 될 수 있습니다. 이 옵션을 지정하지 않으면 티켓은 프록시가 될 수 없습니다.

-f
티켓을 이송할 수 없습니다. 이 옵션을 지정하지 않으면 티켓을 이송할 수 없습니다.

-A
티켓에 클라이언트 주소 리스트를 포함할 수 없습니다. 이 옵션을 지정하지 않으면 티켓에 로컬 호스트 주소 리스트를 포함할 수 없습니다. 초기 티켓에 주소 리스트가 포함되어 있는 경우, 이것은 주소 리스트의 주소들 중 하나로부터만 사용될 수 있습니다.

-l time
티켓 종료 시간 간격. 이 간격이 만기된 후 티켓을 다시 갱신하지 않으면 사용할 수 없습니다. 이 옵션을 지정하지 않으면 간격은 10시간으로 설정됩니다.

-c cache
kinit 명령이 사용할 증명서 캐시의 이름. 이 옵션을 지정하지 않으면 디폴트 증명서 캐시를 사용합니다.

-k
티켓 프린시펄의 키를 키 표로부터 구합니다. 이 옵션을 지정하지 않으면 티켓 프린시펄의 암호를 입력하도록 시스템에서 프롬프트됩니다.

-t keytab
키 표 이름. 이 옵션을 지정하지 않고 -k 옵션을 지정하는 경우, 시스템은 디폴트 키 표를 사용합니다. -t 옵션은 -k 옵션을 포함합니다.

프린시펄
티켓 종료 시간 간격. 명령행에서 프린시펄을 지정하지 않으면 시스템은 증명서 캐시로부터 프린시펄을 구합니다.

권한

참조되는 오브젝트	필요한 권한
-t 옵션이 지정된 경우 키 표 파일 앞에 나오는 경로명의 각 디렉토리	*X
-t가 지정된 경우 키 표 파일	*R
사용될 증명서 캐시 파일의 앞에 나오는 경로명의 각 디렉토리	*X
KRB5CCNAME 환경 변수로 지정하고 파일을 작성 중인 경우, 사용할 캐시 파일의 상위 디렉토리	*WX
증명서 캐시 파일	*RW
구성 파일에 대한 경로의 각 디렉토리	*X
구성 파일	*R

실행 중인 프로세스로부터 보증서 캐시 파일을 찾기 위해 Kerberos 런타임을 작동하면, 캐시 파일의 이름은 **krb5ccname**라는 파일의 홈 디렉토리에 저장됩니다. 캐시 파일명의 저장 위치는 **_EUV_SEC_KRB5CCNAME_FILE** 환경 변수를 설정하여 대체할 수 있습니다. 이 파일에 액세스하려면 경로의 각 디렉토리에 대한 ***X** 권한과 캐시 파일명이 저장되어 있는 파일에 대한 ***R** 권한이 사용자 프로파일에 있어야 합니다. 증명서 캐시를 처음 작성할 때 사용자 프로파일에 상위 디렉토리에 대한 ***WX** 권한이 있어야 합니다.

메세지

- option_name 옵션에 값을 입력하십시오.
- command_option 옵션은 유효한 명령 옵션이 아닙니다.
- 티켓을 갱신하거나 검증할 때는 어떤 옵션도 허용되지 않습니다.
- 디폴트 증명서 캐시의 이름을 구할 수 없습니다.

- file_name 증명서 캐시를 해제할 수 없습니다.
- 초기 티켓을 사용할 수 없습니다.
- 프린시펄명을 지정해야 합니다.
- file_name 증명서 캐시로부터 티켓을 검색할 수 없습니다.
- 초기 티켓을 갱신할 수 없습니다.
- option_value 옵션이 request_name 요구에 유효하지 않습니다.
- 초기 증명서를 구할 수 없습니다.
- 프린시펄명을 분석할 수 없습니다.
- file_name 키 표를 분석할 수 없습니다.
- principal_name의 암호가 올바르지 않습니다.
- 암호를 읽을 수 없습니다.
- file_name 증명서 캐시에 초기 증명서를 저장할 수 없습니다.
- 시간 델타 값이 유효하지 않습니다.

이 명령 사용 방법에 대한 예는 티켓 부여 티켓 가져오기 또는 갱신을 참조하십시오.

증명서 캐시나 키 표 파일 표시

klist 명령은 Kerberos 증명서 캐시나 키 표의 내용을 표시합니다.

디폴트 증명서 캐시의 항목을 모두 나열하고 티켓 플래그를 표시하려면

Qshell 명령행에서 다음을 입력하십시오.

```
klist -f -a
```

또는

iSeries 명령행에서 다음을 입력하십시오.

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

이 Qshell 명령 사용법 및 제한사항에 대한 구체적 내용은 사용법 주의사항을 참조하십시오.

klist

구문

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

디폴트 공용 권한: *USE

klist Qshell 명령은 Kerberos 증명서 캐시나 키 표의 내용을 표시합니다.

옵션

-a

만기된 티켓을 포함한 증명서 캐시의 모든 티켓을 보여줍니다. 이 옵션을 지정하지 않으면 만기된 티켓은 나열되지 않습니다. 이 옵션은 증명서 캐시를 나열한 경우에만 유효합니다.

-e

세션 키와 티켓에 대한 암호화 키를 표시합니다. 이 옵션은 증명서 캐시를 나열한 경우에만 유효합니다.

-c

증명서 캐시의 티켓을 나열합니다. -c나 -k 중 어떤 것도 지정하지 않은 경우, 이것이 디폴트입니다. 이 옵션은 -k 옵션과 상호 배타적입니다.

-f

다음과 같은 약어를 사용하여 티켓 플래그를 보여줍니다.

약어	의미
F	티켓이 이송될 수 있음
f	이송된 티켓
P	티켓이 프록시일 수 있음
p	프록시 티켓
D	티켓이 지연될 수 있음
d	지연된 티켓
R	갱신 가능한 티켓
I	초기 티켓
i	티켓이 유효하지 않음
A	사전 인증이 사용되었음
O	서버가 위임될 수 있음
C	통과 리스트가 KDC에 의해 검사되었음

이 옵션은 증명서 캐시를 나열한 경우에만 유효합니다.

-s
명령 출력을 억제하지만 유효한 티켓 부여 티켓을 증명서 캐시에 있는 경우, 나감 상태를 0으로 설정합니다. 이 옵션은 증명서 캐시를 나열한 경우에만 유효합니다.

-k
키 표의 항목을 나열합니다. 이 옵션은 **-c** 옵션과 상호 배타적입니다.

-t
키 표 항목의 시간 소인을 보여줍니다. 이 옵션은 키 표를 나열한 경우에만 유효합니다.

-K
각 키 표 항목에 대한 암호화 키 값을 표시합니다. 이 옵션은 키 표를 나열한 경우에만 유효합니다.

filename
증명서 캐시나 키 표의 이름을 지정합니다. 아무런 파일명도 지정하지 않으면, 디폴트 증명서 캐시나 키 표가 사용됩니다.

권한

참조되는 오브젝트	필요한 권한
키 표로 -k 옵션을 지정한 경우 파일 앞에 나오는 경로명의 각 디렉토리	*X
-k를 지정한 경우 키 표 파일	*R
-k 옵션을 지정하지 않은 경우 증명서 캐시 파일의 앞에 나오는 경로명의 각 디렉토리	*X
-k 옵션을 지정하지 않은 경우 증명서 캐시 파일	*R

실행 중인 프로세스로부터 보증서 캐시 파일을 찾기 위해 Kerberos 런타임을 작동하면 캐시 파일의 이름은 **krb5ccname**라는 파일의 홈 디렉토리에 저장됩니다. 캐시 파일명의 저장 위치는 **_EUV_SEC_KRB5CCNAME_FILE** 환경 변수를 설정하여 대체할 수 있습니다. 이 파일에 액세스하려면 경로의 각 디렉토리에 대한 ***X** 권한과 캐시 파일명이 저장되어 있는 파일에 대한 ***R** 권한이 사용자 프로파일에 있어야 합니다. 증명서 캐시를 처음 작성할 때 사용자 프로파일에 상위 디렉토리에 대한 ***WX** 권한이 있어야 합니다.

메세지

- option_name 옵션에 값을 입력하십시오.
- command_option 옵션은 유효한 명령 옵션이 아닙니다
- command_option_one 및 command_option_two 은(는) 함께 지정될 수 없습니다.

- 디폴트 증명서 캐시를 찾을 수 없습니다.
- file_name 증명서 캐시를 해제할 수 없습니다.
- file_name 증명서 캐시로부터 프린시펄명을 검색할 수 없습니다.
- file_name 증명서 캐시로부터 티켓을 검색할 수 없습니다.
- 티켓을 해독할 수 없습니다.
- 디폴트 키 표를 찾을 수 없습니다.
- file_name 키 표를 분석할 수 없습니다.

이 명령 사용법에 대한 예는 증명서 캐시나 키표 파일 표시를 참조하십시오.

키 표 파일 관리

keytab 명령은 키 표에 키를 추가 또는 삭제하거나 키 표에 항목을 표시할 때 사용합니다.

예를 들어, ORDEPT.MYCO.COM 영역의 kdc1.ordept.myco.com 호스트에 있는 krbsvr400 서비스 프린시펄에 대한 키를 추가하려면

Qshell 명령행에서 다음을 입력하십시오.

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

또는

iSeries 명령행에서 다음을 입력하십시오.

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

서비스를 KDC에 정의할 때 사용했던 암호를 입력하도록 프롬트됩니다.

이 Qshell 명령 사용법 및 제한사항에 대한 구체적 내용은 사용법 주의사항을 참조하십시오.

keytab

»

구문

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

디폴트 공용 권한: *USE

keytab Qshell 명령은 키 표를 관리합니다.

옵션

-k
키 표 이름. 이 옵션을 지정하지 않으면 디폴트 키 표가 사용됩니다.

-p
암호를 지정하십시오. 이 옵션을 지정하지 않으면 키 표에 항목을 추가할 때 암호를 입력하도록 프롬트됩니다.

-v
키 버전 번호. 이 옵션을 지정하지 않으면, 키를 추가할 때 다음 버전 번호가 지정됩니다. 이 옵션을 지정하지 않으면, 키를 삭제할 때 프린시펄의 모든 키가 삭제됩니다.

프린시펄
프린시펄명. 이 옵션을 지정하지 않으면, 키 표를 나열할 때 프린시펄이 모두 표시됩니다.

권한

참조되는 오브젝트	필요한 권한
열려는 목표 키 표 파일 앞에 나오는 경로명의 각 디렉토리	*X
키 표 파일이 존재하지 않는 경우, add가 지정될 때 목표 키 표 파일의 상위 디렉토리	*WX
list가 지정될 때 키 표 파일	*R
add나 delete가 지정될 때 목표 키 표 파일	*RW
구성 파일에 대한 경로의 각 디렉토리	*X
구성 파일	*R

메세지

- *add*, *delete*, *list* 또는 *merge*를 지정해야 합니다.

- *command_option* 옵션은 유효한 명령 옵션이 아닙니다.
- *command_option_one* 및 *command_option_two*은(는) 함께 지정될 수 없습니다.
- *option_value* 옵션이 *request_name* 요구에 유효하지 않습니다.
- *option_name* 옵션에 값이 필요합니다.
- 프린시펄명을 분석할 수 없습니다.
- 프린시펄명을 지정해야 합니다.
- 암호를 읽을 수 없습니다.
- 디폴트 키 표를 찾을 수 없습니다.
- *key_table* 키 표를 분석할 수 없습니다.
- *key_table* 키 표에서 항목을 읽을 수 없습니다.
- *key_table* 키 표에서 항목을 제거할 수 없습니다.
- *key_table* 키 표에 항목을 추가할 수 없습니다.
- *principal_name* 프린시펄의 항목을 찾을 수 없습니다.
- 값이 유효한 숫자가 아닙니다.
- 키 버전은 1에서 255 사이의 값이어야 합니다.
- *principal_name* 프린시펄의 *key_version* 키 버전을 찾을 수 없습니다.

이 명령 사용 방법에 대한 예는 키표 파일 관리를 참조하십시오.

Kerberos 암호 변경

kpasswd 명령은 암호 변경 서비스를 사용하여 지정한 Kerberos 프린시펄에 대한 암호를 변경합니다. 새 암호 뿐만 아니라 프린시펄에 대한 현재 암호도 제공해야 합니다. 암호 서버는 암호를 변경하기 전에 적용 가능한 모든 암호 정책 규칙을 새 암호에 적용합니다. KDC를 설치하고 구성하는 동안 암호 서버가 구성됩니다. 시스템에 해당하는 문서를 참조하십시오. 네트워크 인증 서비스를 구성하는 동안 암호 서버의 이름을 지정할 수 있습니다. 구성하는 동안 암호 서버를 지정하지 않은 경우, 암호 서버를 추가할 수 있습니다.

kpasswd 명령을 사용하여 티켓 부여 서비스 프린시펄(krbtgt/realm)에 대한 암호를 변경할 수 없습니다.

디폴트 프린시펄에 대한 암호를 변경하려면

Qshell 명령행에서 다음을 입력하십시오.

```
kpasswd
```

또는

명령행에서 다음을 입력하십시오.

```
call qsys/qkrbkpsswd
```

다른 프린시펄의 암호를 변경하려면

Qshell 명령행에서 다음을 입력하십시오.

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

또는

명령행에서 다음을 입력하십시오.

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

이 명령 사용에 대한 자세한 내용은 kpasswd 사용법 주의사항을 참조하십시오.

«

kpasswd

»

구문

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

디폴트 공용 권한: *USE

kpasswd Qshell 명령은 Kerberos 프린시펄의 암호를 변경합니다.

옵션

-A kpasswd 명령에서 사용한 초기 티켓에는 클라이언트 주소 리스트가 포함되지 않습니다. 이 옵션을 지정하지 않으면 티켓에 로컬 호스트 주소 리스트가 포함됩니다. 초기 티켓에 주소 리스트가 있는 경우, 주소 리스트에 포함된 주소들 중 하나만 사용될 수 있습니다.

principal

암호를 변경할 프린시펄입니다. 명령행에서 프린시펄을 지정하지 않은 경우, 디폴트 증명서 캐시에서 프린시펄을 가져옵니다.

메세지

- %3$s 프린시펄은 유효하지 않습니다.
- file_name 디폴트 증명서 캐시를 읽을 수 없습니다.
- 디폴트 증명서 캐시가 없습니다.
- file_name 증명서 캐시로부터 티켓을 검색할 수 없습니다.
- 암호를 읽을 수 없습니다.
- 암호 변경이 취소되었습니다.
- principal_name의 암호가 올바르지 않습니다.
- 초기 티켓을 가져올 수 없습니다.
- 암호 변경 요구가 실패했습니다.

이 명령 사용법에 대한 예는 Kerberos 암호 변경을 참조하십시오.

만기된 증명서 캐시 파일 삭제

kdestroy 명령은 Kerberos 증명서 캐시 파일을 삭제합니다. 사용자는 kdestroy 명령을 사용하여 오래된 증명서를 주기적으로 삭제해야 합니다.

-e 옵션을 사용하면 **kdestroy** 명령은 디폴트 캐시 디렉토리(**/QIBM/UserData/OS400/NetworkAuthentication/creds**)에 있는 증명서 캐시 파일을 모두 검사합니다. *time_delta* 기간이 지나 만기된 티켓만 있는 파일은 모두 삭제됩니다. *time_delta*는 *nwndnhnmns*으로 표시되는데, 여기에서 *n*은 숫자, *w*는 주, *d*는 날, *h*는 시간, *m*은 분, *s*는 초를 나타냅니다. 구성요소들은 반드시 이 순서로 지정되어야 하지만, 어떤 구성요소든 생략할 수 있습니다(예를 들어 *4h5m*은 4시간 5분을 나타내고, *1w2h*는 1주와 2시간을 나타냅니다). 숫자만 지정되면, 디폴트는 시간입니다.

디폴트 증명서 캐시를 삭제하려면 다음을 수행하십시오.

Qshell 명령행에서 다음을 입력하십시오.

```
kdestroy
```

또는

iSeries 명령행에서 다음을 입력하십시오.

```
call qsys/qkrbkdstry
```

하루가 경과된 만기된 티켓이 있는 모든 증명서 캐시 파일을 삭제하려면 다음을 수행하십시오.

Qshell 명령행에서 다음을 입력하십시오.

```
kdestroy -e 1d
```

또는

iSeries 명령행에서 다음을 입력하십시오.

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

이 Qshell 명령 사용법 및 제한사항에 대한 구체적 내용은 사용법 주의사항을 참조하십시오.

kdestroy

구문

```
kdestroy [-c cache_name] [-e time_delta]
```

디폴트 공용 권한: *USE

Qshell 명령인 **kdestroy**는 Kerberos 증명서 캐시를 제거합니다.

옵션

-c cache_name
제거할 증명서 캐시의 이름입니다. 명령 옵션을 지정하지 않으면 디폴트 증명서 캐시가 제거됩니다. 이 옵션은 -e 옵션과 상호 배타적입니다.

-e time_delta

`time_delta` 값을 지난 티켓이 만기되면 만기된 티켓이 포함된 모든 증명서 캐시 파일이 삭제됩니다.

권한

증명서 캐시가 **FILE** 유형인 경우(캐시 유형에 대한 더 자세한 정보는 **krb5_cc_resolve()**를 참조하십시오), 디폴트로 증명서 캐시 파일이 /QIBM/UserData/OS400/NetworkAuthentication/creds 디렉토리에 작성됩니다. 증명서 캐시 파일이 놓일 위치는 KRB5CCNAME 환경 변수 설정에 따라 변경될 수 있습니다.

증명서 캐시 파일이 디폴트 디렉토리에 없는 경우, 다음과 같은 권한이 필요합니다.

참조되는 오브젝트	요구되는 자료 권한	요구되는 오브젝트 권한
증명서 캐시 파일 앞에 나오는 경로명의 각 디렉토리	*X	없음
증명서 캐시 파일의 상위 디렉토리	*WX	없음
증명서 캐시 파일	*RW	*OBJEXIST
구성 파일에 대한 경로의 각 디렉토리	*X	없음
구성 파일	*R	없음

증명서 캐시 파일이 디폴트 디렉토리에 있는 경우, 다음과 같은 권한이 필요합니다.

참조되는 오브젝트	요구되는 자료 권한	요구되는 오브젝트 권한
경로명의 모든 디렉토리	*X	없음
증명서 캐시 파일	*RW	없음
구성 파일에 대한 경로의 각 디렉토리	*X	없음
구성 파일	*R	없음

Kerberos 프로토콜이 실행 중인 프로세스에서 증명서 캐시 파일을 찾아내도록 하기 위해서는, 캐시 파일의 이름이 보통 krb5ccname이라는 홈 디렉토리에 저장됩니다. iSeries에서 Kerberos 인증을 사용하려는 사용자는 홈 디렉토리를 정의해야 합니다. 디폴트로 홈 디렉토리는 /home/입니다. 아무런 명령 옵션도 지정되지 않으면 이 파일이 디폴트 증명서 캐시를 찾는 데 사용됩니다. 캐시 파일 이름 저장 위치는 환경 변수 _EUV_SEC_KRB5CCNAME_FILE을 설정하여 대체할 수 있습니다. 이 파일에 액세스하려면 경로의 각 디렉토리에 대한 ***X** 권한과 캐시 파일명이 저장되어 있는 파일에 대한 ***R** 권한이 사용자 프로파일에 있어야 합니다.

메세지

- *cache_file_name* 증명서 캐시를 분석할 수 없습니다.
- *cache_file_name* 증명서 캐시를 제거할 수 없습니다.
- *function_name* 함수가 오류를 감지했습니다.

- *file_name* 증명서 캐시로부터 티켓을 검색할 수 없습니다.
- *option_name* 옵션에 값이 필요합니다.
- *command_option* 옵션은 유효한 명령 옵션이 아닙니다.
- *command_option_one* 및 *command_option_two*은(는) 함께 지정될 수 없습니다.
- 디폴트 증명서 캐시를 찾을 수 없습니다.
- *value* 시간 델타 값이 유효하지 않습니다.

이 명령 사용 방법에 대한 예는 만기된 증명서 캐시 파일 삭제를 참조하십시오.

LDAP 디렉토리의 Kerberos 서비스 항목 관리

ksetup 명령은 디렉토리 서비스(LDAP) 디렉토리에 있는 Kerberos 서비스 항목을 관리합니다. 다음과 같은 부속 명령이 지원됩니다.

addhost host-name realm-name
이 부속 명령은 지정된 영역의 호스트 항목을 추가합니다. 디폴트 DNS 정의역이 Kerberos 클라이언트에 어떤 영향을 미치건 상관없이 올바르게 해제하도록 완전 규정된 호스트명을 사용해야 합니다. 영역명을 지정하지 않으면 디폴트 영역명이 사용됩니다.

addkdc host-name:port-number realm-name
이 부속 명령은 지정된 영역의 KDC 항목을 추가합니다. 호스트 항목이 이미 존재하는 경우 새로 작성됩니다. 포트 번호를 지정하지 않으면 88로 설정됩니다. 디폴트 DNS 정의역이 Kerberos 클라이언트에 어떤 영향을 미치건 상관없이 올바르게 해제하도록 완전 규정된 호스트명을 사용해야 합니다. 영역명을 지정하지 않으면 디폴트 영역명이 사용됩니다.

delhost host-name realm-name
이 부속 명령은 지정된 영역에서 호스트 항목 및 모든 연관된 KDC 스펙을 삭제합니다. 영역명을 지정하지 않으면 디폴트 영역명이 사용됩니다.

delkdc host-name realm-name
이 부속 명령은 지정된 호스트의 KDC 항목을 삭제합니다. 호스트 항목 자체는 삭제되지 않습니다. 영역명을 지정하지 않으면 디폴트 영역명이 사용됩니다.

listhost realm-name
이 부속 명령은 영역의 호스트 항목을 나열합니다. 영역명을 지정하지 않으면 디폴트 영역명이 사용됩니다.

listkdc realm-name
이 부속 명령은 영역의 KDC 항목을 나열합니다. 영역명을 지정하지 않으면 디폴트 영역명이 사용됩니다.

exit
이 부속 명령은 ksetup 명령을 종료합니다.

예

관리자의 디렉토리 서비스(LDAP) 관리자 ID와 verysecret 암호를 사용하여 ORDEPT.MYCO.COM 영역의 KDC로 kdc1.ordept.myco.com 호스트를 ldapserv.ordept.myco.com 서버에 추가하려면 다음 단계를 완료하십시오.

Qshell 명령행에서 다음을 입력하십시오.

```
ksetup -h ldapserv.ordept.myco.com -n CN=Administrator -p verysecret
```

또는

1. iSeries 명령행에서 다음을 입력하십시오.

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

2. 디렉토리 서비스(LDAP) 서버에 올바르게 연결되면 부속 명령 프롬트가 표시됩니다. 그러면 다음을 입력하십시오.

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

이 Qshell 명령 사용법 및 제한사항에 대한 구체적 내용은 사용법 주의사항을 참조하십시오.

ksetup

구문

```
ksetup -h host-name -n bind-name -p bind-password -e
```
디폴트 공용 권한: *USE

ksetup Qshell 명령은 Kerberos 영역의 디렉토리 서비스(LDAP)에 있는 Kerberos 서비스 항목을 관리합니다.

옵션

-h
디렉토리 서비스(LDAP) 서버의 호스트명. 이 옵션을 지정하지 않으면 Kerberos 구성 파일에 지정된 디렉토리 서비스(LDAP) 서버가 사용됩니다.

-n
디렉토리 서비스(LDAP) 서버에 바인드할 때 사용할 식별명. 이 옵션을 지정하지 않으면 디렉토리 서비스(LDAP)_BINDDN 환경 변수를 사용하여 이름을 가져옵니다.

-p
디렉토리 서비스(LDAP) 서버에 바인드할 때 사용할 암호. 이 옵션을 지정하지 않으면, 디렉토리 서비스(LDAP)_BINDPW 환경 변수를 사용하여 암호를 가져옵니다.

-e
표준 출력을 각 명령행을 에코합니다. 이것은 stdin이 파일로 지정되어 있을 때 유용합니다.

권한

참조되는 오브젝트	필요한 권한
구성 파일에 대한 경로의 각 디렉토리	*X
구성 파일	*R

메세지

- subcommand는 유효한 부속 명령이 아닙니다.
- 유효한 부속 명령은 addhost, addkdc, delhost, delkdc, listhost, listkdc, exit입니다.
- command_option_one 및 command_option_two은(는) 함께 지정될 수 없습니다.
- LDAPclient를 초기화할 수 없습니다.
- 디렉토리 서비스(LDAP) 서버에 바인드할 수 없습니다.
- 영역명을 지정해야 합니다.

- 호스트명을 지정해야 합니다.
- 위치 매개변수가 너무 많습니다.
- host 호스트가 이미 존재합니다.
- domain 루트 정의역이 정의되지 않았습니다.
- realm 영역명은 유효하지 않습니다.
- LDAP function name 함수에서 오류를 감지하였습니다.
- 사용할 수 있는 기억장치가 부족합니다.
- host 호스트명이 유효하지 않습니다.
- port 포트 번호가 유효하지 않습니다.
- host 호스트가 정의되지 않았습니다.
- host 호스트에 대하여 정의된 KDC가 없습니다.
- 디폴트 영역명을 구할 수 없습니다.

이 명령 사용법에 대한 예는 LDAP 디렉토리의 Kerberos 서비스 항목 관리를 참조하십시오.

네트워크 인증 서비스 문제 해결

이 섹션에서는 네트워크 인증 서비스, EIM(Enterprise Identity Mapping), Kerberos 인증을 지원하는 iSeries 고유 어플리케이션의 일반적인 오류에 대한 문제 해결 정보와 연결되는 링크를 제공합니다.

1. 모든 전제조건을 완료해야 합니다.
2. iSeries에 사용자 프로파일이 있고, KDC에 사용자의 프린시펄명이 있는지 확인하십시오. iSeries에서 iSeries Navigator의 사용자 및 그룹을 열거나 명령행에 WRKUSRPRF를 사용하여 사용자가 있는지 확인하십시오. Windows(R) 시스템에서 Active Directory (R) 사용자 및 컴퓨터 폴더에 액세스하여 사용자가 있는지 확인하십시오.
3. Qshell 인터프리터에서 kinit 명령을 사용하여 iSeries가 KDC에 연결되어 있는지 검사하십시오. kinit가 실패하면 iSeries 서비스 프린시펄이 KDC에 등록되었는지 검사하십시오. 등록되어 있지 않으면 KDC에 iSeries 프린시펄명을 추가할 수 있습니다.

특정 메세지에 대한 자세한 정보는 다음 주제를 참조하십시오.

- 네트워크 인증 서비스 오류 및 회복
  네트워크 인증 서비스 마법사가 실행하는 동안이나 iSeries Navigator에서 네트워크 인증 서비스 등록 정보를 관리할 때 이런 메세지가 나타날 수 있습니다.

- 어플리케이션 연결 오류 및 회복
  이 주제에서는 어플리케이션에서 iSeries, 서비스 또는 사용자가 KDC에 연결할 때 발생할 수 있는 네트워크 인증 서비스, EIM 및 일부 iSeries 고유 어플리케이션을 사용할 경우에 나타나는 일반적인 오류 메세지에 대하여 설명합니다.

네트워크 인증 서비스 오류 및 회복

네트워크 인증 서비스 마법사를 실행하는 동안이거나 iSeries Navigator에서 네트워크 인증 서비스 등록 정보를 관리할 때 이런 메세지가 발생할 수 있습니다.

메세지	회복
KRBWIZ_CONFIG_FILE_FORMAT_ERROR 네트워크 인증 서비스 구성 파일의 형식 오류입니다.	네트워크 인증 서비스를 재구성하십시오. 세부사항은 네트워크 인증 서비스 구성을 참조하십시오.
KRBWIZ_CRYPTO_NOT_INSTALLED 필수 암호 제품이 시스템에 설치되어 있지 않습니다.	시스템에 Cryptographic Access Provider(572-AC3)를 설치하십시오.
KRBWIZ_ERROR_READ_CONFIG_FILE 네트워크 인증 서비스 구성 파일 읽는 중 오류가 발생했습니다.	네트워크 인증 서비스를 재구성하십시오. 세부사항은 네트워크 인증 서비스 구성을 참조하십시오.
KRBWIZ_ERROR_WRITE_CONFIG_FILE 네트워크 인증 서비스 구성 파일 쓰기 오류가 발생했습니다.	구성 파일을 쓰기 위해 사용한 서비스를 사용할 수 없습니다. 나중에 다시 시도하십시오.
KRBWIZ_PASSWORD_MISMATCH 새 암호와 새 암호 확인이 같지 않습니다.	새 암호를 다시 입력하고 새 암호를 확인하십시오.
KRBWIZ_PORT_ERROR 포트 번호는 1과 65535 사이여야 합니다.	1과 65535 사이의 포트 번호를 다시 입력하십시오.
KRBWIZ_ERROR_WRITE_KEYTAB 키 표 파일 쓰기 오류	키 표를 쓰기 위해 사용한 서비스를 임시로 사용할 수 없습니다. 나중에 다시 시도하십시오.
KRBWIZ_NOT_AUTHORIZED_CONFIGURE 네트워크 인증 서비스를 구성할 수 있는 권한이 없습니다.	*ALLOBJ 및 *SECADM 권한이 있는지 확인하십시오.
KrbPropItemExists 항목이 이미 존재합니다.	새 항목을 입력하십시오.
KrbPropKDCInListRequired 리스트에 KDC가 있어야 합니다.	지정한 KDC가 리스트에 없습니다. 리스트에서 KDC를 선택하십시오.

KrbPropKDCValueRequired
KDC 이름을 입력해야 합니다.

KDC에 대한 유효한 이름을 입력하십시오. 네트워크의 보안 시스템에 KDC를 구성해야 합니다.

KrbPropPwdServerRequired
암호 서버명을 입력해야 합니다.

암호 서버에 대한 유효한 이름을 입력하십시오.

KrbPropRealmRequired
영역명을 입력해야 합니다.

이 시스템이 속하는 영역명을 입력하십시오.

KrbPropRealmToTrustRequired
신뢰할 영역에 대한 이름을 입력해야 합니다.

신뢰 관계가 설정되는 영역명을 입력하십시오.

KrbPropRealmValueRequired
영역명을 입력해야 합니다.

영역에 대한 유효한 이름을 입력하십시오.

CPD3E3F
네트워크 인증 서비스 오류 &2이(가) 발생했습니다.

이 메세지에 해당하는 특정 회복 정보를 참조하십시오.

어플리케이션 연결 문제점 및 회복

어플리케이션에서 네트워크 인증 서비스를 사용할 경우, 다음 메세지가 표시될 수 있습니다.

문제점
다음 오류를 수신합니다.
디폴트 증명서 캐시의 이름을 구할 수 없습니다.

회복
/home 디렉토리에 iSeries에 사인 온 한 사용자의 디렉토리가 있는지 판별합니다. 디렉토리가 없으면 증명서 캐시의 홈 디렉토리를 작성합니다.

CPD3E3F
네트워크 인증 서비스 오류 &2이(가) 발생했습니다.

이 메세지에 해당하는 특정 회복 정보를 참조하십시오.

이전에 연결한 iSeries 시스템에서 DRDA/DDM 연결이 실패했습니다.

네트워크 인증 서비스 구성이 존재하는 동안 디폴트 영역을 지정했는지 검사하십시오. 디폴트 영역 및 KDC(Key Distribution Center)를 구성하지 않은 경우, 네트워크 인증 서비스 구성이 잘못되고 DRDA/DDM 연결이 실패합니다. 이 오류를 회복하기 위해 다음 타스크 중 하나를 수행할 수 있습니다.

1. Kerberos 인증을 사용하지 않을 경우, 다음을 완료하십시오.
   a. 네트워크 인증 서비스 구성에서 지정한 디폴트 영역을 삭제하십시오.
2. Kerberos 인증을 사용하는 경우, 다음 단계를 완료하십시오.
   a. 네트워크의 보안 시스템에 디폴트 영역과 KDC를 구성하십시오. 시스템에 해당하는 문서를 참조하십시오.
      주: 현재 iSeries에서는 KDC를 지원하지 않습니다.
   b. 1단계에서 작성한 디폴트 영역과 KDC를 지정하여 네트워크 인증 서비스를 재구성하십시오.
   c. Kerberos 인증을 사용하도록 Windows용 iSeries Access 어플리케이션을 구성(29 페이지 참조)하십시오. 그러면 DRDA/DDM을 포함하여 모든 Windows용 iSeries Access 어플리케이션에 Kerberos 인증이 설정됩니다.

이전에 연결한 iSeries 시스템에서 QFileSvr.400 연결이 실패합니다.

네트워크 인증 서비스 구성이 존재하는 동안 디폴트 영역을 지정했는지 검사하십시오. 디폴트 영역 및 KDC(Key Distribution Center)를 구성하지 않은 경우, 네트워크 인증 서비스 구성이 잘못되고 QFileSvr.400 연결이 실패합니다. 이 오류를 회복하기 위해 다음 타스크 중 하나를 수행할 수 있습니다.

1. Kerberos 인증을 사용하지 않을 경우, 다음을 완료하십시오.
   a. 네트워크 인증 서비스 구성에서 지정한 디폴트 영역을 삭제하십시오.
2. Kerberos 인증을 사용하는 경우, 다음 단계를 완료하십시오.
   a. 네트워크의 보안 시스템에 디폴트 영역과 KDC를 구성하십시오. 시스템에 해당하는 문서를 참조하십시오.
      주: 현재 iSeries에서는 KDC를 지원하지 않습니다.
   b. 1단계에서 작성한 디폴트 영역과 KDC를 지정하여 네트워크 인증 서비스를 재구성하십시오.
   c. Kerberos 인증을 사용하도록 Windows용 iSeries Access 어플리케이션을 구성(29 페이지 참조)하십시오. 그러면 DRDA/DDM을 포함하여 모든 Windows용 iSeries Access 어플리케이션에 Kerberos 인증이 설정됩니다.

CWBSY1011
Kerberos 클라이언트 증명서를 찾을 수 없습니다.

사용자에게 TGT(Ticket Granting Ticket)가 없습니다. Windows(R) 2000 정의역에 로그인하지 않은 경우, 클라이언트 PC에 이 연결 오류가 발생합니다. 이 오류를 회복하려면 Windows(R) 2000 정의역에 로그인하십시오.

연결 설정을 확인하는 중에 오류가 발생했습니다. URL에 호스트가 없습니다. **주:** EIM(Enterprise Identity Mapping)을 사용하는 경우, 이 오류가 발생합니다.	이 오류를 회복하려면 다음을 완료하십시오. 1. iSeries Navigator에서 **iSeries** —> **네트워크** —> **서버** —> **TCP/IP**를 확장하십시오. 2. **디렉토리**를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오. 3. **일반** 페이지에서 관리자의 식별명 및 암호가 EIM을 구성하는 동안 입력한 이름과 암호와 일치하는지 확인하십시오.
로컬 디렉토리 서버 구성을 변경하는 중에 오류가 발생했습니다. GLD0232: 구성에 중첩 접미사가 포함될 수 없습니다. **주:** EIM(Enterprise Identity Mapping)을 사용하는 경우, 이 오류가 발생합니다.	이 오류를 회복하려면 다음을 완료하십시오. 1. iSeries Navigator에서 **iSeries** —> **네트워크** —> **서버** —> **TCP/IP**를 확장하십시오. 2. **디렉토리**를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오. 3. **데이터베이스/접미사** 페이지에서 모든 **ibm-eimDomainName** 항목을 제거하고 EIM을 재구성하십시오.
연결 설정을 확인하는 중에 오류가 발생했습니다. iSeries 프로그램을 호출하는 중에 예외가 발생했습니다. 호출된 프로그램은 eimConnect입니다. 세부사항은 com.ibm.as400.data.PcmlException입니다. **주:** EIM(Enterprise Identity Mapping)을 사용하는 경우, 이 오류가 발생합니다.	이 오류를 회복하려면 다음을 완료하십시오. 1. iSeries Navigator에서 **iSeries** —> **네트워크** —> **서버** —> **TCP/IP**를 확장하십시오. 2. **디렉토리**를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오. 3. **데이터베이스/접미사** 페이지에서 모든 **ibm-eimDomainName** 항목을 제거하고 EIM을 재구성하십시오.

관련 정보

Kerberos 프로토콜 스펙

The Kerberos Network Authentication Service(V5)
IETF(Internet Engineering Task Force)는 RFC(Request for Comment) 1510에서 Kerberos 프로토콜을 정식으로 정의합니다.

Kerberos: The Network Authentication Protocol(V5)
Massachusetts Institute of Technology의 Kerberos 프로토콜에 대한 공식 문서에서 프로그래밍 정보를 제공하고 프로토콜 피처를 설명합니다.

GSS(Generic Security Services) API 스펙

Kerberos 및 GSS API에 대한 자세한 정보는 다음 소스를 참조하십시오.

Generic Security Service Application Program Interface Version 2, Update 1
IETF(Internet Engineering Task Force)는 RFC(Request for Comment) 2743에 GSS API를 정식으로 정의합니다.

Generic Security Service API : C-bindings
IETF(Internet Engineering Task Force)는 RFC(Request for Comment) 1509에 GSS API C-바인딩을 지정합니다.

The Kerberos Version 5 GSS-API Mechanism
IETF(Internet Engineering Task Force)는 RFC(Request for Comment) 1964에 Kerberos 버전 5와 GSS API 스펙을 정의합니다.

Information Center 관련 주제

네트워크 인증서비스 API(Application Programmable Interface)
이 Information Center 주제에서는 네트워크 인증 서비스 API 리스트와 해당 기능에 대한 간단한 설명을 제공합니다.

GSS API(Generic Security Service Application Programmable Interface)
이 Information Center 주제에서는 GSS API 리스트와 해당 기능에 대한 간단한 설명을 제공합니다.

EIM(Enterprise Identity Mapping)
EIM(Enterprise Identity Mapping)은 개인이나 엔티티(예: 서비스)를 기업망에서 다양한 사용자 레지스트리의 해당 사용자 ID로 맵핑하는 메카니즘입니다. iSeries에서는 네트워크 인증 서비스를 통해 사용자를 인증할 수 있도록 EIM을 사용하여 OS/400 인터페이스를 활성화합니다. iSeries와 어플리케이션에서는 또한 Kerberos 티켓을 허용하고 EIM을 사용하여 Kerberos 프린시펄과 연관된 시스템의 사용자 ID를 찾을 수 있습니다.

특별 조항 및 조건

다음 조항 및 조건은 라이브러리 QSYS의 서비스 프로그램 QKRBGSS, 라이브러리 QSYSINC의 파일 H에 있는 KRB5 및 /QIBM/ProdData/OS400/NetworkAuthentication/ 디렉토리의 메시지 카달로그 skrbdll.cat 및 skrbkut.cat 에 들어 있는 네트워크 인증 서비스 코드에만 적용됩니다.

IBM은 네크워크 인증 서비스 오브젝트 코드에 대해 상품성 및 특정 목적에의 적합성을 포함하여(단, 이에 한하지 않음) 어떠한 종류의 보증도 없이 "현상태대로" 사용권을 제공합니다.

IBM은 해당 코드의 사용이 제3자의 저작권, 영업 기밀, 특허, 또는 기타 지적 재산권, 소유권 또는 계약권을 침해하지 않는다는 것을 보증하지 않습니다.

해당 관계자는 다음을 표시해야 합니다.

본 소프트웨어를 미국으로 수출하기 위해서는 미국 정부의 특별 면허가 필요합니다. 수출하고자 하는 개인이나 조직은 수출 전에 해당 면허를 획득해야 합니다. 수출하기 전에 해당 면허를 획득하는 것은 수출하고자 하는 개인이나 조직의 책임입니다.

이러한 제한조건 내에서, 본 소프트웨어 및 이에 관한 문서를 용도에 상관없이 사용, 복사, 수정 및 배포할 수 있는 권한이 무료로 부여됩니다. 단, 모든 사본에 상기 저작권을 표시하고, 지원 문서에 상기 저작권 표시 및 이러한 권한을 표시해야하며, 특정한 사전 서면 허가없이 본 소프트웨어의 배포에 관한 광고나 선전물에 M.I.T.의 이름을 사용할 수 없습니다. M.I.T.는 어떠한 목적으로도 본 소프트웨어의 적합성에 대한 보증을 하지 않습니다. 본 소프트웨어는 ″현상태대로″ 제공되며, 어떠한 명시적 또는 묵시적 보증도 하지 않습니다.

본 소프트웨어를 미국으로 수출하기 위해서는 미국 정부의 특별 면허가 필요합니다. 수출하고자 하는 개인이나 조직은 수출 전에 해당 면허를 획득해야 합니다. 수출하기 전에 해당 면허를 획득하는 것은 수출하고자 하는 개인이나 조직의 책임입니다.

이러한 제한조건 내에서, 본 소프트웨어 및 이에 관한 문서를 용도에 상관없이 사용, 복사, 수정 및 배포할 수 있는 권한이 무료로 부여됩니다. 단, 모든 사본에 상기 저작권을 표시하고, 지원 문서에 상기 저작권 표시 및 이러한 권한을 표시해야하며, 특정한 사전 서면 허가없이 본 소프트웨어의 배포에 관한 광고나 선전물에 M.I.T.의 이름을 사용할 수 없습니다. Open Computing Security Group인 M.I.T.나 CyberSAFE Corporation은 어떠한 목적으로도 본 소프트웨어의 적합성에 대한 보증을 하지 않습니다. 본 소프트웨어는 ″현상태대로″ 제공되며, 어떠한 명시적 또는 묵시적 보증도 하지 않습니다.

본 소프트웨어를 미국으로 수출하기 위해서는 미국 정부의 특별 면허가 필요합니다. 수출하고자 하는 개인이나 조직은 수출 전에 해당 면허를 획득해야 합니다. 수출하기 전에 해당 면허를 획득하는 것은 수출하고자 하는 개인이나 조직의 책임입니다.

이러한 제한조건 내에서, 본 소프트웨어를 및 이에 관한 문서를 용도에 상관없이 사용, 복사, 수정 및 배포할 수 있는 권한이 무료로 부여됩니다. 단, 모든 사본에 상기 저작권 표시를 하고 지원 문서에 상기 저작권 표시 및 이러한 권한 표시를 해야 특정한 사전 서면 허가없이 본 소프트웨어의 배포에 관한 광고나 선전물에 Richard P. Basch, Lehman Brothers 및 M.I.T.라는 이름을 사용할 수 없습니다. Richard P. Basch, Lehman Brothers 및 M.I.T.는 어떤 목적으로도 본 소프트웨어의 적합성에 대한 보증을 하지 않습니다. 본 소프트웨어는 ″현상태대로″ 제공되며, 어떠한 명시적 또는 묵시적 보증도 하지 않습니다.

이러한 특별한 조항 및 조건은 위에서 명시된 네트워크 인증 서비스 코드에만 적용되며 OS/400이나 사용권이 있는 내부 코드의 기타 다른 부분에 대해서는 적용되지 않습니다.

Printed in U.S.A