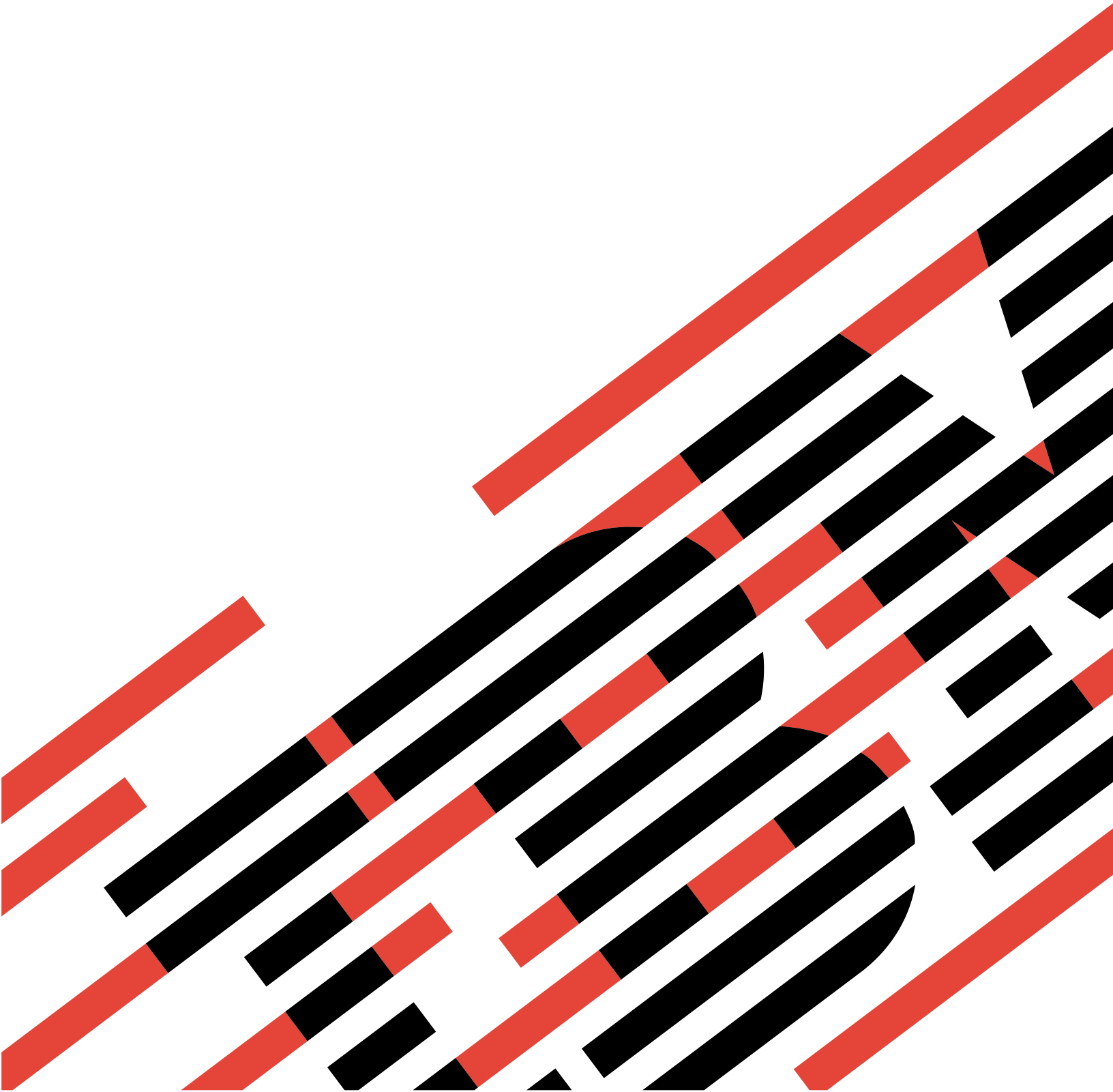
IBM

eserver

iSeries

네트워킹 디렉토리 서비스(LDAP)



IBM

@server

iSeries

네트워킹 디렉토리 서비스(LDAP)

목차

제 1 부 디렉토리 서비스(LDAP)

디렉토리 서비스는 iSeries 서버에 LDAP(Lightweight Directory Access Protocol) 서버를 제공합니다. LDAP는 TCP/IP(Transmission Control Protocol/Internet Protocol)를 통해 실행되고 인터넷과 비인터넷 어플리케이션용 디렉토리 서비스로서 널리 사용되고 있습니다.

디렉토리 서비스에 대해 잘 알고 있으면 이 릴리스에 대한 새로운 사항을 읽으면서 시작할 수 있습니다. 원한다면 디렉토리 서비스 정보에 관한 PDF 버전을 인쇄 또는 표시할 수 있습니다.

다음 주제에서는 디렉토리 서비스를 소개하고, iSeries™ 서버에서 LDAP 서버를 관리하는 데 도움이 되는 정보를 제공합니다.

디렉토리 서비스에 대한 추가 정보는 디렉토리 서비스 웹 페이지  를 방문하십시오.

디렉토리 서비스에서 제공하는 LDAP 서버는 IBM® SecureWay® Directory  입니다.

제 1 장 V5R2의 새로운 사항

디렉토리 서비스에는 다음과 같은 확장 기능과 새로운 피처가 있습니다.

- 디렉토리 서비스는 V5R1에서 시작하는 기본 오퍼레이팅 시스템의 일부입니다. 옵션 32는 V5R2에서 시작할 수 없습니다.
- 디렉토리 서버에 저장된 자료를 보호할 수 있도록 신규 보안 확장 기능을 마련하였습니다.
- 이제 LDAP 디렉토리 서버를 EIM(Enterprise Identity Mapping) 정의역의 정의역 제어기로 사용할 수 있습니다.
- 관리자는 iSeries Navigator 어플리케이션 지원을 통해 오퍼레이팅 시스템의 디렉토리 서비스 관리자(QIBM_DIRSRV_ADMIN) 함수 ID에 대한 액세스 권한이 부여된 사용자에게 디렉토리 서버에 대한 관리자 액세스 권한을 부여하는 데 사용할 수 있는 새 옵션을 사용할 수 있습니다.
- 디렉토리 서버가 특정 IP 주소를 사용하도록 선택하거나 서버에 구성된 모든 IP 주소를 사용하도록 선택할 수 있습니다. 자세한 정보는 22 페이지의 『포트 또는 IP 주소 변경』을 참조하십시오.
- **ldap_set_option** API에는 V5R2를 위한 새로운 디버그 추적 피처가 있습니다. LDAP_OPT_DEBUG 옵션을 사용하여 LDAP C API를 사용하는 클라이언트의 문제점을 진단할 수 있습니다. 자세한 정보는 69 페이지의 『LDAP_OPT_DEBUG 옵션을 사용하여 오류 추적』 또는 iSeries Information Center의 Directory Services APIs 를 참조하십시오.

새로운 사항이나 변경된 사항을 보는 방법

기술적인 변경이 이루어진 장소를 보려면 다음 정보를 사용하십시오.

- 새롭거나 변경된 정보가 시작되는 위치를 표시하는 ▲ 이미지.
- 새롭거나 변경된 정보가 끝나는 위치를 표시하는 ▼ 이미지.

제 2 장 이 주제 인쇄

PDF 버전을 열람하거나 다운로드하려면 디렉토리 서비스(LDAP)(약 323KB 또는 66 페이지)를 선택하십시오.

기타 정보

다음 PDF를 열람하거나 인쇄할 수도 있습니다.

- *LDAP Implementation Cookbook* .
- *Understanding LDAP* .
- *Using LDAP for Directory Integration: IBM SecureWay Directory, Active Directory* 및 *Domino*™ 참조.
- *Implementation and Practical Use of LDAP on the iSeries Server* .

PDF를 열람하거나 인쇄하기 위해 워크스테이션에 저장하려면 다음을 수행하십시오.

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

Adobe Acrobat Reader 다운로드

이 PDF를 보거나 인쇄하는 데 Adobe Acrobat Reader가 필요한 경우, Adobe 웹 사이트 (www.adobe.com/products/acrobat/readstep.html)에서 사본을 다운로드할 수 있습니다.

제 3 장 디렉토리 서비스 시작하기

디렉토리 서비스는 iSeries 서버에 LDAP(Lightweight Directory Access Protocol) 서버를 제공합니다. LDAP는 TCP/IP(전송 제어 프로토콜/인터넷 프로토콜)에서 실행되며, 인터넷과 비인터넷 어플리케이션용 디렉토리 서비스로서 인기를 얻고 있습니다. iSeries Navigator의 GUI(Graphical User Interface)를 통해 OS/400 기반의 LDAP 디렉토리 서버에 대한 대부분의 설정 및 관리 타스크를 수행할 수 있습니다. 디렉토리 서비스를 관리하려면, iSeries 서버에 연결된 PC에 iSeries Navigator가 설치되어 있어야 합니다. LDAP 서버에서 전자 우편 주소를 찾는 메일 어플리케이션 같은 LDAP 작동가능 어플리케이션과 함께 디렉토리 서비스를 사용할 수 있습니다.

디렉토리 서비스에는 LDAP 서버 이외에도 다음이 포함됩니다.

- OS/400 기반의 LDAP 클라이언트. 이 클라이언트는 사용자의 클라이언트 어플리케이션을 작성하기 위해 OS/400® 프로그램에서 사용할 수 있는 API(어플리케이션 프로그램 인터페이스) 세트를 포함합니다. 이러한 API에 대한 정보는 iSeries Information Center의 프로그래밍에서 디렉토리 서비스 주제를 참조하십시오.
- IBM SecureWay Directory Client SDK(소프트웨어 개발 킷)의 버전 3.2. SDK에는 Windows® LDAP 클라이언트와 다음 툴이 들어 있습니다.
  - 디렉토리 내용을 관리하기 위한 그래픽 사용자 인터페이스를 제공하는 IBM SecureWay Directory 관리 툴
  - 명령행 유틸리티(ldapsearch, ldapadd 등)
  - C LDAP API(라이브러리 파일, 헤더 파일 및 샘플 소스 코드)
  - IBM JNDI LDAP 서비스 제공자(ibmjndi.jar)
  - 위의 모든 항목에 대한 온라인 문서. 이러한 HTML 파일의 위치와 이름에 대해서는 Readme 파일을 참조하십시오.

OS/400 이전 릴리스에서 디렉토리 서비스를 사용한 경우, 12 페이지의 『디렉토리 서비스의 이전 릴리스에서 V5R2로 마이그레이트』를 참조하십시오.

LDAP에 대한 소개는 8 페이지의 『LDAP 기본』을 참조하십시오. LDAP 서버를 다른 플랫폼에서 사용하는 경우에도 몇 가지 OS/400 특정 정보가 수록되어 있기 때문에 이 주제를 읽는 데 몇 분이 걸릴 수 있습니다.

기본 정보에 친숙해졌을 때 11 페이지의 『LDAP 디렉토리 서버 계획』으로 가십시오.

디렉토리 서버 설치 및 구성에 관한 정보는 15 페이지의 『디렉토리 서비스 설치 및 구성』을 참조하십시오.

문서

| 디렉토리 서비스 Information Center 주제는 LDAP의 개요를 제공하며, 특히 OS/400의 LDAP 디렉토리 서
| 버 관리에 중점을 두고 있습니다. 또한 이 문서는 SecureWay Directory Client SDK의 전체 문서를 제공합
| 니다. 추가적인 LDAP의 정보는 다음과 같은 LDAP 도서 목록을 참조하십시오.

- *LDAP Implementation Cookbook* .
- *Understanding LDAP* .
- *Using LDAP for Directory Integration: IBM SecureWay Directory, Active Directory* 및 *Domino* 참조.
- *Implementation and Practical Use of LDAP on the iSeries server* .
- Tim Howes와 Mark Smith의 *LDAP: Programming Directory-enabled Applications with Lightweight Directory Access Protocol*.
- Mark C, Smith, Gordon S. Good 및 Tim Howes의 *Understanding and Deploying LDAP Directory Services*.

iSeries 서버의 디렉토리 서비스에 대한 추가 정보는 iSeries 서버 디렉토리 서비스 홈 페이지에서 사용할 수 있습니다.

주: 이 문서에 수록된 자료의 일부는 미시간 대학에서 제공한 LDAP 문서에서 발췌한 것입니다.

LDAP 기본

LDAP(Lightweight Directory Access Protocol)는 TCP/IP 에서 실행되는 디렉토리 서비스 프로토콜입니다. LDAP 버전 2는 Internet Engineering Task Force (IETF) Request for Comments (RFC) 1777, *Lightweight Directory Access Protocol*에서 공식적으로 정의됩니다. LDAP 버전 3은 IETF RFC 2251, *Lightweight Directory Access Protocol (v3)*에서 공식적으로 정의됩니다. 다음 URL에서 인터넷의 이들 RFC를 볼 수 있습니다.

http://www.ietf.org

LDAP 디렉토리 서비스는 클라이언트/서버 모델을 따릅니다. 하나 이상의 LDAP 서버에 디렉토리 자료가 있습니다. LDAP 클라이언트는 LDAP 서버에 연결되고, 요구를 만듭니다. 서버는 응답 또는 다른 LDAP 서버에 대한 포인터(리퍼럴)로 응답합니다.

LDAP의 사용:

LDAP는 데이터베이스가 아니라 디렉토리 서비스이기 때문에 LDAP 디렉토리에 있는 정보는 보통 설명적인 속성 기반 정보입니다. LDAP 사용자는 일반적으로 디렉토리에 있는 정보를 변경하는 것보다 훨씬 자주 정보를 읽습니다. 갱신은 일반적으로 단순한 전부 아니면 전무 변경입니다. LDAP 디렉토리의 공통적인 사용은 온라인 전화 디렉토리와 전자 우편 디렉토리를 포함합니다.

LDAP 디렉토리 구조:

LDAP 디렉토리 서비스 모델은 **항목(오브젝트**라고도 함)을 기준으로 합니다. 각 항목은 이름, 주소 및 **유형**같은 하나 이상의 **속성**으로 구성됩니다. 유형은 일반적으로 공통명의 경우 cn 또는 전자 우편 주소의 경우 mail 같은 니모닉 스트링으로 구성됩니다.

10 페이지의 그림 1에 있는 디렉토리의 예는 *mail* 및 *telephoneNumber* 속성을 포함하는 Tim Jones의 항목을 표시합니다. 그 밖에 가능한 속성으로 *fax, title, sn*(별명의 경우) 및 *jpegPhoto*가 있습니다.

각 항목은 디렉토리의 구조와 내용을 판별하는 규칙 세트인 **스키마**를 가지고 있습니다. LDAP 서버에 대한 스키마 파일을 편집하기 위해 IBM SecureWay DMT(디렉토리 관리 툴)를 사용해야 합니다. 디렉토리 서비스 설치 후, 파일은 /QIBM/UserData/OS400/DirSrv에 위치합니다.

주: 디폴트 스키마 파일의 원본은 /QIBM/ProdData/OS400/DirSrv에서 찾을 수 있습니다. UserData 디렉토리에 있는 파일을 대체해야 할 경우에는 이 파일을 /QIBM/ProdData/OS400/DirSrv 디렉토리에 복사할 수 있습니다.

각 디렉토리 항목은 **objectClass**라고 하는 특수한 속성을 가지고 있습니다. 이 속성은 항목에 필요하고 허용되는 속성을 제어합니다. 즉, objectClass 속성 값은 항목이 준수해야 하는 스키마 규칙을 판별합니다.

각 디렉토리 항목에는 LDAP 서버가 자동으로 유지보수하는 다음 **동작 속성**도 있습니다.

- CreatorsName에는 항목 작성시 사용되는 바인드 DN이 들어 있습니다.
- CreateTimestamp에는 항목을 작성한 시간이 들어 있습니다.
- modifiersName에는 항목의 최종 수정시 사용했던 바인드 DN이 들어 있습니다(초기에는 CreatorsName과 동일함).
- modifyTimestamp에는 항목을 최종으로 수정했던 시간이 들어 있습니다(초기에는 CreateTimestamp과 동일함).

일반적으로, LDAP 디렉토리 항목은 행정적, 지리적 또는 조직적인 경계를 반영하는 계층 구조로 배열됩니다(10 페이지의 그림 1 참조). 국가를 표시하는 항목은 계층의 맨 위에 나타납니다. 주 또는 국가 조직을 표시하는 항목은 계층의 두번째 레벨을 차지합니다. 이때 아래의 항목은 사람, 조직 단위, 프린터, 문서 또는 다른 항목을 나타낼 수 있습니다.

디렉토리를 구조화할 때 일반적인 계층으로 제한되지 않습니다. 예를 들면, 도메인 구성요소 구조는 널리 사용되고 있습니다. 이 구조를 사용하면 항목은 TCP/IP 도메인명의 일부분으로 구성됩니다. 예를 들어, dc=ibm, dc=com이 o=ibm, c=us보다 나을 수 있습니다.

LDAP는 **고유명**(DN)으로 항목을 참조합니다. 고유명은 디렉토리에서 그 위에 있는 오브젝트의 맨 아래부터 맨 위까지의 순서로 된 이름뿐만 아니라 항목 자체의 이름으로 구성됩니다. 예를 들어, 10 페이지의 그림 1의 맨 아래 좌측 가장자리에 있는 항목의 완전한 DN은 cn=Tim Jones, o=IBM, c=US입니다. 각 항목은 항목을 명명하는 데 사용되는 최소한 하나의 속성을 가지고 있습니다. 이 명명 속성을 항목의 **RDN(상대 고유명)**이라고 합니다. 주어진 RDN 위의 항목은 **상위 고유명**이라고 합니다. 위의 예에서, cn=Tim Jones는 항목을 명명한 것이므로 RDN입니다. o=IBM, c=US는 cn=Tim Jones에 대한 상위 DN입니다.

LDAP 서버에 LDAP 디렉토리의 부분을 관리할 수 있는 기능을 부여하기 위해 서버의 구성에 최상위 레벨 상위 고유명을 지정합니다. 이 고유명을 **접미부**라고 합니다. 서버는 디렉토리 계층에서 지정된 접미부 아래에 있는 디렉토리의 모든 오브젝트에 액세스할 수 있습니다. 예를 들어, LDAP 서버에 그림 1에서 표시한 디렉토리가 들어 있는 경우, Tim Jones에 관한 클라이언트 조회에 응답할 수 있으려면 구성에 접미부 `o=ibm, c=us`를 지정해야 합니다.

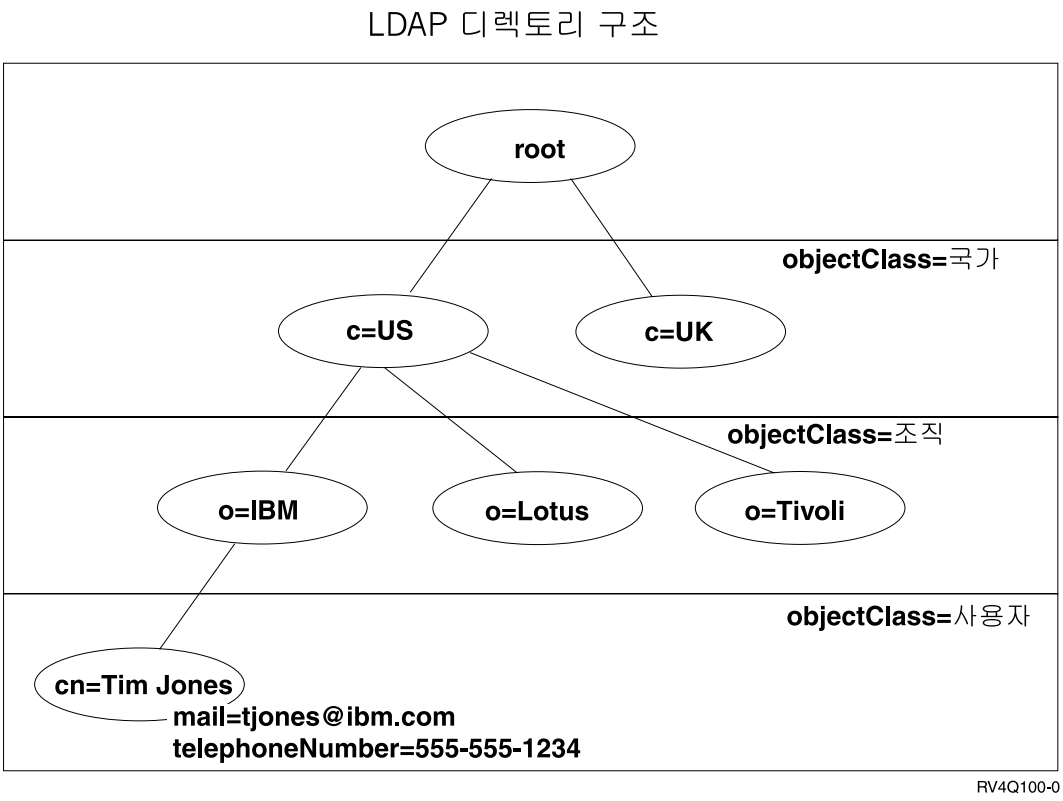


그림 1. 기본 LDAP 디렉토리 구조

LDAP 및 디렉토리 서비스에 대한 참고사항™:

- V4R5부터, OS/400 LDAP 서버와 OS/400 LDAP 클라이언트 모두 LDAP 버전 3에 기초합니다. V3 서버로 V2 클라이언트를 사용할 수 있습니다. 그러나 V2 클라이언트로서 바인드하고 V2 API만을 사용하지 않는 이상 V2 서버로 V3 클라이언트를 사용할 수 없습니다. 자세한 내용은 LDAP V2/V3 고려사항을 참조하십시오.
- 또한 Windows LDAP 클라이언트는 LDAP 버전 3에 기초합니다.
- LDAP가 표준이기 때문에 모든 LDAP 서버는 많은 기본 특성을 가지고 공유합니다. 그러나 구현상의 차이 때문에 서로 완전히 호환될 수는 없습니다. 디렉토리 서비스가 제공하는 LDAP 서버는 IBM SecureWay Directory 및 IBM 디렉토리 제품 그룹에 있는 다른 LDAP 디렉토리 서버와 밀접하게 호환될 수 있습니다. 그러나 다른 LDAP 서버와는 호환이 불가능할 수 있습니다.
- 디렉토리 서비스가 제공하는 LDAP 서버용 자료는 OS/400 데이터베이스에 상주합니다.

추가 정보:

| LDAP 디렉토리 사용에 관한 예는 다음을 참조하십시오.

| • 섹션 1.6 빠른 시작: 레드북 *Understanding LDAP*의 공용 LDAP 예.

| • 섹션 3.3 예 시나리오, 레드북 Understanding LDAP.

LDAP 개념을 더 많이 알려면 37 페이지의 제 5 장 『디렉토리 서비스 개념 및 참조 정보』를 참조하십시오.

LDAP V3으로 LDAP V2를 사용하기 위한 고려사항

V4R5부터, OS/400 LDAP 서버와 OS/400 LDAP 클라이언트는 모두 LDAP 버전 3에 기초합니다. V2 서버로 V3 클라이언트를 사용할 수 없습니다. 그러나 ldap_set_option() API를 사용하여 V3 클라이언트 버전을 V2로 변경할 수 있습니다. 그러면 클라이언트 요구를 V2 서버에 성공적으로 송신할 수 있습니다.

V3 서버로 V2 클라이언트를 사용할 수 있습니다. 그러나 탐색 요구가 있을 때 V3 서버는 UTF-8 형식으로 전범위의 데이터를 되돌려 보낼 수 있는 반면에 V2 클라이언트는 IA5 문자 세트로 데이터만 처리할 수 있다는 사실에 유의하십시오.

주: LDAP 버전 2는 Internet Engineering Task Force (IETF) Request for Comments (RFC) 1777, *Lightweight Directory Access Protocol*에서 공식적으로 정의됩니다. LDAP 버전 3은 IETF RFC 2251, *Lightweight Directory Access Protocol (v3)*에서 공식적으로 정의됩니다. 다음 URL에서 인터넷의 이들 RFC를 볼 수 있습니다.

http://www.ietf.org 

LDAP 디렉토리 서버 계획

디렉토리 서비스를 설치하고, LDAP 디렉토리 구성을 시작하기 전에 디렉토리를 계획하는 시간을 가져야 합니다. 고려해야 할 중요한 사항은 다음과 같습니다.

- **디렉토리 구성**. 디렉토리의 구조를 계획하고 서버에 필요한 접미부와 속성을 판별하십시오.
- **디렉토리의 크기를 결정하십시오**. 필요한 기억장치의 용량을 추정할 수 있습니다. 디렉토리의 크기는 다음 사항에 따라 다릅니다.
  - 서버의 스키마에 있는 속성 수.
  - 서버의 항목 수.
  - 서버에 저장하는 정보 유형.

  예를 들면, 디폴트 디렉토리 서비스 스키마를 사용하는 빈 디렉토리는 약 10MB의 기억영역 공간이 필요합니다. 디폴트 스키마를 사용하고 1000개의 일반 직원 정보 항목을 포함하는 디렉토리는 약 30MB의 기억영역 공간이 필요합니다. 이 수는 사용한 정확한 속성에 따라 달라질 수 있습니다. 또 디렉토리에 영상같은 큰 오브젝트가 저장된 경우, 크게 증가할 수 있습니다.
- **사용자가 취할 보안 수단 결정**. 디렉토리 서비스는 통신 보안을 위해 TLS(변환층 보안)와 함께 SSL(보안 소켓층) 및 디지털 인증의 사용을 지원합니다. V5R1부터 Kerberos 인증 또한 지원합니다.

- 디렉토리 서비스를 사용하면 액세스 제어 리스트(ACL)가 있는 디렉토리 오브젝트에 대한 액세스를 제어할 수 있습니다. 또한 OS/400 보안 감사를 사용하여 디렉토리를 보호할 수 있습니다.

디렉토리 서비스의 이전 릴리스에서 V5R2로 마이그레이트

OS/400의 V5R2에서는 새로운 피처와 기능을 디렉토리 서비스에 도입합니다. 이러한 변경사항은 iSeries Navigator의 LDAP 디렉토리 서버와 그래픽 사용자 인터페이스(GUI)에 모두 영향을 미칩니다. 새로운 GUI 피처를 이용하려면 TCP/IP상에서 iSeries 서버와 통신할 수 있는 PC에 iSeries Navigator를 설치해야 합니다. iSeries Navigator는 Windows용 iSeries Access의 구성요소입니다. iSeries Navigator의 이전 버전이 설치되어 있으면 V5R2로 업그레이드해야 합니다.

OS/400의 V5R2은 V4R5와 V5R1에서 업그레이드를 지원합니다. OS/400의 V5R2로 업그레이드하면 LDAP 디렉토리 자료와 디렉토리 스키마 파일이 모두 자동으로 업그레이드되어 V5R2 형식과 일치하게 됩니다. 디렉토리 서비스 LDAP 서버가 OS/400의 V4R3 또는 V4R4에서 실행되고 있고 V5R2로 서버를 마이그레이트하려는 경우 몇몇 추가 마이그레이션 타스크를 수행해야 합니다.

OS/400의 V5R2로 업그레이드할 때는 일부 마이그레이션 문제에 대해 알고 있어야 합니다.

- V5R2로 업그레이드할 때 디렉토리 서비스가 자동으로 스키마 파일을 V5R2로 마이그레이트하고 기존 스키마 파일을 삭제합니다. 그러나 스키마 파일을 삭제하거나 이름을 변경한 경우, 디렉토리 서비스는 스키마 파일을 마이그레이트할 수 없습니다. 오류를 수신할 수도 있고, 그렇지 않으면 디렉토리 서비스에서 파일이 이미 마이그레이트되었다고 가정할 수도 있습니다.
- 처음으로 서버를 시작하거나 LDIF 파일을 가져올 때 디렉토리 서비스가 디렉토리 자료를 V5R2 형식으로 마이그레이트합니다. 이 마이그레이션이 완료될 때까지 얼마간의 시간을 할애하도록 계획하십시오. V4R4 이전 릴리스에서 V5R2로 업그레이드할 경우, V5R2에는 전보다 두 배 정도 많은 디렉토리 자료가 필요합니다. 이것은 V4R4 이전 버전에서 디렉토리 서비스가 IA5 문자 세트만을 지원하고 자료를 ccsid 37에 저장하기 때문입니다. 디렉토리 서비스가 전체 ISO 10646 문자 세트를 지원합니다.

  V5R2로 업그레이드한 후에는 새로운 자료를 가져오기 전에 서버를 한 번 시작해서 기존 자료를 업그레이드해야 합니다. 서버를 시작하기 전에 자료를 가져오려고 시도했을 때 권한이 충분하지 않으면 가져오기가 실패할 수 있습니다.
- 디렉토리 서비스의 V4R4 이전 릴리스에서는 시간소인 항목을 작성할 때 시간대를 고려하지 않았습니다. V4R5부터 디렉토리에 대한 모든 추가 및 수정 사항에 시간대가 사용됩니다. 따라서 V4R4 이전 릴리스에서 V5R2로 업그레이드하는 경우, 디렉토리 서비스는 올바른 시간대를 반영하도록 기존 `createtimestamp` 및 `modifytimestamp` 속성을 조정합니다. 그렇게 하려면 현재 iSeries 시스템에 정의된 시간대를 디렉토리에 저장된 시간소인에서 제거합니다. 현재의 시간대는 항목이 처음에 작성되거나 수정되었을 때 사용했던 것과 같은 시간대가 아닌 경우, 새로운 시간소인 값은 처음의 시간대를 반영하지 않는다는 점에 주의하십시오.
- 마이그레이션한 뒤에는 TCP/IP가 시작될 때 자동으로 LDAP 디렉토리 서버가 시작됩니다. 디렉토리 서버가 자동으로 시작되지 않게 하려면, iSeries Navigator를 사용하여 설정을 변경하십시오.

V4R3 또는 V4R4 디렉토리 서비스에서 V5R2로 마이그레이트

OS/400의 V5R2는 V4R3에서 직접 업그레이드를 지원하지 않습니다. V4R3 또는 V4R4 디렉토리 서비스 LDAP 서버를 V5R2로 마이그레이트할 경우, 다음 프로시듀어 중의 하나를 수행할 수 있습니다.

- OS/400을 V4R3 또는 V4R4에서 중간 릴리스로 임시 설치
- 데이터베이스 라이브러리를 저장한 후 OS/400을 V4R3 또는 V4R4에서 V5R2로 임시 설치

OS/400을 V4R3 또는 V4R4에서 중간 릴리스로 임시 설치

OS/400의 V4R3 및 V4R4에서 V5R2로 업그레이드가 지원되지 않지만 다음 업그레이드가 지원됩니다.

- V4R3 및 V4R4가 V4R5로 업그레이드됨
- V4R4 및 V4R5가 V5R1로 업그레이드됨
- V4R5 및 V5R1이 V5R2로 업그레이드됨

디렉토리 서비스 서버를 마이그레이트하는 한 가지 방법은 중간 릴리스(V4R5 또는 V5R1)로 업그레이드한 다음, V5R2로 업그레이드하는 것입니다. OS/400 설치 프로시듀어에 대한 자세한 정보는 *소프트웨어 설치* 를 참조하십시오. 마이그레이션을 수행하려면 다음의 일반적인 단계를 수행하십시오.

1. 스키마 파일의 변경사항을 /QIBM/UserData/OS400/DirSrv 디렉토리에 기록하십시오. 스키마 파일이 자동으로 마이그레이트됩니다.
2. V4R4 또는 V4R3의 경우 OS/400의 V4R5 또는 V5R1을 임시 설치하십시오.
3. OS/400의 V5R2로 임시 설치하십시오.
4. 시작되지 않았으면 디렉토리 서비스 서버를 시작하십시오.
5. 디렉토리 관리 툴을 사용하여 1단계에서 기록한 사용자 변경사항에 맞게 스키마 파일을 수정하십시오.
6. 디렉토리 서비스 서버를 다시 시작하십시오.

데이터베이스 라이브러리를 저장한 후 OS/400을 V4R3 또는 V4R4에서 V5R2로 임시 설치

디렉토리 서비스 서버를 마이그레이트하는 다른 방법은 디렉토리 서비스가 V4R3 또는 V4R4에서 사용하는 데이터베이스 라이브러리를 저장한 다음, V5R2 임시 설치 후에 복원하는 것입니다. 그러면 중간 릴리스의 설치 단계를 수행하지 않아도 됩니다. 그러나 서버의 설정이 마이그레이트되지 않기 때문에 서버 설정을 다시 구성해야 합니다. OS/400 설치 프로시듀어에 대한 자세한 정보는 *소프트웨어 설치* 를 참조하십시오. 마이그레이션을 수행하려면 다음의 일반적인 단계를 수행하십시오.

1. 스키마 파일의 변경사항을 /QIBM/UserData/OS400/DirSrv 디렉토리에 기록하십시오. 스키마 파일이 자동으로 마이그레이트되지 않으므로 변경사항을 유지하려면, 스키마 파일을 수동으로 다시 구현해야 합니다.
2. 데이터베이스 라이브러리명을 포함하여 디렉토리 서비스 서버의 등록 정보에 여러 가지 구성 설정을 기록하십시오.
3. 디렉토리 서비스 서버의 구성에 지정된 데이터베이스 라이브러리를 저장하십시오.
4. 게시 구성을 기록하십시오.

5. 시스템을 OS/400의 V5R2로 임시 설치하십시오.
6. EZ 설치를 사용하여 디렉토리 서비스 서버를 구성하십시오.
7. 13 페이지의 3단계에서 저장한 데이터베이스 라이브러리를 복원하십시오.
8. 디렉토리 관리 툴을 사용하여 13 페이지의 1단계에서 기록한 사용자 변경사항에 맞게 스키마 파일을 수정하십시오.
9. iSeries Navigator를 사용하여 디렉토리 서비스를 다시 구성하십시오. 저장 및 복원한 데이터베이스 라이브러리를 지정하십시오.
10. iSeries Navigator를 사용하여 게시를 다시 구성하십시오.
11. 디렉토리 서비스 서버를 다시 시작하십시오.

업그레이드 문제

V4R3에서 임의의 최근 릴리스로 업그레이드할 때 다음 사항을 알고 있어야 합니다.

- **키 링 파일을 키 데이터베이스로 마이그레이트할 경우:**

  V3R2 Client Access는 LDAP 디렉토리 서버에 SSL(보안 소켓층) 연결을 구축하기 위해 키 링 파일을 사용했습니다. Windows용 iSeries Access는 SSL 연결을 구축하기 위해 키 데이터베이스라고 하는 인증 저장소를 사용합니다. 키 링 파일은 이전에 LDAP 디렉토리 서버로 사용한 경우에 SSL을 계속 사용할 수 있도록 키 데이터베이스로 변환해야 합니다. LDAP 디렉토리 서버에 SSL 연결을 처음 시작할 경우, iSeries Navigator가 이 변경에 대해 경고하게 됩니다. 키 변환을 선택한 경우 변환되기 전에 키 데이터베이스에 대한 일부 정보를 지정하라고 프롬트됩니다.

  LDAP 디렉토리 서버는 또한 V4R3에서 SSL 연결을 위해 키 링 파일을 사용했습니다. V4R4에서부터 LDAP 디렉토리 서버는 시스템 인증 저장소를 사용합니다. 서버가 V4R3에서 SSL을 사용하도록 설정된 경우, 키 링 파일의 내용이 시스템 인증 저장소로 마이그레이트됩니다.

- **두 개의 스트림 파일이 제거되었습니다.**

  V4R3에서 디렉토리 서비스가 사용하는 다음 스트림 파일은 더 이상 필요하지 않으며 최근 릴리스를 설치할 때 자동으로 제거됩니다.

  ```
  /QIBM/ProdData/OS400/DirSrv/qgldcert.kyr
  /QIBM/ProdData/OS400/DirSrv/qgldcert.sth
  ```

  이 파일에 대한 조치를 취하지 않아도 됩니다. 이것은 단지 해당 파일이 더 이상 시스템에 없다고 통지되는 경우 걱정하지 않도록 언급됩니다.

또한 기타 릴리스에서 현재 릴리스로 업그레이드와 관련하여 추가 문제가 있을 수 있습니다.

디렉토리 서비스 설치 및 구성

OS/400를 설치할 때 디렉토리 서비스(LDAP)가 자동으로 설치됩니다. 디렉토리 서버에는 TCP/IP가 시작될 때 디렉토리 서버를 자동으로 시작하는 디폴트 구성이 포함되어 있습니다. 또한 디렉토리 서버는 OS/400의 컴퓨터 정보를 디렉토리 서버에 게시하기 시작합니다. LDAP 디렉토리 서버의 설정을 사용자 정의하려면 디렉토리 서비스 구성 마법사를 실행하십시오. 마법사를 사용하려면 *ALLOBJ 및 *IOSYSCFG 특수 권한이 있어야 합니다.

디렉토리 서비스는 V5R1부터 기본 오퍼레이팅 시스템에 통합되었고 V5R2에서 시작하여 옵션 32를 사용할 수 없습니다.

LDAP 디렉토리 서버 구성

다른 LDAP 서버에 정보가 게시되도록 시스템이 구성되지 않고, TCP/IP DNS 서버에 알려진 LDAP 서버가 없으면 디렉토리 서비스는 제한된 디폴트 구성으로 자동 설치됩니다. 디렉토리 서비스는 LDAP 디렉토리 서버를 특정 필요에 맞게 구성할 수 있도록 마법사를 제공합니다. EZ 설치의 일부로서 이 마법사를 실행하거나 나중에 iSeries Navigator에서 마법사를 실행할 수 있습니다. 디렉토리 서버를 초기에 구성할 때 이 마법사를 사용하십시오. 디렉토리 서버를 재구성할 때에도 마법사를 사용할 수 있습니다.

주: 디렉토리 서버를 재구성하기 위해 마법사를 사용할 때 스크래치부터 시작하십시오. 원래 구성은 변경되지 않고 삭제됩니다. 그러나 디렉토리 자료는 삭제되지 않고 설치 시 선택했던 라이브러리에 저장됩니다(디폴트는 QUSRDIRDB). 변경 기록부도 기본적으로 QUSRDIRCL 라이브러리에 손상되지 않고 남아 있습니다.

스크래치에서 완전하게 시작하려는 경우에는 마법사를 시작하기 전에 해당하는 두 라이브러리를 지우십시오.

디렉토리 서버 구성을 변경하지만 완전히 지우지 않을 경우, **디렉토리**를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오. 그러면 원래 구성이 삭제되지 않습니다.

서버를 구성하려면 *ALLOBJ 및 *IOSYSCFG 특수 권한이 있어야 합니다. OS/400 보안 감사를 구성할 경우에는 *AUDIT 특수 권한이 있어야 합니다.

디렉토리 서비스 구성 마법사를 시작하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭하고 **구성**을 선택하십시오.

   주: 디렉토리 서버를 이미 구성한 경우에는 **구성**이 아니라 **재구성**을 클릭하십시오.

LDAP 디렉토리 서버를 구성하려면 디렉토리 서버 구성 마법사가 제공하는 지침에 따르십시오.

주: 또한 디렉토리 자료를 저장하는 라이브러리를 시스템 ASP가 아닌 사용자 ASP(보조 기억장치 풀)에 넣으려고 할 수도 있습니다. 그러나 이 라이브러리를 독립 ASP에 저장할 수 없고 독립 ASP에 있는 라이브러리와 함께 서버를 구성, 재구성 또는 시작하려는 시도는 실패합니다.

마법사가 끝날 때 LDAP 디렉토리 서버는 기본 구성을 가집니다. 시스템에서 Lotus® Domino가 실행되고 있는 경우, 포트 389(LDAP 서버의 디폴트 포트)가 이미 Domino의 LDAP 기능에 사용되고 있을 수 있습니다. 다음 중 하나를 수행해야 합니다.

- Lotus Domino가 사용하는 포트 변경
- 디렉토리 서비스가 사용하는 포트 변경
- 특정 IP 주소 사용

이 시점에서 서버를 시작할 수 있습니다. 그러나 서버를 시작하기 전에 다음 사항 중 일부 또는 전부를 수행할 수도 있습니다.

- 서버에 자료 가져오기
- SSL(보안 소켓 층) 보안 작동가능
- Kerberos 인증 작동 가능
- 리퍼럴 설정

LDAP 디렉토리 서버에서 SSL 작동가능

디지털 인증 관리자가 시스템에 설치되어 있으면 SSL(보안 소켓 계층) 보안을 사용하여 LDAP 디렉토리 서버에 대한 액세스를 보호할 수 있습니다. 디렉토리 서버에서 SSL을 작동할 수 있도록 하기 전에 디렉토리 서비스에서 SSL 사용에 대한 개요를 읽는 것이 도움이 됩니다.

iSeries Navigator에서 LDAP 디렉토리 서버를 관리할 때 SSL 연결을 사용하거나 SSL을 Windows LDAP 클라이언트에서 사용하려면 클라이언트 암호화 제품(5722CE2 또는 5722CE3)의 하나가 PC에 설치되어 있어야 합니다.

LDAP 서버에서 SSL을 작동할 수 있게 하려면 DCM(Digital Certificate Manager) 인터페이스를 사용하십시오. iSeries Navigator에 있는 **인터넷** 폴더 또는 디렉토리 서버의 **특성** 대화상자의 **네트워크** 페이지에서 DCM(Digital Certificate Manager)를 시작할 수 있습니다.

네트워크 페이지에서 DCM(Digital Certificate Manager)을 시작하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
5. **네트워크** 탭을 클릭하십시오.
6. **DCM(Digital Certificate Manager)**을 클릭하십시오.

   DCM(Digital Certificate Manager)이 디폴트 인터넷 브라우저에서 시작합니다.

디지털 인증을 디렉토리 서버에 할당하기 위해 따라야 할 특정 단계에 대해서는 LDAP 디렉토리 서버 보안을 참조하십시오.

SSL을 작동할 수 있게 되면 LDAP 디렉토리 서버가 보안 연결에 사용하는 포트를 변경할 수 있습니다.

LDAP 디렉토리 서버에서 Kerberos 인증 작동

네트워크 인증 서비스가 시스템에 구성되어 있으면 LDAP 디렉토리 서버를 설정하여 Kerberos 인증을 사용할 수 있습니다. Kerberos를 디렉토리 서버에서 작동시키기 전에 디렉토리 서비스의 Kerberos 사용에 대한 개요를 읽는 것이 도움이 됩니다.

Kerberos 인증을 작동할 수 있게 하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
5. **Kerberos** 탭을 클릭하십시오.
6. **Kerberos 인증**을 체크하십시오.
7. 필요하면 **Kerberos** 페이지의 기타 설정을 상황에 맞게 지정하십시오. 개별 필드에 대한 정보는 페이지의 온라인 도움말을 참조하십시오.

디렉토리 서비스의 디폴트 구성

OS/400을 설치할 때 LDAP 디렉토리 서버가 자동으로 설치됩니다. 설치에는 디폴트 구성이 포함됩니다. 디렉토리 서버는 다음 사항이 모두 참일 때 디폴트 구성을 사용합니다.

- 관리자가 디렉토리 서비스 구성 마법사를 실행하지 않았거나 등록 정보 페이지에서 디렉토리 설정을 변경하지 않았습니다.
- 디렉토리 서비스 게시가 구성되지 않았습니다.
- LDAP 디렉토리 서버가 LDAP DNS 정보를 찾을 수 없습니다.

LDAP 디렉토리 서버가 디폴트 구성을 사용하는 경우, 다음 사항이 발생합니다.

- TCP/IP가 시작될 때 LDAP 디렉토리 서버가 자동으로 시작됩니다.
- 시스템에서 디폴트 관리자, cn=Administrator를 작성합니다. 내부에 사용되는 암호도 생성합니다. 관리자 암호를 나중에 사용할 경우, 디렉토리 서비스 등록 정보 페이지에서 신규 암호를 설정할 수 있습니다.
- 시스템의 IP 이름에 근거하여 디폴트 접미사가 작성됩니다. 시스템명을 기초로 시스템 오브젝트의 접미부 또한 작성됩니다. 예를 들어, 시스템의 IP 이름이 mary.acme.com인 경우, 접미사는 dc=mary, dc=acme, dc=com입니다.
- LDAP 디렉토리 서버가 디폴트 자료 라이브러리 QUSRDIRDB를 사용합니다. 시스템은 시스템 ASP에서 라이브러리를 작성합니다.
- 서버가 비보안 통신 포트 389를 사용합니다. LDAP에 대해 디지털 인증이 구성되면, SSL(보안 소켓층)이 작동되고 포트 636이 보안 통신에 사용됩니다.

다음 디폴트 값은 디렉토리 서비스 게시에 사용됩니다.

- 시스템이 로컬 LDAP 디렉토리 서버에 정보를 게시합니다.

- 게시에 SSL이 사용되지 않습니다.
- 게시에 디폴트 접미사 아래의 컨테이너가 사용됩니다.
- 디렉토리 서버를 인증하기 위해 OS/400에서 cn=Administrator ID 및 시스템 생성 암호를 사용합니다.
- 시스템이 시스템 정보만 게시합니다.

IBM SecureWay Directory 관리 툴

IBM SecureWay DMT(디렉토리 관리 툴)는 LDAP 디렉토리 목차를 관리할 수 있는 그래픽 사용자 인터페이스를 제공합니다. DMT로 수행할 수 있는 타스크는 다음과 같습니다.

- 디렉토리 스키마 검색
- 오브젝트 클래스 추가, 편집 및 삭제
- 속성 추가, 편집 및 삭제
- 디렉토리 트리 검색 및 탐색
- 항목 추가, 편집, 보기 및 삭제
- 항목 RDN 편집
- ACL 관리

DMT는 디렉토리 서비스와 같이 들어 있는 Windows LDAP 클라이언트의 일부분입니다. 클라이언트는 통합 파일 시스템 디렉토리에서 제공됩니다.

PC에 DMT가 들어있는 Windows LDAP 클라이언트를 설치하려면 다음 단계에 따르십시오.

1. iSeries Navigator에서 **파일 시스템**을 여십시오.
2. **파일 공유**를 여십시오.
3. **Qdirsrv**를 두 번 클릭하십시오.
4. **UserTools**를 두 번 클릭하십시오.
5. **Windows**를 두 번 클릭하십시오.
6. DMT 설치를 시작하려면 **setup.exe**를 두 번 클릭하십시오. 화면상의 지침에 따라 설치를 완료하십시오.

IBM SecureWay DMT(디렉토리 관리 툴)에 대한 문서는 `dparent.htm` 파일에 있습니다. 이 파일은 클라이언트를 설치할 때 PC의 IBM SecureWay Directory 폴더로 복사됩니다.

제 4 장 LDAP 디렉토리 서버 관리

LDAP 디렉토리 서버를 관리하려면 다음 권한 세트가 있어야 합니다.

- 서버 구성 또는 서버 구성 변경: *ALLOBJ(모든 오브젝트) 및 *IOSYSCFG(I/O 시스템 구성) 특수 권한
- 서버 시작 또는 중단: *JOBCTL(작업 제어) 권한 및 ENDTCP(TCP/IP 종료), STRTCP(TCP/IP 시작), STRTCPSVR(TCP/IP 서버 시작) 및 ENDTCPSVR(TCP/IP 서버 종료) 명령에 대한 오브젝트 권한
- 디렉토리 서버에 대한 감사 작동 설정: *AUDIT(감사) 특수 권한
- 서버 작업 기록부 보기: *SPLCTL(스풀 제어) 특수 권한

디렉토리 오브젝트(액세스 제어 리스트, 오브젝트 소유권 및 복제 포함)를 관리하려면 관리자 DN 또는 적절한 LDAP 권한이 있는 다른 DN으로 해당 디렉토리에 연결하십시오. 권한 통합을 사용 중인 경우 디렉토리 서비스 관리자 기능 ID에 대한 권한을 갖는 프로젝트 사용자도 관리자가 될 수 있습니다.

디렉토리 서버 관리에는 다음 타스크가 포함됩니다.

- 『LDAP 디렉토리 서버 시작』
- 20 페이지의 『LDAP 디렉토리 서버 중단』
- 20 페이지의 『디렉토리 서버의 상태 점검』
- 21 페이지의 『LDAP 디렉토리 서버의 작성 검사』
- 21 페이지의 『이벤트 통지 작동』
- 21 페이지의 『트랜잭션 설정 지정』
- 22 페이지의 『포트 또는 IP 주소 변경』
- 22 페이지의 『시스템 사이에서 LDAP 디렉토리 자료 이동』
- 30 페이지의 『디렉토리 참조에 대한 서버 지정』
- 31 페이지의 『LDAP 디렉토리 서버에 접미부 추가』
- 31 페이지의 『디렉토리 서버에서 접미사 제거』
- 32 페이지의 『디렉토리 서비스 정보 저장 및 복원』
- 32 페이지의 『디렉토리 자료의 소유권 및 액세스 관리』
- 34 페이지의 『LDAP 디렉토리에 대한 액세스 및 변경사항 추적』
- 35 페이지의 『디렉토리 서버에 대해 오브젝트 감사 작동』
- 35 페이지의 『LDAP 디렉토리 서버의 성능 조정』

LDAP 디렉토리 서버 시작

LDAP 디렉토리 서버를 시작하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭하고 **시작**을 선택하십시오.

디렉토리 서버는 서버의 속도와 사용 가능한 메모리의 양에 따라 시작하는 데 몇 분이 걸릴 수 있습니다. 디렉토리 서버를 처음 시작할 경우에는 서버가 신규 파일을 작성해야 하기 때문에 평상시보다 몇 분 더 소요될 수 있습니다. 마찬가지로, 디렉토리 서비스의 이전 버전에서 업그레이드한 후 처음으로 디렉토리 서버를 시작할 때, 서버가 파일을 마이그레이트해야 하기 때문에 평상시보다 더 오래 걸릴 수 있습니다. 서버가 이미 시작했는지 확인하기 위해 정기적으로 서버의 상태 체크를 수행할 수 있습니다.

주: STRTCPSVR *DIRSRV 명령을 입력하여 5250 세션에서도 디렉토리 서버를 시작할 수 있습니다.

뿐만 아니라, TCP/IP가 시작될 때 디렉토리 서버가 시작하도록 구성하는 경우, STRTCP 명령을 입력해서 서버를 시작할 수도 있습니다.

LDAP 디렉토리 서버 중단

디렉토리 서버를 중단하면 중단 시점에 서버를 사용하는 모든 어플리케이션에 영향을 줍니다. 여기에는 현재 EIM 조작에 디렉토리 서버를 사용 중인 EIM(Enterprise Identity Mapping) 어플리케이션이 포함됩니다. 모든 어플리케이션이 디렉토리 서버에서 단절되지만 서버에 재연결하려는 시도를 막을 수 없습니다.

LDAP 디렉토리 서버를 중단하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭하고 **중단**을 선택하십시오.

   디렉토리 서버는 시스템의 속도, 서버의 활동량 및 사용 가능한 메모리의 양에 따라 시작하는 데 몇 분이 걸릴 수 있습니다. 이미 중단되었는지 확인하기 위해 정기적으로 서버의 상태 체크를 수행할 수 있습니다.

주: ENDTCPSVR *DIRSRV, ENDTCPSVR *ALL 또는 ENDTCP 명령을 입력하여 5250 세션에서도 디렉토리 서버를 중단할 수 있습니다. ENDTCPSVR *ALL 및 ENDTCP도 시스템에서 실행되는 기타 TCP/IP 서버에 영향을 미칩니다. 또한 ENDTCP는 TCP/IP 자체를 종료합니다.

디렉토리 서버의 상태 점검

iSeries Navigator는 디렉토리 서버의 상태를 오른쪽 프레임의 **상태** 열에 표시합니다.

디렉토리 서버의 상태를 검사하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오. iSeries Navigator는 디렉토리 서버를 포함하여, 모든 TCP/IP 서버의 상태를 **상태** 열에 표시합니다. 서버의 상태를 갱신하려면 **보기** 메뉴를 클릭하고 **화면정리**를 선택하십시오.
4. 디렉토리 서버의 상태에 대한 자세한 내용을 보려면 **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **상태**를 선택하십시오. 그러면 과거 및 현재 활동 레벨 같은 기타 정보는 물론 활동 중인 연결 수도 표시됩니다.

   이 옵션으로 상태를 보면 추가 정보 제공 이외에도 시간을 절약할 수 있습니다. 다른 TCP/IP 서버의 상태를 점검하는 데 필요한 추가 시간을 소요하지 않고 디렉토리 서버의 상태를 화면정리할 수 있습니다.

LDAP 디렉토리 서버의 작성 검사

때로는 LDAP 디렉토리 서버의 특정 작업을 모니터하고자 합니다. 서버 작업을 체크하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**를 마우스 오른쪽 버튼으로 클릭하고 **서버 작업**을 선택하십시오.

이벤트 통지 작동

| 디렉토리 서비스는 이벤트 통지를 지원하며 이를 통해 디렉토리에 항목이 추가되는 등 지정한 이벤트가 발생할
| 때 통지를 받을 수 있도록 LDAP 서버에 클라이언트를 등록할 수 있습니다.

| 서버를 위한 이벤트 통지를 작동시키려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
5. **이벤트**를 클릭하십시오.
6. **이벤트 통지를 위해 클라이언트가 등록할 수 있음**을 선택하십시오.

또한 연결별로 허용되는 최대 등록 수와 서버가 허용하는 최대 등록 수를 지정할 수 있습니다.

이벤트 통지에 대한 추가 정보는 IBM SecureWay Directory Version 3.2: Client SDK Programming Reference

 매뉴얼에서 Appendix C: Event Notification을 참조하십시오.

트랜잭션 설정 지정

| 디렉토리 서비스는 LDAP 디렉토리 조작 그룹이 한 단위로 처리될 수 있도록 트랙잭션을 지원합니다. 자세한
| 내용은 42 페이지의 『트랜잭션』을 참조하십시오.

서버의 트랜잭션 설정을 구성하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
5. **트랜잭션**을 클릭하십시오.
6. 트랜잭션 설정을 지정하십시오.

주: 트랜잭션 설정이 LDAP 서버의 성능에 영향을 미칠 수 있으므로 다른 설정을 시도해 볼 수 있습니다.

포트 또는 IP 주소 변경

디렉토리 서비스에 의해 작동될 수 있는 LDAP 디렉토리 서버는 다음 디폴트 포트를 사용합니다.
- 보안되지 않은 연결의 경우 389.
- 보안 연결의 경우 636(보안 포트를 사용할 수 있는 어플리케이션으로서 디렉토리 서비스를 작동할 수 있도록 하기 위해 DCM(Digital Certificate Manager)을 사용한 경우).

주: 기본적으로 로컬 시스템에 정의된 모든 IP 주소가 서버에 바인드됩니다.

이 포트를 다른 어플리케이션에 이미 사용하고 있는 경우 다른 포트를 디렉토리 서비스에 지정하거나 어플리케이션이 특정 IP 주소에 대한 바인딩을 지원하면 두 대의 서버에 대해 서로 다른 IP 주소를 사용할 수 있습니다.

iSeries 디렉토리 서비스 LDAP 서버와 충돌하는 Domino LDAP 서버의 예는 동일한 iSeries에서 Host Domino LDAP 및 디렉토리 서비스를 참조하십시오.

LDAP 디렉토리 서버가 사용하는 포트를 변경하려면 다음과 같이 하십시오.
1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
5. **네트워크** 탭을 클릭하십시오.
6. 적절한 포트 번호를 입력한 후 **확인**을 클릭하십시오.

디렉토리 서버가 연결을 허용하는 IP 주소를 변경하려면 다음 단계를 수행하십시오.
1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
5. **네트워크** 탭을 클릭하십시오.
6. **IP 주소...** 단추를 클릭하십시오.
7. **선택한 IP 주소 사용**을 선택하고 연결을 허용할 때 사용할 서버의 IP 주소를 선택하십시오.

시스템 사이에서 LDAP 디렉토리 자료 이동

디렉토리 서비스 LDAP 서버는 다른 서버와 독립적으로 실행할 수 있습니다. 그러나 다른 서버에 대해 작업하도록 하는 것이 유용하다는 사실을 알 수 있습니다. 다음과 같은 것이 포함될 수 있습니다.
- 23 페이지의 『LDIF 파일 가져오기』
- 23 페이지의 『LDIF 파일 내보내기』
- 23 페이지의 『디렉토리 서버의 신규 복제 설정』
- 28 페이지의 『디렉토리 서버에 정보 개시』

LDIF 파일 가져오기

LDAP 자료 교환 형식(LDIF) 파일을 사용하여 정보를 서로 다른 LDAP 디렉토리 서버 사이에 전송할 수 있습니다. 이 프로시듀어를 시작하기 전에 LDIF 파일을 스트림 파일로 iSeries 서버에 전송하십시오.

LDIF 파일을 LDAP 디렉토리 서버에 가져오려면 다음과 같이 하십시오.

1. 디렉토리 서버가 시작되면 중단하십시오. 디렉토리 서버 중단에 대한 정보는 20 페이지의 『LDAP 디렉토리 서버 중단』을 참조하십시오.
2. iSeries Navigator에서 **네트워크**를 여십시오.
3. **서버**를 여십시오.
4. **TCP/IP**를 클릭하십시오.
5. **디렉토리**에서 마우스 오른쪽 버튼을 클릭하고 툴을 선택한 후 **파일 가져오기**를 선택하십시오.

주: ldapadd 유틸리티를 사용하여 LEIF 파일을 가져오기할 수도 있습니다.

LDIF 파일 내보내기

LDAP 자료 교환 형식(LDIF) 파일을 사용하면 정보를 서로 다른 LDAP 디렉토리 서버 사이에 전송할 수 있습니다. 39 페이지의 『LDAP 자료 교환 형식』을 참조하십시오. LDAP 디렉토리의 전체 또는 부분을 LDIF 파일에 내보낼 수 있습니다.

LDIF 파일을 디렉토리 서버에서 내보내려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭하고 툴을 선택한 후 **파일 내보내기**를 선택하십시오.

   주: LDIF 파일을 내보낼 위치를 지정하지 않으면, OS/400 사용자 프로파일에 지정된 기본 디렉토리에 파일이 저장됩니다. 디폴트 디렉토리를 변경하지 않은 경우, 디폴트 디렉토리는 루트 디렉토리입니다.

주:

1. 디렉토리 자료에 대한 권한이 없는 액세스를 방지하려면 LDIF 파일에 권한을 설정해야 합니다. 권한을 설정하려면 iSeries Navigator에 있는 해당 파일에서 마우스 오른쪽 버튼을 클릭한 후 **허가**를 선택하십시오.
2. ldapsearch 유틸리티로 LDIF 파일의 전체 또는 부분을 작성할 수도 있습니다. 58 페이지의 『ldapsearch 유틸리티』를 참조하십시오. -L 옵션을 사용하고 출력을 파일에 재지정하십시오.

디렉토리 서버의 신규 복제 설정

LDAP 디렉토리 서버의 복제본을 다른 iSeries 서버의 디렉토리 서버로 설정할 수 있습니다. 디렉토리 서비스는 표준 LDAP 버전 3 프로토콜을 사용하여 복제합니다.

주:

1. LDAP 버전 3과 LDAP 버전 2 서버 간에는 복제할 수 없습니다. 따라서 복제할 시스템에는 복제할 시스템과 똑같은 LDAP 버전이 사용되고 있어야 합니다. OS/400의 V4R3과 V4R4는 LDAP 버전 2를 지원하고, V4R5 이상의 릴리스는 LDAP 버전 3을 지원합니다.

2. 디렉토리 서비스 디렉토리를 다른 플랫폼의 IBM SecureWay V3.2 이상 서버로 복제할 수 있습니다. 이렇게 하기 위해서는 3.2 ACI 메카니즘을 사용할 수 있도록 OS/400 디렉토리 서버가 구성되어야 합니다. 복제할 때 서버에서 문제가 발생하면 복제가 중단됩니다. 이런 일이 발생하면 복제는 완료되지 않습니다.

디렉토리 서버의 신규 복제를 설정하려면 다음과 같이 하십시오.

1. 미리 설정하지 않은 경우, 마스터 서버와 복제 서버를 모두 구성하십시오.

   주: 스키마와 접미부가 두 서버에서 모두 일치하도록 하십시오.
2. 마스터 서버를 중단하십시오.
3. (선택형) 초기 복제를 위한 LDAP 자료를 설정하십시오. 마스터 서버에서 복제 서버로 전송하려는 초기 자료가 없는 경우에는 이 단계를 건너 뛸 수 있습니다.
4. (선택형) LDAP 자료를 마스터 서버로 이동하십시오. 다음 중 하나가 복제 서버에 적용되면 이 단계를 건너 뛰십시오.
   - 마스터 서버가 신규 LDAP 디렉토리 서버입니다.
   - 마스터 서버에 계속 유지보수할 자료가 들어 있지 않습니다.
5. 신규 복제 서버를 설정하십시오.
6. 신규 복제를 가지기 위해 마스터 서버를 설정하십시오.
7. 마스터 서버가 갱신사항을 허용하는지 확인하십시오.
   a. iSeries Navigator에서, 마스터 디렉토리 서버가 실행되는 시스템을 확장하십시오.
   b. **네트워크**를 여십시오.
   c. **서버**를 여십시오.
   d. **TCP/IP**를 클릭하십시오.
   e. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
   f. 이미 체크하지 않은 경우에는 **디렉토리 갱신사항 허용**을 체크하십시오.

주: 이 지침에서는 마스터 서버와 복제 서버가 모두 동일한 PC의 iSeries Navigator에서 관리하는 시스템에 있는 것으로 가정합니다. 별도의 PC에서 시스템을 관리하는 경우, 두 PC 사이를 이동하면서 이 타스크를 수행할 수 있습니다. 마스터 서버나 복제 서버가 OS/400 이외의 IBM 오퍼레이팅 시스템에서 실행되는 경우, 해당 플랫폼의 문서를 참조하여 서버를 설정하십시오.

초기 복제용 LDAP 자료 설정

신규 복제 서버에 추가할 마스터 LDAP 디렉토리 서버에 기존 자료를 사용할 수도 있습니다. 이를 위해서 맨 먼저 디렉토리를 LDIF 파일에 내보내야 합니다. LDIF 파일을 내보내는 중에는 마스터 서버가 갱신되지 않도록 예방해야 합니다. 이 예방 조치는 다음 방법 중 하나를 사용하여 수행할 수 있습니다.

- LDAP 디렉토리 서버를 중단하십시오. 디렉토리에 있는 자료의 용량에 따라 연장 기간 동안 서버가 중단된 상태를 유지해야 하는 경우도 있습니다.
- 갱신이 허용되지 않도록 서버 등록 정보를 변경하십시오. 서버 등록 정보를 변경함으로써 서버는 LDIF 파일을 내보내는 동안 계속해서 탐색 요구에 응답할 수 있습니다. 이 옵션을 취하려면 다음과 같이 하십시오.
  1. iSeries Navigator에서, 마스터 디렉토리 서버가 실행되는 시스템을 확장하십시오.
  2. **네트워크**를 여십시오.
  3. **서버**를 여십시오.

4. **TCP/IP**를 클릭하십시오.
5. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
6. **디렉토리 갱신 허용**을 체크한 경우에는 체크 표시를 제거하십시오. 그러면 복제가 완전히 설정될 때까지 디렉토리에 대한 갱신이 금지됩니다.
7. **확인**을 클릭하십시오.
8. 중단한 다음 LDAP 디렉토리 서버를 재시작하십시오.

디렉토리 갱신이 허용되지 않도록 서버를 중단하거나 서버 등록 정보를 변경한 후에 다음 타스크를 수행하십시오.

1. 디렉토리를 LDIF 파일에 내보내십시오.
2. LDIF 파일을 복제 서버가 실행되는 시스템으로 전송하십시오.

LDIF 파일이 복제 서버가 실행되는 시스템으로 전송되면 복제 서버에 자료를 가져올 필요가 없습니다.

1. iSeries Navigator에서 복제 디렉토리 서버가 실행되는 시스템을 확장하십시오.
2. 복제 서버가 이미 중단되지 않은 경우에는 지금 중단하십시오. 상태가 **중단됨**일 때까지 서버의 상태를 화면정리하십시오.
3. **네트워크**를 여십시오.
4. **서버**를 여십시오.
5. **TCP/IP**를 클릭하십시오.
6. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
7. **디렉토리 갱신 허용**에 체크 표시가 없는 경우에는 체크하십시오. 그러면 자료를 가져올 수 있습니다.
8. **확인**을 클릭하십시오.
9. 2단계에서 전송한 LDIF 파일을 가져오십시오.
10. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
11. **디렉토리 갱신 허용**에서 체크 표시를 제거하십시오.

마스터 서버로 LDAP 자료 이동

일단 LDAP 디렉토리 서버를 복제 서버로 만들면 자료를 더 이상 갱신할 수 없습니다. 복제 LDAP 디렉토리 서버가 되도록 구성하는 서버에 기존 자료가 있으면 자료를 계속 유지보수할 수 있도록 마스터 서버로 이동하려고 할 것입니다. 이를 수행하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 복제 디렉토리 서버가 실행되는 시스템을 확장하십시오.
2. **네트워크**를 여십시오.
3. **서버**를 여십시오.
4. **TCP/IP**를 클릭하십시오.
5. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
6. **디렉토리 갱신 허용**을 체크한 경우에는 체크 표시를 제거하십시오. 그러면 복제가 완전히 설정될 때까지 디렉토리에 대한 갱신이 금지됩니다.
7. **확인**을 클릭하십시오.
8. LDAP 디렉토리 서버를 중단하십시오.
9. 디렉토리를 LDIF 파일에 내보내십시오.
10. LDIF 파일을 마스터 서버가 실행되는 시스템으로 전송하십시오.

LDIF 파일이 마스터 서버가 실행되는 시스템으로 전송된 후, 자료를 마스터 서버로 가져오지 않아도 됩니다.

1. iSeries Navigator에서, 마스터 디렉토리 서버가 실행되는 시스템을 확장하십시오.
2. 마스터 디렉토리 서버가 이미 중단되지 않은 경우에는 지금 중단하십시오. 상태가 **중단됨**일 때까지 서버의 상태를 화면정리하십시오.
3. **네트워크**를 여십시오.
4. **서버**를 여십시오.
5. **TCP/IP**를 클릭하십시오.
6. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
7. **디렉토리 갱신 허용**에 체크 표시가 없는 경우에는 체크하십시오. 그러면 자료를 가져올 수 있습니다.
8. **확인**을 클릭하십시오.
9. 이전 프로시듀어의 25 페이지의 10단계에서 전송했던 LDIF 파일을 가져오기하십시오.
10. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
11. **디렉토리 갱신 허용**에서 체크 표시를 제거하십시오.

신규 복제 설정

신규 복제 서버를 설정하려면 다음과 같이 하십시오.

주: 이 프로시듀어를 수행하기 전에 복제 서버가 구성되고 중단되어야 합니다.

1. iSeries Navigator에서 복제 디렉토리 서버가 실행되는 시스템을 확장하십시오.
2. **네트워크**를 여십시오.
3. **서버**를 여십시오.
4. **TCP/IP**를 클릭하십시오.
5. 서버가 이미 중단되지 않은 경우에는 지금 서버를 중단하십시오. 상태가 **중단됨**일 때까지 서버의 상태를 화면정리하십시오.
6. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
7. **복제** 탭을 클릭하십시오.
8. **복제 서버로 사용**을 선택하십시오.
9. **마스터 서버가 갱신에 사용한 이름** 필드에서, 갱신 수행시 복제 서버로 로그온할 때 사용할 마스터 서버의 이름을 선택하십시오. 이 이름은 식별명(DN) 또는 Kerberos 사용자가 될 수 있습니다.

   DN을 선택하는 경우

   - **마스터 서버가 갱신에 사용한 이름** 필드 다음의 **암호** 버튼을 클릭하십시오. 갱신을 수행하기 위해 복제 서버에 로그온할 때 사용할 마스터 서버의 암호를 입력하십시오.

     주: 이 암호와 9단계에서 입력한 이름을 기록해야 합니다. 복제를 위한 마스터 서버를 설정할 때 이 정보가 필요합니다.

   Kerberos 사용자 추가를 선택하는 경우

   - 마스터 서버의 Kerberos 이름(`LDAP/`*`hostname`* 형식, 여기에서 *hostname*은 마스터 서버의 정식 이름) 및 디폴트 영역(예: ACME.COM)을 입력하라는 메세지가 표시됩니다.

     주: Kerberos를 사용하려면 마스터 서버와 복제 서버에서 모두 Kerberos를 작동할 수 있어야 합니다.

10. **마스터 서버 URL** 필드에서 마스터 서버 이름을 URL 형식으로 입력하십시오. 마스터 서버가 디폴트 이외의 포트를 사용하는 경우, 이 포트 번호를 URL의 일부로 입력하십시오.
11. **데이터베이스/접미부** 탭을 클릭하십시오. 복제하려는 접미부가 리스트에 없는 경우에는 해당 접미부를 추가하십시오.
12. (선택형) 복제시 SSL(보안 소켓층)을 사용하려는 경우, DCM(Digital Certificate Manager)을 사용하여 서버에 SSL을 작동할 수 있도록 하십시오. **네트워크** 탭에서 DCM(Digital Certificate Manager)을 시작할 수 있습니다. 디렉토리 서버에서 SSL 작동가능에 관한 자세한 내용은 16 페이지의 『LDAP 디렉토리 서버에서 SSL 작동가능』을 참조하십시오.
13. **확인**을 클릭하십시오.

신규 복제를 가지기 위해 마스터 복제 설정

신규 복제를 가지기 위해 마스터 서버를 설정하려면 다음과 같이 하십시오.

주: 이 프로시듀어를 수행하기 전에 마스터 서버를 구성하고 시작했어야 합니다.

1. iSeries Navigator에서, 마스터 디렉토리 서버가 실행되는 시스템을 확장하십시오.
2. **네트워크**를 여십시오.
3. **서버**를 여십시오.
4. **TCP/IP**를 클릭하십시오.
5. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
6. 이미 체크하지 않은 경우에는 **디렉토리 갱신사항 허용**을 체크하십시오.
7. **확인**을 클릭하십시오.
8. LDAP 디렉토리 서버를 중단한 후 다시 시작하십시오. 상태가 **시작됨**일 때까지 서버의 상태를 화면정리하십시오.
9. 다시 **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
10. **복제** 탭을 클릭하십시오. iSeries Navigator에서 연결 정보를 입력하라고 프롬트할 수 있습니다. 이 정보를 입력한 후 **확인**을 클릭하십시오.
11. **추가**를 클릭하십시오.
12. **서버** 필드에 복제 서버의 이름을 URL 형식으로 입력하십시오.
13. 인증 메소드를 선택하십시오.

    식별명(DN)과 암호를 사용하려면 다음을 수행하십시오.

    a. **DN 및 암호 사용**을 선택하십시오.

    b. **연결명** 필드에 복제 서버 설정시 26 페이지의 9단계에 지정했던 이름을 입력하십시오.

    c. **암호**를 누르고, 복제 서버 설정시 26 페이지의 9단계에 지정했던 암호를 입력하십시오.

    Kerberos를 사용하려면 다음을 수행하십시오.

    - **마스터 서버의 Kerberos 계정 사용**을 선택하십시오. 마스터 서버가 해당 Kerberos 프린시펄명을 인증에 사용합니다.

      주: Kerberos를 사용하려면 마스터 서버와 복제 서버에서 모두 Kerberos를 작동할 수 있어야 합니다.

14. 복제시 SSL(보안 소켓 층)을 사용하려면 DCM(Digital Certificate Manager)을 사용하여 서버에 SSL을 작동할 수 있게 하십시오. **네트워크** 탭에서 DCM(Digital Certificate Manager)을 시작할 수 있습니다. 디렉토리 서버에서 SSL 작동가능에 대한 자세한 내용은 16 페이지의 『LDAP 디렉토리 서버에서 SSL 작동가능』을 참조하십시오.
15. 복제 서버가 디폴트 포트를 사용하지 않는 경우에는 **포트** 필드에 포트 번호를 지정하십시오.
16. 마스터 서버의 항목을 변경할 때마다 복제 서버를 갱신하지 않으려면 **시간**을 선택하십시오. 그런 다음, 마스터 서버가 복제를 갱신하기 원하는 빈도를 지정하십시오.
17. **확인**을 클릭하십시오.
18. **데이터베이스/접미부** 탭을 클릭하십시오. 복제하려는 접미부가 리스트에 없는 경우에는 해당 접미부를 추가하십시오.
19. 각 복제 서버에서 디렉토리 갱신을 작동할 수 있게 하십시오.
    a. iSeries Navigator에서 복제 디렉토리 서버가 실행되는 시스템을 확장하십시오.
    b. **네트워크**를 여십시오.
    c. **서버**를 여십시오.
    d. **TCP/IP**를 클릭하십시오.
    e. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
    f. **디렉토리 갱신 허용**이 체크되지 않은 경우에는 체크하십시오.
    g. **확인**을 클릭하십시오.
20. 각 복제 서버가 이미 시작되지 않은 경우에는 지금 시작하십시오.

주: 한 서버가 마스터 서버와 복제 서버 모두로 될 수는 없습니다.

디렉토리 서버에 정보 개시

일부 정보를 동일한 시스템이나 다른 시스템의 LDAP 디렉토리 서버에 게시하도록 시스템을 구성할 수 있습니다. iSeries Navigator를 사용하여 OS/400에서 이 정보를 변경할 때 OS/400는 이 정보를 LDAP 디렉토리 서버에 자동으로 게시합니다. 게시할 수 있는 정보는 시스템(시스템 및 프린터), 인쇄 공유 및 사용자 정보 및 TCP/IP 서비스 품질 정책입니다. 서비스 품질에 대한 자세한 정보는 LDAP 구성 및 QoS를 참조하십시오.

자료를 게시할 상위 DN이 없으면 디렉토리 서비스에서 자동으로 작성합니다. LDAP 디렉토리에 정보를 게시하는 다른 OS/400 어플리케이션을 설치할 수도 있습니다. 뿐만 아니라, LDAP 디렉토리에 다른 유형의 정보 Publishing을 수행하기 위해 사용자 프로그램에서 어플리케이션 프로그램 인터페이스(API)를 호출할 수 있습니다.

주:

1. 정보 유형 사용자를 LDAP 디렉토리 서버에 게시하기 위해서 OS/400를 구성하는 경우에는 시스템 분배 디렉토리의 항목이 자동으로 LDAP 서버로 내보내집니다. 내보내기를 수행하는 데 QGLDSSDD API(어플리케이션 프로그램 인터페이스)가 사용됩니다. LDAP 디렉토리가 또한 시스템 분배 디렉토리에서 수행된 변경과 동기화되도록 유지합니다. QGLDSSDD API에 대한 정보는 iSeries Information Center의 프로그래밍 아래에 있는 OS/400 디렉토리 서비스 주제를 참조하십시오. 사용할 수 있는 정보는 다음과 같습니다.
   - 이 API를 수동으로 호출하는 방법.

- 특정 사용자가 LDAP 서버에 내보내지 않도록 막는 방법.
- 시스템 분배 디렉토리 필드를 내보내는 방법.

2. 정보 유형 시스템을 LDAP 디렉토리 서버에 게시하도록 OS/400를 구성하고, 게시할 프린터를 하나 이상 선택하는 경우, 시스템은 LDAP 디렉토리를 시스템의 해당 프린터에 대해 변경한 사항과 동기화된 상태로 유지합니다. 게시할 수 있는 프린터 정보는 프린터의 위치, 1분당 페이지 속도, 양방향 전송과 색상의 지원 여부, 유형과 모델 및 이에 대한 설명입니다. 이러한 정보는 게시할 시스템에 대한 장치 설명에 근거합니다. 네트워크 환경에서 사용자는 이 정보를 사용해서 프린터를 선택할 수 있습니다.
3. 또한 IBM 스키마를 사용하도록 해당 서버를 구성하는 경우, OS/400 정보를 OS/400에 없는 LDAP 디렉토리 서버에 게시할 수도 있습니다.

OS/400 정보를 LDAP 디렉토리 서버에 게시하도록 시스템을 구성하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 시스템을 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
2. **디렉토리 서비스** 탭을 클릭하십시오.
3. Publishing할 정보의 유형을 클릭하십시오.

   추가 정보:

   둘 이상의 정보 유형을 동일한 위치에 Publishing할 경우에는 한 번에 구성할 복수 정보 유형을 선택하여 시간을 절약할 수 있습니다. 그러면 Operations Navigator는 한 정보 유형을 구성할 때 입력하는 값을 후속 정보 유형을 구성할 때의 디폴트 값으로 사용합니다.
4. **세부사항**을 클릭하십시오.
5. **시스템 정보 게시** 선택란을 클릭하십시오.
6. 해당 인증 정보 뿐만 아니라 서버에서 사용할 **인증 메소드**도 지정하십시오.
7. **디렉토리 서버(활동)** 필드 옆에 있는 **편집** 단추를 클릭하십시오. 표시된 대화상자에서 OS/400 정보를 게시할 LDAP 디렉토리 서버의 이름을 입력한 다음, **확인**을 클릭하십시오.
8. **DN 아래** 필드에 디렉토리 서버에서 추가할 정보의 상위 식별명(DN)을 입력하십시오.
9. 구성에 해당되는 **서버 연결** 프레임의 필드를 채우십시오.

   주: SSL이나 Kerberos를 사용해서 OS/400 정보를 디렉토리 서버에 게시하려면 먼저 해당 프로토콜을 사용하도록 디렉토리 서버를 구성해야 합니다. SSL이나 Kerberos에 대한 자세한 정보는 44 페이지의 『LDAP 디렉토리 서버에서 Kerberos 인증 사용』을 참조하십시오.
10. 디렉토리 서버가 디폴트 포트를 사용하지 않은 경우에는 **포트** 필드에 정확한 포트 번호를 입력하십시오.
11. **확인**을 클릭하여 상위 DN이 서버에 있는지, 연결 정보가 올바른지 확인하십시오. 디렉토리 경로가 없으면 경로를 작성하라는 대화상자가 프롬트됩니다.

    주: 상위 DN이 없고, 작성하지 않은 경우에는 Publishing이 실패합니다.
12. **확인**을 클릭하십시오.

주: OS/400 정보를 다른 플랫폼에 있는 LDAP 디렉토리 서버에 게시할 수도 있습니다. 사용자와 시스템 정보는 디렉토리 서비스 스키마와 호환되는 스키마를 사용하는 디렉토리 서버에 게시해야 합니다. iSeries 디렉토리 서비스를 포함하는 IBM SecureWay Directory 스키마 정의는 디렉토리 서비스 웹 페이지에서 찾을 수 있습니다.

인쇄 공유 사항은 Microsofts의 활동 디렉토리 스키마를 지원하는 디렉토리 서버에 게시해야 합니다. 인쇄 공유 사항을 활동 디렉토리에 게시하면 사용자는 Windows 2000의 프린터 추가 마법사를 사용하여 iSeries 프린터를 해당 Windows 2000 데스크탑에서 직접 구성할 수 있습니다. 프린터 추가 마법사에 서 프린터를 추가하려면 Windows 2000 활동 디렉토리에서 찾으려는 프린터를 지정하십시오.

OS/400 정보를 디렉토리 서버에 게시하기 위한 API server

디렉토리 서비스는 게시에 대한 내장 지원 사용자 및 시스템 정보를 제공합니다. 이러한 항목은 시스템 **등록 정보** 대화상자의 **디렉토리 서비스** 페이지에 나열되어 있습니다. LDAP 서버 구성과 API 게시를 사용하여 다른 유형의 정보를 게시하기 위해 기록하는 OS/400 프로그램을 작동시킬 수 있습니다. 이러한 유형의 정보는 **디렉토리 서비스** 페이지에도 나타납니다. 이러한 정보는 사용자와 시스템과 마찬가지로 초기에는 작동 불가능하며, 동일한 프로시듀어를 사용하여 구성됩니다. 자료를 LDAP 디렉토리에 추가하는 프로그램을 Publishing Agent라고 합니다. **디렉토리 서비스** 페이지에 Publishing 처리 정보 유형이 나타날 때 이것을 에이전트명이라고 합니다.

다음 API를 사용하여 Publishing을 사용자 프로그램에 통합할 수 있습니다.

QgldChgDirSvrA

어플리케이션은 CSVR0500 형식을 사용하여 작동 불가능한 항목으로 표시되는 에이전트명을 초기에 추가합니다. 어플리케이션 사용자에 대한 지침은 사용자가 게시 에이전트를 구성하기 위해 iSeries Navigator를 사용하여 디렉토리 서비스 등록 정보 페이지로 이동하도록 지시해야 합니다. 에이전트명의 예로 **디렉토리 서비스** 페이지에서 자동으로 사용할 수 있는 시스템과 사용자 에이전트명이 있습니다.

QgldLstDirSvrA

API의 LSVR0500 형식을 사용하여 현재 시스템에서 사용할 수 있는 에이전트를 나열합니다.

QgldPubDirObj

정보의 실제 Publishing을 수행하려면 이 API를 사용하십시오.

이러한 API에 대한 자세한 정보는 iSeries Information Center의 프로그래밍에서 LDAP(Lightweight Directory Access Protocol)를 참조하십시오.

디렉토리 참조에 대한 서버 지정

디렉토리 서버에 대해 리퍼럴 서버를 할당하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭하고 **특성**을 선택하십시오.
5. **추가**를 클릭하십시오.
6. 프롬트에서 URL 형식으로 리퍼럴 서버 이름을 지정하십시오. 다음은 기준에 맞는 LDAP URL의 예입니다.
   - ldap://test.server.com

- ldap://test.server.com:400
- ldap://9.9.99.255

주: 리퍼럴 서버가 디폴트 포트를 사용하지 않으면, 포트 400®이 지정되어 있는 위의 두번째 예와 같이 URL의 일부로 올바른 포트 번호를 지정하십시오.

7. **확인**을 클릭하십시오.

LDAP 디렉토리 서버에 접미부 추가

접미부를 LDAP 디렉토리 서버에 추가하면 서버가 디렉토리 트리의 해당 부분을 관리할 수 있습니다.

주: 서버의 다른 접미부 아래에 이미 있는 접미부를 추가하면 안됩니다. 예를 들어 `o=ibm, c=us`가 서버의 접미부인 경우 `ou=rochester, o=ibm, c=us`를 추가하면 안됩니다.

접미부를 디렉토리 서버에 추가하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
5. **데이터베이스/접미부** 탭을 클릭하십시오.
6. **신규 접미부** 필드에 신규 접미부의 이름을 입력하십시오.
7. **추가**를 클릭하십시오.
8. **확인**을 클릭하십시오.

주: 접미사를 추가하면 서버를 디렉토리 섹션에 가리키지만 모든 오브젝트를 작성하지 않습니다. 새 접미사에 해당되는 오브젝트가 없으면 다른 오브젝트와 마찬가지로 오브젝트를 작성해야 합니다.

디렉토리 서버에서 접미사 제거

LDAP 디렉토리 서버에서 접미부를 제거하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
5. **데이터베이스/접미부** 탭을 클릭하십시오.
6. 선택하기 위하여 제거하려는 접미부를 클릭하십시오.
7. **제거**를 클릭하십시오.

주: 접미부 아래의 디렉토리 오브젝트를 삭제하지 않고도 접미부를 삭제하기 위해 선택할 수 있습니다. 이는 자료를 디렉토리 서버에서 액세스할 수 없게 만듭니다. 그러나 접미부를 추가하여 자료에 대한 액세스를 회복할 수 있습니다.

디렉토리 서비스 정보 저장 및 복원

디렉토리 서비스는 다음 위치에 정보를 저장합니다.

- 디렉토리 서버 내용을 포함하는 데이터베이스 라이브러리(디폴트는 QUSRDIRDB).
- 게시 정보를 저장하는데 사용되는 QDIRSRV2 라이브러리.
- QGLD로 시작하는 오브젝트에 여러 항목을 저장하는 QUSRSYS 라이브러리(QUSRSYS/QGLD*를 지정하여 항목 저장).
- 디렉토리 변경사항을 기록하기 위해 디렉토리 서버를 구성하는 경우, 변경 기록부에서 사용하는 QUSRDIRCL 데이터베이스 라이브러리.

디렉토리의 내용이 정기적으로 변경되는 경우, 데이터베이스 라이브러리와 오브젝트를 디렉토리에 정기적으로 저장해야 합니다. 구성 데이터 역시 다음의 디렉토리에 저장됩니다.

```
/QIBM/UserData/OS400/Dirsrv/
```

구성을 변경하거나 PTF를 적용할 때마다 파일을 해당 디렉토리에 저장해야 합니다.

OS/400 자료의 저장 및 복원에 대한 정보는 백업 및 회복, SC41-5304 를 참조하십시오.

디렉토리 자료의 소유권 및 액세스 관리

디렉토리 자료의 소유권 및 액세스 관리는 다음 타스크를 포함합니다.

- 『디렉토리 오브젝트의 소유권 등록 정보에 대한 작업』
- 『액세스 제어 리스트(ACL)에 대한 작업』
- 33 페이지의 『ACL 그룹에 대한 작업』

디렉토리 오브젝트의 소유권 등록 정보에 대한 작업

디렉토리 오브젝트의 소유권 특성을 설정하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭하고 **권한**을 선택하십시오.

   디렉토리 서버에 이미 연결되지 않은 경우에는 **디렉토리 서버에 연결** 대화상자가 나타납니다. 서버 관리자 또는 소유권 특성에 대하여 작업할 오브젝트의 소유자로 연결하십시오.
5. 디렉토리 트리에서 소유권 특성에 대하여 작업할 오브젝트를 선택한 후 **확인**을 클릭하십시오.

액세스 제어 리스트(ACL)에 대한 작업

액세스 제어 리스트(ACL)에 대한 작업에는 디렉토리 오브젝트에 명시 및 내재 ACL 지정, ACL에 사용자 추가, ACL에서 사용자 제거 및 디렉토리 오브젝트 보기 등이 포함됩니다. V5R1부터 ACL을 숙지하지 않은 상태에서 ACL을 사용한 경우, 디렉토리 서비스에서 새로운 ACL 모델을 지원한다는 점을 주의하십시오.

ACL에 대하여 작업하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭하고 **권한**을 선택하십시오.

   디렉토리 서버에 이미 연결되지 않은 경우에는 **디렉토리 서버에 연결** 대화상자가 나타납니다. 서버 관리자 또는 ACL에 대해 작업할 오브젝트의 소유자로 연결하십시오.
5. 디렉토리 트리에서 ACL에 대해 작업할 오브젝트를 선택한 후 **확인**을 클릭하십시오.
6. **ACL** 탭을 클릭하십시오.

ACL 그룹에 대한 작업

ACL 그룹에 대해 작업하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 선택하십시오.
2. **서버**를 선택하십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭하고 **ACL 그룹**을 선택하십시오.

권한이 있는 사용자의 관리 액세스에 대한 작업

V5R2부터 디렉토리 서비스 관리자 (QIBM_DIRSRV_ADMIN) 함수 ID에 대한 액세스 권한이 제공된 사용자 프로파일에 관리자 액세스를 부여할 수 있습니다.

예를 들어 사용자 프로파일 JOHNSMITH에게 디렉토리 서비스 관리자 기능 ID에 대한 액세스를 부여하고 디렉토리 등록 정보 대화상자에서 권한이 있는 사용자에 대한 관리자 액세스 부여 옵션을 선택하면 JOHNSMITH 프로파일이 LDAP 관리자 권한을 갖습니다. 다음 DN, os400-profile=JOHNSMTH, cn=accounts,os400-sys=systemA.acme.com을 사용하여 디렉토리 서버에 바인드하는 데 이 프로파일을 사용하면 사용자가 관리자 권한을 갖습니다. 이 예에서 시스템 오브젝트 접미부는 os400-sys=systemA.acme.com입니다. 프로젝트 사용자에 대한 자세한 정보는 46 페이지의 『오퍼레이팅 시스템 프로젝트 백엔드』를 참조하십시오.

이 옵션을 선택하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
4. **관리자 정보**의 **일반** 탭에서 **권한이 있는 사용자에게 관리자 액세스 부여** 옵션을 선택하십시오.

사용자 프로파일에서 디렉토리 서비스 관리자 권한 기능 ID를 설정하려면 다음 단계를 수행하십시오.

1. iSeries Navigator에서 시스템명을 마우스 오른쪽 버튼으로 클릭하고 **어플리케이션 관리**를 선택하십시오.
2. **호스트 어플리케이션** 탭을 클릭하십시오.
3. **OS/400®**을 확장하십시오.
4. **디렉토리 서비스 관리자**를 클릭하여 이 옵션을 강조표시하십시오.

5. **사용자 정의** 단추를 클릭하십시오.
6. **사용자, 그룹** 또는 **그룹에 없는 사용자** 중 적절한 항목을 확장하십시오.
7. **허용된 액세스** 리스트에 추가할 사용자 또는 그룹을 선택하십시오.
8. **추가** 단추를 클릭하십시오.
9. 변경사항을 저장하려면 **확인**을 클릭하십시오.
10. **어플리케이션 관리** 대화상자에서 **확인**을 클릭하십시오.

LDAP 디렉토리에 대한 액세스 및 변경사항 추적

LDAP 디렉토리에 대한 액세스와 변경사항을 추적할 수 있습니다. LDAP 디렉토리의 변경 기록부를 사용하여 디렉토리의 변경사항을 추적할 수 있습니다. 변경 기록부는 특수 접미사 cn=changelog 아래에 있습니다. 그것은 QUSRDIRCL 라이브러리에 저장됩니다.

변경 기록부를 사용하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
5. **데이터베이스/접미부** 탭을 클릭하십시오.
6. **디렉토리 변경사항 기록**을 선택하십시오.
7. (선택적) **최대 항목 수**에 보유하려는 변경 기록부의 최대 항목 수를 지정하십시오.

   주: 이 매개변수는 선택적이긴 하지만, 최대 항목 수를 지정하는 것에 대해 고려하는 것이 좋습니다. 항목의 최대 수를 지정하지 않으면 변경 기록부가 모든 항목을 보유하게 되어 매우 커질 수 있습니다.

changeLogEntry 오브젝트 클래스는 디렉토리 서버에 적용된 변경사항을 표시하는 데 사용됩니다. 변경 설정은 changeNumber에 의해 정의된 changelog 컨테이너 내에 있는 모든 항목의 설정 순서에 따라 수행됩니다. 변경 기록부 정보는 읽기 전용입니다.

cn=changelog 접미부에 대한 액세스 제어 목록에 들어 있는 모든 사용자는 변경 기록부의 항목을 탐색할 수 있습니다. 변경 기록부의 접미사, cn=changelog에 대한 탐색만 실행해야 합니다. 변경 기록부 접미부에 대한 추가, 변경 또는 삭제는 비록 추가, 변경, 삭제 권한이 있더라도 금지됩니다. 이 금지 규정을 어기면 예측하지 못한 결과를 초래하게 됩니다.

예:

다음은 Idapsearch 명령행 유틸리티를 사용하여 서버에 기록된 모든 변경 기록부 항목을 검색하는 예입니다.

```
ldapsearch -h ldaphost -D cn=admininistrator -w password -b cn=changelog  (changetype=*)
```

디렉토리 서버에 대해 오브젝트 감사 작동

디렉토리 서비스는 OS/400 보안 감사를 지원합니다. QAUDCTL 시스템 값에 *OBJAUD가 지정되어 있으면 iSeries Navigator를 통해 오브젝트 감사를 작동시킬 수 있습니다.

디렉토리 서비스에 대해 오브젝트 감사를 작동시키려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
5. **감사** 탭을 클릭하십시오.
6. 서버에 사용할 감사 설정을 선택하십시오.

감사 설정의 변경사항은 **확인**을 누르는 즉시 적용됩니다. 따라서 LDAP 디렉토리 서버를 다시 시작할 필요가 없습니다. 자세한 내용은 43 페이지의 『디렉토리 서비스 보안』을 참조하십시오.

LDAP 디렉토리 서버의 성능 조정

다음 중 하나를 변경하여 LDAP 디렉토리 서버의 성능을 조정할 수 있습니다.

- 탐색 크기
- 탐색시 허용되는 최대 시간
- 서버 트랜잭션 설정
- 데이터베이스 연결 및 서버 스레드 수

디렉토리 서버의 성능 값을 조정하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
5. **성능** 탭을 클릭하십시오.

서버가 사용하는 데이터베이스 연결 및 서버 스레드 번호를 변경하여 디렉토리 서버의 성능을 조정할 수 있습니다. 이 값을 변경하려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭한 후 **특성**을 선택하십시오.
5. **데이터베이스/접미부** 탭을 클릭하십시오.

제 5 장 디렉토리 서비스 개념 및 참조 정보

다음의 개념 및 참조 정보는 디렉토리 서비스 LDAP 서버에 대해 학습하고 서버를 실행하는 데 도움이 됩니다.

- 『LDAP ACL(액세스 제어 리스트)』
- 39 페이지의 『LDAP 자료 교환 형식』
- 41 페이지의 『자국어 지원(NLS) 고려사항』
- 42 페이지의 『LDAP 디렉토리 오브젝트의 소유권』
- 42 페이지의 『LDAP 디렉토리 리퍼럴』
- 42 페이지의 『트랜잭션』
- 43 페이지의 『복제 LDAP 디렉토리 서버』
- 43 페이지의 『디렉토리 서비스 보안』
- 46 페이지의 『오퍼레이팅 시스템 프로젝트 백엔드』
- 51 페이지의 『디렉토리 서비스 및 OS/400 저널링 지원』

LDAP 기본 및 LDAP 서버 계획에 관한 정보를 위해 7 페이지의 제 3 장 『디렉토리 서비스 시작하기』도 참조하십시오.

LDAP ACL(액세스 제어 리스트)

보통은 LDAP 디렉토리 서버의 자료에 대해 액세스를 제한하려 하지 않을 것입니다. 예를 들어 회사 인트라넷의 LDAP 서버에 회사 직원들의 전화 번호부가 들어 있을 수 있습니다. 이 경우 모든 직원들이 이 전화 번호부에 있는 자료를 볼 수 있도록 할 것입니다.

그러나 회사의 사장이 일부 직원들만 자신의 전화 번호에 액세스하는 것을 원한다고 가정해 보십시오. 이와 같은 경우에 **액세스 제어 리스트(ACL)**를 작성할 수 있습니다. 즉, ACL을 통해 사장이 원하는 직원들만 사장의 전화 번호에 액세스할 수 있도록 제한할 수 있습니다.

ACL을 사용하여 디렉토리 오브젝트의 추가 및 삭제 권한을 가진 사용자를 제어할 수 있습니다. 또한 사용자들이 디렉토리 속성을 읽고, 쓰고, 탐색하고 비교할 수 있도록 할 것인지 지정할 수 있습니다. ACL은 계승시킬 수도 있고 명시적으로 설정할 수도 있습니다. 즉, 다음 방법 중 하나로 ACL을 사용할 수 있습니다.

- 특정 오브젝트에 대해 ACL을 명시적으로 설정합니다.
- 오브젝트가 LDAP 디렉토리 계층에서 상위 오브젝트로부터 ACL을 계승하도록 지정합니다.

위의 예에서 사장은 일부 직원만 자신의 전화 번호에 액세스하기를 원합니다. 즉, 관리자만 액세스하는 것을 원합니다. 이 경우에는 **ACL 그룹**을 사용하여 관리자에게만 권한을 간단히 부여할 수 있습니다. 또한 ACL 그룹을 사용하면 개인이 아니라 특정 사용자 그룹에 액세스 권한을 부여할 수 있습니다. 이 기능은 하나 이상의 오브젝트에 대한 액세스를 동일한 그룹에 부여할 때 특히 유용 합니다. 예를 들어 사장의 전화 번호에 액세스할 수 있는 같은 관리자 그룹이 나중에 급여 항목에 대한 액세스를 필요로 하면 ACL 그룹을 재사용할 수 있습니다.

ACL 모델

디렉토리 서비스의 모든 버전은 액세스 클래스 레벨 권한 모델을 지원합니다. 이 모델에서는 각 LDAP 속성 유형이 Normal, Sensitive 또는 Critical입니다. 속성 스키마 파일이 이러한 분류를 제어합니다. 오브젝트의 ACL에 사용자를 추가할 때 사용자가 읽고, 쓰고, 탐색하고, 비교할 수 있는 분류를 지정합니다. 대부분의 스키마에서 전화 번호는 Normal 속성으로 분류됩니다. 따라서 위의 예에서 관리자들이 사장의 전화 번호에 액세스할 수 있게 하려면 사장의 디렉토리 오브젝트에서 Normal 속성에 대해 읽기 액세스를 허용해야 합니다. Sensitive 및 Critical 정보의 경우에는 관리자들이 여전히 액세스할 수 없습니다. 디렉토리 서비스의 모든 버전이 액세스 클래스 레벨 권한 설정을 지원합니다.

디렉토리 서비스는 속성 레벨 권한 모델도 지원합니다. 이 모델에서는 그 액세스 클래스에 관계없이 특정 속성에 대한 읽기, 쓰기, 탐색 및 비교 권한을 지정할 수 있습니다. 위의 예를 다시 고려해 보십시오. 속성 레벨 권한 모델의 경우, 일반적으로 Normal 속성에 액세스 권한을 부여하지 않아도 `telephoneNumber` 속성에 관리자 읽기 액세스 권한을 제공할 수 있습니다.

속성 레벨 권한 모델은 SecureWay 디렉토리 서비스 버전 3.2 이상의 서버에 대해서만 호환됩니다. 이 모델이 작동되지 않는 것이 디폴트입니다. ACL에 대해 작업할 때 모델을 작동시킬 수 있는 옵션을 사용할 수 있습니다. 모델이 작동 가능하게 한 후에는 서버를 재구성하거나 디렉토리 데이터베이스를 복원해야만 모델을 작동 불가능하게 할 수 있습니다. 이 모델을 작동시키기 전에는 LDAP V2 클라이언트(iSeries Navigator의 이전 V5R1 버전 포함)를 관리할 수 없으므로 무리하게 시도할 경우 ACL 항목이 손상될 수 있습니다.

특수 ACL 값

처음에는 디렉토리 서비스 디렉토리 서버의 모든 오브젝트들이 모든 디렉토리 사용자를 포함하고 있는 특수 ACL 그룹 `CN=Anybody`가 포함된 ACL을 가지고 있습니다. 디폴트로 이 그룹에는 모든 오브젝트를 위한 일반(normal) 클래스 속성에 대해 읽기, 탐색 및 비교 액세스 권한이 있습니다.

일부 오브젝트의 경우 익명이 아닌 연결로 디렉토리 서버에 바인드하는 모든 사용자에 대해 같은 액세스를 허용할 수 있습니다. 이 경우 특수 ACL(액세스 제어 목록) 그룹 `cn=Authenticated`를 사용하십시오.

오브젝트가 가지고 있는 액세스 권한 종류를 지정하기 위하여 특수 DN `cn=this`를 사용할 수 있습니다. 이와 같이 하면 ACL을 계승하는 하위 항목들이 자신이 소유한 오브젝트에 대해 자동으로 조작 권한을 부여받습니다.

추가 정보

iSeries Navigator로 ACL을 관리하기 위해서 디렉토리 서비스가 ACL을 어떻게 구현시키는지 자세히 알 필요는 없습니다. 그러나 LDIF 파일을 사용할 때 ACL 관련 속성을 지정하거나 ACL을 LDAP 명령행 유틸리티에서 사용할 경우에는 ACL이 사용하는 속성을 알고 있어야 합니다. ACL 속성에 대한 정보는 IBM SecureWay Directory Management Tool documentation  의 Access Control Lists reference document  를 참조하십시오.

ACL 및 ACL 그룹을 설정 및 변경하는 것에 대한 정보는 다음 링크를 참조하십시오.

32 페이지의『액세스 제어 리스트(ACL)에 대한 작업』
33 페이지의『ACL 그룹에 대한 작업』

LDAP 자료 교환 형식

LDIF(LDAP 자료 교환 형식)는 LDAP 디렉토리 서버 사이에서 간단하게 디렉토리 정보를 전송하는 방법을 제공합니다. LDIF 파일은 LDAP 디렉토리 항목을 간단한 텍스트 형식으로 보유합니다. 디렉토리 서버가 사용하는 LDIF 파일의 형식은 디렉토리 서비스 V4R5부터 약간 변경되었습니다. LDIF 파일은 디렉토리 항목이나 디렉토리 항목에 대한 일련의 변경을 설명하는 연속적인 행으로 구성되어 있습니다. LDIF 파일은 두 항목을 모두 설명할 수 없습니다.

LDIF 항목의 일반 형식은 다음과 같습니다.

```
version: 1
dn: distinguished name
attrtype1: attrvalue1
...
```

여기에서,

- *version*은 LDIF 파일 형식의 버전을 나타냅니다. 버전 번호가 1이어야 합니다. 버전 번호가 없으면, LDIF 파일이 더 이전의 LDIF 파일 형식을 취하는 것으로 간주합니다. LDIF 파일이 버전 1일 때, 내용은 반드시 UTF-8로 코드화되어 있어야 합니다.
- *distinguished name*은 디렉토리 항목의 고유명
- *attrtype1*은 LDAP 속성 유형(cn 또는 ou 등)
- *attrvalue1*은 속성의 값입니다.

각 항목은 여러 가지 속성을 가질 수 있습니다. 각 속성은 별도의 행에 나타납니다. 속성 값이 단일 행보다 길면 다음 행에 계속될 수 있으며, 공백 또는 탭 문자가 앞에 옵니다.

공백 행은 동일한 LDIF 파일 내에서 복수 항목을 분리합니다. 파운드 기호 (#)로 시작하는 모든 행은 주석 행이고, LDIF 파일을 분석할 때 무시되어야 합니다.

다음의 조건 중 하나를 충족시키는 임의의 고유명이나 속성 값은 base-64로 코드화되어야 합니다.
- 캐리지 리턴 또는 행 진입을 포함합니다.
- 콜론(:), SPACE 또는 미만 부호(<)로 시작합니다.
- 고유명이나 속성 값이 공백으로 끝납니다.

Base-64로 코드화된 속성은 속성명과 값 사이에 두 개의 콜론을 사용하여 지정됩니다.

| 외부 참조는 file:// URL 형식으로 되어 있습니다. 속성 유형과 외부 참조 값 사이에는 콜론과 미만 부호(:<)
| 문자가 있어야 합니다.

다음은 LDIF 파일의 예입니다.

예 1: 두 개의 항목을 포함하는 간단한 LDAP 파일

```
version: 1
   dn: cn=Barbara Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
objectclass: organizationalPerson
   cn: Barbara Jensen
   cn: Barbara J Jensen
   cn: Babs Jensen
sn: Jensen
   uid: bjensen
   telephonenumber: +1 408 555 1212
   description: A big sailing fan.

   dn: cn=Bjorn Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
objectclass: organizationalPerson
   cn: Bjorn Jensen
sn: Jensen
   telephonenumber: +1 408 555 1212
   description:Babs is a big sailing fan, and travels extensively in
   search of perfect sailing conditions.
   title:Product Manager, Rod and Reel Division
```

예 2: base-64로 코드화된 값을 포함하는 파일

```
version: 1
   dn: cn=Gern Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
objectclass: organizationalPerson
   cn: Gern Jensen
   cn: Gern O Jensen
sn: Jensen
   uid: gernj
   telephonenumber: +1 408 555 1212
   description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvdSBhcmUhICBUaGlzIHZhbHVlIGlzIGJ
    hc2UtNjQtZW5jb2RlZCBiZWNhdXNlIGl0IGhhcyBhIGNvbnRyb2wgY2hhcmFjdGVyIGluIGl0ICh
    hIENSKS4NICBCeSB0aGUgd2F5LCB5b3Ugc2hvdWxkIHJlYWxseSBnZXQgb3V0IG1vcmUu
```

예 3: 일련의 변경된 레코드와 주석을 포함하는 파일

주: 변경된 레코드를 포함하는 LDIF 파일은 직접 서버 안으로 가져올 수 없습니다. 그러나 이 파일은 LDAP 셸 유틸리티에서 지원합니다.

```
version: 1
   # Add a new entry
   dn: cn=Fiona Jensen, ou=Rochester, o=Big Company, c=US
   changetype: add
   objectclass: top
   objectclass: person
objectclass: organizationalPerson
   cn: Fiona Jensen
sn: Jensen
   uid: fiona
   telephonenumber: +1 408 555 1212
   jpegphoto:< file:///usr/local/directory/photos/fiona.jpg
```

```
   # Delete an existing entry
   dn: cn=Robert Jensen, ou=Rochester, o=Big Company, c=US
changetype: delete

   # Modify an entrys relative distinguished name
   dn: cn=Paul Jensen, ou=Rochester, o=Big Company, c=US
   changetype: modrdn
   newrdn: cn=Paula Jensen
   deleteoldrdn: 1
```

LDIF 파일에서 항목 순서는 중요합니다. LDIF 파일에 지정되는 항목을 LDAP 디렉토리에 성공적으로 추가하려면 먼저 상위 항목이 디렉토리 이름 공간에 있어야 합니다. 위의 예에서 첫 번째 항목이 없으면 두 번째와 세 번째 항목을 추가할 수 없습니다.

마찬가지로, LDIF 파일을 특정 접미부를 지원하는 서버에 가져오기하려면 LDIF 파일에 그러한 접미부에 대한 항목이 있어야 합니다. 예를 들어 서버에 접미부 ou=Rochester, o=Big Company, c=US가 있으면 위에 표시된 LDIF 파일을 가져오기할 수 있습니다. 그러나 대신 서버에 접미부 o=Big Company, c=US가 있는 경우에는 다음에 표시하는 것처럼 LDIF 파일에 처음 지정한 해당 접미부에 대한 항목이 있어야 합니다.

```
dn: o=Big Company, c=US
objectclass: organization
o: Big Company
```

LDIF 파일의 특정 형식과 내용은 내보내기할 서버의 스키마에 의해 판별됩니다. LDIF 파일이 내보낸 서버와 동일한 스키마를 사용하는 모든 LDAP 서버에 해당 LDIF 파일을 가져올 수 있습니다. 다른 공급자의 LDAP 서버는 서로 다른 스키마(오브젝트 클래스와 속성이 다름)를 사용합니다. 따라서, 한 서버에 의해 작성된 LDIF 파일을 다른 서버에 가져오지 못할 수도 있습니다.

LDIF 파일 스펙의 RFC(주석 요청)은 다음 URL에서 사용할 수 있습니다.

http://www.ietf.org/rfc/rfc2849.txt

관련 프로시듀어:

23 페이지의『LDIF 파일 가져오기』
23 페이지의『LDIF 파일 내보내기』

자국어 지원(NLS) 고려사항

V4R5에서부터, OS/400 디렉토리 서비스 LDAP 서버와 OS/400 LDAP 클라이언트 모두 LDAP 버전 3에 기초합니다. 다음의 NLS 고려사항에 주의하십시오.

- 데이터는 UTF-8 형식의 LDAP 서버와 클라이언트 간에 전송됩니다. 모든 ISO 10646 문자가 허용됩니다.
- 디렉토리 서비스 LDAP 서버는 UTF-16 맵핑 방법을 사용하여 데이터베이스에 데이터를 저장합니다.
- 서버와 클라이언트는 대소문자가 구분되는 스트링 비교를 수행합니다. 대문자 알고리즘은 모든 언어(로케일)에 해당되지 않습니다.

UCS-2에 대한 자세한 정보는 iSeries Information Center의 계획에서 국제화 주제를 참조하십시오.

LDAP 디렉토리 오브젝트의 소유권

LDAP 디렉토리의 각 오브젝트는 최소한 하나의 소유자를 가지고 있습니다. 오브젝트 소유자는 오브젝트 삭제 권한을 가집니다. 소유자 및 서버 관리자가 오브젝트의 소유권 특성과 액세스 제어 리스트(ACL) 속성을 변경할 수 있는 유일한 사용자입니다. 오브젝트의 소유권은 계승되거나 명시될 수 있습니다. 즉, 소유권을 지정하기 위해 다음 중 하나를 수행할 수 있습니다.

- 특정 오브젝트에 대한 소유권을 명시적으로 설정합니다.
- 오브젝트가 LDAP 디렉토리 계층의 더 높은 오브젝트에서 소유자를 계승한다고 지정합니다.

디렉토리 서비스를 사용하면 동일한 오브젝트에 대하여 복수 소유자를 지정할 수 있습니다. 또한 오브젝트가 자체를 소유하도록 지정할 수도 있습니다. 이를 수행하려면, 오브젝트 소유자의 리스트에 특수 DN `cn=this`이 들어 있어야 합니다. 예를 들어, 오브젝트 `cn=A`가 소유자 `cn=this`를 가지고 있는 것으로 가정하십시오. 서버에 `cn=A`로서 연결되는 경우, 모든 사용자는 `cn=A` 오브젝트에 대한 소유자 액세스를 갖습니다.

관련 프로시듀어:

32 페이지의『디렉토리 오브젝트의 소유권 등록 정보에 대한 작업』

LDAP 디렉토리 리퍼럴

참조를 사용하면 LDAP 디렉토리 서버가 팀으로 작업할 수 있습니다. 클라이언트가 요구하는 DN이 한 디렉토리에 없는 경우, 서버는 다른 LDAP 서버에 요구를 자동으로 송신(참조)할 수 있습니다.

디렉토리 서비스를 사용하면 서로 다른 2가지 유형의 리퍼럴을 사용할 수 있습니다. 디폴트 리터럴 서버를 지정할 수 있으며, 여기에서 LDAP 서버는 DN이 디렉토리에 없을 때마다 클라이언트를 참조하게 됩니다. 또한 LDAP 클라이언트를 사용하여 objectClass 리퍼럴을 갖는 디렉토리 서버에 항목을 추가할 수도 있습니다. 그러면 클라이언트가 요구하는 특정 DN을 기준으로 리퍼럴을 지정할 수 있습니다.

주: 디렉토리 서비스의 경우, 참조 오브젝트에는 식별명(`dn`), 오브젝트 클래스(`objectClass`) 및 참조(`ref`) 속성만 있어야 합니다. 이 제한사항을 설명하는 예에 관하여 58 페이지의『ldapsearch 유틸리티』를 참조하십시오.

리퍼럴 서버는 복제 서버와 밀접한 관련이 있습니다. 복제 서버의 자료를 클라이언트로부터 변경할 수 없기 때문에, 복제는 디렉토리 자료를 변경하는 모든 요구를 마스터 서버에 참조합니다.

트랜잭션

클라이언트가 트랜잭션을 사용할 수 있도록 시스템의 LDAP 디렉토리 서버를 구성할 수 있습니다. 트랜잭션은 하나의 장치로 처리되는 LDAP 디렉토리 작업의 그룹입니다. 트랜잭션을 구성하는 개별 LDAP 작업은 트랜잭션의 모든 작업이 성공적으로 완료되고, 트랜잭션이 확약되어야 영구적입니다. 작업에 실패하거나 트랜잭션이 취소되면 다른 작업의 실행도 취소됩니다. 이 기능은 사용자가 LDAP 작업을 구성 상태로 유지하는 데 도움이 됩니다. 예를 들어 사용자는 여러 디렉토리 항목을 삭제하는 트랜잭션을 해당 클라이언트에 설정할 수 있습니다. 클라이언트가 트랜잭션을 통해 서버로의 연결을 어느 정도 끊으면, 항목이 삭제되지 않습니다. 그러므로 사용자는 삭제된 항목을 확인하지 않아도 트랜잭션을 시작할 수 있습니다.

다음의 LDAP 작업은 트랜잭션의 일부가 될 수 있습니다.

- 추가
- 수정
- RDN 수정
- 삭제

주: 트랜잭션의 디렉토리 스키마(cn=schema 접미사)에 변경사항을 포함시키지 마십시오. 변경사항을 포함시킬 수도 있지만 트랜잭션이 실패하면 역처리될 수 없습니다. 이로 인해 디렉토리 서버에 예기치 않은 문제가 발생할 수 있습니다.

트랜잭션에 대한 추가 정보는 IBM SecureWay Directory Client SDK Programming Reference  의 Limited Transaction Support appendix  를 참조하십시오.

복제 LDAP 디렉토리 서버

복제 LDAP 디렉토리 서버에 저장된 정보는 기본 또는 마스터 LDAP 디렉토리 서버의 정보와 동일합니다. LDAP 디렉토리의 하나 이상의 복제를 가지면 다음 2가지 주요한 장점이 있습니다.

- 복제가 디렉토리 탐색을 더 빠르게 만듭니다. 모든 클라이언트가 탐색 요구를 단일 마스터 서버에 지정하는 대신, 요구를 마스터 서버와 복제 서버에서 분할할 수 있습니다.
- 복제는 마스터 서버에 대한 백업을 제공합니다. 마스터 서버를 사용할 수 없는 경우, 복제는 여전히 탐색 요구를 이행하고, 디렉토리 자료에 대한 액세스를 제공할 수 있습니다.

복제 서버는 읽기 전용입니다. 권한을 부여받은 사용자가 복제 서버의 항목을 변경하려고 할 경우, 복제 서버는 마스터 디렉토리 서버에 요구를 참조합니다.

관련 프로시듀어:

23 페이지의『디렉토리 서버의 신규 복제 설정』

디렉토리 서비스 보안

보안 감사

V5R1부터 디렉토리 서비스는 OS/400 보안 감사를 지원합니다. 감사할 수 있는 항목은 다음과 같습니다.

- 디렉토리 서버에 바인드되거나 디렉토리 서버에서 바인드되지 않습니다.
- LDAP 디렉토리 오브젝트의 권한을 변경합니다.
- LDAP 디렉토리 오브젝트의 소유권을 변경합니다.
- LDAP 디렉토리 오브젝트를 작성, 삭제, 탐색 및 변경합니다.
- 관리자의 암호를 변경하고 식별명(DN)을 갱신합니다.
- 사용자의 암호를 변경합니다.

- 파일을 가져오거나 내보냅니다.

디렉토리 항목을 감사하기 전에 OS/400 감사 설정을 변경해야 합니다. QAUDCTL 시스템 값에 *OBJAUD가 지정되어 있으면 iSeries Navigator를 통해 오브젝트 감사를 작동할 수 있습니다. 감사에 대한 자세한 정보는 *보안 - 참조서*  또는 iSeries Information Center의 Security auditing 주제를 참조하십시오.

연결 인증 및 보안

디렉토리 서비스는 LDAP 클라이언트와 LDAP 디렉토리 서버간의 통신 보안을 강화하는 데 사용할 수 있는 다음과 같은 메카니즘을 제공합니다.

- SSL(보안 소켓층) 연결
- Kerberos 인증
- CRAM-MD5 암호 암호화

LDAP 디렉토리 서버에서 SSL(보안 소켓층) 및 변환층 보안 사용

LDAP 디렉토리 서버와의 통신을 더욱 안전하게 하기 위해, 디렉토리 서비스는 SSL(보안 소켓층) 보안을 사용할 수 있습니다.

SSL을 디렉토리 서비스에서 사용하려면 시스템에 암호 액세스 제공자 제품(5722-ACx)중 하나가 설치되어 있어야 합니다. iSeries Navigator에서 SSL을 사용할 경우에도 클라이언트 암호화 제품(5722-CEx)중 하나가 PC에 설치되어 있어야 합니다. 다음 중 하나를 수행하려는 경우, 다음 소프트웨어가 필요합니다.

- SSL 연결을 사용하여 워크스테이션을 통해 디렉토리 서비스 구성 및 관리. 이것은 iSeries Navigator를 통해 수행하는 타스크가 포함됩니다.
- Windows 클라이언트 API(어플리케이션 프로그램 인터페이스)로 작성하는 어플리케이션에서 SSL 연결 사용.

SSL은 인터넷 보안의 표준입니다. 복제 LDAP 서버 뿐만 아니라 LDAP 클라이언트와 통신하기 위해 SSL을 사용할 수 있습니다. 추가 보안을 SSL 연결에 제공하기 위해 서버 인증에 더하여 클라이언트 인증도 사용할 수 있습니다. 클라이언트 인증은 연결되기 전에 서버에 클라이언트의 신원을 확인하는 디지털 인증을 제시하도록 요구합니다.

SSL을 사용하려면, 시스템에 OS/400의 옵션 34인 DCM(Digital Certificate Manager)을 설치해야 합니다. DCM은 디지털 인증과 인증 저장소를 작성 및 관리할 수 있는 인터페이스를 제공합니다. 디지털 인증 및 DCM 사용에 대한 정보는 디지털 인증 관리자 문서를 참조하십시오. iSeries의 SSL에 대한 정보는 SSL을 사용한 어플리케이션 보안을 참조하십시오. iSeries 서버의 TLS에 대한 정보는 지원되는 SSL 및 TLS(전송층 보안) 프로토콜을 참조하십시오.

LDAP 디렉토리 서버에서 Kerberos 인증 사용

디렉토리 서비스에서는 Kerberos 인증을 사용하도록 LDAP 디렉토리 서버를 설정할 수 있습니다. Kerberos는 비밀 키 암호를 사용해서 클라이언트/서버 어플리케이션에 강력한 인증을 제공하는 네트워크 인증 프로토콜입니다.

Kerberos 인증을 작동할 수 있게 하려면 시스템에 암호 서비스 제공자 제품(5722AC2 또는 5722AC3)의 하나가 설치되어 있어야 합니다. 네트워크 인증 서비스도 구성되어야 합니다.

디렉토리 서비스의 Kerberos 지원은 GSSAPI SASL 메카니즘에 대한 지원을 제공합니다. 따라서 SecureWay와 Windows 2000 LDAP 클라이언트를 작동하여 LDAP 디렉토리 서버에서 Kerberos 인증을 사용할 수 있습니다.

서버가 사용하는 **Kerberos 프린시펄명**의 형태는 다음과 같습니다.

```
service-name/host-name@realm
```

service-name은 LDAP이고, host-name은 시스템의 정식 TCP/IP 이름이며, realm은 시스템의 Kerberos 구성에 지정된 디폴트 영역입니다.

예를 들어, ACME.COM의 디폴트 Kerberos 영역을 사용하여, acme.com TCP/IP 정의역에서 my-as400으로 명명된 시스템의 경우, LDAP 서버 Kerberos 프린시펄명은 LDAP/my-as400.acme.com@ACME.COM이 됩니다. 디폴트 Kerberos 영역은 default_realm 지시문(default_realm = ACME.COM)이 있는 Kerberos 구성 파일(기본적으로, /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf)에 지정됩니다. 규약에 의해 Kerberos 영역명에는 대문자가 사용되고, 호스트명에는 소문자가 사용됩니다. LDAP/는 대문자이어야 합니다. 디폴트 영역이 구성되지 않았으면 Kerberos 인증을 사용하도록 디렉토리 서버를 구성할 수 없습니다.

Kerberos 인증이 사용될 때 LDAP 디렉토리 서버는 디렉토리 자료에 대한 액세스를 결정하는 연결에 식별명(DN)을 연관시킵니다. 서버 DN이 다음 메소드 중 하나와 연관되도록 선택할 수 있습니다.

- 서버는 Kerberos ID에 근거하여 DN을 작성할 수 있습니다. 이 옵션을 선택하면 principal@realm 형태의 Kerberos ID가 ibm-kn=principal@realm 형태의 DN을 생성합니다. ibm-kn=은 ibm-kerberosName=에 해당합니다.
- 서버는 디렉토리에서 Kerberos 프린시펄과 영역에 대한 항목이 들어 있는 식별명(DN)을 탐색할 수 있습니다. 이 옵션을 선택하면 서버는 디렉토리에서 다음과 같이 Kerberos ID를 지정하는 항목을 탐색합니다.
  - 서버는 Kerberos 영역과 일치하는 krbRealmName-V2 속성이 있는 krbRealm-V2 오브젝트를 디렉토리에서 탐색합니다. 항목을 찾으면 프린시펄명 및 영역명과 일치하는 krbPrincipalName 속성이 있는 항목의 princSubtree 속성에 지정된 DN이 탐색됩니다. krbAliasedObjectName에 구성된 DN에 이전에 발견된 항목의 DN이 있는 경우 krbAliasedObjectName에 구성된 DN이 사용됩니다. 그렇지 않으면, 이 항목의 DN이 사용됩니다. 일반적으로 이 메소드는 Kerberos KDC가 Kerberos 프린시펄 정보를 LDAP 디렉토리에 저장할 때 사용됩니다.
  - 위에서 설명한 탐색에 실패하면 서버는 ibm-securityIdentities 보조 클래스를 사용하고, KERBEROS:principal@realm의 altSecurityIdentities 속성값이 있는 디렉토리 항목을 탐색합니다. 이 메소드는 KDC가 프린시펄을 디렉토리에 저장하지 않을 때 Kerberos ID를 디렉토리 항목과 연관시키는 데 사용할 수 있습니다.

LDAP 서비스 프린시펄에 대한 키를 포함하는 키 표(keytab) 파일이 있어야 합니다. iSeries 서버의 Kerberos에 대한 자세한 정보는 보안에서 Information Center 주제 네트워크 인증 서비스를 참조하십시오. 네트워크 인증 서비스 구성 섹션에는 키 표 파일에 정보 추가에 대한 내용이 들어 있습니다.

오퍼레이팅 시스템 프로젝트 백엔드

시스템 프로젝트 백엔드에는 OS/400 오브젝트를 LDAP 액세스 가능 디렉토리 트리 내의 항목으로 맵핑하는 능력이 있습니다. 프로젝트 오브젝트는 LDAP 서버 데이터베이스에 저장된 실제 항목이 아닌 OS/400 오브젝트의 LDAP 표시입니다. V5R2에서 OS/400 사용자 프로파일은 디렉토리 트리 내의 항목으로 맵핑되거나 프로젝트되는 오브젝트만 해당합니다. 사용자 프로파일 오브젝트의 맵핑을 OS/400 사용자 프로젝트 백엔드라고 합니다.

LDAP 조작은 기초 OS/400 오브젝트에 맵핑되고 이러한 오브젝트에 액세스하기 위해 오퍼레이팅 시스템 기능을 수행합니다. 사용자 프로파일에서 수행된 모든 LDAP 조작은 클라이언트 연결과 연관된 사용자 프로파일의 권한하에 수행됩니다.

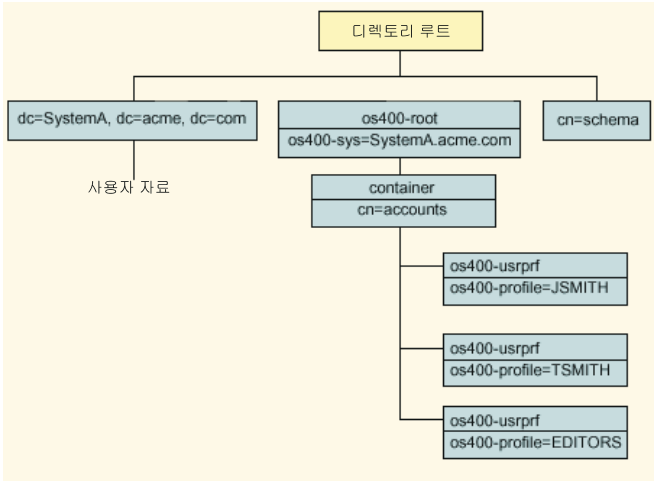
오퍼레이팅 시스템 프로젝트 백엔드에 대한 자세한 정보는 다음을 참조하십시오.

- 『OS/400 사용자 프로젝트 디렉토리 정보 트리』
- 47 페이지의 『LDAP 조작』
- 51 페이지의 『관리자 및 복제 바인드 DN』
- 51 페이지의 『OS/400 사용자 프로젝트 스키마』

OS/400 사용자 프로젝트 디렉토리 정보 트리

아래의 그림은 사용자 프로젝트 백엔드에 대한 샘플 DIT(Directory Information Tree)를 표시합니다. 이 그림은 개인 및 그룹 프로파일을 모두 표시합니다. 이 그림에서 JSMITH 및 TSMITH는 사용자 프로파일로서 GID(그룹 ID), GID=*NONE(또는 0)으로 내부적으로 표시됩니다. EDITORS는 그룹 프로파일로서 0이 아닌 GID로 내부적으로 표시됩니다.

접미부 dc=SystemA, dc=acme, dc=com은 참조용으로 그림에 포함됩니다. 이 접미부는 다른 LDAP 항목을 관리하고 있는 현재 데이터베이스 백엔드를 표시합니다. 접미부 cn=schema는 현재 사용 중인 서버 차원의 스키마입니다.



트리의 루트는 os400-sys=*SystemA.acme.com*이 디폴트인 접미부입니다. 여기에서 *SystemA.acme.com*이 시스템의 이름입니다. 오브젝트 클래스는 os400-root입니다. DIT는 수정하거나 삭제할 수 없지만 시스템 오브젝트의 접미부를 재구성할 수 있습니다. 그러나 현재의 접미부가 ACL이나, 접미부를 변경하기 위해 항목을 수정해야 하는 시스템의 다른 부분에서 사용되지 않도록 해야 합니다.

이전 그림에서 컨테이너 cn=accounts가 루트 아래에 표시됩니다. 이 오브젝트는 수정할 수 없습니다. 컨테이너는 나중에 오퍼레이팅 시스템이 프로젝트할 수 있는 다른 종류의 정보나 오브젝트를 예측하여 이 레벨에 배치됩니다. cn=accounts 컨테이너 아래에는 objectclass=os400-usrprf로 프로젝트되는 사용자 프로파일이 있습니다. 사용자 프로파일은 프로젝트된 사용자 프로파일이라고 하고 os400-profile=JSMITH, cn=accounts, os400-sys=SystemA.acme.com 양식으로 LDAP에 인식됩니다.

LDAP 조작

다음은 프로젝트된 사용자 프로파일을 사용하여 수행할 수 있는 LDAP 조작입니다.

바인드

LDAP 클라이언트는 프로젝트된 사용자 프로파일을 사용하여 LDAP 서버에 바인드(인증)할 수 있습니다. 이 작업은 바인드 DN에 대해 프로젝트된 사용자 프로파일 식별명(DN)과 인증용으로 올바른 OS/400 사용자 프로파일 암호를 지정하여 수행합니다. 바인드 요구에 사용되는 DN의 예는 os400-profile=jsmith, cn=accounts,os400-sys=systemA.acme.com입니다.

클라이언트는 시스템 프로젝트 백엔드의 정보에 액세스할 수 있도록 프로젝트된 사용자로 바인드해야 합니다. 서버는 해당 사용자 프로파일의 권한을 사용하여 모든 조작을 수행합니다. 프로젝트된 사용자 프로파일 DN은 다른 LDAP 항목 DN과 같이 LDAP ACL에서도 사용할 수 있습니다. 바인드 요구 시 프로젝트된 사용자 프로파일을 지정할 때 허용되는 방법이 간단한 바인드 방법으로 유일한 바인드 방법입니다.

탐색

시스템 프로젝트 백엔드는 일부 기본 탐색 필터를 지원합니다. 탐색 필터에 objectclass, os400-profile 및 os400-gid 속성을 지정할 수 있습니다. os400-profile 속성은 와일드 카드를 지원합니다. os400-gid 속성은 개

별 사용자 프로파일인 (os400-gid=0) 또는 그룹 프로파일인 !(os400-gid=0)을 지정하는 것으로 제한됩니다. 암호 및 유사 속성을 제외한 사용자 프로파일의 모든 속성을 검색할 수 있습니다.

특정 필터의 경우 DN objectclass 및 os400-profile 값만 리턴됩니다. 그러나 자세한 정보를 리턴할 수 있도록 후속 탐색을 수행할 수 있습니다.

다음 표는 탐색 조작을 위한 시스템 프로젝트 백엔드의 작동을 설명합니다.

표 1. 탐색 조작을 위한 시스템 프로젝트 백엔드 작동

요구된 탐색	탐색 기본	탐색 범위	탐색 필터	주석
os400-sys=SystemA용, 컨테이너용(선택적) 및 해당 컨테이너의 오브젝트용(선택적) 정보를 리턴합니다.	os400-sys=SystemA.acme.com	기본, 하위 또는 하나	objectclass=* objectclass=os400-root objectclass=container objectclass=os400-usrprf	지정된 범위 및 필터를 기준으로 적절한 속성 및 값을 리턴합니다. 시스템 오브젝트의 접미부 및 소속 컨테이너에 대한 hardcoded 속성 및 값을 리턴합니다.
모든 사용자 프로파일을 리턴합니다.	cn=accounts, os400-sys=SystemA.acme.com	하나 또는 하위	os400-gid=0	프로젝트된 사용자 프로파일에 대해 식별명(DN), objectclass 및 os400-profile 값만 리턴합니다. 다른 필터가 지정된 경우, LDAP_UNWILLING_TO_PERFORM이 리턴됩니다.
모든 그룹 프로파일을 리턴합니다.	cn=accounts, os400-sys=SystemA.acme.com	하나 또는 하위	(!(os400-gid=0))	프로젝트된 사용자 프로파일에 대해 식별명(DN), objectclass 및 os400-profile 값만 리턴합니다. 다른 필터가 지정된 경우, LDAP_UNWILLING_TO_PERFORM이 리턴됩니다.
모든 사용자 및 그룹 프로파일을 리턴합니다.	cn=accounts, os400-sys=SystemA.acme.com	하나 또는 하위	os400-profile=*	프로젝트된 사용자 프로파일에 대해 식별명(DN), objectclass 및 os400-profile 값만 리턴합니다. 다른 필터가 지정된 경우, LDAP_UNWILLING_TO_PERFORM이 리턴됩니다.
사용자 프로파일 JSMITH와 같은 특정 사용자 또는 그룹 프로파일에 대한 정보를 리턴합니다.	cn=accounts, os400-sys=SystemA.acme.com	하나 또는 하위	os400-profile=JSMITH	리턴할 기타 속성을 지정할 수 있습니다.

표 1. 탐색 조작을 위한 시스템 프로젝트 백엔드 작동 (계속)

요구된 탐색	탐색 기본	탐색 범위	탐색 필터	주석
사용자 프로파일 JSMITH와 같은 특정 사용자 또는 그룹 프로파일에 대한 정보를 리턴합니다.	os400-profile=JSMITH, cn=accounts, os400-sys=SystemA.acme.com	기본, 하위 또는 하나	objectclass=os400-usrprf objectclass=* os400-profile=JSMITH	리턴할 기타 속성을 지정할 수 있습니다. 한 레벨의 범위를 지정할 수 있는 경우에도 DIT의 사용자 프로파일 JSMITH 아래에 값이 없기 때문에 탐색 결과가 값을 리턴하지 않습니다.
A부터 시작하여 모든 사용자 및 그룹 프로파일을 리턴합니다.	cn=accounts, os400-sys=SystemA.acme.com	하나 또는 하위	os400-profile=A*	프로젝트된 사용자 프로파일에 대해 식별명(DN), objectclass 및 os400-profile 값만 리턴합니다. 다른 필터가 지정된 경우, LDAP_UNWILLING_TO_PERFORM이 리턴됩니다.
G부터 시작하여 모든 그룹 프로파일을 리턴합니다.	cn=accounts, os400-sys=SystemA.acme.com	하나 또는 하위	(&(!(os400-gid=0)) (os400-profile=G*))	프로젝트된 사용자 프로파일에 대해 식별명(DN), objectclass 및 os400-profile 값만 리턴합니다. 다른 필터가 지정된 경우, LDAP_UNWILLING_TO_PERFORM이 리턴됩니다.
A부터 시작하여 모든 사용자 프로파일을 리턴합니다.	cn=accounts, os400-sys=SystemA.acme.com	하나 또는 하위	(&(os400-gid=0) (os400-profile=A*))	프로젝트된 사용자 프로파일에 대해 식별명(DN), objectclass 및 os400-profile 값만 리턴합니다. 다른 필터가 지정된 경우, LDAP_UNWILLING_TO_PERFORM이 리턴됩니다.

비교

LDAP 비교 조작을 사용하여 프로젝트된 사용자 프로파일의 속성값을 비교할 수 있습니다. os400-aut 및 os400-docpwd 속성은 비교할 수 없습니다.

추가 및 수정

LDAP 추가 조작을 사용하여 사용자 프로파일을 작성할 수 있고 LDAP 수정 조작을 사용하여 사용자 프로파일을 수정할 수도 있습니다.

삭제

LDAP 삭제 조작을 사용하여 사용자 프로파일을 삭제할 수 있습니다. DLTUSRPRF OWNOBJOPT 및 PGPOPT 매개변수의 작동을 지정하기 위해 이제 두 개의 LDAP 서버 제어가 제공됩니다. 이 제어는 LDAP 삭제 조작 시 지정할 수 있습니다. 이 매개변수의 작동에 대한 자세한 정보는 DLTUSRPRF(사용자 프로파일 삭제) 명령을 참조하십시오.

다음은 LDAP 클라이언트 삭제 조작에서 지정할 수 있는 제어 및 OID(오브젝트 ID)입니다.

- os400-dltusrprf-ownobjopt 1.3.18.0.2.10.8

  다음은 제어값입니다.

  - controlValue ::= ownObjOpt [newOwner]
  - ownObjOpt ::= *NODLT / *DLT / *CHGOWN

  ownObjOpt 제어값은 사용자 프로파일이 오브젝트를 소유하는 경우 수행할 조치를 지정합니다. *NODLT 값은 사용자 프로파일이 오브젝트를 소유하는 경우 사용자 프로파일을 삭제하지 않을 것을 표시합니다. *DLT 값은 소유한 오브젝트를 삭제할 것을 표시하고 *CHGOWN 값은 다른 프로파일로 소유권을 전송할 것을 표시합니다.

  newOwner 값은 소유권을 전송할 프로파일을 지정합니다. ownObjOpt를 *CHGOWN으로 설정할 때 이 값이 필요합니다.

  제어값의 예는 다음과 같습니다.

  - *NODLT: 프로파일이 오브젝트를 소유하는 경우 삭제할 수 없음을 지정합니다.
  - *CHGOWN SMITH: 오브젝트의 소유권을 SMITH 사용자 프로파일로 전송할 것을 지정합니다.

- OID(오브젝트 ID)는 ldap.h에 LDAP_OS400_OWNOBJOPT_CONTROL_OID로 정의합니다.
  - os400-dltusrprf-pgpopt 1.3.18.0.2.10.9

    제어값을 다음과 같이 정의합니다.

    controlValue ::=pgpOpt [newPgp [newPgpAut]]
    pgpOpt ::= *NOCHG / *CHGPGP
    newPgp ::= *NONE / user-profile-name
    newPgpAut ::= *OLDPGP / *PRIVATE / *ALL / *CHANGE / *USE / *EXCLUDE

    pgpOpt 값은 삭제 중인 프로파일이 오브젝트의 1차 그룹인 경우 수행할 조치를 지정합니다. *CHGPGP를 지정하는 경우 newPgp도 지정해야 합니다. newPgp 값은 1차 그룹 프로파일명 또는 *NONE을 지정합니다. 새로운 1차 그룹 프로파일을 지정하는 경우 newPgpAut 값도 지정할 수 있습니다. newPgpAut 값은 새로운 1차 그룹이 제공된 오브젝트에 대한 권한을 지정합니다.

  제어값의 예는 다음과 같습니다.

  - *NODLT: 프로파일이 오브젝트의 1차 그룹인 경우 삭제할 수 없음을 지정합니다.
  - *CHGPGP *NONE: 오브젝트의 1차 그룹을 제거할 것을 지정합니다.
  - *CHGPGP SMITH *USE: 1차 그룹을 SMITH 사용자 프로파일로 변경하고 1차 그룹에 *USE 권한을 부여할 것을 지정합니다.

삭제 시 이 제어를 지정하지 않으면 현재 QSYS/DLTUSRPRF 명령에 적용된 디폴트가 대신 사용됩니다.

ModRDN

오퍼레이팅 시스템에서 지원하지 않으므로 프로젝트된 사용자 프로파일의 이름을 변경할 수 없습니다.

API 가져오기 및 내보내기

QgldImportLdif 및 QgldExportLdif API는 시스템 프로젝트 백엔드에 있는 자료의 가져오기 또는 내보내기를 지원하지 않습니다.

관리자 및 복제 바인드 DN

프로젝트된 사용자 프로파일을 구성된 관리자 또는 복제 바인드 DN으로 지정할 수 있습니다. 사용자 프로파일의 암호를 사용합니다. 디렉토리 서버 관리자 기능 ID(QIBM_DIRSRV_ADMIN)에 대한 권한이 있는 경우 프로젝트된 사용자 프로파일은 LDAP 관리자가 될 수도 있습니다. 복수의 사용자 프로파일에게 관리자 액세스를 부여할 수 있습니다.

자세한 내용은 33 페이지의 『권한이 있는 사용자의 관리 액세스에 대한 작업』을 참조하십시오.

OS/400 사용자 프로젝트 스키마

프로젝트된 백엔드의 오브젝트 클래스 및 속성을 서버 차원의 스키마에서 찾을 수 있습니다. LDAP 속성명은 `os400-`*`nnn`* 형식으로 되어 있습니다. 여기에서 *nnn*은 일반적으로 사용자 프로파일 명령의 속성 키워드(예: CRTUSRPRF 또는 CHGUSRPRF)입니다. 자세한 정보는 46 페이지의 『OS/400 사용자 프로젝트 디렉토리 정보 트리』를 참조하십시오.

디렉토리 서비스 및 OS/400 저널링 지원

디렉토리 서비스는 디렉토리 정보를 저장하기 위해 OS/400 데이터베이스 지원을 사용합니다. 디렉토리 서비스는 디렉토리 항목을 데이터베이스에 저장하기 위해 확약 제어를 사용합니다. 여기에는 OS/400 저널링 지원이 필요합니다.

서버나 LDIF 가져오기 툴을 처음 시작할 때, 다음 사항이 구축됩니다.

- 저널
- 저널 리시버
- 처음에 요구되는 임의의 데이터베이스 표

저널 QSQJRN은 구성된 데이터베이스 라이브러리에서 빌드됩니다. 저널 리시버 QSQJRN0001은 구성된 데이터베이스 라이브러리에서 초기에 작성됩니다.

환경, 디렉토리 크기와 구조, 저장 및 복원 전략은 이러한 오브젝트의 관리 방법과 사용되는 크기 임계값을 포함하여 디폴트 값과 약간의 차이를 나타낼 수 있습니다. 필요한 경우 저널링 명령 매개변수를 변경할 수 있습니다. 오래된 리시버를 삭제하도록 LDAP 저널링이 기본적으로 설정됩니다. 변경 기록부를 구성하고 오래된 리시버를 보존하려면 OS/400 명령행에서 다음 명령을 실행하십시오.

```
JRN(QUSRDIRCL/QSQJRN) DLTRCV(*NO)
```

변경 기록부가 구성되면 다음 명령을 사용하여 해당 저널 리시버를 삭제할 수 있습니다.

```
CHGJRN JRN(QUSRDIRCL/QSQJRN)  DLTRCV(*YES)
```

저널링 명령에 대한 정보는 iSeries Information Center의 프로그래밍 아래에 있는 OS/400 명령 주제를 참조하십시오.

제 6 장 LDAP 명령행 유틸리티

디렉토리 서비스에는 OS/400의 Qshell 명령 환경에서 LDAP 디렉토리 서버에 대한 조치를 수행할 수 있는 5개의 유틸리티가 있습니다. 이러한 유틸리티는 LDAP API를 사용합니다. 이러한 유틸리티를 qsh 명령행에서 사용하거나 프로그램에서 호출할 수 있습니다. 또 프로그래밍 예로서 유용하다는 것도 알 수 있습니다. 디렉토리 서비스에 포함되어 있는 Windows LDAP 클라이언트를 설치할 때는 셸 유틸리티의 소스 코드와 매우 유사한 코드도 설치합니다.

유틸리티는 다음과 같습니다.
- LDAP 디렉토리 항목을 추가 및 수정하는 『ldapmodify 및 ldapadd 유틸리티』
- LDAP 디렉토리에서 항목을 제거하는 56 페이지의 『ldapdelete 유틸리티』
- LDAP 디렉토리에 항목이 있는지 탐색하는 58 페이지의 『ldapsearch 유틸리티』
- LDAP 디렉토리 항목의 RDN(상대 고유명)을 수정하는 63 페이지의 『ldapmodrdn 유틸리티』

명령 행 유틸리티에서 SSL 사용에 관한 정보는 65 페이지의 『LDAP 명령행 유틸리티에서 SSL 사용에 관한 참고사항』를 참조하십시오.

ldapmodify 및 ldapadd 유틸리티

ldapmodify 유틸리티를 사용하여 시스템의 QSH 명령 셸에서 LDAP 디렉토리 서버로 항목을 변경하거나 추가할 수 있습니다. ldap_modify, ldap_add 및 ldap_delete API(어플리케이션 프로그램 인터페이스)를 사용합니다. ldapadd 유틸리티는 -a 플래그가 자동으로 켜지는 점을 제외하면 ldapmodify 유틸리티처럼 작동합니다.

형식:

ldapmodify [-a] [-V] [-b] [-c] [-r] [-M] [-n] [-v] [-F] [-R] [-C *charset***] [-d** *debuglevel***] [-D** *binddn***] [-w** *passwd* **] [-m** *mechanism***] [-O***hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-f** *file***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***]**

ldapadd [-V] [-b] [-c] [-r] [-M] [-n] [-v] [-F] [-R] [-C *charset***] [-d** *debuglevel***] [-D** *binddn* **] [-w** *passwd***] [-m** *mechanism***] [-O***hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-f** *file***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***]**

주: **-f** 옵션을 사용하여 *file*에서 항목 정보를 제공하지 않을 경우에는 유틸리티가 표준 입력으로부터 항목을 읽기 위해 대기합니다. 대기를 중단하려면 SysReq 키를 클릭한 다음, 2. 이전 요구 종료를 선택하십시오.

진단:

오류가 발생하지 않은 경우, 나감 상태는 0입니다. 오류가 발생하면 0이 아닌 나감 상태가 되고, 진단 메세지가 표준 오류에 기록됩니다.

이 유틸리티의 사용 예를 보려면 여기를 클릭하십시오.

매개변수:

-V	유틸리티가 LDAP 서버에 바인드하기 위해 사용하는 LDAP 버전을 지정합니다. 기본적으로 LDAP 버전은 LDAP V3 연결을 사용합니다. LDAP V3을 명시적으로 선택하려면 -V 3을 지정하십시오. -V 2를 지정하여 LDAP V2 어플리케이션으로 실행하십시오.
-a	ldapmodify만 이 매개변수를 사용합니다. 이것은 유틸리티가 항목을 수정하는 것이 아니라 기본적으로 항목을 추가하는 것을 나타냅니다. 이 매개변수의 사용법은 ldapadd의 사용법과 동일합니다.
-b	`/로 시작하는 모든 값은 2진값이며, 정상으로 값이 나타나는 위치의 경로를 사용하는 파일에 실제 값이 있는 것으로 가정합니다.
-c	연속 작업 모드. 오류가 보고되지만 ldapmodify 또는 ldapadd가 수정 또는 추가를 계속합니다. 디폴트는 오류 기록 후 나가는 것입니다.
-r	기존값을 디폴트로 대체합니다.
-M	참조 오브젝트를 일반 항목으로 관리합니다.
-n	수행 결과를 표시하되 실제로는 항목을 수정하지 않습니다. -v와 결합하여 디버깅에 유용합니다.
-v	표준 출력에 기록된 많은 진단을 갖고 verbose 모드를 사용합니다.
-F	replica:로 시작하는 입력 행의 내용과 관계없이 모든 변경을 강제로 적용합니다. (복제 기록부 레코드를 실제로 적용시켜야 할 것인지 결정할 때 현재 사용 중인 LDAP 서버 호스트 및 포트에 대해 replica: 행을 비교되는 것이 디폴트입니다.)
-R	리퍼럴이 자동으로 뒤따르지 않도록 지정합니다.
-C *charset*	유틸리티에 대한 입력으로 제공된 스트링은 로컬 문자 세트(*charset*)로 표시되고 반드시 UTF-8로 변환되도록 지정합니다. 입력 스트링 코드 페이지가 작업 코드 페이지 값과 다른 경우는 **-C** charset 옵션을 사용하십시오. 지원되는 *charset* 값을 참조하려면 ldap_set_iconv_local_charset() API에 대한 문서를 참조하십시오.
-d *debuglevel*	디버그 레벨을 *debuglevel*로 설정합니다.
-D *binddn*	LDAP 디렉토리를 바인드하기 위해 *binddn*를 사용합니다. *binddn*은 스트링 표현된 DN이어야 합니다.
-w *passwd*	*passwd*를 인증 암호로 사용합니다.
-m *mechanism*	클라이언트가 서버와의 바인드에 사용하는 SASL 메카니즘을 지정하기 위해 *mechanism*을 사용합니다. 클라이언트는 ldap_sasl_bind_s() API를 사용합니다. 사용 가능한 메카니즘은 CRAM-MD5(암호화 암호), EXTERNAL(SSL에 사용) 및 GSSAPI(Kerberos)입니다. **-V 2**가 설정되어 있으면 명령이 **-m** 매개변수를 무시합니다. **-m**을 지정하지 않으면 간단한 인증이 사용됩니다.
-O*hopcount*	참조를 추적할 때 클라이언트 라이브러리가 사용할 최대 홉 수를 설정하기 위해 *hopcount*를 지정합니다. 디폴트 홉 카운트는 10입니다.
-h *ldaphost*	LDAP 서버가 실행될 대체 호스트를 지정합니다.
-p *ldapport*	LDAP 서버가 청취할 대체 전송 제어 프로토콜(TCP) 포트를 지정합니다. 디폴트 LDAP 포트는 389입니다. 포트가 지정되지 않고 **-Z**가 지정되면 디폴트 LDAP SSL 포트 636이 사용됩니다.
-f *file*	표준 입력 대신에 LDIP 파일로부터 항목 수정 정보를 읽습니다. LDIF 파일이 지정되지 않은 경우에는 갱신 레코드를 LDIP 형식으로 지정하기 위해 표준 입력을 사용해야 합니다.
-Z	LDAP 서버와 통신하기 위해 보안 SSL 연결을 사용합니다. 이 툴의 SSL 작동가능 버전만이 **-Z** 옵션을 지원합니다.
-K *keyfile*	SSL 키 데이터베이스 파일의 이름을 지정합니다. 키 데이터베이스 파일이 현재 디렉토리에 없으면 완전 규정된 키 데이터베이스 파일명을 지정하십시오. 유틸리티가 키 데이터베이스를 찾을 수 없으면 기본적으로 신뢰할 수 있는 인증 기관 루트의 hard-coded 세트가 사용됩니다. 일반적으로 키 데이터베이스 파일에는 클라이언트가 신뢰하는 CAs(인증 기관)의 인증서가 하나 이상 들어 있습니다. 이러한 유형의 X.509 인증서를 신뢰 루트라고도 합니다. 이 매개변수는 **-Z** 스위치를 효과적으로 작동하게 할 수 있습니다.

-P *keyfilepw*	키 데이터베이스 암호를 지정합니다. 이 암호는 키 데이터베이스 파일(개인 키 포함)의 암호화 정보에 액세스하는 데 필요합니다. 암호 stash 파일이 키 데이터베이스 파일과 연관되면 stash 파일에서 암호를 얻을 수 있으므로 이 매개변수가 필요하지 않습니다. 이 매개변수는 **-Z** 또는 **-K**를 지정하지 않으면 무시됩니다.
-N *certificatename*	키 데이터베이스 파일에서 클라이언트 인증서와 연관된 레이블을 지정합니다. LDAP 서버가 서버 인증만 수행하도록 구성되는 경우, 클라이언트 인증서가 필요하지 않다는 사실에 주의하십시오. LDAP 서버가 클라이언트와 서버 인증을 수행하도록 구성되면 클라이언트 인증서가 필요합니다. 디폴트 인증서/개인 키 쌍이 지정된 경우에는 *certiricatename*이 없어도 됩니다. 마찬가지로 지정된 키 데이터베이스 파일에 하나의 인증서/개인 키 쌍이 있는 경우, *certificatename*이 필요하지 않습니다. 이 매개변수는 **-Z** 또는 **-K**를 지정하지 않으면 무시됩니다.

대체 입력 형식:

ldapmodify 유틸리티는 기존 유틸리티 버전과의 호환성을 유지하기 위해 대체 입력 형식을 지원합니다. 이 형식은 공백 행으로 분리되는 하나 이상의 항목으로 구성됩니다. 각 항목의 형식은 다음과 같습니다.

```
식별명(DN)
attr=value
[attr=value ...]
```

여기에서 *attr*는 속성의 이름, *value*는 값입니다. 디폴트로 값이 추가됩니다. **-r** 명령 행 플래그를 제공할 경우의 디폴트는 기존값을 신규값으로 대체하는 것입니다. 주어진 속성이 한 번 이상 나타날 수 있는 점에 유의하십시오. (예를 들면, 한 속성에 대해 둘 이상의 값을 추가할 수 있습니다.) 또한 값이 여러 행에 걸쳐서 계속되고, 값 자체에 신규 행을 보존시키기 위해 뒤에 역슬래시(\)를 사용할 수 있다는 점에도 유의하십시오. 값을 제거하려면 *attr* 값 앞에 대시(-)를 사용하십시오. 전체 속성을 제거하려면 등호(=)와 값을 생략하십시오. **-r** 플래그가 있을 때 값을 추가하려면 *attr* 앞에 더하기 부호(+)를 사용해야 합니다.

예: ldapmodify 및 ldapadd

예 1:

/tmp/entrymods 파일에 다음과 같은 내용이 있는 것으로 가정하십시오.

```
dn: cn=Modify Me, o=University of Higher Learning, c=US
changetype: modify
replace: mail
mail: modme@student.of.life.edu
-
add: title
title: Grand Poobah
-
add: jpegPhoto
jpegPhoto:< file:///tmp/modme.jpeg
-
delete: description
-
```

`ldapmodify -b -r -f /tmp/entrymods` 명령은 다음을 수행합니다.

- Modify Me 항목의 메일 속성을 `modme@student.of.life.edu`로 대체합니다.
- `Grand Poobah`를 제목으로 추가합니다.

- **/tmp/modme.jpeg** 파일의 내용을 jpegPhoto로 추가합니다.
- description 속성을 완전히 제거합니다.

기존 ldapmodify 입력 형식을 사용하여 위와 같이 수정할 수도 있습니다.

```
cn=Modify Me, o=University of Higher Learning, c=US
mail=modme@student.of.life.edu
+title=Grand Poobah
+jpegPhoto=/tmp/modme.jpeg
-description
```

기존 형식을 사용할 경우 명령은 다음과 같습니다.

```
ldapmodify -b -r -f /tmp/entrymods
```

예 2:

/tmp/newentry 파일에 다음과 같은 내용이 있는 것으로 가정하십시오.

```
dn: cn=John Doe, o=University of Higher Learning, c=US
objectClass: person
cn: John Doe
cn: Johnny
sn: Doe
title: Manager
mail: johndoe@student.of.life.edu
uid: jdoe
```

ldapadd -f /tmp/entrymods 명령은 file/tmp/newentry의 값을 사용하여 John Doe에 대한 신규 항목을 추가합니다.

예 3:

/tmp/newentry 파일에 다음과 같은 내용이 있는 것으로 가정하십시오.

```
dn: cn=John Doe, o=University of Higher Learning, c=US
changetype: delete
```

ldapmodify -f /tmp/entrymods 명령은 John Doe에 대한 항목을 제거합니다.

ldapdelete 유틸리티

ldapdelete 유틸리티를 사용하면 LDAP 디렉토리 서버에서 하나 이상의 항목을 삭제할 수 있습니다. 삭제는 OS/400의 QSH 명령 셸을 통해 실행됩니다. 이 유틸리티는 ldap_delete API(어플리케이션 프로그램 인터페이스)를 사용합니다.

형식:

ldapdelete [-V] [-M] [-n] [-v] [-c] [-R] [-C charset] [-d *debuglevel***] [-f** *file***] [-D** *binddn***] [-w** *passwd***] [-m** *mechanism***] [-O** *hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***] [**_dn_**]...**

주: *dn* 인수를 제공하지 않으면 ldapdelete 명령은 표준 입력으로부터 DN 목록을 읽기 위해 대기합니다. 대기를 중단하려면 SysReq 키를 클릭한 다음, 2. 이전 요구 종료를 선택하십시오.

진단:

오류가 발생하지 않은 경우, 나감 상태는 0입니다. 오류가 발생하면 0이 아닌 나감 상태가 되고, 진단 메세지가 표준 오류에 기록됩니다.

ldapdelete 유틸리티 사용에 관한 예를 보려면 여기를 클릭하십시오.

매개변수:

-V	유틸리티가 LDAP 서버에 바인드하기 위해 사용하는 LDAP 버전을 지정합니다. 기본적으로 LDAP 버전은 LDAP V3 연결을 사용합니다. LDAP V3을 명시적으로 선택하려면 -V 3을 지정하십시오. -V 2를 지정하여 LDAP V2 어플리케이션으로 실행하십시오.
-M	참조 오브젝트를 일반 항목으로 관리합니다.
-n	수행할 것을 표시하지만 항목을 실제로 삭제하지 않습니다. **-v**와 결합하여 디버깅에 유용합니다.
-v	표준 출력에 기록된 많은 진단을 갖고 verbose 모드를 사용합니다.
-c	연속 작업 모드. 오류가 보고되지만 ldapdelete가 삭제를 계속합니다. 디폴트는 오류 기록 후 나가는 것입니다.
-R	리퍼럴이 자동으로 뒤따르지 않도록 지정합니다.
-C *charset*	Idapdelete 유틸리티에 대한 입력으로 제공된 DN(고유명)은 로컬 문자 세트(*charset*)로 표시되도록 지정합니다. 스트링이 UTR-8로 공급되어야 하는 경우 디폴트를 대체하려면 **-C** *charset*를 사용하십시오. 입력 스트링 코드 페이지가 작업 코드 페이지 값과 다른 경우는 **-C** charset 옵션을 사용하십시오. 지원되는 *charset* 값을 참조하려면 ldap_set_iconv_local_charset() API에 대한 문서를 참조하십시오.
-d *debuglevel*	디버그 레벨을 *debuglevel*로 설정합니다.
-f *file*	*file*에서 일련의 행을 읽고, 파일의 각 행에 대하여 한 번의 LDAP 삭제를 수행합니다. 파일의 각 행에 단일 DN(고유명)이 들어 있어야 합니다.
-D *binddn*	LDAP 디렉토리를 바인드하기 위해 *binddn*을 사용합니다 *binddn*은 스트링 표현된 DN이어야 합니다.
-w *passwd*	*passwd*를 인증을 위한 암호로 사용합니다.
-m *메카니즘*	*mechanism*을 사용하여 서버에 바인드하는 데 사용되는 SASL 메카니즘을 지정합니다. ldap_sasl_bind_s() API가 사용됩니다. 사용 가능한 메카니즘은 CRAM-MD5(암호화 암호), EXTERNAL(SSL에 사용) 및 GSSAPI(Kerberos)입니다. -m 매개변수는 -V 2를 설정하면 무시됩니다. **-m**을 지정하지 않으면 간단한 인증서가 사용됩니다.
-O *hopcount*	클라이언트 라이브러리가 리퍼럴을 추적할 때 받아들이는 최대 홉 수를 설정하려면 *hopcount*를 지정하십시오. 디폴트 홉 카운트는 10입니다.
-h *ldaphost*	LDAP 서버가 실행될 대체 호스트를 지정합니다.
-p *ldapport*	LDAP 서버가 청취할 대체 전송 제어 프로토콜(TCP) 포트를 지정합니다. 디폴트 LDAP 포트는 389입니다. 포트가 지정되지 않고 **-Z**가 지정되면 디폴트 LDAP SSL 포트 636이 사용됩니다.
-Z	LDAP 서버와 통신하기 위해 보안 SSL 연결을 사용합니다. 이 툴의 SSL 작동가능 버전만이 **-Z** 옵션을 지원합니다.

-K *keyfile*	SSL 키 데이터베이스 파일의 이름을 지정합니다. 키 데이터베이스 파일이 현재 디렉토리에 없으면 완전 규정된 키 데이터베이스 파일명을 지정하십시오. 유틸리티가 키 데이터베이스를 찾을 수 없으면 기본적으로 신뢰할 수 있는 인증 기관 루트의 hard-coded 세트가 사용됩니다. 일반적으로 키 데이터베이스 파일에는 클라이언트가 신뢰하는 CAs(인증 기관)의 인증서가 하나 이상 들어 있습니다. 이러한 유형의 X.509 인증서를 신뢰 루트라고도 합니다. 이 매개변수는 **-Z** 스위치를 효과적으로 작동하게 할 수 있습니다.
-P *keyfilepw*	키 데이터베이스 암호를 지정합니다. 이 암호는 키 데이터베이스 파일(개인 키 포함)의 암호화 정보에 액세스하는 데 필요합니다. 암호 stash 파일이 키 데이터베이스 파일과 연관되면 stash 파일에서 암호를 얻을 수 있으므로 이 매개변수가 필요하지 않습니다. 이 매개변수는 **-Z** 또는 **-K**를 지정하지 않으면 무시됩니다.
-N *certificatename*	키 데이터베이스 파일에서 클라이언트 인증서와 연관된 레이블을 지정합니다. LDAP 서버가 서버 인증만 수행하도록 구성되는 경우, 클라이언트 인증서가 필요하지 않다는 사실에 주의하십시오. LDAP 서버가 클라이언트와 서버 인증을 수행하도록 구성되면 클라이언트 인증서가 필요합니다. 디폴트 인증서/개인 키 쌍이 지정된 경우에는 *certiricatename*이 없어도 됩니다. 마찬가지로 지정된 키 데이터베이스 파일에 하나의 인증서/개인 키 쌍이 있는 경우, *certificatename*이 필요하지 않습니다. 이 매개변수는 **-Z** 또는 **-K**를 지정하지 않으면 무시됩니다.
dn	하나 이상의 *dn* 인수를 지정합니다. 각 *dn*은 스트링이 표시된 DN이어야 합니다.

예: ldapdelete

다음 명령은 University of Life 조직 항목 바로 아래에 commonName Delete Me라고 명명된 항목을 삭제하려고 합니다.

```
ldapdelete cn=Delete Me, o=University of Life, c=US
```

binddn 및 *passwd*를 제공해야 할 수도 있습니다(**-D** 및 **-w** 옵션 참조).

ldapsearch 유틸리티

ldapsearch 유틸리티를 사용하면 OS/400의 QSH 명령 셸에서 LDAP 디렉토리 서버의 항목을 탐색할 수 있습니다. 이 유틸리티는 ldap_search API(어플리케이션 프로그램 인터페이스)를 사용합니다.

탐색은 LDAP 필터용 스트링 표현을 준수하는 필터를 사용합니다. LDAP 탐색 필터에 대한 자세한 정보는 iSeries Information Center의 프로그램의 OS/400 디렉토리 서비스 주제에서 ldap_search API 정보를 참조하십시오.

ldapsearch 유틸리티가 하나 이상의 항목을 찾으면 *attrs*에서 지정한 속성을 검색하고, 항목과 값을 표준 출력에 인쇄합니다. 어떤 속성도 나열하지 않은 경우, 모든 속성이 리턴됩니다.

형식:

ldapsearch [-V] [-n] [-v] [-t] [-A] [-B] [-L] [-M] [-R] [-C *charset***] [-d** *debuglevel***] [-F** *sep***] [-f** *file***] [-D** *binddn***] [-w** *bindpasswd***] [-m** *mechanism***] [-O** *hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***] [-b** *searchbase***] [-s** *scope* **] [-a** *deref***] [-l** *time limit***] [-z** *size limit***]** *filter* **[***attrs...***]**

진단:

오류가 발생하지 않은 경우, 나감 상태는 0입니다. 오류가 발생하면 0이 아닌 나감 상태가 되고, 진단 메세지가 표준 오류에 기록됩니다.

출력 형식:

ldapsearch이 하나 이상의 항목을 찾으면 각 항목을 다음과 같은 양식으로 표준 출력에 기록합니다.

```
식별명(DN)
attributename=value
attributename=value
attributename=value
...
```

복수 항목은 단일 공백 행으로 분리됩니다. 분리 문자를 지정하기 위해 **-F** 옵션을 사용하는 경우, 출력은 등호(=) 문자 대신 해당 분리 문자를 표시합니다. **-t** 옵션을 사용하는 경우에는 임시 파일명이 실제값을 대체합니다. **-A** 옵션을 지정한 경우에는 `attributename` 부분만 기록됩니다.

ldapsearch 유틸리티 사용에 관한 예를 보려면 여기를 클릭하십시오.

매개변수:

-V	유틸리티가 LDAP 서버에 바인드하기 위해 사용하는 LDAP 버전을 지정합니다. 기본적으로 LDAP 버전은 LDAP V3 연결을 사용합니다. LDAP V3을 명시적으로 선택하려면 -V 3를 지정하십시오. -V 2를 지정하여 LDAP V2 어플리케이션으로 실행하십시오.
-n	수행할 것을 표시하지만 탐색을 실제로 수행하지 않습니다. **-v**와 결합하여 디버깅에 유용합니다.
-v	표준 출력에 기록된 많은 진단을 갖고 verbose 모드를 사용합니다.
-t	검색된 값을 임시 파일 세트에 기록합니다. jpegPhoto 또는 오디오 같은 2진 값을 다루는 데 유용합니다.
-A	속성만 검색합니다(값이 없음). 단지 속성이 항목에 있는지를 알고자 하고 특정값에는 관심이 없는 경우에 유용합니다.
-B	2진 값의 표시를 억제하지 않습니다. ISO-8859.1 같은 대체 문자 세트에 나타나는 값을 다룰 때 유용합니다. 이 옵션은 **-L**에 의해 내재됩니다.
-L	탐색 결과를 LDIF 형식으로 표시합니다. 이 옵션은 **-B** 옵션도 켜게 하고, **-F** 옵션을 무시하게 합니다.
-M	참조 오브젝트를 일반 항목으로 관리합니다.
-R	리퍼럴이 자동으로 뒤따르지 않도록 지정합니다.
-C *charset*	유틸리티에 대한 입력으로 제공된 스트링은 로컬 문자 세트(*charset*)로 표시되도록 지정합니다. 스트링 입력은 필터, 바인드 DN 및 기본 DN을 포함합니다. 마찬가지로 자료를 표시할 때 ldapsearch는 LDAP 서버에서 수신한 자료를 지정된 문자로 변환합니다. 입력 스트링 코드 페이지가 작업 코드 페이지 값과 다른 경우는 **-C** charset 옵션을 사용하십시오. 지원되는 *charset* 값을 참조하려면 ldap_set_iconv_local_charset() API에 대한 문서를 참조하십시오. 또한 -C 옵션과 -L 옵션이 모두 지정되어 있으면, 입력은 지정된 문자 세트로 되어 있는 것으로 가정하는 반면 ldapsearch로부터의 출력은 언제나 UTF-8 표시로 보존되거나, 인쇄 불가능한 문자가 감지될 경우 데이터의 Base-64로 코드화된 표시로 보존됩니다. 이러한 경우는 표준 LDIF 파일에만 스트링 데이터의 UTF-8(또는 Base-64로 코드화된 UTF-8) 표시가 포함되어 있기 때문에 발생합니다.
-d *debuglevel*	디버그 레벨을 *debuglevel*로 설정합니다.
-F *sep*	속성 이름과 값 사이에 필드 분리자로 *sep*를 사용하십시오. 디폴트 분리자는 **-L** 플래그를 지정하지 않은 경우에 =이고, 지정되어 있으면 이 옵션이 무시됩니다.

-f *file*	파일에서 일련의 행을 읽고, 파일의 각 행에 대하여 한 번의 LDAP 탐색을 수행합니다. 파일의 각 행에 단일 DN(고유명)이 들어 있어야 합니다.
-D *binddn*	LDAP 디렉토리를 바인드하기 위해 *binddn*를 사용합니다. *binddn*은 스트링 표현된 DN이어야 합니다.
-w *passwd*	*passwd*를 인증을 위한 암호로 사용합니다.
-m *메카니즘*	*mechanism*을 사용하여 서버에 바인드하기 위해 사용되는 SASL 메카니즘을 지정합니다. 사용 가능한 메카니즘은 CRAM-MD5(암호화 암호), EXTERNAL(SSL에 사용) 및 GSSAPI(Kerberos) 입니다. **-m** 매개변수는 **-V** 2가 설정되어 있으면 무시됩니다. **-m**을 지정하지 않으면 간단한 인증서가 사용됩니다.
-O *hopcount*	클라이언트 라이브러리가 리퍼럴을 추적할 때 받아들이는 최대 홉 수를 설정하려면 *hopcount*를 지정하십시오. 디폴트 홉 카운트는 10입니다.
-h *ldaphost*	LDAP 서버가 실행될 대체 호스트를 지정합니다.
-p *ldapport*	LDAP 서버가 청취할 대체 전송 제어 프로토콜(TCP) 포트를 지정합니다. 디폴트 LDAP 포트는 389입니다. 포트가 지정되지 않고 **-Z**가 지정되면 디폴트 LDAP SSL 포트 636이 사용됩니다.
-Z	LDAP 서버와 통신하기 위해 보안 SSL 연결을 사용합니다. 이 툴의 SSL 작동가능 버전만이 **-Z** 옵션을 지원합니다.
-K *keyfile*	SSL 키 데이터베이스 파일의 이름을 지정합니다. 키 데이터베이스 파일이 현재 디렉토리에 없으면 완전 규정된 키 데이터베이스 파일명을 지정하십시오. 유틸리티가 키 데이터베이스를 찾을 수 없으면 기본적으로 신뢰할 수 있는 인증 기관 루트의 hard-coded 세트가 사용됩니다. 일반적으로 키 데이터베이스 파일에는 클라이언트가 신뢰하는 CAs(인증 기관)의 인증서가 하나 이상 들어 있습니다. 이러한 유형의 X.509 인증서를 신뢰 루트라고도 합니다. 이 매개변수는 **-Z** 스위치를 효과적으로 작동하게 할 수 있습니다.
-P *keyfilepw*	키 데이터베이스 암호를 지정합니다. 이 암호는 키 데이터베이스 파일(개인 키 포함)의 암호화 정보에 액세스하는 데 필요합니다. 암호 숨김 파일이 키 데이터베이스 파일과 연관되어 있는 경우, 암호는 숨김 파일로부터 얻게 되므로 이 매개변수는 필요하지 않습니다. 이 매개변수는 **-Z** 또는 **-K**를 지정하지 않으면 무시됩니다.
-N *certificatename*	키 데이터베이스 파일에서 클라이언트 인증서와 연관된 레이블을 지정합니다. LDAP 서버가 서버 인증만 수행하도록 구성되는 경우, 클라이언트 인증서가 필요하지 않다는 사실에 주의하십시오. LDAP 서버가 클라이언트와 서버 인증을 수행하도록 구성되면 클라이언트 인증서가 필요합니다. 디폴트 인증서/개인 키 쌍이 지정된 경우에는 *certiricatename*이 없어도 됩니다. 마찬가지로 지정된 키 데이터베이스 파일에 하나의 인증서/개인 키 쌍이 있는 경우, *certificatename*이 필요하지 않습니다. 이 매개변수는 **-Z** 또는 **-K**를 지정하지 않으면 무시됩니다.
-b *searchbase*	*searchbase*를 디폴트 대신 탐색용 출발점으로 사용합니다. **-b**가 지정되어 있지 않으면 이 유틸리티는 *searchbase* 정의를 위해 LDAP_BASEDN 환경 변수를 조사합니다.
-s *scope*	탐색의 범위를 지정합니다. *scope*는 기준 오브젝트, 1단계 또는 서브트리 탐색을 지정하기 위해 `base`, `one` 또는 `sub`중 하나가 되어야 합니다. 디폴트는 `sub`입니다.
-a *deref*	별명 참조 해제(dereferencing)가 수행되는 방법을 지정합니다. *deref*는 별명이 결코 참조 해제되지 않거나, 항상 참조 해제되거나, 탐색시 참조 해제되거나 탐색할 기준 오브젝트를 찾을 경우에만 참조 해제되는지를 지정하기 위해 never, always, search 또는 find 중 하나이어야 합니다. 디폴트는 별명을 결코 참조 해제하지 않는 것입니다.
-l *timelimit*	탐색이 완료될 때까지 최대 *timelimit* 초를 대기합니다.
-z *sizelimit*	탐색 결과를 최대 *sizelimit* 항목으로 제한합니다. 이것은 탐색 작업시 리턴되는 항목 수에 상한을 설정할 수 있게 됩니다.
filter	탐색시 사용하는 필터의 이름을 지정합니다.
attrs...	탐색에서 하나 이상의 항목을 찾을 경우 유틸리티가 검색하는 속성을 지정합니다. *attrs*에 어떤 값도 나열하지 않는 경우, 유틸리티는 모든 속성을 리턴합니다.

예: ldapsearch

예 1:

ldapsearch cn=john doe cn telephoneNumber 명령은 john doe의 commonName이 있는 항목의 서브트리 탐색(디폴트 탐색 기준 사용)을 수행합니다. 탐색은 commonName 값과 telephoneNumber 값을 검색하여 표준 출력으로 인쇄합니다. 탐색시 2개의 항목이 발견되면 출력이 다음과 비슷하게 보입니다.

```
cn=John E Doe, ou=College of Literature, Science, and the Arts,
ou=Students, ou=People, o=University of Higher Learning, c=US
cn=John Doe
cn=John Edward Doe
cn=John E Doe 1
cn=John E Doe
telephoneNumber=+1 313 555-5432

cn=John B Doe, ou=Information Technology Division,
ou=Faculty and Staff,
ou=People, o=University of Higher Learning, c=US
cn=John Doe
cn=John B Doe 1
cn=John B Doe
telephoneNumber=+1 313 555-1111
```

예 2:

ldapsearch -t uid=jed jpegPhoto audio 명령은 사용자 ID jed를 갖는 항목에 대해 디폴트 탐색 기준을 사용하여 서브트리 탐색을 수행합니다. 탐색은 jpegPhoto 및 오디오 값을 검색하여 임시 파일에 기록합니다. 탐색시 요구된 각 속성에 대하여 값이 하나인 항목을 찾는 경우, 출력은 다음과 비슷하게 보입니다.

```
cn=John E Doe,
ou=Information Technology Division,
ou=Faculty and Staff,
ou=People, o=University of Higher Learning, c=US
audio=/tmp/ldapsearch-audio-a19924
jpegPhoto=/tmp/ldapsearch-jpegPhoto-a19924
```

예 3:

ldapsearch -L -s one -b c=US o=university* o description 명령은 c=US 레벨에서 1단계 탐색을 수행합니다. 이 탐색은 organizationName이 university로 시작되는 모든 조직을 찾습니다. 탐색은 그 결과를 LDIF 형식으로 표시합니다. 탐색은 organizationName 속성 값과 설명 속성 값을 검색하여 다음과 비슷하게 보이는 표준 출력으로 인쇄합니다.

```
dn: o=University of Alaska Fairbanks, c=US
o: University of Alaska Fairbanks
description: Preparing Alaska for a brave new tomorrow
description: leaf node only

dn: o=University of Colorado at Boulder, c=US
o: University of Colorado at Boulder
description: No personnel information
description: Institution of education and research
```

```
dn: o=University of Colorado at Denver, c=US
o: University of Colorado at Denver
o: UCD
o: CU/Denver
o: CU-Denver
description: Institute for Higher Learning and Research

dn: o=University of Florida, c=US
o: University of Florida
o: UFl
description: Shaper of young minds
...
```

예 4:

42 페이지의 『LDAP 디렉토리 리퍼럴』에서 논의한 것처럼, 디렉토리 서비스 LDAP 디렉토리는 다음만 들어 있는 경우에는 리퍼럴 오브젝트를 포함할 수 있습니다.

- 고유명 (dn).
- objectClass (objectClass).
- 리퍼럴 (ref) 속성.

이 예는 리퍼럴 오브젝트가 포함되는 탐색을 보여줍니다.

System_A가 리퍼럴 항목을 보유하는 것으로 가정하십시오.

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
ref: ldap://System_B:389/cn=Barb Jensen,
  ou=Rochester, o=Big Company, c=US
objectclass: referral
```

해당 항목과 관련된 모든 속성은 System_B에 상주해야 합니다.

System_B에 들어 있는 항목은 다음과 같습니다.

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
cn: Barb Jensen
objectclass: organizationalPerson
sn: Jensen
telephonenumber: (800) 555 1212
```

클라이언트가 System_A에 요구를 발행하고 manageDsaIT 제어를 전송하지 않으면 서버가 참조를 리턴합니다. 예를 들어 ldapsearch에서 -M을 사용하여 System_A의 LDAP 서버가 다음 URL로 클라이언트에 응답합니다.

```
ldap://System_B:389/cn=Barb Jensen,
  ou=Rochester, o=Big Company, c=US
```

클라이언트는 System_B에 요구를 발행하기 위해 이 정보를 사용합니다. System_A의 항목에 dn, objectclass 및ref 뿐만 아니라 속성도 들어 있는 경우, 서버는 그러한 속성을 무시합니다.

클라이언트가 서버에서 리퍼럴 응답을 수신할 때, 이번에는 리턴되는 URL이 참조하는 서버에 해당 요구를 다시 발행합니다. 탐색이 한 레벨 범위로 완료되면 참조 요구에서 기본 범위를 사용합니다. 이 탐색의 결과는 탐색 범위에 대하여 지정한 값(**-b**)에 따라 달라집니다.

다음에 표시한 것처럼 `-s sub`를 지정하는 경우,

```
ldapsearch -h System_A -b ou=Rochester, o=Big Company, c=US
     -s sub sn=Jensen
```

탐색은 System_A 및 System_B의 `ou=Rochester, o=Big Company, c=US` 또는 그 아래에 상주하는 sn=Jensen이 있는 모든 항목의 모든 속성을 리턴합니다. 클라이언트는 System_A에서 참조를 수신하고 System_B를 탐색하여 `cn=Barb Jense, ou=Rochester, o=Big Company, c=US`를 리턴합니다.

다음에 표시한 것처럼 `-s one`을 지정하는 경우,

```
ldapsearch -h System_A -b ou=Rochester, o=Big Company, c=US
     -s one sn=Jensen
```

탐색은 어떤 시스템의 항목도 리턴하지 않습니다. 대신, 서버는 다음 리퍼럴 URL을 클라이언트로 리턴합니다.

```
ldap://System_B:389/cn=Barb Jensen,
  ou=Rochester, o=Big Company, c=US??base
```

그 다음에는 클라이언트가 다음 요구를 제출합니다.

```
 ldapsearch -h System_B -b cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
     -s base sn=Jensen
```

이것은 `cn=Barb Jensen, ou=Rochester, o=Big Company, c=US` 항목을 리턴합니다.

ldapmodrdn 유틸리티

ldapmodrdn 유틸리티를 사용하면 LDACP 디렉토리 서버에 있는 항목의 RDN(상대 고유명)을 변경할 수 있습니다. 이 유틸리티는 OS/400의 QSH 명령 셸에서 사용할 수 있습니다. RDN은 ldap_modrdn API(어플리케이션 프로그램 인터페이스)를 사용합니다.

형식:

ldapmodrdn [-V] [-r] [-M] [-n] [-v] [-c] [-R] [-C *charset***] [-d** *debuglevel***] [-D** *binddn***] [-w** *passwd***] [-m** *mechanism***] [-O** *hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***] [-f** *file* **] [***dn rdn***]**

주:

1. 명령 행 인수 *dn* 및 *rdn*이 주어지는 경우, *rdn*은 DN에 의해 지정되는 항목인 *dn*을 RDN으로 대체하게 합니다. 그렇지 않으면 파일의 내용(또는 **-f** 플래그가 주어지지 않은 경우, 표준 입력의 내용)은 하나 이상의 항목으로 구성되어야 합니다.

   식별명(DN)

   상대 식별명(RDN)

하나 이상의 공백 행이 각 DN/RDN 쌍을 분리합니다.

2. **-f** 옵션(또는 *dn* 및 *rdn*)을 사용함으로써 *파일*에서 항목 정보를 공급하지 않으면, ldapmodrdn 명령은 표준 입력에서 항목을 읽기 위해 대기합니다. 대기를 중단하려면 SysReq 키를 클릭한 다음, 2. 이전 요구 종료를 선택하십시오.

진단:

오류가 발생하지 않은 경우, 나감 상태는 0입니다. 오류가 발생하면 0이 아닌 나감 상태가 되고, 진단 메세지가 표준 오류에 기록됩니다.

ldapmodrdn 유틸리티의 사용에 관한 예를 보려면 여기를 클릭하십시오.

매개변수:

-V	유틸리티가 LDAP 서버에 바인드하기 위해 사용하는 LDAP 버전을 지정합니다. 기본적으로 LDAP 버전은 LDAP V3 연결을 사용합니다. LDAP V3을 명시적으로 선택하려면 -V 3을 지정하십시오. -V 2를 지정하여 LDAP V2 어플리케이션으로 실행하십시오.
-r	기존 RDN(상대 식별명) 값을 항목에서 제거합니다. 디폴트는 기존값을 보유하는 것입니다.
-M	참조 오브젝트를 일반 항목으로 관리합니다.
-n	수행할 것을 표시하지만 항목을 실제로 변경하지 않습니다. **-v**와 결합하여 디버깅에 유용합니다.
-v	표준 출력에 기록된 많은 진단을 갖고 verbose 모드를 사용합니다.
-c	연속 작업 모드. 오류가 보고되지만 ldapmodrdn은 수정을 계속하게 됩니다. 디폴트는 오류 기록 후 나가는 것입니다.
-R	리퍼럴이 자동으로 뒤따르지 않도록 지정합니다.
-C *charset*	유틸리티에 대한 입력으로 제공된 스트링은 로컬 문자 세트(*charset*)로 표시되고 반드시 UTF-8로 변환되도록 지정합니다. 입력 스트링 코드 페이지가 작업 코드 페이지 값과 다른 경우는 **-C** charset 옵션을 사용하십시오. 지원되는 *charset* 값을 참조하려면 ldap_set_iconv_local_charset() API에 대한 문서를 참조하십시오.
-d *debuglevel*	디버그 레벨을 *debuglevel*로 설정합니다.
-D *binddn*	LDAP 디렉토리를 바인드하기 위해 *binddn*을 사용합니다 *binddn*은 스트링 표현된 DN이어야 합니다.
-w *passwd*	*passwd*를 인증을 위한 암호로 사용합니다.
-m *메카니즘*	*mechanism*을 사용하여 서버에 바인드하는 데 사용되는 SASL 메카니즘을 지정합니다. ldap_sasl_bind_s() API가 사용됩니다. 사용 가능한 메카니즘은 CRAM-MD5(암호화 암호), EXTERNAL(SSL에 사용) 및 GSSAPI(Kerberos)입니다. -m 매개변수는 -V 2를 설정하면 무시됩니다. **-m**을 지정하지 않으면 간단한 인증서가 사용됩니다.
-O *hopcount*	클라이언트 라이브러리가 리퍼럴을 추적할 때 받아들이는 최대 홉 수를 설정하려면 *hopcount*를 지정하십시오. 디폴트 홉 카운트는 10입니다.
-h *ldaphost*	LDAP 서버가 실행될 대체 호스트를 지정합니다.
-p *ldapport*	LDAP 서버가 청취할 대체 전송 제어 프로토콜(TCP) 포트를 지정합니다. 디폴트 LDAP 포트는 389입니다. 포트가 지정되지 않고 **-Z**가 지정되면 디폴트 LDAP SSL 포트 636이 사용됩니다.
-Z	LDAP 서버와 통신하기 위해 보안 SSL 연결을 사용합니다. 이 툴의 SSL 작동가능 버전만이 **-Z** 옵션을 지원합니다.

-K *keyfile*	SSL 키 데이터베이스 파일의 이름을 지정합니다. 키 데이터베이스 파일이 현재 디렉토리에 없으면 완전 규정된 키 데이터베이스 파일명을 지정하십시오. 유틸리티가 키 데이터베이스를 찾을 수 없으면 기본적으로 신뢰할 수 있는 인증 기관 루트의 hard-coded 세트가 사용됩니다. 일반적으로 키 데이터베이스 파일에는 클라이언트가 신뢰하는 CAs(인증 기관)의 인증서가 하나 이상 들어 있습니다. 이러한 유형의 X.509 인증서를 신뢰 루트라고도 합니다. 이 매개변수는 **-Z** 스위치를 효과적으로 작동하게 할 수 있습니다.
-P *keyfilepw*	키 데이터베이스 암호를 지정합니다. 이 암호는 키 데이터베이스 파일(개인 키 포함)의 암호화 정보에 액세스하는 데 필요합니다. 암호 stash 파일이 키 데이터베이스 파일과 연관되면 stash 파일에서 암호를 얻을 수 있으므로 이 매개변수가 필요하지 않습니다. 이 매개변수는 **-Z** 또는 **-K**를 지정하지 않으면 무시됩니다.
-N *certificatename*	키 데이터베이스 파일에서 클라이언트 인증서와 연관된 레이블을 지정합니다. LDAP 서버가 서버 인증만 수행하도록 구성되는 경우, 클라이언트 인증서가 필요하지 않다는 사실에 주의하십시오. LDAP 서버가 클라이언트와 서버 인증을 수행하도록 구성되면 클라이언트 인증서가 필요합니다. 디폴트 인증서/개인 키 쌍이 지정된 경우에는 *certiricatename*이 없어도 됩니다. 마찬가지로 지정된 키 데이터베이스 파일에 하나의 인증서/개인 키 쌍이 있는 경우, *certificatename*이 필요하지 않습니다. 이 매개변수는 **-Z** 또는 **-K**를 지정하지 않으면 무시됩니다.
-f *file*	표준 입력 또는 명령 행(*dn* 및 신규 *rdn*를 지정하여) 대신 LDIF 파일에서 항목 수정 정보를 읽습니다. 파일(< file)에서도 표준 입력이 제공될 수 있습니다.
dn rdn	재명명할 항목의 고유명과 항목의 신규 상대 고유명을 지정하십시오.

예: ldapmodrdn

텍스트 파일 **/tmp/entrymods**을 이미 작성했고, 파일에 다음과 같은 내용이 있는 것으로 가정하십시오.

```
cn=Modify Me, o=University of Life, c=US
cn=The New Me
```

다음 명령:

```
ldapmodrdn -r -f /tmp/entrymods
```

은 Modify Me 항목의 RDN을 Modify Me에서 The New Me로 변경합니다. 기존 cn인 Modify Me는 제거됩니다.

LDAP 명령행 유틸리티에서 SSL 사용에 관한 참고사항

명령행 유틸리티의 SSL(보안 소켓층) 피처를 사용하려면, 암호 액세스 제공자 제품(5722-ACx)의 하나가 설치되어 있어야 합니다.

44 페이지의 『LDAP 디렉토리 서버에서 SSL(보안 소켓층) 및 변환층 보안 사용』은 디렉토리 서비스 LDAP 서버로 SSL을 사용하는 방법에 대해 설명합니다. 이 정보는 디지털 인증 관리자로 신뢰할 수 있는 인증 기관을 관리 및 작성하는 방법에 대해 설명합니다.

클라이언트가 액세스한 일부 LDAP 서버는 서버 인증만 사용합니다. 이러한 서버의 경우에는 인증서 점포에서 하나 이상의 신뢰되는 루트 인증서를 정의하면 됩니다. 클라이언트는 서버 인증을 통해 목표 LDAP 서버가 신뢰되는 CA(인증 기관) 중 하나에 의해 인증서를 발행했다는 것을 보장할 수 있습니다. 뿐만 아니라 서버와의

SSL 연결로 흐르는 LDAP 트랜잭션이 암호화됩니다. 여기에는 디렉토리 서버에 바인드하는 데 사용되는 API에 제공되는 LDAP Credentials가 포함되어 있습니다. 예를 들어 LDAP 서버가 높은 보장성의 Verisign 인증서를 사용 중이면 다음을 수행해야 합니다.

1. Verisign에서 CA 인증서를 얻습니다.
2. 인증서 점포로 가져오기 위한 DCM을 사용합니다.
3. 신뢰로 표시하기 위해 DCM을 사용합니다.

LDAP 서버가 개인적으로 발행한 서버 인증서를 사용 중인 경우, 서버의 관리자는 서버의 인증서 요구 파일의 사본을 제공할 수 있습니다. 인증서 요구 파일을 인증서 점포에 가져오고, 신뢰됨으로 표시하십시오.

클라이언트 인증과 서버 인증을 모두 사용하는 LDAP 서버에 액세스하기 위해 셀을 사용하는 경우에는 다음을 수행해야 합니다.

- 시스템 인증서 점포에 하나 이상의 신뢰되는 루트 인증서를 정의하십시오. 그러면 목표 LDAP 서버가 신뢰 CA 중 하나에 의해 인증서를 발행했다는 것을 클라이언트가 확신할 수 있게 됩니다. 뿐만 아니라 서버와의 SSL 연결로 흐르는 LDAP 트랜잭션이 암호화됩니다. 여기에는 디렉토리 서버에 바인드하는 데 사용되는 API에 제공되는 LDAP Credentials가 포함되어 있습니다.
- 키 쌍을 작성하고, CA에서 클라이언트 인증서를 요구하십시오. CA에서 서명된 인증서를 수신한 후 인증서를 클라이언트의 키 링 파일로 수신하십시오.

제 7 장 디렉토리 서비스 문제 해결

불행하게도, 디렉토리 서비스 LDAP 서로 같은 신뢰할만한 서버도 간혹 문제를 가지고 있습니다. LDAP 디렉토리 서버에 문제가 있으면 다음 정보를 통해 잘못된 점과 문제 해결 방법을 파악할 수 있습니다.

- 『디렉토리 서비스의 기본 문제점 해결 절차』
- 70 페이지의 『공통적인 LDAP 클라이언트 오류』

일반적인 디렉토리 서비스 문제점에 대한 추가 정보는 아래의 URL에서 디렉토리 서비스 홈 페이지 (http://www.iseries.ibm.com/ldap)를 참조하십시오.

디렉토리 서비스의 기본 문제점 해결 절차

QSYSINC/H.LDAP의 시스템에 있는 ldap.h 파일에서 LDAP 오류에 대한 리턴 코드를 찾을 수 있습니다.

LDAP 디렉토리 서버에 오류가 발생하여 자세한 내용을 보기 위해 취할 수 있는 다른 조치는 QDIRSRV 작업 기록부 열람입니다. 재작성 가능한 오류의 경우 TRCTCPAPP APP(*DIRSRV)(TCP/IP 어플리케이션 추적) 명령을 사용하여 오류 추적을 실행할 수 있습니다. 자세한 정보는 69 페이지의 『TRCTCPAPP를 사용하여 문제점 찾기』를 참조하십시오.

디렉토리 서비스는 여러 가지 SQL 서버를 사용합니다. SQL 오류가 발생하면 QDIRSRV 작업 기록부에 다음 메세지가 들어 있습니다.

```
SQL error -1 occurred
```

이 인스턴스의 경우, QDIRSRV 작업 기록부는 SQL 서버 작업 기록부를 참조합니다. 그러나, 몇몇 경우에 SQL 서버가 문제의 원인인 경우에도 QDIRSRV에 이 메세지와 이 리퍼럴이 들어 있지 않은 경우가 있습니다. 이러한 인스턴스의 경우, 시작해야 할 SQL 서버와 SQL 서버를 위해 디렉토리 서비스가 사용할 것을 아는 것이 도움이 됩니다.

LDAP 디렉토리 서버가 정상적으로 시작되면 다음과 같은 메세지가 생성됩니다.

주: 메세지 및 SQL 서버 작업의 수는 다음 중 어느 하나에 해당하는 경우에 다를 수 있습니다.

- 처음으로 서버를 시작하려고 합니다.
- 마이그레이트해야 합니다.
- 서버가 변경 기록부를 사용중입니다.
- 많은 데이터베이스 연결이 허용되도록 서버가 설정됩니다.

```
                                                          System:   WARMERS
 Job . . :   QDIRSRV       User . . :   QDIRSRV       Number . . . :   174440

  >> CALL PGM(QSYS/QGLDSVR)
     Job 057448/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057340/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057448/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057166/QUSER/QSQSRVR used for SQL server mode processing.
```

```
   Job 057279/QUSER/QSQSRVR used for SQL server mode processing.
Job 057288/QUSER/QSQSRVR used for SQL server mode processing.
   Directory Services server started successfully.
```

디렉토리 서비스는 LDAP 서버 시작 중에 첫 번째 SQL 서버인 057448/QUSER/QSQSRVR을 사용합니다. 디렉토리 서비스는 처음 서버를 시작하려고 할 때, 마이그레이트해야 하거나 서버가 변경 기록부를 사용 중인 경우, 필요에 따라 LDAP 서버를 시작하는 동안에 추가 SQL 서버를 시작할 수 있습니다. 시작 후 이 SQL 서버는 삭제됩니다.

| 이 예에서 마이그레이션이나 서버 시작을 위해 추가 SQL 서버를 사용하지 않았으며 변경 기록부가 구성되지
| 않습니다. 디렉토리 서비스는 복제의 경우에만 세 번째 SQL 서버(057340/QUSER/QSQSRVR)를 사용합니다.

| 이 예(057288/QUSER/QSQSRVR)에서 최종 연결이 add, modify, modrdn 및 delete 연산에 사용됩니다. 다
| 른 연결은 search, bind 및 compare에 사용됩니다.

iSeries Navigator의 디렉토리 서버 **데이터베이스/접미부** 등록 정보 페이지에서 디렉토리 서비스가 서버 시작 후 디렉토리 조작에 사용하는 총 SQL 서버 수를 지정합니다. 또한 하나의 SQL 서버가 항상 복제용으로 구성되어 있습니다.

디렉토리 서비스 작업 기록부에 의한 오류 및 액세스 모니터

LDAP 서버의 작업 기록부를 보면 오류에 대해 경고하고, 서버 액세스를 모니터하는 데 도움이 됩니다.

서버가 시작되면 QDIRSRV 작업 기록부를 보기 위해 다음과 같이 하십시오.

1. iSeries Navigator에서 **네트워크**를 여십시오.
2. **서버**를 여십시오.
3. **TCP/IP**를 클릭하십시오.
4. **디렉토리**에서 마우스 오른쪽 버튼을 클릭하고 **서버 작업**을 선택하십시오.
5. **파일** 메뉴에서 **작업 기록부**를 선택하십시오.

서버가 중단된 경우, QDIRSRV 작업 기록부를 보려면 다음과 같이 하십시오.

1. iSeries Navigator에서 **기본 작업**을 여십시오.
2. **프린터 출력**을 클릭하십시오.
3. QDIRSRV가 iSeries Navigator 우측 패널의 **사용자** 열에 나타납니다. 작업 기록부를 보려면, 동일한 행의 QDIRSRV 좌측에 있는 **Qpjoblog**를 두 번 클릭하십시오.

   주: iSeries Navigator는 스풀 파일만 표시하도록 구성할 수 있습니다. QDIRSRV가 리스트에 나타나지 않으면 **프린터 출력**을 클릭한 후 **옵션** 메뉴에서 **포함**을 선택하십시오. **사용자** 필드에서 **모두**를 지정한 후 **확인**을 클릭하십시오.

주: 디렉토리 서비스는 일부 타스크를 수행하기 위해 다른 시스템 자원을 사용합니다. 그 중 한 자원에서 오류가 발생하면 작업 기록부가 정보가 있는 곳을 표시하게 됩니다. 디렉토리 서비스가 찾을 곳을 판별할 수 없는 경우도 있습니다. 이런 경우에는 문제점이 SQL 서버와 관련되는지 확인하기 위해 SQL(구조화 조회 언어) 서버 작업 기록부를 보십시오.

TRCTCPAPP를 사용하여 문제점 찾기

근거리 통신망(LAN) 또는 광역 네트워크(WAN) 인터페이스와 같은 통신 회선에 대한 자료를 수집할 수 있도록 서버가 통신 추적을 제공합니다. 일반 사용자는 추적 자료의 전체 내용을 이해하지 못할 수 있습니다. 그러나 추적 항목을 사용하여 두 지점 사이에 실제로 자료 교환이 발생하는지 여부를 판별할 수 있습니다.

LDAP 디렉토리 서버에서 *DIRSRV 옵션과 함께 TRCTCPAPP(TCP/IP 어플리케이션 추적) 명령을 사용하여 클라이언트 또는 어플리케이션의 문제점을 찾도록 도울 수 있습니다.

LDAP와 함께 TRCTCPAPP 명령을 사용하는 것에 대한 자세한 정보 및 필수 권한에 대한 제한사항은 TRCTCPAPP(TCP/IP 어플리케이션 추적) 명령 설명을 참조하십시오.

통신 추적 사용에 대한 일반 정보는 통신 추적을 참조하십시오.

LDAP_OPT_DEBUG 옵션을 사용하여 오류 추적

| V5R2부터 **ldap_set_option()** API의 LDAP_OPT_DEBUG 옵션을 사용하여 LDAP C API를 사용하고 있는 클라이언트의 문제점을 추적할 수 있습니다. 디버그 옵션에는 다중 디버그 레벨 설정이 있습니다. 이것을 사용하여 이 어플리케이션에 대한 문제를 해결할 수 있습니다.

| 다음은 클라이언트 추적 디버그 옵션을 작동 가능하게 하는 예입니다.

```
| int debugvalue= LDAP_DEBUG_TRACE | LDAP_DEBUG_PACKETS;
| ldap_set_option(ld, LDAP_OPT_DEBUG, &debugvalue);
```

| 디버그 레벨을 설정하는 대체 방법은 클라이언트 어플리케이션이 실행하는 작업에 대해 LDAP_DEBUG 환경 변수의 숫자값을 **ldap_set_option()** API를 사용하는 경우의 debugvalue의 숫자값과 동일하게 구성하는 것입니다.

| LDAP_DEBUG 환경 변수를 사용하는 클라이언트 추적을 작동 가능하게 하는 예는 다음과 같습니다.

```
| ADDENVVAR ENVVAR(LDAP_DEBUG) VALUE(0x0003)
```

| 사용자에게 있는 문제점을 야기하는 클라이언트를 실행한 후 iSeries 프롬트에서 다음 사항을 입력하십시오.

```
| DMPUSRTRC  ClientJobNumber
```

| 여기에서 ClientJobNumber는 클라이언트 작업의 번호입니다.

| 이 정보를 대화식으로 표시하려면 iSeries 프롬트에서 다음 사항을 입력하십시오.

```
| DSPPFM QAPOZDMP QPOZnnnnnn
```

| 여기서 nnnnnn은 작업 번호입니다.

| 정보를 서비스에 송신하기 위해 이 정보를 저장하려면 다음 단계를 수행하십시오.

| 1. CRTSAVF(SAVE 작성) 명령을 사용하여 SAVE 파일을 작성하십시오.

2. iSeries 명령 프롬트에서 다음 사항을 입력하십시오.

   SAVOBJ OBJ(QAPOZDMP LIB(QTEMP) DEV(*SAVF) SAVF(*xxx*)

   여기에서 *xxx*는 SAVE 파일에 지정한 이름입니다.

공통적인 LDAP 클라이언트 오류

공통적인 LDAP 클라이언트 오류의 원인을 알면 서버 문제점을 해결하는 데 도움이 될 수 있습니다. LDAP 클라이언트 오류 상태의 전체 목록은 iSeries Information Center의 프로그래밍 아래에 있는 OS/400 디렉토리 서비스 주제를 참조하십시오.

클라이언트 오류 메세지는 다음 형식을 갖습니다.

```
[Failing LDAP operation]:[LDAP client API error conditions]
```

주: 이 오류에 대한 설명에서는 클라이언트가 OS/400의 LDAP 서버와 통신하고 있다고 가정합니다. 서로 다른 플랫폼의 서버와 통신하고 있는 클라이언트에서 유사한 오류가 발생할 수 있지만 원인과 해결은 다를 수 있습니다.

공통적인 메세지는 다음과 같습니다.

- 『ldap_search: 시간 제한 초과』
- 『[LDAP 작업 실패]: 작업 오류』
- 71 페이지의 『ldap_bind: 오브젝트가 없음』
- 71 페이지의 『ldap_bind: 부적절한 인증』
- 71 페이지의 『[LDAP 작업 실패]: 충분하지 않은 액세스』
- 71 페이지의 『[LDAP 작업 실패]: LDAP 서버에 접속할 수 없음』
- 71 페이지의 『[LDAP 작업 실패]: ssl 서버 연결에 실패』

ldap_search: 시간 제한 초과

이 오류는 ldapsearches가 느리게 수행할 때 발생합니다. 이 오류를 정정하기 위해 다음 중 하나 또는 모두를 수행할 수 있습니다.

- LDAP 디렉토리 서버에 대한 탐색 시간 제한을 증가시킵니다. 탐색 시간 제한 증가에 관한 정보는 35 페이지의 『LDAP 디렉토리 서버의 성능 조정』을 참조하십시오.
- 시스템 활동을 줄이십시오. 실행 중인 활동 LDAP 클라이언트 작업 수도 줄일 수 있습니다.

[LDAP 작업 실패]: 작업 오류

여러 가지 때문에 이 오류가 발생할 수 있습니다. 특정 인스턴스에 대해 이 오류의 원인에 관한 정보를 얻으려면 67 페이지의 『디렉토리 서비스의 기본 문제점 해결 절차』에서 설명한 QDIRSRV 및 SQL 서버 작업 기록부를 참조하십시오.

ldap_bind: 오브젝트가 없음

이 오류는 일반적으로 사용자가 조작을 수행할 때 입력 실수로 발생합니다. 또 다른 일반적인 원인은 LDAP 클라이언트가 존재하지 않는 DN과 바인드하려고 할 때 발생합니다. 이 오류는 사용자가 잘못 판단한 것을 관리자 DN으로 지정할 때 종종 발생합니다. 예를 들어, 사용자는 실제 관리자 DN이 cn=Administrator와 비슷할 때 QSECOFR 또는 Administrator를 지정할 수 있습니다.

오류에 대한 세부사항은 67 페이지의 『디렉토리 서비스의 기본 문제점 해결 절차』에 설명되어 있는 QDIRSRV 작업 기록부를 참조하십시오.

ldap_bind: 부적절한 인증

| 암호 또는 바인드 DN이 올바르지 않을 때 서버에서 유효하지 않은 증명서를 리턴합니다. 클라이언트가 다음 중 하나로 바인드하려고 시도할 때 서버에서 적당하지 않은 인증을 리턴합니다.

- 사용자 암호 속성이 없는 항목
- OS/400 사용자를 표시하는 항목. 이 항목에는 UID 속성이 있지만 사용자 암호 속성은 없습니다. 따라서 서로 일치하지 않는 지정된 암호와 OS/400 사용자 암호 사이에 비교가 수행됩니다.
- 요구한 샘플 이외의 프로젝트 사용자와 바인드 방법을 표시하는 항목

| 이 오류는 보통 클라이언트가 유효하지 않은 암호와 바인드하려고 할 때 발생합니다. 오류에 대한 세부사항은 67 페이지의 『디렉토리 서비스의 기본 문제점 해결 절차』에 설명되어 있는 QDIRSRV 작업 기록부를 참조하십시오.

[LDAP 작업 실패]: 충분하지 않은 액세스

이 오류는 보통 바인딩 DN에 클라이언트가 요구하는 작업(추가 또는 삭제)을 수행할 권한이 없을 때 발생합니다. 오류에 대한 정보는 67 페이지의 『디렉토리 서비스의 기본 문제점 해결 절차』에서 설명한 QDIRSRV 작업 기록부를 참조하십시오.

[LDAP 작업 실패]: LDAP 서버에 접속할 수 없음

이 오류의 가장 일반적인 원인은 다음과 같습니다.

- LDAP 클라이언트는 지정된 시스템의 LDAP 서버가 켜져서 선택 대기 상태가 되기 전에 요구합니다.
- 사용자가 유효하지 않은 포트 번호를 지정합니다. 예를 들어, 서버가 포트 386에서 청취하고 있지만 클라이언트 요구가 포트 387을 사용하려고 합니다.

오류에 대한 정보는 67 페이지의 『디렉토리 서비스의 기본 문제점 해결 절차』에서 설명한 QDIRSRV 작업 기록부를 참조하십시오. 디렉토리 서비스 서버가 성공적으로 시작한 경우, QDIRSRV 작업 기록부에 디렉토리 서비스 서버가 성공적으로 시작되었음이라는 메세지가 있습니다.

[LDAP 작업 실패]: ssl 서버 연결에 실패

이 오류는 보안 소켓 연결을 구축할 수 없기 때문에 LDAP 서버가 클라이언트 연결을 거부할 때 발생합니다. 원인은 다음과 같습니다.

- 인증 관리 지원에서 서버에 연결하려는 클라이언트의 시도를 거부합니다. 디지털 인증 관리자를 사용하여 인증서가 바르게 설정되었는지 확인한 후, 서버를 다시 시작하고 연결을 시도하십시오.
- *SYSTEM 인증 저장(기본적으로 /QIBM/userdata/ICSS/Cert/Server/default.kdb)에 대한 읽기 액세스 권한이 사용자에게 없을 수 있습니다.

OS/400 C 어플리케이션의 경우, 추가 SSL 오류 정보가 사용될 수 있습니다. 세부사항은 개별 디렉토리 서비스 API 문서를 참조하십시오.

Printed in U.S.A