관리자 설명서

Sun™ ONE Directory Proxy Server

버전 5.2

2003년 6월
817-4655-10

목차

그림 목차

설명서 정보

*관리자 설명서*에서는 Sun™ Open Net Environment (Sun ONE) Directory Proxy Server에 대한 다양한 배포 시나리오와 구성 및 유지 관리 방법에 대한 설명을 제공합니다.

이 서문은 다음 내용으로 구성되어 있습니다.

이 설명서의 사용 대상

Directory Proxy Server 관리자 설명서는 하나 이상의 서버를 구성 및 운영하는 관리자를 위해 제작되었습니다. 이 설명서에서는 사용자가 다음과 같은 배경 지식이 있는 것으로 가정합니다.

- 인터넷 및 LDAP에 대한 일반적인 지식
- Sun ONE Directory Server 5.x 및 해당 관리에 대한 일반적인 지식. 디렉토리 데이터를 읽고 수정할 수 있어야 합니다.

설명서 내용

이 설명서는 다음과 같은 세 부분으로 구성되어 있습니다.

- 1부 “Sun ONE Directory Proxy Server 소개"
- 2부 “콘솔 기반 관리"
- 3부 “부록"

표기 규칙

이 절에서는 본 설명서에 사용된 표기 규칙에 대해 설명합니다.

고정 폭 글꼴—화면에 나타나는 모든 텍스트 또는 사용자가 입력하는 텍스트에 사용됩니다. 이 글꼴은 파일 이름, 함수, 예 등에도 사용됩니다.

주	주 및 주의 사항은 중요한 정보를 나타냅니다. 작업을 계속하기 전에 해당 정보를 반드시 읽어 보십시오.

보다 큼 기호(>)는 연속적인 메뉴 선택 항목에 대한 구분 기호로 사용됩니다. 예를 들어, 객체 > 새로 만들기 > 사용자는 객체 메뉴를 표시하고 마우스를 아래쪽으로 끌어 새로 만들기를 선택한 후 새로 만들기 하위 메뉴에서 사용자를 선택해야 함을 의미합니다.

본 설명서 전체에서 다음과 같은 형태의 경로 참조 정보를 보게 될 것입니다.

```
<server-root>/dps-<hostname>/...
```

여기서 `<server-root>`는 기본 설치 디렉토리이고 `<hostname>`은 Directory Proxy Server가 설치되는 호스트 시스템의 이름입니다. 예를 들어, 설치 디렉토리가 `/usr/sunone/servers`이고 시스템의 호스트 이름이 `testmachine`일 경우 실제 경로는 다음과 같습니다.

```
/usr/sunone/servers/dps-testmachine/ . .
```

이 설명서에 지정된 모든 경로는 UNIX 형식입니다. 따라서, Windows NT 기반 디렉토리 서버를 사용할 경우 이 설명서에 UNIX 파일 경로가 표시될 때마다 NT의 해당 파일 경로를 예상해야 합니다.

관련 정보

Directory Proxy Server에는 이 설명서 외에도 다음과 같은 설명서가 포함되어 있습니다.

- **Sun ONE Directory Proxy Server 릴리스 노트.** 이 릴리스 노트에는 Directory Proxy Server의 출시 시점에 사용 가능한 중요한 정보가 들어 있습니다. 이 문서에서는 새로 추가된 기능과 향상된 기능, 알려진 문제 및 기타 최신 정보를 제공합니다. Directory Proxy Server를 시작하기 전에 이 문서를 읽어 보십시오.
- **Sun ONE Directory Proxy Server 설치 설명서.** 이 설명서에는 Directory Proxy Server 설치 절차와 요구 사항 및 조정 정보가 포함되어 있습니다.

인터넷을 통해 다음 위치에서 Sun ONE 제품에 대한 기타 유용한 정보를 참조할 수 있습니다.

- 온라인 제품 설명서—`http://docs.sun.com`
- 제품 지원 및 상태—`http://www.sun.com/service/support/software/`
- Solaris 패치 및 지원을 위한 Sun Enterprise Services—`http://www.sun.com/service/`
- 개발자 정보—`http://www.sun.com/developers/`
- 지원 및 교육—`http://www.sun.com/supportraining`
- 제품 데이터 시트—`http://www.sun.com/software/`

내게 필요한 옵션 기능

Java™ Foundation Classes (JFC)에 기반을 둔 Sun ONE Directory Proxy Server 콘솔은 장애가 있는 사용자들이 소프트웨어를 손쉽게 사용할 수 있도록 해주는 보조 소프트웨어 및 기술에 대한 지원을 제공합니다. 이 부록에서는 Sun ONE Directory Proxy Server 콘솔의 내게 필요한 옵션 기능 및 액세스 용이성을 향상시키기 위한 설명서 세트의 개선 사항에 대해 설명합니다.

콘솔의 내게 필요한 옵션 기능

다음 절에서 설명하는 대부분의 내게 필요한 옵션 기능은 JFC/Swing! 구성 요소의 사용을 통해 자동으로 제공됩니다.

액세스하기 쉬운 이름 및 설명

모든 객체는 액세스하기 쉬운 이름(객체의 용도에 대한 간결한 설명)을 갖습니다. 이러한 이름은 보조 기술을 통해 객체를 사용자에게 제공할 수 있도록 합니다. 액세스하기 쉬운 설명은 객체에 관한 추가 정보를 제공하는 보다 자세한 설명이며 필요한 시점에 제공됩니다.

사용자 정의 글꼴

텍스트 창, 메뉴, 레이블 및 정보 메시지의 글꼴 스타일과 크기를 사용자 정의할 수 있습니다.

정보 전달을 위해 색상 코딩이 사용되며 그 밖의 방법도 사용됩니다.

동적 GUI 레이아웃

동적 레이아웃은 사용자가 Directory Server 창의 크기와 위치를 지정하도록 하거나 사용자 설정에 따라 해당 창의 크기와 위치가 지정되도록 합니다.

키보드로 포커스 이동 구성 요소

이 내게 필요한 옵션 기능은 마우스 사용에 어려움이 있는 사용자들을 위한 기능입니다. 탭 키를 눌러 구성 요소 간에 입력 포커스를 이동할 수 있으며 Shift-Tab을 누르면 포커스가 반대 방향으로 이동합니다. 화살표 키를 사용하면 마우스를 사용하지 않고도 트리를 탐색할 수 있습니다.

포커스가 프로그래밍 방식으로 제공되므로 보조 소프트웨어가 포커스와 포커스 변경 사항을 추적할 수 있습니다.

텍스트 이외 요소에 대한 텍스트 대체물

이미지가 프로그램 요소를 나타낼 때, 이미지에 의해 전달되는 정보도 텍스트로 사용 가능합니다.

대체 명령줄 인터페이스

콘솔의 대부분의 기능은 명령줄에서 수행될 수 있습니다. 이 명령줄 인터페이스에 대해 자세히 설명되어 있습니다.

설명서의 내게 필요한 옵션 기능

Sun ONE Directory Proxy Server 5.2 설명서 세트는 PDF 및 HTML의 두 가지 형식으로 제공됩니다. 이 절에서는 HTML 버전 설명서의 내게 필요한 옵션 기능을 설명합니다.

텍스트 이외 요소에 대한 텍스트 대체물

대체 텍스트 레이블이 링크 또는 그래픽에 지정되어 있습니다. 그래픽이 자세한 설명을 제공하는 한편, 이러한 설명의 텍스트 버전은 주변 텍스트로 제공되거나 별도의 파일로 제공됩니다.

보조 기술로 해석 가능한 테이블

모든 테이블에 이제 설명 헤더가 포함됩니다. 테이블 내용에 대한 간략한 설명도 주변 텍스트로 제공됩니다.

Sun ONE Directory Proxy Server 소개

Sun ONE Directory Proxy Server 개요

이 장에서는 Sun ONE Directory Proxy Server 제품의 개요를 제공합니다. 이 장은 다음 내용으로 구성되어 있습니다.

소개

Sun ONE Directory Proxy Server는 전자 상거래 솔루션을 위한 디렉토리 서비스에 꼭 필요한 구성 요소입니다. Directory Proxy Server는 향상된 디렉토리 액세스 제어, 스키마 호환성 및 응용 프로그램 레이어 로드 균형 조정과 페일오버를 통한 높은 가용성을 제공하는 LDAP 응용 프로그램 레이어 프로토콜 게이트웨이입니다.

기능적으로 Directory Proxy Server는 LDAP 클라이언트와 LDAP 디렉토리 서버 사이에 위치한 "LDAP 액세스 라우터"입니다. LDAP 클라이언트의 요청을 필터링하여 Directory Proxy Server 구성에 정의된 규칙에 따라 LDAP 디렉토리 서버로 보내고 디렉토리 서버의 결과를 필터링하여 역시 Directory Proxy Server 구성에 정의된 규칙에 따라 클라이언트로 다시 전달할 수 있습니다. 이 과정은 LDAP 디렉토리 서버와 마찬가지로 Directory Proxy Server 에 연결된 LDAP 클라이언트에도 투명합니다.

Directory Proxy Server는 엑스트라넷과 인트라넷 인프라 양쪽에 다음과 같은 높은 가용성, 보안성, 클라이언트 호환성 기능을 제공하는 제품입니다.

- 자동 로드 균형 조정

- 투명한 서버 페일오버 및 페일백
- 자동 참조 따라가기
- 엑스트라넷/인트라넷 액세스 제어 그룹
- 안전한 클라이언트 및 서버 인증
- 동적 쿼리 및 응답 필터링
- 동적 스키마 매핑
- 디렉토리 기반 또는 파일 기반 구성
- 구성 가능한 로깅

Directory Proxy Server는 새로운 LDAP 디렉토리 인프라와 기존 LDAP 디렉토리 인프라와 공존하여 상호 보완 작용을 하며 기업 엑스트라넷과 인트라넷에 이미 배포되어 있는 디렉토리 사용 가능 응용 프로그램과도 완벽하게 통합되므로 고객의 기존 디렉토리 인프라를 활용하도록 배포될 수 있습니다. Directory Proxy Server는 모든 LDAP 호환 디렉토리 서버와 상호 운용되므로 Directory Proxy Server는 고유 LDAP 디렉토리, LDAP 사용 가능 X.500 디렉토리, LDAP 사용 가능 관계 데이터베이스 등 어떤 LDAP 사용 가능 디렉토리와도 함께 사용할 수 있습니다.

Directory Proxy Server는 LDAPv3 인터넷 사양을 구현하며 LDAPv2를 사용하는 이미 배포된 디렉토리 사용 가능 클라이언트 응용 프로그램과의 호환성을 위해 기능성이 다소 떨어지는 이전의 LDAPv2 사양도 지원합니다. Directory Proxy Server는 UNIX 및 Windows NT 플랫폼에서 별도의 시스템 서버 프로세스로 실행됩니다. 멀티스레드 서버는 수천 건의 LDAP 클라이언트 요청을 처리할 수 있으며 각 요청에 대해 액세스 제어 규칙과 프로토콜 필터링 규칙을 적용할 수 있습니다.

Directory Proxy Server를 사용하면 인증되지 않은 액세스로부터 기업의 사적인 디렉토리 정보를 보호하고 공개 정보를 안전하게 게시할 수 있습니다. 또한 Directory Proxy Server는 Directory Information Tree (DIT)의 각 부분에 대해 어떤 사용자가 어떤 유형의 작업을 수행할 수 있는지 제어하는 등 세분화된 LDAP 디렉토리 액세스 제어 정책을 구성할 수 있습니다. 또한 정보 수집을 위해 웹 트롤러와 로봇에 의해 주로 수행되는 특정한 작업을 허용하지 않도록 Directory Proxy Server를 구성할 수 있습니다.

Directory Proxy Server는 웹 프록시 서버와 달리 역방향 프록시 모드로 작동하므로 방화벽 내부의 클라이언트에서 인터넷 상의 임의 서버로 연결을 전달하지 않고 검색 결과를 캐시에 저장하지도 않습니다. 그 주된 이유는 액세스 제어를 데이터에 적용하는 문제 때문입니다. 현재 데이터에 대한 액세스 제어 적용은 액세스 제어가 유지 관리되는 LDAP 디렉토리 서버에서만 수행되며 Directory Proxy Server는 디렉토리 서버 액세스 제어에 관여하지 않습니다.

Directory Proxy Server 기능

Directory Proxy Server는 높은 가용성, 로드 균형 조정, 페일오버, 방화벽급 보안, 클라이언트-서버 호환성의 세 가지 기능을 제공합니다.

높은 가용성

Directory Proxy Server는 복제된 LDAP 디렉토리 서버들 간의 자동 로드 균형 조정과 자동 페일오버/페일백을 모두 제공함으로써 고가용성 디렉토리 배포를 지원하도록 디자인된 제품입니다. 엑스트라넷과 인트라넷 환경에서는 업무에 중요한 디렉토리 사용 가능 클라이언트와 응용 프로그램이 디렉토리 데이터에 하루 24시간 주 7일간 액세스할 수 있도록 보장하는 것이 필요한 경우가 많습니다. Directory Proxy Server는 인식된 모든 디렉토리 서버에 대한 연결 상태 정보를 유지 관리하며, 구성된 디렉토리 서버들 간의 비례적인 LDAP 작업 로드 균형 조정을 동적으로 수행할 수 있습니다. 한 개 이상의 디렉토리 서버를 사용할 수 없게 되면 작업 로드가 나머지 서버들 사이에 적절하게 재분배되고, 디렉토리 서버가 다시 온라인 상태로 돌아오면 작업 로드도 그에 따라 동적으로 재할당됩니다.

예를 들어, 디렉토리 서버 A에서 LDAP 클라이언트 로드의 40%를 받아들이고 서버 B, 서버 C, 서버 D에서 각각 20%씩 받아들이도록 구성된 경우를 생각해 보십시오. 디렉토리 서버 B에 장애가 발생할 경우 Directory Proxy Server에서는 서버 A가 서버 C나 서버 D의 두 배가 되는 로드를 수행하도록 구성된 것을 인식하고 서버 B의 몫인 20%의 로드를 재분배하여 이제 서버 A에서 50%, 서버 C와 서버 D에서 각각 25%씩을 처리하도록 할 것입니다. 디렉토리 서버 B가 복구되면 Directory Proxy Server에서 이를 자동으로 감지하고 4개의 서버에 구성된 원래의 로드 비율로 되돌려 놓습니다.

네트워크 레이어 IP 로드 균형 조정 장치는 LDAP 프로토콜 레이어에 대한 액세스 권한이 없습니다. 그러나 Directory Proxy Server는 로드 균형 조정 기능을 액세스 제어, 쿼리 필터링 및 쿼리 라우팅과 통합하며 지적인 응용 프로그램 레이어 액세스 제어와 LDAP 라우팅 결정을 수행할 수 있습니다.

로드 균형 조정

로드 균형 조정은 7장, "등록 정보 객체 정의 및 관리"에 설명된 로드 균형 조정 속성을 사용하여 Directory Proxy Server를 구성해야 합니다. Directory Proxy Server가 통신할 수 있는 각 백엔드 디렉토리 서버는 총 클라이언트 로드의 일정 비율을 받아들이도록 구성됩니다. Directory Proxy Server에서는 클라이언트 쿼리를 구성에 정의된 로드 기준에 맞도록 각 백엔드 서버에 분배합니다. 한 서버에 장애가 발생하면 Directory Proxy Server에서는 정해진 로드 비율에 따라 해당 서버의 로드 비율을 나머지 사용 가능한 서버에 분배합니다. 모든 백엔드 LDAP 서버를 사용할 수 없는 경우에는 Directory Proxy Server에서 클라이언트 쿼리를 거부하기 시작합니다.

Directory Proxy Server의 로드 균형 조정은 세션별로 이루어집니다. 즉 클라이언트의 쿼리가 보내질 특정 서버를 선택하는 결정 기능은 클라이언트 세션 당 한 번씩 적용됩니다. 해당 세션의 이후 모든 클라이언트 쿼리는 세션 시작 때 선택한 서버로 보내집니다.

Directory Proxy Server가 로드 균형을 조정할 수 있는 백엔드 LDAP 서버의 수는 Directory Proxy Server를 실행하는 호스트의 크기, 사용 가능한 네트워크 대역폭, Directory Proxy Server에서 받는 쿼리, 클라이언트 세션의 길이 및 Directory Proxy Server의 구성과 같은 몇 가지 요인에 따라 달라집니다. 일반적으로 대부분의 세션이 짧고 쿼리가 컴퓨터 사용면에서 집약적인 경우 Directory Proxy Server가 지원하는 서버의 수는 더 적습니다. 컴퓨터 사용면에서 집약적인 쿼리는 108페이지의 "속성 이름 바꾸기 등록 정보"에 설명된 속성 이름 바꾸기 기능이 사용될 때처럼 전체 메시지 검사가 필요한 쿼리입니다.

Directory Proxy Server는 모니터 프로세스를 사용하여 SSL을 통해서만 통신하는 것을 포함하여 백엔드 서버에 대해 상태를 점검합니다. 이 기능은 로드 균형 조정이 사용될 경우 자동으로 사용할 수 있게 됩니다. Directory Proxy Server는 각 백엔드 디렉토리 서버에 대해 매 10초마다 익명의 Root DSE 검색 작업을 수행합니다. 어느 한 서버가 사용할 수 없게 되거나 응답하지 않으면 Directory Proxy Server는 사용 중인 로드 균형 조정된 서버 집합에서 해당 서버를 제거합니다. 서버를 다시 사용할 수 있게 되면 집합에 다시 투입합니다.

페일오버

Directory Proxy Server는 연결 시도가 연결 거부 오류와 함께 반환되거나 시간이 초과되어 서버를 사용할 수 없게 될 때를 감지합니다. 이 두 경우는 세션의 초기 단계에 발생하며 그 세션에 대해 아직 어떤 작업도 처리되지 않았기 때문에 Directory Proxy Server는 다른 서버로 페일오버됩니다. 연결 시도 시간 초과인 경우 클라이언트에서 응답을 얻기까지 상당히 지연될 수 있습니다. Directory Proxy Server와 백엔드 서버 사이의 연결이 갑자기 끊어지면 Directory Proxy Server는 영향을 받는 클라이언트에 대한 모든 처리되지 않은 작업에 LDAP_BUSY 오류를 반환하고 이어서 Directory Proxy Server는 해당 클라이언트 세션을 다른 디렉토리 서버로 페일오버합니다.

Directory Proxy Server가 디렉토리 배포의 단일 실패 지점이 되는 것을 피하려면 하나의 IP 장치와 함께 최소한 두 개의 Directory Proxy Server를 사용하도록 합니다.

보안

Directory Proxy Server는 디렉토리 서버에 의해 제공되는 기본적인 액세스 제어를 향상시켜 주는 유연한 외부 디렉토리 액세스 제어 설비를 제공합니다. 이 액세스 제어 메커니즘은 여러 사용자 및 사용자 커뮤니티를 특정 액세스 그룹과 연관시켜 관리자가 정의한 보안 제한 사항과 쿼리 필터를 적용할 수 있도록 해줍니다. 관리자는 LDAP 인증 정보, IP 주소, 도메인 이름 및 기타 기준에 따라 항목에 대한 액세스를 제어할 수 있습니다.

Directory Proxy Server가 제공하는 중요한 보안 기능 중 하나는 LDAP 클라이언트와 LDAP 디렉토리 서버 사이에 설정된 연결의 수를 보호하는 것입니다. Directory Proxy Server가 동시 클라이언트 작업 수, 한 클라이언트가 연결 당 요청할 수 있는 작업 수 및 특정 클라이언트 그룹의 연결 수 등 몇 가지 특정한 측정치를 모니터하도록 구성함으로써 LDAP 디렉토리 서버를 연결 공격으로부터 보호할 수 있습니다. 또한 활동이 없는 클라이언트에 대해서는 시간 초과를 적용할 수 있습니다.

주어진 측정치를 초과하지 않도록 특정한 임계값 제한과 함께 Directory Proxy Server를 구성하면 Directory Proxy Server에서 이 측정치를 모니터하여 임계값을 초과하지 않도록 할 수 있습니다. Directory Proxy Server는 특정 호스트로부터 열려 있는 연결 수, 특정 세션에 대해 수행되는 작업 수 등 몇 가지 측정치를 계속 모니터하여 디렉토리 트롤링과 서비스 거부 공격을 받지 않도록 그 수를 제한합니다. 이러한 매개 변수 구성에 대한 자세한 설명은 65페이지의 “시스템 구성 인스턴스 만들기”를 참조하십시오.

Directory Proxy Server는 또한 (cn=A*) 또는 (cn>A)와 같은 일정한 종류의 필터를 허용하지 않음으로써 트롤링을 제한합니다. 필터의 필터링 구성 방법에 대한 자세한 내용은 6장, “그룹 만들기 및 관리“를 참조하십시오.

Directory Proxy Server는 인증받은 클라이언트가 디렉토리 서비스에 대한 액세스 제어를 변경하도록 허용합니다. 따라서 인증받은 클라이언트는 보안 네트워크 외부에 있더라도 디렉토리 정보에 대해 보다 큰 액세스 권한을 가질 수 있습니다.

Directory Proxy Server는 Secure Socket Layer (SSL) 전송 프로토콜을 지원함으로써 데이터 보호를 제공합니다. 예를 들면 보호되는 네트워크 외부에서 디렉토리 서비스로 액세스하는 모든 클라이언트에 SSL 세션 설정이 필요하도록 Directory Proxy Server를 구성할 수 있습니다. Directory Proxy Server에서의 SSL 구성에 대한 자세한 내용은 157페이지의 “보안 구성”을 참조하십시오.

이러한 기능들을 사용하면 빈번히 발생하는 "서비스 거부" 공격과 "대량 유입 공격"을 방지할 수 있습니다. Directory Proxy Server는 임계값에 도달했음을 감지하면 디렉토리 서버에 대한 연결을 거부하기 시작하여 디렉토리 서버가 공격받는 것을 방지합니다.

클라이언트-서버 호환성

Directory Proxy Server는 인증 자격 증명에 따라 모바일 사용자를 식별하는 것을 포함하여 LDAP Distinguished Name (DN) 및 그룹 액세스 권한에 따라 쿼리 라우팅 결정을 내립니다. Directory Proxy Server는 확장성이 큰 분산된 디렉토리 서비스를 지원하여 디렉토리 서버에 의해 반환되는 LDAP 참조를 자동으로 따라갑니다. 자동 참조 따라가기는 일련의 디렉토리 서버들 사이에 실제로 디렉토리 정보를 분산시켜야 하지만 분산된 디렉토리를 사용자에게 하나의 논리적인 디렉토리로 표시해야 하는 대규모 디렉토리 배포에 매우 유리합니다. Directory Proxy Server는 확장 가능한 분산된 디렉토리 서비스를 지원하여 분산된 디렉토리 데이터를 논리적으로 통합하는 능력을 제공함으로써 이러한 배포 시나리오를 지원합니다.

Directory Proxy Server는 LDAPv2 또는 LDAPv3을 준수하는 클라이언트 응용 프로그램을 지원합니다. 디렉토리 서버의 스키마와 항상 일치하는 것은 아닌 고정된 스키마를 사용하는 클라이언트 응용 프로그램을 수용하도록 스키마를 다시 작성할 수 있습니다. 예를 들어 Microsoft Outlook™ 전자 메일 클라이언트는 디렉토리 서버가 기업의 보다 일반적인 스키마 요구 사항과 일치하지 않을 수 있는 Microsoft 정의 속성을 구현할 것을 기대합니다. 스키마 재작성 기능을 사용하여 디렉토리 시스템 관리자는 일반적인 목적의 기업 스키마를 구현하고

그 스키마의 특정 요소를 클라이언트 응용 프로그램에서 요구하는 일련의 속성 유형에 동적으로 매핑할 수 있습니다. Directory Proxy Server는 RFC1274, X.520, X.521, LIPS, PKIX, inetOrgPerson 및 DEN을 비롯한 기본적이고 *특별한* 업계의 스키마 정의에 정해진 속성 유형과 객체 클래스를 모두 받아들입니다.

2장

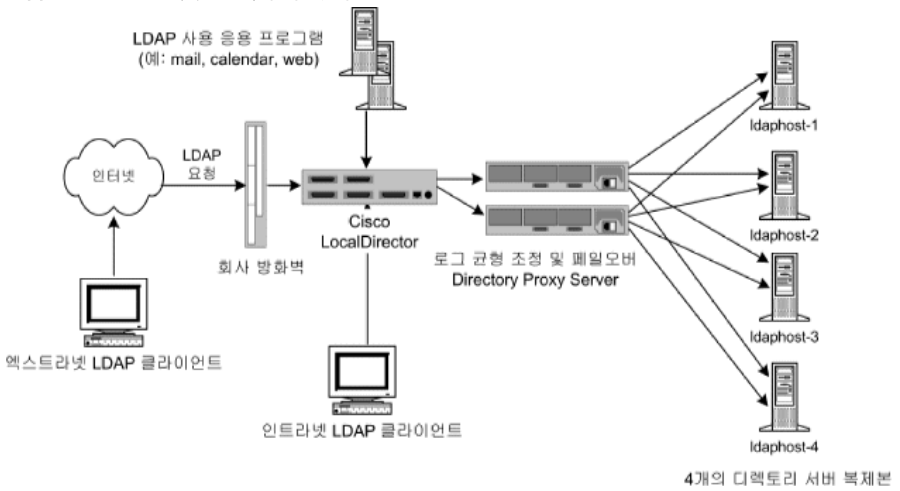
Sun ONE Directory Proxy Server 배포 시나리오

Sun ONE Directory Proxy Server는 컴퓨팅 환경에 따라 여러 가지 방법으로 배포될 수 있습니다. 이 장에서는 다음을 포함하여 일반적인 배포에 대해 설명합니다.

내부 고가용성 구성

그림 2-1에 표시된 구성의 경우 고객이 LDAP 인프라를 회사 내부용으로 배포했습니다. 따라서 이 구성에는 회사 LDAP 서비스에 대한 외부 네트워크 액세스 요구 사항이 없습니다. 이 고객은 방화벽 외부에서 시도되는 내부 LDAP 서비스에 대한 액세스를 거부하도록 회사 방화벽을 배포했습니다. 고가용성을 위해 내부에서 초기화된 모든 클라이언트 LDAP 요청 역시 Cisco LocalDirector를 통해 Directory Proxy Server를 통과해야 합니다. 여기에서 Cisco LocalDirector는 클라이언트가 하나 이상의 Directory Proxy Server에 대한 액세스 권한이 있음을 확인하는 IP 패킷 전환의 예로만 표시됩니다. 이 고객은 Sun ONE Directory Proxy Server를 실행하는 호스트를 제외한 모든 사용자가 디렉토리 서버에 직접 액세스하지 못하도록 금지합니다. 방화벽을 배포하여 직접 액세스를 금지하면 디렉토리 서버 및 Directory Proxy Server를 실행하는 호스트를 보호할 수 있습니다.

그림 2-1 내부 고가용성 구성



분산 LDAP 디렉토리 인프라

다음 절에서는 분산 LDAP 디렉토리 인프라에서의 Directory Proxy Server의 역할에 대해 설명합니다.

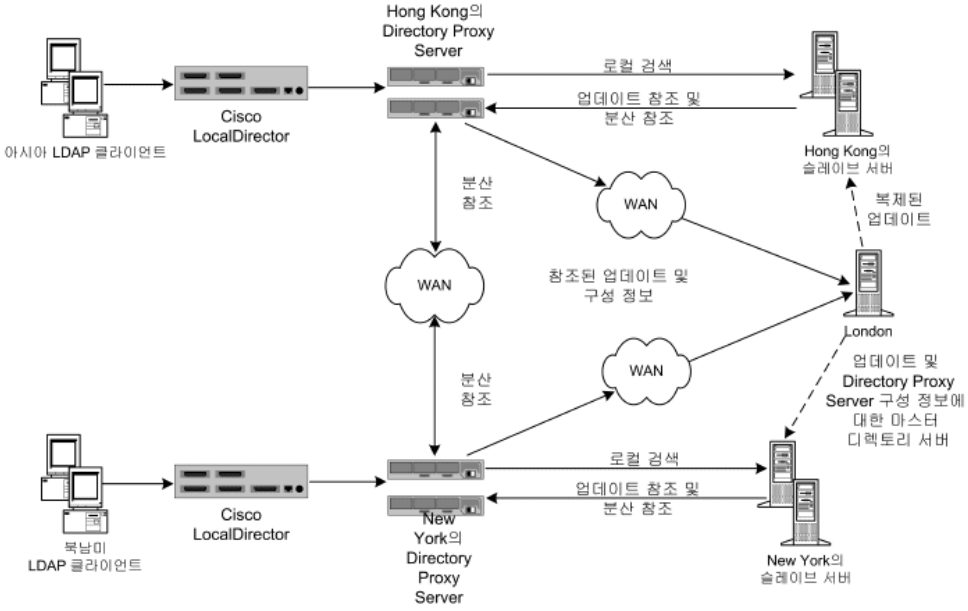
- 고객 시나리오
- 고객 배포
- LDAP 요청 흐름

고객 시나리오

그림 2-2의 구성에 표시된 대형 금융 기관은 London에 본사를 두고 London, New York 및 Hong Kong에 데이터 센터를 가지고 있습니다. 현재 직원들이 사용할 수 있는 대부분의 데이터는 London의 레거시 RDBMS 저장소에 집중되어 있습니다. 이 금융 기관의 클라이언트 커뮤니티는 항상 WAN (Wide Area Network)을 통해 이 데이터에 액세스합니다. 이 회사는 집중화된 모델의 확장성 및 성능 문제에 직면하여 분산 데이터 모델로 전환하고, 동시에 LDAP 디렉토리 인프라를 배포하기로 결정했습니다. 문제의 데이터는 "미션 크리티컬" 데이터로 간주되기 때문에 가용성이 높은 내결함성 인프라에 배포되어야 합니다. 클라이언트 응용 프로그램 프로필

분석을 통해 데이터는 고객을 기반으로 하기 때문에 지리적으로 분포한 클라이언트 커뮤니티에서 액세스하는 데이터의 95%가 해당 커뮤니티에 한정된다는 사실을 밝혀냈습니다. 즉, 아시아의 클라이언트가 북아메리카의 고객 데이터에 액세스할 수는 있지만 그런 일은 극히 드물게 발생하는 현상입니다. 또한 클라이언트 커뮤니티는 고객 정보를 자주 업데이트해야 합니다.

그림 2-2 분산 LDAP 디렉토리 인프라



고객 배포

이 금융 회사는 프로필을 통해 데이터 액세스의 95%가 해당 지역의 데이터에 한정된다는 사실을 확인하고 자사의 LDAP 디렉토리 인프라를 지역적으로 분산하기로 결정했습니다. 그 결과 다중 디렉토리 고객 서버를 각 지역(예: Hong Kong, New York 및 London, London 고객 서버는 다이어그램에 표시 안 됨)에 배포했습니다. 해당 지역의 고객 데이터는 각 고객 서버에 보관하도록 구성되어 있습니다. 즉, 유럽과 중동 지역의 고객 데이터는 London 고객 서버에 보관되고, 북아메리카와 남아메리카 지역의 고객 데이터는 New York 고객 서버에 보관되고, 아시아 환태평양 지역의 고객 데이터는 Hong Kong 고객 서버에 보관됩니다. 이 배포에는 로컬 클라이언트 커뮤니티의 압도적인 데이터 요구 사항이 해당 커뮤니티에 있습니다. 이 배포에서는 클라이언트 요청을 로컬로 처리하여 네트워크 오버헤드를 줄이고, 각 디렉토리 서버에

디렉토리 인프라를 효과적으로 분할하여 향상된 디렉토리 서버 성능과 확장성을 제공하기 때문에 집중화된 모델에 비해 성능 향상이 두드러집니다. 각 고객 디렉토리 서버는 클라이언트가 업데이트 요청을 제출하거나 다른 지역의 데이터를 검색 요청할 경우 참조를 반환하도록 구성되어 있습니다.

LDAP 요청 흐름

클라이언트 LDAP 요청은 Cisco LocalDirector를 통해 Sun ONE Directory Proxy Server로 보내집니다. 여기에 표시된 LocalDirector 제품은 클라이언트가 항상 하나 이상의 Directory Proxy Server에 액세스할 수 있는 권한을 갖는지를 확인하는 IP 패킷 전환의 예로만 제공됩니다. 로컬로 배포된 Directory Proxy Server는 로컬 고객 데이터가 보관된 로컬 디렉토리 서버 배열에 모든 요청을 라우팅합니다. Directory Proxy Server 인스턴스는 디렉토리 서버 배열을 통해 로드 균형을 조정하여 자동 페일오버 및 페일백을 제공하도록 구성되어 있습니다. 로컬 고객 정보에 대한 클라이언트 검색 요청은 로컬 디렉토리에서 처리되며 해당 응답은 Directory Proxy Server를 통해 클라이언트에게 반환됩니다. "외부"(지리적) 고객 정보에 대한 클라이언트 검색 요청은 로컬 디렉토리 서버에서 Directory Proxy Server로 참조를 다시 반환하여 처리됩니다.

이 참조에는 지리적으로 적절히 분산된 Directory Proxy Server 인스턴스를 가리키는 LDAP URL이 포함되어 있습니다. 로컬 Directory Proxy Server는 로컬 클라이언트 대신 참조를 처리하여 분산된 해당 Directory Proxy Server 인스턴스에 검색 요청을 보냅니다. 분산 Directory Proxy Server는 검색 요청을 분산 디렉토리 서버로 전달하고 해당 응답을 받습니다. 그런 다음 이 응답을 Directory Proxy Server의 분산 인스턴스 및 로컬 인스턴스를 통해 로컬 클라이언트에 반환합니다.

로컬 Directory Proxy Server가 받은 업데이트 요청 또한 로컬 디렉토리 서버에서 반환된 참조를 기준으로 처리됩니다. 또한 Directory Proxy Server는 로컬 클라이언트를 대신하여 참조를 따르지만 이 경우에는 업데이트 요청을 London에 있는 공급업체 디렉토리 서버에 전달합니다. 공급업체 디렉토리 서버는 공급업체 데이터베이스에 업데이트를 적용한 다음 로컬 Directory Proxy Server를 통해 로컬 클라이언트에 응답을 보냅니다. 공급업체 디렉토리 서버는 업데이트를 해당 고객 디렉토리 서버로 전파합니다.

모든 Sun ONE Directory Proxy Server는 시작한 다음 공급업체 디렉토리 서버에서 해당 구성을 조사하도록 구성되어 있습니다. 이렇게 하면 여러 Directory Proxy Server 인스턴스를 지리적으로 분산할 수 있습니다. 이 경우에도 해당 구성은 집중 방식으로 관리됩니다.

집중 LDAP 디렉토리 인프라

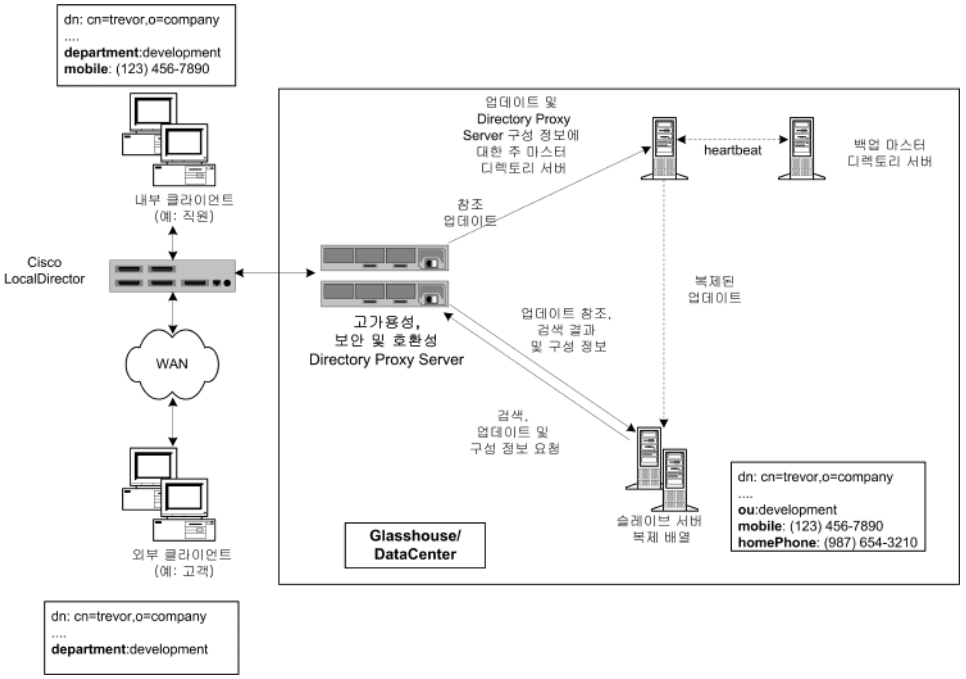
다음 절에서는 집중 LDAP 디렉토리 인프라에서 Directory Proxy Server의 역할에 대해 설명합니다.

- 고객 시나리오
- 고객 배포
- LDAP 요청 흐름

고객 시나리오

그림 2-3에서는 고객과 직원이 전세계에 분산되어 있는 대형 글로벌 기업에 대해 설명합니다. 이 회사에서는 회사 화이트 페이지 및 옐로우 페이지(전자 전화 번호부)를 배포하여 전화 번호부 인쇄비를 줄이고, 회사 정보의 정확도를 높이고, 환경 자원의 사용을 줄이려고 합니다. 화이트 페이지 및 옐로우 페이지 정보는 해당 액세스 권한이 있는 고객과 직원이 모두 사용할 수 있어야 합니다. 고객과 직원이 전세계의 모든 시간대에 분산되어 있기 때문에 이러한 정보는 24시간 연중무휴로 사용 가능하고 미션 크리티컬로 분류되어야 합니다.

그림 2-3 집중 LDAP 디렉토리 인프라



고객 배포

글로벌 기업에서 집중 LDAP 디렉토리 인프라를 배포하여 화이트 페이지 및 옐로우 페이지의 배포를 지원하기로 결정했습니다. 화이트 페이지 및 옐로우 페이지는 회사 직원 전용이기 때문에 이 인스턴스에서 집중 배포를 선택했습니다. 이 데이터베이스는 고객이 일부 정보에 액세스할 수 있지만 고객 데이터베이스가 아닙니다. 확장성과 성능이 고려되지 않았기 때문에 데이터베이스의 프로젝트 크기(~200,000 항목)가 부족하여 이보다 복잡한 분산 배포 모델은 요청할 수 없습니다.

고가용성 요구 사항으로 인해 이 회사는 단일 공급업체 디렉토리 서버에서 제공하는 다중 고객 디렉토리 서버 복제본을 배포하기로 결정했습니다. 단일 공급업체 디렉토리 서버에서 발생되는 단일 사고점을 제거하기 위해 이 회사는 백업 공급업체 디렉토리 서버를 배포했습니다.

Sun ONE Directory Proxy Server는 세 가지 이유로 배포되었습니다. 첫째, 모든 LDAP 클라이언트와 디렉토리 서버 복제본 배열 간의 로드 균형 조정 및 자동 페일오버/페일백을 제공합니다. 둘째, 외부 클라이언트와 내부 클라이언트를 구별하고 해당 액세스 권한을 설정할 수 있습니다. 셋째, 화이트 페이지 및 옐로우 페이지를 사용하는 LDAP 클라이언트와 디렉토리 서버 간의 호환성을 제공합니다. LDAP 클라이언트는 사용자 작성 화이트 페이지 및 옐로우 페이지 응용 프로그램뿐만 아니라 고정 스키마 요구 사항에 부합하는 많은 기성 LDAP 사용 응용 프로그램을 사용합니다. 이러한 스키마 요구 사항이 회사에서 설계한 디렉토리 스키마와 항상 일치하는 것은 아니기 때문에 일부 기본 스키마 속성을 매핑해야 합니다. 또한 클라이언트가 사용하는 모든 LDAP 사용 응용 프로그램이 디렉토리 서버로부터 받은 참조를 올바르게 처리할 수 있는 것은 아닙니다. Sun ONE Directory Proxy Server는 클라이언트를 대신하여 이러한 참조를 따르도록 구성되었습니다.

LDAP 요청 흐름

보낸 사람이 내부 클라이언트인지 외부 클라이언트인지 여부와 검색 요청인지 업데이트 요청인지 여부에 관계 없이 모든 클라이언트 요청은 Cisco LocalDirector를 통해 Directory Proxy Server 인스턴스로 보내집니다. 여기에 표시된 LocalDirector 제품은 클라이언트가 항상 하나 이상의 Directory Proxy Server에 액세스할 수 있는 권한을 갖는지를 확인하는 IP 패킷 전환의 예로만 제공됩니다. 단일 사고점이 발생하지 않도록 여러 Directory Proxy Server 인스턴스를 배포합니다. Directory Proxy Server 인스턴스는 클라이언트로부터 받은 모든 요청을 배열에 있는 모든 고객 디렉토리 서버로 분산하여 로드 균형을 조정합니다. 또한 Directory Proxy Server는 고객 서버의 실패를 감지하여 배열 내의 사용 가능한 고객 서버에 페일오버합니다.

고객 서버는 읽기 전용 복제본이기 때문에 클라이언트로부터 업데이트 요청을 받을 경우 LDAP 참조를 반환하도록 구성됩니다. 이 참조에는 공급업체 디렉토리 서버를 가리키는 LDAP URL이 포함되어 있습니다. 디렉토리 서버가 참조를 반환하면 Directory Proxy Server는 참조를 인식하여 클라이언트 대신 해당 참조를 따릅니다. 그런 다음 공급업체 디렉토리 서버에 바인드하여 업데이트 요청을 보냅니다. 공급업체 디렉토리 서버는 공급업체 데이터베이스에 업데이트를 적용한 다음 Directory Proxy Server를 통해 클라이언트에 응답을 보냅니다. 공급업체 디렉토리 서버는 업데이트를 해당 고객 디렉토리 서버로 전파합니다.

클라이언트가 보낸 검색 요청은 Directory Proxy Server를 통해 고객 디렉토리 서버 복제 배열에 라우팅됩니다. 검색 요청을 디렉토리 서버에 보내기 전에 "검사"하여 특정 클라이언트 그룹에 대해 구성된 액세스 제어 및 보안 규칙에 맞지 않는 요청을 필터링하고 필요한 매핑을 수행하도록 Sun ONE Directory Proxy Server를 구성할 수 있습니다. 또한 디렉토리 서버에서 반환되는 검색 결과를 "검사"하여 해당 필터링 및 매핑을 다시 수행하도록 Directory Proxy Server를 구성할 수 있습니다. 그림 2-3에 표시된 예에서 내부 클라이언트와 외부 클라이언트가 모두 "Trevor"에 속하는 항목에 대한 검색을 요청했습니다. 이러한 인바운드 요청은 클라이언트 유형에 관계 없이 Directory Proxy Server에서 동일하게 처리됩니다. 디렉토리 서버는 요청을

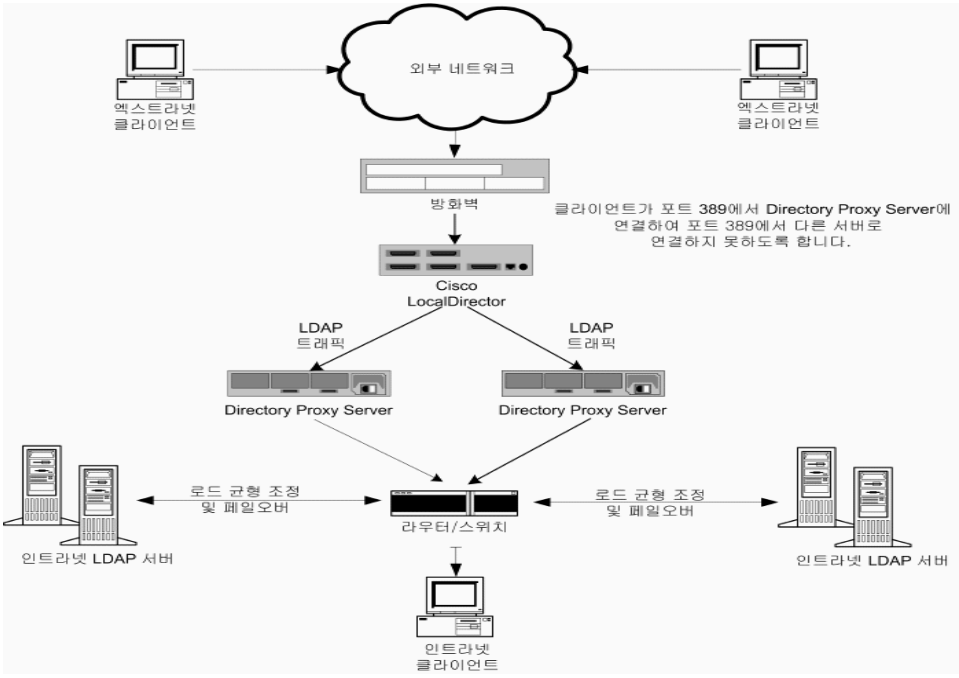
성공적으로 실행하고 "Trevor"에 대한 항목을 Directory Proxy Server에 다시 반환합니다. Directory Proxy Server는 원본 요청을 보낸 사람이 내부 클라이언트인지 외부 클라이언트인지에 따라 검색 결과를 다르게 조작하도록 구성되어 있습니다. 외부 클라이언트의 경우에는 휴대 전화 번호 필드와 집 전화 번호 필드가 모두 고객에게 부적합한 데이터이기 때문에 필터링됩니다. ou: development 속성/값 쌍이 department: development에 매핑되었습니다. 클라이언트가 디렉토리에 액세스하는 데 사용하는 응용 프로그램(예: Outlook, Outlook Express) 중 하나에 회사 디렉토리 서버에 배포된 스키마 엘리먼트와 일치하지 않는 고정 스키마 요소가 있기 때문에 이 과정이 필요합니다. 내부 클라이언트의 경우에는 휴대 전화 번호는 직원 간에 공유할 중요한 데이터 요소이지만 집 전화 번호는 중요한 데이터 요소가 아닙니다. 따라서 내부 클라이언트의 경우 집 전화 번호만 필터링하고 클라이언트가 휴대 전화 번호는 볼 수 있도록 Directory Proxy Server를 구성합니다. ou 속성의 동일한 매핑이 department 속성에도 수행됩니다.

모든 Sun ONE Directory Proxy Server는 시작한 다음 공급업체 디렉토리 서버에서 해당 구성을 조사하도록 구성되어 있습니다. 그렇게 하면 여러 Directory Proxy Server 구성을 한 디렉토리에서 집중 관리할 수 있습니다.

단일 방화벽이 있는 Directory Proxy Server 배포

LDAP 클라이언트만 Directory Proxy Server가 실행 중인 시스템 및 포트에 액세스할 수 있도록 허용하려면 조직의 방화벽을 그림 2-4에 표시된 것처럼 구성해야 합니다. 일반적으로 LDAP 클라이언트는 TCP 포트 389에 연결합니다. 여기서는 액세스 권한이 없는 클라이언트가 무단으로 액세스하지 못하도록 Directory Proxy Server를 실행하는 호스트를 보호합니다. 또한 라우터 스위치를 사용하여 프록시 서버를 실행하는 호스트를 자체 LAN에 배치하여 불필요한 트래픽으로 네트워크 용량 초과 등과 같은 서비스 거부(DoS) 공격으로부터 내부 네트워크를 보호합니다. 방화벽은 LDAP가 LDAP Directory Server에서 "숨겨진" 시스템 및 포트에 액세스하지 못하게 하여 LDAP 디렉토리 데이터베이스를 보호해야 합니다.

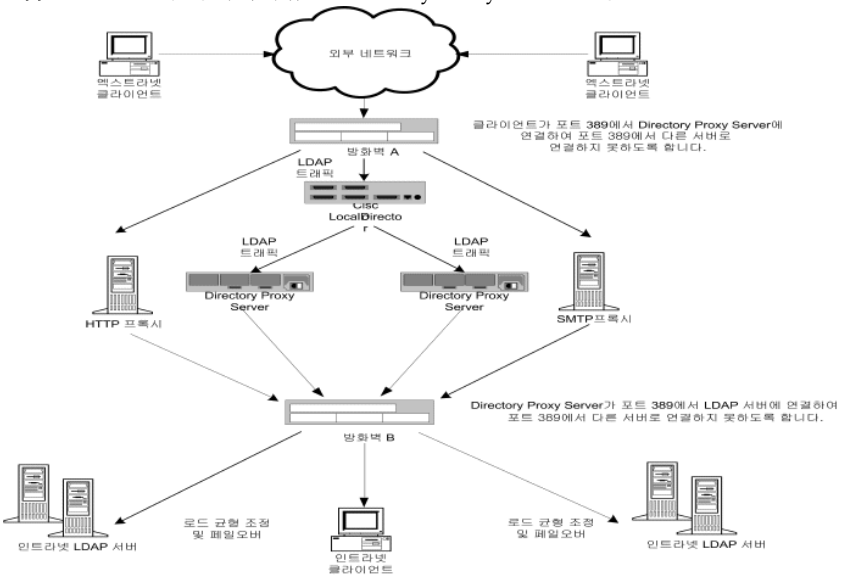
그림 2-4 단일 방화벽이 있는 Directory Proxy Server 설정



두 방화벽이 있는 Directory Proxy Server 배포

그림 2-5에 표시된 구성은 그림 2-4에 표시된 구성의 모든 장점을 가지며 몇 가지 추가 보안을 제공합니다. 사이트 관리자가 외부 네트워크로부터의 트래픽을 제한할 수 있도록 두 방화벽을 설치하여 "프록시" 주위에 통제 영역을 만듭니다. 또한 "프록시" 서버 중 하나를 손상시켜 내부 네트워크에 있는 다른 시스템을 직접 공격할 수 없습니다. 방화벽 A는 대상 IP 주소가 해당 TCP 또는 UDP 프로토콜을 처리하는 프록시의 IP 주소일 경우 들어오는 패킷만 허용하도록 구성되어 있습니다. 방화벽 B는 프록시가 액세스하는 데 필요한 서버에 해당하는 프록시 시스템에서 가져온 패킷만 허용하도록 구성되어 있습니다.

그림 2-5 두 방화벽이 있는 Directory Proxy Server 설정



콘솔 기반 관리

3장, “Directory Proxy Server 콘솔 소개“

4장, “Directory Proxy Server 시작, 다시 시작 및 중지“

5장, “시스템 구성 인스턴스 만들기“

6장, “그룹 만들기 및 관리“

7장, “등록 정보 객체 정의 및 관리“

8장, “이벤트 객체 만들기 및 관리“

9장, “작업 객체 만들기 및 관리“

10장, “로그 구성 및 모니터링“

11장, “보안 구성“

Directory Proxy Server 콘솔 소개

Sun ONE Directory Proxy Server를 설치한 후 디렉토리 배포 기능을 사용하도록 구성한 다음 해당 작업을 자세히 모니터합니다. Directory Proxy Server 관리 작업에는 서버 시작, 중지 및 다시 시작, 그룹 만들기, 특정 이벤트를 식별하고 해당 작업을 실행하도록 서버 설정, 구성 변경, 일상적인 서버 유지 관리 작업 수행, 로그 모니터 등과 같은 서버 관련 작업이 포함됩니다.

이러한 서버 관련 작업을 빠르고 쉽게 수행할 수 있도록 Directory Proxy Server는 *Directory Proxy Server 서버 콘솔*및 *Directory Proxy Server 구성 편집기 콘솔*이라는 GUI 기반 관리 도구를 제공합니다. 두 도구 모두 콘솔 내에서 액세스할 수 있습니다. 이 장에서는 Sun ONE 및 Directory Proxy Server 콘솔에 대한 개요를 제공합니다.

이 장은 다음 내용으로 구성되어 있습니다.

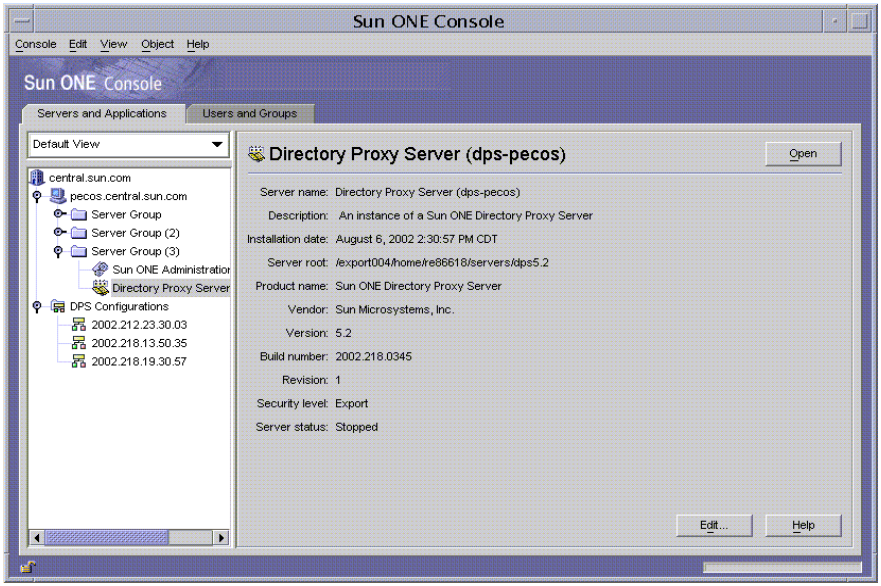
주 Sun ONE Console에서는 다양한 네트워크 자원을 관리할 수 있습니다. 이 장에서는 Sun ONE Console을 사용하여 Directory Proxy Server를 관리하는 작업에 대해서만 중점적으로 설명합니다. Sun ONE Console에 대한 자세한 내용은 Directory Proxy Server 설명서와 함께 제공되는 *Managing Servers with Sun ONE Console*을 참조하십시오. `http://docs.sun.com/`에서도 이 설명서의 복사본을 구할 수 있습니다.

Sun ONE Console 시작

Sun ONE Console은 조직의 *구성 디렉토리*에 등록된 모든 네트워크 자원에 GUI 기반 프런트엔드를 제공하는 독립 실행형 Java 응용 프로그램입니다. 이 통합 관리 인터페이스는 네트워크를 통해 설치된 모든 Sun ONE 5.x 버전 서버 인스턴스에 액세스 지점을 제공하여 네트워크 관리를 단순화합니다. 또한, 사용자 디렉토리에 통합 관리 인터페이스를 제공하여 기본 사용자 및 그룹 관리를 단순화합니다.

그림 3-1은 Sun ONE Console의 "서버 및 응용 프로그램" 탭에서 Directory Proxy Server 인스턴스가 선택된 상태를 보여줍니다.

그림 3-1 Sun ONE Console: 서버 및 응용 프로그램 탭



서버 및 응용 프로그램 탭

Sun ONE Console의 모든 인스턴스의 경우, 해당 인스턴스에서 관리할 수 있는 네트워크 제한은 동일한 구성 디렉토리에 구성 정보가 저장되는 자원 집합 즉, Sun ONE Console에서 모니터할 수 있는 최대 호스트 및 서버 집합에 의해 정의됩니다. *수퍼관리자*(구성 디렉토리를 관리하는 사람)는 구성 디렉토리에 등록된 모든 네트워크 자원에 대한 액세스 권한을 설정할 수 있습니다. 따라서, Sun ONE Console을 사용하는 관리자의 경우 수퍼관리자가 설정한 액세스 권한에 따라 실제로 표시되는 호스트 및 서버 수가 더 적을 수 있습니다.

"서버 및 응용 프로그램" 탭은 특정 구성 디렉토리에 등록된 모든 서버를 표시하여 사용자가 제어할 수 있는 모든 서버 소프트웨어 및 자원에 대한 통합된 뷰를 제공합니다. 제어할 수 있는 항목은 수퍼관리자가 설정한 액세스 권한에 따라 결정됩니다.

이 뷰에서 임의의 그룹 또는 서버 클러스터 작업을 한 번에 수행할 수 있습니다. 즉, "서버 및 응용 프로그램" 탭을 사용하여 단일 서버나 한 시스템의 서로 다른 포트에 설치되는 여러 서버를 관리할 수 있습니다. 또한, 해당 서버 인스턴스 항목(SIE)의 아이콘을 두 번 눌러 개별 서버 콘솔 또는 관리 인터페이스에 액세스할 수 있습니다.

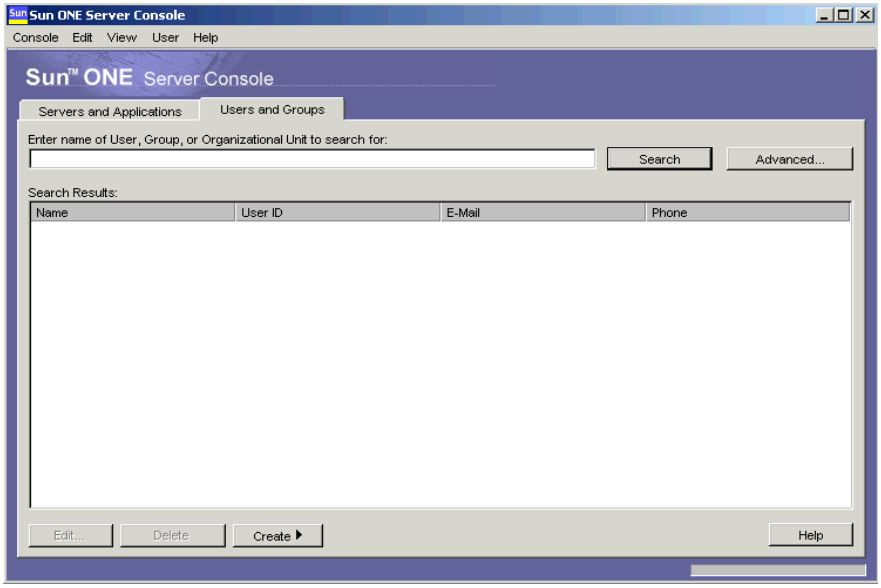
"서버 및 응용 프로그램" 탭에서 다음과 같은 다양한 Directory Proxy Server 관련 작업을 수행할 수 있습니다.

- Directory Proxy Server 서버 콘솔 시작
- Directory Proxy Server 구성 편집기 콘솔 시작(Directory Proxy Server 그룹을 구성할 수 있음)
- Directory Proxy Server에 대한 액세스 권한 설정
- Administration Server Console 시작(Directory Proxy Server 관리를 위해 Administration Server 인스턴스를 구성할 수 있음)

사용자 및 그룹 탭

"사용자 및 그룹" 탭(그림 3-2 참조)에서는 개별 사용자 및 그룹에 대한 사용자 계정, 그룹 목록 및 액세스 제어 정보를 관리합니다. Sun ONE Console 프레임워크에 등록된 모든 응용 프로그램은 회사 차원 사용자 데이터를 위한 전역 디렉토리인 사용자 디렉토리에 있는 핵심 사용자 및 그룹 정보를 공유합니다.

그림 3-2 Sun ONE Console: 사용자 및 그룹 탭



이 탭에서 다음과 같은 다양한 사용자 및 그룹 관련 작업을 수행할 수 있습니다.

- 사용자 디렉토리에서 사용자 및 그룹 정보 추가, 수정 및 삭제
- 사용자 디렉토리에서 특정 사용자 및 그룹 항목 검색

Sun ONE Administration Server

Sun ONE Administration Server는 Sun ONE Console을 통해 Directory Proxy Server를 포함한 모든 Sun ONE 서버를 구성할 수 있게 해주는 웹 기반(HTTP) 서버입니다. 이러한 서버를 구성하려면 Administration Server와 해당 서버의 구성 디렉토리를 먼저 실행해야 합니다. Administration Server는 모든 Sun ONE 서버와 함께 제공되며 *서버 그룹*에 첫 번째 서버를 설치할 때 설치됩니다. 서버 그룹은 서버 루트 디렉토리에 설치되고 Administration Server의 단일 인스턴스에 의해 관리되는 서버를 말합니다.

Sun ONE Console 로그인 화면에 URL을 입력하여 Administration Server에 액세스합니다. 44페이지의 "단계 1. Sun ONE Console에 로그인"을 참조하십시오. 이 URL은 Directory Proxy Server를 설치할 때 선택한 컴퓨터 호스트 이름과 포트 번호를 기반으로 합니다. URL 형식은 다음과 같습니다.

```
http://<machine_name>.<your_domain>.<domain>:<port>
```

Administration Server에 액세스하려고 시도할 때마다 사용자 아이디와 비밀번호를 입력하여 구성 디렉토리에 대한 인증을 받아야 합니다. 사용자 아이디와 비밀번호는 컴퓨터에 Directory Proxy Server(또는 서버 그룹의 첫 번째 서버) 및 Administration Server를 설치할 때 지정한 *관리자* 아이디 및 비밀번호입니다. Administration Server가 실행 중인 경우 Sun ONE Console을 사용하여 Directory Proxy Server를 포함하여 그룹에 있는 모든 서버를 관리할 수 있습니다.

Administration Server에 대한 자세한 내용은 *Managing Servers with Sun ONE Console*을 참조하십시오. Directory Proxy Server 설치에서 이 설명서의 온라인 버전을 보려면 다음 파일을 엽니다. `<server-root>/manual/en/admin/ag/contents.htm`

아래 사이트에서도 이 설명서의 최신 버전을 구할 수 있습니다.

`http://docs.Sun ONE.com/docs/manuals/console.html`

Administration Server 시작

Directory Proxy Server 설치 프로그램은 설치하는 동안 식별한 Administration Server 인스턴스를 자동으로 시작하여 Directory Proxy Server를 모니터합니다. Directory Proxy Server 설치 후에 Administration Server를 중지한 경우 Directory Proxy Server 콘솔에서 Directory Proxy Server를 관리하려면 Administration Server를 다시 시작해야 합니다.

명령줄이나 Windows NT 서비스 패널에서 Administration Server를 시작할 수 있습니다.

- 명령줄에서 Administration Server를 시작하려면 다음을 수행합니다.

  명령 프롬프트에서 다음 행을 입력합니다. `<server-root>/start-admin`

- Administration Server가 Windows NT 시스템에서 서비스로 실행됩니다. Windows NT 서비스 패널을 사용하여 서비스를 직접 시작할 수 있습니다.

위에서 설명한 모든 방법은 설치하는 동안 지정한 포트 번호에서 Administration Server를 시작합니다. 서버가 실행 중이면 Sun ONE Console을 사용하여 Directory Proxy Server에 액세스할 수 있습니다.

Administration Server 중지

Administration Server를 사용하지 않을 때는 종료하는 것이 보안상 좋습니다. 이렇게 하면 다른 사람이 구성을 변경하는 것을 최대한 방지할 수 있습니다. Sun ONE Console, 명령줄 또는 Windows NT 서비스 패널에서 서버를 종료할 수 있습니다.

- Sun ONE Console에서 Administration Server를 종료하려면 다음을 수행합니다.

  a. Sun ONE Console에 로그인합니다(44페이지의 "단계 1. Sun ONE Console에 로그인" 참조).

  b. "서버 및 응용 프로그램" 탭에서 종료할 Administration Server 인스턴스를 찾아서 해당 항목을 두 번 누릅니다.

  Administration Server Console이 나타납니다.

  a. 작업 탭에서 서버 중지를 누릅니다.

- 명령줄에서 Administration Server를 종료하려면 다음을 수행합니다.

  명령 프롬프트에서 다음 행을 입력합니다. `<server-root>/stop-admin`

- Administration Server가 Windows NT 시스템에서 서비스로 실행되고, Windows NT 서비스 패널을 사용하여 서비스를 직접 중지할 수 있습니다.

Directory Proxy Server 콘솔 액세스

Directory Proxy Server 콘솔에서 Directory Proxy Server 관리 작업을 수행하려면 서버 콘솔을 먼저 열어야 합니다.

- 단계 1. Sun ONE Console에 로그인
- 단계 2. 해당 Directory Proxy Server 콘솔 열기

단계 1. Sun ONE Console에 로그인

해당 구성 디렉토리 및 Administration Server가 실행 중일 때만 Sun ONE Console을 시작 및 사용할 수 있습니다. 서버가 실행되고 있지 않은 경우 명령줄로 이동하여 서버를 시작하십시오. 명령줄에서 Administration Server를 시작하는 방법에 대한 자세한 내용은 43페이지의 "Administration Server 시작"을 참조하십시오. 구성 디렉토리 시작과 관련한 자세한 내용은 Sun ONE Directory Server 설명서를 참조하십시오.

Sun ONE Console을 시작하면 로그인 창이 표시됩니다. 액세스 권한이 있는 서버 그룹을 나타내는 Administration Server의 관리자 아이디, 비밀번호 및 URL (포트 번호 포함)을 입력하여 구성 디렉토리에 대한 인증을 받아야 합니다. 네트워크에 있는 하나 이상의 서버 그룹에 대한 액세스 권한이 없는 경우에는 Sun ONE Console을 사용할 수 없습니다.

1. 해당 옵션을 사용하여 Sun ONE Console 응용 프로그램을 엽니다.

   - UNIX 시스템에 로컬로 액세스할 경우 명령줄 프롬프트에서 다음 행을 입력합니다.
     `<server-root>/start-console`
   - Windows NT 시스템에서 로컬로 액세스할 경우 바탕 화면의 Sun ONE Console 아이콘을 두 번 누릅니다. 이 아이콘은 Sun ONE 서버를 처음 설치할 때 만들어집니다.

   Sun ONE Console 로그인 창이 나타납니다.

2. 구성 디렉토리에 대한 인증을 받습니다.

   사용자 아이디. 시스템에 Administration Server를 설치할 때 지정한 *관리자 아이디*를 입력합니다. Administration Server는 Sun ONE 서버를 처음 설치할 때 또는 Directory Proxy Server를 설치할 때 설치됩니다.

   비밀번호. Directory Proxy Server 설치 중에 Administration Server를 시스템에 설치할 때 지정한 *관리자* 비밀번호를 입력합니다.

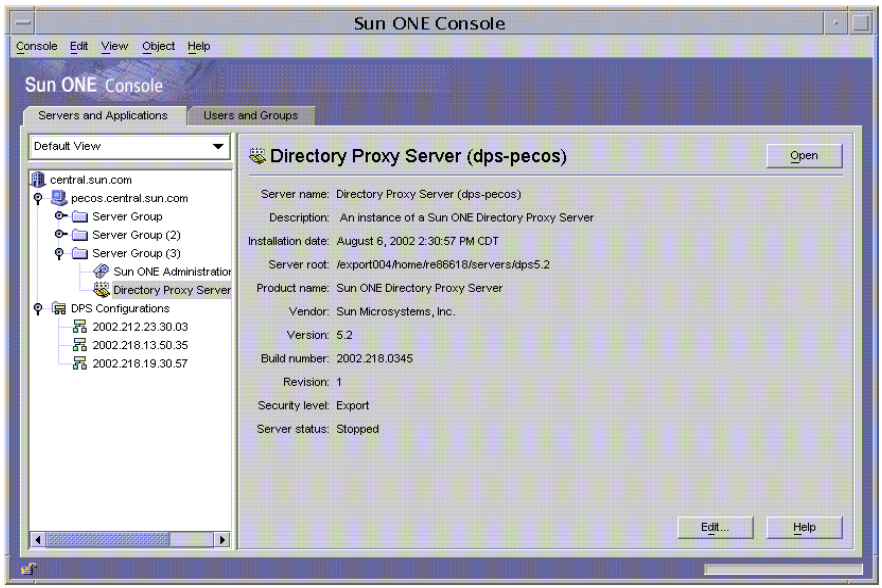
   관리 URL. 이 필드에 Administration Server에 대한 URL이 표시됩니다. URL이 표시되지 않거나 원하는 Administration Server URL이 없는 경우 이 필드에 해당 URL을 입력합니다. URL은 Directory Proxy Server를 설치할 때 선택한 컴퓨터 호스트 이름과 Administration Server 포트 번호로 이루어집니다. 다음 형식을 사용하십시오.

   `http://<machine_name>.<your_domain>.<domain>:<port_number>`

   예를 들어, 도메인 이름이 `sun`일 경우 Administration Server를 `myHost`라는 호스트 시스템에 설치하고 포트 번호로 `12345`를 지정했다면 URL은 다음과 같습니다.
   `http://myHost.sun.com:12345`

3. 확인을 누릅니다.

   Sun ONE Console이 열리고 제어할 수 있는 모든 서버 및 자원 목록이 표시됩니다.



단계 2. 해당 Directory Proxy Server 콘솔 열기

Sun ONE Console에는 Directory Proxy Server에 대한 두 항목이 있습니다. 하나는 Directory Proxy Server 인스턴스 노드에 대한 항목이고 또 하나는 Directory Proxy Server 구성 노드에 대한 항목입니다. Directory Proxy Server 인스턴스 노드는 Directory Proxy Server 서버 인스턴스에 해당하고 Directory Proxy Server 구성 노드는 여러 Directory Proxy Server 인스턴스에서 공유하는 구성에 해당합니다.

각 노드는 GUI 기반 관리 인터페이스에 연결됩니다.

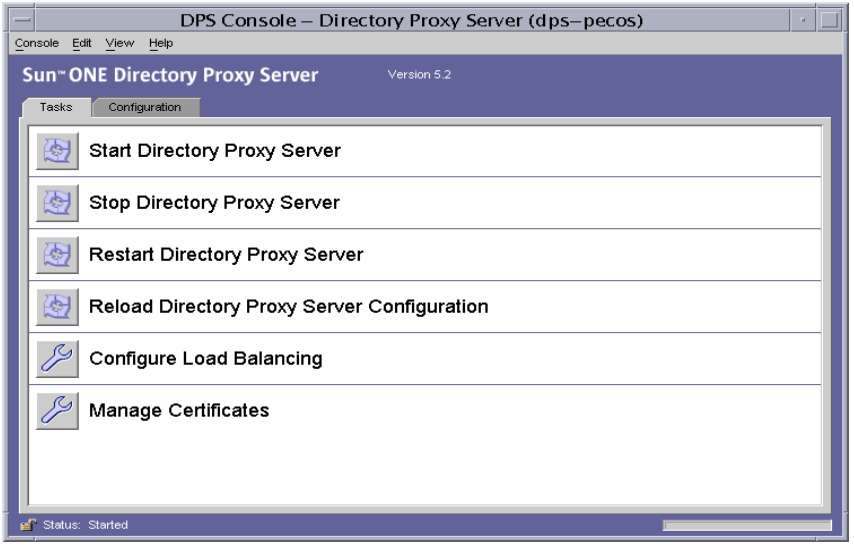
- Directory Proxy Server 콘솔 - 이 관리 인터페이스를 사용하여 Directory Proxy Server 인스턴스를 작성, 구성 및 관리(예: 시작, 중지, 구성 지정, 로그 모니터 등)할 수 있습니다. Directory Proxy Server 서버 콘솔을 사용하여 서버에 로컬 또는 원격으로 액세스할 수 있습니다. Directory Proxy Server에서 만들고 구성한 Directory Proxy Server 인스턴스는 해당 구성을 사용하는 모든 Directory Proxy Server 인스턴스에 영향을 미칩니다.

- Directory Proxy Server 구성 편집기 콘솔 - 여러 Directory Proxy Server 인스턴스에서 논리 및 시스템 구성을 공유합니다. Directory Proxy Server 인스턴스에서 구성 정보를 공유할 수 있으므로 Directory Proxy Server 클러스터를 간편하게 관리할 수 있습니다. Directory Proxy Server 구성 편집기 콘솔은 Directory Proxy Server 클러스터를 구성 및 관리할 수 있는 관리 인터페이스입니다. 이 인터페이스를 통해 편집한 내용은 편집된 구성을 사용하는 모든 Directory Proxy Server 인스턴스에 적용됩니다.

Directory Proxy Server 서버 콘솔 열기

Sun ONE Console에 로그인하고 나면 Directory Proxy Server 서버 콘솔을 열 수 있습니다. Sun ONE Console의 탐색 트리에서 Directory Proxy Server 인스턴스가 속하는 서버 그룹을 포함하는 호스트 이름을 확장하고, 서버 그룹 노드를 확장한 다음 원하는 Directory Proxy Server 인스턴스에 해당하는 항목을 선택하고 열기를 누릅니다. Directory Proxy Server 콘솔이 열립니다(그림 3-3).

그림 3-3 Directory Proxy Server 서버 콘솔: 작업 탭

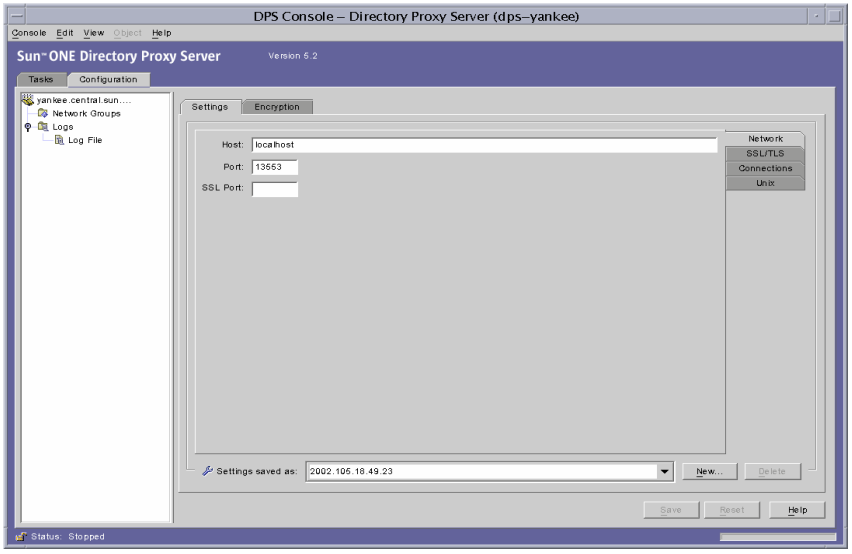


Directory Proxy Server 콘솔에는 특정 관리 영역을 담당하는 두 개의 탭인 작업 탭과 구성 탭이 있습니다.

작업 탭에서는 서버 시작, 중지, 다시 시작 및 다시 로드, 여러 LDAP 디렉토리로 로드 분산 또는 균형 조정, 인증서 관리 등과 같은 일반적인 작업을 수행할 수 있습니다. Directory Proxy Server 시작, 중지 및 다시 시작에 대한 자세한 내용은 4장, “Directory Proxy Server 시작, 다시 시작 및 중지“를 참조하십시오. 로드 균형 조정에 대한 자세한 내용은 7장, “등록 정보 객체 정의 및 관리“를 참조하십시오. 인증서 관리에 대한 자세한 내용은 11장, “보안 구성“을 참조하십시오.

구성 탭(그림 3-4)에서는 특정 인스턴스의 구성을 보고 수정할 수 있습니다.

그림 3-4 Directory Proxy Server 서버 콘솔: 구성 탭의 설정 탭



설정 탭과 암호화 탭은 Directory Proxy Server의 특정 인스턴스가 구성되어 있는 방법과 관련이 있습니다.

설정 탭(그림 3-4)에서는 다음 매개 변수를 구성할 수 있습니다.

네트워크. Directory Proxy Server의 이 인스턴스에 대한 호스트 이름, 포트 및 SSL 포트를 표시합니다.

SSL/TLS. Directory Proxy Server에서 보내고 서버와 클라이언트의 SSL 인증서에서 필요로 하는 현재 선택된 구성을 표시합니다. 또한 Directory Proxy Server에 대한 클라이언트의 SSL/TLS 버전과 백엔드 통신에 대한 Directory Proxy Server의 SSL/TLS 버전을 식별합니다.

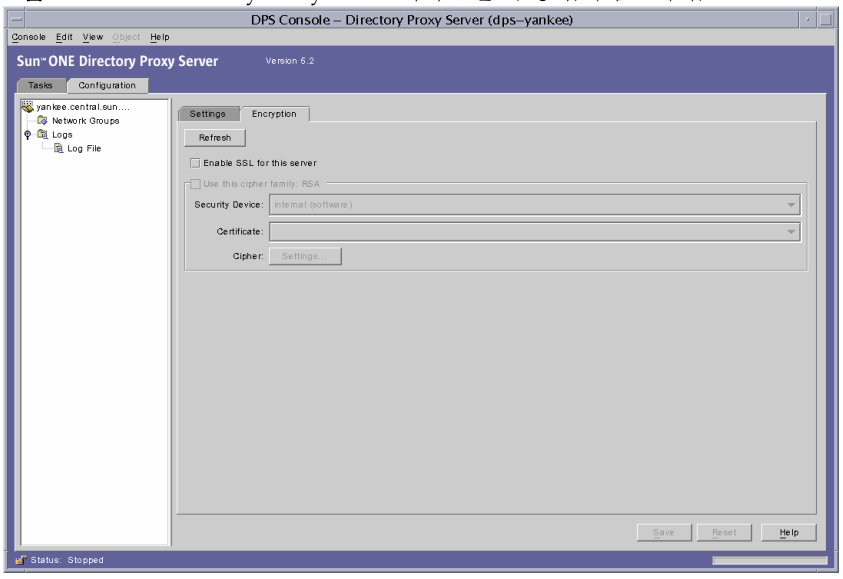
연결. Directory Proxy Server 연결 백로그 값을 표시하며, 사용자가 최대 연결 수를 지정하고 연결 풀 시간 초과 값을 설정할 수 있도록 합니다.

Unix. Directory Proxy Server의 이 인스턴스에 대한 UNIX 사용자 아이디와 작업 디렉토리를 표시합니다.

다음 이름으로 설정 저장. 사용자가 목록 상자에 현재 표시된 편집 세션에 대해 Directory Proxy Server 이름 값을 지정할 수 있도록 합니다. 구성을 새로 만들거나 이전 Directory Proxy Server 구성을 삭제할 수도 있습니다.

구성 탭의 암호화 탭(그림 3-5)에서는 암호화 설정을 보고 수정할 수 있습니다.

그림 3-5 Directory Proxy Server 서버 콘솔: 구성 탭의 암호화 탭



암호화 탭에서는 다음 매개 변수를 구성할 수 있습니다.

갱신. 현재 화면 값을 갱신하여 새로 추가된 인증서를 볼 수 있습니다.

이 서버에 SSL 사용. 이 Directory Proxy Server 인스턴스에 SSL 암호화를 사용합니다.

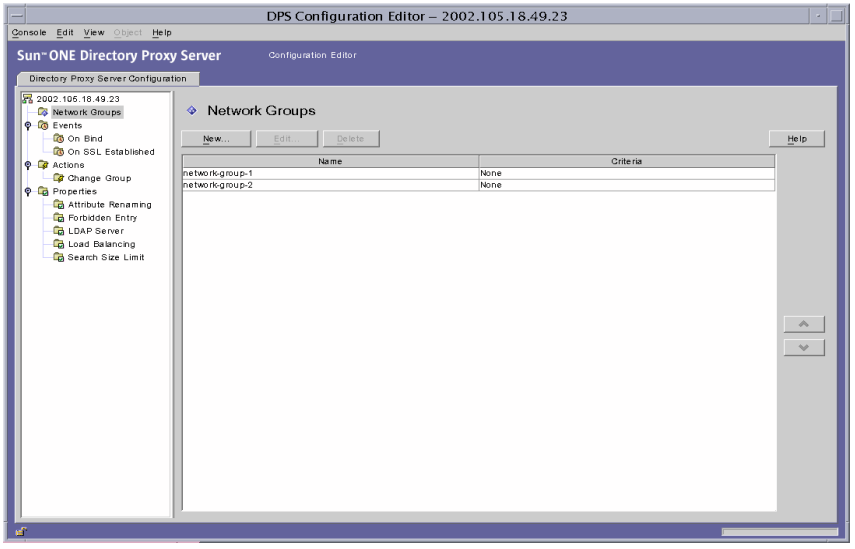
이 암호 패밀리 RSA 사용. Directory Proxy Server의 이 인스턴스에 대해 보안 장치, 인증서 및 암호 설정을 지정할 수 있습니다.

시스템에서 암호화를 설정하는 것과 관련한 자세한 내용은 65페이지의 “시스템 구성 인스턴스 만들기”를 참조하십시오.

Directory Proxy Server 구성 편집기 콘솔 열기

DPS 콘솔에 로그인한 경우 Directory Proxy Server 구성 편집기 콘솔을 열 수 있습니다. DPS 콘솔의 탐색 트리에서 Directory Proxy Server 구성 노드를 확장하고, 항목을 선택한 다음 확인을 누릅니다. Directory Proxy Server 구성 편집기 콘솔이 열립니다(그림 3-6).

그림 3-6 Directory Proxy Server 구성 편집기 콘솔



왼쪽에 있는 탐색 트리에는 각 Directory Proxy Server의 기본 구성 객체에 대한 노드가 포함되어 있습니다. 기본 노드 중 하나를 확장하면 객체 하위 유형 각각에 대한 트리 노드가 표시됩니다. 트리 노드를 누르면 오른쪽에 선택한 트리 노드가 나타내는 유형의 모든 객체가 들어 있는 테이블이 표시됩니다. 네트워크 그룹처럼 순서가 중요한 객체 테이블에는 개별 객체를 위로 올리거나 아래로 내려서 순서를 바꿀 수 있는 위쪽/아래쪽 버튼 집합이 있습니다.

표 3-1에는 탐색 트리에 표시되는 구성 객체 유형이 나열되어 있습니다.

표 3-1 Directory Proxy Server 구성 편집기 콘솔의 구성 객체

구성 객체 유형	설명
네트워크 그룹	각 네트워크 그룹 객체는 특정 클라이언트 커뮤니티를 식별하고 해당 그룹과 일치하는 클라이언트에 적용할 제한 사항을 지정합니다. 자세한 내용은 6장, "그룹 만들기 및 관리"를 참조하십시오.
이벤트	이벤트 객체는 미리 지정된 특정 상태에서 발생하는 조건을 지정하는 데 사용됩니다. 특정 이벤트에 조건을 연결하여 해당 조건이 충족되면 Directory Proxy Server에서 특정 작업을 수행하도록 할 수 있습니다. 자세한 내용은 8장, "이벤트 객체 만들기 및 관리"를 참조하십시오.
작업	작업은 이벤트가 발생할 때 수행할 작업을 지정하는 데 사용됩니다. 자세한 내용은 9장, "작업 객체 만들기 및 관리"를 참조하십시오.
등록 정보	등록 정보는 클라이언트에 보다 세부적인 제한을 적용하는 데 사용됩니다. 각 그룹 객체는 등록 정보 객체에 의해 정의된 등록 정보 집합을 포함할 수 있습니다. 자세한 내용은 7장, "등록 정보 객체 정의 및 관리"를 참조하십시오.

Directory Proxy Server 시작, 다시 시작 및 중지

이 장에서는 Sun ONE Directory Proxy Server를 시작, 중지 및 다시 시작하는 방법과 서버의 현재 상태를 확인하는 방법에 대해 설명합니다.

이 장은 다음 내용으로 구성되어 있습니다.

주 Directory Proxy Server 콘솔은 해당 Directory Server(*구성* 디렉토리)와 Administration Server가 실행되고 있을 때만 사용할 수 있습니다. Administration Server는 Directory Proxy Server를 설치하는 동안 지정한 포트에서 시작해야 합니다. 보안 위험을 최소화하기 위해 Sun ONE Console 사용을 끝낸 후에는 Administration Server를 종료하십시오. Administration Server의 시작 및 종료에 대한 설명은 42페이지의 "Sun ONE Administration Server"를 참조하십시오.

Directory Proxy Server 시작 및 중지

Directory Proxy Server는 일단 설치되면 시스템 부트 시에 일반적으로 시작되는 UNIX 데몬 프로세스나 Windows NT 서비스로서 지속적으로 실행되면서 요청을 수신하고 받아들입니다.

다음과 같은 몇 가지 방법으로 Directory Proxy Server를 시작하고 중지할 수 있습니다.

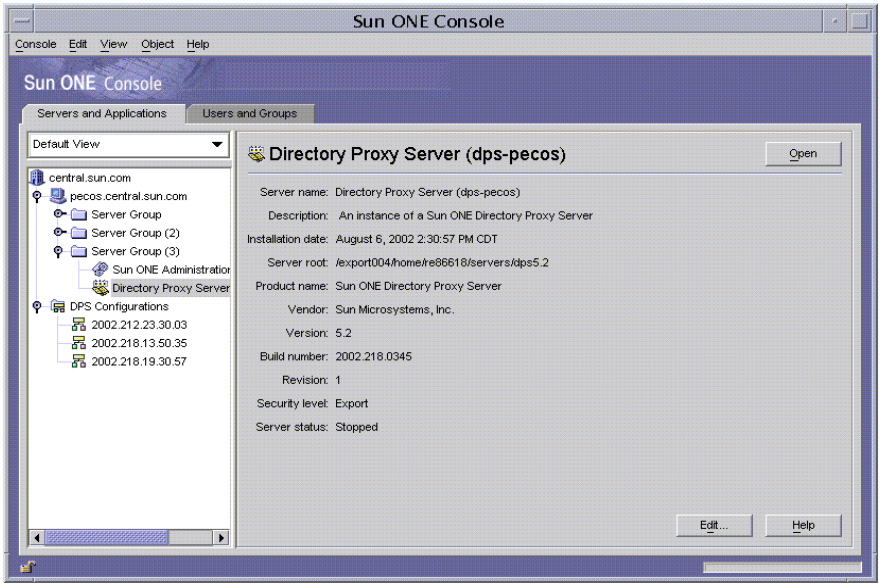
- Sun ONE Console에서(로컬 및 원격으로)
- 명령줄에서(로컬로만)
- Windows NT 시스템의 Windows NT 서비스 패널에서

Directory Proxy Server를 중지하면 모든 구성 요소가 완전히 종료되어 서버를 다시 시작할 때까지 서비스가 중단됩니다. 호스트 시스템에 장애가 발생하거나 오프라인 상태가 되면 서버가 중지되고 처리 중이던 요청은 모두 손실됩니다. 서비스를 복원하려면 서버를 다시 시작해야 합니다.

Sun ONE Console에서 Directory Proxy Server 시작 및 중지

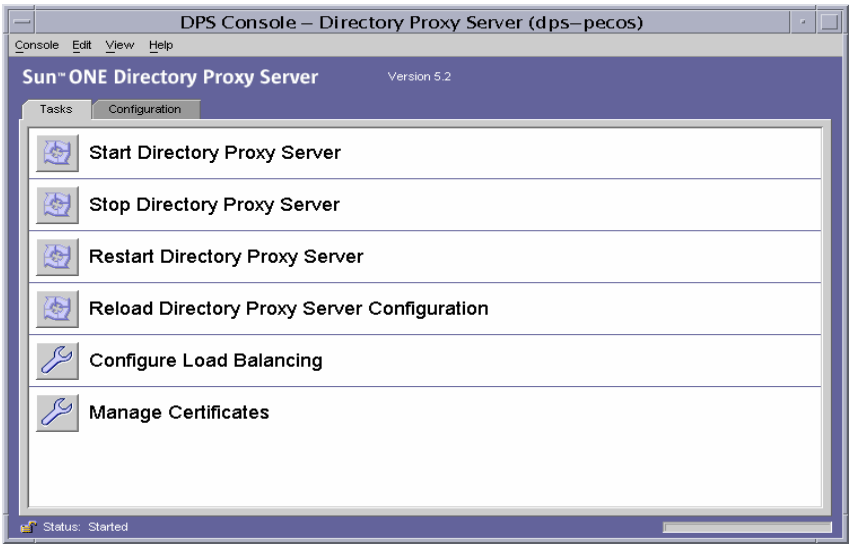
Sun ONE Console을 사용하여 로컬 또는 원격 호스트에 설치된 Directory Proxy Server를 시작하거나 중지할 수 있습니다. Directory Proxy Server를 시작하거나 중지하려면 다음을 수행합니다.

1. Sun ONE Console에 로그인합니다(44페이지의 “단계 1. Sun ONE Console에 로그인” 참조).
2. "서버 및 응용 프로그램" 탭에서 호스트 이름과 시작하려는 Directory Proxy Server 인스턴스가 포함된 서버 그룹을 차례로 확장합니다.
3. 탐색 트리에서 시작하거나 중지하려는 Directory Proxy Server 인스턴스를 찾아 해당 항목을 선택하고 열기를 누릅니다.



Directory Proxy Server 서버 콘솔이 열립니다.

4. 작업 탭에서 Directory Access Router 시작을 눌러 서버를 시작하거나 Directory Access Router 중지를 눌러 서버를 중지합니다.



명령줄에서 Directory Proxy Server 시작 및 중지

명령줄에서 Directory Proxy Server를 시작하거나 중지하려면 다음을 수행합니다.

1. 서버에 대한 단말기 창을 엽니다.
2. UNIX 시스템에서는 서버가 1024보다 낮은 포트에서 실행되면 `root`로 로그인하고 그 외에는 `root` 또는 서버의 사용자 계정으로 로그인합니다. 기본적으로 Directory Proxy Server가 `root`에 의해 실행되면 사용자 아이디는 `nobody`로 변경됩니다.
3. 명령줄 프롬프트에서 다음 행 중 하나를 입력합니다.

   Directory Proxy Server를 시작할 경우
   `<server-root>/dps-<hostname>/start-dps[.exe]`

   Directory Proxy Server를 중지할 경우
   `<server-root>/dps-<hostname>/stop-dps[.exe]`

   `<server-root>`는 Directory Proxy Server 이진 파일이 저장되어 있는 디렉토리입니다. 이 디렉토리는 설치 시에 지정됩니다.

   `<hostname>`은 이 Directory Proxy Server 인스턴스가 설치되어 있는 호스트의 이름입니다.

.exe는 파일 확장자를 지정하며, Windows NT 시스템에서 유틸리티를 실행하는 경우에만 필요합니다.

주 Directory Proxy Server가 이미 실행되고 있는 경우에는 시작 명령이 실패합니다. 먼저 `stop-dps` 명령을 사용하여 서버를 중지한 다음 `start-dps` 명령을 사용하십시오.

Windows NT 서비스 패널에서 Directory Proxy Server 시작 및 중지

Directory Proxy Server를 Windows NT 시스템에 설치한 경우에는 Windows NT 서비스 패널에서 서버를 서비스로서 시작하거나 중지할 수 있습니다. Directory Proxy Server 서비스의 이름은 다음과 같습니다. `Sun ONE Directory Proxy Server`

Windows NT 서비스 패널에서 Directory Proxy Server를 시작하거나 중지하려면 다음을 수행합니다.

1. 바탕 화면에서 시작 > 설정 > 제어판을 선택합니다.
2. 제어판 창이 나타나면 서비스를 두 번 누릅니다.
3. 서비스 목록에서 Directory Proxy Server 인스턴스에 해당하는 서비스를 찾습니다.
4. 서비스를 시작하려면 Directory Proxy Server 인스턴스를 선택하고 시작을 누릅니다. 서비스를 중지하려면 Directory Proxy Server 인스턴스를 선택하고 중지를 누릅니다.

Directory Proxy Server 다시 시작

Directory Proxy Server 구성을 변경할 때마다 변경 사항을 구성 디렉토리에 저장해야 합니다. 구성을 변경하면 변경 사항을 저장한 후 Directory Proxy Server를 다시 시작해야 합니다. 다시 시작할 필요가 있는 경우에는 콘솔에 프롬프트가 자동으로 표시됩니다.

다시 시작하는 동안 Directory Proxy Server는 구성을 다시 읽고, 이후의 연결에 새로운 구성을 사용합니다. 이미 설정된 클라이언트 연결은 끊어질 때까지 이전 구성을 계속 사용합니다. 다시 시작 기능은 UNIX 플랫폼에서만 사용할 수 있습니다. Windows NT의 경우 Directory Proxy Server를 다시 시작하는 것은 Directory Proxy Server를 중지했다가 시작하는 것과 같습니다.

다음 두 가지 방법으로 Directory Proxy Server를 다시 시작할 수 있습니다.

- Directory Proxy Server 서버 콘솔에서(로컬 및 원격으로)
- 명령줄에서(로컬로만)

명령줄에서 Directory Proxy Server 다시 시작

명령줄에서 Directory Proxy Server를 다시 시작하려면 다음을 수행합니다.

1. 서버에 대한 단말기 창을 엽니다.
2. Unix 시스템에서는 `root`로 로그인하거나 서버의 사용자 계정을 사용하여(이 방법으로 서버를 시작한 경우) 로그인합니다.
3. 명령줄 프롬프트에서 다음 행을 입력합니다.

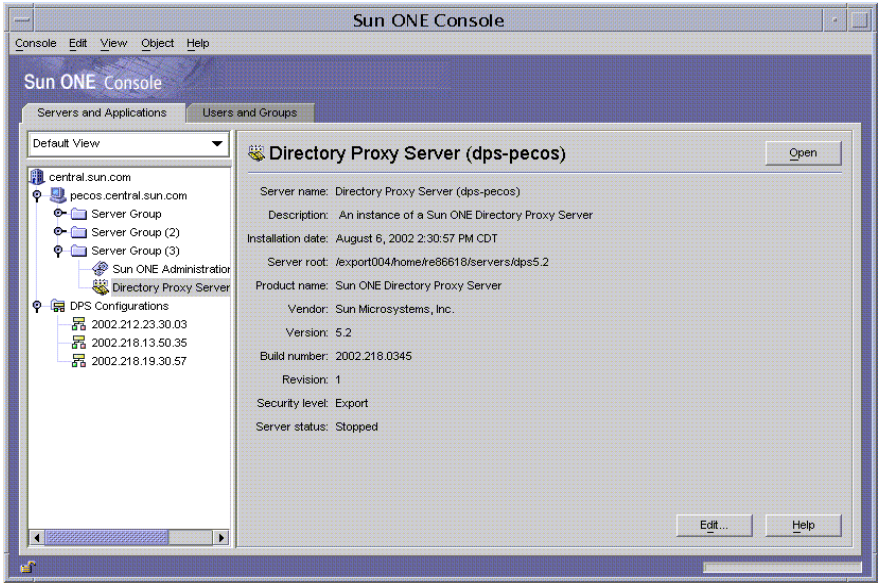
   ```
   <server-root>/dps-<hostname>/restart-dps[.exe]
   ```

UNIX 플랫폼의 Sun ONE Console에서 Directory Proxy Server 다시 로드

UNIX 플랫폼에서는 Directory Proxy Server 서버 콘솔을 사용하여 로컬 또는 원격 호스트에 설치된 Directory Proxy Server 구성을 다시 로드할 수 있습니다. UNIX 플랫폼에서 Directory Proxy Server 구성을 변경할 때마다 Directory Proxy Server 구성을 다시 로드해야 변경 사항이 적용됩니다. NT 플랫폼에서는 Directory Proxy Server 구성을 반드시 다시 시작해야 합니다.

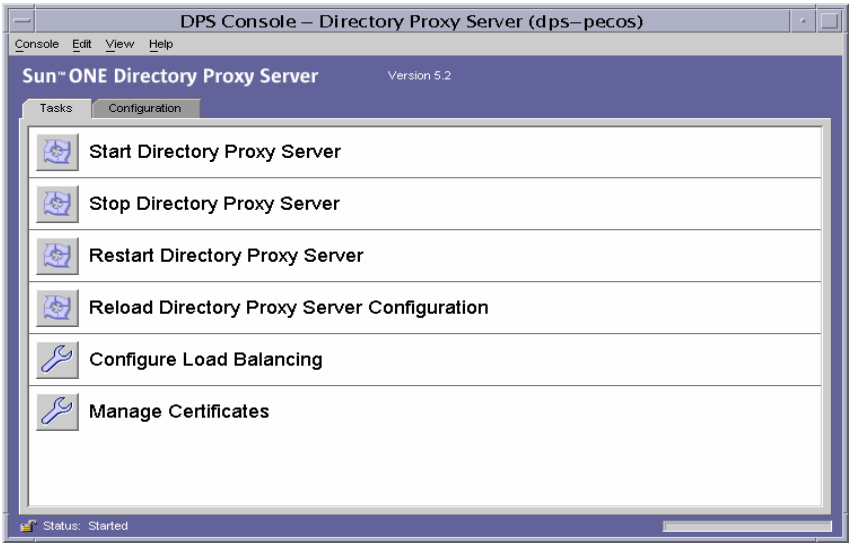
Directory Proxy Server 콘솔에서 Directory Proxy Server를 다시 로드하려면 다음을 수행합니다.

1. 아직 Directory Proxy Server 서버 콘솔이 표시되어 있지 않은 경우에는 Sun ONE Console에 로그인합니다(44페이지의 “단계 1. Sun ONE Console에 로그인” 참조).
2. "서버 및 응용 프로그램" 탭에서 호스트 이름과 다시 시작하려는 Directory Proxy Server 인스턴스가 포함된 서버 그룹을 차례로 확장합니다.
3. 탐색 트리에서 시작하거나 중지하려는 Directory Proxy Server 인스턴스를 찾아 해당 항목을 선택하고 열기를 누릅니다.



Directory Proxy Server 서버 콘솔이 열립니다.

4. 작업 탭에서 라우터 구성 다시 로드를 눌러 서버를 다시 로드합니다.



Directory Proxy Server 시스템 상태 확인

다음 두 가지 방법을 사용하여 Directory Proxy Server의 특정 인스턴스가 시작되었는지 또는 중지되었는지 여부를 확인할 수 있습니다.

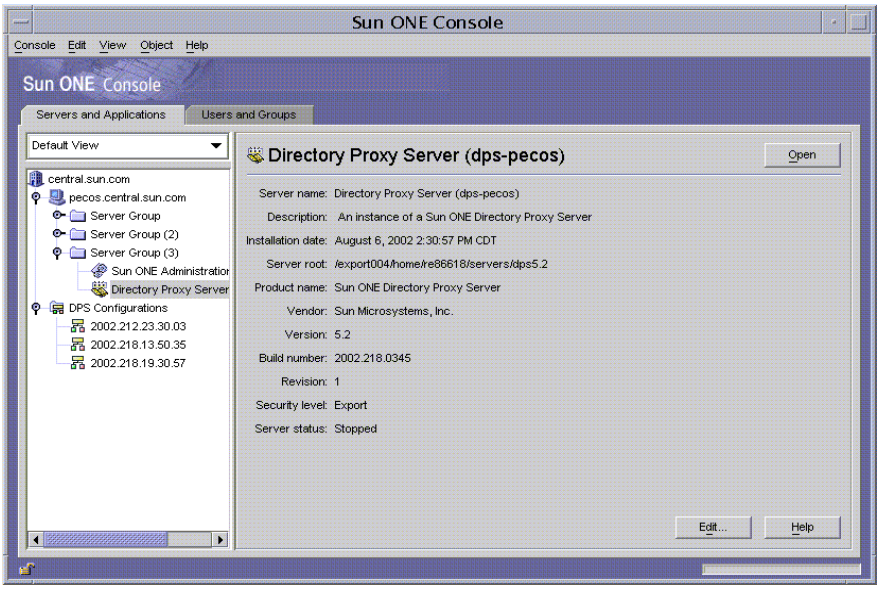
- Sun ONE Console에서(로컬 및 원격으로)
- 명령줄에서(로컬로만)

Sun ONE Console에서 Directory Proxy Server 상태 확인

Sun ONE Console을 사용하여 특정 Directory Proxy Server 인스턴스가 실행 중인지 여부를 확인할 수 있습니다.

1. Sun ONE Console에 로그인합니다(44페이지의 “단계 1. Sun ONE Console에 로그인” 참조).

2. "서버 및 응용 프로그램" 탭에서 상태를 확인하려는 Directory Proxy Server 인스턴스에 해당하는 항목을 선택합니다.



3. 오른쪽 창에서 서버 상태 필드를 확인합니다.

선택한 Directory Proxy Server 인스턴스가 실행되고 있는 경우 상태는 *시작됨*입니다. 그 외에는 *경고*, *중지됨* 또는 *알 수 없음*입니다. SIE 이름이 기울임꼴로 표시되는 경우에도 서버 상태는 중지됨입니다.

명령줄에서 Directory Proxy Server 상태 확인

명령줄에서 특정 Directory Proxy Server 인스턴스가 실행 중인지 여부를 확인할 수 있습니다.

1. 서버에 대한 단말기 창을 엽니다.
2. Unix 시스템에서는 `root`로 로그인하거나 서버의 사용자 계정을 사용하여(이 방법으로 서버를 시작한 경우) 로그인합니다.
3. 명령줄 프롬프트에서 다음 행을 입력합니다.

```
<server-root>/dps-<hostname>/status-dps[.exe]
```

명령줄에서 Directory Proxy Server 시작 및 중지

Directory Proxy Server 프로그램은 시스템 부트 시에 일반적으로 시작되는 UNIX 데몬 프로세스 또는 NT 서비스로 실행됩니다.

모든 플랫폼에서 Directory Proxy Server의 시작 프로그램은 다음 위치에 있습니다.

```
<server-root>/dps-<hostname>/start-dps
```

시작 구성 파일은 다음 위치에 있습니다.

```
<server-root>/dps-<hostname>/etc/tailor.txt
```

Directory Proxy Server는 다음 위치에 있는 스크립트를 통해 시작하거나 중지할 수 있습니다.

```
<server-root>/dps-<hostname>
```

Windows NT에서 Directory Proxy Server를 시작하고 중지하려면 Windows NT 서비스 관리자를 사용해야 합니다. Windows NT 이외의 플랫폼인 경우 유효한 사용자 아이디가 실제 사용자 아이디와 동일하면 장애가 발생할 때 Directory Proxy Server에서 `core` 이미지만 생성합니다. 따라서 Directory Proxy Server가 core를 생성하도록 하려면 `ids-proxy-sch-GlobalConfiguration` 객체 클래스의 `ids-proxy-con-userid` 속성을 Directory Proxy Server 프로세스를 시작한 사용자와 동일하게 설정해야 합니다. 기본적으로 Directory Proxy Server가 `root`에 의해 실행되면 사용자 아이디는 `nobody`로 변경됩니다.

지원되는 플래그

시작 및 중지 스크립트에서 지원하는 플래그는 표 4-1에서 설명합니다.

표 4-1 시작 및 중지 스크립트에서 지원하는 플래그

플래그	설명
`-d`	이 플래그가 지정되면 Directory Proxy Server는 들어오는 연결을 한 번에 하나씩만 처리하고 보다 자세한 내부 추적 정보를 로그 파일로 보냅니다. 이 플래그는 Directory Proxy Server 데몬이 해당 데몬을 제어하는 단말기에서 분리되지 못하도록 하므로 일반 작업에서는 사용하지 말아야 합니다.

표 4-1 시작 및 중지 스크립트에서 지원하는 플래그 *(계속)*

플래그	설명
-D	이 플래그는 Directory Proxy Server가 로그 파일에 더 자세한 추적 정보를 보내도록 지시합니다. Directory Proxy Server는 여전히 여러 개의 클라이언트 연결을 처리하고 데몬으로 실행됩니다. -d 플래그와 -D 플래그는 동시에 사용할 수 없습니다.
-t <시작 구성 파일>	이 옵션은 대체 시작 구성 파일을 지정하는 데 사용할 수 있습니다. 반드시 구성 파일에 대한 절대 경로를 지정해야 합니다.
-s	이 옵션은 LOG_DAEMON 기능을 사용하여 초기 로그 메시지를 syslogd로 보내도록 Directory Proxy Server에 지시합니다. Windows NT에서는 이 플래그가 무시됩니다. 환경 변수 dps_ROOT가 정의되지 않은 경우에는 이 값이 기본값입니다.
-M	이 플래그가 지정되면 Directory Proxy Server는 자신을 모니터하기 위해 다른 프로세스를 생성합니다. Directory Proxy Server가 강제 종료될 경우 30초 동안 기다린 후 모니터 프로세스가 Directory Proxy Server를 다시 시작합니다. Windows NT에서는 이 플래그를 사용할 수 없습니다.
-r	이 플래그는 하드 코드된 레지스트리 경로의 뒷부분에 값을 추가하는 데 사용됩니다. 결과 레지스트리 경로는 Directory Proxy Server 서비스가 루트 또는 인스턴스 루트 이름과 같은 구성 정보를 가리키도록 합니다. Windows 시스템에서는 한 호스트에 하나의 Directory Proxy Server 인스턴스만 설치할 수 있습니다.
-v	이 플래그는 Directory Proxy Server의 버전 정보를 인쇄합니다. Windows NT에서는 이 플래그를 명령줄에서만 사용해야 합니다.

Directory Proxy Server 다시 시작

UNIX 플랫폼에서는 Directory Proxy Server에 SIGHUP 신호를 보내 구성을 다시 읽도록 할 수 있습니다. 구성을 성공적으로 다시 읽은 경우 Directory Proxy Server는 이후의 연결에 새로운 구성을 사용합니다. 이미 설정된 클라이언트 연결은 클라이언트 연결이 끊어질 때까지 이전 구성을 계속 사용합니다.

Directory Proxy Server가 구성을 다시 읽도록 신호를 보내려면 <server-root>/dps-<hostname>의 hup-dps 명령을 사용합니다.

일부 속성 값은 HUP 신호 기능을 사용하여 변경할 수 없습니다. 다음과 같은 구성 매개 변수를 변경하려면 Directory Proxy Server를 종료했다가 다시 시작해야 합니다.

```
ids-proxy-con-listen-port
ids-proxy-con-listen-host
ids-proxy-con-ldaps-port
ids-proxy-con-foreground
ids-proxy-con-listen-backlog
ids-proxy-con-ssl-cert
ids-proxy-con-ssl-key
```

또한 로깅 등록 정보인 ids-proxy-sch-LogProperty도 이 기능을 사용하여 변경할 수 없습니다.

모든 플랫폼에서 restart-dps 명령은 <server-root>/dps-<hostname>에 있습니다. 이 다시 시작 명령은 앞에 언급된 디렉토리에 있는 stop-dps 명령과 start-dps 명령을 단순히 호출하기만 합니다.

시스템 구성 인스턴스 만들기

시스템 매개 변수는 Sun ONE Directory Proxy Server의 기능 동작에 영향을 주는 매개 변수입니다. 이 장에서는 시스템 구성을 지정하고 저장하는 방법을 설명합니다.

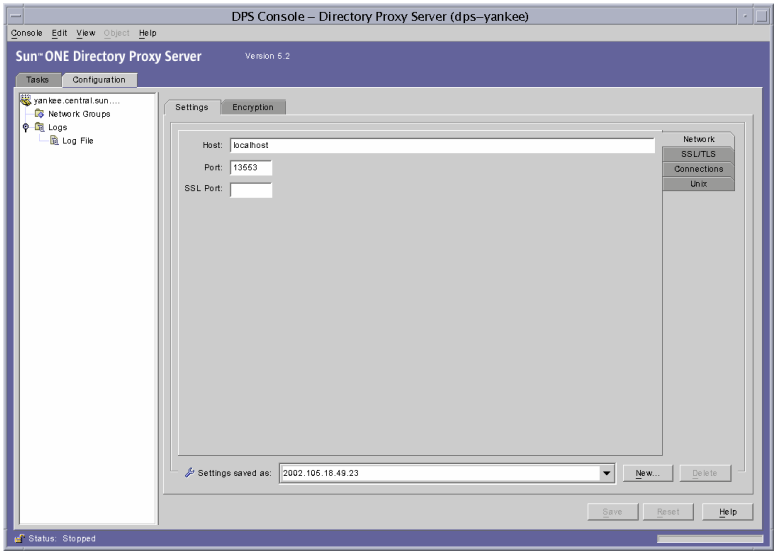
이 장은 다음 내용으로 구성되어 있습니다.

시스템 구성 인스턴스 만들기

이 절에서는 Directory Proxy Server 인스턴스의 시스템별 매개 변수를 구성하는 방법을 설명합니다. 시스템 구성을 위한 객체를 만들려면 다음을 수행합니다.

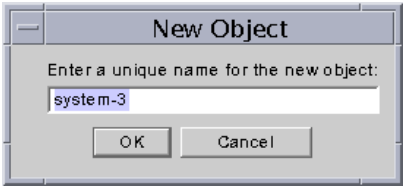
1. Directory Proxy Server 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.
2. 탐색 트리에서 해당 Directory Proxy Server 인스턴스를 선택하고 열기를 누릅니다.

   Directory Proxy Server 콘솔에서 구성 탭을 누릅니다.



3. 새로 만들기를 누릅니다.

   새 객체 창이 나타납니다.



4. 이름 필드에 시스템 구성 이름을 입력합니다. 이 이름은 고유한 영숫자 문자열이어야 합니다. 확인을 누릅니다.

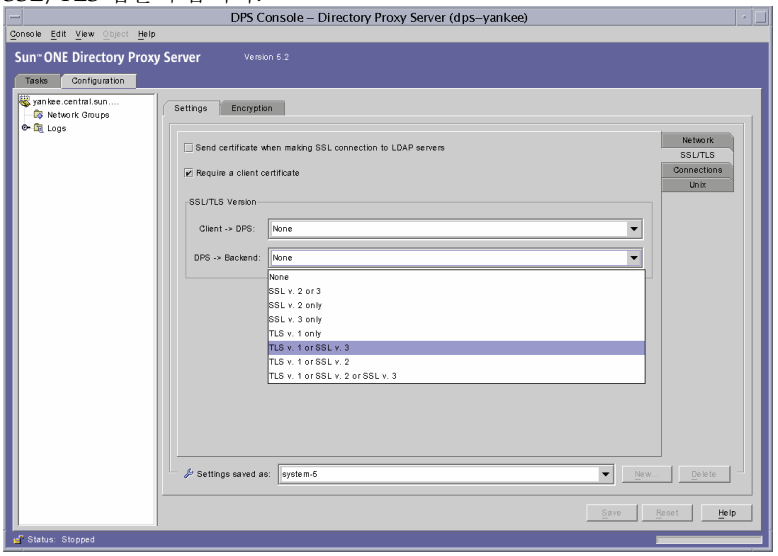
5. 네트워크 탭에서 이 시스템 구성에 대한 일반 설정을 지정합니다.

   호스트. Directory Proxy Server가 연결을 수신하는 호스트 인터페이스의 이름을 입력합니다. 이 속성은 Directory Proxy Server를 실행하는 호스트에 여러 개의 네트워크 인터페이스가 있을 경우에만 필요합니다. 기본적으로 호스트 이름은 "localhost"로 설정됩니다. 즉, Directory Proxy Server가 사용 가능한 모든 네트워크 인터페이스에서 수신합니다. "localhost"를 지정하면 공유 시스템 등록 정보가 허용됩니다.

포트. Directory Proxy Server가 받는 연결을 수신할 포트 번호를 입력합니다. 이 필드에 유효한 값은 1에서 65535까지입니다. 기본적으로 이 값은 LDAP에 대해 지정된 대로 389로 설정됩니다. 이 포트 번호는 같은 호스트에서 실행 중인 다른 LDAP 서버에서 사용하는 포트 번호와는 달라야 합니다. UNIX 플랫폼에서 서버는 루트로 시작해야 1024 이하의 포트 번호에서 수신할 수 있습니다.

SSL 포트. LDAPS (SSL에서의 LDAP) 연결을 수신할 포트 번호를 나타내는 값을 입력합니다. 기본적으로 Directory Proxy Server는 LDAPS 클라이언트에서 연결을 수신하지 않습니다. 이 값이 있어야 636 같은 값으로 이러한 비표준 기능을 사용하여 클라이언트에서 LDAPS 연결을 설정할 수 있습니다. 이 값은 호스트 값과는 달라야 합니다. 이 옵션을 사용하려면 암호화 탭에 있는 TLS/SSL 구성이 필요합니다.

6. SSL/TLS 탭을 누릅니다.



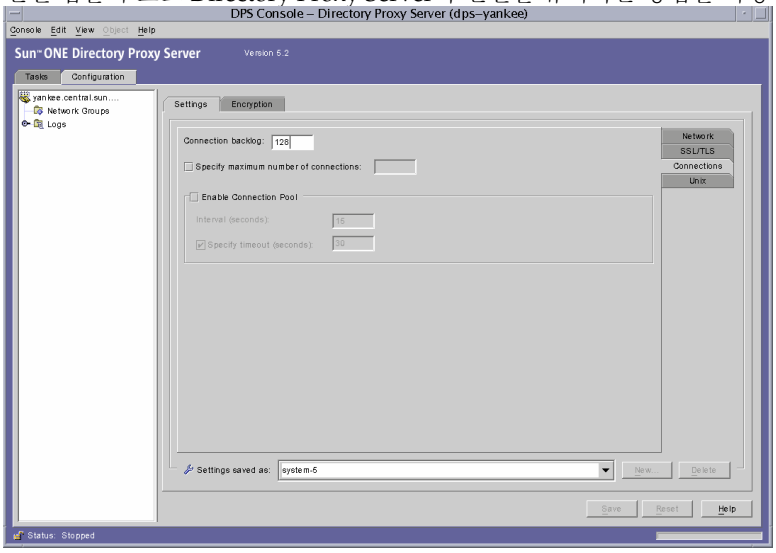
Directory Proxy Server에서 보내고 서버와 클라이언트의 SSL 인증서에서 필요로 하는 기본 구성을 표시합니다. 다음에 대한 항목을 선택합니다.

LDAP 서버로 SSL 연결 시 인증서 보내기. Directory Proxy Server에서 TLS 연결 시 해당 인증서를 백엔드 LDAP 디렉토리 서버로 보내도록 하려면 이 설정을 지정합니다. 기본적으로 이 설정은 비활성화되어 있습니다.

클라이언트 인증서 필요. Directory Proxy Server에서 SSL 세션을 설정한 모든 클라이언트에 인증서 체인 제출을 요청하도록 지정하려면 이 설정을 사용합니다. 인증서 체인이 제출되지 않으면 Directory Proxy Server에서 연결을 끊습니다. 이 옵션은 Directory Proxy Server와 백엔드 서버 간의 SSL 세션에 영향을 주지 않습니다. 기본적으로 이 설정은 비활성화되어 있습니다.

SSL/TLS 버전. 클라이언트 > Directory Proxy Server 및 Directory Proxy Server > 백엔드 옆에 있는 드롭다운 창을 선택하여 각 경우에 적합한 SSL/TLS 버전을 선택합니다. SSL이 시스템에서 사용되는 경우에는 버전을 반드시 지정해야 합니다.

7. 연결 탭을 누르고 Directory Proxy Server가 연결을 유지하는 방법을 지정합니다.



Directory Proxy Server 연결 백로그 값을 표시하고 사용자가 최대 연결 수를 지정하고 연결 풀 시간 초과 값을 설정하도록 합니다. 다음에 대한 항목을 선택합니다.

연결 백로그. 0보다 큰 값을 입력하여 수신 소켓의 대기열에서 해결되지 않은 최대 연결 수를 지정합니다. 기본 연결 수는 128개입니다. 최대값은 기존 운영 체제 구성에 따라 다릅니다.

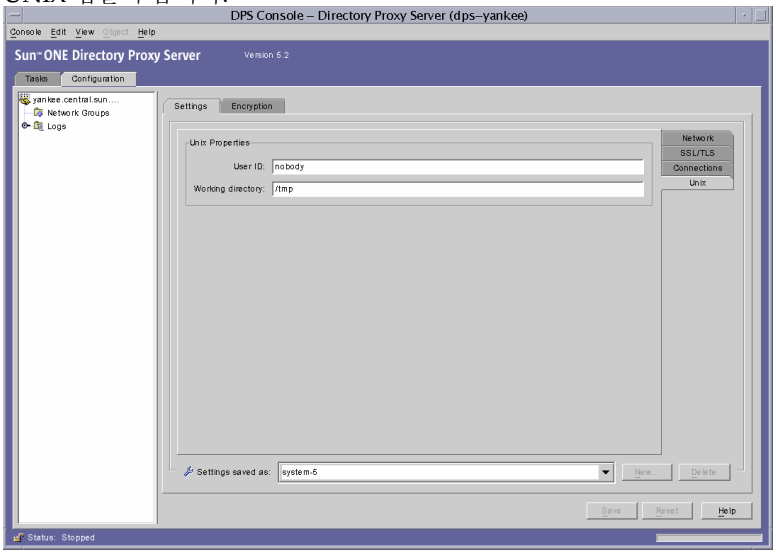
최대 연결 수 지정. 옵션을 선택하고 0보다 큰 값을 입력하여 Directory Proxy Server가 받아들일 수 있는 최대 동시 클라이언트 연결 수를 지정합니다. 동시 연결 수를 무제한 허용하려면 이 옵션을 선택하지 마십시오.

연결 풀 사용. Directory Proxy Server에서 디렉토리 서버로 미리 연결할 연결 풀 모듈을 설정합니다. 이 설정에 대한 기본값은 비활성화되어 있습니다. 연결 풀이 설정되면 Directory Proxy Server는 백엔드 LDAP 서버에 대한 기존 연결을 다시 사용하려 합니다. 백엔드 서버가 WAN에 있을 경우 이 옵션을 전환하면 성능이 상당히 향상될 수 있습니다. 다음 값을 입력합니다.

간격. 다음 작업을 예상하기 위해 Directory Proxy Server이 받는 요청을 샘플화하는 간격을 초 단위(0보다 크거나 같음)로 입력합니다. 기본값은 15입니다.

시간 초과 지정. 옵션을 선택하고 0보다 크거나 같은 시간을 초 단위(0보다 크거나 같음)로 입력하여 LDAP 서버에 대한 유휴 연결을 종료하기 전에 대기할 시간(초)을 지정합니다. 확인란이 선택되지 않은 경우 시간 초과가 적용되지 않습니다. 기본값은 30입니다. 이 값은 백엔드 LDAP 서버의 유휴 연결 시간 초과 값보다 작아야 합니다.

8. UNIX 탭을 누릅니다.

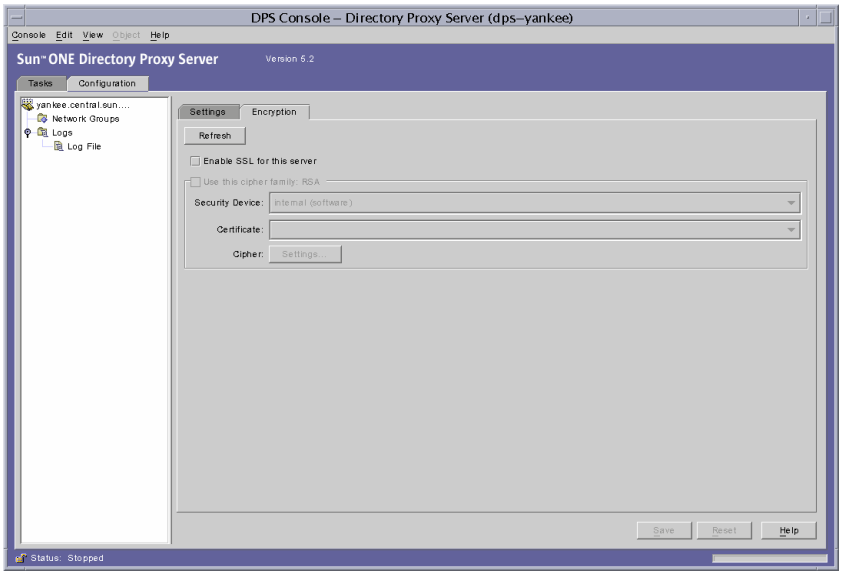


이 패널에는 UNIX 환경에서만 Directory Proxy Server 서버에 속하는 속성이 포함되어 있습니다.

사용자 아이디. Directory Proxy Server에서 실행할 사용자 아이디를 입력합니다. Directory Proxy Server가 *root*로 실행된 경우 해당 uid를 여기에 지정된 uid로 변경합니다. 기본값은 *nobody*로 전환하는 것입니다. 이 옵션은 Windows NT에서 적용할 수 없습니다.

작업 디렉토리. Directory Proxy Server가 실행될 디렉토리를 입력합니다. Directory Proxy Server는 해당 작업 디렉토리를 시작 시 이 속성 값으로 지정된 디렉토리로 변경합니다. 기본값은 `/tmp`입니다. 이 속성은 Windows NT 이외의 플랫폼에만 적용됩니다.

9. 암호화 탭을 선택하고 SSL 사용 통신에 대해 Directory Proxy Server를 구성합니다. SSL 통신을 위한 서버 구성과 관련한 자세한 내용은 보안 구성을 참조하십시오.



암호화 탭을 사용하면 다음 매개 변수를 구성할 수 있습니다.

갱신. 현재 화면 값을 갱신하려면 누릅니다. 새로 만든 인증서를 보려면 화면을 갱신합니다.

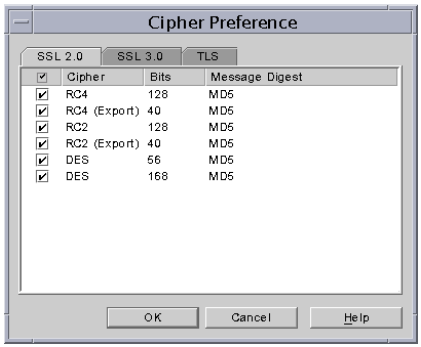
이 서버에 SSL 사용. Directory Proxy Server에서 보안 연결로 수신하는 데 필요한 SSL/TLS 정보를 활성화하려면 이 상자를 선택합니다. SSL 포트가 지정되어 있는 경우 이 구성을 저장하려면 이 설정을 지정해야 합니다.

이 암호 패밀리 RSA 사용. Directory Proxy Server의 이 인스턴스에 대해 보안 장치, 인증서 및 암호 설정을 지정하려면 이 상자를 선택합니다.

보안 장치. 사용 가능한 옵션에서 선택하려면 드롭다운 창을 누릅니다. 기본값은 내부(소프트웨어)입니다.

인증서. 사용 가능한 옵션에서 선택하려면 드롭다운 창을 누릅니다.

암호. SSL 2.0, SSL 3.0 및 TLS 암호 기본 설정을 지정하려면 설정을 선택합니다. SSL 2.0, SSL 3.0 및 TLS 탭을 누르고 각각에 대해 사용할 암호 옆에 있는 상자를 선택합니다.



10. 저장을 눌러 객체를 저장합니다.

Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 지금 서버를 다시 시작하지 말고, 모든 구성 변경을 완료한 후에 다시 시작하십시오.

11. 추가 객체를 만들려면 단계 3에서 단계 10까지 반복합니다.

12. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

주 설정 탭에서 호스트, 포트 및 "SSL 포트" 필드를 변경하면 Directory Proxy Server를 중지했다가 시작해야 합니다.

Directory Proxy Server 중지 및 시작에 대한 자세한 내용은 53페이지의 “Directory Proxy Server 시작 및 중지”를 참조하십시오.

구성 저장

`dpsconfig2ldif` 유틸리티는 Directory Proxy Server 구성을 다운로드하여 LDIF 파일에 저장하는 데 사용됩니다. 이 유틸리티는 다음 위치에서 참조할 수 있습니다.

```
<Install Root>/bin/dps_utilities/dpsconfig2ldif
```

이 유틸리티에는 다음과 같은 두 인수가 필요합니다.

인수	의미
-t *파일 이름*	*파일 이름*은 시작 구성 파일의 경로이며, 일반적으로 etc 디렉토리에 있는 tailor.txt 파일입니다.
-o *파일 이름*	구성을 출력할 파일 이름

6장

그룹 만들기 및 관리

LDAP 클라이언트가 LDAP 디렉토리에서 서비스를 요청할 때는 Sun ONE Directory Proxy Server에 연결한 다음 클라이언트 프로필에서 클라이언트의 액세스 권한을 식별하여 해당 클라이언트가 디렉토리로부터 서비스를 요청할 권한이 있는지 확인한 다음 구성된 제한을 적용한 다음 요청을 해당 디렉토리에 전달합니다. 이 장에서는 Directory Proxy Server 구성 편집기 콘솔을 사용하여 클라이언트를 식별하고 제한을 적용하도록 Directory Proxy Server를 구성하는 방법을 설명합니다.

이 장은 다음 내용으로 구성되어 있습니다.

그룹 개요

Directory Proxy Server 네트워크 그룹은 Directory Proxy Server의 작업 방법을 이해하는 핵심으로 Directory Proxy Server가 LDAP 클라이언트를 식별하는 방법과 Directory Proxy Server가 해당 그룹과 일치하는 클라이언트에 적용해야 하는 제한 사항을 정의합니다. 따라서, LDAP 클라이언트의 디렉토리 액세스를 효과적으로 제어하려면 Directory Proxy Server 그룹에 대해 잘 알고 있어야 합니다.

네트워크 그룹을 사용하여 다음을 식별합니다.

- 클라이언트
- Directory Proxy Server가 클라이언트의 요청을 전달할 수 있는 LDAP 디렉토리 집합입니다.

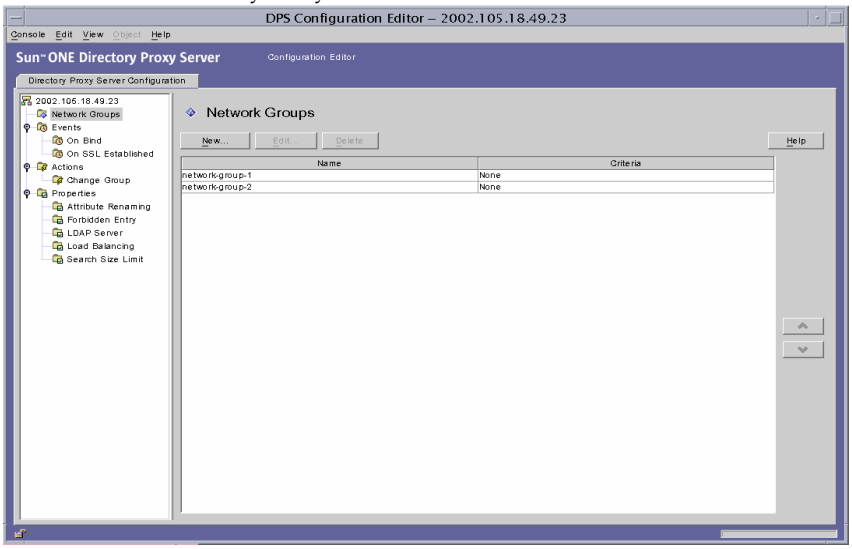
- 클라이언트가 디렉토리 집합과 상호 작용하면서 수행할 수 있는 일련의 작업입니다.
- 클라이언트가 디렉토리 집합과 상호 작용하면서 액세스할 수 있는 데이터입니다. Directory Proxy Server를 사용하면 디렉토리에서 특정 항목을 숨기고 속성 이름을 바꿀 수 있기 때문에 디렉토리 내부에서 클라이언트가 볼 수 있는 데이터를 효과적으로 제어할 수 있습니다.

Directory Proxy Server는 연결 시작 속성을 그룹 조건과 일치시켜 클라이언트에 대한 그룹 구성원을 결정합니다. 서버는 현재 구성된 그룹을 우선 순위가 가장 높은 그룹에서 가장 낮은 그룹으로 내림차순으로 검사합니다. 연결 시작 속성과 일치하는 첫 번째 네트워크 그룹 조건이 연결을 받습니다. 따라서, 일반 조건과 특정 조건별로 별도의 그룹을 만들어 가장 특정한 그룹에서 가장 일반적인 그룹까지 그룹의 우순 순위를 지정해야 합니다.

클라이언트와 일치하는 그룹이 없으면 클라이언트의 요청이 거부되고 연결이 끊깁니다. 따라서, Directory Proxy Server 구성에 하나 이상의 그룹 항목이 있어야 합니다.

그룹의 우선 순위는 Directory Proxy Server 구성 편집기 콘솔의 네트워크 그룹 창에서 배치된 순서에 의해 지정됩니다(그림 6-1 참조). 이 창에서 목록 아래쪽에 있는 그룹은 위쪽에 있는 그룹보다 우선 순위가 낮습니다. 우선 순위가 같은 그룹의 평가 순서는 정의되어 있지 않습니다.

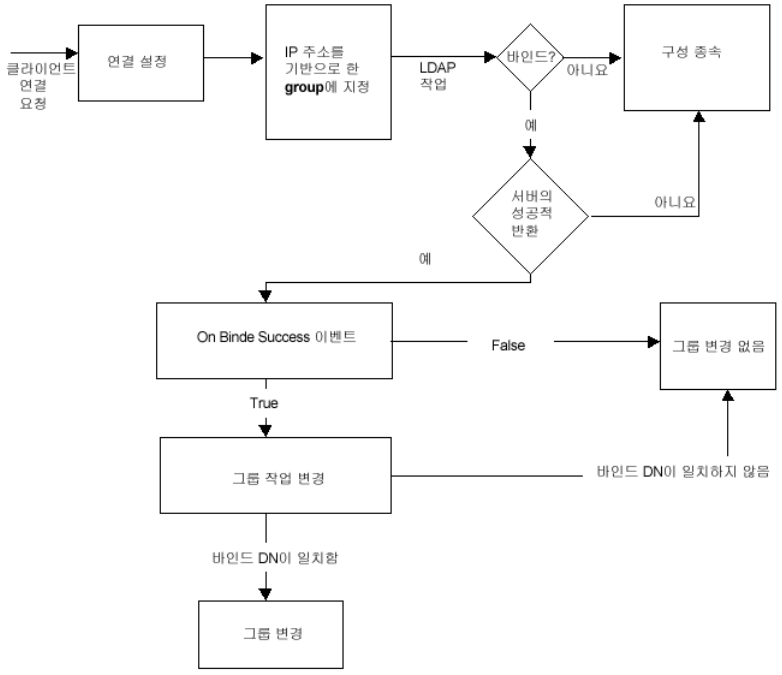
그림 6-1 Directory Proxy Server 구성 편집기 콘솔: 네트워크 그룹 창



클라이언트는 연결되는 네트워크 주소(예: IP 주소 및/또는 도메인 이름)를 기준으로 처음에는 하나의 그룹으로 식별됩니다. 성공적으로 바인드된 후에는 클라이언트가 자신의 그룹을 변경할 수 있습니다. 자세한 내용은 8장, “이벤트 객체 만들기 및 관리“를 참조하십시오. 클라이언트가 그룹의 구성원이 되면 그룹의 모든 등록 정보가 해당 클라이언트에게 적용됩니다.

그림 6-2에서는 Directory Proxy Server에서 클라이언트 쿼리에 응답하여 그룹을 평가하는 방법을 설명합니다.

그림 6-2 그룹 구성원 결정을 위한 Directory Proxy Server 결정 트리



그룹의 네트워크 조건은 다음을 기준으로 할 수 있습니다.

- 호스트의 IP 주소 또는 네트워크 마스크
  - 단일 IP 주소(예: `129.153.129.14`)
  - IP 쿼드/일치 비트(예: `129.153.129.0/24`)
  - IP 쿼드/일치 쿼드(예: `129.153.129.0/255.255.255.128`)
- 호스트의 도메인 이름
  - 전체 이름(예: `box.eng.sun.com`)
  - 접미사 이름(예: `.eng.sun.com`)

클라이언트를 식별하는 데 도메인 이름 접미사 규칙을 사용하는 경우에는 DNS 쿼리에 대해 정규화된 이름을 반환하도록 DNS를 설정해야 합니다. 단축 이름이 반환되는 경우에는 이 기능을 사용할 수 없습니다.

- 특수
  - 모두("catch-all" 그룹에 사용)

- `0.0.0.0`(클라이언트가 바인드될 때 클라이언트를 전환하는 데만 그룹을 사용하는 경우처럼 초기 구성원이 고려되지 않는 그룹에 사용)

Directory Proxy Server가 그룹을 평가하는 방법과 관련된 자세한 내용은 표 6-1에 나열된 샘플 그룹을 참조하십시오. 이 표에는 일반 네트워크 조건에 따라 만들어지고 우선 순위 내림차순으로 나열된 5개의 그룹이 있습니다.

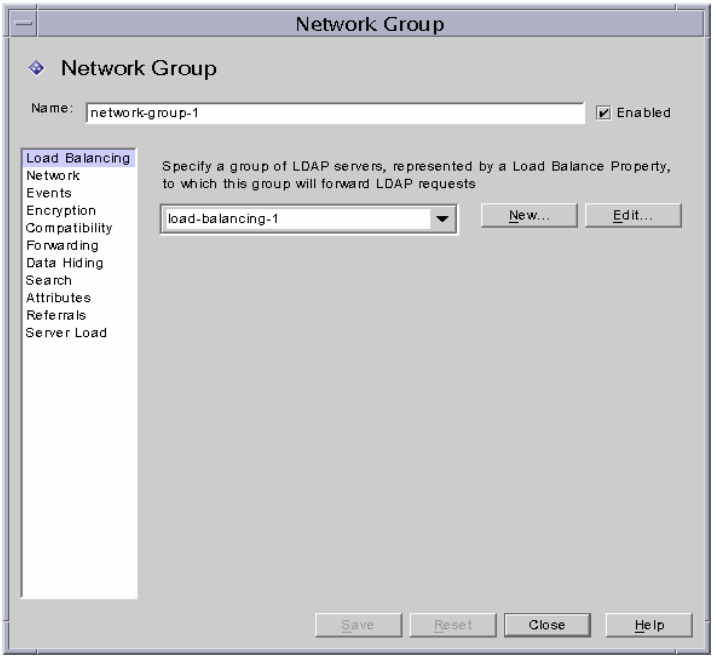
표 6-1 샘플 그룹

우선 순위	그룹 이름	네트워크 조건
5	Admin-machine	129.153.129.72
4	IT-management-subnet	129.153.120.0/24
3	Operations	.ops.sun.com
2	Catch-all	ALL
1	Trusted	0.0.0.0

LDAP 클라이언트가 LDAP 디렉토리로부터 서비스를 요청하면 Directory Proxy Server는 IP 주소 `129.153.129.72`에서 요청되었는지를 확인합니다. 이 IP 주소에서 요청된 것이 아니면 Directory Proxy Server는 요청이 `129.153.129.0/24`와 일치하는지 확인합니다. 역시 일치하지 않으면 Directory Proxy Server는 요청이 `.ops.sun.com`에서 시작되었는지 확인합니다. 이 경우도 아니면 Directory Proxy Server는 `catch-all` 그룹에 연결을 배치한 다음 결정 트리의 다음 단계로 이동합니다(그림 6-2 참조).

그림 6-3에서는 그룹을 만들 수 있는 Directory Proxy Server 구성 편집기 콘솔 부분을 보여 줍니다.

그림 6-3 Directory Proxy Server 네트워크 그룹 정의



네트워크 그룹을 만들 때 조건의 조합을 지정할 수 있습니다. 조건의 조합은 표 6-2에 요약되어 있습니다.

표 6-2 사용 가능한 네트워크 그룹 조건 목록

조건	설명
로드 균형 조정	LDAP 요청을 로드 균형 등록 정보에 전달하고 이 등록 정보에 표시된 LDAP 서버 그룹을 지정할 수 있습니다. 자세한 내용은 121페이지의 “로드 균형 조정 등록 정보”를 참조하십시오.
네트워크	클라이언트 요청이 해당 그룹에 정렬되거나 필터링되도록 클라이언트에 대한 연결 정보와 기타 네트워크 조건을 지정할 수 있습니다.
이벤트	클라이언트가 지정된 디렉토리에 성공적으로 바인드한 후 그룹을 효과적으로 변경할 수 있도록 그룹에 연결할 이벤트(있는 경우)를 지정할 수 있습니다. 이벤트에 대한 기존 객체 목록을 표시합니다. 자세한 내용은 80페이지의 “그룹 만들기”를 참조하십시오.

표 6-2 사용 가능한 네트워크 그룹 조건 목록 *(계속)*

조건	설명
암호화	그룹에 대한 암호화 조건을 지정할 수 있습니다(예: 클라이언트가 SSL 세션을 요청할 수 있는지 여부 지정).
호환성	LDAP v2 사양(RFC 1777)에서는 클라이언트가 한 세션에서 여러 번 바인드할 수 없도록 합니다. 하지만 일부 클라이언트에서는 이 기능이 필요합니다. 이러한 클라이언트와 상호 운용되도록 이 옵션을 설정할 수 있습니다.
전달	바인드, 비교 및 기타 LDAP 요청을 서버에 전달하는 조건을 지정할 수 있습니다.
데이터 숨기기	그룹에서 숨길 디렉토리 내의 하위 트리, 항목, 항목 속성 등을 지정할 수 있습니다. 금지 항목 등록 정보에 대한 기존 객체 목록을 표시합니다. 자세한 내용은 111페이지의 “금지 항목 등록 정보”를 참조하십시오.
검색	그룹에 대한 검색 범위와 크기 제한을 지정할 수 있습니다. 검색 크기 제한 등록 정보에 대한 기존 객체 목록을 표시합니다. 자세한 내용은 125페이지의 “검색 크기 제한 등록 정보”를 참조하십시오.
속성	특정 종류의 검색 및 비교 작업을 LDAP 서버에 전달하지 못하도록 금지하는 규칙을 지정할 수 있습니다. 속성 이름 바꾸기 등록 정보에 대한 기존 객체 목록을 표시합니다. 자세한 내용은 108페이지의 “속성 이름 바꾸기 등록 정보”를 참조하십시오.
참조	그룹이 서버에서 반환되는 참조를 전달할지, 따를지, 무시할지 여부를 지정할 수 있습니다. LDAPv3을 구현하지 않은 클라이언트는 전달된 참조를 이해하지 못합니다. 이 설정은 연속적인 검색 참조를 제외한 모든 참조에 적용됩니다.
서버 로드	그룹에 대한 총 연결 수, 연결 당 동시/총 작업 수, IP 주소 당 동시 작업 수 등과 같은 세부 정보를 지정할 수 있습니다.

그룹 만들기

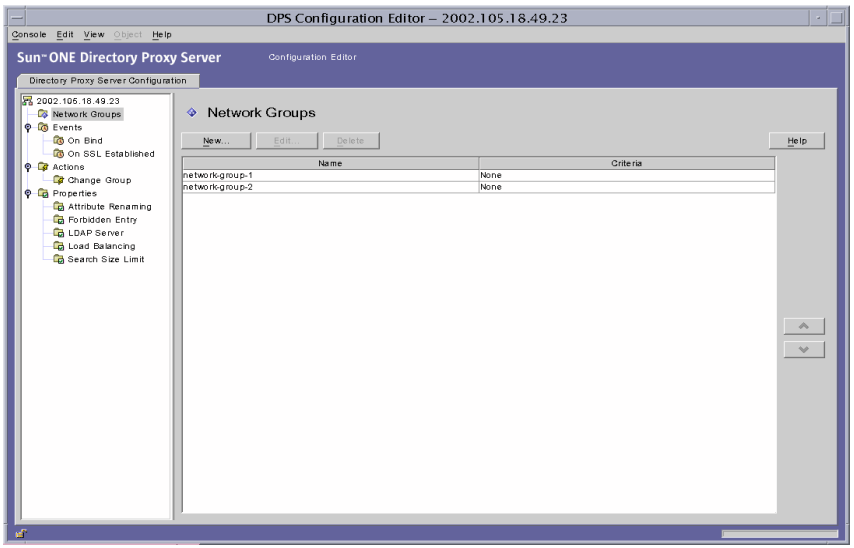
이 절에서는 Directory Proxy Server 구성 편집기 콘솔을 사용하여 그룹을 만드는 방법을 설명합니다. 그룹 만들기를 시작하기 전에 73페이지의 “그룹 개요” 절을 읽어보고 Directory Proxy Server 그룹의 중요성을 이해해야 합니다. 필요한 그룹을 만들고 우선 순위를 지정한 후 구성을 테스트하여 해당 그룹이 클라이언트 요청을 올바르게 필터링하는지 확인해야 합니다.

네트워크 그룹을 만들 때 다양한 조건을 지정할 수 있습니다. 이 절에 제공된 지침에서는 이러한 모든 조건을 UI에 나타나는 순서대로 표시하고, 사용자의 판단에 따라 그룹에 적절한 조건을 설정하도록 합니다.

Directory Proxy Server에서 네트워크 그룹을 만들려면 다음 단계를 따르십시오.

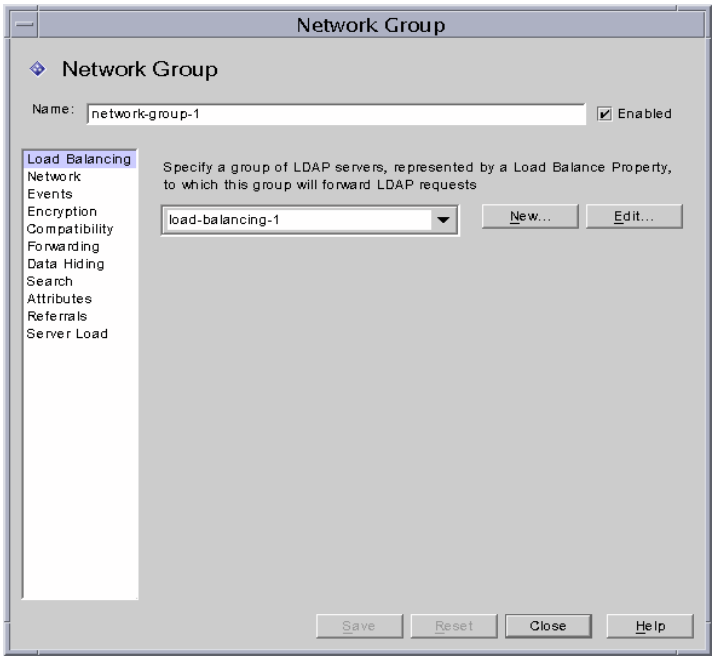
1. Directory Proxy Server 구성 편집기 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.
2. 탐색 트리에서 네트워크 그룹을 선택합니다.

   오른쪽 창에 기존 그룹의 목록이 표시됩니다.



3. 새로 만들기를 누릅니다.

   네트워크 그룹 창이 나타납니다.



4. 이름 필드에 그룹 이름을 입력합니다. 이 이름은 고유한 영숫자 문자열이어야 합니다.

5. 사용 가능 옵션이 선택되었는지 확인합니다. 기본적으로 이 옵션은 선택되어 있습니다. 그룹이 Directory Proxy Server 구성의 일부가 되게 하려면 이 옵션을 선택해야 합니다. 구성에서 그룹을 비활성화려면 이 옵션을 선택 취소합니다.

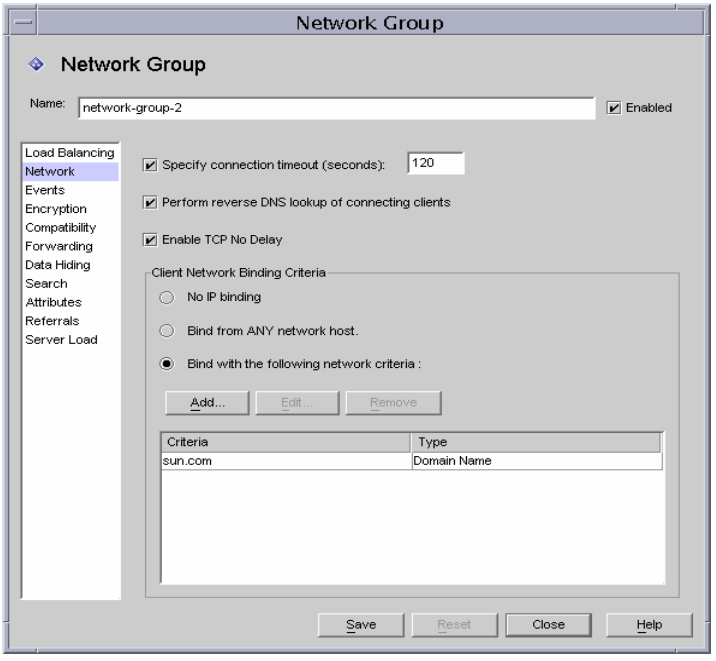
6. 원한다면 드롭다운 메뉴에서 로드 균형 등록 정보를 지정합니다. 이 등록 정보는 이 그룹에서 로드 균형 등록 정보를 사용하여 클라이언트의 요청을 처리하기 위해 LDAP 요청을 전달할 LDAP 서버의 그룹을 식별합니다. 관련된 드롭다운 목록에 로드 균형 등록 정보에 대한 기존 객체가 표시됩니다. 121페이지의 "로드 균형 조정 등록 정보"를 참조하십시오. 적절한 객체를 선택합니다. 기본적으로 객체가 선택되지 않습니다(<없음>). 객체가 없으면 새로 만들기 버튼을 눌러 신속하게 객체를 만들 수 있습니다.

   새로 만들기. 새 로드 균형 등록 정보를 만들 대화 상자를 표시합니다.

   편집. 기존 로드 균형 등록 정보를 편집할 대화 상자를 표시합니다.

7. 요청을 정렬 또는 필터링할 그룹에 대한 네트워크 조건을 지정하려면 왼쪽 프레임에서 네트워크를 선택합니다. 그런 다음 화면의 요소 설명을 참조하여 적절한 네트워크 값을 지정합니다.

- 커넥터 시간 초과를 지정합니다. 기본적으로 값이 표시되지 않습니다. 즉, 연결 시간 초과가 적용되지 않습니다.
- 클라이언트 연결에 대해 역방향 DNS 조회를 사용합니다.
- TCP 지연 없음 사용을 선택합니다.
- 클라이언트 네트워크 바인드 조건을 정의합니다.



다음은 화면에 표시되는 요소에 대한 설명입니다.

연결 시간 초과 지정. Directory Proxy Server에서 클라이언트에 대한 연결을 끊은 후의 클라이언트 비활성 기간을 입력하려면 이 상자를 선택합니다. 이 값은 초 단위의 숫자이며 일반적으로 120 이상입니다. 기본적으로 값이 표시되지 않습니다. 즉, 연결 시간 초과가 적용되지 않습니다. TCP 연결 유지가 활성화되지 않은 경우 이 속성이 있어야 Directory Proxy Server가 끊긴 클라이언트 연결로 인해 방해를 받지 않습니다.

클라이언트 연결에 대해 역방향 DNS 조회 수행. 기본적으로 이 옵션은 활성화되어 있습니다. 역방향 DNS 조회가 비활성화되어 있으면 Directory Proxy Server는 연결하는 클라이언트의 도메인 이름을 찾을 때 역방향 DNS 조회를 수행하지 않습니다. 역방향 DNS 조회를 비활성화하면 Directory Proxy Server 성능이 크게 향상되는 경우가 있습니다. 도메인 이름이나 도메인 이름 접미사를 "클라이언트 네트워크 바인드 조건"의 값으로 사용한 경우 역방향 DNS 조회를 활성화해야 합니다. 그렇지 않으면 Directory Proxy Server가 제대로 작동하지 않습니다. 조회 쿼리에 전체 호스트 이름을 반환하도록 DNS를 구성해야 합니다.

TCP 지연 없음 사용. 기본적으로 이 옵션은 활성화되어 있습니다. 이 옵션이 비활성화되어 있으면 Directory Proxy Server는 자신과 이 그룹에 속한 클라이언트 간의 연결에 Nagle 알고리즘을 사용하지 않습니다. Directory Proxy Server와 클라이언트 간의 네트워크 대역폭이 작은 경우에만 "TCP 지연 없음"을 비활성화해야 합니다. 하지만 이때 성능이 크게 저하될 수 있습니다.

클라이언트 네트워크 바인드 조건. 이 절에서는 이 네트워크 그룹에서 바인드할 수 있는 클라이언트를 지정합니다.

IP 바인드 없음. 클라이언트가 그룹에 바인드할 때만 전환될 경우 이 옵션을 선택합니다. 기본적으로 이 옵션은 선택되어 있습니다. 클라이언트가 바인드될 때 클라이언트를 전환하는 데만 그룹을 사용하는 경우 이 옵션을 선택 취소합니다.

모든 네트워크 호스트에서 바인드. 이 네트워크 그룹에서 모든 호스트가 바인드할 수 있는 경우 이 옵션을 선택합니다.

다음 조건으로 바인드. 네트워크 그룹과 일치하는 호스트의 도메인 이름 또는 IP 주소를 지정하려면 이 옵션을 선택합니다. 이 경우 그룹은 바인드되는 호스트의 도메인 이름 또는 IP 주소를 지정해야 합니다.

추가. 네트워크 조건을 추가할 대화 상자를 표시합니다. "도메인 이름", "IP 주소", "IP 주소 및 비트", "IP 및 쿼드"의 네 가지 옵션이 있습니다.

편집. 네트워크 조건을 편집할 대화 상자를 표시합니다.

제거. 네트워크 조건을 제거할 대화 상자를 표시합니다.

도메인 이름 대화 상자.네트워크 그룹에 바인드할 수 있는 클라이언트의 도메인 이름 접미사 또는 클라이언트의 전체 이름(예: `foo.sun.com`)을 지정합니다. Directory Proxy Server는 기본적으로 도메인 접미사를 가정하지 않습니다. 따라서 전체 도메인 이름을 제공해야 합니다. 앞에 마침표가 있는 도메인 이름 접미사(예: `.sun.com`)는 해당 접미사로 끝나는 도메인 이름을 가진 모든 호스트를 일치시킵니다.

또한, 도메인 이름 접미사 규칙을 사용하여 클라이언트를 식별하는 경우 DNS 쿼리에 정규화된 이름을 반환하도록 DNS를 설정해야 합니다. 단축 이름이 반환되는 경우에는 이 기능을 사용할 수 없습니다.

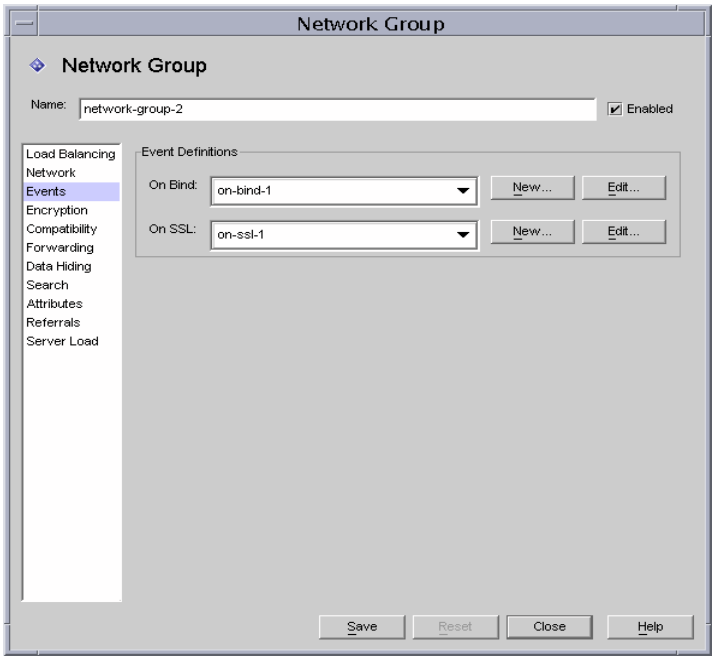
IP 주소. 점으로 구분된 십진수 형식(예: `198.214.11.1`)으로 단일 IP 주소를 지정합니다.

IP 주소 및 비트. <네트워크 번호>/<마스크 비트> 형식(예: `198.241.11.0/24`)으로 IP 네트워크 마스크를 지정합니다. 처음 반은 네트워크 번호이고 나머지 반은 일치시키는 데 필요한 네트워크 번호의 비트 수를 나타냅니다.

IP 주소 및 쿼드. 점으로 구분된 4개의 십진수 한 쌍(예: `198.241.11.0/255.255.255.128`)으로 IP 네트워크 마스크를 지정합니다. 처음 반은 네트워크 번호이고 나머지 반은 일치시키는 데 필요한 네트워크 번호의 비트를 나타냅니다. 예를 들어, `198.214.11.0/255.255.255.128`은 IP 주소가 `198.214.11.63`인 호스트와 일치하지만 IP 주소가 `198.214.11.191`인 호스트와는 일치하지 않습니다.

도메인 이름이나 도메인 이름 접미사를 사용하려면 "클라이언트 연결에 대해 역방향 DNS 조회 수행"이 활성화되어 있어야 합니다.

8. 이벤트 구동 작업을 그룹에 연결하려면(예: 다른 그룹으로 클라이언트 변경) 왼쪽 프레임에서 이벤트를 선택하고 오른쪽 프레임에서 해당 값을 지정합니다.



다음은 화면에 표시되는 요소에 대한 설명입니다.

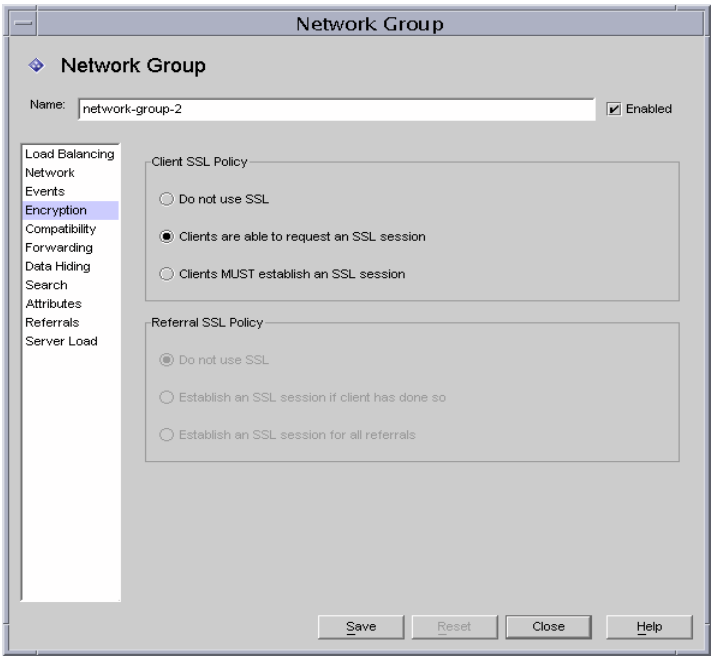
바인드. 드롭다운 목록에 OnBindSuccess 이벤트에 대한 기존 객체가 표시됩니다. 132페이지의 "OnBindSuccess 이벤트 객체 만들기"를 참조하십시오. 클라이언트가 바인드 작업을 성공적으로 완료하면 수행될 객체의 이름을 선택합니다. 기본적으로 객체가 선택되지 않습니다(<없음>). 객체가 없으면 새로 만들기 버튼을 눌러 신속하게 객체를 만들 수 있습니다.

SSL. 드롭다운 목록에 OnSSLEstablished 이벤트에 대한 기존 객체가 표시됩니다. 135페이지의 "OnSSLEstablished 이벤트 객체 만들기"를 참조하십시오. 클라이언트가 SSL 세션을 성공적으로 설정하면 수행될 객체의 이름을 선택합니다. 객체가 없으면 새로 만들기 버튼을 눌러 신속하게 객체를 만들 수 있습니다.

편집. 이벤트 동작을 편집할 대화 상자를 표시합니다.

새로 만들기. 새 이벤트를 만들 대화 상자를 표시합니다.

9. 그룹에 대한 암호화 조건을 지정하려면(예: 클라이언트가 SSL 세션을 요청할 수 있는지 여부 지정) 왼쪽 프레임에서 암호화를 선택하고 오른쪽 프레임에서 해당 값을 지정합니다.



다음은 화면에 표시되는 요소에 대한 설명입니다.

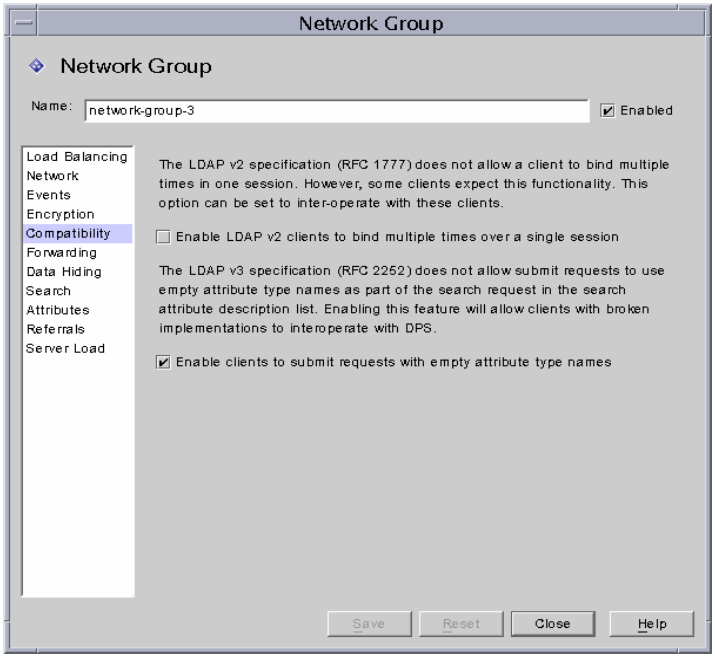
클라이언트 SSL 정책. 클라이언트 SSL 정책을 구성합니다.

- **SSL 사용 안 함.** SSL 암호화를 사용하지 않으려면 이 옵션을 선택합니다.
- **클라이언트가 SSL 세션을 요청할 수 있음.** 그룹의 클라이언트가 SSL을 요청하는 SSL 세션을 설정하는 경우 이 옵션을 선택합니다.
- **클라이언트가 SSL 세션을 설정해야 함.** 그룹의 클라이언트가 작업을 수행하기 전에 SSL 세션을 설정해야 할 경우 이 옵션을 선택합니다.

참조 SSL 정책. SSL 정책을 구성하면서 참조를 따릅니다.

- **SSL 사용 안 함.** SSL 암호화를 사용하지 않으려면 이 옵션을 선택합니다.
- **클라이언트가 SSL 세션을 설정한 경우 SSL 세션 설정.** 이 옵션을 사용하면 Directory Proxy Server는 클라이언트가 이미 Directory Proxy Server와 SSL 세션을 이미 설정한 경우 해당 그룹의 클라이언트에 대해서만 SSL을 시작합니다.
- **모든 참조에 대해 SSL 세션 설정.** 참조 시 작업이 전달되기 전에 Directory Proxy Server가 SSL 세션을 시작할 경우 이 옵션을 활성화합니다.

10. 그룹에 대한 호환성 조건을 지정하려면(예: 클라이언트가 한 세션에서 여러 번 바인드할 수 있도록 허용) 왼쪽 프레임에서 호환성을 선택하고 오른쪽 프레임에서 해당 값을 지정합니다.



다음은 화면에 표시되는 요소에 대한 설명입니다.

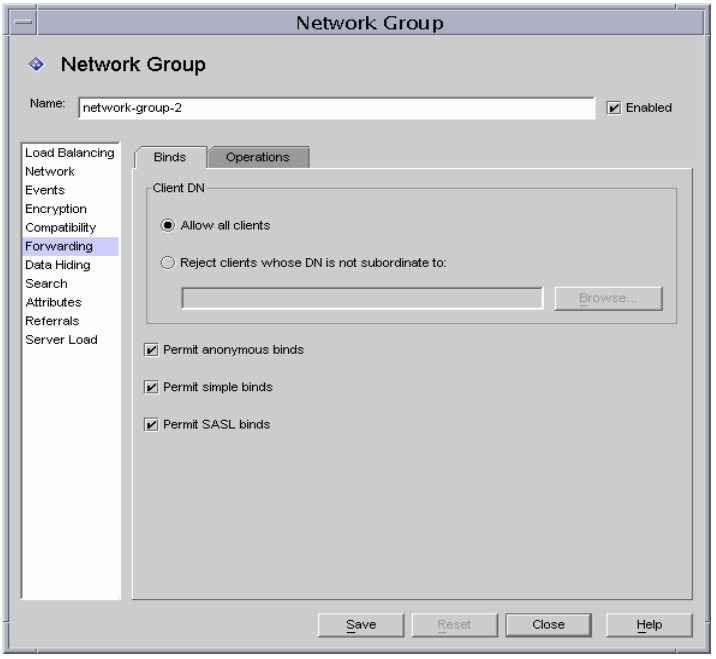
LDAP v2 클라이언트가 한 세션에서 여러 번 바인드할 수 있게 함. LDAP v2 사양(RFC 1777)에서는 클라이언트가 한 세션에서 여러 번 바인드할 수 없도록 합니다. 하지만 일부 클라이언트에서는 이 기능이 필요합니다. 이 그룹에서 클라이언트가 속성 요청 목록에 하나 이상의 속성이 NULL인 검색 요청을 제출할 수 있게 하려면 이 옵션을 선택합니다. 이 호환성 기능을 사용하면 Directory Proxy Server에서 일부 차단된 JAVA 기반 클라이언트와 상호 작용할 수 있습니다. 속성 요청 목록의 NULL 속성 이름을 사용하면 LDAP 프로토콜을 위반하는 것입니다. 기본적으로 이 옵션은 TRUE로 설정되어 있습니다.

클라이언트가 빈 속성 유형 이름을 사용하여 요청을 제출할 수 있게 함. 그룹에서 요청이 속성 유형 이름을 식별하지 않더라도 클라이언트가 요청을 제출할 수 있게 하려면 이 옵션을 선택합니다.

11. 그룹에 대한 요청 전달 조건을 지정하려면 왼쪽 프레임에서 전달을 선택하고 오른쪽 프레임에서 해당 값을 지정합니다.

Directory Proxy Server가 클라이언트의 연결을 받아들이고 일치하는 그룹을 찾으면 클라이언트가 LDAP 작업을 보낼 때까지 기다립니다. Directory Proxy Server는 "클라이언트 DN", "익명 바인드 허용", "SASL 바인드 허용" 등을 사용하여 바인드 요청을 서버에 전달하는지 바인드 요청을 거부하고 클라이언트 연결을 닫을지 여부를 결정합니다.

클라이언트의 바인드에서 활성화된 테스트를 전달하면 Directory Proxy Server는 해당 테스트를 서버로 전달합니다. 서버가 바인드를 허용하면 연결이 설정됩니다. 그러나 서버가 바인드 요청에 대해 오류 표시를 반환하면 Directory Proxy Server는 오류 표시를 클라이언트에 전달한 다음 클라이언트가 LDAPv2를 사용하는 경우 클라이언트에 대한 연결을 끊습니다.



다음은 바인드 탭의 요소에 대한 설명입니다.

모든 클라이언트 허용. 기본적으로 이 옵션은 활성화되어 있으므로 모든 클라이언트의 액세스가 허용됩니다.

DN이 종속되지 않은 클라이언트 거부. 그룹이 고유 이름(DN)을 확인하게 하려면 이 옵션을 선택합니다. 지정된 DN에 종속되지 않은 고유 이름을 바인드에 제공하는 클라이언트는 모두 거부됩니다. 찾아보기 버튼을 사용하여 DN을 구성할 LDAP 디렉토리를 찾습니다.

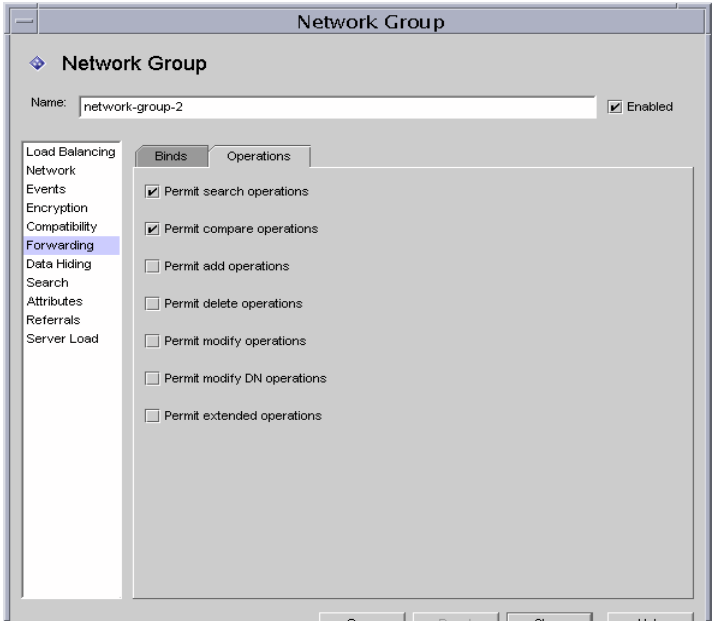
익명 바인드 허용. 기본적으로 이 옵션은 활성화되어 있으며 클라이언트가 비밀번호를 제공하지 않아도 바인드를 허용합니다. 익명 바인드를 금지하려면 이 옵션을 비활성화합니다.

단순 바인드 허용. 기본적으로 이 옵션은 활성화되어 있으며 클라이언트가 일반 텍스트로 비밀번호를 제공할 수 있습니다. 일반 텍스트 비밀번호로 인증된 바인드 요청을 금지하려면 이 옵션을 비활성화합니다.

SASL 바인드 허용. 기본적으로 이 옵션은 활성화되어 있으며 SASL 바인드를 허용할 것인지 여부를 지정합니다. SASL 인증을 금지하려면 이 옵션을 비활성화합니다.

12. 작업 탭을 선택하고 전달할 작업을 지정합니다.

Directory Proxy Server는 기본적으로 검색 및 비교 요청을 전달합니다. 또한, Directory Proxy Server는 언바인드 요청을 인식하고 LDAP 서버에 대한 연결을 끊습니다.



다음은 작업 탭의 요소에 대한 설명입니다.

검색 작업 허용. 기본적으로 이 옵션은 활성화되어 있습니다. Directory Proxy Server가 검색 요청을 서버에 전달하지 못하게 하려면 이 옵션을 비활성화합니다.

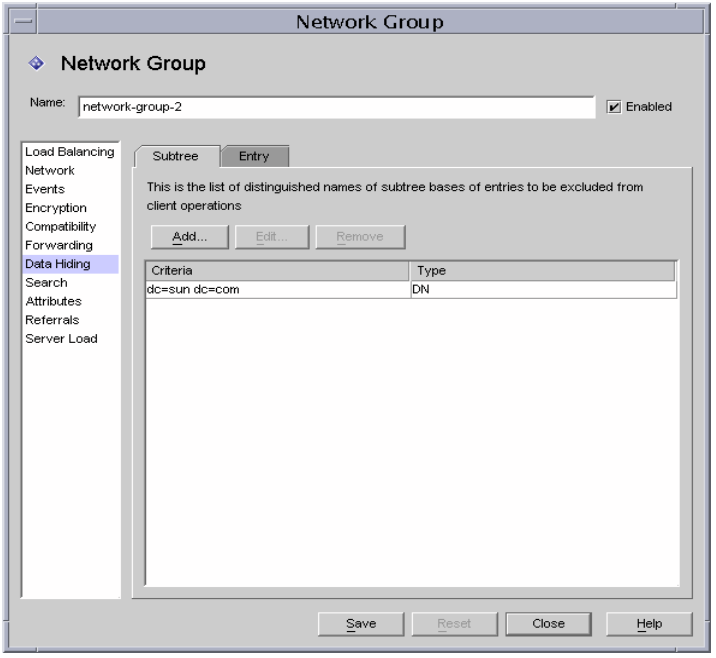
비교 작업 허용. 기본적으로 이 옵션은 활성화되어 있습니다. Directory Proxy Server가 비교 요청을 서버에 전달하지 못하게 하려면 이 옵션을 비활성화합니다.

추가, 삭제, 수정, DN 수정 및 확장 작업 허용. 기본적으로 Directory Proxy Server는 추가, 수정, 삭제, DN 수정 또는 확장 작업 요청을 전달하지 않습니다. 이러한 작업 전달을 허용하려면 허용할 해당 작업을 활성화합니다.

클라이언트가 TLS 시작을 교섭할 수 있게 하려면 "확장 작업 허용"을 활성화해야 합니다.

13. 그룹에 대한 데이터 숨기기 조건을 지정하려면 왼쪽 프레임에서 데이터 숨기기를 선택하고 오른쪽 프레임에서 해당 값을 지정합니다.

    숨길 디렉토리 트리 부분을 지정하려면 하위 트리 탭을 사용하고 숨길 항목 또는 속성을 지정하려면 항목 탭을 사용합니다.



다음은 하위 트리 탭의 요소에 대한 설명입니다.

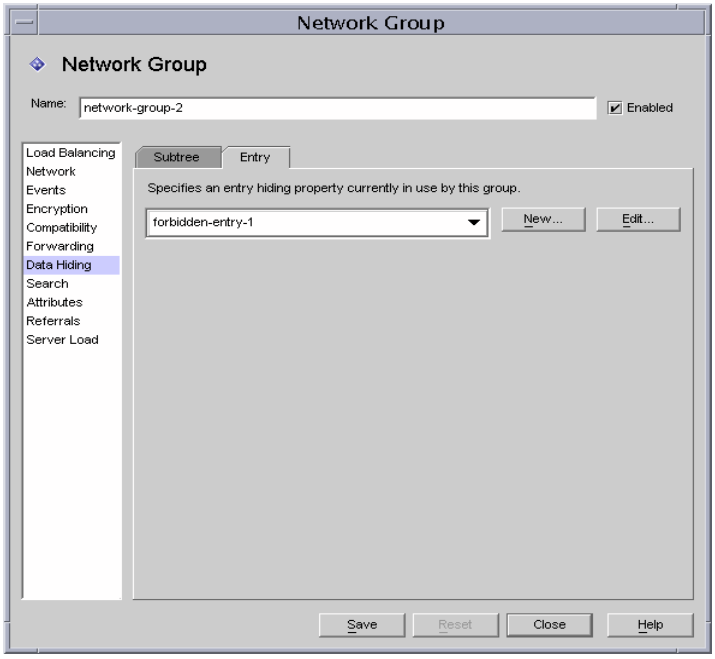
하위 트리 항목 숨기기. 금지된 하위 트리에 있는 항목이나 그 아래에 있는 항목을 요청하는 작업은 액세스 권한 부족 오류로 거부됩니다. 검색 필터와 일치하는 항목과 금지된 하위 트리 내에 있는 항목은 삭제됩니다. 이 옵션은 DN 구문 속성의 값이 해당 하위 트리에 속하는 경우에는 결과의 일부로 반환되는 항목으로부터 이 속성을 제거하지 않습니다.

추가. 제외할 항목의 하위 트리 기준 목록에 고유 이름을 추가하는 대화 상자를 표시합니다. 고유 이름이 네트워크 그룹에 없으면 기본적으로 디렉토리의 모든 항목에 대한 액세스가 허용됩니다. 목록의 항목에는 DN 구문이 있습니다.

편집. 고유 이름을 편집할 대화 상자를 표시합니다.

제거. 목록에서 고유 이름을 제거합니다.

14. 항목 탭을 선택하고 숨길 항목 또는 속성을 지정합니다.



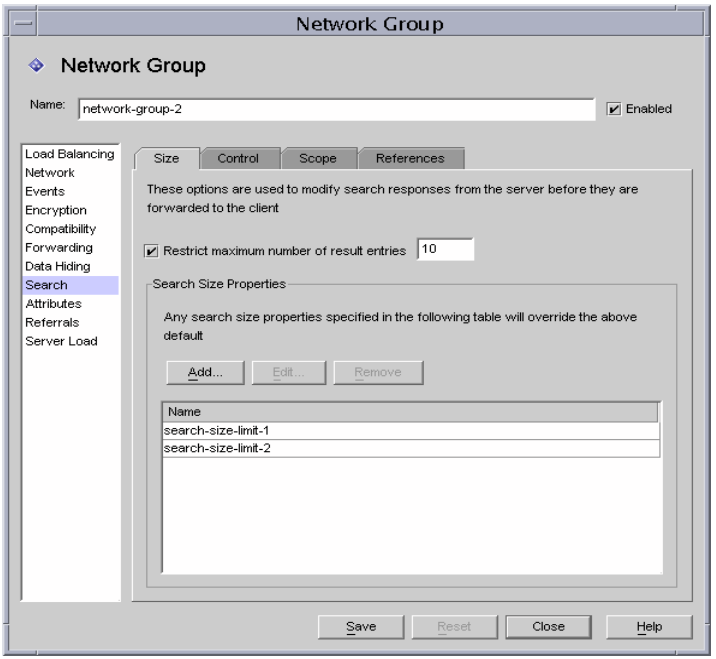
다음은 항목 탭의 요소에 대한 설명입니다.

이 그룹에서 현재 사용 중인 항목 숨기기 등록 정보 지정. 드롭다운 목록에 금지 항목 등록 정보에 대한 기존 객체가 표시됩니다. 111페이지의 “금지 항목 등록 정보”를 참조하십시오. 객체 이름 선택. 기본적으로 객체가 선택되지 않습니다(<없음>). 객체가 없으면 새로 만들기 버튼을 눌러 신속하게 객체를 만들 수 있습니다.

새로 만들기. 새 금지 항목 등록 정보를 만들 대화 상자를 표시합니다.

편집. 기존 금지 항목 등록 정보를 편집할 대화 상자를 표시합니다.

15. 그룹에 대한 검색 속성을 지정하려면 왼쪽 프레임에서 검색을 선택하고 오른쪽 프레임에서 해당 값을 지정합니다.



다음은 크기 탭의 요소에 대한 설명입니다.

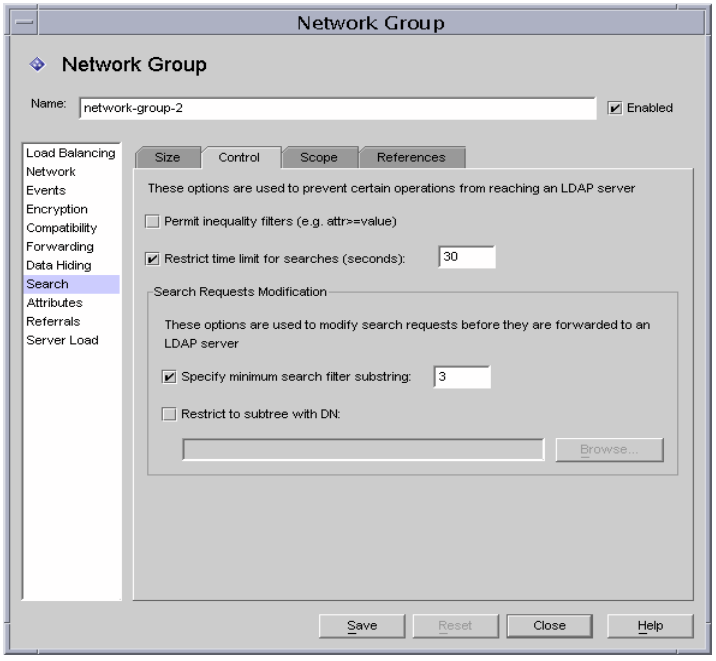
최대 결과 항목 수 제한. 단일 검색 작업에서 한 클라이언트에게 한 번에 반환될 수 있는 최대 결과 항목 수를 지정하려면 이 옵션을 설정합니다. 이 값은 0보다 큰 수일 수 있고 한계에 도달하면 `administrativeLimitExceeded` 오류를 일으켜 클라이언트와 다음 항목이 무시됩니다. 기본적으로 이 등록 정보가 비활성화되어 있으면 항목을 무시하지 않습니다.

추가. 검색 크기 제한 등록 정보를 추가할 대화 상자를 표시합니다. 자세한 내용은 125페이지의 "검색 크기 제한 등록 정보"를 참조하십시오.

편집. 검색 크기 제한 등록 정보를 편집할 대화 상자를 표시합니다.

제거. 검색 크기 제한 등록 정보를 제거할 대화 상자를 표시합니다. 이 작업은 대화 상자를 표시하지 않고 등록 정보를 그룹에서 제거합니다.

16. 제어 탭을 선택하고 검색 필터 제어를 위한 조건을 지정합니다.



다음은 제어 탭의 요소에 대한 설명입니다.

부등호 필터 허용. 기본적으로 이 옵션은 활성화되어 있습니다. 부등호 필터 허용은 클라이언트가 부등호 필터 (`attr>=value`) 및 (`attr<=value`)가 있는 검색을 요청할 수 있는지 여부를 지정합니다. 네트워크 그룹이 다른 검색을 수행할 수 없도록 하려면 이 옵션을 비활성화합니다.

검색 시간 제한. 네트워크 그룹이 검색 작업을 할 수 있는 최대 시간을 지정하려면 이 옵션을 활성화하고 값을 초 단위로 입력합니다. 클라이언트가 이 옵션에 제공된 값보다 큰 시간 제한을 지정하면 이 네트워크 그룹에 지정된 값에 의해 클라이언트의 요청이 무시됩니다. 기본적으로 이 옵션은 비활성화되어 있으므로 네트워크 그룹에서 클라이언트가 시간 제한(예: 제한 없음)을 설정하도록 할 수 있습니다.

최소 검색 필터 하위 문자열 지정. 검색 필터에서 허용 가능한 하위 문자열 길이를 지정하려면 이 옵션을 활성화하고 값을 입력합니다. 이 값은 1보다 커야 합니다. 기본적으로 이 옵션이 비활성화되어 있으므로 검색 필터에서 하위 문자열의 길이에는 제한이 없습니다. 웹 로봇이 수행할 수 있는 검색 종류를 제한하려면 네트워크 그룹에서 이 옵션을 활성화해야 합니다. 예를 들어, 값 2는 (cn=A*)와 같은 검색을 차단합니다.

주 이 속성은 기존 필터(attrname=*)에는 영향을 미치지 않습니다. 특정 기존 필터를 허용하지 않으려면 금지 비교 구성을 사용합니다.

DN이 있는 하위 트리 제한. 이 옵션을 활성화하고 모든 작업에 대해 하위 트리의 기준을 지정합니다. 이 옵션에는 DN 구문이 있습니다. 이 옵션이 비활성화되어 있는 경우 최소 기준에 제한이 없습니다.

이 옵션은 최소 기준 항목이나 최소 기준 항목 아래에 있는 대상 항목의 작업에 영향을 줍니다. 대상 항목이 최소 기준 항목보다 상위인 상태에서 하위 트리 검색 작업을 하면 쿼리를 서버에 보내기 전에 대상 항목을 최소 기준이 되도록 다시 작성합니다. 대상 항목이 최소 기준 이하이거나 최소 기준보다 상위이면 그러한 객체 오류 없이 요청이 거부됩니다.

예를 들어, "DN이 있는 하위 트리 제한"을 다음과 같이 설정하고

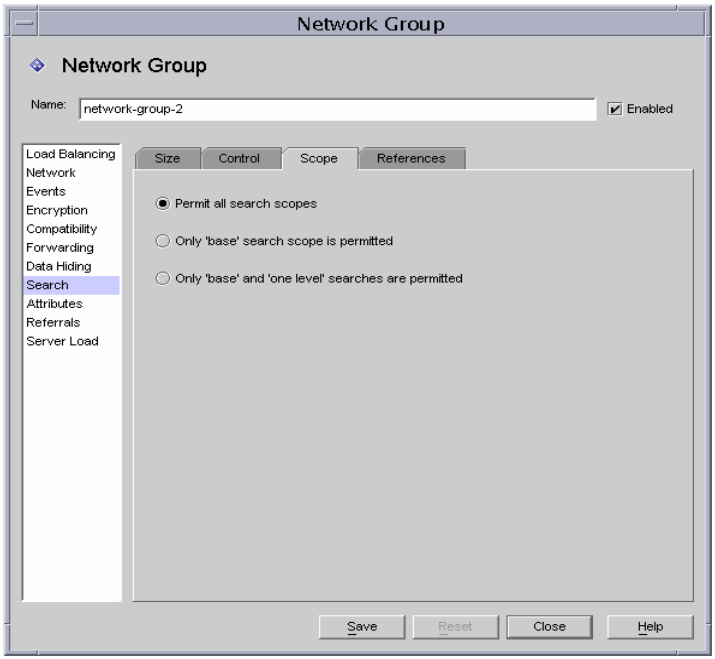
```
o=sun, st=California, c=US
```

st=California, c=US의 하위 트리 검색을 받으면 서버가 다음에 대한 하위 트리 검색을 수행하도록 검색이 다시 작성됩니다.

```
o=sun, st=California, c=US
```

찾아보기. 유효한 DN을 구성할 수 있는 대화 상자를 표시합니다.

17. 범위 탭을 선택하고 클라이언트가 검색 요청에서 지정할 수 있는 검색 범위를 지정합니다.



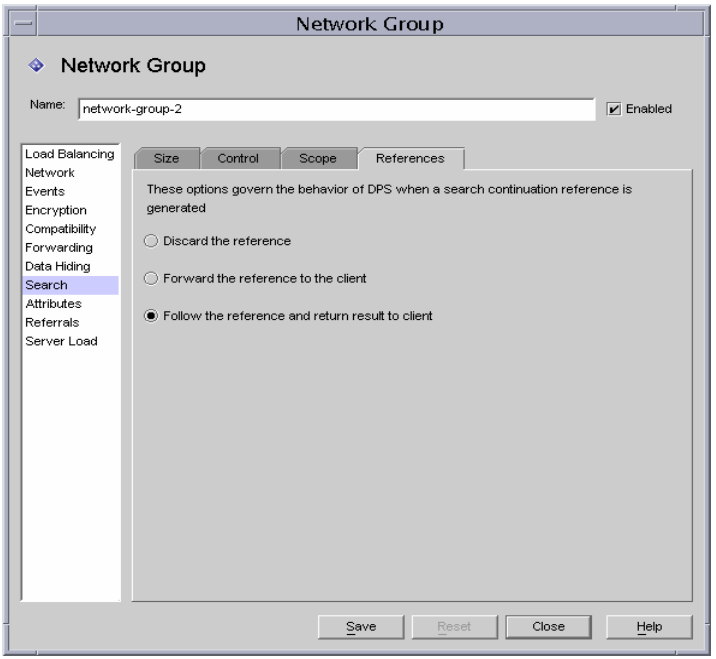
다음은 범위 탭의 요소에 대한 설명입니다.

모든 검색 범위 허용. 기본적으로 이 옵션은 활성화되어 있으므로 클라이언트의 모든 검색 범위를 허용합니다.

'기본' 검색 범위만 허용. 기본 검색 범위만 허용하려면 이 옵션을 설정합니다.

'기본'과 '한 수준' 검색만 허용. 기본 검색과 한 수준 검색만 허용하려면 이 옵션을 설정합니다.

18. 참고 탭을 선택하고 검색 도중 연속적인 검색 참고가 생성될 경우 수행할 작업을 지정합니다.



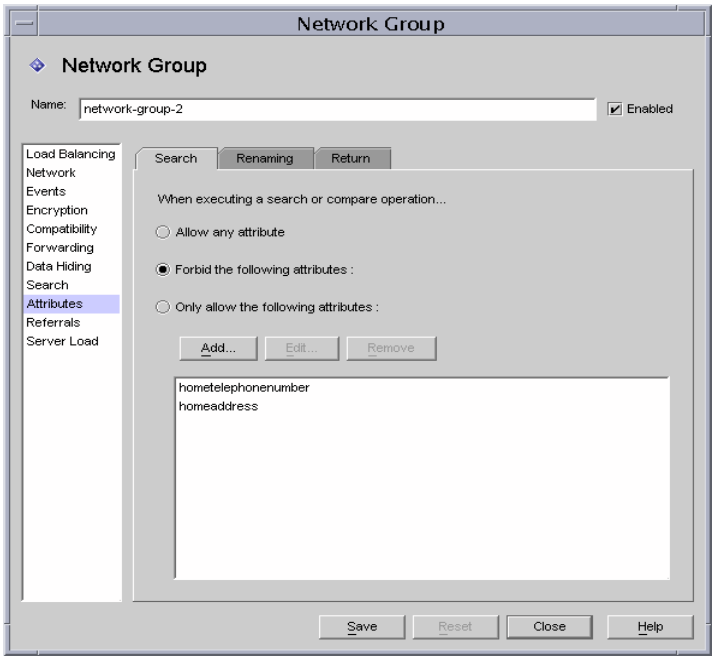
다음은 참고 탭의 요소에 대한 설명입니다.

참고 무시. 기본적으로 이 옵션은 활성화되어 있으므로 검색 도중 참고가 생성될 경우 해당 참고가 무시됩니다.

클라이언트에 참고 전달. 연속적인 검색 참고를 전달하려는 경우에만 이 옵션을 설정합니다.

참고를 따르고 클라이언트에 결과 반환. 연속적인 검색 참고 결과를 따르고 반환하려면 이 옵션을 설정합니다. 연속적인 검색 참고는 쿼리의 일부가 원래 디렉토리 서버에 의해 만족되었지만 그 디렉토리 서버는 쿼리를 만족시키는 더 많은 데이터를 가진 다른 디렉토리 서버에 대한 참고를 가진다는 점에서 특별한 경우의 참조입니다. 이 옵션을 사용하여 이름 지정 컨텍스트가 다른 LDAP 서버에서 제어되는 디렉토리 정보 트리의 일부를 숨길 수 있습니다. 또한 이 옵션은 클라이언트가 이 서버가 실행되는 네트워크 주소와 포트를 찾을 수 없게 합니다.

19. 그룹에 대한 속성 조건을 지정하려면 왼쪽 프레임에서 속성을 선택하고 오른쪽 프레임에서 해당 값을 지정합니다.



다음은 검색 탭의 요소에 대한 설명입니다.

이 탭은 특정 종류의 검색 및 비교 작업이 LDAP 서버에 도달하지 않도록 할 때 사용합니다. 클라이언트의 요청이 이 제한 사항에 해당하면 Directory Proxy Server는 클라이언트에 액세스 권한 부족 오류를 반환합니다.

모든 속성 허용. 기본적으로 이 옵션은 모든 속성이 검색 필터와 비교에 사용되도록 활성화되어 있습니다.

다음 속성 금지. 검색 필터나 비교 요청에 클라이언트가 사용할 수 없는 속성의 이름을 지정하려면 이 옵션을 활성화합니다.

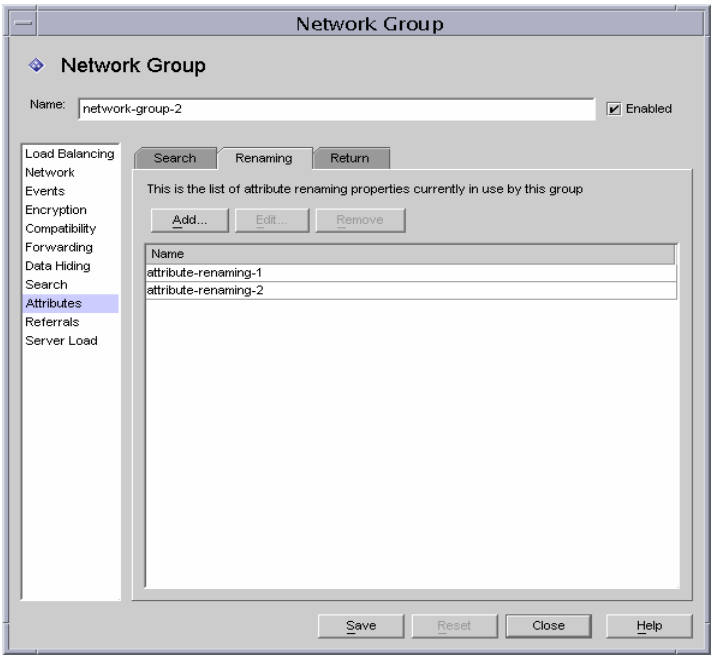
다음 속성만 허용. 검색 필터나 비교 요청에 사용할 수 있는 속성의 이름을 지정하려면 이 옵션을 활성화합니다. 하나 이상의 속성 값이 네트워크 그룹 테이블에 있고 비교가 이러한 속성 값 중 하나와 일치하지 않으면 Directory Proxy Server에서 요청을 거부합니다. 네트워크 그룹 테이블에 속성이 없고 한 속성이 임의 속성과 일치하지 않으면 클라이언트에서 그 속성을 사용할 수 있습니다. 예를 들어, cn, dn 및 mail 속성만 클라이언트에서 검색하도록 하려면 이러한 속성을 테이블에 추가합니다.

추가. 속성을 테이블에 추가할 수 있는 대화 상자를 표시합니다. 이러한 속성을 금지할 것인지 허용할 것인지 여부를 지정해야 합니다.

편집. 테이블에서 선택한 속성을 편집할 대화 상자를 표시합니다.

제거. 테이블에서 속성을 제거합니다.

20. 이름 바꾸기 탭을 선택하고 속성 이름 바꾸기 규칙을 지정합니다.



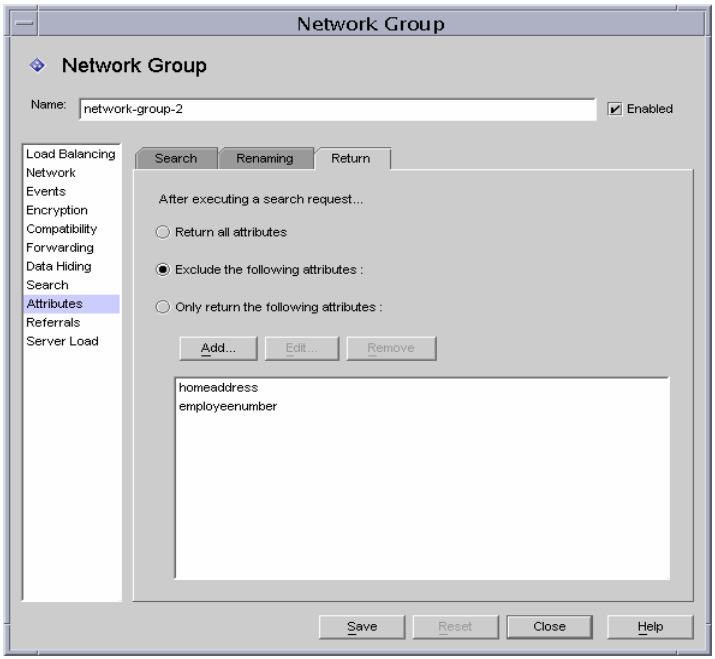
다음은 이름 바꾸기 탭의 요소에 대한 설명입니다.

추가. 이 네트워크 그룹에서 사용할 하나 이상의 기존 속성 이름 바꾸기 등록 정보를 아래 테이블에 추가하는 대화 상자를 표시합니다(108페이지의 “속성 이름 바꾸기 등록 정보”).

편집. 선택한 속성 이름 바꾸기 등록 정보를 편집할 대화 상자를 표시합니다.

제거. 테이블에서 속성 이름 바꾸기 등록 정보를 제거합니다.

21. 반환 탭을 선택하고 서버에서 반환되는 검색 결과를 클라이언트에 전달하기 전에 검색 결과에 적용할 제한 사항을 지정합니다.



다음은 반환 탭의 요소에 대한 설명입니다.

모든 속성 반환. 기본적으로 이 옵션은 활성화되어 있으며 모든 속성이 반환될 수 있도록 허용합니다.

다음 속성 제외. 검색 결과 항목에서 제외할 속성 이름을 지정하려면 이 옵션을 활성화합니다.

다음 속성만 반환. 검색 결과에서 반환될 수 있는 속성의 이름을 지정하려면 이 옵션을 활성화합니다.

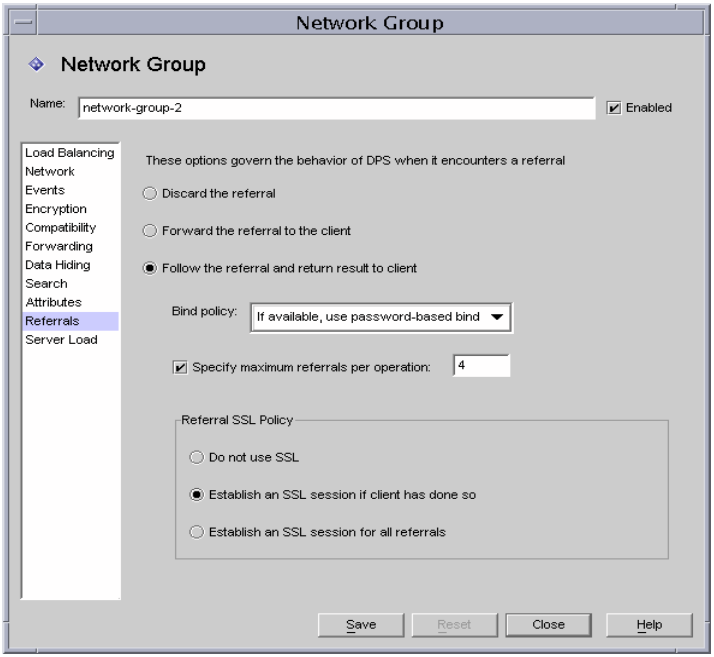
검색 결과의 일부로 반환된 속성이 "다음 속성만 반환" 테이블에 없는 경우 해당 속성은 반환되지 않습니다. 테이블이 비어 있고 속성이 "다음 속성 제외" 테이블에 없는 경우 해당 속성은 반환됩니다.

추가. 속성을 테이블에 추가할 수 있는 대화 상자를 표시합니다. 이러한 속성을 금지할 것인지 허용할 것인지 여부를 위에서 지정해야 합니다.

편집. 테이블에서 선택한 속성을 편집할 대화 상자를 표시합니다.

제거. 테이블에서 속성을 제거합니다.

22. 그룹에 대한 참조(예: 그룹이 서버에서 반환되는 참조를 전달하는지, 따르는지, 무시하는지 여부)를 지정하려면 왼쪽 프레임에서 참조를 선택하고 오른쪽 프레임에서 해당 값을 지정합니다.



다음은 화면에 표시되는 요소에 대한 설명입니다.

참조 무시. 네트워크 그룹이 서버에서 반환한 모든 참조를 무시하는 경우 이 옵션을 설정합니다.

클라이언트에 참조 전달. 기본적으로 이 옵션은 활성화되어 있으며 서버에서 반환한 참조를 전달합니다.

참조를 따르고 클라이언트에 결과 반환. 네트워크 그룹이 서버에서 반환한 참조를 전달하고 클라이언트에 결과를 반환하는 경우 이 옵션을 설정합니다.

바인드 정책. 이 옵션은 작업을 참조하고 참조를 따르는 경우 바인드 정책을 제어합니다.

Directory Proxy Server에서 SASL 메커니즘을 사용하여 바인드된 클라이언트에 대한 바인드를 재생할 수 없습니다. 그러므로 "필수"가 지정되고 클라이언트가 SASL 메커니즘을 사용하여 바인드하면 참조 작업이 거부됩니다.

항상. Directory Proxy Server가 이 네트워크 그룹에 연결된 클라이언트에 대한 참조를 따르면서 항상 익명으로 바인드해야 하는 경우 이 옵션을 선택합니다.

모두. 클라이언트가 비밀번호 기반 바인드를 사용한 경우 네트워크 그룹에서 단순 바인드를 사용하고 그 외에는 익명으로 바인드해야 하면 이 옵션을 선택합니다. 이것이 기본값입니다.

필수. 클라이언트가 비밀번호 기반 바인드를 사용하지 않는 경우 네트워크 그룹에서 참조된 작업을 거부해야 하면 이 옵션을 선택합니다.

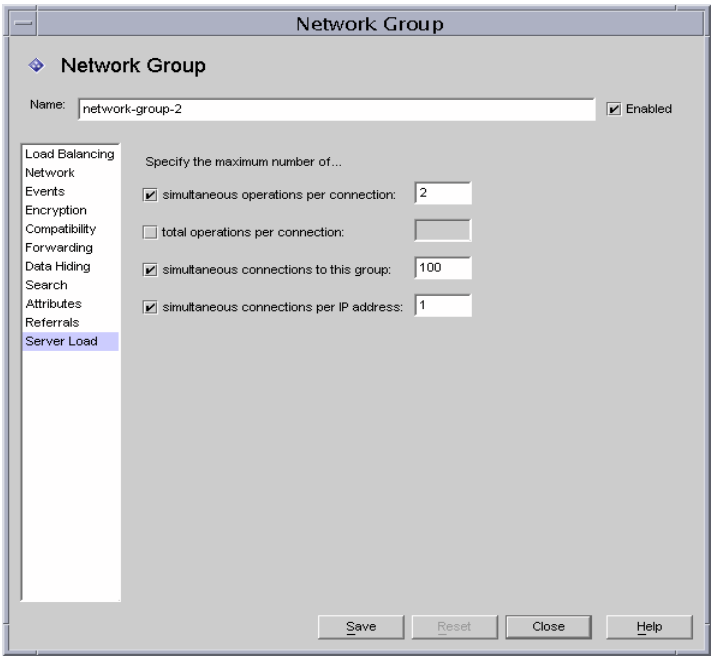
작업 당 최대 참조 수. 0보다 크거나 같은 정수 값을 입력합니다. 이것은 단일 작업에 대해 따라야 하는 최대 참고 수를 제한합니다. 기본값은 15입니다. 값이 0이면 제한이 적용되지 않습니다.

참조 SSL 정책. 참조 SSL 정책 패널을 활성화하려면 암호화 뷰에서 "SSL 사용 가능" 옵션을 설정해야 합니다.

클라이언트가 SSL 세션을 설정한 경우. 클라이언트가 이미 Directory Proxy Server와 SSL 세션을 설정한 상태에서 네트워크 그룹이 SSL을 시작할 경우에만 이 옵션을 설정합니다. 이것이 기본값입니다.

모든 참조에 대해. 참조 시 작업이 전달되기 전에 그룹이 SSL 세션을 시작할 경우 "모든 참조에 대해" 옵션을 설정합니다.

23. 그룹에 대한 서버 로드 조건을 지정하려면 왼쪽 프레임에서 서버 로드를 선택하고 오른쪽 프레임에서 해당 값을 지정합니다.



다음은 화면에 표시되는 요소에 대한 설명입니다.

연결 당 동시 작업 수. Directory Proxy Server가 해당 그룹에서 연결 당 처리할 수 있는 동시 작업 수를 제한하려면 이 옵션을 선택합니다. 값은 0보다 큰 정수입니다. 이 속성이 없으면 제한이 실행되지 않습니다. 예를 들어, 이 값을 1로 설정하면 해당 그룹의 모든 클라이언트는 동기 LDAP 작업을 수행하도록 지정됩니다. 작업 중단 요청을 제외한 추가 동시 요청은 Server Busy 오류로 실패합니다.

연결 당 총 작업 수. Directory Proxy Server가 한 그룹에서 연결 당 허용하는 총 작업 수를 제한하려면 이 옵션을 선택합니다. 값은 0보다 큰 정수입니다. 클라이언트가 한 연결에서 해당 그룹에 허용된 최대 작업 수를 초과하면 Directory Proxy Server에서 해당 연결을 닫습니다. 이 속성이 없으면 제한이 설정되지 않습니다.

이 그룹에 연결. 이 네트워크 그룹에 대한 동시 연결 수를 제한하려면 이 옵션을 선택하고 수를 지정합니다.

IP 주소 당 동시 연결 수. 클라이언트가 단일 IP 주소에서 만들 수 있는 동시 연결 수를 제한하려면 이 옵션을 선택합니다. 기본적으로 모든 연결 수가 허용됩니다.

24. 저장을 눌러 그룹을 만듭니다.

    Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 지금 서버를 다시 시작하지 말고, 모든 구성 변경을 완료한 후에 다시 시작하십시오.

25. 추가 그룹을 만들려면 단계 3에서 단계 24까지 반복합니다.

26. 네트워크 그룹 창(단계 2 참조)으로 이동하여 그룹의 우선 순위를 적절하게 지정합니다.

27. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

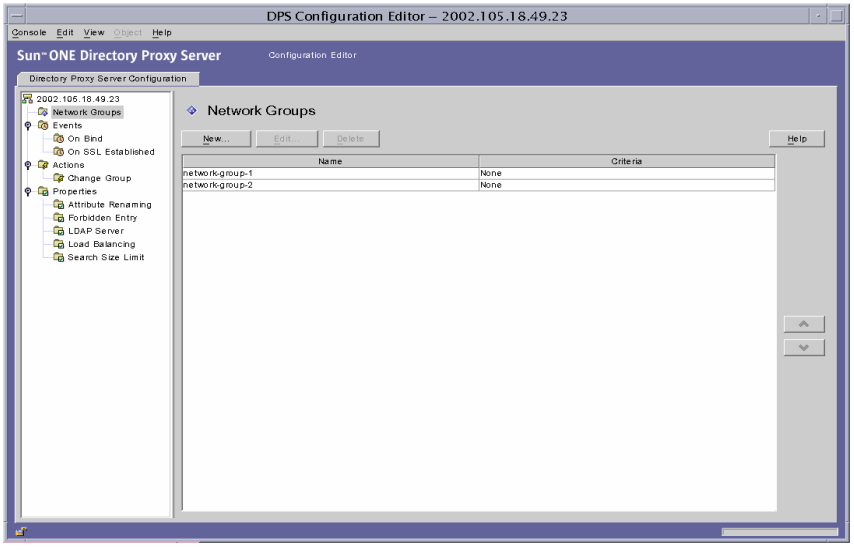
그룹 수정

그룹을 수정하려면 다음을 수행합니다.

1. Directory Proxy Server 구성 편집기 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.

2. 탐색 트리에서 네트워크 그룹을 선택합니다.

   오른쪽 창에 기존 그룹의 목록이 표시됩니다.



3. 목록에서 수정할 그룹을 선택하고 편집을 누릅니다.

4. 필요한 내용을 수정합니다.

5. 저장을 눌러 변경 내용을 저장합니다.

   Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 지금 서버를 다시 시작하지 말고, 모든 구성 변경을 완료한 후에 다시 시작하십시오.

6. 추가 그룹을 수정하려면 단계 3에서 단계 5까지 반복합니다.

7. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

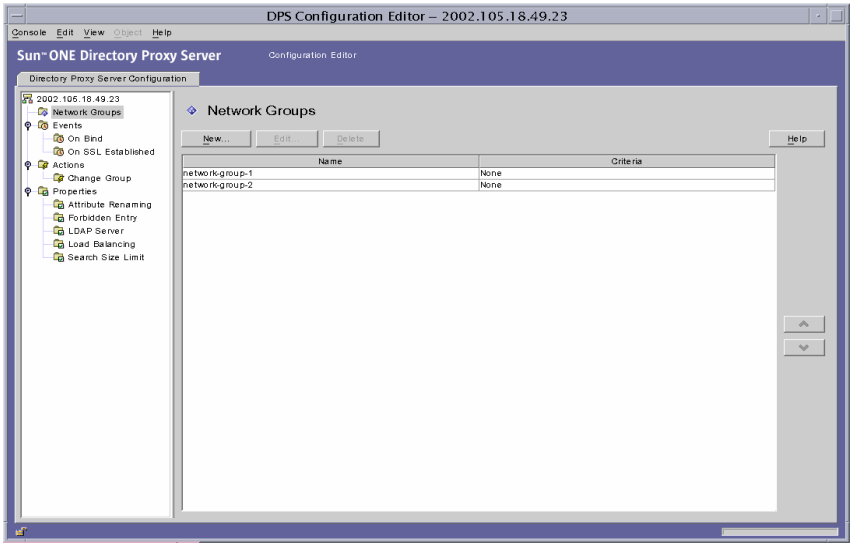
그룹 삭제

Directory Proxy Server 구성에서 원하지 않는 네트워크 그룹을 삭제할 수 있습니다. 그룹을 삭제하려면 다음을 수행합니다.

1. Directory Proxy Server 구성 편집기 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.

2. 탐색 트리에서 네트워크 그룹을 선택합니다.

   오른쪽 창에 기존 그룹의 목록이 표시됩니다.



3. 목록에서 삭제할 그룹을 선택하고 삭제를 누릅니다.

4. 작업을 확인합니다.

   삭제한 그룹의 이름이 목록에서 제거됩니다. Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 지금 서버를 다시 시작하지 말고, 모든 구성 변경을 완료한 후에 다시 시작하십시오.

5. 추가 그룹을 삭제하려면 단계 3과 단계 4를 반복합니다.

6. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

등록 정보 객체 정의 및 관리

이 설명서의 배포 장에 설명된 대로 Sun ONE Directory Proxy Server는 *LDAP 액세스 라우터* 역할을 할 수 있으므로 사용자의 공개 정보를 안전하게 게시할 수 있게 하면서 개인 디렉토리 정보를 인증되지 않은 액세스로부터 보호합니다. 서버는 수천 개의 LDAP 클라이언트 요청을 처리할 수 있으며 요청을 디렉토리 서버에 라우팅하기 전에 각 요청에 세부 액세스 제어 규칙 및 프로토콜 필터링 규칙을 적용할 수 있습니다.

Directory Proxy Server의 등록 정보 객체를 사용하여 LDAP 클라이언트가 따라야 하는 전문화된 제한 사항을 지정할 수 있습니다. 그런 다음 제한을 적용해야 하는 다른 항목에 이러한 등록 정보를 포함시킬 수 있습니다. 이 장에서는 각 등록 정보에 대한 개요를 제공하고 Directory Proxy Server 구성 편집기 콘솔을 사용하여 등록 정보 객체를 만드는 방법을 설명합니다.

이 장은 다음 내용으로 구성되어 있습니다.

속성 이름 바꾸기 등록 정보

일반적으로 LDAP 디렉토리에는 조직 내의 사람 및 네트워크 자원 등과 같은 항목에 대한 정보가 포함되어 있습니다. 디렉토리에는 각 엔티티에 대한 항목이 있습니다. 디렉토리의 각 항목은 고유 이름(DN)으로 식별되고 속성 및 해당 값 집합으로 표시됩니다. 각 항목에는 해당 항목이 설명하는 객체 종류를 설명하고 항목에 포함된 추가 속성 집합을 정의하는 객체 클래스 속성이 있습니다. 각 속성은 항목의 특성을 설명합니다. 예를 들어, 항목은 해당 항목이 특정 조직 내의 사람임을 나타내는 `organizationalPerson` 객체 클래스일 수 있습니다. 이 객체 클래스는 `givenname` 및 `telephoneNumber` 속성을 허용합니다. 이 속성에 할당된 값은 항목이 나타내는 사람의 이름과 전화 번호를 제공합니다.

대부분의 디렉토리 배포에 있어 LDAP 클라이언트쪽에 정의된 속성은 서버쪽에 정의된 속성에 매핑되지 않습니다. 그런 설정에서 클라이언트와 서버 간의 통신을 용이하게 하기 위해 Directory Proxy Server는 속성 이름 바꾸기를 지원합니다. 즉, Directory Proxy Server는 클라이언트 쿼리에서 속성 이름을 디렉토리 서버에서 인식할 수 있는 형식으로 바꾼 다음 쿼리를 디렉토리 서버에 전달할 수 있으며, 서버 응답에서도 동일한 과정을 수행하여 응답을 클라이언트에게 전달할 수 있습니다.

그림 7-1에서는 Directory Proxy Server의 속성 이름 바꾸기 기능을 스키마 매핑에 사용하는 방법을 설명합니다.

그림 7-1 속성 이름 바꾸기 등록 정보를 사용하여 스키마 매핑

전자 메일 클라이언트는 사용자의 성을 "surname" 속성의 값이라고 예상하지만 LDAP 서버에서는 성이 "sn" 속성에 지정됩니다. Directory Proxy Server가 이 두 속성을 매핑할 경우 속성 이름만 영향을 받으며, 속성 값은 변경되지 않고 그대로 유지됩니다.

속성 이름 바꾸기 등록 정보를 사용하여 클라이언트 및 서버 속성 이름 바꾸기를 제어하는 규칙을 정의할 수 있습니다. 해당 서버 속성에 매핑해야 할 클라이언트 속성 이름을 지정할 수도 있고, 클라이언트 속성 이름을 지정한 다음 해당 서버 속성에 매핑할 수도 있습니다. 이 방식은 서버에서 알 수 없는 속성 이름이 클라이언트 요청에 포함되어 있는 경우 Directory Proxy Server는 해당 속성을 서버에 알려진 이름으로 매핑하여 클라이언트와 서버 간의 통신을 도울 수 있습니다. 마찬가지로 서버가 응답할 때 Directory Proxy Server는 클라이언트에서 알 수 없는 속성을 알려진 형식으로 해석합니다.

다음 절에서는 Directory Proxy Server 구성 편집기 콘솔에서 속성 이름 바꾸기 등록 정보에 대한 객체를 만드는 방법을 설명합니다.

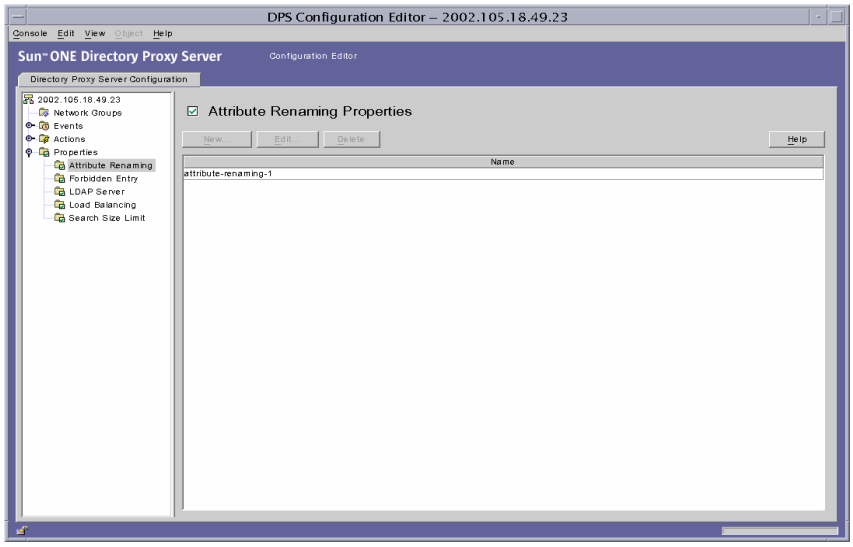
주 속성 이름 바꾸기 등록 정보에 대해 만든 객체는 서버 속성과 클라이언트 속성을 모두 가지고 있어야 합니다. 그렇지 않으면 Directory Proxy Server가 시작되지 않습니다.

속성 이름 바꾸기 등록 정보 객체 만들기

Directory Proxy Server에서 이름을 바꾸어야 하는 클라이언트 및 서버 속성을 식별하려면 다음을 수행합니다.

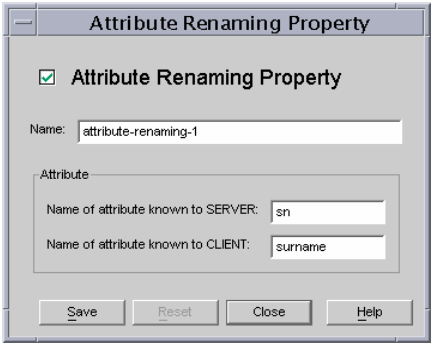
1. Directory Proxy Server 구성 편집기 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.
2. 탐색 트리에서 등록 정보 노드를 확장한 다음 속성 이름 바꾸기를 선택합니다.

   오른쪽 창에 속성 이름 바꾸기 등록 정보에 대한 기존 객체 목록이 표시됩니다.



3. 새로 만들기를 누릅니다.

속성 이름 바꾸기 등록 정보 창이 나타납니다.



4. 이름 필드에 등록 정보 객체 이름을 입력합니다. 이 이름은 고유한 영숫자 문자열이어야 합니다.

주 속성 이름에는 7비트 문자만 사용할 수 있습니다.

5. 이름 바꾸기 필드에서 매핑할 속성을 식별합니다.

   속성 이름 바꾸기 값은 `2.5.4.10`처럼 구성 요소가 점으로 구분된 십진수로 작성할 수 있습니다. 속성 이름 바꾸기 값은 속성 유형에 대해 하나 이상의 텍스트 이름을 지정할 수도 있습니다. 이러한 이름은 문자로 시작해야 하며 ASCII 문자, 아라비아 숫자 및 하이픈만 사용할 수 있습니다. 이 값은 대소문자를 구분하지 않습니다.

   서버에 알려진 속성 이름. 서버에 알려진 속성 이름을 지정하려면 값을 입력합니다.

   클라이언트에 알려진 속성 이름. 클라이언트에 알려진 속성 이름을 지정하려면 값을 입력합니다.

   클라이언트 요청에 "클라이언트에 알려진 속성 이름"에 지정된 속성 이름이 있으면 그 이름은 "서버에 알려진 속성 이름"의 값으로 변환됩니다. 마찬가지로, 서버가 보낸 결과에 "서버에 알려진 속성 이름"에 지정된 속성 이름이 있으면 그 이름은 "클라이언트에 알려진 속성 이름" 값으로 변환됩니다.

6. 저장을 눌러 객체를 만듭니다.

   Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 아직은 서버를 다시 시작하지 말고, 모든 구성 변경을 완료한 후에 다시 시작하십시오.

7. 추가 객체를 만들려면 단계 3에서 단계 6까지를 반복합니다.

8. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

금지 항목 등록 정보

여러 가지 이유로 LDAP 디렉토리의 특정 항목 또는 해당 항목을 나타내는 속성을 LDAP 클라이언트가 보지 못하도록 숨겨야 할 수 있습니다. 예를 들어, 디렉토리에 모든 직원에 대한 항목이 있고 각 항목에 이름, 부서, 사무소 위치, 사무실 전화 번호, 집 전화 번호 등과 같은 직원 데이터 관련 속성이 포함되어 있는 경우 모든 직원의 집 전화 번호를 클라이언트가 보지 못하도록 숨길 수 있습니다.

금지 항목이란 LDAP 클라이언트에게 숨겨야 하는 LDAP 디렉토리의 항목을 말합니다. 그런 설정에서 클라이언트와 디렉토리 서버 간의 통신을 용이하게 하기 위해 Directory Proxy Server는 금지 항목을 지원합니다. 즉, Directory Proxy Server는 LDAP 항목과 해당 항목의 속성을 LDAP 클라이언트가 보지 못하도록 숨길 수 있습니다.

금지 항목 등록 정보를 사용하여 디렉토리 항목과 해당 속성의 숨기기를 제어하는 규칙을 정의합니다. 이 등록 정보를 사용하여 숨겨야 하는 항목 목록 또는 항목 속성을 여러 가지 방법으로 지정할 수 있습니다. 예를 들어, 다음을 지정할 수 있습니다.

- 숨길 항목의 항목 또는 속성 DN
- 숨길 항목의 항목 또는 속성 DN에 대한 정규 표현식(예: `.*OU=INTERNAL.*`)
- 항목의 속성 이름/값 쌍(예: `secret:yes`). 항목에 지정된 속성 이름/값 쌍과 일치하는 속성 이름/값 쌍이 있으면 해당 항목이나 해당 내용의 일부가 숨겨집니다.

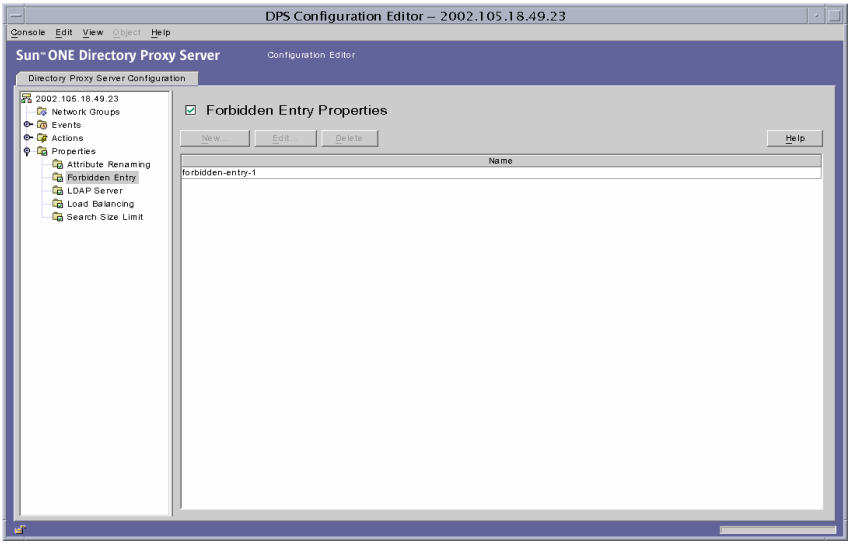
다음 절에서는 Directory Proxy Server 구성 편집기 콘솔에서 금지 항목 등록 정보에 대한 객체를 만드는 방법을 설명합니다.

금지 항목 등록 정보 객체 만들기

Directory Proxy Server가 클라이언트로부터 숨겨야 하는 항목 또는 항목 속성을 식별하려면 다음을 수행합니다.

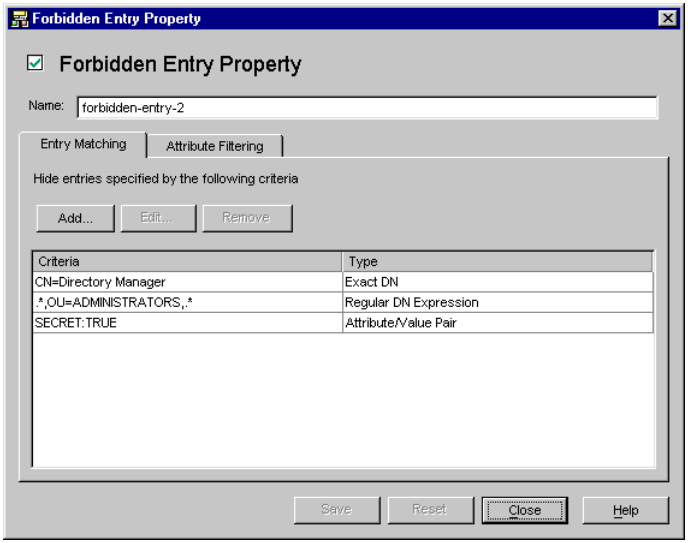
1. Directory Proxy Server 구성 편집기 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.
2. 탐색 트리에서 등록 정보 노드를 확장한 다음 금지 항목을 선택합니다.

   오른쪽 창에 금지 항목 등록 정보에 대한 기존 객체 목록이 표시됩니다.



3. 새로 만들기를 누릅니다.

   금지 항목 등록 정보 창이 나타납니다.



4. 이름 필드에 등록 정보 객체 이름을 입력합니다. 이 이름은 고유한 영숫자 문자열이어야 합니다.

5. 항목 일치 탭에서 해당 값을 지정하여 탭에 이 등록 정보의 이름과 숨길 LDAP 항목에 대한 설정을 표시합니다.

추가. LDAP 항목을 숨길 조건을 추가할 수 있는 메뉴를 표시합니다. 조건은 정확한 DN, 정규 DN 표현식 또는 속성/값 쌍 형식일 수 있습니다. 항목을 입력하거나 디렉토리 정보 트리에서 기존 항목을 찾을 수 있습니다.

정확한 DN. 숨길 항목의 DN을 입력할 대화 상자를 표시합니다.

정규 DN 표현식. 숨길 항목의 정규 DN 표현식을 입력할 대화 상자를 표시합니다. DN의 정규 표현식을 일반적인 형식으로 지정해야 합니다. 즉, RDN 구성 요소와 "=" 기호 사이에 공백이 없고 속성 이름과 값을 모두 대문자로 입력해야 합니다.

예를 들어, DN을 "ou=internal"의 RDN 구성 요소와 일치시키려면 다음과 같이 지정해야 합니다.

.*OU=INTERNAL.*

속성 필터링 탭에 포함할 속성 이름이 있고 속성이 나열된 이름 중 하나와 일치하지 않으면 속성이 반환되지 않습니다. LDAP 항목에 속성 필터링 탭에서 제외할 속성과 일치하는 속성이 없으면 LDAP 항목이 반환됩니다.

정규 표현식에 대한 자세한 내용은 *Mastering Regular Expressions*(저자: Friedl 및 Oram, 발행: O'Reilly, ISBN: 1565922573)를 참조하십시오.

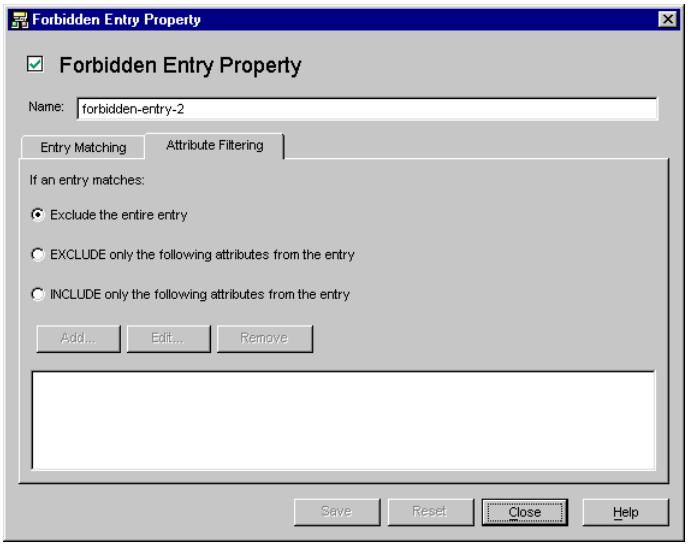
속성/값 쌍. 속성 이름/값 쌍을 지정할 때 사용할 대화 상자를 표시합니다. 항목에 지정된 속성 이름/값 쌍과 일치하는 속성 이름/값 쌍이 있으면 해당 항목이나 해당 내용의 일부가 숨겨집니다.

예를 들어, "ou=internal" 또는 "secret=yes"를 속성으로 갖는 모든 항목을 제한하려면 "ou"의 속성 및 "internal."의 값을 가지도록 지정할 수 있습니다.

편집. 테이블에서 현재 선택한 항목을 편집할 대화 상자를 표시합니다.

제거. 테이블에서 현재 선택한 항목을 제거합니다.

6. 속성 필터링 탭을 선택하고 해당 값을 지정합니다.



이 탭에는 특정 속성을 제외하거나 특별히 포함할 수 있도록 하는 설정이 있습니다.

전체 항목 제외. 속성 필터링을 수행하지 않고 전체 항목이 숨겨지도록 하려면 이 옵션을 선택합니다.

항목에서 다음 속성만 제외. 테이블에 위 사양과 일치하는 항목에서 제외할 속성 이름 목록이 있음을 나타내려면 이 옵션을 선택합니다.

항목에서 다음 속성만 포함. 테이블에 위 사양과 일치하는 항목의 일부로 반환될 수 있는 속성 이름 목록이 있음을 나타내려면 이 옵션을 선택합니다.

7. 저장을 눌러 객체를 만듭니다.

   Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 아직은 서버를 다시 시작하지 말고, 모든 구성 변경을 완료한 후에 다시 시작하십시오.

8. 추가 객체를 만들려면 단계 3에서 단계 7까지를 반복합니다.

9. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

LDAP 서버 등록 정보

디렉토리 배포에서 Directory Proxy Server는 LDAP 클라이언트와 LDAP 디렉토리 서버 사이에 있으며, LDAP 클라이언트의 요청을 필터링한 후 LDAP 디렉토리 서버에 라우팅하고, 디렉토리 서버의 응답을 필터링하여 클라이언트에게 전달합니다. 또한, Directory Proxy Server는 복제된 디렉토리 서버 간의 자동 로드 균형 조정 및 자동 페일오버/페일백을 지원합니다.

LDAP 서버 등록 정보를 사용하여 Directory Proxy Server에서 백엔드 서버로 사용해야 하는 디렉토리 서버를 식별합니다. 이 등록 정보를 지정할 때 Directory Proxy Server에서 디렉토리 서버와 통신하는 데 필요한 모든 정보(예: 디렉토리 서버의 IP 주소 또는 정규화된 이름, 디렉토리 서버가 클라이언트 연결을 수신할 포트 번호, 서버에서 지원되는 LDAP 버전, Directory Proxy Server와 이 서버 간의 통신에 사용할 버전 등)를 지정합니다.

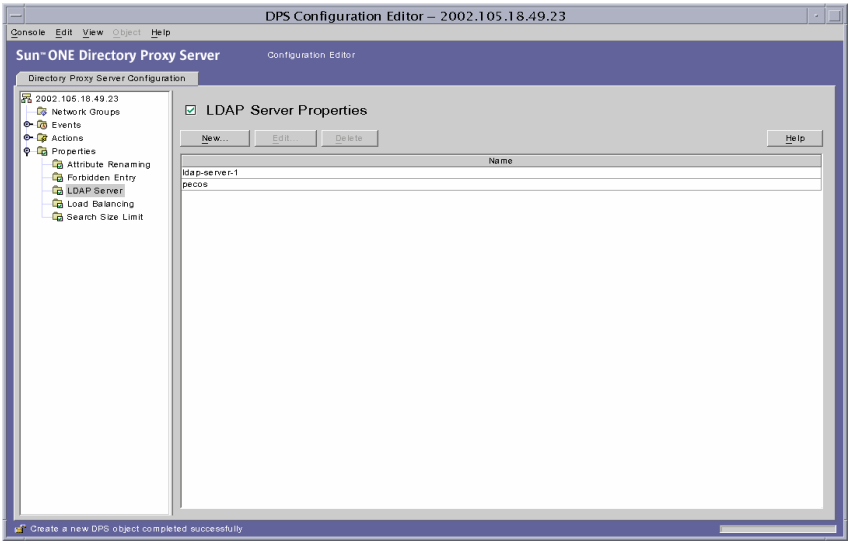
다음 절에서는 Directory Proxy Server 구성 편집기 콘솔에서 LDAP 서버 등록 정보에 대한 객체를 만드는 방법을 설명합니다.

LDAP 서버 등록 정보 객체 만들기

Directory Proxy Server가 통신해야 하는 디렉토리 서버를 식별하려면 다음을 수행합니다.

1. Directory Proxy Server 구성 편집기 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.
2. 탐색 트리에서 등록 정보 노드를 확장한 다음 LDAP 서버를 선택합니다.

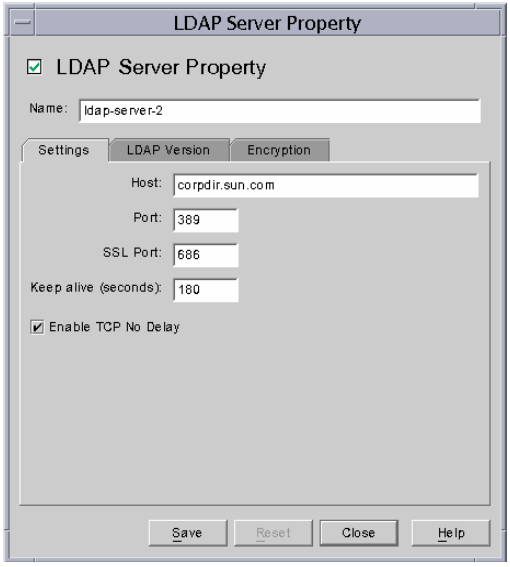
   오른쪽 창에 LDAP 서버 등록 정보에 대한 기존 객체 목록이 표시됩니다.



3. 새로 만들기를 누릅니다.

   LDAP 서버 등록 정보 창이 나타납니다.

4. 이름 필드에 등록 정보 객체 이름을 입력합니다. 이 이름은 고유한 영숫자 문자열이어야 합니다.



5. 설정 탭에서 이 등록 정보가 참조하는 LDAP 서버의 기본 설정을 지정합니다.

   호스트. 백엔드 LDAP 서버가 실행 중인 호스트의 전체 도메인 이름 또는 IP 주소를 지정하는 값을 입력합니다. 이 속성은 필수입니다.

   포트. 백엔드 LDAP 서버가 실행 중인 포트를 지정하는 번호를 입력합니다. 이 속성이 없을 경우 사용되는 기본 포트는 389입니다.

   SSL 포트. 백엔드 LDAP 서버에서 LDAPS (SSL에서의 LDAP) 연결을 수신하는 포트를 지정하는 번호를 입력합니다. 백엔드 LDAP 서버가 LDAPS를 지원하지 않을 경우 이 속성 값을 설정하지 마십시오.

   연결 유지 간격. LDAP 디렉토리 서버에 대한 네트워크 연결이 끊어졌는지 여부나 LDAP 디렉토리 서버가 응답하지 않는지 여부를 확인하기 위해 Directory Proxy Server에서 응답하지 않는 서버를 포크한 이후의 시간(초)을 입력합니다. Directory Proxy Server에 연결한 클라이언트에 보류 중인 작업이 있고 Directory Proxy Server가 여기에 지정된 시간(초) 동안 연결된 LDAP 서버로부터 데이터를 받지 못할 경우 Directory Proxy Server는 다른 통신 채널을 입력하여 LDAP 서버의 가용성을 테스트합니다. Directory Proxy Server에서 작업이 성공적으로 완료되면 사용 가능한 다른 LDAP 서버에 페일오버됩니다. 이 속성의 기본값은 180초입니다. LDAP 서버가 Directory Proxy Server와 같은 로컬 네트워크에 있지 않으면 이 값을 늘리는 것이 좋습니다.

   TCP 지연 없음 사용. Directory Proxy Server에서 이 서버에 연결 시 Nagel 알고리즘을 사용하도록 하려면 이 옵션을 비활성화합니다. Directory Proxy Server와 이 객체 항목에 정의된 서버 간의 네트워크 대역폭이 크게 제한된 경우에만 이 옵션을 비활성화해야 합니다. 기본적으로 이 설정은 활성화되어 있습니다.

6. LDAP 버전 탭을 선택하고 해당 값을 지정합니다.

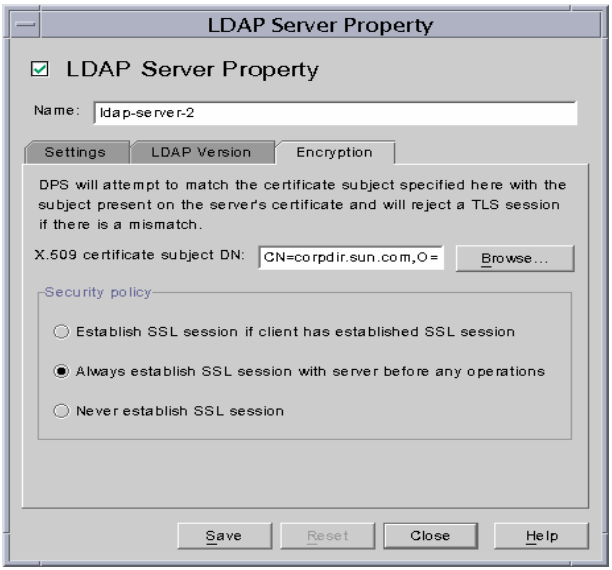
이 탭에는 이 서버에서 지원하는 LDAP 버전 및 Directory Proxy Server와 이 서버 간의 통신에 사용해야 하는 버전을 나타내는 설정이 표시됩니다.

지원되는 LDAP 버전. LDAP 버전 2 및 3 또는 LDAP 버전 2 전용 옵션 중 하나를 선택합니다. 기본값은 LDAP 버전 2 및 3입니다.

사용할 LDAP 버전. 클라이언트가 사용하는 모든 버전, "LDAP 버전 3 전용", "LDAP 버전 2 전용" 중 하나의 옵션을 선택합니다. 이 속성은 이 항목이 정의한 백엔드 서버와 통신할 때 사용할 기본 설정 LDAP 프로토콜 버전을 Directory Proxy Server에 알립니다. 기본적으로 "클라이언트가 사용하는 모든 버전"이 선택됩니다.

이 옵션은 Directory Proxy Server가 참조를 따라야 하는 LDAPv2 클라이언트가 있을 경우 유용합니다. 이 경우 Directory Proxy Server 자체에서 LDAPv3 클라이언트로 백엔드 서버에 연결해야 백엔드 서버에서 참조를 다시 이 서버로 보낼 수 있습니다. LDAP 버전 3 전용 옵션은 이 등록 정보를 참조하는 네트워크 그룹이 여러 LDAP 버전 2 바인드를 허용할 경우 선택해야 합니다.

7. 암호화 탭을 선택하고 해당 값을 지정합니다.



이 탭에는 이 등록 정보에서 참조한 LDAP 서버의 통신 보호와 관련된 설정이 표시됩니다.

X.509 인증서 주체 DN. LDAP 서버의 인증서 주체 이름을 지정합니다. 인증서 주체를 지정하면 Directory Proxy Server는 인증서 주체를 LDAP 서버의 인증서에 있는 주체와 일치시키고 일치하지 않으면 TLS 세션을 거부합니다. Directory Proxy Server에서는 이 속성을 사용하여 연결할 LDAP 서버를 인증할 수 있습니다. Directory Proxy Server에서는 이 속성이 설정되어 있지 않은 경우 모든 이름을 허용합니다.

보안 정책. Directory Proxy Server와 백엔드 서버 간에 연결할 보안 정책을 정의하는 "클라이언트가 SSL 세션을 설정한 경우 SSL 세션 설정", "작업 전에 항상 서버와 SSL 세션 설정" 또는 "SSL 세션 설정 안 함" 옵션 중 하나를 선택합니다.

8. 저장을 눌러 객체를 만듭니다.

   Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 아직은 서버를 다시 시작하지 말고, 모든 구성 변경을 완료한 후에 다시 시작하십시오.

9. 추가 객체를 만들려면 단계 3에서 단계 8까지를 반복합니다.

10. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

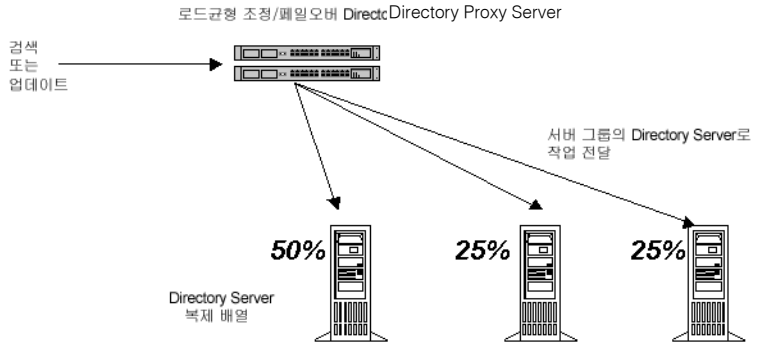
로드 균형 조정 등록 정보

Directory Proxy Server에서는 복제된 LDAP 디렉토리 서버 간의 자동 로드 균형 조정 및 자동 페일오버/페일백을 모두 제공하여 디렉토리 배포 가용성을 높입니다. Directory Proxy Server에서 가용성을 높이려면 Directory Proxy Server가 작업할 디렉토리 서버를 식별하고 클라이언트 로드를 해당 서버 간에 분산하는 방법을 지정해야 합니다.

Directory Proxy Server에서 로드 균형 조정 등록 정보를 사용하여 로드 균형 조정하도록 구성합니다. 이 등록 정보를 사용하면 Directory Proxy Server가 통신할 백엔드 디렉토리 서버를 식별하고 각 디렉토리 서버가 받을 총 클라이언트 로드의 비율을 지정할 수 있습니다. 구성한 경우 Directory Proxy Server는 구성에 정의된 로드 조건에 따라 클라이언트 요청을 다른 디렉토리 서버로 자동으로 분산시킵니다. 디렉토리 서버를 사용할 수 없는 경우 Directory Proxy Server는 해당 서버에 로드될 부분을 해당 로드 비율을 기준으로 사용 가능한 다른 서버에 나누어 배포합니다. Directory Proxy Server는 모든 백엔드 LDAP 서버를 사용할 수 없는 경우 클라이언트 쿼리를 거부합니다.

그림 7-2에서는 세 디렉토리 서버 복제에 분산된 클라이언트 로드를 표시합니다.

그림 7-2 LDAP 디렉토리 복제 간 로드 균형 조정



Directory Proxy Server의 로드 균형 조정은 세션을 기반으로 합니다. 즉, 클라이언트의 쿼리를 전달할 특정 디렉토리 서버를 선택하는 결정 함수가 클라이언트 세션이 시작될 때 클라이언트 세션 당 한 번씩 적용됩니다. 해당 세션의 모든 후속 클라이언트 쿼리는 세션을 시작할 때 선택한 디렉토리 서버에 전달됩니다.

Directory Proxy Server에서 로드 균형 조정할 수 있는 백엔드 디렉토리 서버 수는 여러 가지 요소에 따라 달라집니다. 이러한 요소는 다음과 같습니다.

- Directory Proxy Server를 실행하는 호스트의 크기
- 사용 가능한 네트워크 대역폭
- Directory Proxy Server에서 받는 쿼리 혼합
- 클라이언트 세션의 길이
- Directory Proxy Server 구성

일반적으로 Directory Proxy Server는 대부분의 세션이 잠깐 동안 실행되고 쿼리가 계산에 집중될 경우 더 적은 수의 디렉토리 서버를 지원할 수 있습니다. 계산 중심 쿼리는 속성 이름 바꾸기(108페이지의 "속성 이름 바꾸기 등록 정보" 참조) 기능을 사용할 때처럼 전체 메시지를 검사해야 하는 쿼리입니다.

Directory Proxy Server는 연결 거부 오류가 발생하거나 연결 시간 초과가 발생할 경우 디렉토리 서버가 사용 불가능하게 되는 때를 검색합니다. 이러한 경우는 모두 세션의 초기 단계에서 발생하여 해당 세션에 대한 어떠한 작업도 처리되지 않기 때문에 Directory Proxy Server는 투명하게 사용할 수 있는 다른 서버에 페일오버합니다. 연결 시도 시간 초과가 발생할 경우 클라이언트가 응답을 받는 데 많은 시간이 지연될 수 있습니다. Directory Proxy Server와 백엔드 서버 간의 연결이 갑자기 끊어질 경우 Directory Proxy Server는 해당 클라이언트에 해결되지 않은 모든 작업에 대한 `LDAP_BUSY` 오류를 반환합니다. 그런 다음 Directory Proxy Server는 해당 클라이언트 세션을 다른 디렉토리 서버에 페일오버합니다.

Directory Proxy Server가 디렉토리 배포에 대한 단일 오류 지점이 되지 않게 하려면 IP 장치가 앞에 있는 두 대 이상의 Directory Proxy Server를 사용하는 것이 좋습니다. 이 내용은 2장, "Sun ONE Directory Proxy Server 배포 시나리오"에 설명되어 있습니다. 이런 방법으로 Directory Proxy Server를 배포할 수 없는 경우 -M 스위치를 사용하는 것이 좋습니다. 이 스위치는 Directory Proxy Server가 자체적으로 모니터할 수 있게 해줍니다.

Directory Proxy Server는 모니터 프로세스를 사용하여 백엔드 서버의 상태를 검사합니다. 로드 균형 조정을 사용할 경우 이 기능이 자동으로 활성화됩니다. Directory Proxy Server는 각 백엔드 디렉토리 서버에 대해 익명 Root DSE 검색 작업을 10초마다 수행합니다. 백엔드 디렉토리 서버 중 하나가 사용할 수 없게 되거나 응답하지 않는 경우 Directory Proxy Server는 활성 로드 균형 서버 집합에서 해당 서버를 제거합니다. 그런 다음 서버가 다시 사용할 수 있게 되면 해당 집합에 다시 넣습니다. 모니터 기능을 효과적으로 사용하려면 *Directory Proxy Server 설치 설명서*의 2장 "컴퓨터 시스템 요구 사항"에 설명된 `idsktune</code>` 유틸리티 권장 사항에 따라 Directory Proxy Server를 실행할 호스트를 구성해야 합니다. 한 서버에서만 보안 포트를 사용하는 경우 Directory Proxy Server는 상태 검사를 보안된 방법으로 수행하려고 시도합니다.

다음 절에서는 Directory Proxy Server 구성 편집기 콘솔에서 로드 균형 조정 등록 정보에 대한 객체를 만드는 방법을 설명합니다.

주 로드 균형 조정 등록 정보에 대해 만든 객체에는 LDAP 서버 등록 정보가 하나 이상 있어야 하며 비율을 최대 100%까지 추가해야 합니다. 그렇지 않으면 Directory Proxy Server가 시작되지 않습니다.

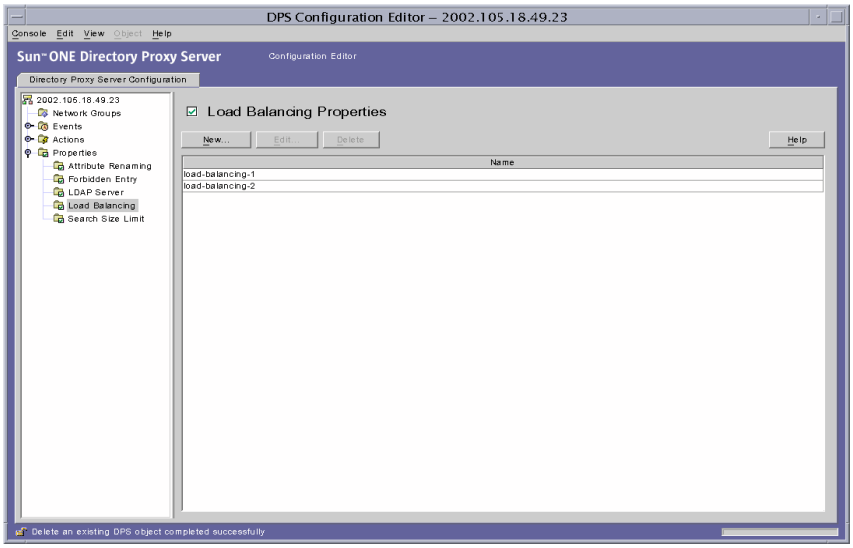
로드 균형 조정 등록 정보 객체 만들기

이 절에서는 로드 균형 조정을 위해 Directory Proxy Server를 구성하는 방법을 설명합니다. 로드 균형 조정 등록 정보에 대한 객체를 만들기 전에 Directory Proxy Server에서 클라이언트 로드 균형 조정에 사용할 LDAP 디렉토리 서버를 식별해야 합니다. 자세한 내용은 116페이지의 “LDAP 서버 등록 정보”를 참조하십시오.

Directory Proxy Server가 디렉토리 서버 집합 간에 로드 균형을 조정하는 방법을 정의하려면 다음을 수행합니다.

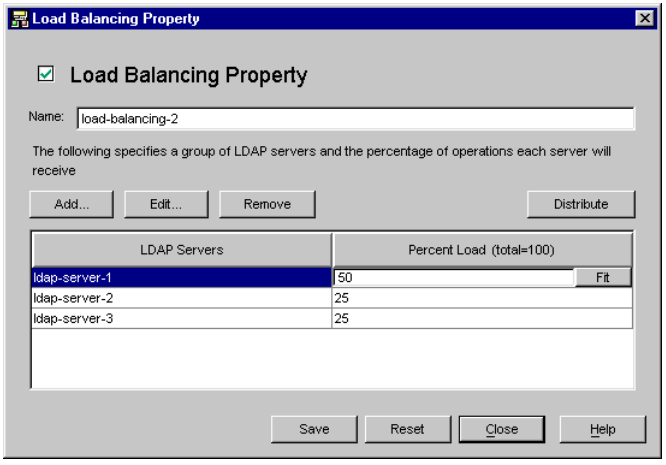
1. Directory Proxy Server 구성 편집기 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.
2. 탐색 트리에서 등록 정보 노드를 확장한 다음 로드 균형 조정을 선택합니다.

   오른쪽 창에 로드 균형 조정 등록 정보에 대한 기존 객체 목록이 표시됩니다.



3. 새로 만들기를 누릅니다.

   로드 균형 조정 등록 정보 창이 나타납니다.



4. 이름 필드에 등록 정보 객체 이름을 입력합니다. 이 이름은 고유한 영숫자 문자열이어야 합니다.

5. 나머지 양식 요소를 사용하여 원하는 결과를 얻습니다.

비율을 편집하려면 LDAP 서버가 포함된 행 옆의 로드 비율 열을 누르고, 0에서 100 사이의 숫자를 입력한 다음, 맞춤 버튼을 누릅니다. 이 작업은 현재 행에 비율을 할당하고 모든 비율의 합계를 100으로 만들려고 시도합니다. 현재 비율의 합계가 로드 비율 열 머리글에 표시됩니다.

추가. LDAP 서버 등록 정보에 참조를 추가할 대화 상자를 표시합니다. 기본적으로 추가된 첫 번째 서버에 다음 추가 설정이 0%인 로드의 100%가 지정됩니다.

편집. 테이블에서 현재 선택한 항목을 편집할 대화 상자를 표시합니다.

제거. 로드 균형 조정을 수행할 서버 목록에서 현재 선택한 LDAP 서버를 제거합니다.

배포. 이 테이블에서 현재 참조한 모든 LDAP 서버로 로드 비율을 균등하게 배포합니다.

6. 저장을 눌러 객체를 만듭니다.

   Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 아직은 서버를 다시 시작하지 말고, 모든 구성 변경을 완료한 후에 다시 시작하십시오.

7. 추가 객체를 만들려면 단계 3에서 단계 6까지를 반복합니다.

8. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

검색 크기 제한 등록 정보

LDAP 디렉토리는 조직에서 배포된 LDAP 클라이언트가 정보를 조사할 수 있는 조직의 중앙 저장소 역할을 합니다. LDAP 클라이언트는 일반적으로 검색 필터로 특정 정보를 검색하여 정보를 조사합니다. 항목을 검색할 때 클라이언트는 일반적으로 해당 항목 유형과 관련된 속성을 지정합니다. 예를 들어, 사람 항목을 검색할 경우 CN 속성을 사용하여 특정 이름을 갖는 사람을 검색할 수 있습니다.

Directory Proxy Server는 수천 개의 LDAP 클라이언트 요청을 처리할 수 있으며 DIT (Directory Information Tree)의 서로 다른 부분에서 서로 다른 유형의 작업을 수행할 수 있는 사람 제어와 같은 LDAP 디렉토리에 관한 세부 액세스 제어 정책을 적용하도록 구성될 수 있습니다. 웹 트롤러 및 로봇이 디렉토리에 포함된 정보를 수집하기 위해 수행한 작업과 같은 특정 종류의 작업을 허용하지 않도록 Directory Proxy Server를 구성할 수도 있습니다.

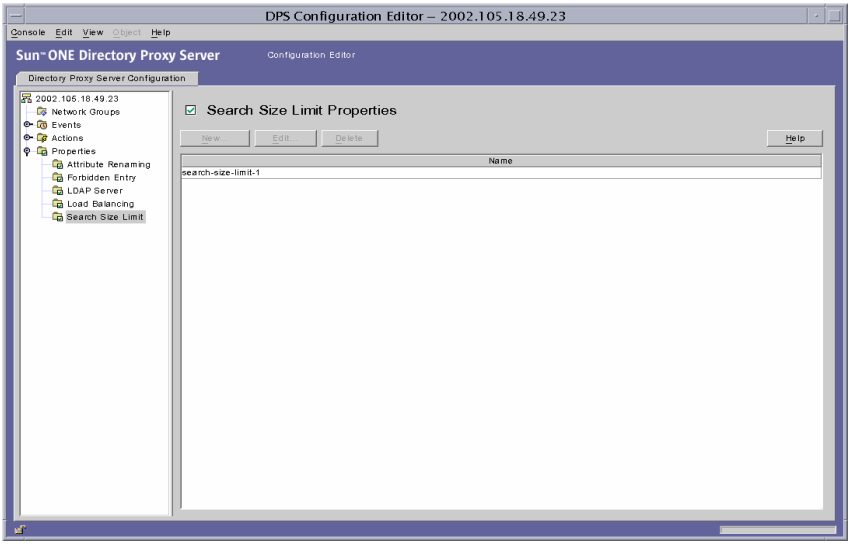
검색 기준 및 검색 범위를 기반으로 크기 제한을 적용하려면 검색 크기 제한 등록 정보를 사용합니다. 이 등록 정보 객체에 지정된 검색 기준과 검색 범위가 모두 지정된 검색과 일치하지 않는 경우 크기 제한에서는 네트워크 그룹 객체 항목에 지정된 크기 제한을 기본값으로 사용합니다. 6장, "그룹 만들기 및 관리"를 참조하십시오.

다음 절에서는 Directory Proxy Server 구성 편집기 콘솔에서 검색 크기 제한 등록 정보에 대한 객체를 만드는 방법을 설명합니다.

검색 크기 제한 등록 정보 객체 만들기

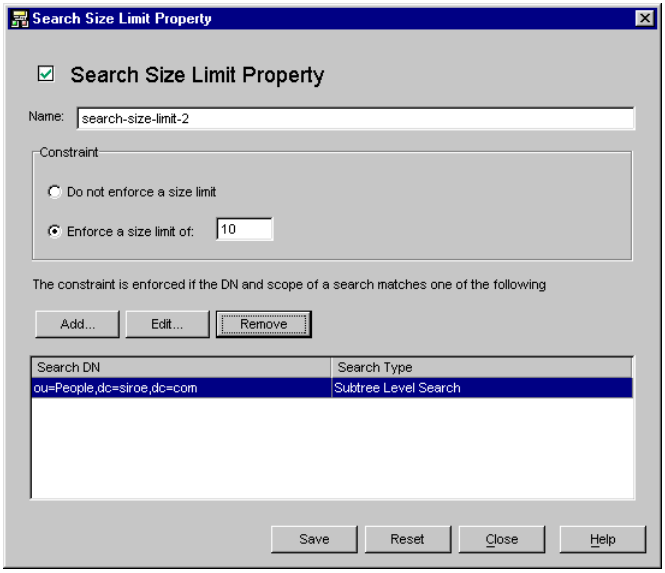
Directory Proxy Server에서 검색 크기를 제한하는 방법을 정의하려면 다음을 수행합니다.

1. Directory Proxy Server 구성 편집기 콘솔에 액세스합니다. 44페이지의 "Directory Proxy Server 콘솔 액세스"를 참조하십시오.
2. 탐색 트리에서 등록 정보 노드를 확장한 다음 검색 크기 제한을 선택합니다.



3. 새로 만들기를 누릅니다.

   검색 크기 제한 등록 정보 창이 나타납니다.



4. 이름 필드에 등록 정보 객체 이름을 입력합니다. 이 이름은 고유한 영숫자 문자열이어야 합니다.

5. 나머지 양식 요소를 사용하여 원하는 결과를 얻습니다.

   제약 조건. 크기 제한 제약 조건을 적용할 것인지 여부를 지정합니다.

   크기 제한 적용 안 함. 크기 제한이 적용되지 않게 지정하려면 이 옵션을 선택합니다.

   크기 제한 적용. 이 옵션을 선택하고 정수 값을 입력하면 적용할 크기 제한이 지정됩니다.

   추가. 크기 제한 조건을 추가할 메뉴를 표시합니다. 이 조건은 한 수준 검색 및 하위 트리 수준 검색 중 하나여야 합니다.

   한 수준 검색. DN을 입력하고 조건 테이블에 추가할 대화 상자를 표시합니다. 한 수준 검색의 검색 기준 DN이 조건 테이블의 한 수준 검색에 지정된 고유 이름 중 하나와 일치하면 지정된 크기 제한은 해당 검색 크기 제한으로 적용됩니다.

   하위 트리 수준 검색. DN을 입력할 대화 상자를 표시합니다. 하위 트리 검색의 검색 기준 DN이 조건 테이블의 하위 트리 수준 검색에 지정된 고유 이름 중 하나와 일치하면 지정된 크기 제한은 해당 검색 크기 제한으로 적용됩니다.

   편집. 테이블에서 현재 선택한 항목을 편집할 대화 상자를 표시합니다.

제거. 테이블에서 현재 선택한 항목을 제거합니다.

6. 저장을 눌러 객체를 만듭니다.

   Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 아직은 서버를 다시 시작하지 말고, 모든 구성 변경을 완료한 후에 다시 시작하십시오.

7. 추가 객체를 만들려면 단계 3에서 단계 6까지를 반복합니다.

8. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

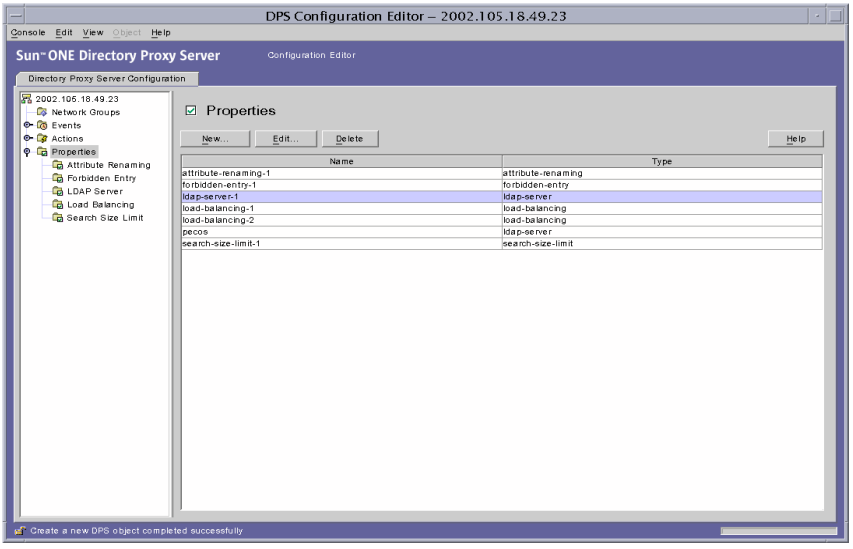
등록 정보 객체 수정

등록 정보 객체를 수정하려면 다음을 수행합니다.

1. Directory Proxy Server 구성 편집기 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.

2. 탐색 트리에서 등록 정보 노드를 선택합니다.

   오른쪽 창에 기존 등록 정보 객체의 목록이 표시됩니다. 특정 등록 정보에 속하는 객체를 보려면 등록 정보 노드를 확장한 다음, 원하는 등록 정보를 선택합니다.



3. 목록에서 수정할 객체를 선택하고 편집을 누릅니다.

4. 필요한 내용을 수정합니다.
5. 저장을 눌러 변경 내용을 저장합니다.

   Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 아직은 서버를 다시 시작하지 말고, 모든 구성 변경을 완료한 후에 다시 시작하십시오.
6. 추가 객체를 수정하려면 단계 3에서 단계 5까지를 반복합니다.
7. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

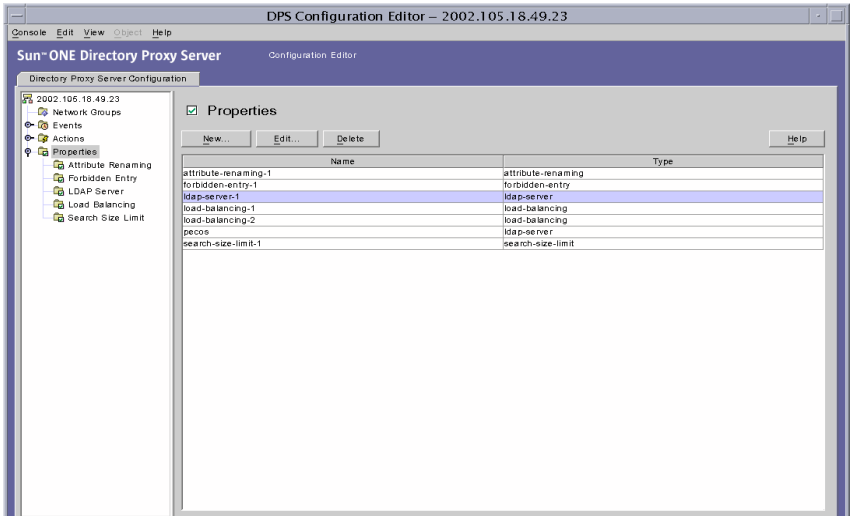
등록 정보 객체 삭제

Directory Proxy Server 구성에서 원하지 않는 등록 정보 객체를 삭제할 수 있습니다. 객체를 삭제하기 전에 해당 객체가 다른 구성 항목에 사용되지 않는지 확인합니다.

등록 정보 객체를 삭제하려면 다음을 수행합니다.

1. Directory Proxy Server 구성 편집기 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.
2. 탐색 트리에서 등록 정보 노드를 선택합니다.

   오른쪽 창에 기존 등록 정보 객체의 목록이 표시됩니다. 특정 등록 정보에 속하는 객체를 보려면 등록 정보 노드를 확장한 다음 원하는 등록 정보를 선택합니다.



3. 목록에서 삭제할 객체를 선택하고 삭제를 누릅니다.
4. 작업을 확인합니다.

   Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 아직은 서버를 다시 시작하지 말고, 모든 구성 변경을 완료한 후에 다시 시작하십시오.
5. 추가 객체를 삭제하려면 단계 3과 단계 4를 반복합니다.
6. 서버를 다시 시작합니다. 58페이지의 "Directory Proxy Server 다시 시작"을 참조하십시오.

이벤트 객체 만들기 및 관리

Sun ONE Directory Proxy Server는 이벤트 구동 작업을 지원합니다. 즉, 특정 이벤트가 발생할 때 지정된 작업을 실행하도록 Directory Proxy Server를 구성할 수 있습니다. 이 장에서는 Directory Proxy Server 구성 편집기 콘솔을 사용하여 이벤트 객체를 만들고 관리하는 방법을 설명합니다.

이 장은 다음 내용으로 구성되어 있습니다.

이벤트 개요

*이벤트*는 실행하는 동안 특정 지점에서의 특정 Directory Proxy Server 상태입니다. 이벤트 객체를 사용하여 Directory Proxy Server가 미리 지정된 상태에서 평가해야 하는 조건을 지정합니다. 또한, 이벤트 객체 정의 과정에서 조건이 충족될 경우에 Directory Proxy Server가 수행해야 하는 작업을 지정합니다. 작업에 대한 자세한 내용은 9장, "작업 객체 만들기 및 관리"를 참조하십시오.

현재 Directory Proxy Server는 두 가지 유형의 이벤트를 인식하거나 추적할 수 있습니다.

- OnBindSuccess 이벤트 - 이 이벤트는 클라이언트가 바인드 작업을 성공적으로 완료할 때 평가됩니다.

- OnSSLEstablished 이벤트 - 이 이벤트는 클라이언트가 SSL 세션을 성공적으로 구성한 경우에 평가됩니다. 이 이벤트에는 관련된 조건이 없으며 항상 자신의 작업 목록을 실행합니다.

이 두 이벤트만을 기반으로 하여 이벤트 객체를 정의할 수 있습니다. 예를 들어, 클라이언트가 바인드를 성공적으로 완료했을 때는 감지하기 위한 이벤트 객체를 정의할 수 있습니다. 이 정의 과정에서 이벤트가 발생하면 특정 작업(예: 해당 클라이언트의 액세스 그룹 변경)을 수행하도록 할 수 있습니다. 그룹에 대한 자세한 내용은 6장, "그룹 만들기 및 관리"를 참조하십시오.

이벤트 객체 만들기

이 절에서는 OnBindSuccess 및 OnSSLEstablished 이벤트를 기반으로 하는 이벤트 객체를 만드는 방법을 설명합니다. 이 이벤트에 대한 자세한 내용은 131페이지의 "이벤트 개요"를 참조하십시오.

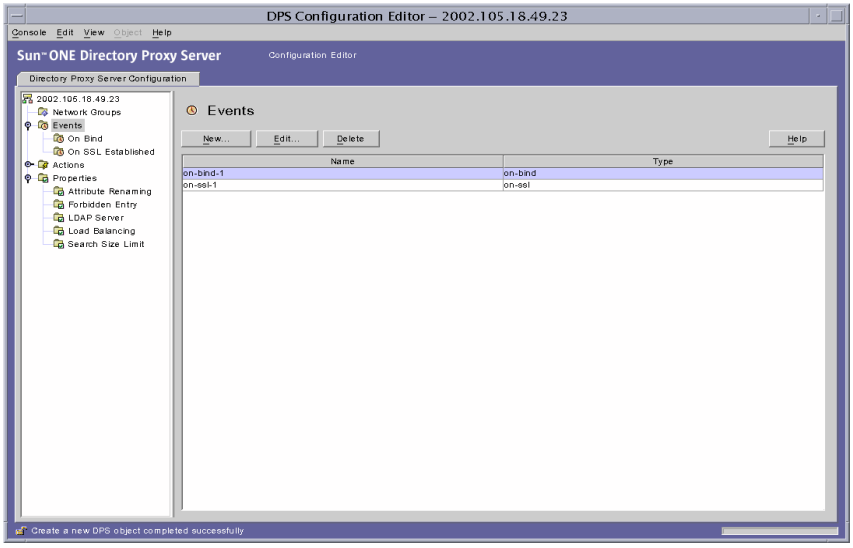
- OnBindSuccess 이벤트 객체 만들기
- OnSSLEstablished 이벤트 객체 만들기

OnBindSuccess 이벤트 객체 만들기

OnBindSuccess 이벤트를 기반으로 이벤트 객체를 만들려면 다음을 수행하십시오.

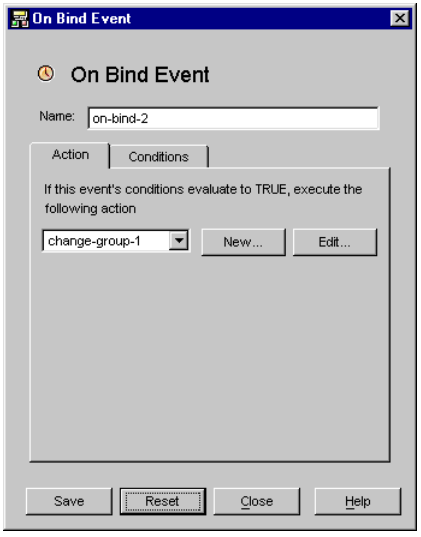
1. Directory Proxy Server 구성 편집기 콘솔에 액세스합니다. 44페이지의 "Directory Proxy Server 콘솔 액세스"를 참조하십시오.
2. 탐색 트리에서 이벤트 노드를 확장한 다음 바인드를 선택합니다.

   오른쪽 창에 OnBindSuccess 이벤트를 기반으로 하는 기존 이벤트 객체 목록이 표시됩니다.



3. 새로 만들기를 누릅니다.

   바인드 이벤트 창이 나타납니다.



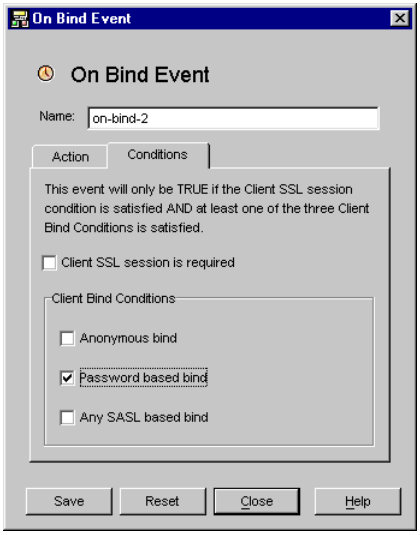
4. 이름 필드에 이벤트 객체 이름을 입력합니다. 이 이름은 고유한 영숫자 문자열이어야 합니다.

5. 작업 탭에서 이벤트가 발생할 때(이벤트가 TRUE로 평가될 때) 수행할 작업을 선택합니다.

새로 만들기. 새로 만들기 버튼을 눌러 새 작업 객체를 정의할 수도 있습니다.

편집. 편집 버튼을 눌러 현재 선택한 작업 객체에 속하는 매개 변수를 수정할 수 있습니다.

6. 조건 탭을 선택하고 조건을 지정합니다.



이벤트는 지정한 조건을 만족하는 경우에만 TRUE로 평가됩니다. 즉, 이 탭에 지정된 기준이 TRUE로 평가되어야 작업 탭에 지정된 작업이 수행됩니다. 조건은 클라이언트 SSL 세션 조건을 만족하고 3개의 클라이언트 바인드 조건 중 적어도 하나를 만족하는 경우에만 TRUE입니다.

클라이언트 SSL 세션 필요. 클라이언트가 Directory Proxy Server와 SSL 세션을 설정한 경우에만 조건이 True가 되게 하려면 이 옵션을 선택합니다. 기본값은 FALSE입니다.

클라이언트 바인드 조건. 조건은 "익명 바인드", "비밀번호 기반 바인드", "모든 SASL 기반 바인드" 중 하나입니다.

익명 바인드. 클라이언트 SSL 세션 요구 사항을 만족하고 클라이언트가 성공적으로 익명 바인드를 완료한 경우에만 조건이 True가 되게 하려면 이 옵션을 선택합니다.

비밀번호 기반 바인드. 클라이언트 SSL 세션 요구 사항을 만족하고 클라이언트가 성공적으로 비밀번호 기반 바인드를 완료한 경우에만 조건이 True가 되게 하려면 이 옵션을 선택합니다.

모든 SASL 기반 바인드. 클라이언트 SSL 세션 요구 사항을 만족하고 클라이언트가 SASL 메커니즘을 사용하여 성공적으로 바인드를 완료한 경우에만 조건이 True가 되게 하려면 이 옵션을 선택합니다.

7. 저장을 눌러 이벤트 객체를 만듭니다.

   Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 지금 서버를 다시 시작하지 말고, 모든 구성 변경을 완료한 후에 다시 시작하십시오.

8. 추가 객체를 만들려면 단계 3에서 단계 7까지 반복합니다.

9. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

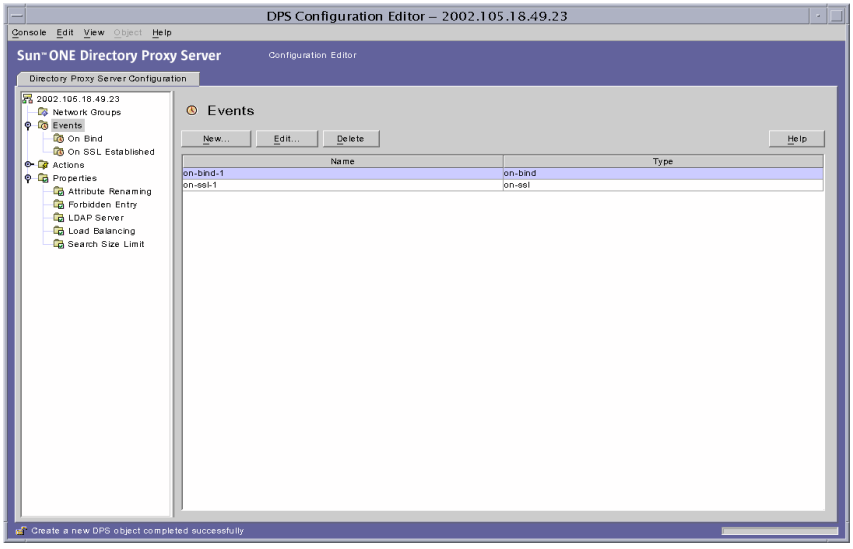
OnSSLEstablished 이벤트 객체 만들기

OnSSLEstablished 이벤트를 기반으로 이벤트 객체를 만들려면 다음을 수행하십시오.

1. Directory Proxy Server 구성 편집기 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.

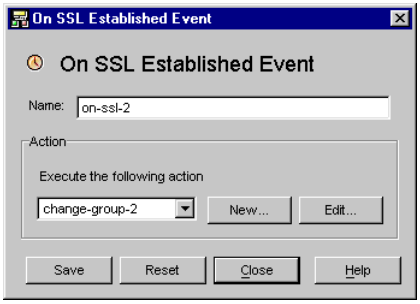
2. 탐색 트리에서 이벤트 노드를 확장한 다음 SSL 확립을 선택합니다.

   오른쪽 창에 OnSSLEstablished 이벤트를 기반으로 하는 기존 이벤트 객체의 목록이 표시됩니다.



3. 새로 만들기를 누릅니다.

   SSL 확립 이벤트 창이 나타납니다.



4. 이름 필드에 이벤트 객체 이름을 입력합니다. 이 이름은 고유한 영숫자 문자열이어야 합니다.

5. 작업 섹션에서 이벤트가 발생할 때(이벤트가 TRUE로 평가될 때) 수행할 작업을 선택합니다.

   편집 버튼을 눌러 현재 선택한 작업에 속하는 매개 변수를 수정할 수 있습니다. 새로 만들기 버튼을 눌러 새 작업을 정의할 수도 있습니다.

6. 저장을 눌러 이벤트 객체를 만듭니다.

   Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 지금 서버를 다시 시작하지 말고, 모든 구성 변경을 완료한 후에 다시 시작하십시오.

7. 추가 객체를 만들려면 단계 3에서 단계 6까지 반복합니다.

8. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

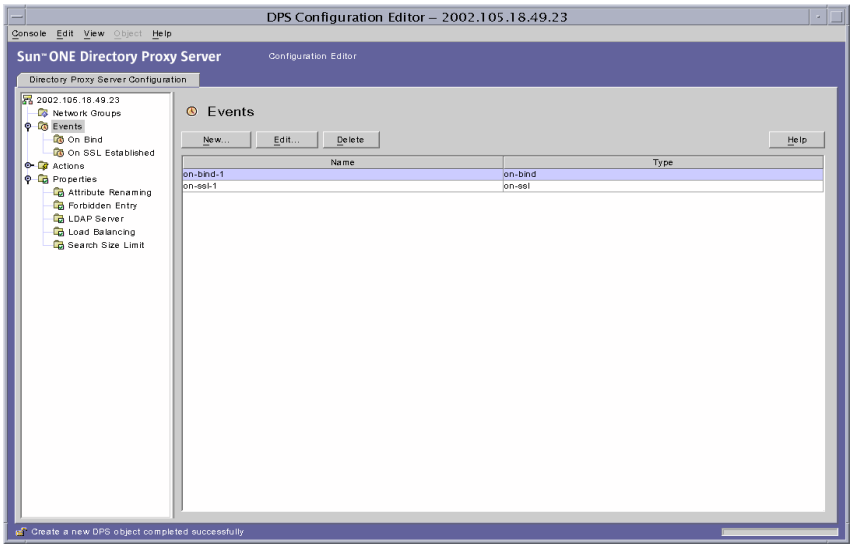
이벤트 객체 수정

이벤트 객체를 수정하려면 다음을 수행하십시오.

1. Directory Proxy Server 구성 편집기 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.

2. 탐색 트리에서 이벤트를 선택합니다.

   오른쪽 창에 기존 이벤트 객체의 목록이 표시됩니다. 이벤트 유형에 속하는 객체를 보려면 이벤트 노드를 확장한 다음 원하는 이벤트 유형을 선택합니다.



3. 목록에서 수정할 이벤트 객체를 선택하고 편집을 누릅니다.
4. 필요한 내용을 수정합니다.
5. 저장을 눌러 변경 내용을 저장합니다.

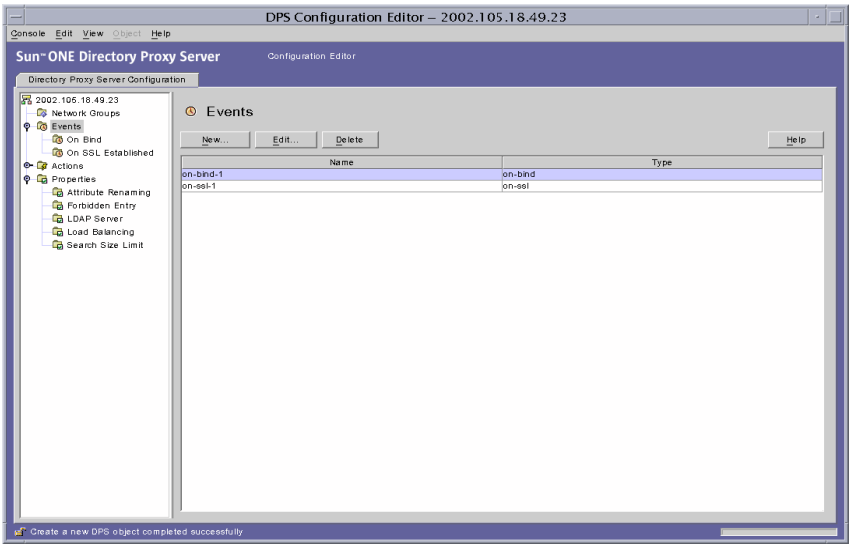
   Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 지금 서버를 다시 시작하지 말고, 모든 구성 변경을 완료한 후에 다시 시작하십시오.
6. 추가 객체를 수정하려면 단계 3에서 단계 5까지 반복합니다.
7. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

이벤트 객체 삭제

Directory Proxy Server 구성에서 원하지 않는 이벤트 객체를 삭제할 수 있습니다. 이벤트 객체를 삭제하려면 다음을 수행하십시오.

1. Directory Proxy Server 구성 편집기 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.
2. 탐색 트리에서 이벤트 노드를 선택합니다.

   오른쪽 창에 기존 이벤트 객체의 목록이 표시됩니다. 이벤트 유형에 속하는 객체를 보려면 이벤트 노드를 확장한 다음 원하는 이벤트 유형을 선택합니다.



3. 목록에서 삭제할 이벤트 객체를 선택하고 삭제를 누릅니다.
4. 확인 메시지가 표시되면 작업을 확인합니다.

   삭제한 이벤트 객체의 이름이 목록에서 제거됩니다. Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 지금 서버를 다시 시작하지 말고, 모든 구성 변경을 완료한 후에 다시 시작하십시오.
5. 추가 객체를 삭제하려면 단계 3과 단계 4를 반복합니다.
6. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

작업 객체 만들기 및 관리

Sun ONE Directory Proxy Server는 이벤트 구동 작업을 지원합니다. 즉, 특정 이벤트가 발생할 때 지정된 작업을 실행하도록 Directory Proxy Server를 구성할 수 있습니다. 이 장에서는 Directory Proxy Server 구성 편집기 콘솔을 사용하여 작업 객체를 만들고 관리하는 방법을 설명합니다.

이 장은 다음 내용으로 구성되어 있습니다.

작업 개요

*작업*은 Directory Proxy Server에서 실행할 수 있는 작업을 말합니다. 작업 객체를 사용하여 이벤트 객체에서 정의한 규칙 또는 조건이 `TRUE`일 때 Directory Proxy Server에서 수행해야 하는 작업을 지정합니다. 이벤트 객체는 Directory Proxy Server가 미리 지정된 상태에서 평가하는 조건을 지정하는 데 사용됩니다. 이벤트에 대한 자세한 내용은 8장, "이벤트 객체 만들기 및 관리"를 참조하십시오.

현재 Directory Proxy Server는 `ChangeGroup`이라는 한 가지 작업만 실행할 수 있습니다. 이 작업을 사용하면 규칙 평가 결과에 따라 클라이언트를 다른 액세스 그룹으로 변경하도록 Directory Proxy Server를 구성할 수 있습니다. 그룹에 대한 자세한 내용은 6장, "그룹 만들기 및 관리"를 참조하십시오.

그룹 변경 기능은 모바일 사용자처럼 서로 다른 여러 IP 주소 또는 서로 다른 물리적 위치에서 디렉토리에 연결하는 사용자에 대한 정보가 LDAP 디렉토리에 포함되어 있는 경우에 특히 유용합니다. 모바일 사용자가 동적 IP 주소를 사용하여 Directory Proxy Server에 연결하고 "기본" 액세스 그룹에 속하도록 Directory Proxy Server를 설정할 수 있습니다. "기본" 액세스 그룹에는 `OnBindSuccess` 이벤트를 기반으로 하는 규칙이 있습니다. 이 이벤트는 모바일 사용자가 제공한 바인드 인증서가 인증되는 경우에만 TRUE로 평가됩니다. 또한, 이 규칙에는 모바일 사용자의 액세스 그룹을 "기본값"에서 정적 IP 주소를 사용하여 Directory Proxy Server에 액세스할 때 일반적으로 할당되는 액세스 그룹으로 변경하도록 `ChangeGroup` 작업이 구성됩니다.

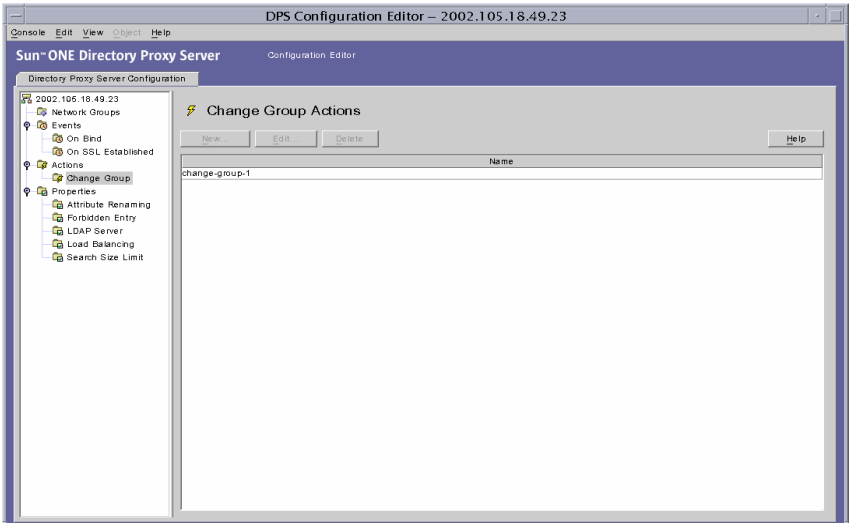
작업 객체 만들기

특정 이벤트가 발생할 때 실행해야 하는 작업에 대한 객체를 만들 수 있습니다. 아래 지침에서는 그룹 변경을 위한 작업 객체를 만드는 방법에 대해 설명합니다.

클라이언트를 다른 그룹으로 변경하는 작업 객체를 만들려면 다음을 수행합니다.

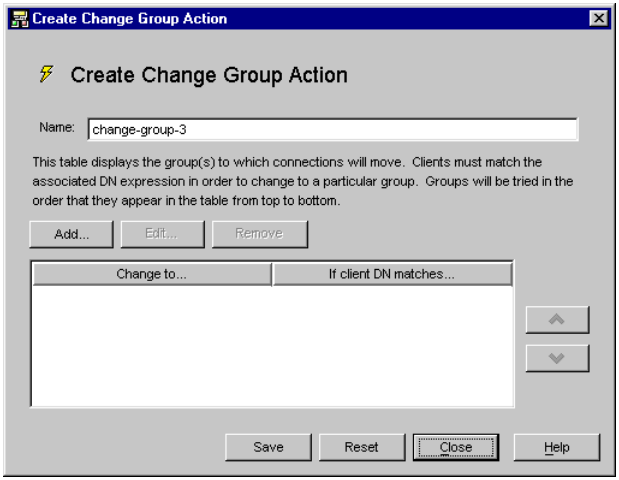
1. Directory Proxy Server 구성 편집기 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.
2. 탐색 트리에서 작업 노드를 확장한 다음 그룹 변경을 선택합니다.

   오른쪽 창에 기존 작업 객체의 목록이 표시됩니다.



3. 새로 만들기를 누릅니다.

   그룹 변경 작업 만들기 창이 나타납니다.



4. 이름 필드에 객체 이름을 입력합니다. 이름은 고유한 영숫자 문자열이어야 합니다.

5. 작업 탭에서 이벤트가 발생할 때(이벤트가 TRUE로 평가될 때) 수행할 작업을 선택합니다.

   변경... 클라이언트를 변경할 수 있는 그룹 목록을 표시합니다. 그룹을 변경하려면 클라이언트가 각 그룹과 관련된 DN 표현식과 일치해야 합니다. 특정 그룹 또는 "변경 없음" 항목과 관련된 DN 표현식을 편집하려면 테이블의 "클라이언트 DN이 일치하는 경우" 열을 누릅니다. DN 표현식이 일치될 때까지 목록의 위에서 아래로 차례대로 평가합니다. 따라서 모든 표현식이 평가되도록 목록의 맨 아래에 가장 일반적인 DN 표현식이 오도록 해야 합니다.

   정규 표현식은 표준화되어야 합니다. 예를 들어 RDN 구성 요소와 등호(=) 사이에 공백이 없어야 하고 속성 이름과 값을 모두 대문자로 지정해야 합니다.

   정규 표현식에 대한 내용은 *Mastering Regular Expressions*(저자: Friedl and Oram, 발행: O'Reilly, ISBN: 1565922573)를 참조할 수 있습니다.

   추가. 클라이언트 연결을 변경할 수 있는 그룹을 추가하기 위한 메뉴를 표시합니다. 그룹 변경 항목은 "그룹 변경 항목"이나 "변경 없음 항목" 유형 중 하나가 될 수 있습니다.

그룹 변경 항목. 관련된 DN 표현식이 TRUE로 평가되는지 여부에 따라 클라이언트를 변경할 네트워크 그룹을 선택하는 대화 상자를 표시합니다.

변경 없음 항목. 관련된 DN 표현식이 TRUE로 평가되는 경우 변경 없음을 나타내는 행을 테이블에 추가합니다. 이것은 그룹 변경 목록의 평가에 대한 "단순 회로"를 제공할 때 유용합니다.

편집. 테이블에서 현재 선택한 항목을 편집할 대화 상자를 표시합니다.

제거. 테이블에서 현재 선택한 항목을 제거합니다.

6. 저장을 눌러 작업 객체를 만듭니다.

   Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 지금 서버를 다시 시작하지 말고, 모든 구성 변경을 완료한 후에 다시 시작하십시오.

7. 추가 객체를 만들려면 단계 3에서 단계 6까지 반복합니다.

8. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

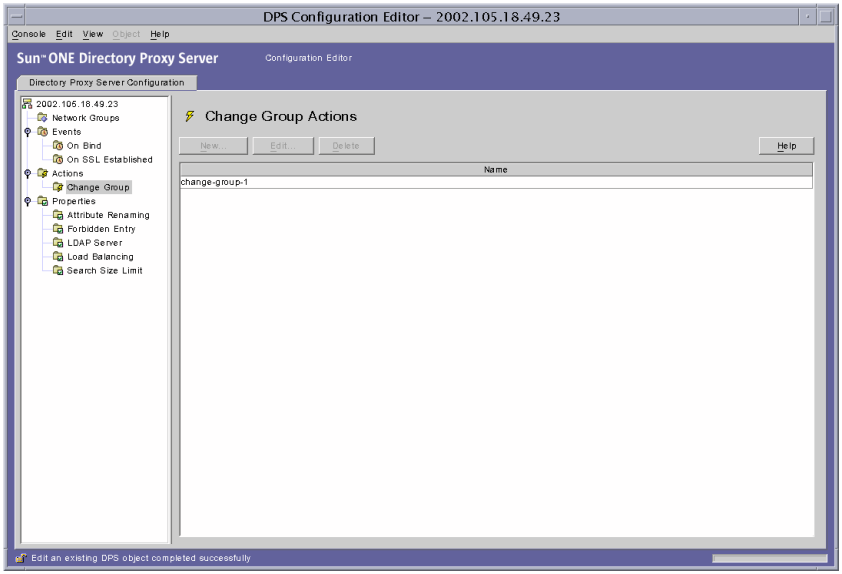
작업 객체 수정

작업 객체를 수정하려면 다음을 수행하십시오.

1. Directory Proxy Server 구성 편집기 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.

2. 탐색 트리에서 작업을 선택합니다.

   오른쪽 창에 기존 작업 객체의 목록이 표시됩니다.



3. 목록에서 수정할 작업 객체를 선택하고 편집을 누릅니다.
4. 필요한 내용을 수정합니다.
5. 저장을 눌러 변경 내용을 저장합니다.

   Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 지금 서버를 다시 시작하지 말고, 모든 구성 변경을 완료한 후에 다시 시작하십시오.
6. 추가 객체를 수정하려면 단계 3에서 단계 5까지 반복합니다.
7. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

작업 객체 삭제

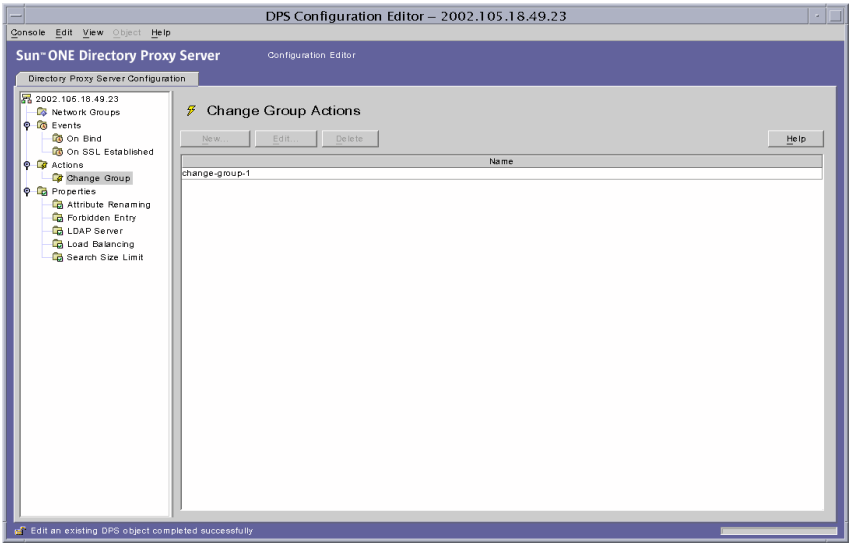
Directory Proxy Server 구성에서 원하지 않는 작업 객체를 삭제할 수 있습니다. 작업 객체를 삭제하기 전에 해당 객체가 이벤트 객체 구성에 사용되지 않는지 확인합니다.

작업 객체를 삭제하려면 다음을 수행하십시오.

1. Directory Proxy Server 구성 편집기 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.

2. 탐색 트리에서 작업을 선택합니다.

   오른쪽 창에 기존 작업 객체의 목록이 표시됩니다.



3. 목록에서 삭제할 작업을 선택하고 삭제를 누릅니다.

4. 작업을 확인합니다.

   삭제한 객체의 이름이 목록에서 제거됩니다. Directory Proxy Server 구성이 수정되고 이 구성에 따라 서버를 다시 시작할지 묻는 메시지가 표시됩니다. 지금 서버를 다시 시작하지 말고 모든 구성 변경을 완료한 후에 다시 시작하십시오.

5. 추가 객체를 삭제하려면 단계 3과 단계 4를 반복합니다.

6. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

로그 구성 및 모니터링

이 장에서는 Sun ONE Directory Proxy Server에서 항목 또는 메시지를 기록한 다음 Directory Proxy Server 서버 콘솔을 사용하여 기록된 항목을 참조하여 해당 작업을 모니터링하는 방법을 설명합니다.

이 장은 다음 내용으로 구성되어 있습니다.

로깅 개요

Directory Proxy Server는 두 가지 유형의 로그를 유지 관리할 수 있습니다.

- 시스템 로그
- 감사 로그

다음 절에서는 두 로그 유형에 대해 자세히 설명합니다.

시스템 로그

Directory Proxy Server에서는 사용자가 시스템을 모니터링하고 디버그할 수 있도록 여러 이벤트 및 시스템 오류의 로그 레코드를 광범위하게 유지 관리할 수 있습니다. 모든 로그 레코드는 텍스트 파일로 관리할 수 있으며 쉽고 빠르게 검색할 수 있도록 로컬 파일 시스템에 저장할 수 있습니다. 기본적으로 Directory Proxy Server는 이 파일에 로그 항목을 기록합니다.

```
<server-root>/dps-<hostname>/logs/fwd.log
```

로그 파일의 각 메시지에는 타임스탬프가 있습니다. 또한, Directory Proxy Server에 속하는 프로세스 번호와 메시지 번호가 있습니다.

식별 및 필터링의 편의를 위해 Directory Proxy Server에서 기록되는 이벤트는 다양한 범주로 분류됩니다. 이러한 범주는 표 10-1에 나열되어 있습니다. 각 범주에는 동일하거나 비슷한 특성을 갖거나 특정 기능 영역에 속하는 메시지가 표시됩니다. 로그 파일에는 그 구성에 따라 이러한 범주 중 하나 이상에 속하는 항목을 기록할 수 있습니다.

Directory Proxy Server 구성에서 각 메시지 범주는 특정 로그 수준에 해당합니다. 로그 수준은 서버에서 수행할 로깅 수준(로깅의 정보 수준)을 나타냅니다.

- 우선 순위가 높을수록 더 적은 정보가 필요하기 때문에 우선 순위가 높은 이벤트만 기록됩니다.
- 우선 순위가 낮을수록 더 많은 정보가 제공되기 때문에 로그 파일에 더 많은 종류의 이벤트가 기록됩니다.

표 10-1에는 메시지 범주가 우선 순위를 기준으로 내림차순으로 나열되어 있습니다. 즉, 위험이 우선 순위 수준이 가장 높고 세부 정보 추적이 우선 순위 수준이 가장 낮습니다.

표 10-1 로그 수준

로그 수준 또는 심각도	설명
필수	필수 메시지는 로그에 항상 기록되는 메시지입니다. 이 메시지는 Directory Proxy Server에서 시작할 때 읽는 Directory Proxy Server 버전 번호 등과 같은 구성을 나타냅니다. 이 수준에 속하는 메시지는 구성할 수 없습니다.
위험	이 메시지는 Directory Proxy Server에서 발생한 즉각적인 주의를 필요로 하는 문제를 나타냅니다(예: *Directory Proxy Server process 1234 has exited, attempting restart in 10 seconds).*
예외	이러한 메시지는 Directory Proxy Server가 형식이 올바르지 않은 LDAP 메시지 등과 같은 예기치 않은 오류 조건을 클라이언트/서버로부터 수신했음을 나타냅니다(예: *Could not decode search request).*
경고	이러한 메시지는 Directory Proxy Server에서 무시할 수도 있지만 관리자가 조사해야 하는 오류 조건을 지정합니다(예: *Local host name lookup failed. System default group may not function correctly).*

표 10-1 로그 수준 *(계속)*

로그 수준 또는 심각도	설명
알림	이러한 메시지는 정보 제공용입니다(예: *Received NULL continuation reference from server. Discarding..*).
추적	이것은 디버깅 메시지입니다(예: *Result received from server lderr =32, matched=o=sun.com, errtxt=no such object)*. 추적 메시지에는 프로토콜 덤프가 포함되어 있습니다. 추적 수준을 사용하면 매우 큰 로그 파일을 빠르게 생성할 수 있습니다.
세부 정보 추적	이러한 메시지는 연결을 다시 사용하기 위해 요청한 익명 바인드와 같은 세부 디버깅 정보를 제공합니다. 이러한 메시지에는 일반적으로 Directory Proxy Server 엔지니어링 및 지원 팀에서 필요로 하는 중요한 정보가 있습니다.

Directory Proxy Server에서는 로깅의 양을 지정할 수 있습니다. 즉, 로그 수준을 사용하여 이벤트의 심각도에 따라 로그 항목을 필터링할 수 있습니다. 기본적으로 이 수준은 경고로 설정되어 있습니다.

주 로그 수준은 부가적인 것입니다. 즉, 로그 수준으로 경고를 선택하면 경고, 예외 및 위험 수준 메시지가 기록됩니다. 특히 로깅 수준이 더 낮을수록 로그 데이터의 볼륨이 커질 수 있습니다. 호스트 시스템에 모든 로그 파일에 필요한 디스크 공간이 충분히 있는지 확인합니다.

선택적으로 Windows NT 이외의 플랫폼에서 로그 메시지를 파일 대신 `syslog` 데몬에 보내도록 Directory Proxy Server를 구성할 수 있지만, 로그 메시지를 파일과 `syslog` 데몬 모두에 동시에 보낼 수는 없습니다. 이 구성을 선택할 경우 `syslogd`를 정확하게 구성해야 합니다. 예를 들어, 모든 메시지를 특정 파일인 `/var/adm/messages`에 기록하게 하려면 `/etc/syslog.conf`에 다음 행을 추가해야 합니다.

```
daemon.crit;daemon.warning;daemon.info;daemon.debug /var/adm/messages
```

Directory Proxy Server에서는 `daemon` 기능을 `crit`, `warning`, `info` 및 `debug` 우선 순위 또는 로그 수준으로 사용합니다. 표 10-1은 syslog 이벤트와 Directory Proxy Server 이벤트 사이의 매핑을 나타냅니다.

표 10-2 로그 수준 매핑

Directory Proxy Server 이벤트	syslog 이벤트
필수	info
위험	crit
예외	err
경고	warning
알림	info
추적	info
세부 정보 추적	info

Directory Proxy Server 로그를 회전하고 다른 로깅 기능을 제어하려면 다음 객체 클래스를 사용합니다.

`ids-proxy-sch-LogProperty`

이 객체 클래스와 그 사용 방법에 대한 자세한 내용은 195페이지의 “dpsconfig2ldif”를 참조하십시오.

감사 로그

Directory Proxy Server에서는 로깅 시스템과 오류 메시지 외에도 모든 이벤트와 연결 통계에 대한 감사 추적을 관리할 수 있습니다. 예를 들어, LDAP 디렉토리에 방금 바인드/언바인드를 완료한 클라이언트의 DN을 기록할 수 있습니다.

기본적으로 Directory Proxy Server는 감사 메시지를 기록하도록 구성되어 있지 않습니다. 언제든지 이 기능을 활성화할 수 있습니다. 또한, 감사 메시지를 시스템 로그 항목이 기록되는 파일에 기록할지 대체 파일에 기록할지 여부를 지정할 수 있습니다. 다른 파일에 기록하도록 구성하지 않은 경우 감사 메시지는 시스템 로그 항목이 기록되는 파일에 다른 로그 메시지와 함께 기록됩니다. 자세한 내용은 145페이지의 “시스템 로그”를 참조하십시오.

주 감사 레코드를 사용하여 인증되지 않은 액세스 또는 작업을 검색할 수 있습니다. 이 기능을 사용하는 것이 좋습니다. 또한, 보안을 위해 Directory Proxy Server 감사 로그를 주기적으로 검사하여 잘못된 작업을 확인하십시오.

로그 구성

Directory Proxy Server에서 항목을 기록하도록 구성하려면 다음 단계를 따릅니다.

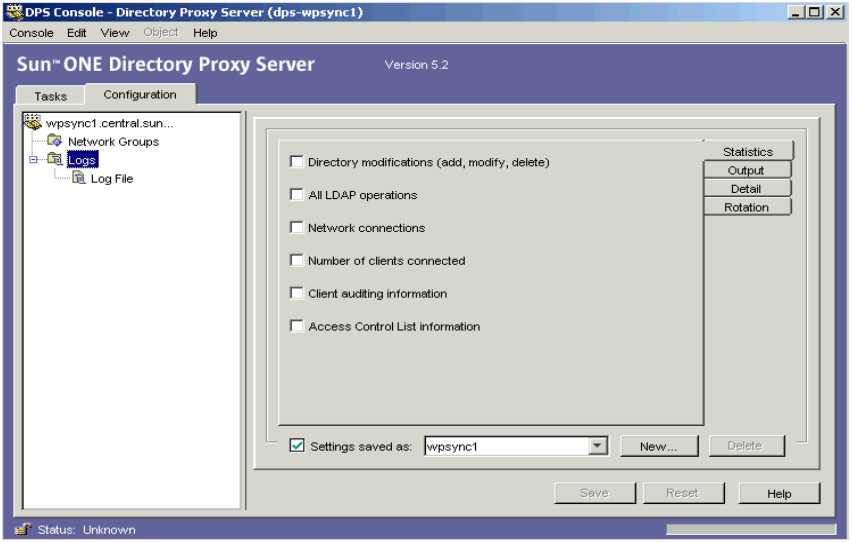
- 단계 1. 로그 설정 정의
- 단계 2. 사용할 로깅 등록 정보 지정

단계 1. 로그 설정 정의

로그 등록 정보에 대한 객체를 만들거나 정의하려면 이 단계를 반드시 수행해야 합니다. 로그 등록 정보에 대한 객체를 이미 만든 경우 해당 객체 중 하나를 사용하려면 다음 단계로 건너뜁니다.

1. Directory Proxy Server 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.
2. 구성 탭을 선택한 다음 탐색 트리에서 로그를 확장합니다.

   오른쪽 창의 오른쪽에 로깅 등록 정보에 대한 기존 객체 목록이 표시됩니다.



3. 새로 만들기를 눌러 새 객체를 정의합니다.

   로그 등록 정보 창 통계 탭이 활성화됩니다.

4. 이름 필드에 객체 이름을 입력합니다. 이 이름은 고유한 영숫자 문자열이어야 합니다.

5. 통계 탭에서 기록할 정보 종류를 지정합니다.

   원하는 로깅 메시지 유형을 참조하는 상자를 선택합니다. 기본적으로 아무 옵션도 선택되지 않습니다. 로그 메시지는 디렉토리 수정, 모든 LDAP 작업, 네트워크 연결, 연결된 클라이언트 수 및 클라이언트 감사 정보 그룹으로 분류됩니다.

   디렉토리 수정. 추가, 수정 및 삭제처럼 디렉토리에 작성하는 작업에 대한 통계가 기록됩니다.

   모든 LDAP 작업. 모든 LDAP 작업에 대한 통계가 기록됩니다.

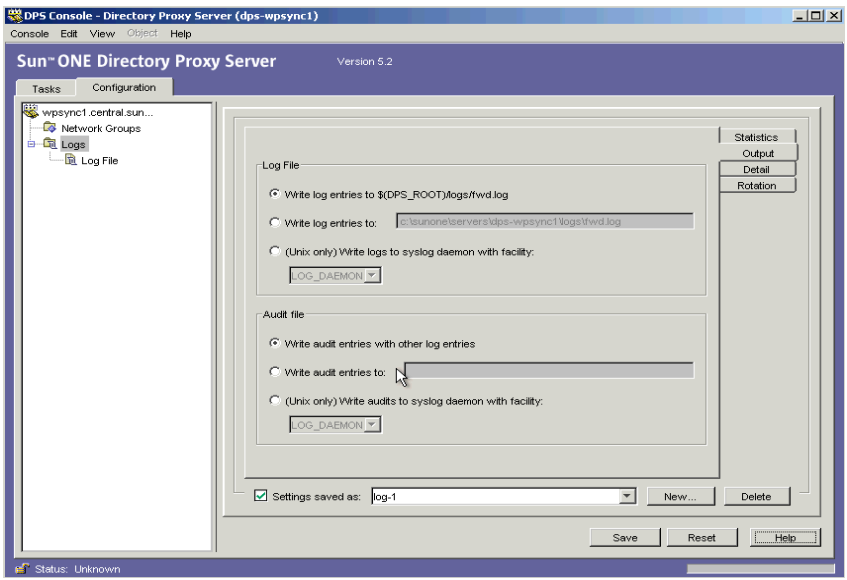
   네트워크 연결. 네트워크 연결에 대한 통계가 기록됩니다.

   연결된 클라이언트 수. 연결된 클라이언트 수와 같은 일반 통계가 기록됩니다.

   클라이언트 감사 정보. 바인드/언바인드를 방금 완료한 클라이언트의 DN과 같은 감사 정보가 기록됩니다.

   액세스 제어 목록 정보. 이 정보에는 로그 정보에 액세스할 권한이 있는 사용자의 목록이 있습니다.

6. 출력 탭을 선택하고 로그 항목을 보낼 위치와 감사 추적을 기록할지 여부를 지정합니다.



로그 파일. Directory Proxy Server에서 해당 로그 항목을 기록할 위치를 제어하는 옵션을 표시합니다.

로그 항목을 $(dps_ROOT)/logs/fwd.log에 기록. 이 설정은 Directory Proxy Server에서 로그 항목을 `$(dps_ROOT)/logs/fwd.log` 파일에 기록하는 기본 설정입니다. 여기서 `$(dps_ROOT)`는 Directory Proxy Server가 설치되는 서버 루트 아래에 있는 디렉토리이며, 일반적으로 `/usr/sunone/servers/dps-<hostname>` 또는 `\Program\Files\sunone\Servers\dps-<hostname>`입니다.

로그 항목 기록 대상. Directory Proxy Server에서 해당 로그 항목을 기록할 대체 파일을 지정합니다. 파일 분리자는 플랫폼에 관계없이 UNIX 규약 다음에 와야 합니다.

기능이 있는 syslog 데몬에 로그 기록. (UNIX 전용) Directory Proxy Server에서 항목을 기록할 때 사용할 syslog 기능 코드를 선택합니다. 이 로그 등록 정보가 UNIX 시스템에 설치된 Directory Proxy Server 서버에 사용될 경우에만 이 설정을 선택해야 합니다. Windows NT 시스템에 설치된 Directory Proxy Server에 대해 이 옵션 지정하면 시스템이 작동하지 않게 됩니다. 이 속성 값을 지정하려면 Windows NT 및 UNIX에 대한 별도의 로그 등록 정보를 만드는 것이 좋습니다.

감사 파일. Directory Proxy Server에서 해당 감사 로그 항목을 기록할 위치를 제어하는 옵션을 표시합니다. 이 기능이 작동하려면 통계 탭에서 "클라이언트 감사 정보" 옵션을 선택하여 감사 로깅을 활성화해야 합니다.

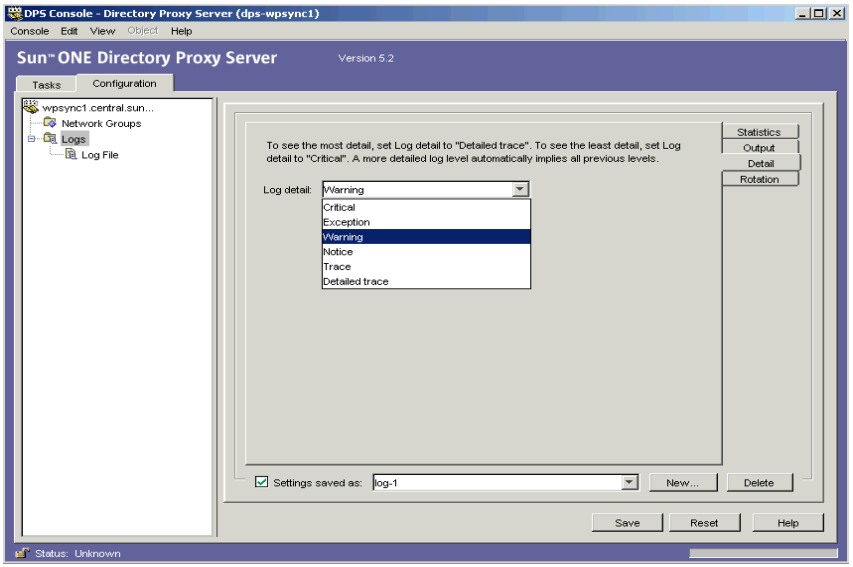
다른 로그 항목과 함께 감사 항목 기록. 이것은 Directory Proxy Server에서 위의 로그 파일 설정에 지정된 출력 파일에 해당 감사 로그 항목을 기록하는 기본 설정입니다.

로그 항목 기록 대상. Directory Proxy Server에서 해당 감사 로그 항목을 기록할 대체 파일을 지정합니다. 파일 분리자는 플랫폼에 관계없이 UNIX 규약 다음에 와야 합니다.

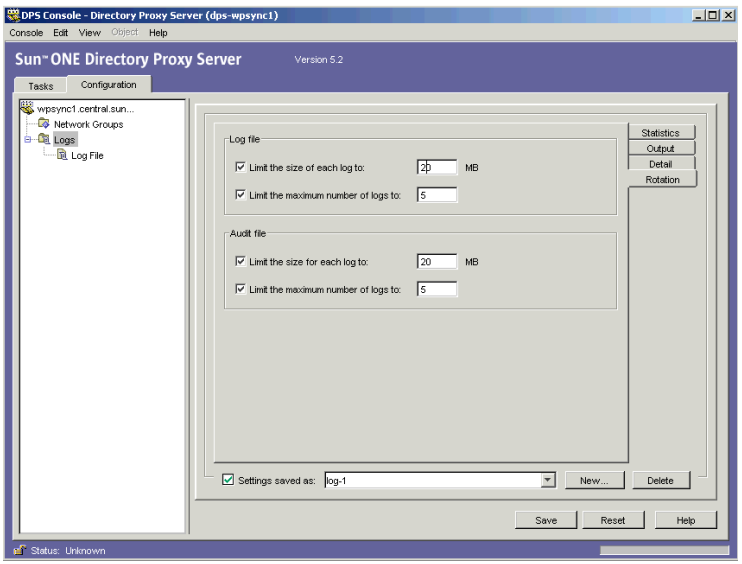
기능이 있는 syslog 데몬에 감사 기록.(UNIX 전용) Directory Proxy Server에서 감사 항목을 기록할 때 사용할 syslog 기능 코드를 선택합니다. 이 로그 등록 정보가 UNIX 시스템에 호스트된 Directory Proxy Server 서버에 사용될 경우에만 이 설정을 선택해야 합니다. 이 옵션을 지정하면 Windows NT 기반 Directory Proxy Server가 작동하지 않게 됩니다. 이 속성 값을 지정하려면 Windows NT 및 UNIX에 대한 별도의 로그 등록 정보 객체를 만드는 것이 좋습니다.

7. 세부 정보 탭을 선택하고 로그 수준(원하는 로깅 정보 양)을 지정합니다.

   드롭다운 메뉴에서 로깅 수준을 선택합니다.



8. 회전 탭을 선택하여 로그의 크기와 회전량을 제어합니다.



로그 파일. Directory Proxy Server 로그 파일의 크기와 최대 수를 제한하는 옵션을 표시합니다.

각 로그의 크기 제한. 각 로그 파일의 최대 크기(MB)를 입력합니다.

최대 로그 파일 수 제한. 만들고 회전시킬 최대 로그 파일 수를 입력합니다.

감사 파일. Directory Proxy Server 감사 파일의 크기 및 최대 수를 제한하는 옵션을 표시합니다.

각 로그의 크기 제한. 각 감사 로그 파일의 최대 크기(MB)를 입력합니다.

최대 로그 파일 수 제한. 만들고 회전시킬 최대 감사 로그 파일 수를 입력합니다.

9. 저장을 눌러 변경 내용을 저장합니다.

   객체 이름이 목록에 표시됩니다. Directory Proxy Server 구성이 수정되고 서버를 다시 시작하라는 메시지가 표시됩니다.

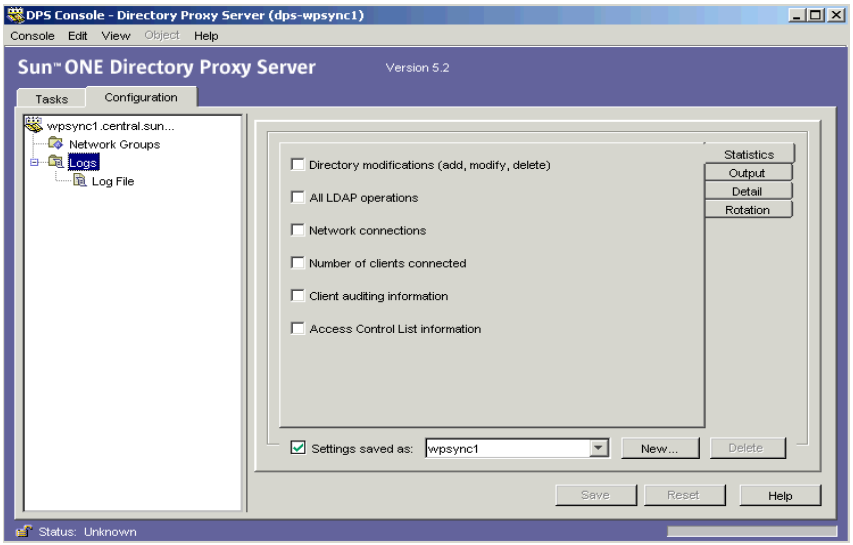
10. 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

단계 2. 사용할 로깅 등록 정보 지정

이 단계에서는 로깅 메시지에 사용할 기존 로그 등록 정보를 선택합니다.

1. Directory Proxy Server 서버 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.
2. 구성 탭을 선택한 다음 탐색 트리에서 로그를 선택합니다.

   오른쪽 창에 현재 시스템 등록 정보에 지정된 로그 등록 정보에 관한 정보가 표시됩니다.



3. "다음 이름으로 설정 저장" 드롭다운 목록에서 사용할 등록 정보를 선택합니다.
4. 저장을 눌러 변경 내용을 저장합니다.

   Directory Proxy Server가 구성에 정의된 대로 메시지를 기록하도록 구성됩니다. Directory Proxy Server 구성이 수정되고 서버를 다시 시작하라는 메시지가 표시됩니다.
5. 작업 탭을 선택하고 서버를 다시 시작합니다. 58페이지의 “Directory Proxy Server 다시 시작”을 참조하십시오.

Directory Proxy Server 서버 콘솔에서 로그 모니터링

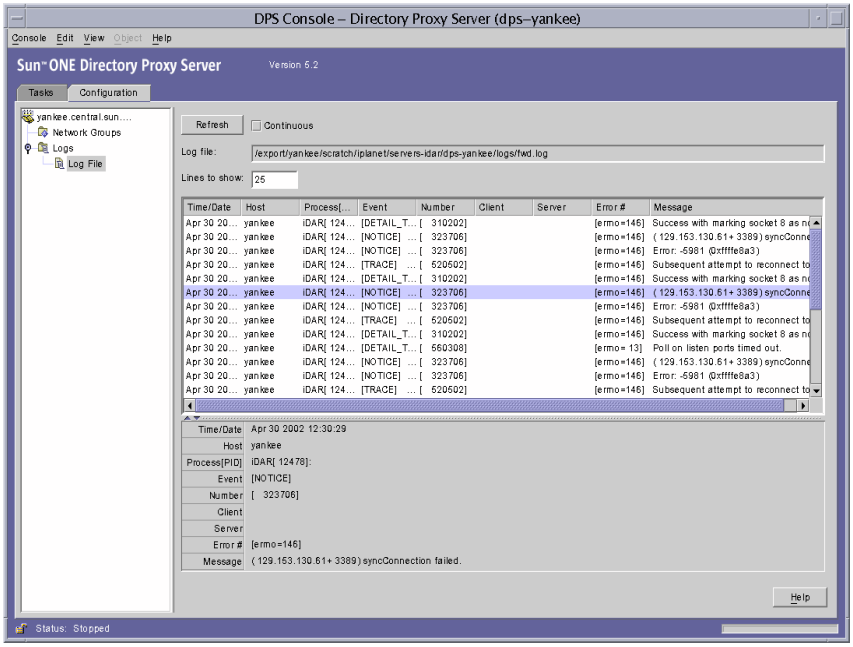
Directory Proxy Server에서 메시지를 기록하도록 구성한 경우(149페이지의 “로그 구성” 참조) 로그 메시지를 보고 작업을 모니터링할 수 있습니다. 예를 들어, Directory Proxy Server에 문제가 발생하여 문제를 해결해야 할 경우 서버에 기록된 오류 또는 정보 메시지를 참조하여 도움을 받을 수 있습니다. 또한, 로그 파일을 조사하여 Directory Proxy Server 작업을 모니터링할 수 있습니다.

이 기능을 사용할 수 있도록 Directory Proxy Server 서버 콘솔은 로그 파일의 내용을 볼 수 있는 간단한 메커니즘을 제공합니다. 보기 위해 선택한 로그 파일의 내용은 표 형식으로 표시됩니다. 테이블은 두 개의 창으로 나뉩니다. 위쪽 창에는 테이블 형식으로 로그 레코드가 표시되고 아래쪽 창에는 현재 선택한 레코드가 자세히 표시됩니다. 각 로그 레코드에는 메시지가 기록된 날짜와 시간, 메시지의 심각도, 로그에 대한 일반 설명 등과 같은 정보가 포함되어 있습니다.

로그 파일을 열어서 볼 때 표시할 레코드 또는 항목의 수를 지정하여 내용을 부분적으로 볼 수 있습니다. 아래 지침에서는 로그 레코드를 파일로 보는 방법을 설명합니다.

1. Directory Proxy Server 서버 콘솔에 액세스합니다. 44페이지의 “Directory Proxy Server 콘솔 액세스”를 참조하십시오.
2. 구성 탭을 선택한 다음 탐색 트리에서 로그를 확장합니다.
3. 로그 파일을 선택합니다.

   오른쪽 창에 파일에 기록된 항목 보기 옵션이 표시됩니다. 현재 로그 등록 정보에 지정된 로그 파일을 선택할 수 있습니다. Directory Proxy Server는 개별 로깅 및 감사 정보 파일을 포함할 수 있습니다(구성된 경우).



형식 요소에 대한 설명은 다음과 같습니다.

갱신. 로그를 읽고 아래 표에 레코드를 표시합니다.

계속. 이 뷰가 가장 최신 레코드로 계속 갱신되도록 하려면 이 설정을 선택합니다.

로그 파일. 현재 보고 있는 파일의 이름을 표시합니다.

표시할 행. 로그 파일에서 읽을 최대 행 수를 지정합니다.

보안 구성

Sun ONE Directory Proxy Server는 클라이언트와 백엔드 디렉토리 서버 간의 보안 통신을 위해 SSL/TLS를 지원합니다.

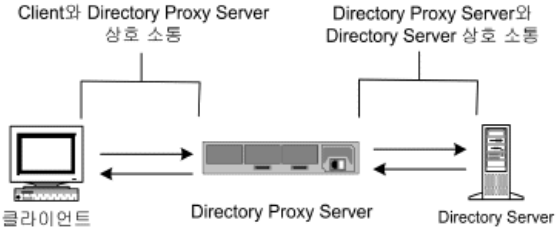
- SSL 및 TLS 설정 준비
- SSL 통신 설정

이 절의 내용 중 일부는 이 설명서를 읽는 사용자가 공개 키 암호화 및 SSL (Secure Sockets Layer) 프로토콜의 기본 개념을 잘 알고 있으며 인트라넷, 엑스트라넷을 비롯하여 인터넷 보안 개념과 기업 내 디지털 인증서의 개념에 대해 이해하고 있다는 가정하에 쓰여진 것입니다. 이러한 개념을 처음 접하는 사용자는 본 설명서의 보안 관련 부록인 *Managing Servers with Sun ONE Console*을 먼저 읽어 보십시오.

iDAR 5.0x에서 업그레이드하는 경우 SSL 구성을 이전하기 위한 절차는 *Directory Proxy Server 설치 설명서*에 자세히 설명되어 있습니다.

Directory Proxy Server에는 개별적으로 구성할 수 있는 두 개의 통신 링크가 있습니다. 각 통신 링크는 일반 텍스트일 수도 있고 TLS (Transport Layer Security) 또는 SSL (Secure Sockets Layer) 프로토콜을 사용하여 암호화할 수도 있습니다. 두 개의 통신 링크를 사용할 수 있으므로 LDAP 클라이언트와 Directory Proxy Server 사이, 그리고 Directory Proxy Server와 LDAP 디렉토리 사이에 TLS 또는 SSL을 사용하는 통신을 구성할 수 있습니다. 그림 11-1은 Directory Proxy Server의 이러한 기능을 보여줍니다.

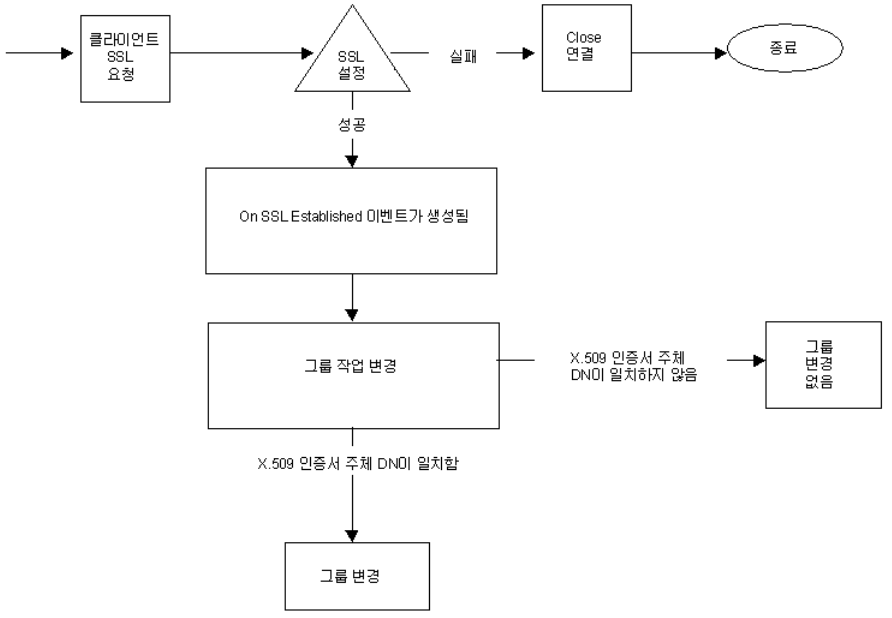
그림 11-1 Directory Proxy Server 두 개의 개별적인 통신 링크



Directory Proxy Server는 클라이언트 인증서와 서버 인증서 두 가지를 모두 확인할 수 있습니다. 단, 확인 중인 인증서에 대해 신뢰할 수 있는 루트 CA 인증서가 설치되어 있고 이 인증서를 Directory Proxy Server에서 사용할 수 있어야 합니다.

그림 11-2는 SSL 세션을 설정한 후 Directory Proxy Server가 클라이언트에서 제공한 인증서를 확인하는 방법을 보여줍니다.

그림 11-2 클라이언트의 인증서 기반 인증



SSL 및 TLS 설정 준비

내부 보안 장치나 외부 하드웨어 장치 또는 두 가지 모두 중 어느 것을 사용하는지에 따라 SSL과 TLS를 설정하는 방법이 달라집니다. 이 절에서는 이러한 설정 방법에 대해 설명합니다.

내부 보안 장치와 함께 SSL 또는 TLS를 설정하는 방법

SSL 또는 TLS를 내부 보안 장치와 함께 설정하려면 인증서를 요청하여 설치해야 합니다. 인증서를 요청하려면 인증서 요청 마법사를 실행하고 인증서를 설치하려면 인증서 설치 마법사를 실행합니다. 프롬프트가 나타나면 내부 보안 장치에 인증서를 설치할 것임을 지정하십시오.

외부 보안 장치와 함께 SSL 또는 TLS를 설정하는 방법

FORTEZZA와 같은 외부 보안 장치와 함께 SSL을 설정하려면 먼저 외부 장치 제조업체에서 제공하는 PKCS #11 모듈을 설치한 다음 인증서 요청 마법사를 실행하여 프롬프트가 표시되면 외부 보안 장치를 지정합니다.

내부 및 외부 보안 장치와 함께 SSL을 설정하는 방법

기업에 있는 서버와 클라이언트 중에는 내부 보안 장치만 사용하는 것도 있지만 내부 보안 장치와 외부 보안 장치를 모두 사용하는 것도 있습니다. 서버가 내부 및 외부 보안 장치를 모두 실행하는 제품과 통신해야 하는 경우에는 인증서 요청 마법사를 *두 번* 실행하십시오. 처음 사용할 때 프롬프트가 나타나면 내부 보안 장치를 지정합니다. 두 번째로 사용할 때 프롬프트가 나타나면 외부 보안 장치를 지정합니다.

SSL 통신 설정

일반적으로 SSL 사용 통신을 위해 Directory Proxy Server를 설정하려면 다음 단계를 수행해야 합니다.

- 단계 1. Directory Proxy Server를 위한 서버 인증서 설치
- 단계 2. Directory Proxy Server와 클라이언트 간의 SSL 연결 설정
- 단계 3. Directory Proxy Server와 LDAP 서버 간의 SSL 연결 설정

단계 1. Directory Proxy Server를 위한 서버 인증서 설치

인증서를 요청하고 설치할 때는 두 개의 마법사를 사용합니다. 새로운 서버 인증서를 요청하거나 이미 사용하고 있는 인증서를 갱신하려면 인증서 요청 마법사를 사용합니다. *인증 기관*(CA)에서 받은 인증서를 설치하려면 인증서 설치 마법사를 사용합니다. 또한 인증서 요청 마법사를 처음 사용할 때 *키 및 인증서 데이터베이스*가 자동으로 만들어지고 설치됩니다.

Directory Proxy Server를 위한 서버 인증서를 설치하려면 다음 단계를 수행합니다.

- 단계 A. 서버 인증서 요청 생성
- 단계 B. 서버 인증서 요청 보내기
- 단계 C. 인증서 설치
- 단계 D. CA 인증서 또는 서버 인증서 체인 설치
- 단계 E. 인증서 데이터베이스 백업 및 복원

SSL 인증서

Sun ONE Directory Proxy Server는 서버 인증서, 서버 인증서 체인, 신뢰할 수 있는 CA 인증서 등의 세 가지 인증서를 설치할 수 있습니다.

*서버 인증서*는 서버와 관련된 단일 인증서로서 클라이언트에 대해 서버를 식별해 줍니다. 이러한 유형의 인증서를 받으려면 CA에 요청해야 합니다. 서버 인증서를 구해서 설치하려면 요청을 만들어 CA에 보낸 다음 인증서를 받아서 설치하십시오.

*서버 인증서 체인*은 회사 내부 인증서 서버나 알려진 CA에 의해 자동으로 작성된 인증서 모음입니다. 체인에 속한 인증서는 해당 인증서를 발급한 CA를 찾아서 인증 확인을 받습니다. 이 확인 과정은 새로운 서버 인증서를 얻거나 설치할 때마다 필요합니다.

*신뢰할 수 있는 CA 인증서*는 회사 내부 인증서 서버나 알려진 CA에 의해 자동으로 작성된 단일 인증서입니다. 신뢰할 수 있는 CA 인증서는 클라이언트를 인증하는 데 사용됩니다.

신뢰할 수 있는 CA 인증서를 구하려면 내부 인증서 서버 또는 CA의 웹 사이트로 가서 필요한 인증서 정보를 복사하여 파일에 저장한 다음 인증서 설치 마법사를 사용하여 인증서를 설치합니다.

한 서버에 SSL 인증서를 원하는 대로 설치할 수 있습니다. Directory Server 인스턴스를 위해 SSL을 설정할 때는 최소한 한 개의 서버 인증서와 한 개의 신뢰할 수 있는 CA 인증서를 설치해야 합니다.

단계 A. 서버 인증서 요청 생성

Sun ONE Directory Proxy Server를 사용하여 인증 기관(CA)에 제출할 인증서 요청을 생성할 수 있습니다.

1. Sun ONE Directory Proxy Server 탐색 트리에서 SSL 암호화를 사용하려는 서버 인스턴스를 선택합니다.
2. 서버 인스턴스를 두 번 누르거나 열기를 눌러 서버 인스턴스의 관리 창을 엽니다.
3. 콘솔 메뉴에서 보안> 인증서 관리를 선택합니다.

   인증서 관리 작업을 누를 수도 있습니다.

   보안 장치에 비밀번호가 없으면 새 비밀번호를 입력하라는 프롬프트가 표시됩니다.
4. 요청을 눌러 인증서 요청 마법사를 엽니다.
5. "인증서를 수동으로 요청"을 선택하고 다음을 누릅니다.

6. 요청된 정보를 입력합니다.

   서버 이름. (선택 사항) 인증서를 요청하는 시스템의 전체 호스트 이름을 입력합니다.

   조직. (선택 사항) 조직의 이름을 입력합니다.

   조직 구성 단위. (선택 사항) 부서 또는 기타 조직 구성 단위를 입력합니다.

   구/군/시. (선택 사항) 조직 구성 단위가 위치한 구, 군, 시를 입력합니다.

   시/도. (선택 사항) 조직 구성 단위가 위치한 시 또는 도를 입력합니다.

   국가/지역. (선택 사항) 드롭다운 메뉴에서 조직 구성 단위가 위치한 국가 또는 지역을 선택합니다.

   다음 두 버튼을 사용하여 요청 양식의 두 가지 뷰 간을 전환할 수 있습니다.

   DN 표시. 요청자 정보를 고유 이름(DN) 형식으로 표시하려면 이 버튼을 누릅니다. 이 버튼은 필드에 정보를 입력하고 있을 때만 볼 수 있습니다.

   필드 표시. 요청자 정보를 필드에 표시하려면 이 버튼을 누릅니다. 이 버튼은 DN 형식으로 정보를 입력하고 있을 때만 볼 수 있습니다.

7. 다음을 누릅니다.

8. 이 인증서를 저장할 보안 장치의 비밀번호를 입력합니다.

   내부(소프트웨어) 보안 장치를 사용하는 경우에는 키 및 인증서 데이터베이스의 비밀번호입니다. 외부(하드웨어) 모듈을 사용하는 경우에는 스마트 카드 또는 기타 보안 장치의 비밀번호입니다.

9. 다음을 누릅니다.

10. 다음 중 하나를 선택합니다.

    클립보드로 복사. 인증서 요청을 클립보드에 복사하려면 이 버튼을 누릅니다.

    파일에 저장. 인증서 요청을 텍스트 파일로 저장하려면 이 버튼을 누릅니다. 파일 이름과 위치를 선택하라는 프롬프트가 표시됩니다.

11. 완료를 눌러 인증서 요청 마법사를 닫습니다.

단계 B. 서버 인증서 요청 보내기

서버 인증서 요청을 생성한 다음에는 CA에 보내야 합니다. 많은 CA의 경우 웹 사이트를 통해 인증서 요청을 제출할 수 있지만 요청을 전자 메일로 보내야 할 경우도 있습니다.

1. 전자 메일 프로그램을 사용하여 새 전자 메일 메시지를 작성합니다.
2. 인증서 요청을 메시지에 붙여 넣습니다.

   인증서 요청을 파일에 저장한 경우에는 텍스트 편집기에서 파일을 엽니다. 요청을 복사하여 메시지 본문에 붙여 넣습니다.

   인증서 요청을 클립보드에 복사한 경우에는 그대로 메시지 본문에 붙여 넣습니다.
3. 요청의 제목과 받는 사람을 입력합니다. 제목과 받는 사람의 유형은 사용하는 CA에 따라 다릅니다. 자세한 정보는 CA 웹 사이트를 참조하십시오.
4. 전자 메일 메시지를 CA에 보냅니다.

인증서 요청을 제출한 다음에는 CA에서 인증서를 보낼 때까지 기다려야 합니다. 인증서를 받기까지 걸리는 시간은 CA에 따라 크게 차이가 납니다. 회사 내부에 CA가 있는 경우에는 하루나 이틀만에 인증서를 받을 수 있지만 외부 CA인 경우에는 몇 주씩 걸릴 수도 있습니다.

단계 C. 인증서 설치

CA에 따라 전자 메일 메시지로 인증서를 받을 수도 있고 CA 웹 사이트를 통해 발급받을 수도 있습니다. 일단 인증서를 받으면 백업을 하고 나서 설치합니다.

1. CA에서 받은 인증서 데이터를 텍스트 파일에 저장합니다.

   인증서 데이터가 없어질 경우에는 이 백업 파일을 사용하여 인증서를 다시 설치할 수 있습니다.
2. Sun ONE Directory Proxy Server 탐색 트리에서 인증서를 설치하려는 서버 인스턴스를 선택합니다.
3. 열기를 눌러 서버 인스턴스의 관리 창을 엽니다.
4. 작업 탭에서 인증서 관리 버튼을 누릅니다.

   콘솔 메뉴를 열고 보안 > 인증서 관리를 선택할 수도 있습니다.

5. 서버 인증서 탭을 누릅니다.
6. 이 인증서를 저장할 위치를 지정합니다.
   - 이 인증서를 내부 보안 장치에 저장하려면 보안 장치 드롭다운 목록에서 내부(소프트웨어) 장치를 선택한 다음 설치를 누릅니다.
   - 이 인증서를 외부 하드웨어 장치에 저장하려면 보안 장치 드롭다운 목록에서 해당 장치를 선택한 다음 설치를 누릅니다.
7. 인증서의 위치를 입력하거나 해당 텍스트를 입력합니다.

   다음 로컬 파일. 인증서가 시스템에 텍스트 파일로 저장되어 있으면 해당 파일의 전체 경로를 입력합니다.

   다음 인코딩된 텍스트 블록. 인증서를 클립보드에 복사한 경우에는 붙여넣기 버튼을 눌러 텍스트 필드에 붙여 넣습니다.
8. 다음을 누릅니다.

   위에 입력한 인증서 정보가 유효하면 인증서 정보가 포함된 페이지가 나타납니다.
9. 인증서 정보가 맞는지 확인한 후 다음을 누릅니다.
10. 인증서 이름을 입력하고 다음을 누릅니다.
11. 이 인증서를 저장할 보안 장치의 비밀번호를 입력합니다.

    내부(소프트웨어) 보안 장치에 인증서를 설치하는 경우에는 키 및 인증서 데이터베이스의 비밀번호를 입력하고 외부(하드웨어) 보안 장치에 설치하는 경우에는 해당 장치의 비밀번호를 입력합니다.
12. 완료를 누릅니다.

단계 D. CA 인증서 또는 서버 인증서 체인 설치

1. CA로부터 CA 인증서나 서버 인증서 체인을 발급받습니다.
2. Sun ONE Directory Proxy Server 탐색 트리에서 CA 인증서를 설치하려는 서버 인스턴스를 선택합니다.
3. 열기를 눌러 서버 인스턴스의 관리 창을 엽니다.
4. 작업 탭에서 인증서 관리 버튼을 누릅니다.

   콘솔 메뉴를 열고 보안 > 인증서 관리를 선택할 수도 있습니다.

5. CA 인증서 탭을 선택한 다음 설치를 누릅니다.
6. 인증서의 위치를 입력하거나 해당 텍스트를 입력합니다.

   다음 로컬 파일. 인증서가 시스템에 텍스트 파일로 저장되어 있으면 해당 파일의 전체 경로를 입력합니다.

   다음 인코딩된 텍스트 블록. 인증서를 클립보드에 복사한 경우에는 붙여넣기 버튼을 눌러 텍스트 필드에 붙여 넣습니다.
7. 다음을 누릅니다.

   위에 입력한 인증서 정보가 맞으면 인증서 정보가 포함된 페이지가 나타납니다.
8. 인증서의 정보가 맞는지 확인한 후 다음을 누릅니다.
9. 인증서 이름을 입력하고 다음을 누릅니다.
10. 이 인증서의 신뢰 옵션을 선택합니다.

    클라이언트의 연결 허용. 이 CA에서 발급한 클라이언트 인증서를 신뢰하려면 이 확인란을 선택합니다.

    다른 서버에 연결. 이 CA에서 발급한 서버 인증서를 신뢰하려면 이 확인란을 선택합니다.
11. 완료를 누릅니다.

단계 E. 인증서 데이터베이스 백업 및 복원

인증서를 설치할 때마다 인증서 데이터베이스를 백업해야 합니다. 데이터베이스가 손상될 경우 이 백업으로부터 인증서 정보를 복원할 수 있습니다.

인증서 데이터베이스를 백업하는 방법

1. 서버 루트 폴더를 엽니다.
2. `alias` 폴더에 있는 모든 파일을 다른 위치(가능하면 다른 디스크)에 복사합니다.

   이 폴더에는 인증서뿐 아니라 트러스트 데이터베이스의 개인 키가 포함되어 있습니다.

백업으로부터 인증서 데이터베이스를 복원하는 방법

- 백업 파일을 서버 루트 폴더의 `alias` 하위 폴더에 복사합니다.

주의 백업으로부터 인증서 데이터베이스를 복원하면 백업을 만든 후에 설치한 인증서는 손실됩니다. 인증서 데이터베이스를 복원하기 전에 나중에 다시 설치할 경우를 대비하여 모든 인증서를 복사해 놓으십시오.

단계 2. Directory Proxy Server와 클라이언트 간의 SSL 연결 설정

Directory Proxy Server와 LDAP 클라이언트 간에 SSL 연결을 설정하려면 다음 단계를 수행합니다.

- 단계 A. Directory Proxy Server CA 인증서를 클라이언트의 트러스트 데이터베이스에 추가
- 단계 B. Directory Proxy Server 시스템 구성 변경
- 단계 C. Directory Proxy Server 네트워크 그룹 변경

단계 A. Directory Proxy Server CA 인증서를 클라이언트의 트러스트 데이터베이스에 추가

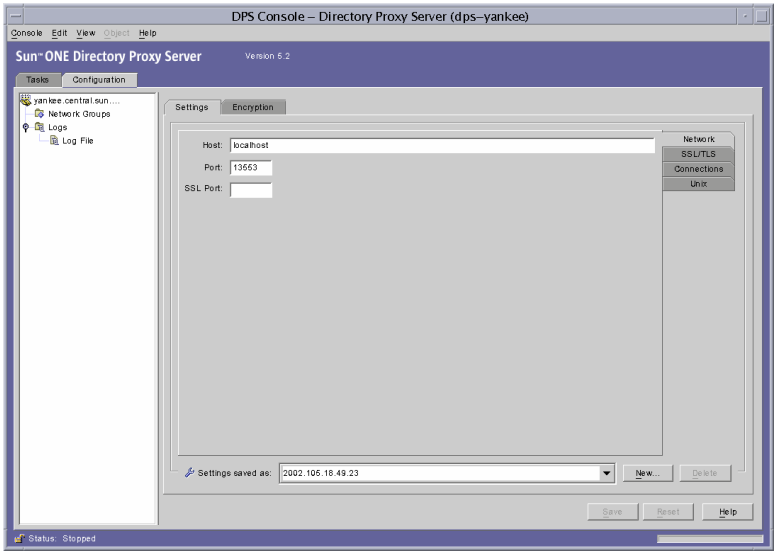
주 이 단계는 클라이언트가 서버 인증서를 확인하는 경우에만 필요합니다. 모든 Netscape 및 Sun 클라이언트는 확인 작업을 수행합니다. 그러나 확인을 수행하지 않는 클라이언트도 있습니다. 이 경우에는 트러스트 설정이 필요하지 않습니다.

Directory Proxy Server가 LDAP 클라이언트에게 인증서를 제공하면 클라이언트에서는 인증서의 유효성 여부를 확인합니다. 이 확인 과정의 일부로서 클라이언트는 인증서를 발급한 CA를 신뢰할 수 있는지 여부를 확인합니다. 이러한 이유 때문에 Directory Proxy Server의 서버 인증서를 발급한 CA의 루트 인증서가 클라이언트의 트러스트 데이터베이스에 설치되어 있어야 합니다.

Directory Proxy Server의 서버 인증서를 설치하는 마지막 단계에서 Directory Proxy Server의 CA 인증서를 텍스트 파일에 복사했습니다. 각 클라이언트 응용 프로그램의 설명서에 따라 CA 인증서를 해당 트러스트 데이터베이스에 설치하십시오.

단계 B. Directory Proxy Server 시스템 구성 변경

Directory Proxy Server 콘솔 창의 설정 탭과 암호화 탭을 사용하여 Directory Proxy Server를 위한 SSL 사용 통신 기준을 정의할 수 있습니다. 자세한 내용은 65페이지의 “시스템 구성 인스턴스 만들기”를 참조하십시오.



해당 시스템 구성 인스턴스에 대해 다음 사항을 변경하고 변경 사항을 저장합니다.

- 설정 탭에서 "SSL 포트" 필드에 값을 지정합니다. Directory Proxy Server는 LDAPS (LDAP over SSL) 연결용으로 지정된 포트 번호를 통해 연결을 수신합니다. 기본적으로 Directory Proxy Server는 LDAPS 클라이언트로부터 연결을 수신하지 않습니다. 대체 포트 636을 사용하여 TLS/SSL을 설정하는 클라이언트로부터 LDAPS 연결을 수신하려면 이 값을 반드시 입력해야 합니다. 이 값은 포트 필드의 값과 달라야 합니다. 또한 이 옵션을 사용하려면 암호화 탭에 TLS/SSL 구성이 있어야 합니다.

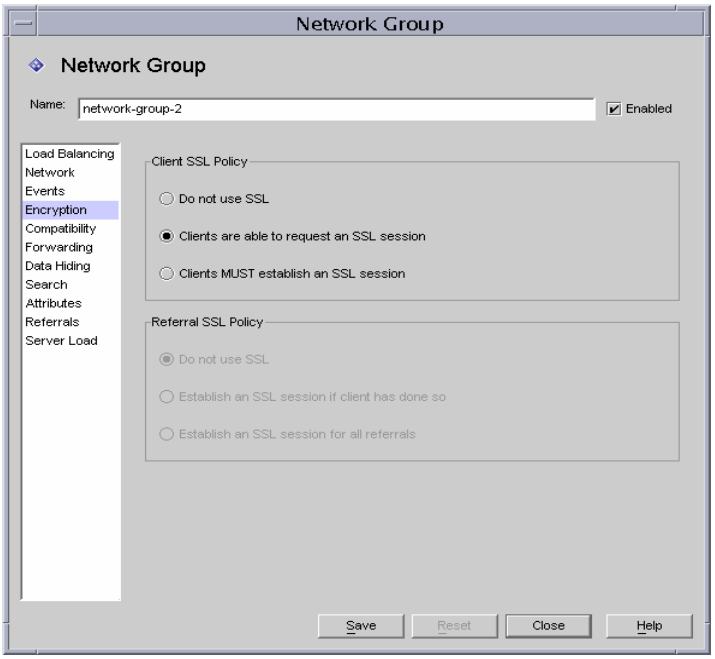
  매개 변수에 대한 설명을 보려면 도움말 버튼을 누르십시오.

- SSL/TLS 암호화 탭에서 필요한 정보를 모두 지정합니다.

  매개 변수에 대한 설명을 보려면 도움말 버튼을 누르십시오.

단계 C. Directory Proxy Server 네트워크 그룹 변경

Directory Proxy Server는 네트워크 그룹을 사용하여 클라이언트를 식별하고 LDAP 디렉토리에 포함된 정보에 대한 액세스 권한을 결정합니다. 자세한 내용은 6장, “그룹 만들기 및 관리“를 참조하십시오.



구성한 각 그룹에 대해 암호화 탭에서 해당 옵션을 설정하여 클라이언트가 LDAP 작업을 보내기 전에 TLS 세션을 시작하도록 할 것인지, 클라이언트가 자체적으로 결정하도록 할 것인지 또는 클라이언트가 TLS 세션을 시작하지 못하도록 할 것인지 여부를 지정합니다. 예를 들어, "SSL 사용 가능" 옵션과 "클라이언트가 SSL 세션을 설정해야 함" 옵션을 선택할 수 있습니다. 암호화 탭의 옵션에 대한 자세한 내용은 6장, “그룹 만들기 및 관리“의 85페이지에서 단계 9를 참조하십시오.

참조 따라가기가 사용 가능하면 참조 SSL 정책을 선택해야 합니다. 참조 따라가기는 창의 왼쪽에 있는 목록에서 참조를 선택하면 사용 가능해집니다.

Directory Proxy Server는 백엔드 서버에 의해 반환된 참조를 따라갑니다. LDAP URL의 반환된 참조는 RFC 2255 형식이어야 합니다. 호스트 포트가 지정되지 않은 경우에는 클라이언트가 연결할 LDAP 서버에 대해 어느 정도 알고 있어야 합니다.

Directory Proxy Server는 호스트나 포트 번호가 없는 LDAP URL을 참조를 보낸 호스트에 대한 참조로 해석합니다. 예를 들면 다음과 같습니다.

`ldap:///dc=central,dc=sun,dc=com`	동일 호스트에 대한 참조, 기반이 다른 포트.
`ldap://:10389/`	동일한 호스트에 대한 참조, 다른 포트.
`ldap://host/`	기본 포트 389에서 "host" 호스트에 대한 참조.

단계 3. Directory Proxy Server와 LDAP 서버 간의 SSL 연결 설정

Directory Proxy Server와 LDAP 서버 간에 SSL 연결을 설정하려면 다음 단계를 수행합니다.

- 단계 A. CA 인증서 또는 서버 인증서 체인 설치
- 단계 B. Directory Proxy Server CA 인증서를 LDAP 서버의 트러스트 데이터베이스에 추가
- 단계 C. LDAP 서버 등록 정보 변경

단계 A. CA 인증서 또는 서버 인증서 체인 설치

이 단계는 Directory Proxy Server가 LDAP 서버에서 제공한 인증서를 확인하도록 할 때 필요합니다. 자세한 내용은 164페이지의 “단계 D. CA 인증서 또는 서버 인증서 체인 설치”를 참조하십시오.

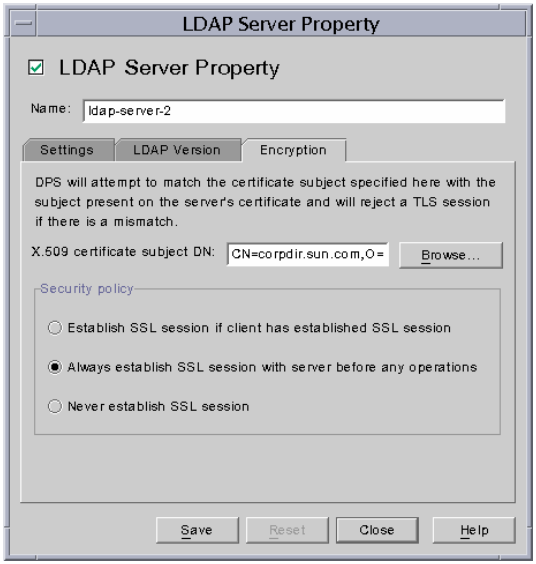
단계 B. Directory Proxy Server CA 인증서를 LDAP 서버의 트러스트 데이터베이스에 추가

Directory Proxy Server가 LDAP 서버에 인증서를 제공하면 서버에서는 인증서의 유효성 여부를 확인합니다. 이 확인 과정의 일부로서 서버는 Directory Proxy Server의 인증서를 발급한 CA를 신뢰할 수 있는지 확인합니다. 이러한 이유 때문에 Directory Proxy Server의 서버 인증서를 발급한 CA의 루트 인증서가 LDAP 서버의 트러스트 데이터베이스에 설치되어 있어야 합니다.

Directory Proxy Server의 서버 인증서를 설치하는 마지막 단계에서 Directory Proxy Server의 CA 인증서를 텍스트 파일에 복사했습니다. 각 LDAP 서버의 설명서에 따라 CA 인증서를 해당 트러스트 데이터베이스에 설치하십시오. Sun ONE Directory Server를 사용하는 경우에는 인증서 관리 마법사를 사용하여 CA 인증서를 Directory Server의 트러스트 데이터베이스에 추가할 수 있습니다. 인증서 관리 마법사는 Directory Server Console의 작업 탭에서 시작할 수 있습니다.

단계 C. LDAP 서버 등록 정보 변경

LDAP 서버 등록 정보 창의 암호화 탭을 사용하여 각 LDAP 서버의 SSL 사용 통신 기준을 정의할 수 있습니다. 자세한 내용은 116페이지의 “LDAP 서버 등록 정보 객체 만들기”를 참조하십시오.



해당 LDAP 서버 등록 정보 객체에 대해 다음 사항을 변경하고 변경 사항을 저장합니다.

- "보안 정책" 옵션을 적절한 값으로 설정하여 Directory Proxy Server가 항상 백엔드 서버에 대해 SSL/TLS를 설정하도록 할 것인지, 백엔드 서버에 TLS/SSL을 설정하지 않도록 할 것인지, 또는 클라이언트가 Directory Proxy Server에 대해 SSL/TLS를 설정할 경우에만 백엔드 서버에 대해 SSL/TLS를 설정할 것인지 등을 지정합니다.

- "X.509 인증서 주체 DN" 필드를 LDAP 서버 인증서의 주체 이름(X.509 인증서의 주체 속성)으로 설정합니다. Directory Proxy Server는 지정된 인증서 주체가 LDAP 서버 인증서 주체와 일치하는지 확인한 후 일치하지 않으면 TLS 세션을 거부합니다. Directory Proxy Server는 이 속성을 사용하여 연결하고 있는 LDAP 서버를 인증할 수 있습니다. 이 속성이 설정되지 않은 경우 Directory Proxy Server는 모든 이름을 허용합니다.

부록

부록 A

Directory Proxy Server 결정 기능

이 부록에서는 Directory Proxy Server의 일부 특정 기능에 대한 제어 흐름을 설명합니다. 이 부록은 다음 내용으로 구성되어 있습니다.

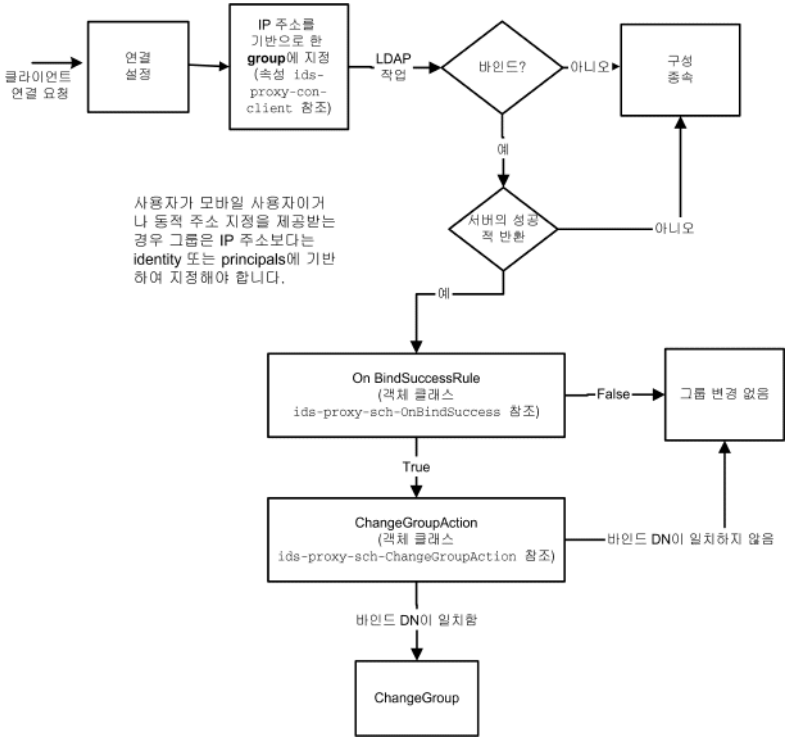
연결에 대한 그룹 설정

클라이언트가 Directory Proxy Server에 연결할 때 일치 항목을 찾을 때까지 `ids-proxy-sch-NetworkGroup` 객체 항목에서 `ids-proxy-con-Client` 속성을 검사합니다. `ids-proxy-sch-NetworkGroup` 객체는 `ids-proxy-con-priority` 속성에 정의된 우선 순위가 가장 높은 객체부터 우선 순위가 가장 낮은 객체까지 순서대로 검색됩니다. Directory Proxy Server는 `ids-proxy-con-client` 속성이 클라이언트의 IP 주소와 일치하는 첫 번째 그룹에 클라이언트를 넣습니다. 일치하는 그룹이 없는 경우 연결이 닫힙니다.

바인드할 때 그룹 변경

클라이언트는 처음에 연결될 때 IP 주소를 기반으로 그룹에 배치됩니다. 디렉토리에 바인드될 때 다른 액세스 제어를 사용하여 클라이언트를 다른 그룹으로 이동할 수 있습니다. 그렇게 하려면 초기 그룹 객체에 성공적인 바인드 작업을 평가하는 규칙 객체가 포함되어 있어야 합니다. 규칙에서 TRUE로 평가되면 그룹 변경 작업을 수행하여 클라이언트를 다른 위치로 이동합니다. 그림 11-3에 이 기능이 설명되어 있습니다.

그림 11-3 바인드할 때 그룹 변경



바인드할 때 그룹 변경 구성

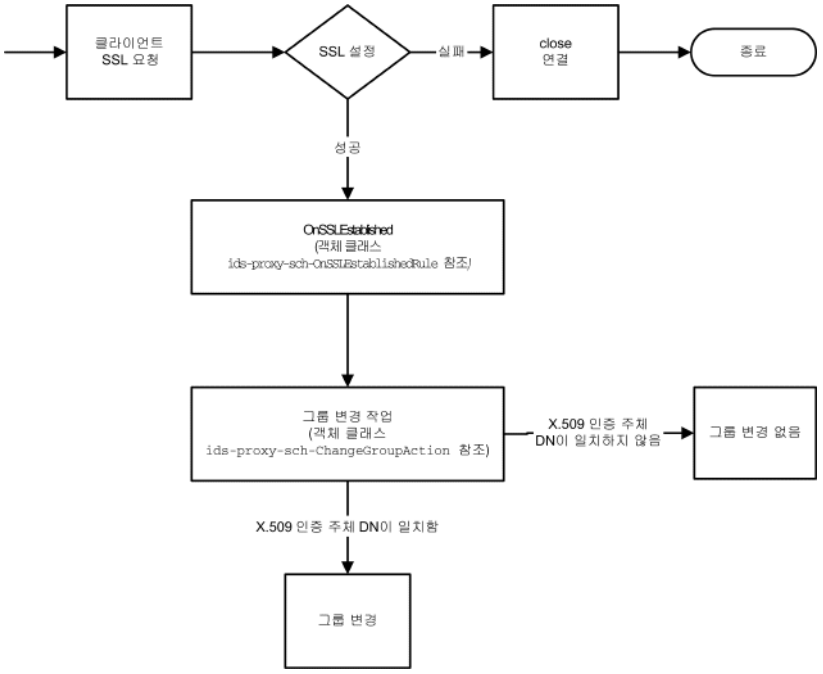
다음 단계에서는 단순 바인드 인증 메커니즘을 사용하여 "cn=Directory Manager"에 성공적으로 바인드될 때 그룹을 변경하도록 Directory Proxy Server를 구성하는 방법을 설명합니다.

1. 성공적으로 바인드될 경우 사용자 cn="Directory Manager"가 이동할 새 네트워크 그룹을 만듭니다. 보다 자세한 내용은 80페이지의 “그룹 만들기”를 참조하십시오. 그룹을 변경하여 사용자가 이 그룹에만 속할 수 있는 경우 네트워크 그룹 패널의 네트워크 탭에서 "IP 바인드 없음"을 설정합니다. 또한, 이 그룹이 일부 IP 바인딩이 허용되는 모든 다른 네트워크 그룹의 뒤에 오게 해야 합니다.
2. 새 "그룹 변경" 작업 만들기. 보다 자세한 내용은 140페이지의 “작업 객체 만들기”를 참조하십시오. 설정이 단계 1에서 만든 그룹 이름으로 변경됩니다. "if DN matches"를 "cn=Directory Manager"로 설정합니다. 또한, 모든 다른 그룹(예: ".*")에 대해 "없음"(그룹 변경 안 함)을 설정할 수 있습니다.
3. 바인드 이벤트 만들기. 보다 자세한 내용은 132페이지의 “OnBindSuccess 이벤트 객체 만들기”를 참조하십시오. 작업 탭에서 작업을 단계 2에서 만든 그룹 변경 작업으로 설정합니다. 조건 탭에서 "비밀번호 기반 바인드"를 선택합니다.
4. 단계 1에서 만든 네트워크 그룹에 있는 이벤트 탭의 단계 3에서 만든 바인드 이벤트를 선택합니다. 보다 자세한 내용은 103페이지의 “그룹 수정”을 참조하십시오.

TLS를 설정할 때 그룹 변경

TLS 설정 시 그룹을 변경하는 방법은 바인드 메커니즘에서 그룹을 변경하는 방법과 비슷하지만 TLS 세션이 성공적으로 구성될 경우 클라이언트가 그룹을 변경할 수 있습니다. 클라이언트가 TLS를 구성하면 그룹 변경 작업이 수행되기 이전에 SSL 확립 규칙이 평가됩니다. 이 기능은 그림 11-4에 설명되어 있습니다.

그림 11-4 TLS를 설정할 때 그룹 변경



고가용성 설정

여러 백엔드 디렉토리 서버를 구성한 경우 각 서버로 로드 균형을 조정하여 백엔드 서버 중 하나가 종료될 경우 다른 서버로 페일오버하도록 Directory Proxy Server를 설정할 수 있습니다. 그렇게 하려면 로드 균형 등록 정보(121페이지의 "로드 균형 조정 등록 정보" 참조)를 만들어 로드 균형을 조정할 그룹 객체에 포함시켜야 합니다. 또한 각 백엔드 서버에 대한 LDAP 서버 등록 정보(116페이지의 "LDAP 서버 등록 정보" 참조)를 만들어 로드 균형 등록 정보에 포함시켜야 합니다. 각 백엔드 서버가 로드 균형 등록 정보 객체에서 처리해야 하는 로드량을 총 로드에 대한 비율로 지정해야 합니다. 이 설정을 사용하여 Directory Proxy Server는 백엔드 서버 중 하나가 종료될 경우 각 백엔드 서버로 로드를 다시 배포합니다. 첫 번째 백엔드 서버가 종료할 경우 클라이언트를 다른 서버에 페일오버합니다. Directory Proxy Server는 LDAP 서버와의 네트워크 연결이 끊어지거나 LDAP 서버가 응답하지 않는 경우에도 페일오버됩니다.

주 클라이언트가 SASL 메커니즘을 사용하여 바운드된 경우에는 Directory Proxy Server가 페일오버될 수 없습니다.

참조

LDAPv2 클라이언트에 대한 참조를 따르도록 Directory Proxy Server를 설정할 수 있습니다. 백엔드 LDAP 디렉토리 서버는 참조를 보낼 수 있어야 합니다. 즉, LDAP v3 표준을 지원해야 합니다. Directory Proxy Server가 디렉토리 서버로부터 참조를 받도록 하려면 Directory Proxy Server와 백엔드 LDAP 서버 사이에서 LDAP v3을 사용하도록 구성합니다. 그런 다음 그룹 참조와 연속 참조 정책을 설정합니다.

Directory Proxy Server FAQ, 기능 및 문제 해결

이 부록에는 Sun ONE Directory Proxy Server에 관한 유용한 정보가 포함되어 있습니다. 이 부록에는 자주 묻는 질문(FAQ)에 대한 대답, 특정 Directory Proxy Server 기능 설명 및 문제 해결 정보가 포함되어 있습니다.

부록은 다음 내용으로 구성되어 있습니다.

Directory Proxy Server FAQ

Directory Proxy Server란 무엇입니까?

Directory Proxy Server는 LDAP 클라이언트 및 LDAP 서버를 위한 LDAP 프록시입니다. LDAP 클라이언트의 요청을 Directory Proxy Server 구성에 정의된 규칙에 따라 LDAP 서버에 전달합니다. 그런 다음 서버의 결과를 해당 규칙에 따라 클라이언트에게 다시 전달합니다. 이 프로세스는 클라이언트에 대해 완전히 투명하므로 클라이언트가 LDAP 서버에 연결하기만 하면 Directory Proxy Server에 연결됩니다.

LDAP Proxy Server가 필요한 이유는 무엇입니까?

많은 기업에서는 디렉토리 정보의 일부에 대해서는 내부적으로 보안을 유지하면서 일부만 외부에 공개하기를 원합니다. Directory Proxy Server를 사용하면 외부 클라이언트에 디렉토리 비밀번호를 할당하지 않고도 이러한 목표를 쉽게 달성할 수 있습니다. 로드 균형 조정 및 페일오버 기능을 통해 Directory Proxy Server를 엔터프라이즈 디렉토리 서비스에 대한 고가용성 솔루션으로 사용할 수도 있습니다.

또한 서비스 공격(DoS) 거부 방지, 검색 제한 등과 같은 추가 보안 기능을 제공합니다.

Directory Proxy Server에서 지원하는 LDAP 프로토콜 버전은 무엇입니까?

Directory Proxy Server는 LDAPv2 또는 LDAPv3 프로토콜을 지원하는 LDAP 클라이언트 또는 체인 LDAP 서버를 지원합니다.

Directory Proxy Server는 보안 인증과 암호화를 지원합니까?

Directory Proxy Server는 인증서를 통한 공개 키 기반 데이터 암호화를 위한 SSLv3 서비스를 지원합니다. LDAP 클라이언트에 사용할 수 있는 보안 인증 및 암호화에서는 Diffie-Hellman, DSA (Digital Signature Standard) 및 Triple-DES 알고리즘을 사용하는 LDAP 포트 또는 인터넷 TLS (Transport Layer Security) 모델을 사용합니다.

Directory Proxy Server는 LDAP 사용 디렉토리 서버에서 작동합니까?

Directory Proxy Server는 LDAP 호환 디렉토리 서버에서 작동합니다. 일부 디렉토리 제품 공급업체에서 자사 마케팅 환경에 맞게 LDAP를 구현해 달라고 요구하지만 실제로는 그렇지를 못합니다. Directory Proxy Server는 Sun ONE Directory Server에서 철저하게 테스트를 거쳤습니다.

Directory Proxy Server 5.0 Console을 사용할 경우 지원되는 구성 디포지토리는 Sun ONE Directory Server 5.0입니다.

Directory Proxy Server를 구성할 수 있는 구성 유틸리티가 있습니까?

Directory Proxy Server 5.0에는 Directory Proxy Server를 구성하는 데 사용할 수 있는 Java 기반 GUI (콘솔)가 포함되어 있습니다. 콘솔은 Sun ONE Directory Server를 사용하여 생성된 구성을 저장합니다.

Directory Proxy Server 기능

Directory Proxy Server를 사용하여 서비스 거부(DoS) 공격을 방지할 수 있습니까?

그렇습니다. 연결 당 처리되는 동시 작업 수, 연결 당 허용되는 작업 수, 총 동시 연결 수, 정의된 그룹(네트워크, 하위 네트워크 또는 바인드 DN 기반) 당 최대 동시 연결 수, 단일 IP 주소에 대한 최대 동시 연결 수 등을 제한할 수 있습니다.

Directory Proxy Server는 "역방향" 프록싱을 지원합니까?

엄격한 의미에서 Directory Proxy Server는 역방향 프록시이지만 LDAP 프로토콜은 역방향 프록싱 개념을 지원하지 않습니다.

Directory Proxy Server를 사용하여 LDAP 디렉토리의 "트롤링"을 방지할 수 있습니까?

그렇습니다. 트롤링은 디렉토리의 많은 부분을 다운로드하도록 설계된 매우 광범위한 쿼리이며, 많은 사이트에서는 금지하는 기능입니다. Directory Proxy Server는 다음과 같은 여러 방법으로 트롤링을 금지하거나 제한합니다.

- 검색 범위를 디렉토리 트리의 단일 수준으로 제한하고, 전체 하위 트리를 숨기고, 쿼리에 대한 응답으로 반환되는 항목 수에 대한 하드 한계를 설정할 수 있습니다.
- 부등호 검색을 금지하여 길이를 제한할 수 있는 제외 및 하위 문자열 검색을 기반으로 많은 결과를 반환하는 검색을 허용하지 않습니다(예: 성이 문자 A-Z로 시작하는 모든 항목에 대한 검색 금지).
- 또한 색인화되지 않은 검색을 거부하도록 Directory Proxy Server를 구성할 수 있습니다. 색인화되지 않은 검색은 비효율적이며 성능에 부정적인 영향을 미칠 수 있습니다.

Directory Proxy Server는 쿼리에 대한 자동 로드 균형 조정을 수행합니까?

Directory Proxy Server는 백엔드 LDAP 서버 간의 자동 서버 로드 균형 조정을 지원합니다. 또한 Directory Proxy Server는 주 LDAP 서버가 종료될 경우 보조 LDAP 서버에 자동 페일오버를 지원합니다.

Directory Proxy Server 서버 한 대가 로드 균형 조정할 수 있는 LDAP 서버 수는 얼마입니까?

디렉토리 서버의 성능 요구 사항 및 Directory Proxy Server에서 수행되는 작업의 복잡도에 따라 Directory Proxy Server가 로드 균형 조정해야 하는 최적의 디렉토리 서버 수가 결정됩니다. 예를 들어, Directory Proxy Server에서 속성 이름 바꾸기와 같은 복잡한 작업을 수행할 경우에는 Directory Proxy Server에서 로드 균형을 조정하도록 구성되는 디렉토리 서버 수를 줄여야 합니다. 이 경우 Directory Proxy Server 장치를 더 추가하여 복잡한 Directory Proxy Server 구성으로 인한 성능의 효과를 보완하는 것이 좋습니다.

검색 요청을 필터링할 수 있습니까?

그렇습니다. 특정 속성을 찾으려고 시도하는 검색을 거부하도록 Directory Proxy Server를 구성할 수 있습니다. 또한 수신하는 검색 요청을 지정된 최소 검색 기준, 검색 범위 및 시간 제한에 맞게 수정하도록 Directory Proxy Server를 구성할 수 있습니다.

검색 결과를 필터링할 수 있습니까?

그렇습니다. 반환되는 항목 수 및 결과 집합에 포함되는 속성을 조건으로 결과를 필터링할 수 있습니다. 항목 DN 또는 내용을 기반으로 검색 결과 항목을 필터링할 수도 있습니다.

정의된 그룹에 액세스하는 방법은 무엇입니까?

클라이언트는 클라이언트의 네트워크 주소에 따라 디렉토리에 다양한 수준으로 액세스할 수 있습니다. 따라서, 회사 방화벽 외부, 방화벽 내부, 실무용 하위 네트워크, 개인 시스템 등에 위치하는 각 클라이언트에게 서로 다른 수준의 액세스를 허용할 수 있습니다. 또한 클라이언트가 LDAP 바인드 작업을 성공적으로 완료했을 때, SSL 세션이 구성될 때 등에 대한 액세스 수준을 변경할 수 있습니다.

Directory Proxy Server는 보호된 비밀번호 인증을 지원합니까?

그렇습니다. SASL 메커니즘을 사용하여 다양한 보호된 비밀번호 인증 스키마를 구현할 수 있습니다. 이러한 메커니즘은 백엔드 디렉토리 서버에서 지원해야 합니다. Directory Proxy Server는 연결 보호 및 SASL EXTERNAL 메커니즘과 함께 SASL 메커니즘을 지원하지 않습니다.

Directory Proxy Server는 참조를 자동으로 따릅니까?

액세스 그룹을 기반으로 다음과 같은 참조를 구성할 수 있습니다. 자동으로 참조를 따르거나, 참조를 반환하거나, 참조를 무시하도록 다양한 액세스 그룹을 구성할 수 있습니다.

Directory Proxy Server는 검색 결과 정보를 캐싱합니까?

Directory Proxy Server 버전 5.0 SP1는 검색 결과 캐싱을 지원하지 않습니다.

Directory Proxy Server에서 속성 이름 바꾸기를 수행할 수 있습니까?

Directory Proxy Server는 클라이언트와 서버 사이에서 속성 이름을 투명하게 바꿀 수 있습니다.

문제 해결

연결 시도 로그를 분석하는 방법은 무엇입니까?

`syslog`를 사용하거나 지정된 로그 파일에 기록하도록 Directory Proxy Server를 구성할 수 있습니다. Stanford University의 ftp(`ftp://ftp.stanford.edu/general/security-tools/swatch`)에서 swatch라는 잘 알려진 UNIX 유틸리티를 다운로드하여 사용할 수 있습니다. Swatch를 사용하면 Directory Proxy Server에서 생성된 로그 파일을 모니터링하고 거부된 이벤트가 발생할 경우 관리자에게 알릴 수 있습니다.

참조를 따르도록 Directory Proxy Server를 구성했지만, LDAPv2 클라이언트에서 검색을 수행하면 오류 32(No such object) 또는 일부 다른 오류가 표시됩니다.

Directory Proxy Server는 백엔드 서버로부터 참조를 받으려면 LDAPv3을 사용해야 합니다. 각 LDAP 서버 등록 정보에서 "LDAP 버전 3 전용"을 선택했는지 확인하십시오.

로그 파일에 모든 백엔드 서버가 실행 중인 동안에도 일부 유휴 클라이언트 연결이 실패한다는 메시지가 있습니다.

백엔드 디렉토리 서버가 유휴 연결에 시간 초과를 적용하여 닫습니다. 이러한 닫힌 연결에 대해서는 Directory Proxy Server가 실패합니다. Directory Proxy Server에 대해서도 유휴 연결 시간 초과를 설정해야 합니다. 그렇게 하면 유휴 및 누출 클라이언트 연결이 정리되고 단일 형식 서비스 거부(DoS) 공격으로부터 보호됩니다.

존재하는 필터를 포함하는 검색 요청을 제한하는 방법이 있습니까?

Directory Proxy Server 버전 5.0 SP1에는 클라이언트가 존재하는 필터를 사용하지 못하도록 제한하는 직접 메커니즘이 없습니다. 이 문제를 해결하는 두 가지 간접 방식이 있습니다.

`ids-proxy-con-forbidden-compare`를 비교하지 않을 속성의 이름으로 설정할 수 있습니다. 이 방법은 지나치게 제한적이라서 (mail=*) 필터와 (mail=Andy*) 필터를 모두 포함하는 검색을 거부하게 됩니다.

또한 존재하는 필터(attrName=*)가 항상 동일한 결과(데이터가 변경되지 않는다고 가정)를 생성하기 때문에 ids-proxy-con-size-limit 속성과 `ids-proxy-sch-SizeLimitProperty`를 사용하여 피해를 제한할 수 있습니다. LDAP는 항목을 지정된 순서로 반환할 필요는 없지만, 대부분(모든) 구현에서 결과 집합은 항상 정렬된 순서 또는 정렬되지 않은 순서로 반환됩니다. 따라서, 크기 제한(크기 제한 속성 또는 SizeLimitProperty 사용)을 사용하여 Directory Proxy Server를 구성할 경우 항상 해당 집합 중 처음 'n'개만 반환됩니다. 이러한 'n'개 항목 집합이 두 개만 존재할 수 있기 때문에 디렉토리 트롤링 위험이 크게 감소됩니다.

Directory Proxy Server는 가능할 경우 요청 자체에 이 크기 제한을 설정하려고 시도하기 때문에 디렉토리 서버에는 모든 항목을 보내야 하는 부담이 없습니다.

크기 제한 등록 정보에는 필요할 경우 크기 제한에 예외를 적용할 수 있는 옵션이 있습니다. 예를 들어, o=A이라는 항목이 있고 그 아래에 400개의 조직 단위가 있다고 가정합니다. 각각의 'U' 아래에는 사용자가 있습니다. 클라이언트가 모든 'U'를 볼 수 있지만 한 번에 5명의 사용자만 볼 수 있게 하려면 기준 o=A 및 한 수준 범위 검색에는 제한을 적용하지 않도록 `SizeLimitProperty`를 설정할 수 있습니다. 모든 다른 검색에 대해서는 제한값 5를 적용합니다.

작업을 실행하거나 일부 콘솔 기능을 수행하면 Administration Server가 제대로 실행되고 있고 이 호스트가 Administration Server에 대한 연결 권한이 있는지 확인하라는 오류 메시지가 표시됩니다.

해당 콘솔이 오류 메시지를 생성한 Directory Proxy Server를 관리하는 Administration Server에 로그인합니다. Administration Server의 호스트 시스템에서 Sun ONE Console을 시작해야 할 수 있습니다. 작업을 호출하지 못한 Directory Proxy Server를 관리하는 Administration Server의 서버 콘솔을 엽니다. 구성 탭을 누른 다음 네트워크 탭을 누릅니다. 연결 제한 하에서 Directory Proxy Server를 관리하지 못하는 Sun ONE Console의 호스트 시스템에 대해 Administration Server에 대한 액세스가 제한되지 않도록 확인해야 합니다. 자세한 내용은 Sun ONE Console *Server Management Guide*를 참조하십시오.

부록 C

Directory Proxy Server 시작 구성 파일

이 부록에는 Directory Proxy Server 구성 파일에 대한 정보가 포함되어 있습니다. 이 부록은 다음 내용으로 구성되어 있습니다.

구성 파일 개요

`tailor.txt` 파일에는 Directory Proxy Server가 기본 구성을 찾는 데 필요한 부트스트랩 정보가 포함되어 있습니다. 이 파일의 지시어는 Directory Proxy Server가 기본 구성에 대한 추가 파일을 사용하는 경우 또는 Directory Proxy Server가 LDAP 서버로부터 기본 구성을 요청하는 경우를 지시합니다. 기본적으로 Directory Proxy Server는 설치 인스턴스 디렉토리의 `etc` 하위 디렉토리에서 시작 구성 파일인 `tailor.txt`를 찾기를 기대합니다. 주: `-t` 명령줄 매개변수를 사용하여 Directory Proxy Server에 대체 파일을 시작 구성 파일로 사용하도록 지시할 수 있습니다.

고가용성 구성을 지원하도록 돕기 위해 시작 구성 파일은 기본 구성 검색을 위한 여러 연락 지점을 나열할 수 있습니다. 연락 지점은 두 키워드, 즉 `Begin`과 `End`를 사용하여 시작 구성 파일 내에 표시됩니다. Directory Proxy Server는 연락처 정보를 지정된 순서대로 하나씩 처리합니다. 각 연락 지점에서 Directory Proxy Server의 동작은 지정된 연락 지점의 유형(LDAP URL 또는 절대 파일 경로 이름)에 따라 다릅니다.

LDAP-URL 기반 연락 지점의 경우 Directory Proxy Server는 지정된 호스트에 연락을 시도합니다. 호스트가 구성을 반환하지 않거나 반환할 수 없는 경우 Directory Proxy Server는 다음 연락 지점으로(있는 경우) 이동합니다. 호스트가 구성을 반환하는 경우 Directory Proxy Server는 반환된 내용을 편집한 다음 기본 구성 지시어를 따르거나 구성이 유효하지 않은 경우 실행을 종료합니다.

파일 기반 연락 지점의 경우 Directory Proxy Server는 지정된 파일을 기본 구성으로 로드하려고 시도합니다. 지정한 구성이 없거나 유효하지 않은 경우 Directory Proxy Server는 실행을 종료합니다. Directory Proxy Server는 파일 기반 연락 지점을 찾을 경우 다음 연락 지점으로 이동하지 않습니다.

Directory Proxy Server가 LDAP 호스트에서 기본 구성을 검색하는 경우 Directory Proxy Server는 익명, 단순 또는 SASL의 세 방법 중 하나를 사용하여 호스트에 바인딩할 수 있습니다.

*익명 바인딩*은 `configuration_bind_pw` 및 `configuration_bind_dn` 지시어를 생략하여 수행됩니다. 즉, 시작 구성의 연락처 정보에서 `configuration_url` 지시어만 지정합니다.

*단순 바인딩*은 `configuration_bind_pw` 지시어와 `configuration_bind_dn` 지시어를 모두 사용하여 지원됩니다.

*SASL 바인딩*에서는 `sasl_bind_mechanism` 및 `conguration_bind_pw` 지시어와 `configuration_bind_dn` 또는 `configuration_username` 지시어 중 하나를 지정해야 합니다.

시작 구성 키워드

열거된 각 연락 지점에서는 `Begin` 키워드를 사용하여 연락 지점 항목의 시작을 나타냅니다. 반대로 `End` 키워드를 사용하여 각 연락 지점 항목을 종료합니다. 시작 구성 파일에 명시되는 모든 지시어는 각각 한 줄로 표시됩니다. 시작 구성 파일에서는 줄 연속이 인식되지 않고 지원되지도 않습니다. 구성 옵션은 옵션, 콜론(;), 값의 세 부분으로 지정됩니다.

configuration_url

configuration_url 옵션은 Directory Proxy Server 구성이 저장되는 디렉토리에 있는 항목의 고유 이름과 LDAP 디렉토리 서버 또는 LDIF 형식의 로컬 파일을 지정합니다. 예를 들어, Directory Proxy Server 구성이 포트 389 에서 실행하는 LDAP 서비스가 있는 ldap.sun.com 호스트에 있는 LDAP 디렉토리에 저장되고 Directory Proxy Server 항목의 고유 이름이 "ids-proxy-con-Server-Name=Directory Proxy Server"일 경우 구성 파일에 다음이 추가됩니다.

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name=Directory Proxy
Server
End
```

구성을 LDAP 서버에 보관할 경우 호스트 디렉토리의 이름 지정 컨텍스트와 호환성을 유지하도록 ids-proxy-con-Server-Name=Directory Proxy Server 뒤에 접미어를 지정해야 할 수 있습니다. 예를 들면 다음과 같습니다.

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name=Directory Proxy
Server,
ou=services, dc=sun, dc=com
End
```

각 시작 구성 지시어는 구성 파일 내에서 연속하는 한 줄로 지정되어야 합니다.

주 configuration_url 예에 있는 줄 바꾸기를 구성 파일에 줄 바꿈을 삽입하라는 지시로 해석하지 마십시오.

구성이 LDIF 형식 파일(예: <server-root>/dps-<hostname>/etc/tailor.ldif)에 저장되는 경우 구성 파일에 다음이 추가됩니다.

```
Begin
configuration_url:
file://<server-root>/dps-<hostname>/etc/tailor.ldif#ids-proxy-con-Ser
ver-Name=Directory Proxy Server
End
```

configuration_bind_dn

configuration_bind_dn 옵션은 Directory Proxy Server가 configuration_url 옵션에 지정된 LDAP 서버에 바인딩될 때 사용할 고유 이름을 지정합니다. Directory Proxy Server는 이 고유 이름과 configuration_bind_pw 값을 비밀 번호로 사용하여 단순 바인딩을 수행합니다. 예를 들면 다음과 같습니다.

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name=Directory Proxy
Server
configuration_bind_dn: cn=Directory Manager
configuration_bind_pw: secret
End
```

configuration_bind_dn 옵션은 configuration_url이 "파일" 형식일 경우에는 필요하지 않으므로 무시됩니다. 주: configuration_bind_dn 지시어와 configuration_username 지시어는 상호 배타적입니다.

configuration_bind_pw

configuration_bind_pw 옵션은 LDAP 디렉토리에 바인딩할 때 사용할 비밀번호를 지정하는 데 사용됩니다. 이 지시어는 단순 또는 SASL 기반 바인딩에 사용할 비밀번호를 지정하는 데 사용됩니다. 보안 유지를 위해 권한이 없는 사용자가 읽지 못하도록 구성 파일을 보호해야 합니다. configuration_bind_pw 옵션은 configuration_url이 "파일" 형식일 경우에는 필요하지 않으므로 무시됩니다. configuration_bind_dn의 예를 참조하십시오.

configuration_username

configuration_username 옵션은 Directory Proxy Server가 configuration_url 옵션에 지정된 LDAP 서버에 바인딩될 때 사용할 사용자 이름을 지정합니다. 이 옵션은 SASL 바인드 메커니즘을 사용할 경우에만 사용됩니다. 주: configuration_bind_dn 지시어와 configuration_username 지시어는 상호 배타적입니다.

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name=Directory Proxy
Server
```

```
configuration_username: administrator
configuration_bind_pw: secret
sasl_bind_mechanism: CRAM-MD5
End
```

sasl_bind_mechanism

Directory Proxy Server에서 사용할 SASL 바인드 메커니즘에 따라 `sasl_bind_mechanism` 옵션을 `CRAM-MD5` 또는 `DIGEST-MD5`로 설정할 수 있습니다. Directory Proxy Server는 이 옵션이 없는 경우 단순 바인드 또는 익명 바인드를 수행합니다. `DIGEST-MD5`는 `CRAM-MD5`보다 더 높은 수준의 보안을 제공하지만 `DIGEST-MD5`는 `CRAM-MD5`만큼 폭넓게 적용되지 않습니다.

부록 D

명령 참조

이 부록에서는 Sun ONE Directory Proxy Server와 관련된 유용한 명령줄 프로그램에 대해 설명합니다.

부록은 다음 내용으로 구성되어 있습니다.

dpsconfig2ldif

`dpsconfig2ldif` 유틸리티는 Directory Proxy Server 구성을 다운로드하여 LDIF 파일에 저장하는 데 사용됩니다. 이 유틸리티는 다음 위치에서 참조할 수 있습니다.

```
<Install Root>/bin/dps_utilities/dpsconfig2ldif
```

이 유틸리티에는 다음과 같은 두 인수가 필요합니다.

인수	설명
-t *파일 이름*	*파일 이름*은 시작 구성 파일의 경로이며, 일반적으로 etc 디렉토리에 있는 tailor.txt 파일입니다.
-o *파일 이름*	구성을 출력할 파일 이름

dpsldif2config

ImportConfigLdif는 dpsConfig2Ldif에 의해 생성된 LDIF 파일을 가져옵니다. 이 유틸리티는 다음 위치에서 참조할 수 있습니다.

```
<Install Root>/bin/dps_utilities/dpsldif2config
```

이 유틸리티에는 다음과 같은 인수가 필요합니다.

인수	설명
ldif	다음과 같은 Directory Proxy Server 객체 옵션을 포함하는 ldif 파일 이름
-C	만들 구성(지정하지 않은 경우 "가져온 구성")의 이름
-h	디렉토리 호스트 이름(지정하지 않은 경우 로컬 호스트)
-p	디렉토리 포트 번호(지정하지 않은 경우 389)
-D	디렉토리 사용자 dn(지정하지 않은 경우 익명 바인드)
-w	디렉토리 사용자 비밀번호(지정하지 않은 경우 익명 바인드)
-v	세부 정보 표시

ImportConfigLdif는 다음과 같은 세 종류의 객체를 가져옵니다.

- 공유 구성(예: "Directory Proxy Server 구성" 노드의 주 콘솔 토폴로지 트리에 있는 구성)
- 공유 시스템 등록 정보
- 공유 로그 등록 정보

"구성 이름" 매개 변수는 방금 설명한 공유 구성 객체에만 적용됩니다. 시스템 및 로그 등록 정보는 ldif 파일로부터 "있는 그대로" 추가됩니다. 지정한 매개 변수 이름을 갖는 공유 구성 객체가 없는 경우 이 스크립트는 지정한 매개 변수 이름을 사용하여 새 구성을 만듭니다. 지정한 이름의 구성이 이미 있는 경우 가져오기가 수행되지 않습니다. 시스템 및 로그 등록 정보는 지정한 이름의 구성이 디렉토리에 이미 있는 경우 추가되지 않습니다.

구성을 가져온 경우 주 콘솔을 다시 시작해야 토폴로지 트리에서 해당 구성을 볼 수 있습니다. 구성을 사용하려면 Directory Proxy Server 인스턴스 서버가 각 구성에 할당되어야 합니다. 공유 구성은 Directory Proxy Server 서버 콘솔에 네트워크 그룹 노드를 통해 할당되고, 시스템 등록 정보는 Directory Proxy Server 서버 콘솔("다른 이름으로 저장된 설정...")에 시스템 노드를 통해 할당되고, 로그 등록 정보는 Directory Proxy Server 서버 콘솔("다른 이름으로 저장된 설정...")에 로그 노드를 통해 할당됩니다.

사전 조건:

- 5.0(sp 1)으로부터의 이전 완료

사후 조건:

- 가져온 ldif 파일에서 속성 무시

색인

가

다

라

마

바

사

아

자

타

파

A

C

D

I

L