Oracle® Solaris 11.1에서 이름 지정 및 디렉토리 서비스 작업

부품 번호: E36690–02
2012년 10월

ORACLE

121210@25097

목차

표

코드 예

머리말

Oracle Solaris 11.1에서 이름 지정 및 디렉토리 서비스 작업에서는 Oracle Solaris 운영 체제(OS) 이름 지정 및 디렉토리 서비스인 DNS, NIS 및 LDAP의 설정과 관리에 대해 설명합니다. 이 설명서는 Oracle Solaris 관리 정보의 중요한 부분을 다루는 다중 볼륨 세트의 일부입니다.

주 – 본 Oracle Solaris 릴리스는 프로세서 아키텍처의 SPARC 및 x86 제품군을 사용하는 시스템을 지원합니다. 지원되는 시스템은 **Oracle Solaris OS: 하드웨어 호환성 목록**을 참조하십시오. 이 설명서에서는 플랫폼 유형에 따른 구현 차이가 있는 경우 이에 대하여 설명합니다.

관련 문서

- **Oracle Directory Server Enterprise Edition 배포 설명서**
- **Oracle Directory Server Enterprise Edition 관리 설명서**
- **DNS and Bind**, 저자 Cricket Liu and Paul Albitz, (5th Edition, O'Reilly, 2006)
- **Understanding and Deploying LDAP Directory Services**, 저자 Timothy A. Howes, Ph.D. and Mark C. Smith

Oracle Support에 액세스

Oracle 고객은 My Oracle Support를 통해 온라인 지원에 액세스할 수 있습니다. 자세한 내용은 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info`를 참조하거나, 청각 장애가 있는 경우 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`를 방문하십시오.

활자체 규약

다음 표는 이 설명서에서 사용되는 활자체 규약에 대해 설명합니다.

표 P–1 활자체 규약

활자체	설명	예
`AaBbCc123`	명령, 파일, 디렉토리 이름 및 컴퓨터 화면에 출력되는 내용입니다.	`.login` 파일을 편집하십시오. 모든 파일 목록을 보려면 `ls -a` 명령을 사용하십시오. `machine_name% you have mail.`
`AaBbCc123`	사용자가 입력하는 내용으로 컴퓨터 화면의 출력 내용과 대조됩니다.	`machine_name%` **`su`** `Password:`
AaBbCc123	위치 표시자: 실제 이름이나 값으로 바뀝니다.	`rm` *filename* 명령을 사용하여 파일을 제거합니다.
AaBbCc123	설명서 제목, 새 용어, 강조 표시할 용어입니다.	**사용자 설명서**의 6장을 읽으십시오. **캐시**는 로컬로 저장된 복사본입니다. 파일을 저장하면 **안 됩니다**. **주:** 일부 강조된 항목은 온라인에서 굵은체로 나타납니다.

명령 예의 셸 프롬프트

다음 표에서는 Oracle Solaris OS에 포함된 셸의 UNIX 시스템 프롬프트 및 수퍼유저 프롬프트를 보여 줍니다. 명령 예에서 셸 프롬프트는 일반 사용자 명령을 실행해야 하는지, 아니면 권한 있는 사용자가 실행해야 하는지를 나타냅니다.

표 P–2 셸 프롬프트

셸	프롬프트
Bash 셸, Korn 셸 및 Bourne 셸	`$`
수퍼유저용 Bash 셸, Korn 셸 및 Bourne 셸	`#`
C 셸	`machine_name%`
수퍼유저용 C 셸	`machine_name#`

제 1 부

이름 지정 및 디렉토리 서비스 정보

1부에서는 Oracle Solaris OS에 대한 이름 지정 및 디렉토리 서비스를 소개합니다. 또한 여러 로컬 및 원격 디렉토리 서비스를 통해 조회를 조정할 수 있도록 SMF(서비스 관리 기능)를 사용하여 이름 지정 서비스를 구성하는 방법에 대해 설명합니다. DNS(도메인 이름 서비스)와 Active Directory 클라이언트를 구성하는 방법에 대해서도 설명합니다.

◆ ◆ ◆ 1 장

1 이름 지정 및 디렉토리 서비스(개요)

이 장에서는 Oracle Solaris 릴리스에 포함된 이름 지정 및 디렉토리 서비스의 개요를 제공합니다. 또한 DNS, NIS 및 LDAP 이름 지정 서비스에 대해 간단하게 설명합니다.

이 장에서는 다음 내용을 다룹니다.

이름 지정 서비스 정의

이름 지정 서비스는 다음과 같은 저장된 정보를 조회합니다.

- 호스트 이름 및 주소
- 사용자 이름
- 암호
- 액세스 권한
- 그룹 구성원, 자동 마운트 맵 등

이 정보는 사용자가 호스트에 로그인하고, 리소스에 액세스하고, 권한이 부여될 수 있도록 하기 위해 제공됩니다. 다양한 형식의 데이터베이스 파일에 로컬로 또는 중앙 네트워크 기반 저장소나 데이터베이스에 이름 서비스 정보를 저장할 수 있습니다.

중앙 이름 지정 서비스가 없으면 각 호스트가 이 정보의 고유한 복사본을 유지 관리해야 합니다. 파일, 맵 또는 데이터베이스 테이블에 이름 지정 서비스 정보를 저장할 수 있습니다. 모든 데이터를 중앙에 배치하면 관리가 더 쉬워집니다.

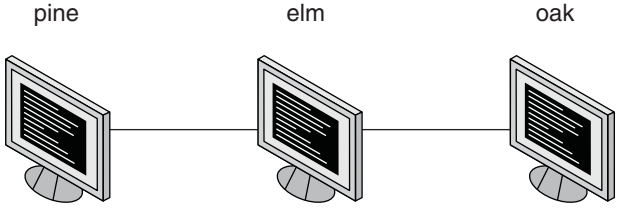
이름 지정 서비스는 모든 컴퓨팅 네트워크의 기본 요소입니다. 다른 기능 중에서도 이름 지정 서비스는 다음 작업을 수행하는 기능을 제공합니다.

- 이름을 객체에 연결(**바인딩**)
- 이름을 객체로 확인

- 바인딩 제거
- 이름 나열
- 정보 이름 바꾸기

네트워크 정보 서비스를 사용하면 숫자 주소 대신 일반 이름으로 시스템을 식별할 수 있습니다. 이렇게 하면 사용자가 192.168.0.0 등의 성가신 숫자 주소를 기억하거나 입력할 필요가 없으므로 통신이 더 간단해집니다.

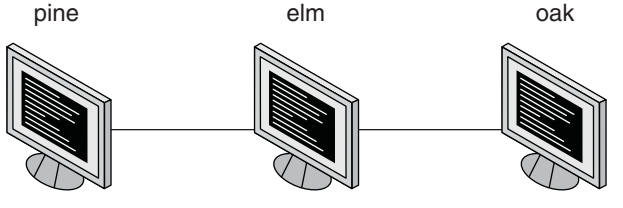
예를 들어, pine, elm 및 oak라는 3개 시스템의 네트워크를 만듭니다. pine이 elm 또는 oak에 메시지를 보내려면 먼저 pine이 해당 숫자 네트워크 주소를 알고 있어야 합니다. 이런 이유로 pine은 해당 시스템을 비롯하여 네트워크에 있는 모든 시스템의 네트워크 주소를 저장하는 /etc/inet/hosts 파일을 유지합니다.



/etc/inet/hosts

```
10.0.3.1 pine
10.0.3.2 elm
10.0.3.3 oak
```

마찬가지로, elm 및 oak가 pine과 통신하거나 서로 통신하려면 시스템에서 유사한 파일을 유지해야 합니다.



/etc/inet/hosts

```
10.0.3.1 pine
10.0.3.2 elm
10.0.3.3 oak
```

/etc/inet/hosts

```
10.0.3.1 pine
10.0.3.2 elm
10.0.3.3 oak
```

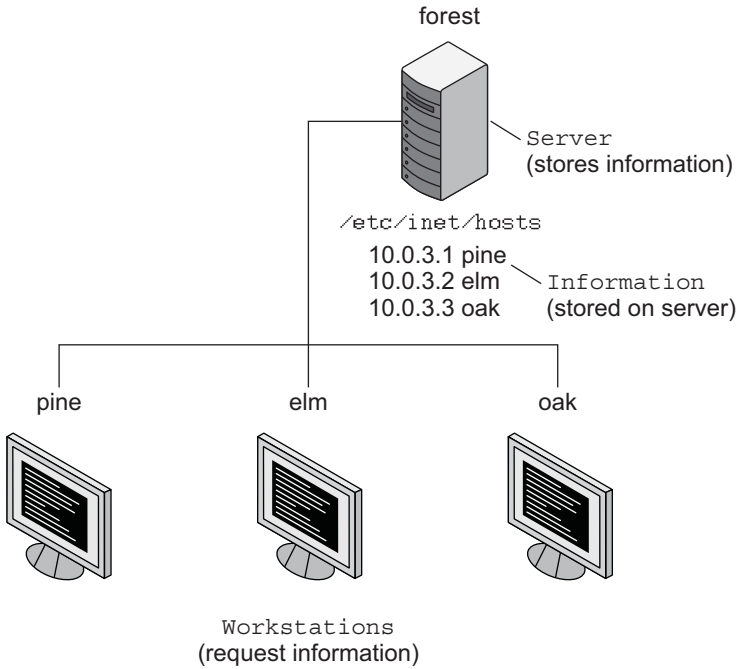
/etc/inet/hosts

```
10.0.3.1 pine
10.0.3.2 elm
10.0.3.3 oak
```

주소 저장 외에도 시스템은 보안 정보, 메일 데이터, 네트워크 서비스 정보 등을 저장합니다. 네트워크에서 더 많은 서비스를 제공할수록 저장된 정보 목록이 커집니다. 따라서 각 시스템에서 `/etc/inet/hosts`와 유사한 전체 파일 세트를 유지할 수도 있습니다.

네트워크 정보 서비스는 모든 시스템에서 질의할 수 있는 서버에 네트워크 정보를 저장합니다.

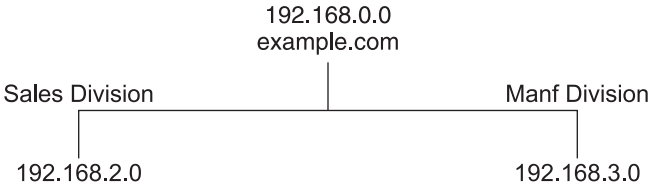
시스템을 서버의 **클라이언트**라고 합니다. 다음 그림에서는 클라이언트-서버 배열을 보여 줍니다. 네트워크 정보가 변경될 때마다 각 클라이언트의 로컬 파일을 업데이트하는 대신 관리자는 네트워크 정보 서비스에서 저장하는 정보만 업데이트합니다. 이렇게 하면 오류, 클라이언트 간의 불일치 및 작업의 전체 크기가 감소합니다.



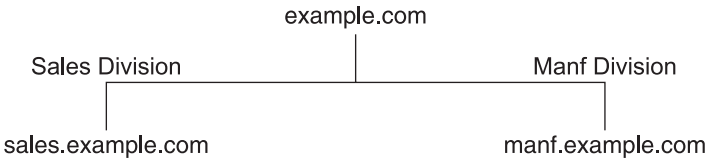
서버에서 네트워크의 클라이언트에 중앙집중 서비스를 제공하는 이 배열을 **클라이언트-서버 컴퓨팅**이라고 합니다.

네트워크 정보 서비스의 주요 목적은 정보를 중앙 집중화하는 것이지만 네트워크 정보 서비스에서 네트워크 이름을 간소화할 수도 있습니다. 예를 들어, 회사에서 인터넷에 연결된 네트워크를 설정했다고 가정합니다. 인터넷에서 네트워크에 네트워크 주소 `192.168.0.0`과 도메인 이름 `example.com`을 지정했습니다. 회사에 Sales 및

Manufacturing(Manf)의 두 부서가 있으므로 네트워크는 기본 네트워크와 각 부서에 대한 서브넷 1개로 나뉩니다. 각 네트워크에 고유한 주소가 있습니다.



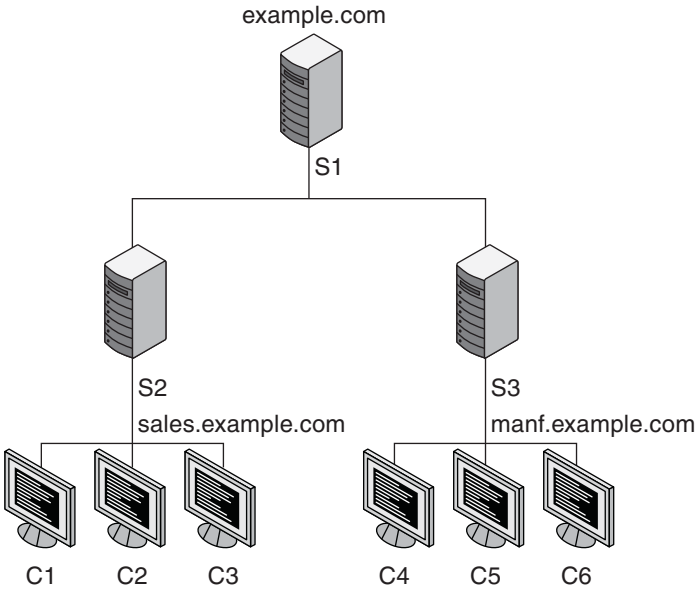
각 부서는 위와 같이 네트워크 주소로 식별될 수도 있지만 이름 지정 서비스에서 지정한 설명이 포함된 이름을 사용하는 것이 좋습니다.



메일 또는 다른 네트워크 통신의 주소를 `198.168.0.0`으로 지정하는 대신 메일 주소를 `example.com`으로 지정할 수 있습니다. 메일 주소를 `192.168.2.0` 또는 `192.168.3.0`으로 지정하는 대신 메일 주소를 `sales.example.com` 또는 `manf.example.com`으로 지정할 수 있습니다.

또한 이름이 물리적 주소보다 더 유연합니다. 물리적 네트워크는 안정적인 경향이 있지만 회사 조직은 변하기 마련입니다.

예를 들어, `example.com` 네트워크가 `S1`, `S2` 및 `S3`의 3개 서버에서 지원된다고 가정합니다. 서버 중 `S2`와 `S3` 2개는 클라이언트를 지원한다고 가정합니다.

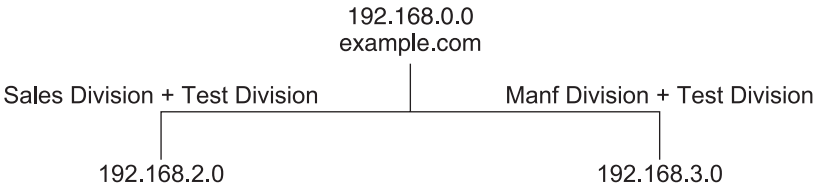


C1, C2 및 C3 클라이언트는 S2 서버에서 네트워크 정보를 가져옵니다. C4, C5 및 C6 클라이언트는 S3 서버에서 네트워크 정보를 가져옵니다. 결과 네트워크는 다음 표에 요약되어 있습니다. 이 표는 해당 네트워크의 일반화된 표현이지만 실제 네트워크 정보 맵과 유사하지는 않습니다.

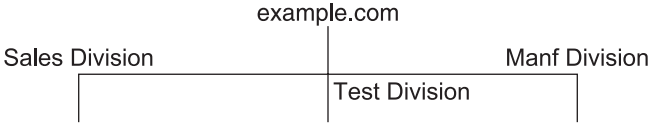
표 1–1 example.com 네트워크의 표현

네트워크 주소	네트워크 이름	서버	클라이언트
192.168.1.0	example.com	S1	
192.168.2.0	sales.example.com	S2	C1, C2, C3
192.168.3.0	manf.example.com	S3	C4, C5, C6

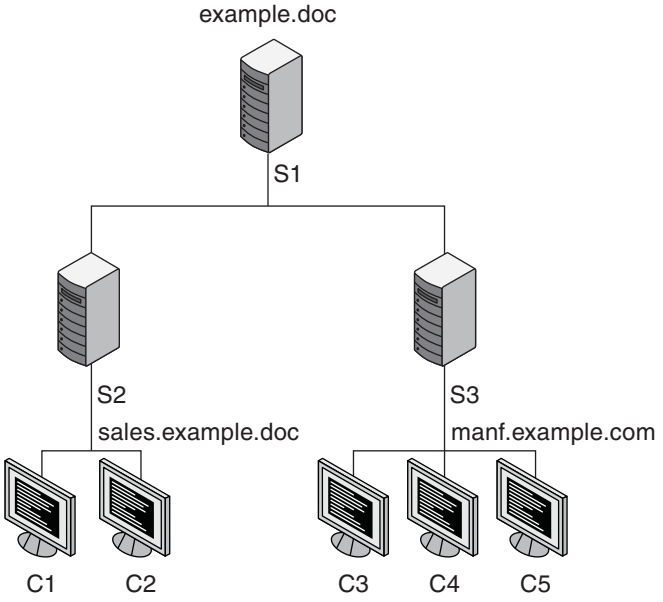
이제 다른 두 부서에서 일부 리소스를 빌린 세번째 부서 Testing을 만들지만 세번째 서브넷을 만들지 않았다고 가정합니다. 그러면 물리적 네트워크가 더 이상 회사 구조와 유사하지 않습니다.



Test Division에 대한 트래픽은 해당 서브넷이 없고 대신 `192.168.2.0`와 `192.168.3.0` 간에 분할됩니다. 그러나 네트워크 정보 서비스를 사용할 경우 Test Division 트래픽이 해당 전용 네트워크를 사용할 수 있습니다.



따라서 조직이 변경되면 해당 네트워크 정보 서비스에서 여기 표시된 대로 매핑을 변경할 수 있습니다.



이제 `C1` 및 `C2` 클라이언트가 `S2` 서버에서 해당 정보를 가져옵니다. `C3`, `C4` 및 `C5`는 `S3` 서버에서 정보를 가져옵니다.

조직의 이후 변경 사항은 네트워크 구조를 재구성하지 않고 네트워크 정보 구조만 변경하여 수용됩니다.

Oracle Solaris 이름 지정 서비스

Oracle Solaris 플랫폼은 다음과 같은 이름 지정 서비스를 제공합니다.

- DNS(Domain Name System)(27 페이지 "DNS 이름 지정 서비스에 대한 설명" 참조)
- `/etc` 파일, 원래 UNIX 이름 지정 시스템(28 페이지 "/etc 파일 이름 지정 서비스에 대한 설명" 참조)
- NIS(네트워크 정보 서비스)(28 페이지 "NIS 이름 지정 서비스에 대한 설명" 참조)
- LDAP(Lightweight Directory Access Protocol)(제3부 **LDAP 이름 지정 서비스 설정 및 관리** 참조)

대부분의 최신 네트워크는 이러한 서비스 중 2개 이상을 조합해서 사용합니다. 특정 조회에 사용되는 이름 지정 서비스는 이름 서비스 스위치에 의해 조정됩니다. 이 내용은 2 장, "이름 서비스 스위치(개요)"에서 설명합니다.

DNS 이름 지정 서비스에 대한 설명

DNS(*Domain Name System*)는 TCP/IP 네트워크에 구현된 계층적 분산 데이터베이스입니다. 주로 인터넷 호스트 이름의 IP 주소와 IP 주소의 호스트 이름을 조회하는 데 사용됩니다. 데이터는 네트워크에 분산되고 오른쪽에서 왼쪽으로 읽는 마침표로 구분된 이름을 사용하여 찾습니다. DNS는 메일 교환 경로 지정 정보, 위치 데이터, 사용 가능한 서비스 등 다른 인터넷 관련 호스트 정보를 저장하는 데도 사용됩니다. 서비스의 계층적 특성은 로컬 도메인의 로컬 관리를 가능하게 하는 동시에 인터넷, 인트라넷 또는 둘 다에 연결된 다른 도메인의 국제 서비스 범위를 제공합니다.

DNS 클라이언트는 하나 이상의 이름 서버에서 호스트 이름 정보를 요청하고 응답을 기다립니다. DNS 서버는 DNS 마스터의 파일 또는 타사 데이터베이스에서, 네트워크를 통한 협력 DNS 슬레이브 서버에서, 그리고 이전 질의로부터 저장된 정보에서 로드된 정보 캐시의 요청에 응답합니다. 응답이 없고 서버가 해당 도메인을 담당하지 않으면 허용될 경우 서비스에서 다른 서버의 호스트 이름을 재귀적으로 요청하고 해당 응답을 캐시합니다.

멀티캐스트 DNS 및 서비스 검색에 대한 설명

DNS 프로토콜에 대한 두 가지 확장은 `svc:network/dns/multicast` 서비스에서 관리됩니다. mDNS(멀티캐스트 DNS)는 기존 DNS 서버가 설치되지 않은 소규모 네트워크에서 DNS를 구현합니다. DNS-SD(DNS 서비스 검색)는 멀티캐스트 DNS를

확장하여 간단한 서비스 검색(네트워크 검색) 기능도 제공합니다. 자세한 내용은 39 페이지 “멀티캐스트 DNS” 및 40 페이지 “멀티캐스트 DNS 서비스 검색”을 참조하십시오.

주의 – mDNS 서비스는 `.local` 도메인 이름을 사용하므로 가능한 충돌을 방지하려면 해당 이름을 DNS에서도 사용하면 안됩니다.

/etc 파일 이름 지정 서비스에 대한 설명

원래 호스트 기반 UNIX 이름 지정 시스템은 독립형 UNIX 시스템으로 개발된 다음 네트워크 사용에 맞게 조정되었습니다. 대부분의 이전 UNIX 운영 체제와 시스템은 여전히 로컬 파일만 사용하여 모든 이름 지정 데이터를 관리합니다. 그러나 로컬 파일을 사용하여 호스트, 사용자 및 기타 이름 지정 데이터를 관리하는 것은 복잡한 대규모 네트워크에 적합하지 않습니다. 각 `/etc` 파일은 연관된 매뉴얼 페이지에서 설명합니다. 예를 들어, `/etc/inet/hosts` 파일은 `hosts(4)` 매뉴얼 페이지에서 설명합니다.

NIS 이름 지정 서비스에 대한 설명

NIS(**네트워크 정보 서비스**)는 DNS와 독립적으로 개발되었습니다. DNS는 숫자 IP 주소 대신 시스템 이름을 사용하여 통신을 더 간소화합니다. NIS는 다양한 네트워크 정보에 대한 중앙집중 제어를 제공하여 네트워크 관리를 더 용이하게 하는 데 주력합니다. NIS는 네트워크, 시스템 이름 및 주소, 사용자, 네트워크 서비스 등에 대한 정보를 저장합니다. 이 네트워크 정보 모음을 *NIS* **이름 공간**이라고 합니다.

NIS 이름 공간 정보는 NIS 맵에 저장됩니다. NIS 맵은 UNIX `/etc` 파일과 기타 구성 파일을 대체하도록 고안되었습니다. NIS 맵은 이름과 주소뿐 아니라 다른 많은 정보를 저장합니다. 따라서 NIS 이름 공간에는 큰 맵 세트가 있습니다. 자세한 내용은 93 페이지 “NIS 맵 작업”을 참조하십시오.

NIS는 DNS와 유사한 클라이언트-서버 배열을 사용합니다. 복제된 NIS 서버는 NIS 클라이언트에 서비스를 제공합니다. 주 서버를 **마스터** 서버라고 하며, 안정성을 위해 서버에 백업 또는 **슬레이브** 서버가 있습니다. 마스터 및 슬레이브 서버는 모두 NIS 검색 소프트웨어를 사용하고 NIS 맵을 저장합니다. NIS 구조 및 NIS 관리에 대한 자세한 내용은 6 장, “NIS 설정 및 구성(작업)” 및 7 장, “NIS 관리(작업)”를 참조하십시오.

LDAP 이름 지정 서비스에 대한 설명

LDAP(Lightweight Directory Access Protocol)은 분산 이름 지정과 기타 디렉토리 서비스를 위해 디렉토리 서버에 액세스하는 데 사용되는 보안 네트워크 프로토콜입니다. 이 표준 기반 프로토콜은 계층적 데이터베이스 구조를 지원합니다. 동일한 프로토콜을 사용하여 UNIX 및 다중 플랫폼 환경에서 이름 지정 서비스를 제공할 수 있습니다.

Oracle Solaris OS는 Oracle Directory Server Enterprise Edition(이전의 Sun Java System Directory Server) 및 기타 LDAP 디렉토리 서버와 함께 LDAP을 지원합니다.

LDAP 이름 지정 서비스에 대한 자세한 내용은 9 장, “LDAP 이름 지정 서비스 소개(개요)”를 참조하십시오.

NIS에서 LDAP으로 전환에 대한 자세한 내용은 15 장, “NIS에서 LDAP으로 전환(작업)”을 참조하십시오.

Single Sign-On과 Kerberos 인증 서비스의 설정 및 유지 관리에 대한 자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 제VI부, “Kerberos 서비스”를 참조하십시오.

이름 서비스 스위치에 대한 설명

이름 서비스 스위치는 클라이언트가 DNS, LDAP, NIS 또는 로컬 파일 데이터 소스에서 이름 지정 정보를 검색할 수 있게 하는 방식입니다. 스위치는 `svc:/system/name-service/switch` 서비스를 통해 관리합니다. 자세한 내용은 2 장, “이름 서비스 스위치(개요)”를 참조하십시오.

이름 지정 서비스: 빠른 비교

	DNS	NIS	LDAP	파일
이름 공간	계층적	플랫	계층적	파일
데이터 저장소	파일/리소스 레코드	2열 맵	디렉토리(가변) 색인화된 데이터베이스	텍스트 기반 파일
서버	마스터/슬레이브	마스터/슬레이브	마스터/복제본 다중 마스터 복제본	없음
보안	DNSSEC, 가변	없음(root 또는 nothing)	Kerberos, TLS, SSL, 가변	없음
전송	TCP/IP	RPC	TCP/IP	파일 I/O
스케일	전역	LAN	전역	로컬 호스트만
데이터	호스트	모두	모두	모두

주 – DNS는 LDAP 및 파일 기반 이름 지정을 위한 호스트 또는 네트워크 주소 조회에 권장되는 서비스입니다.

◆ ◆ ◆ 2 장

2 이름 서비스 스위치(개요)

이 장에서는 이름 서비스 스위치에 대해 설명합니다. 이름 서비스 스위치를 사용하여 여러 이름 지정 서비스의 사용을 조정합니다. 이 장에서는 다음 내용을 다룹니다.

이름 서비스 스위치 정보

이름 서비스 스위치는 관리자가 각 네트워크 정보 유형에 사용할 이름 정보 서비스 또는 소스를 지정할 수 있게 하는 구성 가능한 선택 서비스입니다. 이 서비스를 데이터베이스라고 합니다. 이름 서비스 스위치는 다음과 같은 `getXbyY()` 인터페이스를 호출하는 클라이언트 응용 프로그램에서 사용됩니다.

- `gethostbyname ()`
- `getpwuid ()`
- `getpwnam ()`
- `getaddrinfo ()`

SMF 저장소에는 각 시스템의 고유한 구성이 있습니다. 이름 서비스 스위치에 정의된 각 등록 정보는 호스트, 암호, 그룹 등의 특정 데이터베이스를 식별합니다. 각 등록 정보에 지정된 값은 정보를 요청할 소스를 하나 이상 나열합니다. 이러한 값에 지침이나 옵션이 포함된 경우도 있습니다. 지침에는 서비스 시도 횟수, 적용할 시간 초과 또는 서비스가 실패할 경우 수행할 작업 등이 포함될 수 있습니다.

이름 서비스 스위치의 데이터베이스 및 소스

이름 서비스 스위치에서 지원하는 데이터베이스는 다음과 같습니다.

표 2–1 이름 서비스 스위치의 데이터베이스

정보 데이터베이스	설명
alias	전자 메일 주소와 별칭 나열
auth_attr	권한 부여 이름 및 설명 나열
automount	로컬로 마운트할 수 있는 원격 파일 시스템에 대한 정보 나열
bootparam	디스크 없는 클라이언트에 대한 부트 정보 나열
ether	이더넷 주소 및 일치하는 호스트 이름 나열
group	파일 액세스를 공유하는 데 사용될 수 있는 그룹에 대한 정보 나열
host	IP 주소 및 일치하는 호스트 이름 나열
netgroup	공유 NFS 파일 시스템에 대한 정보 나열
netmask	IP 서브넷을 구현하는 데 사용되는 네트워크 마스크 나열
network	각 네트워크의 이름 및 번호 나열
password	사용자 계정 정보 나열
prof_attr	실행 프로파일 이름, 설명 및 기타 속성 나열
project	프로젝트 이름, 고유 식별자 및 연관된 리소스 지정 나열
protocol	인터넷 프로토콜 이름, 번호 및 모든 별칭 나열
publickey	공개 키 정보 나열
rpc	RPC 프로그램의 이름 및 번호 나열
service	인터넷 서비스의 이름, 포트 및 프로토콜 나열
tnrhdb	Oracle Solaris의 Trusted Extensions 기능을 사용하여 호스트의 보안 속성 나열
tnrhtp	Trusted Extensions에서 사용되는 템플리트 나열

또한 이름 서비스 스위치의 default 등록 정보는 그렇지 않을 경우 정의되지 않는 데이터베이스의 소스 문자열을 정의합니다. 네트워크에서 대부분의 데이터베이스에 동일한 소스를 사용하는 경우 default 등록 정보를 변경하고 각 데이터베이스의 특성은 변경하지 않을 수 있습니다. 절차는 37 페이지 “모든 이름 지정 데이터베이스의 소스를 변경하는 방법”을 참조하십시오.

이전 릴리스를 지원하려면 enable_passwd_compat 및 enable_group_compat 등록 정보를 true로 설정하여 암호 및 그룹 정보에 대해 compat 모드를 사용으로 설정할 수 있습니다. 이 모드에서는 해당 데이터베이스에서 이전 스타일 + 또는 - 구문을 지원합니다. 현재 릴리스에서 이 기능은 pam_list 모듈로 대체되었습니다.

다음 표에서는 위에 나열된 데이터베이스의 이름 서비스 스위치에 나열될 수 있는 소스 종류에 대해 설명합니다.

표 2–2 이름 서비스 스위치의 정보 소스

정보 소스	설명
ad	Active Directory 서버에 저장된 데이터베이스를 식별합니다.
compat	암호 및 그룹 정보에 compat를 사용하여 /etc/passwd, /etc/shadow 및 /etc/group 파일에서 이전 스타일 + 또는 - 구문을 지원할 수 있습니다. 이 기능은 pam_list 모듈로 대체되었습니다.
dns	DNS에서 호스트 정보를 가져오도록 지정합니다.
files	클라이언트의 /etc 디렉토리에 저장된 파일(예: /etc/passwd)을 지정합니다.
ldap	LDAP 디렉토리에서 항목을 가져오도록 지정합니다.
mdns	mDNS(멀티캐스트 DNS)를 사용하여 호스트 정보를 지정합니다.
nis	NIS 맵(예: hosts 맵)을 지정합니다.

이름 서비스 스위치의 검색 조건

다음 검색 조건 형식을 사용하여 정보 소스를 하나 이상 선택하고 소스가 사용되는 순서를 지정할 수 있습니다.

- **단일 소스** — 정보 유형에 소스가 1개뿐인 경우(예: files) 스위치를 사용하는 검색 루틴에서 해당 소스의 정보**만** 검색합니다. 루틴에서 정보를 찾으면 success 상태 메시지를 반환합니다. 루틴에서 정보를 찾지 못하면 검색을 중지하고 다른 상태 메시지를 반환합니다. 루틴에서 상태 메시지에 대해 수행하는 작업은 루틴마다 다릅니다.
- **다중 소스** — 데이터베이스에 특정 정보 유형의 소스가 여러 개 포함되어 있는 경우 스위치가 첫번째 나열된 소스에서 검색하도록 검색 루틴에 지시합니다. 루틴에서 정보를 찾으면 success 상태 메시지를 반환합니다. 루틴이 첫번째 소스에서 정보를 찾지 못하면 다음 소스를 시도합니다. 루틴은 정보를 찾거나 루틴이 return 지정에 의해 중단될 때까지 모든 소스를 검색합니다. 나열된 모든 소스가 검색했는데 정보를 찾지 못한 경우 루틴은 검색을 중지하고 non-success 상태 메시지를 반환합니다.

기본적으로 Oracle Solaris 11 릴리스에서 첫번째 소스는 files입니다. 이 구성에서는 나열된 다음 소스를 사용할 수 없어도 시스템이 중단되지 않습니다.

이름 서비스 스위치의 상태 메시지

루틴에서 정보를 찾으면 success 상태 메시지를 반환합니다. 루틴에서 정보를 찾지 못하면 세 가지 오류 상태 메시지 중 하나를 반환합니다. 다음 표에는 가능한 상태 메시지가 나열되어 있습니다.

표 2–3 이름 서비스 스위치의 상태 메시지

상태 메시지	설명
SUCCESS	지정한 소스에서 요청된 항목을 찾았습니다.
UNAVAIL	소스가 응답하지 않거나 사용할 수 없습니다. 즉, 데이터베이스 소스를 찾을 수 없거나 액세스할 수 없습니다.
NOTFOUND	소스가 "No such entry"로 응답했습니다. 즉, 데이터베이스에 액세스했지만 필요한 정보를 찾을 수 없습니다.
TRYAGAIN	소스가 사용 중이며 다음에 응답할 수도 있습니다. 즉, 데이터베이스가 있지만 질의에 응답할 수 없습니다.

이름 서비스 스위치의 스위치 작업 옵션

다음 표에 표시된 2가지 **작업** 중 하나로 상태 메시지에 응답하도록 이름 서비스 스위치에 지시할 수 있습니다.

표 2–4 이름 서비스 스위치의 상태 메시지에 응답

작업	설명
return	정보 검색을 중지합니다.
continue	다음 소스를 시도합니다.

또한 TRYAGAIN 상태 메시지의 경우 다음 작업을 정의할 수 있습니다.

- forever – 현재 소스를 무기한 재시도합니다.
- *n* – 현재 소스를 *n*회 더 시도합니다.

이름 서비스 스위치의 기본 검색 조건

이름 서비스 스위치 상태 메시지와 작업 옵션의 조합에 따라 각 단계에서 검색 루틴이 수행하는 작업이 결정됩니다. 상태 메시지와 작업 옵션의 조합에 따라 **검색 조건**이 구성됩니다.

스위치의 기본 검색 조건은 모든 소스에서 동일합니다. 이 목록에는 여러 검색 조건에 대한 설명이 포함되어 있습니다.

- SUCCESS=return. 정보 검색을 중지합니다. 찾은 정보를 사용하여 계속합니다.
- UNAVAIL=continue. 다음 이름 서비스 스위치 소스로 이동하고 계속 검색합니다. 이 소스가 마지막 또는 유일한 소스인 경우 NOTFOUND 상태로 반환합니다.
- NOTFOUND=continue. 다음 이름 서비스 스위치 소스로 이동하고 계속 검색합니다. 이 소스가 마지막 또는 유일한 소스인 경우 NOTFOUND 상태로 반환합니다.
- TRYAGAIN=continue. 다음 이름 서비스 스위치 소스로 이동하고 계속 검색합니다. 이 소스가 마지막 또는 유일한 소스인 경우 NOTFOUND 상태로 반환합니다.

앞의 목록에 표시된 *STATUS=action* 구문을 통해 다른 조건을 명시적으로 지정하여 기본 검색 조건을 변경할 수 있습니다. 예를 들어, NOTFOUND 조건의 기본 작업은 다음 소스를 계속 검색하는 것입니다. 네트워크 데이터베이스의 검색 조건은 다음과 같이 보고될 수 있습니다.

```
svc:/system/name-service/switch> listprop config/network
config/network  astring             "nis [NOTFOUND=return] files"
```

networks: nis [NOTFOUND=return] files 항목은 NOTFOUND 상태에 대해 기본 조건이 아닌 조건을 지정합니다. 기본 조건이 아닌 조건은 대괄호로 구분됩니다.

이 예에서 검색 루틴은 다음과 같이 동작합니다.

- network 데이터베이스가 사용 가능하고 필요한 정보를 포함하는 경우 루틴에서 SUCCESS 상태 메시지로 반환합니다.
- network 데이터베이스를 사용할 수 없는 경우 루틴에서 UNAVAIL 상태 메시지로 반환합니다. 기본적으로 루틴은 나열된 다음 조건을 사용하여 계속 검색합니다.
- network 데이터베이스가 사용 가능하고 있지만 데이터베이스에 필요한 정보가 포함되지 않은 경우 루틴에서 NOTFOUND 메시지로 반환합니다. 그러나 기본 동작인 다음 소스를 계속 검색하는 대신 루틴이 검색을 중지합니다.
- network 데이터베이스가 사용 중인 경우 루틴에서 TRYAGAIN 상태 메시지로 반환하고 기본적으로 network 데이터베이스를 계속 검색합니다.

주 – 이름 서비스 스위치의 조회는 항목이 나열된 순서대로 수행됩니다. 그러나 passwd -r *repository* 명령을 사용하여 달리 지정되지 않은 경우 암호 업데이트는 반대 순서로 수행됩니다. 자세한 내용은 38 페이지 “이름 서비스 스위치 및 암호 정보”를 참조하십시오.

구문이 잘못된 경우 어떻게 됩니까?

클라이언트 라이브러리 루틴에는 특정 SMF 등록 정보나 default SMF 등록 정보가 이름 서비스 스위치에 정의되어 있지 않거나 등록 정보의 구문이 잘못된 경우 사용되는 compiled-in 기본 항목이 들어 있습니다. 일반적으로 이러한 compiled-in 기본값은 “files”뿐입니다.

auto_home 및 auto_master

auto_home 및 auto_master 테이블과 맵에 대한 스위치 검색 조건은 automount라는 단일 범주로 결합됩니다.

timezone 및 이름 서비스 스위치

timezone 테이블은 이름 서비스 스위치를 사용하지 않으므로 테이블이 스위치의 등록 정보 목록에 포함되지 않습니다.

이름 서비스 스위치의 keyserv 및 publickey 항목

주의 – 변경 사항을 적용하려면 이름 서비스 스위치를 변경한 후 keyserv 데몬을 다시 시작해야 합니다.

keyserv 데몬은 keyserv가 시작된 경우에만 이름 서비스 스위치에서 publickey 등록 정보를 읽습니다. 이름 서비스 스위치 등록 정보를 변경할 경우 keyserv는 svcadm refresh svc:/network/rpc/keyserv:default를 사용하여 keyserv 데몬을 다시 시작할 때까지 변경 사항을 등록하지 않습니다. 등록 정보를 변경하고 name-service/switch 서비스를 새로 고쳐 등록 정보 변경 사항을 SMF 저장소에 로드한 후에만 이 명령을 실행해야 합니다.

이름 서비스 스위치 관리

시스템의 이름 지정 서비스를 변경할 때는 시스템의 이름 서비스 스위치 정보도 알맞게 수정해야 합니다. 예를 들어, 파일에서 시스템의 이름 지정 서비스를 NIS로 변경하는 경우 NIS를 사용하도록 이름 서비스 스위치를 구성해야 합니다.

▼ 레거시 nsswitch.conf 파일을 사용하는 방법

1. **관리자로 전환합니다.**

   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2. **nsswitch.conf 파일을 새 시스템에 복사합니다.**

   파일 이름을 /etc/nsswitch.conf로 지정해야 합니다.

3. **파일의 정보를 SMF 저장소에 로드합니다.**

   ```
   # nscfg import -f svc:/system/name-service/switch:default
   ```

4. **이름 서비스 스위치 서비스를 새로 고칩니다.**

   ```
   # svcadm refresh name-service/switch
   ```

▼ 데이터베이스의 소스를 전환하는 방법

1. **관리자로 전환합니다.**

   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **선택한 데이터베이스에 대한 소스 정의를 변경합니다.**

이 예에서 데이터베이스 검색 순서는 files, nis 순입니다.

```
# svccfg -s system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files nis"
svc:/system/name-service/switch> quit
```

3 **이름 서비스 스위치 서비스를 새로 고칩니다.**

```
# svcadm refresh name-service/switch
```

▼ 모든 이름 지정 데이터베이스의 소스를 변경하는 방법

1 **관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **config/default 등록 정보를 변경합니다.**

이 등록 정보는 가장 일반적인 소스 정의를 사용해야 합니다. 이 예에서 데이터베이스 검색 순서는 files, nis 순입니다.

```
# svccfg -s system/name-service/switch
svc:/system/name-service/switch> setprop config/default = astring: "files nis"
svc:/system/name-service/switch> quit
```

3 **(옵션) 개별 데이터베이스의 등록 정보를 변경합니다.**

이 명령을 사용하여 config/default 등록 정보에서 선택된 순서를 사용하지 않는 데이터베이스에 대한 소스 정의를 변경합니다.

```
# svccfg -s system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files dns nis"
svc:/system/name-service/switch> quit
```

4 **이름 서비스 스위치 서비스를 새로 고칩니다.**

```
# svcadm refresh name-service/switch
```

DNS 및 인터넷 액세스

이름 서비스 스위치는 다음 장에 설명된 대로 클라이언트에 대한 DNS 전달도 제어합니다. DNS 전달은 클라이언트에 인터넷 액세스 권한을 부여합니다.

이름 서비스 스위치 및 암호 정보

files, nis 등의 여러 저장소에 암호 정보를 포함하고 액세스할 수 있습니다. 그런 다음 이름 서비스 스위치의 config/password 등록 정보를 사용하여 해당 정보의 조회 순서를 설정할 수 있습니다.

주의 – 시스템에서 DoS(서비스 거부) 공격을 방지하려면 files가 passwd 정보에 대한 이름 서비스 스위치의 첫번째 소스여야 합니다.

NIS 환경에서 이름 서비스 스위치의 config/password 등록 정보는 다음 순서로 저장소를 나열해야 합니다.

```
config/password  astring              "files nis"
```

참고 – files를 첫번째로 나열하면 시스템에서 네트워크 또는 이름 지정 서비스 문제가 발생해도 대부분의 경우 root 사용자가 로그인할 수 있습니다.

동일한 사용자에 대해 저장소를 여러 개 유지하지 마십시오. 대부분의 경우 이름 지정 서비스는 첫번째 정의만 조회하고 반환합니다. 중복 항목은 대체로 보안 문제를 마스킹합니다.

예를 들어, 파일과 네트워크 저장소에 동일한 사용자가 있으면 config/password name-service/switch 구성에 따라 한 로그인 ID가 사용되고 다른 로그인 ID는 사용되지 않습니다. 특정 시스템과 일치하는 첫번째 ID가 로그인 세션에 사용되는 ID가 됩니다. 파일과 네트워크 저장소 둘 다에 ID가 있고 네트워크 저장소가 보안을 위해 사용 안함으로 설정된 경우 해당 ID가 있고 네트워크 ID가 사용 안함으로 설정되기 전에 액세스된 모든 시스템은 이제 안전하지 않으며 불필요한 비보안 액세스에 취약해질 수 있습니다.

◆ ◆ ◆ 3 장

3 DNS 관리(작업)

이 장에서는 DNS 서버 및 클라이언트 서비스에 대한 정보를 제공합니다. 다음 항목을 다룹니다.

DNS 개요

대부분의 네트워킹 프로토콜과 마찬가지로 DNS는 응답을 제공하는 서비스와 서비스를 질의하는 클라이언트인 두 부분으로 구성됩니다. Oracle Solaris 운영 체제에서 기본 DNS 서비스는 BIND, ISC(Internet Systems Consortium) 및 연결된 `named` 데몬에 의해 제공됩니다. DNS 클라이언트는 유틸리티 및 라이브러리 컬렉션으로 구성됩니다.

멀티캐스트 DNS

mDNS(멀티캐스트 DNS)는 로컬 링크의 시스템에 대해 설정 및 유지 관리하기 쉬운 이름 지정 서비스 시스템을 제공합니다. 동일한 로컬 링크에 참가하는 모든 네트워크 장치는 유니캐스트 대신 mDNS를 사용하여 표준 DNS 기능을 수행하며 유니캐스트 DNS 서버가 필요 없습니다. 관리자의 경우 mDNS의 주요 장점은 로컬 네트워크에서 유니캐스트 DNS를 유지 관리할 필요가 없다는 것입니다. 예를 들어, mDNS를 사용하는 로컬 링크의 시스템에 대해 호스트 이름을 IP 주소로 변환하는 요청을 확인하기 위해 파일에서 호스트 이름을 업데이트하고 유지 관리할 필요가 없습니다.

멀티캐스트 DNS 서비스 검색

네트워크 서비스에는 인쇄, 파일 전송, 음악 공유, 사진, 문서 및 기타 파일 공유를 위한 서버, 기타 로컬 장치가 제공하는 서비스 등이 포함됩니다. Oracle Solaris의 DNS 서비스 검색 지원에는 이 Oracle Solaris 릴리스에서 응용 프로그램이 DNS를 사용하여 네트워크 서비스를 알리고 검색할 수 있도록 Apple Inc.의 오픈 소스 프레임워크와 도구가 포함됩니다.

사용자의 경우 네트워크 서비스 검색은 사용자가 수동으로 서비스를 찾을 필요 없이 네트워크에서 서비스를 찾아볼 수 있게 하여 컴퓨팅을 용이하게 합니다. 다른 회사와 그룹에서 수행한 기존 표준과 작업도 플랫폼간 지원에 사용 가능하게 해 줍니다.

DNS에 대한 관련 자료

DNS 및 BIND 관리에 대한 자세한 내용은 다음 설명서를 참조하십시오.

- **BIND 9 Administrator's Manual** - ISC 웹 사이트(http://www.isc.org)
- BIND 9 Migration Notes 설명서 - `/usr/share/doc/bind/migration.txt` 파일
- BIND 기능, 알려진 버그 및 결함 목록과 추가 자료 링크 - ISC 웹 사이트(http://www.isc.org)
- **DNS and Bind (5th Edition)** - 저자 Paul Albitz, Cricket Liu(O'Reilly, 2006)

DNS 및 서비스 관리 기능

DNS 서버 데몬 `named`는 SMF(서비스 관리 기능)를 사용하여 관리해야 합니다. SMF 개요는 **Oracle Solaris 11.1에서 서비스 및 결함 관리**의 1 장, "서비스 관리(개요)"를 참조하십시오. 또한 자세한 내용은 `svcadm`(1M), `svcs`(1) 및 `svccfg`(1M) 매뉴얼 페이지를 참조하십시오.

다음 목록에서는 SMF 서비스를 사용하여 DNS 서비스를 관리하는 데 필요한 중요한 정보를 간단하게 설명합니다.

- 사용으로 설정, 사용 안함으로 설정, 다시 시작 등 이 서비스에 대한 관리 작업을 수행하려면 `svcadm` 명령을 사용합니다.

  참고 – `-t` 옵션을 사용하여 서비스를 일시적으로 사용 안함으로 설정하면 서비스 구성이 보호됩니다. `-t` 옵션을 사용하여 서비스를 사용 안함으로 설정하면 재부트 후 서비스에 대한 원래 설정이 복원됩니다. `-t`를 사용하지 않고 서비스를 사용 안함으로 설정하면 재부트 후에도 서비스가 사용 안함으로 유지됩니다.

- DNS 서비스의 FMRI(오류 관리 리소스 식별자)는 `svc:/network/dns/server:`*instance* 및 `svc:/network/dns/client:`*instance*입니다.

- svcs 명령을 사용하여 DNS 서버 및 클라이언트의 상태를 질의할 수 있습니다.
  - 다음은 svcs 명령과 해당 출력의 예입니다.

```
# svcs \*dns\*
STATE          STIME    FMRI
disabled       Nov_16   svc:/network/dns/multicast:default
online         Nov_16   svc:/network/dns/server:default
online         Nov_16   svc:/network/dns/client:default
```

  - 다음은 svcs - l 명령과 해당 출력의 예입니다.

```
# svcs -l /network/dns/server
fmri         svc:/network/dns/server:default
name         BIND DNS server
enabled      true
state        online
next_state   none
state_time   Tue Jul 26 19:26:12 2011
logfile      /var/svc/log/network-dns-server:default.log
restarter    svc:/system/svc/restarter:default
contract_id  83
manifest     /lib/svc/manifest/network/dns/server.xml
dependency   require_all/none svc:/system/filesystem/local (online)
dependency   require_any/error svc:/network/loopback (online)
dependency   optional_all/error svc:/network/physical (online)
```

- 다른 옵션으로 DNS 서비스를 시작해야 하는 경우 svccfg 명령을 사용하여 svc:/network/dns/server 서비스의 등록 정보를 변경합니다. 예를 보려면 43 페이지 “DNS 서버 옵션을 구성하는 방법”을 참조하십시오.

DNS 서버 데몬 named가 SMF에서 관리되는 경우 예기치 않은 이벤트가 발생하여 named가 비정상적으로 종료되면 서버가 자동으로 다시 시작됩니다. svcadm 명령을 사용하여 서비스를 다시 시작할 수도 있습니다. rndc 명령을 통해 사용할 수 있는 BIND 관련 관리 기능은 SMF와 동시에 사용할 수 있습니다.

DNS 관리(작업)

다음 작업을 설명합니다.

▼ DNS 패키지를 설치하는 방법

일반적으로 DNS 패키지는 Oracle Solaris 릴리스와 함께 자동으로 설치됩니다. 서버를 설치할 때 패키지가 포함되지 않은 경우 다음 절차에 따라 패키지를 설치합니다.

1 **관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **DNS 패키지를 설치합니다.**

```
# pkg install pkg:/service/network/dns/bind
```

▼ DNS 서버를 구성하는 방법

주 – named를 구성하여 루트 디렉토리 변경을 지정하는 것은 권장되지 않습니다. 더 안전한 옵션은 Solaris 영역을 만들고 해당 영역 내에서 실행되도록 named를 구성하는 것입니다.

1 **관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **DNS 구성 파일을 만들고 확인합니다.**

named 데몬이 시작되기 전에 유효한 구성 파일이 있어야 합니다. 기본적으로 이 파일의 이름은 /etc/named.conf입니다. named의 구성은 매우 단순할 수 있습니다. DNS 루트 서버에 액세스할 수 있는 경우 빈 파일만 있으면 서버만으로 캐싱을 구성하는 데 필요한 정보가 제공됩니다.

```
# touch /etc/named.conf
# named-checkconf -z /etc/named.conf
```

3 **(옵션) rndc 구성 파일을 만듭니다.**

이 파일은 DNS 서버의 원격 제어 액세스를 구성하는 데 사용됩니다.

```
# rndc-confgen -a
wrote key file "/etc/rndc.key"
```

4 **(옵션) dns/server 서비스에 대한 구성 정보를 변경합니다.**

43 페이지 "DNS 서버 옵션을 구성하는 방법"을 참조하십시오.

5 **DNS 서비스를 시작합니다.**

```
# svcadm enable network/dns/server
```

▼ rndc.conf 파일을 만드는 방법

/etc/rndc.conf 파일은 rndc 명령을 사용하여 DNS 서버 데몬 named의 원격 제어 액세스를 구성하는 데 사용됩니다. 기본 파일을 만들려면 다음 절차를 사용합니다. 추가 옵션은 rndc.conf(4) 매뉴얼 페이지를 참조하십시오.

1 **관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **rndc 구성 파일을 만듭니다.**

```
# rndc-confgen -a
wrote key file "/etc/rndc.key
```

3 **DNS 서비스를 다시 시작합니다.**

```
# svcadm restart dns/server:default
```

▼ DNS 서버 옵션을 구성하는 방법

이 절차에서는 named 트래픽을 위한 IPv4 전송 프로토콜을 선택하는 방법에 대해 설명합니다. named(1M) 매뉴얼 페이지를 참조하십시오.

1 **관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **dns/server 서비스에 대한 구성 정보를 변경합니다.**

```
# svccfg -s network/dns/server
svc:/network/dns/server:default> setprop options/ip_interfaces = "IPv4"
svc:/network/dns/server:default> quit
```

3 **SMF 저장소를 업데이트하고 DNS 서비스를 사용으로 설정합니다.**

```
# svcadm refresh network/dns/server
# svcadm enable network/dns/server
```

▼ DNS 서비스를 대체 사용자로 실행하는 방법

이 절차에서는 named 데몬 관리를 위한 관련 권한을 사용자에게 지정하는 방법에 대해 설명합니다.

1 **관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **사용자를 적절한 역할에 추가합니다.**

```
# usermod -A solaris.smf.manage.bind dnsadmin
```

3 **사용자에 대한 서비스 등록 정보를 설정합니다.**

```
# svccfg -s network/dns/server
svc:/network/dns/server:default> setprop start/user = dnsadmin
svc:/network/dns/server:default> setprop start/group = dnsadmin
svc:/network/dns/server:default> exit
```

4 **새 프로세스 ID 파일의 디렉토리를 만듭니다.**

root에만 기본 프로세스 ID 파일 /var/run/named/named.pid를 만들 수 있는 쓰기 권한이 있으므로 대체 파일을 사용하도록 named 데몬을 구성해야 합니다.

```
# mkdir /var/named/tmp
# chown dnsadmin /var/named/tmp
```

5 **새 디렉토리를 사용하도록 구성을 변경합니다.**

named.conf 파일에 다음 라인을 추가합니다.

```
# head /etc/named.conf
options {
directory "/var/named";
pid-file "/var/named/tmp/named.pid";
};
```

6 **SMF 저장소를 업데이트하고 DNS 서비스를 다시 시작합니다.**

```
# svcadm refresh svc:/network/dns/server:default
# svcadm restart svc:/network/dns/server:default
```

▼ DNS 클라이언트를 사용으로 설정하는 방법

1 **관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **DNS 도메인을 구성합니다.**

먼저 검색할 도메인과 DNS 이름 서버의 IP 주소를 나열합니다. 그런 다음 SMF 저장소를 업데이트합니다.

```
# svccfg -s network/dns/client
svc:/network/dns/client> setprop config/search = astring: ("example.com" "sales.example.com")
svc:/network/dns/client> setprop config/nameserver = net_address: (192.168.1.10 192.168.1.11)
svc:/network/dns/client> select network/dns/client:default
svc:/network/dns/client:default> refresh
svc:/network/dns/client:default> quit
```

3 **DNS를 사용하도록 이름 서비스 스위치 정보를 업데이트합니다.**

첫번째 명령은 SMF 저장소의 DNS 구성 정보를 업데이트합니다.

```
# svccfg -s system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files dns"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch:default> quit
```

4 **/etc/resolv.conf 파일에 새 정보를 씁니다.**

/etc/resolv.conf가 일부 프로세스에서 여전히 사용되므로 파일 내용이 변경되는 SMF 저장소 변경 후에는 파일을 다시 만들어야 합니다.

```
# nscfg export svc:/network/dns/client:default
```

5 **DNS 클라이언트를 실행하는 데 필요한 서비스를 시작합니다.**

```
# svcadm enable network/dns/client
# svcadm enable system/name-service/switch
```

▼ DNS 서버 시작 문제를 해결하는 방법

이러한 단계를 모두 수행해야 하는 것은 아닙니다. 초기 단계에서 문제를 발견한 경우 6단계까지 모두 진행하면 서비스가 올바르게 실행됩니다.

1 **관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **DNS 서비스 상태를 확인합니다.**

```
# svcs -x dns/server:default
svc:/network/dns/server:default (BIND DNS server)
 State: online since Tue Oct 18 19:35:00 2011
   See: named(1M)
   See: /var/svc/log/network-dns-server:default.log
Impact: None.
```

3 **DNS 서비스 로그 파일을 확인합니다.**

```
# tail /var/svc/log/network-dns-server:default.log
```

4 **syslog 메시지를 확인합니다.**

```
# grep named /var/adm/messages
```

5 **named 데몬을 수동으로 시작합니다.**

전면에서 named를 실행하면 문제를 식별하기 쉽도록 모두 표준 오류에 로깅됩니다.

```
# named -g
```

6 **문제가 해결되면 유지 관리 필요 상태를 지웁니다.**

```
# svcadm clear dns/server:default
# svcs dns/server:default
STATE          STIME    FMRI
online         17:59:08 svc:/network/dns/server:default
```

▼ DNS 구성을 확인하는 방법

DNS 구성을 수정하는 경우 `named-checkzone` 명령을 사용하여 `/etc/named.conf` 파일의 구문을 확인할 수 있습니다.

1 **관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **필요에 따라 구성 파일을 변경합니다.**

이 예에서는 기본 디렉토리가 변경되었습니다.

```
# echo 'options {directory "/var/named";};' > /etc/named.conf
```

3 **파일 내용을 확인합니다.**

```
# named-checkconf
/etc/named.conf:1: change directory to '/var/named' failed: file not found

/etc/named.conf:1: parsing failed
```

이 예에서는 `/var/named` 디렉토리가 아직 생성되지 않았으므로 검사에 실패했습니다.

4 **보고된 오류를 모두 수정합니다.**

```
# mkdir /var/named
```

5 **오류가 보고되지 않을 때까지 3단계와 4단계를 반복합니다.**

6 **(옵션) 실행 중인 서비스에 변경 사항을 반영하려면 아래 방법 중 하나를 사용합니다.**

- **변경 사항에 따라 `rndc` 명령에 `reload` 또는 `reconfig` 옵션을 사용하여 구성을 업데이트합니다.**
- **`named` 서비스를 다시 시작합니다.**

  ```
  # svcadm restart svc:/network/dns/server:default
  ```

멀티캐스트 DNS 관리

다음 절에서는 mDNS(멀티캐스트 DNS) 및 DNS 서비스 검색을 사용으로 설정하는 방법에 대해 설명합니다. DNS 서비스 검색을 위해 리소스를 알리는 방법의 예도 제공됩니다.

▼ mDNS 및 DNS 서비스 검색을 사용으로 설정하는 방법

mDNS 및 DNS 서비스 검색이 작동하려면 mDNS에 참가해야 하는 모든 시스템에 mDNS를 배포해야 합니다. mDNS 서비스는 시스템에 제공되는 서비스의 가용성을 알리는 데 사용됩니다.

1 관리자로 전환합니다.

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 필요한 경우 mDNS 패키지를 설치합니다.

```
# pkg install pkg:/service/network/dns/mdns
```

3 이름 서비스 스위치 정보를 업데이트합니다.

로컬 호스트를 확인할 수 있으려면 `mdns`를 소스로 포함하도록 `name-service/switch` 서비스의 `config/host` 등록 정보를 변경합니다. 예를 들면 다음과 같습니다.

```
#  /usr/sbin/svccfg -s svc:/system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files dns mdns"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch> quit
```

4 mDNS 서비스를 사용으로 설정합니다.

```
# svcadm enable svc:/network/dns/multicast:default
```

이런 방식으로 mDNS를 사용으로 설정하면 업그레이드 및 재부트 후에도 변경 사항이 유지됩니다. 자세한 내용은 `svcadm`(1M) 매뉴얼 페이지를 참조하십시오.

5 (옵션) 필요한 경우 mDNS 오류 로그를 확인합니다.

mDNS 서비스 로그 `/var/svc/log/network-dns-multicast:default.log`에서 오류나 메시지를 확인합니다.

DNS에 대한 리소스 알림

`ping` 또는 `traceroute` 명령을 사용하는 방법과 유사하게, `dns-sd` 명령을 네트워크 진단 도구로 사용하여 서비스를 찾거나 검색합니다.

시간이 지나면 명령줄 인자와 출력 형식이 변경될 수 있으며, 이 경우 셸 스크립트에서의 명령 호출이 예측할 수 없고 위험하기 때문에 `dns-sd` 명령은 주로 대화식으로 사용됩니다. 또한 DNS-SD(DNS 서비스 검색)의 비동기 특성상, 스크립트 지향 프로그래밍이 쉽게 적용되지 않습니다.

전체 정보는 `dns-sd` (1M) 매뉴얼 페이지를 참조하십시오. 응용 프로그램에 DNS 서비스를 통합하려면 `libdns-sd`(3DNS_SD) 매뉴얼 페이지를 참조하십시오.

다음은 DNS 서비스 검색을 사용하여 서비스를 알리는 방법의 예입니다.

예 3–1 인쇄 서비스 알림

다음 명령은 `My Test` 시스템의 포트 `515`에 LPR 인쇄 서비스가 있음을 알려 DNS-SD 호환 인쇄 클라이언트가 사용할 수 있게 합니다.

```
# dns-sd -R "My Test" _printer._tcp. . 515 pdl=application/postscript
```

이 등록이 유용하려면 포트 `515`에서 LPR 서비스를 사용할 수 있어야 합니다.

예 3–2 웹 페이지 알림

다음 명령은 `My Test` 시스템의 포트 `80`에서 HTTP 서버가 제공하는 웹 페이지를 알립니다. 이 웹 페이지는 Safari 및 다른 DNS-SD 호환 웹 클라이언트의 Bonjour 목록에 표시됩니다.

```
# dns-sd -R "My Test" _http._tcp . 80 path=/path-to-page.html
```

DNS 참조

이 절에는 DNS 서비스와 연관된 파일, 데몬 및 명령에 대한 표가 있습니다. ISC 버전의 BIND를 구축할 때 사용된 일부 플래그에 대한 표도 있습니다.

DNS 파일

다음 표에서는 DNS 서비스와 연관된 파일에 대해 설명합니다.

표 3–1 DNS 파일

파일 이름	기능
`/etc/named.conf`	`named` 데몬에 대한 구성 정보를 제공합니다. 자세한 내용은 `named.conf(4)` 매뉴얼 페이지를 참조하십시오.
`/etc/rndc.conf`	`rndc` 명령에 대한 구성 정보를 제공합니다. 자세한 내용은 `rndc.conf(4)` 매뉴얼 페이지를 참조하십시오.

DNS 명령 및 데몬

다음 표에서는 DNS 서비스와 연관된 명령 및 데몬에 대해 설명합니다.

표 3–2 DNS 명령 및 데몬

파일 이름	기능
/usr/bin/dns-sd	mDNS 서비스에서 사용하는 리소스를 찾거나 나열합니다. 자세한 내용은 dns-sd(1M) 매뉴얼 페이지를 참조하십시오.
/usr/sbin/dig	DNS 서버의 DNS 응답을 요청합니다. 주로 문제를 해결하는 데 사용됩니다. 자세한 내용은 dig(1M) 매뉴얼 페이지를 참조하십시오.
/usr/sbin/dnssec-dsfromkey	키 파일에서 DS RR을 생성합니다. 자세한 내용은 dnssec-dsfromkey(1M) 매뉴얼 페이지를 참조하십시오.
/usr/sbin/dnssec-keyfromlabel	암호화 장치에서 선택한 키를 검색하고 키 파일을 작성합니다. 자세한 내용은 dnssec-keygen(1M) 매뉴얼 페이지를 참조하십시오.
/usr/sbin/dnssec-keygen	보안 DNS와 트랜잭션 서명(TSIG)에 대한 키와 키 파일을 만듭니다. 자세한 내용은 dnssec-keygen(1M) 매뉴얼 페이지를 참조하십시오.
/usr/sbin/dnssec-signzone	DNS 영역에 서명합니다. 자세한 내용은 dnssec-signzone(1M) 매뉴얼 페이지를 참조하십시오.
/usr/sbin/dnssec-dsfromkey	간단한 DNS 조회를 수행하고, 주로 호스트 이름을 IP 주소로 변환하거나 IP 주소를 호스트 이름으로 변환합니다. 자세한 내용은 host(1M) 매뉴얼 페이지를 참조하십시오.
/usr/sbin/named	클라이언트의 정보 요청에 응답하는 DNS 서버 데몬입니다. 자세한 내용은 named(1M) 매뉴얼 페이지를 참조하십시오.
/usr/sbin/named-checkconf	named.conf 파일의 구문을 확인합니다. 자세한 내용은 named(1M) 매뉴얼 페이지를 참조하십시오.
/usr/sbin/named-checkzone	DNS 영역 파일의 구문과 무결성을 확인합니다. 자세한 내용은 named-checkzone(1M) 매뉴얼 페이지를 참조하십시오.
/usr/sbin/named-compilezone	DNS 영역 파일을 변환합니다. 자세한 내용은 named-compilezone(1M) 매뉴얼 페이지를 참조하십시오.
/usr/sbin/nscfg	SMF 저장소에서 resolv.conf 내용을 가져오거나 내보내는 레거시 이름 서비스 구성 유틸리티입니다. 자세한 내용은 nscfg(1M) 매뉴얼 페이지를 참조하십시오.
/usr/sbin/nslookup	사용되지 않음: DNS 서버를 질의합니다. 대신 dig 명령을 사용합니다.
/usr/sbin/nsupdate	DNS 업데이트 요청을 DNS 서버로 제출합니다. 자세한 내용은 nsupdate(1M) 매뉴얼 페이지를 참조하십시오.

표 3–2 DNS 명령 및 데몬 (계속)

파일 이름	기능
/usr/sbin/rndc	DNS 서버 데몬의 원격 제어를 제공합니다. 자세한 내용은 rndc(1M) 매뉴얼 페이지를 참조하십시오.
/usr/sbin/rndc-confgen	rndc 명령에 대한 구성 파일을 생성합니다. 자세한 내용은 rndc-confgen(1M) 매뉴얼 페이지를 참조하십시오.

BIND를 구축할 때 사용된 컴파일 플래그

named -V 명령을 사용하여 BIND를 컴파일하는 데 사용된 플래그를 확인할 수 있습니다. 다음 표에서는 Oracle Solaris 11 릴리스에 대해 ISC 버전의 BIND를 구축할 때 사용된 컴파일 플래그를 보여 줍니다.

표 3–3 BIND 컴파일 플래그

플래그 이름	기능
with-openssl	암호화 및 SSL(Secure Sockets Layer) 지원을 사용하여 DNSSEC에 필요한 BIND를 작성합니다.
enable-threads	멀티스레딩을 사용으로 설정합니다.
enable-devpoll	많은 파일 설명자를 고속 폴링하기 위해 /dev/poll 드라이버를 사용합니다.
disable-openssl-version-check	OpenSSL은 별도의 동적 라이브러리에서 제공되기 때문에 OpenSSL 버전 검사를 사용 안함으로 설정합니다.
enable-fixed-rrset	역방향 호환성에 필요한 고정 리소스 레코드 세트 순서 지정을 사용으로 설정합니다.
with-pkcs11	OpenSSL 암호화 하드웨어 지원을 사용으로 설정합니다.

◆ ◆ ◆ 4 장

4 Oracle Solaris Active Directory 클라이언트 설정(작업)

nss_ad 이름 지정 서비스 모듈은 passwd, shadow 및 group 파일의 백엔드를 제공합니다. nss_ad 모듈은 AD(Active Directory) 및 고유 스키마를 이름 지정 서비스로 사용하여 AD 포리스트에서 사용자 및 그룹 이름과 ID를 확인합니다. 다음과 같은 항목으로 구성됩니다.

nss_ad 이름 지정 서비스 모듈 개요

Oracle Solaris 클라이언트가 AD 도메인에 가입해야 nss_ad를 비롯한 AD 상호 운용성 기능을 사용할 수 있습니다. kclient 유틸리티는 클라이언트를 AD에 결합하는 데 사용됩니다. 결합 작업 중에 kclient는 클라이언트에서 Kerberos v5를 구성합니다. 그런 후에 nss_ad를 사용하면 지원되는 데이터베이스의 nsswitch.conf 파일에서 ad를 소스로 지정하여 이름 지정 서비스 요청을 확인할 수 있습니다. nss_ad 모듈은 호스트 자격 증명을 사용하여 AD에서 이름 지정 서비스 정보를 조회합니다.

nss_ad 모듈은 DNS 서버 레코드를 사용하여 도메인 컨트롤러, 전역 카탈로그 서버 등의 AD 디렉토리 서버를 자동 검색합니다. 따라서 Oracle Solaris 클라이언트에서 DNS를 올바르게 구성해야 합니다. 또한 nss_ad 모듈은 LDAP v3 프로토콜을 사용하여 AD 서버의 이름 지정 정보에 액세스합니다. nss_ad는 고유 AD 스키마에서 작동하므로 AD 서버 스키마를 수정할 필요가 없습니다.

nss_ad 모듈은 현재 Windows 사용자의 Oracle Solaris 시스템 로그인을 지원하지 않습니다. 이러한 로그인이 지원될 때까지 해당 사용자는 계속해서 nis, ldap 등의 기존 백엔드를 사용하여 로그인해야 합니다.

nss_ad를 사용하려면 idmap 및 svc:/system/name-service/cache 서비스를 사용으로 설정해야 합니다. nss_ad 모듈은 idmap 서비스를 사용하여 Windows SID(보안 식별자), UNIX UID(사용자 식별자) 및 GID(그룹 식별자) 간에 매핑합니다.

모든 AD 사용자 및 그룹 이름은 정규화된 도메인 이름이어야 합니다(예: user@domain 또는 group@domain). 예를 들어, dana가 domain 도메인에서 유효한 Windows 사용자인 경우 getpwnam(dana)은 실패하지만 getpwnam(dana@domain)은 성공합니다.

nss_ad 모듈에는 다음 추가 규칙도 적용됩니다.

- AD와 마찬가지로, nss_ad는 일치하는 사용자와 그룹 이름의 대소문자 무시를 수행합니다.
- 사용자와 그룹의 이름에 ASCII 문자만 포함된 도메인이나 UTF-8 로케일에서만 nss_ad 모듈을 사용합니다.
- 잘 알려진 SID는 Windows에서 일반 사용자나 일반 그룹을 식별하는 SID 세트입니다. 도메인과 관련이 없으며 모든 Windows 운영 체제에서 값이 일정하게 유지됩니다. 잘 알려진 SID의 이름은 정규화된 BUILTIN 문자열입니다(예: Remote Desktop Users@BUILTIN).
- nss_ad 모듈은 열거를 지원하지 않습니다. 따라서 getpwent() 및 getgrent() 인터페이스와 두 인터페이스를 사용하는 명령(예: getent passwd 및 getent group)은 AD에서 정보를 검색할 수 없습니다.
- nss_ad 모듈은 현재 passwd 및 group 파일만 지원합니다. nss_ad는 passwd 항목을 따르는 다른 이름 지정 서비스 데이터베이스(예: audit_user 및 user_attr)를 지원하지 않습니다. ad 백엔드가 구성에 따라 처리되면 이러한 데이터베이스에 대해 NOT FOUND를 반환합니다.

▼ nss_ad 모듈을 구성하는 방법

nss_ad 모듈에서는 Oracle Solaris 클라이언트가 호스트 확인 시 DNS를 사용합니다.

1 DNS 서비스를 구성합니다.

자세한 내용은 44 페이지 “DNS 클라이언트를 사용으로 설정하는 방법”을 참조하십시오.

주 – AD 도메인 이름은 domain 지시어를 통해 또는 search 지시어로 지정된 목록의 첫번째 항목으로 지정해야 합니다.

두 지시어가 모두 지정된 경우 마지막 지시어가 우선 적용됩니다. idmap 자동 검색 기능이 제대로 작동하려면 AD 도메인 이름이 필요합니다.

다음 예에서 dig 명령은 이름과 IP 주소를 사용하여 AD 서버인지 결정하기 위해 확인합니다.

```
# dig -x 192.168.11.22 +short
myserver.ad.example
# dig myserver.ad.example +short
192.168.11.22
```

2 hosts의 이름 지정 서비스 목록에 dns를 추가합니다.

```
# svccfg -s svc:/system/name-service/switch
svc:/system/name-service/switch> setprop config/host = astring: "files dns"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch:default> quit
```

주 – 호스트 결정을 위해 nis 또는 ldap 같은 이름 지정 서비스를 추가로 포함하려면 dns 뒤에 추가하십시오.

---

3 DNS 서비스가 사용으로 설정되고 온라인 상태인지 확인합니다.

예를 들면 다음과 같습니다.

```
# svcs svc:/network/dns/client
STATE STIME FMRI
online Oct_14 svc:/network/dns/client:default
```

4 kclient 유틸리티를 사용하여 시스템을 AD 도메인에 연결합니다.

예를 들면 다음과 같습니다.

```
# /usr/sbin/kclient -T ms_ad
```

5 password 및 group의 이름 지정 서비스 목록에 ad를 추가합니다.

```
# svccfg -s svc:/system/name-service/switch
svc:/system/name-service/switch> setprop config/password = astring: "files nis ad"
svc:/system/name-service/switch> setprop config/group = astring: "files nis ad"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch:default> quit
```

6 idmap 서비스를 사용으로 설정합니다.

```
# svcadm enable idmap
```

7 이름 서비스 스위치 서비스의 SMF 저장소를 업데이트합니다.

```
# svcadm refresh name-service/switch
```

주 – 필요한 경우 이름 서비스 스위치를 새로 고칠 때마다 nscd 모듈이 자동으로 다시 시작됩니다.

---

8 AD에서 user 및 group 정보에 액세스할 수 있는지 확인합니다.

예를 들면 다음과 같습니다.

```
# getent passwd 'test_user@example'
test_user@example:x:2154266625:2154266626:test_user::
# getent passwd 2154266625
test_user@example:x:2154266625:2154266626:test_user::
```

암호 업데이트

passwd(4) 매뉴얼 페이지에는 이름 서비스 스위치의 config/passwd 등록 정보에 유효한 형식 목록이 포함되어 있습니다. 이러한 구성에 ad를 추가할 수 있습니다. 하지만 passwd 명령을 통해 AD 사용자 암호를 변경할 수는 없습니다. 암호를 업데이트하는 동안 passwd 항목에서 발견된 ad는 건너뜁니다. AD 사용자 암호를 업데이트하려면 kpasswd 명령을 사용합니다.

이름 서비스 스위치의 유효한 기존 password 및 group 항목에 ad 검색 순서를 추가할 수 있습니다. 예를 들면 다음과 같습니다.

```
# svccfg -s svc:/system/name-service/switch
svc:/system/name-service/switch> setprop config/password = astring: "files nis ad"
svc:/system/name-service/switch> setprop config/group = astring: "files nis ad"
svc:/system/name-service/switch> select system/name-service/switch:default
svc:/system/name-service/switch:default> refresh
svc:/system/name-service/switch:default> quit
```

nss_ad 이름 지정 서비스 모듈이 AD에서 데이터를 검색하는 방법

다음 절에서는 nss_ad 모듈이 AD에서 해당 데이터를 검색하여 passwd, shadow 및 group 파일에 대한 이름 지정 서비스 요청을 확인하는 방법에 대해 설명합니다.

passwd 정보 검색

다음 구문은 passwd 항목의 올바른 형식을 보여 줍니다.

username:*password*:*uid*:*gid*:*gecos*:*home-directory*:*login-shell*

자세한 내용은 passwd(4) 매뉴얼 페이지를 참조하십시오.

nss_ad 모듈은 다음과 같이 AD에서 passwd 정보를 검색합니다.

- *username* – 이 필드는 samAccountName AD 속성의 값을 사용하며 객체가 상주하는 도메인 이름으로 정규화됩니다(예: terryb@example.com).
- *password* – AD 객체에서 사용자 암호를 사용할 수 없기 때문에 이 필드는 x 값을 사용합니다.
- *uid* – 이 필드는 objectSID AD 속성의 Windows 사용자 SID를 사용합니다. SID는 idmap 서비스를 사용하여 UID에 매핑됩니다.
- *gid* – 이 필드는 Windows 사용자의 기본 그룹 SID를 사용합니다. SID는 idmap 서비스를 사용하여 GID에 매핑됩니다. primaryGroupID AD 속성의 값을 도메인 SID에 추가하여 그룹 SID를 가져옵니다. AD 사용자의 경우 primaryGroupID 속성은 선택적

속성이므로 없을 수도 있습니다. 속성이 없는 경우 nss_ad는 idmap 대각선 매핑 기능을 사용하여 objectSID 속성의 사용자 SID를 매핑합니다.

- *gecos* – CN AD 속성의 값입니다.
- *home-directory* – homeDirectory AD 속성의 값입니다(값이 있는 경우). 그렇지 않으면 이 필드는 비어 있습니다.
- *login-shell* – 고유 AD 스키마에 로그인 셸 속성이 없으므로 이 필드는 비어 있습니다.

shadow 정보 검색

다음 구문에서는 shadow 항목의 올바른 형식을 보여 줍니다.

username:*password*:*lastchg*:*min*:*max*:*warn*:*inactive*:*expire*:*flag*

자세한 내용은 shadow(4) 매뉴얼 페이지를 참조하십시오.

nss_ad 모듈은 다음과 같이 AD에서 shadow 정보를 검색합니다.

- *username* – 이 필드는 samAccountName AD 속성의 값을 사용하며 객체가 상주하는 도메인 이름으로 정규화됩니다(예: terryb@example.com).
- *password* – AD 객체에서 사용자 암호를 사용할 수 없기 때문에 이 필드는 *NP* 값을 사용합니다.

shadow 필드는 AD 및 Kerberos v5와 관련이 없으므로 나머지 shadow 필드는 비어 있습니다.

group 정보 검색

다음 구문에서는 group 항목의 올바른 형식을 보여 줍니다.

groupname:*password*:*gid*:*user-list*

자세한 내용은 group(4) 매뉴얼 페이지를 참조하십시오.

nss_ad 모듈은 다음과 같이 AD에서 정보를 검색합니다.

- *groupname* – 이 필드는 samAccountName AD 속성의 값을 사용하며 객체가 상주하는 도메인 이름으로 정규화됩니다(예: admins@example).
- *password* – Windows 그룹에 암호가 없으므로 이 필드는 비어 있습니다.
- *gid* – 이 필드는 objectSID AD 속성의 Windows 그룹 SID를 사용합니다. SID는 idmap 서비스를 사용하여 GID에 매핑됩니다.
- *user-list* – 이 필드는 비어 있습니다.

제 2 부

NIS 설정 및 관리

이 부분에서는 NIS(네트워크 정보 서비스) 이름 지정 서비스와 Oracle Solaris OS 내의 NIS 설정, 관리 및 문제 해결의 개요를 제공합니다.

◆ ◆ ◆ 5 장

5 네트워크 정보 서비스(개요)

이 장에서는 NIS(네트워크 정보 서비스)의 개요를 제공합니다.

NIS는 분산 이름 지정 서비스입니다. 네트워크 객체와 리소스를 식별하고 찾기 위한 방식입니다. 전송 프로토콜 및 매체 독립적 방식으로 네트워크 전체 정보를 저장하고 검색하는 통합적 방법을 제공합니다.

이 장에서는 다음 내용을 다룹니다.

NIS 소개

NIS를 실행하면 시스템 관리자가 **맵**이라는 관리 데이터베이스를 여러 서버(**마스터** 및 **슬레이브**)에 배포할 수 있습니다. 관리자는 안정적인 자동 방식으로 중앙 위치에서 이러한 데이터베이스를 업데이트하여 모든 클라이언트가 전체 네트워크에서 일관된 방식으로 동일한 이름 지정 서비스 정보를 공유하도록 합니다.

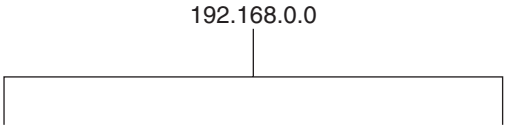
NIS는 DNS와 독립적으로 개발되었으며, 주력하는 부분은 약간 다릅니다. DNS는 숫자 IP 주소 대신 시스템 이름을 사용하여 통신을 더 간소화하는 데 주력하고, NIS는 다양한 네트워크 정보에 대한 중앙집중 제어를 제공하여 네트워크 관리를 더 용이하게 하는 데 주력합니다. NIS는 시스템 이름 및 주소에 대한 정보뿐 아니라 사용자, 네트워크 자체 및 네트워크 서비스에 대한 정보도 저장합니다. 이 네트워크 **정보** 모음을 NIS **이름 공간**이라고 합니다.

주 – 일부 컨텍스트에서 **시스템** 이름은 **호스트** 이름 또는 **시스템** 이름으로 참조됩니다. 여기서는 **시스템**을 사용하지만 일부 화면 메시지나 NIS 맵 이름에서는 **호스트** 또는 **시스템**을 사용할 수 있습니다.

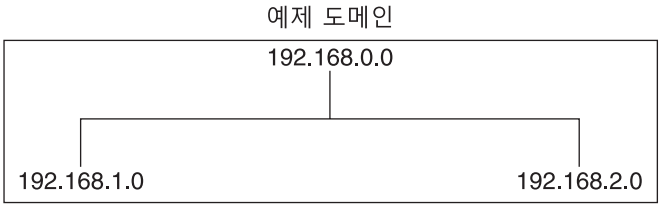
NIS 구조

NIS는 클라이언트-서버 배열을 사용합니다. NIS 서버는 NIS 클라이언트에 서비스를 제공합니다. 주 서버를 **마스터** 서버라고 하며, 안정성을 위해 여러 개의 백업 서버 또는 **슬레이브** 서버를 포함할 수 있습니다. 마스터 및 슬레이브 서버는 모두 NIS 정보 검색 소프트웨어를 사용하고 NIS 맵을 저장합니다.

NIS는 도메인을 사용하여 시스템, 사용자 및 네트워크를 이름 공간에 배열합니다. 그러나 도메인 계층은 사용되지 않습니다. NIS 이름 공간은 플랫입니다.



따라서 이 물리적 네트워크는 NIS 도메인 1개로 배열됩니다.



NIS만 사용하여 NIS 도메인을 인터넷에 직접 연결할 수는 없습니다. 그러나 NIS를 사용하고 인터넷에도 연결하려는 조직은 NIS를 DNS와 함께 사용할 수 있습니다. NIS를 사용하여 모든 로컬 정보를 관리하고 인터넷 호스트 조회 시 DNS를 사용할 수 있습니다. NIS는 NIS 맵에서 정보를 찾을 수 없을 경우 호스트 조회를 DNS로 전달하는 전달 서비스도 제공합니다. 또한 Oracle Solaris 시스템을 사용하면 호스트 조회 요청을 다음과 같은 방식으로 보낼 수 있도록 이름 서비스 스위치 서비스를 설정할 수 있습니다.

- DNS에만 액세스
- DNS에 액세스하지만 DNS에서 호스트를 찾을 수 없을 경우 NIS에 액세스
- NIS에 액세스하지만 NIS에서 호스트를 찾을 수 없을 경우 DNS에 액세스

상호 운용성을 최대화하려면 호스트 조회 시 DNS를 사용하는 것이 좋습니다. 자세한 내용은 2 장, “이름 서비스 스위치(개요)”를 참조하십시오.

NIS 시스템 유형

세 가지 유형의 NIS 시스템이 있습니다.

- 마스터 서버
- 슬레이브 서버
- NIS 서버의 클라이언트

모든 시스템이 NIS 클라이언트가 될 수 있지만 디스크가 있는 시스템만 NIS 서버(마스터 또는 슬레이브)가 되어야 합니다. 보통 서버 자신이 클라이언트가 되기도 합니다.

NIS 서버

NIS 서버는 마스터와 슬레이브라는 두 가지 종류로 제공됩니다. 마스터 서버로 지정된 시스템에는 시스템 관리자가 필요에 따라 만들고 업데이트하는 맵 세트가 있습니다. 각 NIS 도메인에는 성능 저하가 거의 없이 NIS 업데이트를 전파할 수 있는 마스터 서버 1개만 있어야 합니다.

도메인에 추가되는 NIS 서버를 슬레이브 서버로 지정할 수 있습니다. 슬레이브 서버에는 NIS 맵 마스터 세트의 전체 복사본이 있습니다. 마스터 서버 맵을 업데이트할 때마다 업데이트가 슬레이브 서버에 전파됩니다. 슬레이브 서버는 마스터 서버의 요청 오버플로우를 처리하여 “server unavailable”(서버를 이용할 수 없습니다.) 오류를 최소화할 수 있습니다.

일반적으로 시스템 관리자는 모든 NIS 맵에 대해 마스터 서버 1개를 지정합니다. 그러나 각 개별 NIS 맵에 마스터 서버의 시스템 이름이 인코딩되어 있으므로 다른 서버를 각 맵에 대해 마스터 및 슬레이브 서버의 역할을 수행하도록 지정할 수 있습니다. 혼동을 최소화하기 위해, 단일 도메인 내에 만든 모든 맵에 대한 마스터로 단일 서버를 지정합니다. 이 장의 예에서는 한 서버가 도메인의 모든 맵에 대한 마스터라고 가정합니다.

NIS 클라이언트

NIS 클라이언트는 서버에 있는 맵의 데이터를 요청하는 프로세스를 실행합니다. 모든 NIS 서버에 동일한 정보가 있어야 하므로 클라이언트는 마스터 서버와 슬레이브 서버를 구분하지 않습니다.

주 – Oracle Solaris OS는 NIS 클라이언트와 고유 LDAP 클라이언트가 동일한 클라이언트 시스템에서 함께 사용되는 구성을 지원하지 않습니다.

NIS 요소

NIS 이름 지정 서비스는 다음 요소로 구성되어 있습니다.

- 도메인(62 페이지 "NIS 도메인" 참조)
- 데몬(62 페이지 "NIS 데몬" 참조)
- 명령(63 페이지 "NIS 명령" 참조)
- 맵(64 페이지 "NIS 맵" 참조)

NIS 도메인

NIS **도메인**은 공통 NIS 맵 세트를 공유하는 호스트 모음입니다. 각 도메인에는 도메인 이름이 있고, 공통 맵 세트를 공유하는 각 시스템은 해당 도메인에 속합니다.

NIS 도메인과 DNS 도메인이 반드시 같아야 하는 것은 아닙니다. 일부 환경에서는 NIS 도메인이 엔터프라이즈 수준의 네트워크 서브넷 관리 레이아웃에 따라 정의됩니다. DNS 이름과 도메인은 인터넷 DNS 이름 지정 표준과 계층으로 정의됩니다. 두 이름 지정 도메인 이름 지정 시스템이 일치하도록 구성될 수도 있고 그렇지 않을 수도 있습니다. 두 서비스의 도메인 이름은 별도로 제어되며 다르게 구성될 수도 있습니다.

동일한 네트워크나 서브넷에 해당 도메인 맵의 서버가 있기만 하면 모든 호스트가 특정 도메인에 속할 수 있습니다. NIS 도메인 조회는 RPC(원격 프로시저 호출)를 사용합니다. 따라서 NIS에서는 모든 클라이언트와 해당 클라이언트에 직접적인 서비스를 제공하는 모든 서버 시스템이 액세스 가능한 동일한 서브넷에 있어야 합니다. 각 관리 서브넷은 개별 NIS 도메인(엔터프라이즈 수준의 DNS 도메인과는 별도임)으로 관리되는 것이 일반적이지만 공통 마스터 시스템에서 관리되는 공통 데이터베이스를 사용해야 합니다. NIS 도메인 이름과 모든 공유 NIS 구성 정보는 `svc:/network/nis/domain` SMF 서비스를 통해 관리됩니다.

NIS 데몬

NIS 서비스는 다음 표에 나열된 데몬으로 제공됩니다. NIS 서비스는 SMF를 통해 관리됩니다. `svcadm` 명령을 사용하여 사용으로 설정, 사용 안함으로 설정, 다시 시작 등 이 서비스에 대한 관리 작업을 수행할 수 있습니다. SMF 개요는 **Oracle Solaris 11.1에서 서비스 및 결함 관리**의 1 장, "서비스 관리(개요)"를 참조하십시오. 자세한 내용은 `svcadm`(1M) 및 `svcs`(1) 매뉴얼 페이지를 참조하십시오.

표 5–1 NIS 데몬

데몬	기능
nscd	svc:/system/name-service/cache 서비스에서 관리되는 대부분의 이름 서비스 요청에 대한 캐시를 제공하는 클라이언트 서비스
rpc.yppasswdd	svc:/network/nis/passwd 서비스에서 관리되는 NIS 암호 업데이트 데몬 **주 –** rpc.yppasswdd 데몬은 r로 시작하는 모든 셸이 제한된다고 간주합니다. 예를 들어, /bin/rksh에 있는 경우 해당 셸에서 다른 셸로 변경할 수 없습니다. r로 시작하지만 제한되지 않아야 하는 셸이 있는 경우 임시해결책은 8 장, “NIS 문제 해결”을 참조하십시오.
rpc.ypupdated	publickey 등의 다른 맵을 수정하고 svc:/network/nis/update 서비스에서 관리되는 데몬
ypbind	svc:/network/nis/client 서비스에서 관리되는 바인딩 프로세스
ypserv	svc:/network/nis/server 서비스에서 관리되는 서버 프로세스
ypxfrd	svc:/network/nis/xfr 서비스에서 관리되는 고속 맵 전송 데몬

NIS 명령

NIS 서비스는 다음 표에 설명된 여러 명령을 통해 지원됩니다.

표 5–2 NIS 명령 요약

명령	설명
make	/var/yp 디렉토리에서 명령을 실행할 경우 /var/yp/Makefile을 읽어 NIS 맵을 업데이트합니다. make를 사용하여 입력 파일을 기준으로 모든 맵을 업데이트하거나 개별 맵을 업데이트할 수 있습니다. NIS의 make 기능은 ypmake(1M) 매뉴얼 페이지에 설명되어 있습니다.
makedbm	입력 파일을 받아서 dbm.dir 및 dbm.pag 파일로 변환합니다. NIS는 유효한 dbm 파일을 맵으로 사용합니다. makedbm -u를 사용하여 맵을 역어셈블할 수도 있어서 맵을 구성하는 키-값 쌍을 확인할 수 있습니다.
ypcat	NIS 맵의 내용을 표시합니다.
ypinit	입력 파일에서 NIS 서버에 대한 맵을 자동으로 만듭니다. 클라이언트의 초기 /var/yp/binding/ *domain*/ypservers 파일을 생성하는 데도 사용됩니다. 마스터 NIS 서버와 슬레이브 NIS 서버를 처음 설정하려면 ypinit를 사용합니다.
ypmatch	NIS 맵에 하나 이상 지정된 키에 대한 값을 출력합니다. 보고 있는 NIS 서버 맵의 버전을 지정할 수는 없습니다.
yppoll	지정한 서버에서 실행 중인 NIS 맵의 버전을 표시합니다. 또한 맵의 마스터 서버를 나열합니다.

표 5–2 NIS 명령 요약 *(계속)*

명령	설명
yppush	NIS 마스터 서버에서 해당 슬레이브로 NIS 맵의 새 버전을 복사합니다. 마스터 NIS 서버에서 yppush 명령을 실행합니다.
ypset	명명된 NIS 서버에 바인딩하도록 ypbind 프로세스에 지시합니다. 이 명령은 일반적인 용도의 명령이 아니며 보안과 관련이 있으므로 사용하지 않는 것이 좋습니다. ypbind 프로세스의 ypset 및 ypsetme 옵션에 대한 자세한 내용은 ypset(1M) 및 ypbind(1M) 매뉴얼 페이지를 참조하십시오.
ypwhich	현재 클라이언트가 NIS 서비스에 사용 중인 NIS 서버를 표시합니다. -m *mapname* 옵션을 사용하여 호출할 경우 이 명령은 각 맵의 마스터인 NIS 서버를 표시합니다. -m만 사용할 경우 이 명령은 사용 가능한 모든 맵의 이름과 해당 마스터 서버를 표시합니다.
ypxfr	NIS 자체를 전송 매체로 사용하여 원격 서버에서 로컬 /var/yp/*domain* 디렉토리로 NIS 맵을 끌어옵니다. crontab 파일에서 대화식 또는 주기적으로 ypxfr을 실행할 수 있습니다. 전송을 시작하도록 ypserv에서도 호출됩니다.

NIS 맵

NIS 맵의 정보는 ndbm 형식으로 저장됩니다. 맵 파일의 형식은 ypfiles(4) 및 ndbm(3C) 매뉴얼 페이지에 설명되어 있습니다.

NIS 맵은 시스템 네트워크에서 동일한 데이터를 공유할 수 있도록 UNIX /etc 데이터와 passwd, shadow, group 등의 기타 구성 파일에 대한 액세스를 확장합니다. 이러한 파일 공유는 데이터 파일의 관리 업데이트 및 관리를 간소화합니다. NIS는 최소한의 조작으로 간단하게 배포할 수 있습니다. 그러나 대형 엔터프라이즈, 특히 보안 요구 사항이 있는 엔터프라이즈에서는 대신 LDAP 이름 지정 서비스 사용을 고려해야 합니다. NIS 실행 네트워크에서는 각 NIS 도메인의 NIS 마스터 서버가 도메인의 다른 시스템에서 질의할 NIS 맵 세트를 유지 관리합니다. NIS 슬레이브 서버도 마스터 서버 맵의 복제본을 유지 관리합니다. NIS 클라이언트 시스템은 마스터 또는 슬레이브 서버에서 이름 공간 정보를 가져올 수 있습니다.

NIS 맵은 기본적으로 2열 테이블입니다. 한 열은 **키**에 해당되며 다른 열은 키와 관련된 정보입니다. NIS는 키를 통해 검색하여 클라이언트에 대한 정보를 찾습니다. 각 맵이 다른 키를 사용하기 때문에 일부 정보는 여러 맵에 저장됩니다. 예를 들어, 시스템의 이름과 주소는 hosts.byname과 hosts.byaddr의 두 맵에 저장됩니다. 서버에 시스템 이름이 있고 해당 주소를 찾아야 하는 경우 hosts.byname 맵에서 찾습니다. 주소가 있고 이름을 찾아야 하는 경우에는 hosts.byaddr 맵에서 찾습니다.

NIS Makefile은 설치 시 NIS 서버로 지정된 시스템의 /var/yp 디렉토리에 저장됩니다. 해당 디렉토리에서 make를 실행하면 makedbm이 입력 파일에서 기본 NIS 맵을 만들거나 수정합니다.

주 – 슬레이브에서 만든 맵은 마스터 서버로 자동으로 푸시되지 않으므로 항상 마스터 서버에서 맵을 만듭니다.

기본 NIS 맵

Oracle Solaris 시스템에는 기본 NIS 맵 세트가 제공됩니다. 이러한 모든 맵을 사용하거나 일부만 사용할 수 있습니다. NIS는 다른 소프트웨어 제품을 설치할 때 만들거나 추가하는 맵을 사용할 수도 있습니다.

NIS 도메인의 기본 맵은 각 서버의 `/var/yp/`*domain-name* 디렉토리에 있습니다. 예를 들어, `test.com` 도메인에 속하는 맵은 각 서버의 `/var/yp/test.com` 디렉토리에 있습니다.

다음 표에서는 기본 NIS 맵에 대해 설명하고 각 맵에 적합한 소스 파일 이름을 나열합니다.

표 5–3 NIS 맵 설명

맵 이름	해당 소스 파일	설명
`audit_user`	`audit_user`	사용자 감사 사전 선택 데이터를 포함합니다.
`auth_attr`	`auth_attr`	권한 부여 이름과 설명을 포함합니다.
`bootparams`	`bootparams`	부트 중에 클라이언트에 필요한 파일의 경로 이름(root, swap 등)을 포함합니다.
`ethers.byaddr`	`ethers`	시스템 이름과 이더넷 주소를 포함합니다. 이더넷 주소는 맵의 키입니다.
`ethers.byname`	`ethers`	키가 이더넷 주소 대신 시스템 이름이라는 점을 제외하고 `ethers.byaddr`과 동일합니다.
`exec_attr`	`exec_attr`	프로파일 실행 속성을 포함합니다.
`group.bygid`	`group`	그룹 ID를 키로 사용하여 그룹 보안 정보를 포함합니다.
`group.byname`	`group`	그룹 이름을 키로 사용하여 그룹 보안 정보를 포함합니다.
`hosts.byaddr`	`hosts`	IP 주소를 키로 사용하여 시스템 이름과 IP 주소를 포함합니다.
`hosts.byname`	`hosts`	시스템(호스트) 이름을 키로 사용하여 시스템 이름과 IP 주소를 포함합니다.
`mail.aliases`	`aliases`	별칭을 키로 사용하여 별칭과 메일 주소를 포함합니다.
`mail.byaddr`	`aliases`	메일 주소를 키로 사용하여 메일 주소와 별칭을 포함합니다.

표 5–3 NIS 맵 설명 (계속)

맵 이름	해당 소스 파일	설명
netgroup.byhost	netgroup	그룹 이름, 사용자 이름 및 시스템 이름을 포함합니다.
netgroup.byuser	netgroup	키가 사용자 이름이라는 점을 제외하고 netgroup.byhost와 같습니다.
netgroup	netgroup	키가 그룹 이름이라는 점을 제외하고 netgroup.byhost와 같습니다.
netid.byname	passwd, hosts group	UNIX 스타일 인증에 사용됩니다. 시스템 이름과 메일 주소(도메인 이름 포함)를 포함합니다. 사용 가능한 netid 파일이 있는 경우 다른 파일을 통해 제공되는 데이터 외에도 해당 파일이 참조됩니다.
publickey.byname	publickey	보안 RPC에서 사용되는 공개 키 데이터베이스를 포함합니다.
netmasks.byaddr	netmasks	주소를 키로 사용하여 IP 제출 시 사용할 네트워크 마스크를 포함합니다.
networks.byaddr	networks	주소를 키로 사용하여 시스템에 알려진 네트워크 이름과 해당 IP 주소를 포함합니다.
networks.byname	networks	키가 네트워크 이름이라는 점을 제외하고 networks.byaddr과 같습니다.
passwd.adjunct.byname	passwd 및 shadow	C2 클라이언트에 대한 감사 정보와 숨겨진 암호 정보를 포함합니다.
passwd.byname	passwd 및 shadow	사용자 이름을 키로 사용하여 암호 정보를 포함합니다.
passwd.byuid	passwd 및 shadow	키가 사용자 ID라는 점을 제외하고 passwd.byname과 같습니다.
prof_attr	prof_attr	실행 프로파일의 속성을 포함합니다.
protocols.byname	protocols	네트워크에 알려진 네트워크 프로토콜을 포함합니다.
protocols.bynumber	protocols	키가 프로토콜 번호라는 점을 제외하고 protocols.byname과 같습니다.
rpc.bynumber	rpc	시스템에 알려진 RPC의 프로그램 번호와 이름을 포함합니다. 키는 RPC 프로그램 번호입니다.
services.byname	services	네트워크에 알려진 인터넷 서비스를 나열합니다. 키는 포트 또는 프로토콜입니다.

표 5–3 NIS 맵 설명 *(계속)*

맵 이름	해당 소스 파일	설명
services.byservice	services	네트워크에 알려진 인터넷 서비스를 나열합니다. 키는 서비스 이름입니다.
user_attr	user_attr	사용자와 역할의 확장 속성을 포함합니다.
ypservers	해당 없음	네트워크에 알려진 NIS 서버를 나열합니다.

ageing.byname 매핑에는 NIS-to-LDAP 전환이 구현된 경우 yppasswdd 데몬이 암호 에이징 정보를 읽고 DIT(디렉토리 정보 트리)에 쓰는 데 사용하는 정보가 포함되어 있습니다. 암호 에이징이 사용되지 않는 경우 매핑 파일에서 주석 처리할 수 있습니다. NIS-to-LDAP 전환에 대한 자세한 내용은 15 장, “NIS에서 LDAP으로 전환(작업)”을 참조하십시오.

NIS 맵 사용

NIS를 사용하면 /etc 파일 시스템을 사용할 경우보다 훨씬 간단하게 네트워크 데이터베이스를 업데이트할 수 있습니다. 네트워크 환경을 수정할 때마다 더 이상 모든 시스템의 관리 /etc 파일을 변경하지 않아도 됩니다.

그러나 NIS는 /etc 파일 이상의 보안을 추가 제공하지는 않습니다. 네트워크 데이터베이스 액세스 제한, SSL을 사용하여 네트워크를 통해 검색 결과 보내기, Kerberos 보안 검색과 같은 고급 기능 사용 등의 추가 보안이 필요한 경우 LDAP 이름 지정 서비스를 대신 사용해야 합니다.

예를 들어, NIS 실행 네트워크에 새 사용자를 추가하는 경우 마스터 서버에서 입력 파일을 업데이트하고 make 명령을 실행하면 됩니다. 이 명령은 passwd.byname 및 passwd.byuid 맵을 자동으로 업데이트합니다. 이러한 맵은 슬레이브 서버로 전송된 다음 도메인의 모든 클라이언트 시스템과 해당 프로그램에서 사용할 수 있습니다. 클라이언트 시스템 또는 응용 프로그램이 사용자 이름이나 UID를 사용하여 정보를 요청하는 경우 NIS 서버는 passwd.byname 또는 passwd.byuid 맵을 적절하게 참조하고 요청된 정보를 클라이언트에 보냅니다.

ypcat 명령을 사용하여 맵의 값을 표시할 수 있습니다. ypcat 기본 형식은 다음과 같습니다.

```
% ypcat mapname
```

여기서 *mapname*은 검사하려는 맵의 이름 또는 해당 *nickname*입니다. ypservers와 같이 맵이 키로만 구성된 경우 ypcat -k를 사용합니다. 그렇지 않으면 ypcat가 빈 라인을 출력합니다. ypcat에 대한 추가 옵션은 ypcat(1) 매뉴얼 페이지에 설명되어 있습니다.

ypwhich 명령을 사용하여 특정 맵의 마스터인 서버를 확인할 수 있습니다. 다음을 입력합니다.

```
% ypwhich -m mapname
```

여기서 *mapname*은 마스터를 찾으려는 맵의 이름 또는 별명입니다. ypwhich는 마스터 서버의 이름을 표시하여 응답합니다. 자세한 내용은 ypwhich(1) 매뉴얼 페이지를 참조하십시오.

NIS 맵 별명

별명은 전체 맵 이름의 별칭입니다. passwd.byname에 대한 passwd 등 사용 가능한 맵 별명 목록을 가져오려면 ypcat -x 또는 ypwhich -x를 입력합니다.

별명은 맵 별명과 맵의 전체 이름을 공백으로 구분하여 포함하는 /var/yp/nicknames 파일에 저장됩니다. 이 목록에 추가하거나 수정할 수 있습니다. 현재 500개 별명으로 제한됩니다.

NIS 바인딩

NIS 클라이언트는 바인딩 프로세스를 통해 NIS 서버에 연결됩니다. 이 프로세스는 svc:/network/nis/client 및 svc:/network/nis/domain 서비스에서 지원됩니다. NIS 서비스가 작동하려면 이러한 서비스를 사용으로 설정해야 합니다.
svc:/network/nis/client 서비스는 서버 목록 또는 브로드캐스트의 두 가지 모드 중 하나로 작동할 수 있습니다.

- 서버 목록 — 서버 목록 모드에서는 ypbind 프로세스가 svc:/network/nis/domain 서비스에서 도메인의 모든 NIS 서버 이름을 질의합니다. ypbind 프로세스는 이 파일에 있는 서버에만 바인딩합니다.

  svccfg 명령을 사용하여 NIS 서버를 추가할 수 있습니다. NIS 서버는 svc:/network/nis/domain 서비스의 config/ypservers 등록 정보에 추가됩니다. 각 등록 정보 값은 특정 NIS 서버를 나타냅니다.

  또한 NIS 바인딩이 작동하려면 svc:/network/nis/domain 서비스에 지정된 모든 서버 이름에 대한 항목이 /etc/inet/hosts 파일에 포함되어야 합니다.
- 브로드캐스트 — ypbind 프로세스에서 RPC 브로드캐스트를 사용하여 바인딩을 시작할 수도 있습니다. 브로드캐스트는 더 이상 경로 지정되지 않는 로컬 서브넷 이벤트일 뿐이므로 클라이언트와 동일한 서브넷에 최소한 서버(마스터 또는 슬레이브) 1개가 있어야 합니다. 맵 전파는 서브넷 경계를 넘어서도 작동하기 때문에 서버 자체가 서로 다른 하위 네트워크에 있을 수 있습니다. 서브넷 환경에서 한 가지 일반적인 방법은 서브넷 라우터를 NIS 서버로 만드는 것입니다. 이렇게 하면 도메인 서버가 서브넷 인터페이스의 클라이언트에 서비스를 제공할 수 있습니다.

  일반적으로 브로드캐스트 모드가 권장되는 작업 모드입니다. 브로드캐스트 모드에서는 추가 호스트 항목을 지정하거나 /etc/inet/hosts를 변경할 필요가 없습니다.

일반적으로 클라이언트가 서버에 바인딩된 후에는 바인딩이 변경될 때까지 해당 서버에 바인딩된 상태로 유지됩니다. 예를 들어, 서버의 서비스가 중단되면 해당 서버에서 서비스를 제공받던 클라이언트가 새 서버에 바인딩됩니다.

현재 특정 클라이언트에 서비스를 제공 중인 NIS 서버를 확인하려면 다음 명령을 사용합니다.

```
% ypwhich machinename
```

여기서 *machinename*은 클라이언트 이름입니다. 시스템 이름을 언급하지 않으면 `ypwhich` 명령은 기본적으로 로컬 시스템(즉, 명령이 실행된 시스템)으로 설정됩니다.

서버 목록 모드

서버 목록 모드의 바인딩 프로세스는 다음과 같이 작동합니다.

1. NIS 맵에서 제공하는 정보가 필요한 NIS 클라이언트 시스템에서 실행 중인 프로그램이 서버 이름에 대해 `ypbind`를 요청합니다.
2. `ypbind` 데몬이 `/var/yp/binding/`*domainname*`/ypservers` 파일에서 도메인의 NIS 서버 목록을 찾습니다.
3. `ypbind` 데몬이 목록의 첫번째 서버에 대한 바인딩을 시작합니다. 서버가 응답하지 않을 경우 `ypbind`는 서버를 찾거나 목록이 끝날 때까지 그 다음 서버를 시도합니다.
4. `ypbind` 데몬이 클라이언트 프로세스에 통신할 서버를 알립니다. 그러면 클라이언트가 요청을 서버에 직접 보냅니다.
5. NIS 서버의 `ypserv` 데몬이 적절한 맵을 참조하여 요청을 처리합니다.
6. `ypserv` 데몬이 요청된 정보를 다시 클라이언트에 보냅니다.

브로드캐스트 모드

브로드캐스트 모드 바인딩 프로세스는 다음과 같이 작동합니다.

1. 브로드캐스트 옵션을 설정하여(`broadcast`) `ypbind` 데몬을 시작해야 합니다.
2. `ypbind` 데몬이 NIS 서버를 찾기 위해 RPC 브로드캐스트를 실행합니다.

주 – 이러한 클라이언트를 지원하려면 NIS 서비스가 필요한 각 서브넷에 NIS 서버가 있어야 합니다.

---

3. `ypbind` 데몬이 브로드캐스트에 응답하는 첫번째 서버에 대한 바인딩을 시작합니다.
4. `ypbind` 데몬이 클라이언트 프로세스에 통신할 서버를 알립니다. 그러면 클라이언트가 요청을 서버에 직접 보냅니다.
5. NIS 서버의 `ypserv` 데몬이 적절한 맵을 참조하여 요청을 처리합니다.
6. `ypserv` 데몬이 요청된 정보를 다시 클라이언트에 보냅니다.

◆ ◆ ◆ 6 장

6 NIS 설정 및 구성(작업)

이 장에서는 NIS(네트워크 정보 서비스)의 초기 설정과 구성에 대해 설명합니다.

주 – 일부 컨텍스트에서 **시스템** 이름은 **호스트** 이름 또는 **시스템** 이름으로 참조됩니다. 여기서는 "시스템"을 사용하지만 일부 화면 메시지나 NIS 맵 이름에서는 **호스트** 또는 **시스템**을 사용할 수 있습니다.

이 장에서는 다음 내용을 다룹니다.

NIS 작업 맵 구성

작업	설명	지침
변환할 소스 파일을 준비합니다.	NIS 맵을 작성하기 전에 로컬 `/etc` 파일을 정리합니다.	75 페이지 "변환할 소스 파일을 준비하는 방법"
마스터 서버를 설정합니다.	NIS 정보의 주 소스인 마스터 서버를 만듭니다.	78 페이지 "마스터 서버를 설정하는 방법"
마스터 서버에서 NIS를 시작합니다.	NIS 서버에서 NIS 정보 제공을 시작합니다.	80 페이지 "NIS 서버에서 NIS 서비스 시작 및 중지"

작업	설명	지침
슬레이브 서버를 설정합니다.	NIS 정보의 보조 소스인 슬레이브 서버를 만듭니다.	83 페이지 “슬레이브 서버를 설정하는 방법”
NIS 클라이언트를 설정합니다.	클라이언트가 NIS 정보를 사용할 수 있도록 합니다.	86 페이지 “NIS 클라이언트 관리”

NIS 구성을 시작하기 전에

NIS 이름 공간을 구성하기 전에 다음을 수행해야 합니다.

- NIS 도메인을 계획합니다. 자세한 내용은 73 페이지 “NIS 도메인 계획”을 참조하십시오.
- NIS를 사용할 모든 시스템에 올바르게 구성된 이름 서비스 스위치 정보를 설치합니다. 자세한 내용은 2 장, “이름 서비스 스위치(개요)”를 참조하십시오.

NIS 및 서비스 관리 기능

NIS 서비스는 서비스 관리 기능을 통해 관리됩니다. SMF 개요는 **Oracle Solaris 11.1에서 서비스 및 결함 관리**의 1 장, “서비스 관리(개요)”를 참조하십시오. 자세한 내용은 `svcadm`(1M) 및 `svcs`(1) 매뉴얼 페이지를 참조하십시오.

다음 목록에서는 SMF 서비스를 사용하여 NIS를 관리하는 데 필요한 중요한 정보를 간단하게 설명합니다.

- `svcadm` 명령을 사용하여 사용으로 설정, 사용 안함으로 설정, 다시 시작 등 이 서비스에 대한 관리 작업을 수행할 수 있습니다. 그러나 명령줄에서 `ypstart` 및 `ypstop`을 사용하여 NIS를 시작하거나 중지할 수도 있습니다. 자세한 내용은 `ypstart`(1M) 및 `ypstop`(1M) 매뉴얼 페이지를 참조하십시오.

  참고 – `-t` 옵션을 사용하여 서비스를 일시적으로 사용 안함으로 설정하면 서비스 구성이 보호됩니다. `-t` 옵션을 사용하여 서비스를 사용 안함으로 설정하면 재부트 후 서비스에 대한 원래 설정이 복원됩니다. `-t`를 사용하지 않고 서비스를 사용 안함으로 설정하면 재부트 후에도 서비스가 사용 안함으로 유지됩니다.

- NIS FMRI(Fault Manager Resource Identifier)는 다음과 같습니다.
  - NIS 서버의 `svc:/network/nis/server`
  - NIS 클라이언트의 `svc:/network/nis/client`
  - 도메인 이름의 `svc:/network/nis/domain`
- `svcs` 명령을 사용하여 NIS 서비스의 상태를 질의할 수 있습니다.
  - 다음은 `svcs` 명령과 해당 출력의 예입니다.

```
$ svcs network/nis/server
STATE        STIME    FMRI
online       Jan_10   svc:/network/nis/server:default

$ svcs \*nis\*
STATE          STIME    FMRI
online         Oct_09   svc:/network/nis/domain:default
online         Oct_09   svc:/network/nis/client:default
```

- 다음은 svcs - l 명령과 해당 출력의 예입니다.

```
$ svcs -l /network/nis/client
fmri         svc:/network/nis/client:default
name         NIS (YP) client
enabled      true
state        online
next_state   none
state_time   Tue Aug 23 19:23:28 2011
logfile      /var/svc/log/network-nis-client:default.log
restarter    svc:/system/svc/restarter:default
contract_id  88
manifest     /lib/svc/manifest/network/nis/client.xml
manifest     /lib/svc/manifest/network/network-location.xml
manifest     /lib/svc/manifest/system/name-service/upgrade.xml
manifest     /lib/svc/manifest/milestone/config.xml
dependency   require_all/none svc:/system/filesystem/minimal (online)
dependency   require_all/restart svc:/network/rpc/bind (online)
dependency   require_all/restart svc:/network/nis/domain (online)
dependency   optional_all/none svc:/network/nis/server (absent)
dependency   optional_all/none svc:/network/location:default (online)
dependency   optional_all/none svc:/system/name-service/upgrade (online)
dependency   optional_all/none svc:/milestone/config (online)
dependency   optional_all/none svc:/system/manifest-import (online)
dependency   require_all/none svc:/milestone/unconfig (online)
```

- svccfg 유틸리티를 사용하여 서비스에 대한 자세한 정보를 얻을 수 있습니다. svccfg(1M) 매뉴얼 페이지를 참조하십시오.
- ps 명령을 사용하여 데몬의 존재를 확인할 수 있습니다.

```
$ ps -ef |grep ypbind
daemon 100813   1   0   Aug 23 ?     0:00 /usr/lib/netsvc/yp/ypbind -broadcast
```

NIS 도메인 계획

시스템을 NIS 서버 또는 클라이언트로 구성하기 전에 NIS 도메인을 계획해야 합니다.

NIS 도메인에 포함할 시스템을 결정합니다. NIS 도메인에서 DNS 도메인을 미러링할 필요는 없습니다. DNS 도메인에는 NIS 도메인이 2개 이상 있을 수 있고, NIS 도메인 외부에 있는 DNS 도메인에 시스템이 존재할 수 있습니다.

NIS 도메인 이름은 256자일 수 있습니다. 도메인 이름은 32자 이내로 제한하는 것이 좋습니다. NIS 도메인 이름은 대소문자를 구분합니다. 편의상 인터넷 도메인 이름을 NIS 도메인 이름의 기초로 사용할 수 있습니다. NIS 도메인 이름에 대문자가 있는데 DNS 이름에는 없는 경우 사용자에게 혼동을 줄 수도 있습니다. 예를 들어, 인터넷 도메인

이름이 example.com인 경우 NIS 도메인 이름을 example.com으로 지정할 수도 있습니다. example.com을 NIS 도메인 2개(예: 영업 부서와 제조 부서에 대해 각각 하나씩)로 나누려는 경우 한 도메인 이름은 sales.example.com, 다른 도메인 이름은 manf.example.com으로 지정할 수 있습니다.

주 – 분할된 NIS 도메인을 병합하고 관리하기 어려울 수 있으므로 NIS 도메인을 분할할 명확한 이유가 있어야 합니다.

시스템이 NIS 서비스를 사용할 수 있으려면 올바른 NIS 도메인 이름과 시스템 이름을 설정해야 합니다. 시스템 이름은 hostname 명령으로 설정합니다. 시스템의 도메인 이름은 domainname 명령으로 설정합니다. hostname 및 domainname 명령을 사용하여 시스템 이름과 NIS 도메인 이름을 표시할 수 있습니다.

NIS 서버 및 클라이언트 식별

마스터 서버로 사용할 시스템 1개를 선택합니다. 슬레이브 서버로 사용할 시스템을 결정합니다.

NIS 클라이언트로 사용할 시스템을 결정합니다. 필수는 아니지만, 일반적으로 NIS 도메인의 모든 시스템이 NIS 클라이언트로 설정됩니다.

마스터 서버 준비

다음 절에서는 마스터 서버에 대한 소스 파일과 passwd 파일을 준비하는 방법에 대해 설명합니다.

소스 파일 디렉토리

소스 파일은 대체로 마스터 서버의 /etc 디렉토리에 있습니다. 그러나 /etc에 그대로 두면 맵의 내용이 마스터 서버의 로컬 파일 내용과 동일하기 때문에 바람직하지 않습니다. 모든 사용자가 마스터 서버 맵에 액세스할 수 있고 root 암호가 passwd 맵을 통해 모든 NIS 클라이언트에 전달되기 때문에 passwd 및 shadow의 경우 특히 문제가 됩니다. 자세한 내용은 75 페이지 “passwd 파일 및 이름 공간 보안”을 참조하십시오.

그러나 다른 디렉토리에 소스 파일을 배치하는 경우 DIR=/etc 라인을 DIR=/ *your-choice*로 변경하여 /var/yp의 Makefile을 수정해야 합니다. 여기서 *your-choice*는 소스 파일을 저장하는 데 사용할 디렉토리의 이름입니다. 이렇게 하면 서버의 로컬 파일을 클라이언트의 파일처럼 처리할 수 있습니다. 먼저 원본 Makefile의 복사본을 저장하는 것이 좋습니다.

또한 기본값이 아닌 디렉토리에서 audit_user, auth_attr, exec_attr 및 prof_attr NIS 맵을 만들어야 합니다. RBACDIR =*/etc/security*를 *RBACDIR=/your-choice*로 변경하여 /var/yp/Makefile을 수정합니다.

passwd 파일 및 이름 공간 보안

보안상, 권한 없는 루트 액세스를 방지하기 위해 NIS 암호 맵을 작성하는 데 사용되는 파일에는 root에 대한 항목을 포함하면 안됩니다. 따라서 마스터 서버의 /etc 디렉토리에 있는 파일에서 암호 맵을 작성하면 안됩니다. 암호 맵을 작성하는 데 사용되는 암호 파일에서 root 항목을 제거하고 허용되지 않은 액세스로부터 보호할 수 있는 디렉토리에 배치해야 합니다.

예를 들어, 파일 자체가 다른 파일에 대한 링크가 아니거나 해당 위치가 Makefile에 지정된 경우 마스터 서버 암호 입력 파일을 /var/yp 등의 디렉토리나 선택한 모든 디렉토리에 저장해야 합니다. Makefile에 지정된 구성에 따라 올바른 디렉토리 옵션이 자동으로 설정됩니다.

주의 – PWDDIR에 지정된 디렉토리의 passwd 파일에 root에 대한 항목이 포함되지 않도록 합니다.

소스 파일이 /etc 이외의 디렉토리에 있는 경우 passwd 및 shadow 파일이 있는 디렉토리를 참조하도록 /var/yp/Makefile의 PWDIR 암호 매크로를 변경해야 합니다. PWDIR=/etc 라인을 PWDIR=/ *your-choice*로 변경합니다. 여기서 *your-choice*는 passwd 맵 소스 파일을 저장하는 데 사용할 디렉토리의 이름입니다.

▼ 변환할 소스 파일을 준비하는 방법

이 절차에서는 NIS 맵으로 변환할 소스 파일을 준비하는 방법에 대해 설명합니다.

1. **관리자로 전환합니다.**
   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2. **마스터 서버의 소스 파일을 검사하여 시스템이 반영되는지 확인합니다.**
   다음 파일을 확인합니다.

   - audit_user
   - auth_attr
   - auto.home 또는 auto_home
   - auto.master 또는 auto_master
   - bootparams

- ethers
- exec_attr
- group
- hosts
- ipnodes
- netgroup
- netmasks
- networks
- passwd
- protocols
- rpc
- service
- shadow
- user_attr

3 **passwd 및 shadow를 제외하고 이러한 소스 파일을 모두 선택한 소스 디렉토리에 복사합니다.**

소스 디렉토리는 DIR 매크로에 의해 /var/yp/Makefile에서 정의됩니다.

4 **passwd 및 shadow 파일을 선택한 암호 소스 디렉토리에 복사합니다.**

암호 소스 디렉토리는 PWDIR 매크로에 의해 Makefile에서 정의됩니다.

5 **audit_user, auth_attr, exec_attr 및 prof_attr 파일을 선택한 RBAC 소스 디렉토리에 복사합니다.**

RBAC 소스 디렉토리는 RBACDIR 매크로에 의해 /var/yp/Makefile에서 정의됩니다. 원하는 경우 복사하기 전에 /etc/security/auth_attr.d 디렉토리에 있는 파일 내용을 auth_attr 파일의 복사본에 병합합니다. 마찬가지로, 원하는 경우 exec_attr.d 및 prof_attr.d 디렉토리에 있는 파일을 exec_attr 및 prof_attr과 결합합니다.

주의 – 시스템을 업그레이드할 때마다 이러한 파일을 다시 병합해야 하므로 /etc/security/*.d 디렉토리의 릴리스 파일과 로컬 파일을 별도로 유지합니다.

6 **/etc/mail/aliases 파일을 확인합니다.**

다른 소스 파일과 달리, /etc/mail/aliases 파일은 다른 디렉토리로 이동할 수 없습니다. 이 파일은 /etc/mail 디렉토리에 있어야 합니다. 자세한 내용은 aliases(4) 매뉴얼 페이지를 참조하십시오.

주 – /var/yp/Makefile의 ALIASES = /etc/mail/aliases 항목에서 다른 위치를 가리켜 NIS 관련 메일 별칭 파일을 추가할 수 있습니다. make 명령을 실행하면 ALIASES 항목은 mail.aliases 맵을 만듭니다. /etc/nsswitch.conf 파일이 files 외에도 nis를 올바르게 대상으로 지정하는 경우 sendmail 서비스는 /etc/mail/aliases 파일은 물론 이 맵도 사용합니다. 96 페이지 "/var/yp/Makefile 수정 및 사용"을 참조하십시오.

7 **소스 파일에서 모든 주석과 기타 관련 없는 라인과 정보를 정리합니다.**

sed 또는 awk 스크립트를 통해 또는 텍스트 편집기를 사용하여 이러한 작업을 수행할 수 있습니다. /var/yp/Makefile은 일부 파일 정리를 자동으로 수행하지만 make 명령을 실행하기 전에 수동으로 이러한 파일을 검사하고 정리하는 것이 좋습니다.

8 **모든 소스 파일의 데이터 형식이 올바른지 확인합니다.**

소스 파일 데이터는 해당 특정 파일에 올바른 형식이어야 합니다. 여러 파일의 매뉴얼 페이지를 참조하여 각 파일이 올바른 형식인지 확인합니다.

/var/yp/Makefile 준비

소스 파일을 검사하고 소스 파일 디렉토리로 복사한 후 이제 소스 파일을 NIS 서비스에서 사용되는 ndbm 형식 맵으로 변환해야 합니다. 78 페이지 "마스터 서버를 설정하는 방법"에 설명된 대로 마스터 서버에서 호출하면 ypinit에서 자동으로 이 작업을 수행합니다.

ypinit 스크립트는 /var/yp/Makefile을 사용하는 make 프로그램을 호출합니다. 기본 파일 복사본은 /var/yp 디렉토리에 제공되며 소스 파일을 원하는 ndbm 형식 맵으로 변환하는 데 필요한 명령을 포함합니다.

기본 Makefile을 그대로 사용하거나 수정할 수 있습니다. 기본 Makefile을 수정하는 경우 나중에 필요한 경우를 위해 원래 기본 Makefile을 먼저 복사하고 저장해야 합니다. Makefile에 대해 다음 수정 작업 중 하나 이상을 수행해야 할 수도 있습니다.

- **기본 맵이 아닌 맵**

  기본 파일이 아닌 소스 파일을 만들었으며 해당 파일을 NIS 맵으로 변환하려는 경우 이러한 소스 파일을 Makefile에 추가해야 합니다.

- **DIR 값**

  74 페이지 "소스 파일 디렉토리"에 설명된 대로 Makefile에서 /etc 이외의 디렉토리에 저장된 소스 파일을 사용하려는 경우 Makefile의 DIR 값을 사용하려는 디렉토리로 변경해야 합니다. Makefile에서 이 값을 변경하는 경우 라인을 들여쓰지 마십시오.

- **PWDIR 값**

  Makefile에서 /etc 이외의 디렉토리에 저장된 passwd, shadow 및 adjunct 소스 파일을 사용하려는 경우 Makefile의 PWDIR 값을 사용하려는 디렉토리로 변경해야 합니다. Makefile에서 이 값을 변경하는 경우 라인을 들여쓰지 마십시오.

- **RBACDIR 값**

  Makefile에서 /etc 이외의 디렉토리에 저장된 audit_user, auth_attr, exec_attr 및 prof_attr 소스 파일을 사용하려는 경우 Makefile의 RBACDIR 값을 사용하려는 디렉토리로 변경해야 합니다. Makefile에서 이 값을 변경하는 경우 라인을 들여쓰지 마십시오.

- **도메인 이름 분석기**

  NIS 서버에서 현재 도메인에 없는 시스템에 도메인 이름 분석기 사용하려는 경우 Makefile의 B= 라인을 주석 처리하고 B=- b 라인의 주석 처리를 해제합니다.

Makefile의 기능은 all 아래에 나열된 각 데이터베이스에 적합한 NIS 맵을 만드는 것입니다. makedbm을 통과한 후 mapname.dir 및 mapname.pag의 두 파일에 데이터가 수집됩니다. 두 파일은 마스터 서버의 /var/yp/*domainname* 디렉토리에 있습니다.

Makefile은 /PWDIR/passwd, /PWDIR/shadow 및 /PWDIR/security/passwd.adjunct 파일에서 passwd 맵을 적절하게 작성합니다.

▼ NIS 마스터 서버 패키지를 설치하는 방법

일반적으로 NIS 마스터 서버 패키지는 필요한 경우 Oracle Solaris 릴리스와 함께 설치됩니다. 시스템을 설치할 때 패키지가 포함되지 않은 경우 다음 절차에 따라 패키지를 설치합니다.

1. **관리자로 전환합니다.**

   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2. **NIS 마스터 서버 패키지를 설치합니다.**

```
# pkg install pkg:/service/network/nis
```

▼ 마스터 서버를 설정하는 방법

ypinit 스크립트는 마스터 서버 및 슬레이브 서버와 NIS를 사용할 클라이언트를 설정합니다. 또한 초기에 make 명령을 사용하여 마스터 서버에 맵을 만듭니다.

ypinit 명령을 사용하여 마스터 서버에 새로운 NIS 맵 세트를 작성하려면 다음 절차를 완료합니다.

1. **NIS 마스터 서버의 관리자로 전환합니다.**

   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 /etc/inet/hosts 파일을 편집합니다.

각 NIS 서버의 호스트 이름 및 IP 주소를 추가합니다. *IPaddress FQDN-hostname aliases* 형식을 사용합니다.

예를 들면 다음과 같습니다.

```
129.0.0.1    master.example.com master
129.0.0.2    slave1.example.com slave1
129.0.0.3    slave2.example.com slave2
```

3 마스터 서버에서 새 맵을 작성합니다.

```
# /usr/sbin/ypinit -m
```

4 NIS 서버의 이름을 입력합니다.

ypinit가 NIS 슬레이브 서버로 사용할 다른 시스템 목록을 묻는 메시지를 표시하면 작업 중인 서버의 이름을 /etc/inet/hosts 파일에서 지정한 NIS 슬레이브 서버의 이름과 함께 입력합니다.

5 NIS 도메인 이름이 설정되었는지 확인합니다.

```
# domainname
example.com
```

6 y를 입력하여 치명적이지 않은 오류가 발생할 경우 프로세스를 중지합니다.

ypinit에서 치명적이지 않은 첫번째 오류가 발생할 때 절차를 종료할지, 아니면 치명적이지 않은 오류에 관계없이 계속할지 물을 경우 **y**를 입력합니다. **y**를 선택하면 첫번째 문제가 발생할 때 ypinit가 종료됩니다. 그런 다음 문제를 해결하고 ypinit를 다시 시작할 수 있습니다. ypinit를 처음 실행 중인 경우에 권장됩니다. 계속하려는 경우 발생하는 모든 문제를 수동으로 해결한 다음 ypinit를 다시 시작할 수 있습니다.

주 – 맵 파일 중 일부가 없으면 치명적이지 않은 오류가 발생할 수 있습니다. 이것은 NIS 작동에 영향을 주는 오류가 아닙니다. 자동으로 생성되지 않은 경우 수동으로 맵을 추가해야 할 수도 있습니다. 모든 기본 NIS 맵에 대한 설명은 65 페이지 “기본 NIS 맵”을 참조하십시오.

---

7 소스 파일을 삭제해야 하는지 여부를 선택합니다.

ypinit 명령은 /var/yp/*domain-name* 디렉토리의 기존 파일을 삭제할 수 있는지 여부를 묻습니다. 이 메시지는 NIS가 이전에 설치된 경우에만 표시됩니다. 일반적으로 이전 설치의 파일을 정리하려는 경우 소스 파일을 삭제하도록 선택합니다.

8 ypinit 명령이 서버 목록을 생성한 후 make 명령을 호출합니다.

이 프로그램은 /var/yp에 있는 Makefile(기본 파일 또는 수정한 파일)에 포함된 지침을 사용합니다. make 명령은 지정한 파일에서 나머지 주석 라인을 정리합니다. 또한 파일에서 makedbm을 실행하여 적절한 맵을 만들고 각 맵에 대한 마스터 서버의 이름을 설정합니다.

Makefile에 의해 푸시되는 맵이 마스터의 domainname 명령에 의해 반환된 것과 다른 도메인에 해당하는 경우 다음과 같이 DOM 변수의 올바른 ID로 ypinit 셸 스크립트에서 make를 시작하여 올바른 도메인으로 푸시되도록 할 수 있습니다.

```
# make DOM=domain-name passwd
```

이 명령은 마스터가 속하는 도메인이 아니라 의도한 도메인으로 passwd 맵을 푸시합니다.

9 **필요한 경우 이름 서비스 스위치를 변경합니다.**

36 페이지 "이름 서비스 스위치 관리"를 참조하십시오.

▼ 한 마스터 서버에서 여러 NIS 도메인을 지원하는 방법

일반적으로 NIS 마스터 서버는 NIS 도메인 1개만 지원합니다. 그러나 마스터 서버를 사용하여 다중 도메인을 지원 중인 경우 추가 도메인에 서비스를 제공하도록 서버를 설정할 때 78 페이지 "마스터 서버를 설정하는 방법"에 설명된 대로 단계를 약간 수정해야 합니다.

1 **NIS 마스터 서버의 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **NIS 도메인 이름을 변경합니다.**

```
# domainname sales.example.com
```

3 **NIS 파일을 작성합니다.**

```
# make DOM=sales.example.com
```

NIS 서버에서 NIS 서비스 시작 및 중지

이제 마스터 맵이 생성되었으므로 마스터 서버에서 NIS 데몬을 시작하고 서비스를 시작할 수 있습니다. NIS 서비스를 사용으로 설정하면 ypserv 및 ypbind 데몬이 서버에서 시작됩니다. 클라이언트가 서버의 정보를 요청할 경우 NIS 맵에서 조회하여 클라이언트의 정보 요청에 응답하는 데몬은 ypserv입니다. ypserv 및 ypbind 데몬은 하나의 단위로 관리됩니다.

다음은 서버에서 NIS 서비스를 시작하거나 중지할 수 있는 세 가지 방법입니다.

- NIS 서비스가 이전에 사용으로 설정된 경우 부트 프로세스 중에 SMF 서비스가 NIS 서비스를 자동으로 시작합니다.
- 기본 수동 방법은 svcadm enable *fmri* 및 svcadm disable *fmri* 명령을 사용하는 것입니다.

- SMF를 사용하여 NIS 서비스를 관리할 수 있도록 `svcadm` 명령을 사용하는 것이 좋지만 `ypstart` 및 `ypstop` 명령도 다른 수동 방법을 제공합니다.

자동으로 NIS 서비스 시작

`svc:/network/nis/server` 서비스가 사용으로 설정된 경우 부트 시 `ypserv` 데몬이 자동으로 시작됩니다. 자세한 내용은 78 페이지 "마스터 서버를 설정하는 방법"을 참조하십시오.

▼ 수동으로 NIS 서버 서비스를 사용으로 설정하는 방법

`svcadm` 명령을 사용할 때는 서비스 인스턴스를 2개 이상 실행 중인 경우에만 인스턴스 이름이 필요합니다. 자세한 내용은 72 페이지 "NIS 및 서비스 관리 기능" 또는 `svcadm(1M)` 매뉴얼 페이지를 참조하십시오.

1. **관리자로 전환합니다.**

   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2. **필요한 NIS 서버 서비스를 시작합니다.**

```
# svcadm enable network/nis/domain
# svcadm enable network/nis/server
```

주 – `svcadm` 명령이 기본 방법이지만 `ypstart` 명령을 사용하여 NIS 서비스를 사용으로 설정할 수도 있습니다.

▼ NIS 서버 서비스를 사용 안함으로 설정하는 방법

`svcadm` 명령을 사용할 때는 특정 서비스 인스턴스를 2개 이상 실행 중인 경우에만 인스턴스 이름이 필요합니다. 자세한 내용은 72 페이지 "NIS 및 서비스 관리 기능" 또는 `svcadm(1M)` 매뉴얼 페이지를 참조하십시오.

1. **관리자로 전환합니다.**

   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2. **필요한 NIS 서버 서비스를 사용 안함으로 설정합니다.**

```
# svcadm disable network/nis/domain
# svcadm disable network/nis/server
```

주 – `ypstop` 명령을 사용하여 NIS 서비스를 사용 안함으로 설정할 수도 있습니다.

▼ NIS 서버 서비스를 새로 고치는 방법

이 절차에서는 구성이 변경된 후 NIS 서버서비스를 새로 고치는 방법에 대해 설명합니다.

`svcadm` 명령을 사용할 때는 특정 서비스 인스턴스를 2개 이상 실행 중인 경우에만 인스턴스 이름이 필요합니다. 자세한 내용은 72 페이지 “NIS 및 서비스 관리 기능” 또는 `svcadm(1M)` 매뉴얼 페이지를 참조하십시오.

1. **관리자로 전환합니다.**

   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 “지정된 관리 권한을 사용하는 방법”을 참조하십시오.

2. **필요한 NIS 서버 서비스를 새로 고칩니다.**

```
# svcadm refresh network/nis/domain
# svcadm refresh network/nis/server
```

NIS 슬레이브 서버 설정

네트워크에 슬레이브 서버가 1개 이상 있을 수 있습니다. 슬레이브 서버를 사용하면 마스터 서버를 사용할 수 없는 경우에도 NIS 서비스를 계속 제공할 수 있습니다.

슬레이브 서버 준비

`ypinit` 명령을 실제로 실행하여 슬레이브 서버를 만들기 전에 먼저 `svc:/network/nis/domain` 서비스가 구성되었는지 확인합니다.

주 – DNS 도메인 이름은 대소문자를 구분하지 않지만 NIS 도메인 이름은 대소문자를 구분합니다.

NIS 슬레이브 서버를 구성하기 전에 네트워크가 제대로 작동하는지 확인합니다. 특히 `sshd` 명령을 사용하여 마스터 NIS 서버에서 NIS 슬레이브로 파일을 보낼 수 있는지 확인합니다.

▼ 슬레이브 서버를 설정하는 방법

다음 절차에서는 슬레이브 서버를 설정하는 방법에 대해 설명합니다. NIS 슬레이브 서버로 구성하려는 각 시스템에 대해 이 절차를 반복합니다.

1 관리자로 전환합니다.

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 `/etc/inet/hosts` 파일을 편집합니다.

다른 각 NIS 서버의 이름 및 IP 주소를 추가합니다. *IPaddress FQDN-hostname aliases* 형식을 사용합니다.

예를 들면 다음과 같습니다.

```
129.0.0.1    master.example.com master
129.0.0.2    slave1.example.com slave1
129.0.0.3    slave2.example.com slave2
```

3 슬레이브 서버에서 디렉토리를 `/var/yp`로 변경합니다.

주 – 마스터 서버에서 NIS 맵을 처음으로 가져올 수 있도록 먼저 새 슬레이브 서버를 NIS 클라이언트로 구성해야 합니다. 자세한 내용은 86 페이지 "NIS 클라이언트 관리"를 참조하십시오.

---

4 슬레이브 서버를 NIS 클라이언트로 초기화합니다.

```
# /usr/sbin/ypinit -c
```

`ypinit` 명령에서 NIS 서버 목록을 묻는 메시지를 표시합니다. 먼저 작업 중인 로컬 슬레이브의 이름을 입력한 다음 마스터 서버 이름과 도메인의 다른 NIS 슬레이브 서버 이름을 차례로 입력합니다. 다른 슬레이브 서버의 경우 네트워크 측면에서 물리적으로 가장 가까운 서버에서 가장 먼 서버 순서를 따릅니다.

5 클라이언트 서비스가 실행 중인지 확인한 다음 필요에 따라 서비스를 시작하거나 다시 시작합니다.

```
# svcs \*nis\*
STATE          STIME     FMRI
online         20:32:56  svc:/network/nis/domain:default
online         20:32:56  svc:/network/nis/client:default
```

서비스가 `online` 상태로 표시되는 경우 NIS가 실행 중입니다. 서비스 상태가 `disabled`인 경우 NIS가 실행되고 있지 않습니다.

a. 클라이언트 서비스가 실행 중이면 클라이언트 서비스를 다시 시작합니다.

```
# svcadm restart network/nis/domain
# svcadm restart network/nis/client
```

b. **클라이언트 서비스가 실행되고 있지 않으면 클라이언트 서비스를 시작합니다.**

```
# svcadm enable network/nis/domain
# svcadm enable network/nis/client
```

6 **NIS 마스터 서버가 실행 중인지 확인한 다음 필요에 따라 서비스를 시작하거나 다시 시작합니다.**

```
# svcs network/nis/server
STATE          STIME     FMRI
offline        20:32:56  svc:/network/nis/server:default
```

a. **마스터 NIS 서버가 실행 중이면 서비스를 다시 시작합니다.**

```
# svcadm restart network/nis/server
```

b. **마스터 NIS 서버가 실행되고 있지 않으면 서비스를 시작합니다.**

```
# svcadm enable network/nis/server
```

7 **이 시스템을 슬레이브 서버로 초기화합니다.**

```
# /usr/sbin/ypinit -s master
```

여기서 *master*는 기존 NIS 마스터 서버의 시스템 이름입니다.

▼ 슬레이브 서버에서 NIS를 시작하는 방법

다음 절차에서는 슬레이브 서버에서 NIS를 시작하는 방법에 대해 설명합니다.

1 **관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **클라이언트 서비스를 다시 시작하고 모든 NIS 서버 프로세스를 시작합니다.**

```
# svcadm restart network/nis/domain
# svcadm restart network/nis/client
# svcadm enable network/nis/server
```

▼ 새 슬레이브 서버를 추가하는 방법

NIS를 실행한 후 `ypinit` 명령에 지정된 초기 목록에 포함하지 않은 NIS 슬레이브 서버를 만들어야 할 수도 있습니다. 새 NIS 슬레이브 서버를 추가하려면 이 절차를 사용합니다.

1 **NIS 마스터 서버의 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **NIS 도메인 디렉토리로 변경합니다.**

```
# cd /var/yp/domainname
```

3 **ypservers 파일을 역어셈블합니다.**

```
# makedbm -u ypservers >/tmp/temp_file
```

makedbm 명령은 ypservers를 ndbm 형식에서 임시 ASCII 파일 /tmp/temp_file로 변환합니다.

4 **/tmp/temp_file 파일을 편집합니다.**

새 슬레이브 서버의 이름을 서버 목록에 추가합니다. 그런 다음 파일을 저장하고 닫습니다.

5 **temp_file을 입력 파일로 사용하고 ypservers를 출력 파일로 사용하여 makedbm 명령을 실행합니다.**

```
# makedbm /tmp/temp_file ypservers
```

makedbm 명령은 ypservers를 다시 ndbm 형식으로 변환합니다.

6 **ypservers 맵이 올바른지 확인합니다.**

ypservers에 대한 ASCII 파일이 없으므로 슬레이브 서버에서 다음을 입력합니다.

```
slave3# makedbm -u ypservers
```

makedbm 명령은 ypservers의 각 항목을 화면에 표시합니다.

주 – 시스템 이름이 ypservers에 없는 경우 yppush는 이 맵에서 슬레이브 서버 목록을 참조하므로 맵 파일 업데이트를 받지 못합니다.

---

7 **새 NIS 슬레이브 서버의 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

8 **NIS 도메인 이름이 설정되었는지 확인합니다.**

```
# domainname
example.com
```

9 **새 슬레이브 서버의 NIS 도메인 디렉토리를 설정합니다.**

마스터 서버에서 설정된 NIS 맵을 복사한 다음 NIS 클라이언트를 시작합니다. ypinit 명령을 실행하는 경우 프롬프트에 따라 NIS 서버를 원하는 순서대로 나열합니다.

```
slave3# cd /var/yp
slave3# ypinit -c
```

10 **이 시스템을 슬레이브로 초기화합니다.**

```
slave3# /usr/sbin/ypinit -s ypmaster
```

여기서 *ypmaster*는 기존 NIS 마스터 서버의 시스템 이름입니다.

11 NIS 클라이언트로 실행 중인 시스템을 중지합니다.

```
slave3# svcadm disable network/nis/client
```

12 클라이언트 서비스가 실행 중인지 확인한 다음 필요에 따라 서비스를 시작하거나 다시 시작합니다.

```
# svcs \*nis\*
STATE          STIME     FMRI
online         20:32:56  svc:/network/nis/domain:default
online         20:32:56  svc:/network/nis/client:default
```

서비스가 `online` 상태로 표시되는 경우 NIS가 실행 중입니다. 서비스 상태가 `disabled`인 경우 NIS가 실행되고 있지 않습니다.

a. 클라이언트 서비스가 실행 중이면 클라이언트 서비스를 다시 시작합니다.

```
# svcadm restart network/nis/domain
# svcadm restart network/nis/client
```

b. 클라이언트 서비스가 실행되고 있지 않으면 클라이언트 서비스를 시작합니다.

```
# svcadm enable network/nis/domain
# svcadm enable network/nis/client
```

13 NIS 서버가 실행 중인지 확인한 다음 필요에 따라 서비스를 시작하거나 다시 시작합니다.

```
# svcs network/nis/server
STATE          STIME     FMRI
offline        20:32:56  svc:/network/nis/server:default
```

a. NIS 서버가 실행 중이면 서비스를 다시 시작합니다.

```
slave3# svcadm restart network/nis/server
```

b. NIS 서버가 실행되고 있지 않으면 서비스를 시작합니다.

```
slave3# svcadm enable network/nis/server
```

NIS 클라이언트 관리

이 절에서는 NIS를 이름 지정 서비스로 사용하도록 클라이언트 시스템을 구성하는 두 가지 방법에 대해 설명합니다.

주 – Oracle Solaris OS는 NIS 클라이언트와 고유 LDAP 클라이언트가 동일한 클라이언트 시스템에서 함께 사용되는 구성을 지원하지 않습니다.

- **브로드캐스트 방법** — NIS를 사용하도록 클라이언트 시스템을 구성하는 기본 방법입니다. 자세한 내용은 87 페이지 “브로드캐스트 모드에서 NIS 클라이언트를 구성하는 방법”을 참조하십시오.

- **서버 목록 방법** — ypinit 명령으로 서버를 지정하여 클라이언트 시스템을 구성하는 또 다른 방법입니다. 자세한 내용은 87 페이지 "특정 NIS 서버를 사용하여 NIS 클라이언트를 구성하는 방법"을 참조하십시오.

▼ 브로드캐스트 모드에서 NIS 클라이언트를 구성하는 방법

이것은 NIS 클라이언트를 설정하는 기본 방법입니다.

nis/client 서비스를 시작하면 서비스에서 ypbind 명령을 실행하고, 이 명령은 로컬 서브넷에서 NIS 서버를 검색합니다. 서브넷이 있으면 ypbind가 해당 서브넷에 바인딩합니다. 이 검색을 **브로드캐스팅**이라고 합니다. 클라이언트의 로컬 서브넷에 NIS 서버가 없으면 ypbind가 바인딩하지 못하며 클라이언트 시스템이 NIS 서비스에서 이름 공간 데이터를 가져올 수 없습니다. 자세한 내용은 87 페이지 "특정 NIS 서버를 사용하여 NIS 클라이언트를 구성하는 방법"을 참조하십시오.

1. **관리자로 전환합니다.**
   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.
2. **NIS 도메인 이름을 설정합니다.**

   ```
   # domainname example.com
   ```
3. **필요한 경우 이름 서비스 스위치를 변경합니다.**
   36 페이지 "이름 서비스 스위치 관리"를 참조하십시오.
4. **NIS 클라이언트 서비스를 시작합니다.**

   ```
   # svcadm enable network/nis/domain
   # svcadm enable network/nis/client
   ```

▼ 특정 NIS 서버를 사용하여 NIS 클라이언트를 구성하는 방법

시작하기 전에 다음 절차를 수행하려면 3단계에서 입력한 호스트 이름을 DNS로 확인할 수 있어야 합니다. DNS를 사용하지 않거나 IP 주소 대신 호스트 이름을 입력하는 경우 클라이언트의 /etc/hosts 파일에 각 NIS 서버에 적합한 항목을 추가해야 합니다. 자세한 내용은 ypinit(1M) 매뉴얼 페이지를 참조하십시오.

1. **관리자로 전환합니다.**
   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **NIS 도메인 이름을 설정합니다.**

```
# domainname example.com
# svcadm enable network/nis/domain
```

3 **클라이언트 구성 스크립트를 실행합니다.**

```
# ypinit -c
```

클라이언트가 이름 지정 서비스 정보를 가져오는 NIS 서버의 이름을 지정하라는 메시지가 표시됩니다. 마스터 서버와 원하는 개수만큼 슬레이브 서버를 나열할 수 있습니다. 나열하는 서버는 도메인의 모든 위치에 배치될 수 있습니다. 먼저 네트워크 측면에서 시스템에 가장 가까운 서버를 나열한 다음 네트워크에서 더 먼 위치에 있는 서버를 나열하는 것이 좋습니다.

▼ NIS 클라이언트 서비스를 사용 안함으로 설정

1 **관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **NIS 클라이언트 서비스를 사용 안함으로 설정합니다.**

```
# svcadm disable network/nis/domain
# svcadm disable network/nis/client
```

◆ ◆ ◆ 7 장

7 NIS 관리(작업)

이 장에서는 NIS를 관리하는 방법에 대해 설명합니다. 다음 항목을 다룹니다.

주 – NIS 서비스는 서비스 관리 기능을 통해 관리됩니다. `svcadm` 명령을 사용하여 사용으로 설정, 사용 안함으로 설정, 다시 시작 등 이 서비스에 대한 관리 작업을 수행할 수 있습니다. NIS와 함께 SMF를 사용하는 방법에 대한 자세한 내용은 72 페이지 “NIS 및 서비스 관리 기능”을 참조하십시오. SMF 개요는 **Oracle Solaris 11.1에서 서비스 및 결함 관리**의 1 장, “서비스 관리(개요)”를 참조하십시오. 자세한 내용은 `svcadm`(1M) 및 `svcs`(1) 매뉴얼 페이지를 참조하십시오.

`ypstart` 및 `ypstop` 명령을 사용하여 NIS 서비스를 시작하고 중지할 수도 있습니다. 자세한 내용은 `ypstart`(1M) 및 `ypstop`(1M) 매뉴얼 페이지를 참조하십시오.

암호 파일 및 이름 공간 보안

보안을 위해 다음 지침을 따릅니다.

- 마스터 서버의 NIS 맵에 대한 액세스를 제한하는 것이 좋습니다.
- 허용되지 않은 액세스로부터 보호하려면 NIS 암호 맵을 작성하는 데 사용되는 파일에 `root` 항목을 포함하면 안됩니다. 이렇게 하려면 암호 맵을 작성하는 데 사용되는 암호 파일에서 `root` 항목을 제거하고 마스터 서버의 `/etc` 디렉토리가 아닌 디렉토리에 배치해야 합니다. 이 디렉토리는 허용되지 않은 액세스부터 보호해야 합니다.

예를 들어, 파일 자체가 다른 파일에 대한 링크가 아니거나 Makefile에 지정된 경우 마스터 서버 암호 입력 파일을 `/var/yp` 등의 디렉토리나 선택한 모든 디렉토리에 저장할

수 있습니다. 보안 관리 기능이나 ypstart 스크립트를 사용하여 NIS 서비스를 시작하는 경우 Makefile에 지정된 구성에 따라 올바른 디렉토리 옵션이 설정됩니다.

주 – 이전 Solaris 1 버전의 passwd 파일 형식 외에도 이 NIS 구현에서는 NIS 암호 맵 작성을 위한 입력으로 Solaris 2 passwd 및 shadow 파일 형식을 허용합니다.

NIS 사용자 관리

이 절에는 사용자 암호 설정, NIS 도메인에 새 사용자 추가, netgroups에 사용자 지정 등에 대한 정보가 포함되어 있습니다.

▼ NIS 도메인에 새 NIS 사용자를 추가하는 방법

1 NIS 마스터 서버의 관리자로 전환합니다.

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 useradd 명령을 사용하여 새 사용자의 로그인 ID를 만듭니다.

```
# useradd userID
```

여기서 *userID*는 새 사용자의 로그인 ID입니다. 이 명령은 마스터 NIS 서버의 /etc/passwd 및 /etc/shadow 파일에 항목을 만듭니다.

3 새 사용자의 초기 암호를 만듭니다.

새 사용자가 로그인하는 데 사용할 수 있는 초기 암호를 만들려면 passwd 명령을 실행합니다.

```
# passwd userID
```

여기서 *userID*는 새 사용자의 로그인 ID입니다. 이 사용자에게 지정할 암호를 묻는 메시지가 표시됩니다.

이 단계는 useradd 명령으로 만든 암호 항목이 잠겨 있어서 새 사용자가 로그인할 수 없기 때문에 필요합니다. 초기 암호를 지정하여 항목을 잠금 해제합니다.

4 새 항목을 마스터 서버의 passwd 맵 입력 파일에 복사합니다.

마스터 서버의 맵 소스 파일은 /etc 이외의 디렉토리에 있어야 합니다. /etc/passwd 및 /etc/shadow 파일의 새 라인을 서버의 passwd 맵 입력 파일에 복사하여 붙여 넣습니다. 자세한 내용은 89 페이지 "암호 파일 및 이름 공간 보안"을 참조하십시오.

예를 들어, 새 사용자 brown을 추가한 경우 passwd 입력 파일에 복사하는 /etc/passwd의 라인은 다음과 같습니다.

```
brown:x:123:10:User brown:/home/brown:/bin/csh:
```

/etc/shadow에서 복사하는 brown 관련 라인은 다음과 같습니다.

```
brown:$5$YiFpYWXb$6jJkG/gKdfkKtlTbemORnbeH.qsvO9MwBD3ulTihq9B:6445::::::
```

5 **Makefile에서 암호 입력 파일이 있는 디렉토리를 올바르게 지정하는지 확인합니다.**

6 **/etc/passwd 및 /etc/shadow 입력 파일에서 새 사용자 항목을 삭제합니다.**

보안을 위해 NIS 마스터 서버 /etc/passwd 및 /etc/shadow 파일에 사용자 항목을 유지하지 마십시오. 새 사용자에 대한 항목을 다른 디렉토리에 저장된 NIS 맵 소스 파일에 복사한 후 마스터 서버에서 userdel 명령을 사용하여 새 사용자를 삭제합니다.

예를 들어, 마스터 서버의 /etc 파일에서 새 사용자 brown을 삭제하려면 다음을 입력합니다.

```
# userdel brown
```

userdel에 대한 자세한 내용은 userdel(1M) 매뉴얼 페이지를 참조하십시오.

7 **NIS passwd 맵을 업데이트합니다.**

마스터 서버의 passwd 입력 파일을 업데이트한 후 소스 파일이 포함된 디렉토리에서 make를 실행하여 passwd 맵을 업데이트합니다.

```
# userdel brown
# cd /var/yp
# make passwd
```

8 **새 사용자의 로그인 ID에 지정한 초기 암호를 사용자에게 알립니다.**

로그인 후 새 사용자는 언제든지 passwd를 실행하여 다른 암호를 설정할 수 있습니다.

사용자 암호 설정

사용자는 passwd를 실행하여 암호를 변경합니다.

% **passwd** *username*

사용자가 암호를 변경할 수 있으려면 마스터 서버에서 rpc.yppasswdd 데몬을 시작하여 암호 파일을 업데이트해야 합니다.

rpc.yppasswdd 데몬은 마스터 서버에서 자동으로 시작됩니다. rpc.yppasswdd에 -m 옵션을 지정하면 파일 수정 후에 즉시 /var/yp에서 make 명령이 실행됩니다. passwd 파일을 변경할 때마다 make 명령이 실행되지 않도록 하려면 ypstart 스크립트의 rpc.yppasswd 명령에서 -m 옵션을 제거하고 crontab 파일을 통한 passwd 맵의 푸시를 제어합니다.

NIS 넷 그룹

NIS 넷 그룹은 관리를 위해 정의하는 사용자 또는 시스템 그룹(세트)입니다. 예를 들어, 다음을 수행하는 넷 그룹을 만들 수 있습니다.

- 특정 시스템에 액세스할 수 있는 사용자 세트 정의
- 특정 파일 시스템 액세스를 제공할 NFS 클라이언트 시스템 세트 정의
- 특정 NIS 도메인의 모든 시스템에서 관리자 권한이 있는 사용자 세트 정의

각 넷 그룹에 넷 그룹 이름이 지정됩니다. 넷 그룹은 권한이나 액세스 권한을 직접 설정하지 않습니다. 대신 넷 그룹 이름은 일반적으로 사용자 이름이나 시스템 이름이 사용되는 위치에서 다른 NIS 맵에 의해 사용됩니다. 예를 들어, `netadmins`라는 네트워크 관리자 넷 그룹을 만들었다고 가정합니다. `netadmins` 넷 그룹의 모든 구성원에게 특정 시스템에 대한 액세스 권한을 부여하려면 해당 시스템의 `/etc/passwd` 파일에 `netadmin` 항목만 추가하면 됩니다. `/etc/netgroup` 파일에 넷 그룹 이름을 추가하고 NIS `netgroup` 맵으로 전파할 수도 있습니다. 넷 그룹 사용에 대한 자세한 내용은 `netgroup(4)` 매뉴얼 페이지를 참조하십시오.

NIS를 사용하는 네트워크에서 마스터 NIS 서버의 `netgroup` 입력 파일은 `netgroup`, `netgroup.byuser` 및 `netgroup.byhost`의 세 가지 맵을 생성하는 데 사용됩니다. `netgroup` 맵에는 `netgroup` 입력 파일의 기본 정보가 포함됩니다. 시스템 또는 사용자 이름이 지정된 경우 다른 두 NIS 맵에는 넷 그룹 정보 조회를 가속화하는 형식으로 정보가 포함됩니다.

`netgroup` 입력 파일의 항목은 *name ID* 형식을 사용합니다. 여기서 *name*은 넷 그룹에 지정하는 이름이고, *ID*는 넷 그룹에 속하는 시스템 또는 사용자를 식별합니다. 원하는 경우 넷 그룹에 ID(구성원)를 원하는 개수만큼 쉼표로 구분하여 지정할 수 있습니다. 예를 들어, 구성원이 3개인 넷 그룹을 만들려면 `netgroup` 입력 파일 항목이 *name ID*, *ID*, *ID* 형식을 사용합니다. `netgroup` 입력 파일 항목의 구성원 ID는 다음 형식을 사용합니다.

```
([-|machine], [-|user], [domain])
```

여기서 *machine*은 시스템 이름이고, *user*는 사용자 ID이고, *domain*은 시스템 또는 사용자의 NIS 도메인입니다. *domain* 요소는 선택 사항이며, 다른 NIS 도메인의 시스템 또는 사용자를 식별하는 데만 사용해야 합니다. 각 구성원 항목의 *machine* 및 *user* 요소는 필수이지만 대시(-)를 사용하여 null을 나타냅니다. 항목의 시스템 및 사용자 요소 간에는 필요한 관계가 없습니다.

다음은 각각 원격 도메인 `sales`와 `altair` 및 `sirius` 시스템에 있는 사용자 `hauri` 및 `juanita`로 구성된 `admins` 넷 그룹을 만드는 샘플 `netgroup` 입력 파일 항목 2개입니다.

```
admins (altair, hauri), (sirius,juanita,sales)
admins (altair,-), (sirius,-), (-,hauri), (-,juanita,sales)
```

로그인, 원격 마운트, 원격 로그인 및 원격 셸 생성 중 권한 검사를 위해 넷 그룹 NIS 맵을 사용하는 프로그램이 많습니다. 이러한 프로그램에는 `mountd` 및 `login`이 포함됩니다. `login` 명령은 `passwd` 데이터베이스에서 넷 그룹 이름을 발견할 경우 사용자 분류를 위한

넷 그룹 맵을 참조합니다. mountd 데몬은 /etc/dfs/dfstab 파일에서 넷 그룹 이름을 발견할 경우 시스템 분류를 위한 넷 그룹 맵을 참조합니다. 실제로 ruserok 인터페이스를 사용하는 프로그램은 /etc/hosts.equiv 또는 .rhosts 파일에서 넷 그룹 이름을 발견할 경우 시스템 및 사용자 분류를 위한 넷 그룹 맵을 모두 확인합니다.

네트워크에 새 NIS 사용자나 시스템을 추가하는 경우 netgroup 입력 파일의 적절한 넷 그룹에 추가해야 합니다. 그런 다음 make 및 yppush 명령을 사용하여 넷 그룹 맵을 만들고 모든 NIS 서버에 푸시합니다. 넷 그룹 및 넷 그룹 입력 파일 구문에 대한 자세한 내용은 netgroup(4) 매뉴얼 페이지를 참조하십시오.

NIS 맵 작업

이 절에서는 다음 내용을 다룹니다.

맵 정보 가져오기

사용자는 언제든지 ypcat, ypwhich 및 ypmatch 명령을 사용하여 맵 정보를 가져올 수 있습니다. 이후 예에서 *mapname*은 맵의 공식 이름과 해당 별명(있는 경우)을 모두 나타냅니다.

맵의 모든 값을 나열하려면 다음을 입력합니다.

```
% ypcat mapname
```

맵의 키와 값(있는 경우)을 모두 나열하려면 다음을 입력합니다.

```
% ypcat -k mapname
```

모든 맵 별명을 나열하려면 다음 명령 중 하나를 입력합니다.

```
% ypcat -x
% ypmatch -x
% ypwhich -x
```

사용 가능한 모든 맵과 해당 마스터를 나열하려면 다음을 입력합니다.

```
% ypwhich -m
```

특정 맵의 마스터 서버를 나열하려면 다음을 입력합니다.

```
% ypwhich -m mapname
```

키를 맵의 항목과 일치시키려면 다음을 입력합니다.

```
% ypmatch key mapname
```

찾고 있는 항목이 맵의 키가 아닌 경우 다음을 입력합니다.

```
% ypcat mapname | grep item
```

여기서 *item*은 검색 중인 항목에 대한 정보입니다. 다른 도메인에 대한 정보를 가져오려면 이러한 명령의 `-d domainname` 옵션을 사용합니다.

기본값이 아닌 도메인의 정보를 요청 중인 시스템에 요청된 도메인에 대한 바인딩이 없는 경우 `ypbind`는 해당 도메인의 서버 목록에 대해 `/var/yp/binding/`*domainname*`/ypservers` 파일을 참조합니다. 이 파일이 없으면 서버에 대해 RPC 브로드캐스트를 실행합니다. 이 경우 요청 시스템과 동일한 서브넷에 요청된 도메인의 서버가 있어야 합니다.

맵의 마스터 서버 변경

선택한 맵의 마스터 서버를 변경하려면 먼저 새 NIS 마스터에서 맵을 작성해야 합니다. 이전 마스터 서버 이름은 기존 맵에서 키-값 쌍으로 발생하기 때문에(이 쌍은 `makedbm`에 의해 자동으로 삽입됨) `ypxfr`을 사용하여 복사본을 새 마스터로 전송하거나 맵을 새 마스터에 복사하는 것만으로 충분하지 않습니다. 키를 새 마스터 서버 이름과 다시 연결해야 합니다. 맵에 ASCII 소스 파일이 있는 경우 이 파일을 새 마스터에 복사해야 합니다.

▼ 맵의 마스터 서버를 변경하는 방법

1. **NIS 마스터 서버의 관리자로 전환합니다.**
   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2. **디렉토리를 변경합니다.**

   ```
   newmaster# cd /var/yp
   ```

3. **작성할 맵을 지정하기 전에 `/var/yp/Makefile`에 새 맵에 대한 항목이 있어야 합니다.**
   그렇지 않은 경우 지금 `Makefile`을 편집합니다. 이 예에서는 `sites.byname` 맵의 항목을 추가합니다.

4. **맵을 업데이트하거나 다시 만들려면 다음을 입력합니다.**

   ```
   newmaster# make sites.byname
   ```

5 이전 마스터가 NIS 서버로 유지되는 경우 이전 마스터에 원격 로그인(ssh)하고 /var/yp/Makefile을 편집합니다.

sites.byname 맵을 만든 Makefile 섹션을 주석 처리하여 맵이 더 이상 만들어지지 않도록 합니다.

6 sites.byname이 ndbm 파일로만 존재하는 경우 새 마스터 서버에서 다시 만듭니다.

먼저 ypcat 명령을 사용하여 sites.byname 파일의 복사본을 역어셈블합니다. 그런 다음 makedbm을 통해 역어셈블된 버전을 실행합니다.

```
newmaster# cd /var/yp
newmaster# ypcat sites.byname | makedbm domain/sites.byname
```

새 마스터에 맵을 만든 후 새 맵의 복사본을 다른 슬레이브 서버로 보내야 합니다. 다른 슬레이브는 새 마스터 대신 이전 마스터에서 새 복사본을 가져오기 때문에 yppush를 사용하지 마십시오. 이를 피하는 일반적인 방법은 새 마스터의 맵 복사본을 다시 이전 마스터로 전송하는 것입니다. 이렇게 하려면 이전 마스터 서버에서 수퍼유저가 되거나 이에 상응하는 역할을 사용하고 다음을 입력합니다.

```
oldmaster# /usr/lib/netsvc/yp/ypxfr -h newmaster sites.byname
```

이제 yppush를 실행해도 됩니다. 나머지 슬레이브 서버는 여전히 이전 마스터가 현재 마스터라고 간주하고 이전 마스터에서 현재 버전의 맵을 가져오려고 합니다. 클라이언트가 이 작업을 수행하면 새 마스터 이름을 현재 마스터로 지정하는 새 맵을 가져오게 됩니다.

이 방법이 실패하면 각 NIS 서버에서 루트로 로그인하고 표시된 대로 ypxfr 명령을 실행할 수 있습니다.

구성 파일 수정

NIS는 설정 파일을 지능적으로 구문 분석합니다. 이렇게 하면 NIS 관리가 더 쉬워지지만 NIS 동작이 설정 및 구성 파일의 변경 사항에 더 민감해집니다.

다음 중 하나를 수행하는 경우 이 절의 절차를 사용합니다.

- /var/yp/Makefile을 사용하여 지원되는 맵 추가 또는 삭제
- $PWDIR/security/passwd.adjunct를 추가하거나 삭제하여 C2 보안 허용 또는 거부($PWDIR은 /var/yp/Makefile에 정의됨)

▼ 구성 파일을 수정하는 방법

다음 사항에 주의합니다.

- NIS 마스터 서버에서 맵 또는 소스 파일을 삭제해도 슬레이브 서버에서 해당 항목이 자동으로 삭제되지는 않습니다. 슬레이브 서버에서 맵과 소스 파일을 수동으로 삭제해야 합니다.

- 새 맵은 기존 슬레이브 서버에 자동으로 푸시되지 않습니다. 슬레이브에서 `ypxfr`을 실행해야 합니다.

1 **관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **NIS 서버를 중지합니다.**

```
# svcadm disable network/nis/server
```

3 **필요에 따라 파일을 변경합니다.**

4 **NIS 서버를 시작합니다.**

```
# svcadm enable network/nis/server
```

/var/yp/Makefile 수정 및 사용

기본적으로 `/var/yp`에 제공되는 `Makefile`을 요구에 맞게 수정할 수 있습니다. 맵을 추가하거나 삭제하고 일부 디렉토리의 이름을 변경할 수 있습니다.

참고 – 나중에 참조하기 위해 원래 `Makefile`의 수정하지 않은 복사본을 보관합니다.

Makefile 작업

새 NIS 맵을 추가하려면 맵에 대한 `ndbm` 파일의 복사본을 도메인의 각 NIS 서버에 있는 `/var/yp/`*domainname* 디렉토리로 가져와야 합니다. 일반적으로 이 작업은 `Makefile`에서 자동으로 수행됩니다. 맵의 마스터로 사용할 NIS 서버를 결정한 후 맵을 편리하게 재구성할 수 있도록 마스터 서버의 `Makefile`을 수정합니다. 각 서버를 다른 맵의 마스터로 사용할 수 있지만 대부분의 경우 이로 인해 관리 작업에 혼동이 초래됩니다. 한 서버만 모든 맵의 마스터로 설정하십시오.

일반적으로 사람이 읽을 수 있는 텍스트 파일은 `awk`, `sed` 또는 `grep`을 통해 필터링되어 `makedbm` 입력에 적합하게 만듭니다. 예는 기본 `Makefile`을 참조하십시오. `make` 명령에 대한 일반적인 정보는 `make(1S)`를 참조하십시오.

`make`에서 인식되는 종속성을 만드는 방법을 결정할 때는 `Makefile`에 이미 적용된 방식을 사용합니다. `make`는 종속성 규칙 내 라인의 시작 부분에 탭이 있는지 여부에 매우 민감합니다. 탭이 없으면 달리 구성에 문제가 없는 항목이 무효화될 수 있습니다.

`Makefile`에 항목을 추가하는 과정에는 다음이 포함됩니다.

- `all` 규칙에 데이터베이스 이름 추가
- `time` 규칙 작성
- 데이터베이스에 대한 규칙 추가

예를 들어, Makefile이 자동 마운트 입력 파일에서 작동하려면 auto_direct.time 및 auto_home.time 맵을 NIS 데이터베이스에 추가해야 합니다.

이러한 맵을 NIS 데이터베이스에 추가하려면 Makefile을 수정해야 합니다.

Makefile 매크로/변수 변경

등호(=) 오른쪽의 값을 변경하여 Makefile에 정의된 변수의 설정을 변경할 수 있습니다. 예를 들어, /etc에 있는 파일을 맵의 입력으로 사용하지 않고 /var/etc/domainname 등의 다른 디렉토리에 있는 파일을 사용하려는 경우 DIR을 DIR=/etc에서 DIR=/var/etc/*domainname*으로 변경해야 합니다. 또한 PWDIR을 PWDIR=/etc에서 PWDIR=/var/etc/*domainname*으로 변경해야 합니다.

변수는 다음과 같습니다.

- *DIR*= passwd 및 shadow를 제외한 모든 NIS 입력 파일이 포함된 디렉토리입니다. 기본값은 /etc입니다. 마스터 서버의 /etc 디렉토리에 있는 파일을 NIS 입력 파일로 사용하지 않는 것이 좋으므로 이 값을 변경해야 합니다.
- *PWDIR* = passwd 및 shadow NIS 입력 파일이 포함된 디렉토리입니다. 마스터 서버의 /etc 디렉토리에 있는 파일을 NIS 입력 파일로 사용하지 않는 것이 좋으므로 이 값을 변경해야 합니다.
- *DOM*= NIS 도메인 이름입니다. DOM의 기본값은 domainname 명령을 사용하여 설정할 수 있습니다.

Makefile 항목 수정

다음 절차에서는 Makefile에 데이터베이스를 추가하고 삭제하는 방법에 대해 설명합니다.

▼ 특정 데이터베이스를 사용하도록 /var/yp/Makefile을 수정하는 방법

이 절차를 수행하려면 NIS 마스터 서버를 이미 구성한 상태여야 합니다.

1 관리자로 전환합니다.

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 추가하려는 데이터베이스의 이름을 추가하여 all 단어로 시작하는 라인을 수정합니다.

```
all: passwd group hosts ethers networks rpc services protocols \
    netgroup bootparams aliases netid netmasks \
    audit_user auth_attr exec_attr prof_attr \
  auto_direct auto_home auto_direct.time auto_home.time
```

항목 순서는 관련이 없으며 구성 라인의 시작 부분에 있는 빈 공간은 공백이 아니라 탭이어야 합니다.

3 **Makefile 파일의 끝에 다음 라인을 추가합니다.**

```
auto_direct: auto_direct.time
auto_home: auto_home.time
```

4 **파일 중간에 auto_direct.time에 대한 항목을 추가합니다.**

```
auto_direct.time: $(DIR)/auto_direct
 @(while read L; do echo $$L; done < $(DIR)/auto_direct
 $(CHKPIPE)) | \ (sed -e "/^#/d" -e "s/#.*$$//" -e "/^ *$$/d"
 $(CHKPIPE)) | \ $(MAKEDBM) - $(YPDBDIR)/$(DOM)/auto_direct;
 @touch auto_direct.time;
 @echo "updated auto_direct";
 @if [ ! $(NOPUSH) ]; then $(YPPUSH) auto_direct; fi
 @if [ ! $(NOPUSH) ]; then echo "pushed auto_direct"; fi
```

구문 설명

- CHKPIPE는 결과를 다음 명령으로 파이프하기 전에 파이프(|) 왼쪽의 작업이 성공적으로 완료되었는지 확인합니다. 파이프 왼쪽의 작업이 성공적으로 완료되지 않은 경우 프로세스가 종료되고 NIS make terminated 메시지가 표시됩니다.
- NOPUSH는 makefile이 새 맵을 슬레이브 서버로 전송하기 위해 yppush를 호출하지 못하도록 합니다. NOPUSH를 설정하지 않으면 푸시가 자동으로 완료됩니다.

시작 부분의 while 루프는 입력 파일에서 백슬래시 확장 라인을 제거하기 위한 것입니다. sed 스크립트는 주석과 빈 라인을 제거합니다.

auto_home이나 기본 맵이 아닌 맵 등 다른 모든 자동 마운트 맵에 대해 동일한 절차를 따릅니다.

5 **make 명령을 실행합니다.**

```
# make mapname
```

여기서 *mapname*은 만들려는 맵의 이름입니다.

▼ 데이터베이스를 삭제하도록 /var/yp/Makefile을 수정하는 방법

Makefile을 사용하여 특정 데이터베이스에 대한 맵을 생성하지 않으려면 다음과 같이 Makefile을 편집합니다.

1 **all 규칙에서 데이터베이스 이름을 삭제합니다.**

2 **삭제하려는 데이터베이스에 대한 데이터베이스 규칙을 삭제하거나 주석 처리합니다.**

예를 들어, hosts 데이터베이스를 삭제하려면 hosts.time 항목을 제거해야 합니다.

3 **time 규칙을 제거합니다.**

예를 들어, hosts 데이터베이스를 삭제하려면 hosts: hosts.time 항목을 제거해야 합니다.

4 **마스터 및 슬레이브 서버에서 맵을 제거합니다.**

기존 맵 업데이트 및 수정

NIS를 설치한 후 일부 맵은 자주 업데이트해야 하는 반면 다른 맵은 변경할 필요가 없다는 것을 발견할 수 있습니다. 예를 들어, `passwd.byname` 맵은 큰 회사의 네트워크에서 자주 변경될 수 있지만 `auto_master` 맵은 거의 변경되지 않습니다.

65 페이지 "기본 NIS 맵"에서 언급한 대로 기본 NIS 맵의 기본 위치는 `/var/yp/`*domainname*의 마스터 서버에 있습니다. 여기서 *domainname*은 NIS 도메인의 이름입니다. 맵을 업데이트해야 하는 경우 기본 맵인지 여부에 따라 두 가지 업데이트 절차 중 하나를 사용할 수 있습니다.

- 기본 맵은 네트워크 데이터베이스에서 `ypinit` 명령으로 생성되는 기본 세트의 맵입니다.
- 기본 맵이 아닌 맵은 다음 중 하나일 수 있습니다.
  - 공급업체로부터 구매한 응용 프로그램에 포함된 맵
  - 사이트에 맞게 생성된 맵
  - 텍스트가 아닌 파일에서 생성된 맵

다음 절에서는 다양한 업데이트 도구를 사용하는 방법에 대해 설명합니다. 실제로 시스템이 이미 작동하여 실행 중인 후에 NIS 서버 세트를 변경하거나 기본 맵이 아닌 맵을 추가하는 경우에만 사용하도록 결정할 수 있습니다.

▼ 기본 세트와 함께 제공된 맵을 업데이트하는 방법

기본 세트와 함께 제공된 맵을 업데이트하려면 다음 절차를 사용합니다.

1. **NIS 마스터 서버의 관리자로 전환합니다.**

   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2. **변경하려는 맵의 소스 파일을 편집합니다.**

   이 파일은 `/etc`나 선택한 다른 디렉토리에 있을 수 있습니다.

3. **`make` 명령을 실행합니다.**

   ```
   # cd /var/yp
   # make mapname
   ```

   `make` 명령은 해당 파일의 변경 사항에 따라 맵을 업데이트합니다. 또한 다른 서버에 변경 사항을 전파합니다.

업데이트된 맵 유지 관리

다음 절에서는 기본 세트와 함께 제공된 맵의 업데이트를 완료한 후의 추가 절차에 대해 설명합니다.

NIS 맵 전파

맵이 변경된 후 Makefile은 yppush를 사용하여 새 맵을 슬레이브 서버로 전파합니다(Makefile에 NOPUSH가 설정되지 않은 경우). 이 작업을 위해 ypserv 데몬에 알리고 맵 전송 요청을 보냅니다. 슬레이브의 ypserv 데몬은 ypxfr 프로세스를 시작하고, 이 프로세스가 마스터 서버의 ypxfrd 데몬과 연결됩니다. 일부 기본 검사(예: 실제로 맵이 변경되었는지 여부)가 수행된 다음 맵이 전송됩니다. 슬레이브의 ypxfr이 yppush 프로세스로 응답을 보내 전송에 성공했는지 여부를 나타냅니다.

주 – 슬레이브 서버에 아직 없는 새로 만든 맵에서는 위 절차가 작동하지 **않습니다**. 슬레이브에서 ypxfr을 실행하여 새 맵을 슬레이브 서버로 보내야 합니다.

맵이 전파되지 않는 경우가 있으며 수동으로 ypxfr을 사용하여 새 맵 정보를 보내야 합니다. root crontab 파일을 통해 주기적으로 또는 명령줄에서 대화식으로 ypxfr을 사용하도록 선택할 수 있습니다. 이러한 접근 방법은 다음 절에서 설명합니다.

맵 전송 시 cron 명령 사용

맵에는 여러 가지 변경 등급이 있습니다. 예를 들어, 기본 맵 중 protocols.byname과 기본 맵이 아닌 맵 중 auto_master 같은 일부 맵은 몇 달 동안 변경되지 않을 수 있습니다. 그러나 passwd.byname은 하루에 여러 번 변경될 수 있습니다. crontab 명령을 사용하여 맵 전송을 예약하면 개별 맵에 대해 특정 전파 시간을 설정할 수 있습니다.

맵에 적합한 비율로 주기적으로 ypxfr을 실행하려면 각 슬레이브 서버의 루트 crontab 파일에 적절한 ypxfr 항목이 포함되어야 합니다. ypxfr은 마스터 서버의 복사본이 로컬 복사본보다 최신인 경우에만 마스터 서버에 연결하고 맵을 전송합니다.

주 – 마스터 서버가 기본 -m 옵션을 사용하여 rpc.yppasswdd를 실행하면 누구든지 해당 yp 암호를 변경할 때마다 passwd 데몬이 make를 실행하고 passwd 맵이 재구성됩니다.

---

cron 및 ypxfr과 함께 셸 스크립트 사용

각 맵에 대해 개별 crontab 항목을 만드는 대신 루트 crontab 명령이 모든 맵을 주기적으로 업데이트하는 셸 스크립트를 실행하도록 하는 것이 좋습니다. 샘플 맵 업데이트 셸 스크립트는 /usr/lib/netsvc/yp 디렉토리에 있습니다. 스크립트 이름은 ypxfr_1perday, ypxfr_1perhour 및 ypxfr_2perday입니다. 사이트 요구 사항에 맞게 이러한 셸 스크립트를 수정하거나 바꿀 수 있습니다. 다음 예에서는 기본 ypxfr_1perday 셸 스크립트를 보여 줍니다.

예 7–1 ypxfr_1perday 셸 스크립트

```
#! /bin/sh
#
# ypxfr_1perday.sh - Do daily yp map check/updates
PATH=/bin:/usr/bin:/usr/lib/netsvc/yp:$PATH
```

예 7–1 ypxfr_1perday 셸 스크립트 *(계속)*

```
export PATH
# set -xv
ypxfr group.byname
ypxfr group.bygid
ypxfr protocols.byname
ypxfr protocols.bynumber
ypxfr networks.byname
ypxfr networks.byaddr
ypxfr services.byname
ypxfr ypservers
```

루트 crontab을 매일 실행할 경우 이 셸 스크립트는 하루에 한 번 맵을 업데이트합니다. 매주 한 번, 매달 한 번, 매 시간 한 번 등으로 맵을 업데이트하는 스크립트를 사용할 수도 있습니다. 그러나 맵을 자주 전파할 경우의 성능 저하에 주의해야 합니다. 자세한 내용은 crontab(1) 매뉴얼 페이지를 참조하십시오.

NIS 도메인에 대해 구성된 각 슬레이브 서버에서 root와 동일한 셸 스크립트를 실행합니다. 마스터 작동에 방해가 되지 않도록 한 서버에서 다른 서버로의 정확한 실행 시간을 변경합니다.

특정 슬레이브 서버에서 맵을 전송하려는 경우 셸 스크립트 내에서 ypxfr의 -h *machine* 옵션을 사용합니다. 다음은 스크립트에 배치하는 명령의 구문입니다.

```
# /usr/lib/netsvc/yp/ypxfr -h machine [ -c ] mapname
```

여기서 *machine*은 전송하려는 맵이 있는 서버의 이름이고, *mapname*은 요청된 맵의 이름입니다. 시스템을 지정하지 않고 -h 옵션을 사용하면 ypxfr은 마스터 서버에서 맵을 가져오려고 합니다. ypxfr을 실행할 때 ypserv가 로컬에서 실행되고 있지 않으면 ypxfr에서 현재 맵 지우기 요청을 로컬 ypserver로 보내지 않도록 -c 플래그를 사용해야 합니다.

-s *domain* 옵션을 사용하여 다른 도메인에서 로컬 도메인으로 맵을 전송할 수 있습니다. 이러한 맵은 도메인 간에 동일해야 합니다. 예를 들어, 두 도메인이 동일한 services.byname 및 services.byaddr 맵을 공유할 수 있습니다. 또는 제어를 강화하기 위해 rcp 또는 rsync를 사용하여 도메인 간에 파일을 전송할 수 있습니다.

직접 ypxfr 명령 호출

ypxfr 명령을 호출하는 두번째 방법은 명령으로 실행하는 것입니다. 일반적으로 예외적인 상황에서만 이 방법을 사용합니다. 예를 들어, 테스트 환경을 만들기 위해 임시 NIS 서버를 설정하는 경우나 서비스가 중단된 NIS 서버를 신속하게 다른 서버와 일치시키려는 경우에 사용합니다.

ypxfr 작업 기록

ypxfr의 전송 시도와 결과는 로그 파일에 캡처될 수 있습니다. /var/yp/ypxfr.log 파일이 있으면 결과가 파일에 추가됩니다. 로그 파일의 크기는 제한되지 않습니다. 파일이 무한히 커지지 않도록 때때로 다음을 입력하여 파일을 비웁니다.

```
# cd /var/yp
# cp ypxfr.log ypxfr.log.old
# cat /dev/null > /var/yp/ypxfr.log
```

crontab에서 이러한 명령을 매주 한 번 실행하도록 할 수 있습니다. 로깅을 해제하려면 로그 파일을 제거합니다.

기본 맵이 아닌 맵 수정

기본 맵이 아닌 맵을 업데이트하려면 다음을 수행해야 합니다.

1. 해당 텍스트 파일을 만들거나 편집합니다.
2. 새 맵이나 업데이트된 맵을 작성(또는 재구성)합니다. 맵을 작성하는 두 가지 방법이 있습니다.
   - Makefile을 사용합니다. Makefile을 사용하여 기본 맵이 아닌 맵을 작성하는 것이 좋습니다. Makefile에 맵에 대한 항목이 있는 경우 make *name*을 실행합니다. 여기서 *name*은 작성하려는 맵의 이름입니다. 맵에 Makefile 항목이 없는 경우 96 페이지 "/var/yp/Makefile 수정 및 사용"의 지침에 따라 새로 만듭니다.
   - /usr/sbin/makedbm 프로그램을 사용합니다. makedbm(1M) 매뉴얼 페이지에서 이 명령에 대해 자세히 설명합니다.

makedbm 명령을 사용하여 기본 맵이 아닌 맵 수정

입력 파일이 없는 경우 makedbm을 사용하여 맵을 수정하는 다음 두 가지 방법이 있습니다.

- makedbm -u 출력을 임시 파일로 재지정하고 파일을 수정한 다음 수정된 파일을 makedbm의 입력으로 사용합니다.
- makedbm -u의 출력이 makedbm에 제공되는 파이프라인 내에서 작동하도록 합니다. 이 방법은 awk, sed 또는 cat 추가를 사용하여 역어셈블된 맵을 업데이트할 수 있는 경우에 적합합니다.

텍스트 파일에서 새 맵 만들기

마스터에서 편집기나 셸 스크립트를 사용하여 텍스트 파일 /var/yp/mymap.asc를 만들었다고 가정합니다. 이 파일에서 NIS 맵을 만들고 *home-domain* 하위 디렉토리에 배치하려고 합니다. 이렇게 하려면 마스터 서버에서 다음을 입력합니다.

```
# cd /var/yp
# makedbm mymap.asc home-domain/mymap
```

이제 *mymap* 맵이 마스터 서버의 *home-domain* 디렉토리에 있습니다. 슬레이브 서버에 새 맵을 배포하려면 ypxfr을 실행합니다.

파일 기반 맵에 항목 추가

mymap에 항목을 간단하게 추가할 수 있습니다. 먼저 텍스트 파일 /var/yp/ *mymap*.asc를 수정해야 합니다. 해당 텍스트 파일을 수정하지 않고 실제 dbm 파일을 수정하면 수정 내용이 손실됩니다. 그런 다음 위와 같이 makedbm을 실행합니다.

표준 입력에서 맵 만들기

원본 텍스트 파일이 없는 경우 아래와 같이 makedbm에 대한 입력을 입력하여 키보드에서 NIS 맵을 만듭니다(Control-D로 끝내기).

```
ypmaster# cd /var/yp
ypmaster# makedbm home-domain/mymap key1 value1 key2 value2 key3 value3
```

표준 입력에서 만든 맵 수정

나중에 맵을 수정해야 하는 경우 makedbm을 사용하여 맵을 역어셈블하고 임시 텍스트 중간 파일을 만들 수 있습니다. 맵을 역어셈블하고 임시 파일을 만들려면 다음을 입력합니다.

```
% cd /var/yp
% makedbm -u homedomain/mymap > mymap.temp
```

결과 임시 파일 *mymap*.temp에는 라인당 항목이 1개 있습니다. 텍스트 편집기를 사용하여 필요에 따라 이 파일을 편집할 수 있습니다.

맵을 업데이트하려면 다음을 입력하여 makedbm에 수정된 임시 파일의 이름을 지정합니다.

```
% makedbm mymap.temp homedomain/mymap
% rm mymap.temp
```

그런 다음 root가 되고 다음을 입력하여 슬레이브 서버에 맵을 전파합니다.

```
# yppush mymap
```

앞의 단락에서는 makedbm을 사용하여 맵을 만드는 방법에 대해 설명했습니다. 그러나 실제로 수행해야 하는 거의 모든 작업은 시스템이 이미 작동하여 실행 중인 후에 NIS 서버 세트를 변경하거나 기본 맵이 아닌 맵을 데이터베이스에 추가하는 경우가 아니면 ypinit 명령과 /var/yp/Makefile을 사용하여 완료할 수 있습니다.

/var/yp 또는 다른 절차에서 Makefile을 사용하는지에 관계없이 목적은 동일합니다. 잘 구성된 새로운 dbm 파일 쌍이 마스터 서버의 맵 디렉토리에 배치되어야 합니다.

NIS 서버 작업

다음 절차에서는 특정 NIS 서버에 바인딩하고, NIS 도메인 이름을 설정하고, 호스트 조회를 DNS로 전달하고, NIS 서비스를 해제하여 NIS 구성을 수정하는 방법을 보여 줍니다.

특정 NIS 서버에 바인딩

지정하는 NIS 서버에 바인딩하려면 다음 단계를 사용합니다. 자세한 내용은 ypinit(1M), ypstart(1M) 및 svcadm(1M) 매뉴얼 페이지를 참조하십시오.

1. /etc/inet/hosts 파일에 NIS 서버의 호스트 이름 및 IP 주소를 추가합니다.
2. NIS 도메인 이름이 설정되었는지 확인합니다.

```
# domainname
example.com
```

3. NIS 서버 호스트 이름을 묻는 메시지가 표시됩니다.

```
# /usr/sbin/ypinit -c
Server name:        Type the NIS server host name
```

4. 다음 단계 중 하나를 수행하여 NIS 서비스를 다시 시작합니다.
   - 재부트 후에도 서비스를 유지하려면 svcadm 명령을 실행합니다.

     ```
     # svcadm enable svc:/network/nis/client
     ```
   - 재부트할 때까지만 서비스를 유지하려면 ypstop 및 ypstart 명령을 실행합니다.

     ```
     # /usr/lib/netsvc/yp/ypstop
     # /usr/lib/netsvc/yp/ypstart
     ```

▼ 시스템의 NIS 도메인 이름을 설정하는 방법

시스템의 NIS 도메인 이름을 변경하려면 다음 절차를 사용합니다.

1 관리자로 전환합니다.

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 NIS 도메인 이름을 정의합니다.

```
# domainname research.example.com
```

3 **도메인 이름 서비스를 업데이트하고 실행합니다.**

```
# svccfg -s nis/domain:default refresh
# svcadm enable nis/domain
```

4 **시스템을 NIS 클라이언트, 슬레이브 서버 또는 마스터 서버로 설정합니다.**

자세한 내용은 6 장, “NIS 설정 및 구성(작업)”을 참조하십시오.

▼ NIS 및 DNS를 통한 시스템 호스트 이름 및 주소 조회를 구성하는 방법

일반적으로 NIS 클라이언트는 `nsswitch.conf` 파일을 사용하여 시스템 이름과 주소 조회에 NIS만 사용하도록 구성됩니다. 이 조회 유형이 실패하면 NIS 서버는 이러한 조회를 DNS로 전달할 수 있습니다.

1 **관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 “지정된 관리 권한을 사용하는 방법”을 참조하십시오.

2 **`YP_INTERDOMAIN` 키를 추가합니다.**

`hosts.byname` 및 `hosts.byaddr` 맵 파일 2개에는 `YP_INTERDOMAIN` 키가 포함되어야 합니다. 이 키를 테스트하려면 `/var/yp/Makefile`을 편집하고 다음 라인을 수정합니다.

```
#B=-b
B=
```

변경 후

```
B=-b
#B=
```

이제 `makedbm`이 맵을 만들 때 `-b` 플래그로 시작되며, `YP_INTERDOMAIN` 키가 `ndbm` 파일에 삽입됩니다.

3 **`make` 명령을 실행하여 맵을 재구성합니다.**

```
# make hosts
```

4 **DNS 이름 서버가 올바르게 설정되었는지 확인합니다.**

다음 명령은 DNS 이름 서버의 IP 주소를 모두 나열합니다.

```
# svcprop -p config/nameserver network/dns/client
```

5 **DNS 전달을 사용으로 설정하려면 각 서버를 다시 시작합니다.**

```
# svcadm restart network/nis/server:instance
```

이 NIS 구현에서 `ypserv` 데몬은 자동으로 `-d` 옵션으로 시작되어 요청을 DNS로 전달합니다.

NIS 서비스 해제

NIS 마스터의 ypserv 데몬이 사용 안함으로 설정된 경우 더 이상 NIS 맵을 업데이트할 수 없습니다.

- 클라이언트에서 NIS를 사용 안함으로 설정하려면 다음을 입력합니다.

```
# svcadm disable network/nis/domain
# svcadm disable network/nis/client
```

- 특정 슬레이브 또는 마스터 서버에서 NIS를 사용 안함으로 설정하려면 서버에서 다음을 입력합니다.

```
# svcadm disable network/nis/domain
# svcadm disable network/nis/server
```

◆ ◆ ◆ 8 장

8 NIS 문제 해결

이 장에서는 NIS를 실행 중인 네트워크에서 발생하는 문제를 해결하는 방법에 대해 설명합니다. NIS 클라이언트와 NIS 서버에서 발생하는 문제를 모두 다룹니다.

NIS 서버 또는 클라이언트를 디버그하기 전에 NIS 환경에 대해 설명하는 5 장, "네트워크 정보 서비스(개요)"를 검토하십시오. 그런 다음 이 절에서 해당 문제를 가장 잘 설명하는 하위 제목을 찾습니다.

주 – NIS 서비스는 서비스 관리 기능을 통해 관리됩니다. `svcadm` 명령을 사용하여 사용으로 설정, 사용 안함으로 설정, 다시 시작 등 이 서비스에 대한 관리 작업을 수행할 수 있습니다. NIS와 함께 SMF를 사용하는 방법에 대한 자세한 내용은 72 페이지 "NIS 및 서비스 관리 기능"을 참조하십시오. SMF 개요는 **Oracle Solaris 11.1에서 서비스 및 결함 관리**의 1 장, "서비스 관리(개요)"를 참조하십시오. 자세한 내용은 `svcadm`(1M) 및 `svcs`(1) 매뉴얼 페이지를 참조하십시오.

`ypstart` 및 `ypstop` 명령을 사용하여 NIS 서비스를 시작하고 중지할 수도 있습니다. 자세한 내용은 `ypstart`(1M) 및 `ypstop`(1M) 매뉴얼 페이지를 참조하십시오.

NIS 바인딩 문제

NIS 바인딩 문제의 증상

NIS 바인딩 문제의 일반적인 증상은 다음과 같습니다.

- `ypbind`에서 서버를 찾거나 통신할 수 없다는 메시지
- 서버가 응답하지 않는다는 메시지
- NIS를 사용할 수 없다는 메시지
- 클라이언트의 명령이 백그라운드 모드에서 제대로 작동하지 않거나 정상적인 경우보다 훨씬 느리게 작동함

- 클라이언트의 명령이 중단됨. 전체 시스템이 정상적으로 표시되고 새 명령을 실행할 수 있는 경우에도 때때로 명령이 중단됩니다.
- 클라이언트의 명령이 충돌하고 모호한 메시지가 표시되거나 메시지가 표시되지 않음

한 클라이언트에 영향을 주는 NIS 문제

NIS 바인딩 문제를 나타내는 증상이 한두 개 클라이언트에서만 발생하는 경우 해당 클라이언트에 문제가 있는 것입니다. 많은 NIS 클라이언트가 올바르게 바인딩하지 못하는 경우에는 NIS 서버 중 하나 이상에 문제가 있는 것입니다. 111 페이지 “많은 클라이언트에 영향을 주는 NIS 문제”를 참조하십시오.

ypbind가 클라이언트에서 실행되고 있지 않음

한 클라이언트에 문제가 있지만 동일한 서브넷의 다른 클라이언트는 정상적으로 작동합니다. 문제 클라이언트에서 클라이언트 /etc/passwd 파일에 없는 파일을 비롯하여 많은 사용자가 소유한 파일을 포함하는 /usr 등의 디렉토리에서 ls -l을 실행합니다. 결과 표시에 로컬 /etc/passwd에 없는 파일 소유자가 이름 대신 번호로 표시되는 경우 NIS 서비스가 클라이언트에서 작동하고 있지 않은 것입니다.

이러한 증상은 대체로 ypbind 프로세스가 실행되고 있지 않음을 의미합니다. NIS 클라이언트 서비스가 실행 중인지 확인합니다.

```
client# svcs \*nis\*
STATE          STIME    FMRI
disabled       Sep_01   svc:/network/nis/domain:default
disabled       Sep_01   svc:/network/nis/client:default
```

서비스가 disabled 상태인 경우 root로 로그인하거나 이에 상응하는 역할을 사용하고 NIS 클라이언트 서비스를 시작합니다.

```
client# svcadm enable network/nis/domain
client# svcadm enable network/nis/client
```

누락 또는 잘못된 도메인 이름

한 클라이언트에 문제가 있고 다른 클라이언트는 정상적으로 작동 중이지만 ypbind가 문제 클라이언트에서 실행 중입니다. 클라이언트에 잘못 설정된 도메인이 있을 수 있습니다.

클라이언트에서 domainname 명령을 실행하여 설정된 도메인 이름을 확인합니다.

```
client7# domainname
example.com
```

NIS 마스터 서버의 /var/yp에 있는 실제 도메인 이름과 출력을 비교합니다. 실제 NIS 도메인은 /var/yp 디렉토리에 하위 디렉토리로 표시됩니다.

```
client7# ls -l /var/yp
-rwxr-xr-x 1 root Makefile
drwxr-xr-x 2 root binding
drwx------ 2 root example.com
```

시스템에서 domainname을 실행하여 반환된 도메인 이름이 /var/yp에 디렉토리로 나열된 서버 도메인 이름과 다른 경우 시스템의 /etc/defaultdomain 파일에 지정된 도메인 이름이 잘못된 것입니다. 104 페이지 “시스템의 NIS 도메인 이름을 설정하는 방법”에 표시된 대로 NIS 도메인 이름을 재설정합니다.

주 – NIS 도메인 이름은 대소문자를 구분합니다.

클라이언트가 서버에 바인딩되어 있지 않음

도메인 이름이 올바르게 설정되었으며 ypbind가 실행 중인데 명령이 중단되는 경우 ypwhich 명령을 실행하여 클라이언트가 서버에 바인딩되어 있는지 확인합니다. 방금 ypbind를 시작한 경우 ypwhich를 여러 번 실행합니다. 일반적으로 첫번째 시도에서는 도메인이 바인딩되어 있지 않다고 보고하고 두번째 시도는 정상적으로 성공합니다.

서버를 사용할 수 없음

도메인 이름이 올바르게 설정되었으며 ypbind가 실행 중인데 클라이언트에서 서버와 통신할 수 없다는 메시지가 표시되는 경우 다음과 같은 다양한 문제를 나타낼 수 있습니다.

- 클라이언트에 바인딩할 서버 목록을 포함하는 /var/yp/binding/*domainname*/ypservers 파일이 있습니까? 없는 경우 ypinit -c를 실행하고 이 클라이언트에서 바인딩해야 하는 서버를 원하는 순서대로 지정합니다.
- 클라이언트에 /var/yp/binding/ *domainname*/ypservers 파일이 있는 경우 한두 개의 서버가 사용할 수 없게 되어도 충분한 서버가 나열되어 있습니까? 충분한 서버가 나열되어 있지 않으면 ypinit -c를 실행하여 목록에 서버를 더 추가합니다.
- 선택한 NIS 서버에 대한 항목이 /etc/inet/hosts 파일에 있습니까? 선택한 NIS 서버를 보려면 svcprop -p config/ypservers nis/domain 명령을 사용합니다. 이러한 호스트가 로컬 /etc/inet/hosts 파일에 없는 경우 hosts NIS 맵에 서버를 추가하고 93 페이지 “NIS 맵 작업”에 설명된 대로 ypinit -c 또는 ypinit -s 명령을 실행하여 맵을 재구성합니다.
- NIS뿐 아니라 시스템의 로컬 hosts 파일을 검사하도록 이름 서비스 스위치가 설정되었습니까? 스위치에 대한 자세한 내용은 2 장, “이름 서비스 스위치(개요)”를 참조하십시오.
- services 및 rpc에 대해 files를 먼저 검사하도록 이름 서비스 스위치가 설정되었습니까? 스위치에 대한 자세한 내용은 2 장, “이름 서비스 스위치(개요)”를 참조하십시오.

ypwhich 표시가 일치하지 않음

동일한 클라이언트에서 ypwhich를 여러 번 사용할 경우 NIS 서버 변경 때문에 결과 표시가 달라집니다. 이것은 정상적인 동작입니다. 네트워크 또는 NIS 서버가 사용 중인 경우 NIS 서버에 대한 NIS 클라이언트 바인딩이 시간에 따라 변경됩니다. 가능한 경우 모든 클라이언트가 NIS 서버로부터 허용되는 응답 시간을 받는 시점에 네트워크가 안정됩니다. 클라이언트 시스템이 NIS 서비스를 얻기만 하면 어디에서 서비스가 제공되는지는 중요하지 않습니다. 예를 들어, 한 NIS 서버 시스템이 네트워크의 다른 NIS 서버에서 NIS 서비스를 얻을 수 있습니다.

서버 바인딩이 가능하지 않은 경우

로컬 서버 바인딩이 가능하지 않은 극단적인 경우에 ypset 명령을 사용하면 다른 네트워크나 서브넷의 다른 서버(사용 가능한 경우)에 일시적으로 바인딩할 수 있습니다. 그러나 -ypset 옵션을 사용하려면 -ypset 또는 -ypsetme 옵션을 사용하여 ypbind를 시작해야 합니다. 자세한 내용은 ypbind(1M) 매뉴얼 페이지를 참조하십시오.

```
# /usr/lib/netsvc/yp/ypbind -ypset
```

다른 방법은 104 페이지 “특정 NIS 서버에 바인딩”을 참조하십시오.

주의 – 보안을 위해 -ypset 및 -ypsetme 옵션은 사용하지 않는 것이 좋습니다. 제어된 상황에서 디버깅 용도로만 이러한 옵션을 사용합니다. -ypset 및 -ypsetme 옵션을 사용하면 데몬이 실행되는 동안 누구든지 서버 바인딩을 변경할 수 있고 이로 인해 다른 사용자에게 문제가 발생하거나 중요한 데이터에 대한 허용되지 않은 액세스가 허용될 수 있으므로 심각한 보안 위반이 초래될 수 있습니다. 이러한 옵션으로 ypbind 데몬을 시작해야 하는 경우 문제를 해결한 후 ypbind 프로세스를 강제 종료하고 이러한 옵션 없이 다시 시작해야 합니다.

ypbind 데몬을 다시 시작하려면 다음과 같이 SMF를 사용합니다.

```
# svcadm enable -r svc:/network/nis/client:default
```

ypbind 충돌

ypbind 데몬을 daemon crashes almost immediately each time it is started, look for a problem in the svc:/network/nis/client:default service log. 다음을 입력하여 rpcbind 데몬이 있는지 확인합니다.

```
% ps -e |grep rpcbind
```

rpcbind가 없거나, 작동하지 않거나, 이상하게 동작하는 경우 svc:/network/rpc/bind:default 로그 파일을 확인합니다. 자세한 내용은 rpcbind(1M) 및 rpcinfo(1M) 매뉴얼 페이지를 참조하십시오.

정상적으로 작동하는 시스템에서 문제 클라이언트의 rpcbind와 통신할 수도 있습니다. 작동하는 시스템에서 다음을 입력합니다.

```
% rpcinfo client
```

문제 시스템의 rpcbind가 정상인 경우 rpcinfo에서 다음 출력을 생성합니다.

```
    program    version    netid     address    service    owner
...
    100007    3    udp6       ::.191.161          ypbind     1
    100007    3    tcp6       ::.135.200          ypbind     1
    100007    3    udp        0.0.0.0.240.221     ypbind     1
    100007    2    udp        0.0.0.0.240.221     ypbind     1
    100007    1    udp        0.0.0.0.240.221     ypbind     1
    100007    3    tcp        0.0.0.0.250.107     ypbind     1
    100007    2    tcp        0.0.0.0.250.107     ypbind     1
    100007    1    tcp        0.0.0.0.250.107     ypbind     1
    100007    3    ticlts     2\000\000\000       ypbind     1
    100007    2    ticlts     2\000\000\000       ypbind     1
    100007    3    ticotsord  9\000\000\000       ypbind     1
    100007    2    ticotsord  9\000\000\000       ypbind     1
    100007    3    ticots     @\000\000\000       ypbind     1
...
```

시스템에 다른 주소가 지정됩니다. 주소가 표시되지 않는 경우 ypbind에서 서비스를 등록할 수 없습니다. 시스템을 재부트하고 rpcinfo를 다시 실행합니다. ypbind 프로세스가 있고 NIS 서비스를 다시 시작할 때마다 변경되면 rpcbind 데몬이 실행 중인 경우에도 시스템을 재부트합니다.

많은 클라이언트에 영향을 주는 NIS 문제

NIS 바인딩 문제를 나타내는 증상이 한두 개 클라이언트에서만 발생하는 경우 해당 클라이언트에 문제가 있는 것입니다. 108 페이지 “한 클라이언트에 영향을 주는 NIS 문제”를 참조하십시오. 많은 NIS 클라이언트가 올바르게 바인딩하지 못하는 경우에는 NIS 서버 중 하나 이상에 문제가 있는 것입니다.

rpc.yppasswdd에서 r로 시작하는 제한되지 않는 셸을 제한되는 셸로 간주함

1. 특수 문자열 "check_restricted_shell_name=1"이 포함된 /etc/default/yppasswdd를 만듭니다.
2. "check_restricted_shell_name=1" 문자열을 주석 처리하면 'r' 확인이 수행되지 않습니다.

네트워크 또는 서버에 연결할 수 없음

네트워크 또는 NIS 서버가 과부하되어 ypserv 데몬이 시간 초과 기간 내에 클라이언트 ypbind 프로세스에 대한 응답을 받지 못할 경우 NIS가 중단될 수 있습니다. 네트워크가 다운된 경우에도 NIS가 중단됩니다.

이러한 경우 네트워크의 모든 클라이언트에서 동일한 문제나 유사한 문제가 발생합니다. 대부분 이 상태는 일시적입니다. NIS 서버가 재부트되고 ypserv를 다시 시작하거나, NIS 서버 또는 네트워크 자체의 로드가 감소하거나, 네트워크가 정상 작동을 계속하면 일반적으로 메시지가 사라집니다.

서버 오작동

서버가 작동하고 실행 중인지 확인합니다. 물리적으로 서버 근처에 없는 경우 ping 명령을 사용합니다.

NIS 데몬이 실행되고 있지 않음

서버가 작동하고 실행 중인 경우 정상적으로 동작하는 클라이언트 시스템을 찾은 다음 ypwhich 명령을 실행합니다. ypwhich가 응답하지 않으면 강제 종료합니다. 그런 다음 NIS 서버에서 root로 로그인하고 다음을 입력하여 NIS 프로세스가 실행 중인지 확인합니다.

```
# ptree |grep ypbind
100759 /usr/lib/netsvc/yp/ypbind -broadcast
        527360 grep yp
```

ypserv(NIS 서버) 및 ypbind(NIS 클라이언트) 데몬이 둘 다 실행되고 있지 않으면 다음을 입력하여 다시 시작합니다.

```
# svcadm restart network/nis/client
```

NIS 서버에서 ypserv 및 ypbind 프로세스가 실행 중이면 ypwhich 명령을 실행합니다. 명령이 응답하지 않으면 ypserv 데몬이 중단된 것이며 다시 시작해야 합니다. 서버에서 root로 로그인하는 동안 다음을 입력하여 NIS 서비스를 다시 시작합니다.

```
# svcadm restart network/nis/server
```

서버에 NIS 맵의 여러 버전이 있음

NIS는 서버에 맵을 전파하기 때문에 네트워크의 다양한 NIS 서버에 동일한 맵의 여러 버전이 있는 것을 발견할 수 있습니다. 차이가 오랫동안 지속되지 않을 경우 이 버전 불일치는 정상적이며 허용됩니다.

맵 불일치의 가장 일반적인 원인은 정상적인 맵 전파를 방해하는 것이 있는 경우입니다. 예를 들어, 한 NIS 서버나 NIS 서버 간의 라우터가 다운되었습니다. 모든 NIS 서버와 서버 간의 라우터가 실행 중이면 ypxfr이 성공해야 합니다.

서버와 라우터가 제대로 작동 중이면 다음을 확인합니다.

- ypxfr 로그 출력을 확인합니다. 113 페이지 “ypxfr 출력 확인”을 참조하십시오.
- svc:/network/nis/xfr:default 로그 파일에 오류가 있는지 확인합니다.
- 제어 파일을 확인합니다. 113 페이지 “crontab 파일 및 ypxfr 셸 스크립트 확인”을 참조하십시오.
- 마스터 서버의 ypservers 맵을 확인합니다. 113 페이지 “ypservers 맵을 확인합니다.”을 참조하십시오.

ypxfr 출력 확인

특정 슬레이브 서버에 맵 업데이트 문제가 있는 경우 해당 서버에 로그인한 다음 ypxfr 명령을 대화식으로 실행합니다. 명령이 실패하면 실패한 이유가 표시되고 문제를 해결할 수 있습니다. 명령이 성공하지만 때때로 실패했다고 의심되는 경우 로그 파일을 만들어 메시지 로깅을 사용으로 설정합니다. 로그 파일을 만들려면 슬레이브에서 다음을 입력합니다.

```
ypslave# cd /var/yp
ypslave# touch ypxfr.log
```

이렇게 하면 ypxfr의 모든 출력을 저장하는 ypxfr.log 파일이 생성됩니다.

이 출력은 ypxfr이 대화식으로 실행될 때 표시하는 출력과 비슷하지만 로그 파일의 각 라인에 시간이 기록되어 있습니다. 시간 기록 방식에 특이한 순서가 표시될 수도 있습니다. 이것은 정상적인 동작입니다. 시간 기록 방식은 ypxfr 실행이 시작된 시간을 알려줍니다. ypxfr의 여러 복사본이 동시에 실행되었지만 소요된 작업 시간이 다른 경우 실제로 호출된 순서와 다른 순서로 로그 파일에 요약 상태 라인을 기록할 수 있습니다. 종종 발생하는 오류의 모든 패턴이 로그에 표시됩니다.

주 – 문제를 해결했으면 로그 파일을 제거하여 로깅을 해제합니다. 제거하지 않으면 파일이 제한 없이 계속 커집니다.

---

crontab 파일 및 ypxfr 셸 스크립트 확인

root crontab 파일을 검사하고 이 파일에서 호출되는 ypxfr 셸 스크립트를 확인합니다. 이러한 파일에 맞춤법 오류가 있으면 전파 문제가 발생할 수 있습니다. /var/spool/cron/crontabs/root 파일 내의 셸 스크립트를 참조하지 못하거나 셸 스크립트 내의 맵을 참조하지 못할 경우에도 오류가 발생할 수 있습니다.

ypservers 맵을 확인합니다.

또한 NIS 슬레이브 서버가 도메인에 대한 마스터 서버의 ypservers 맵에 나열되는지 확인합니다. 나열되지 않는 경우 슬레이브 서버가 여전히 서버로 작동하지만 yppush에서 맵 변경 사항을 슬레이브 서버로 전파하지 않습니다.

끊어진 슬레이브 서버의 맵을 업데이트하기 위한 임시해결책

NIS 슬레이브 서버 문제가 명확하지 않은 경우 문제를 디버깅하는 동안 scp 또는 ssh 명령을 통해 정상적인 NIS 서버에서 일치하지 않는 맵의 최근 버전을 복사하여 임시해결책을 수행할 수 있습니다. 다음은 문제 맵을 전송하는 방법을 보여 줍니다.

```
ypslave# scp ypmaster:/var/yp/mydomain/map.\* /var/yp/mydomain
```

* 문자는 ypslave에서 로컬로 확장되는 대신 ypmaster에서 확장되도록 명령줄에서 이스케이프되었습니다.

ypserv 충돌

ypserv 프로세스가 거의 즉시 충돌하고 활성화를 반복해도 작동이 유지되지 않는 경우의 디버깅 프로세스는 110 페이지 “ypbind 충돌”에 설명된 것과 거의 동일합니다. 먼저, 다음 명령을 실행하여 오류가 보고되는지 확인합니다.

```
# svcs -vx nis/server
```

다음과 같이 rpcbind 데몬이 있는지 확인합니다.

```
# ptree |grep rpcbind
```

데몬이 없는 경우 서버를 재부트합니다. 그렇지 않고 데몬이 실행 중이면 다음을 입력하고 유사한 출력을 찾습니다.

```
% rpcinfo -p ypserver

% program     vers     proto     port     service
100000    4    tcp    111    portmapper
100000    3    tcp    111    portmapper
100068    2    udp    32813    cmsd
...
100007    1    tcp    34900    ypbind
100004    2    udp    731    ypserv
100004    1    udp    731    ypserv
100004    1    tcp    732    ypserv
100004    2    tcp    32772    ypserv
```

시스템에 다른 포트 번호가 있을 수도 있습니다. ypserv 프로세스를 나타내는 4개 항목은 다음과 같습니다.

```
100004     2     udp     731     ypserv
100004     1     udp     731     ypserv
100004     1     tcp     732     ypserv
100004     2     tcp     32772     ypserv
```

항목이 없고 ypserv에서 해당 서비스를 rpcbind에 등록할 수 없는 경우 시스템을 재부트합니다. 항목이 있으면 ypserv를 다시 시작하기 전에 rpcbind에서 서비스를 등록 해제합니다. rpcbind에서 서비스를 등록 해제하려면 서버에서 다음을 입력합니다.

```
# rpcinfo -d number 1
# rpcinfo -d number 2
```

여기서 *number*는 rpcinfo에서 보고된 ID 번호(앞의 예에서는 100004)입니다.

제 3 부

LDAP 이름 지정 서비스

이 부분에서는 LDAP 이름 지정 서비스의 개요를 제공합니다. 또한 Oracle Directory Server Enterprise Edition 사용에 중점을 두며 Oracle Solaris OS에서 LDAP 이름 지정 서비스를 설정, 구성 및 관리하고 해당 문제를 해결하는 방법에 대해 설명합니다.

◆ ◆ ◆ 9 장

9 LDAP 이름 지정 서비스 소개(개요)

LDAP 장에서는 Oracle Directory Server Enterprise Edition(이전의 Sun Java System Directory Server)에서 작동하도록 LDAP 이름 지정 서비스 클라이언트를 설정하는 방법에 대해 설명합니다. 그러나 Oracle Directory Server Enterprise Edition 사용은 권장 사항이지 필수 사항은 아닙니다. 14 장, “LDAP 이름 지정 서비스(참조)”에는 일반적인 디렉토리 서버 요구 사항에 대한 간단한 설명이 포함되어 있습니다.

주 – 디렉토리 서버가 반드시 LDAP 서버인 것은 아닙니다. 그러나 이 장에서는 "디렉토리 서버"라는 용어가 "LDAP 서버"와 동의어로 사용되었습니다.

이 장에서는 다음 내용을 다룹니다.

대상 가정

LDAP 이름 지정 서비스 장은 LDAP에 대한 실제적인 지식을 가지고 있는 시스템 관리자를 위해 작성되었습니다. 다음은 독자가 잘 알고 있어야 하는 개념 중 일부입니다. 이러한 개념에 대해 잘 모를 경우 본 설명서를 사용하여 Oracle Solaris 시스템에 LDAP 이름 지정 서비스를 배포하기가 어려울 수 있습니다.

- LDAP 정보 모델(항목, 객체 클래스, 속성, 유형, 값)
- LDAP 이름 지정 모델(DIT(디렉토리 정보 트리) 구조)
- LDAP 기능 모델(검색 매개변수: 기본 객체(DN), 범위, 크기 제한, 시간 제한, 필터(Oracle Directory Server Enterprise Edition의 색인 검색), 속성 목록)
- LDAP 보안 모델(인증 방법, 액세스 제어 모델)
- 데이터를 계획하는 방법과 DIT, 토폴로지, 복제 및 보안을 설계하는 방법을 비롯한 LDAP 디렉토리 서비스의 전체 계획 및 설계

배경 지식을 늘리기 위한 추천 자료

앞서 설명한 개념이나 LDAP 및 일반적인 디렉토리 서비스 배포에 대해 자세히 알아보려면 다음 자료를 참조하십시오.

- **Oracle Directory Server Enterprise Edition 배포 설명서**

  본 설명서에서는 디렉토리 설계, 스키마 설계, 디렉토리 트리, 토폴로지, 복제 및 보안을 비롯하여 디렉토리 계획을 세우기 위한 기초를 제공합니다. 마지막 장에서는 간단한 소규모 배포와 복잡한 전세계 배포를 모두 계획하는 데 유용한 샘플 배포 시나리오를 제공합니다.
- **Oracle Directory Server Enterprise Edition 관리 설명서**

추가 필수 조건

Oracle Directory Server Enterprise Edition을 설치해야 하는 경우 사용 중인 Oracle Directory Server Enterprise Edition 버전에 대한 **설치 설명서**를 참조하십시오.

LDAP 이름 지정 서비스와 다른 이름 지정 서비스 비교

DNS, NIS 및 LDAP 이름 지정 서비스를 비교한 정보는 29 페이지 “이름 지정 서비스: 빠른 비교”를 참조하십시오.

LDAP 이름 지정 서비스의 장점

- LDAP을 사용하면 응용 프로그램별 데이터베이스를 대체하여 정보를 통합할 수 있습니다. 이렇게 하면 관리할 개별 데이터베이스 수가 줄어듭니다.
- LDAP을 사용하면 여러 이름 지정 서비스에서 데이터를 공유할 수 있습니다.
- LDAP은 중앙 데이터 저장소를 제공합니다.
- LDAP을 사용하면 마스터와 복제본 간에 데이터를 더 자주 동기화할 수 있습니다.
- LDAP은 다중 플랫폼 및 다중 공급업체와 호환됩니다.

LDAP 이름 지정 서비스의 제한 사항

다음은 LDAP 이름 지정 서비스와 연관된 몇 가지 제한 사항입니다.

- LDAP 서버는 현재 자체 클라이언트가 될 수 없습니다.
- LDAP 이름 지정 서비스 설정과 관리는 더 복잡하며 신중한 계획이 필요합니다.
- 동일한 클라이언트 시스템에서 NIS 클라이언트와 고유 LDAP 클라이언트를 함께 사용할 수 없습니다.

주 – 디렉토리 서버(LDAP 서버)는 자신의 클라이언트가 될 수 **없습니다**. 즉, 디렉토리 서버 소프트웨어를 실행 중인 시스템을 LDAP 이름 지정 서비스 클라이언트로 구성할 수 없습니다.

LDAP 이름 지정 서비스 설정(작업 맵)

작업	지침
네트워크 모델을 계획합니다.	145 페이지 “LDAP 네트워크 모델 계획”
디렉토리 정보 트리를 계획합니다.	10 장, “LDAP 이름 지정 서비스에 대한 계획 요구 사항(작업)”
복제 서버를 설정합니다.	148 페이지 “LDAP 및 복제 서버”
보안 모델을 계획합니다.	149 페이지 “LDAP 보안 모델 계획”
클라이언트 프로파일과 기본 속성 값을 선택합니다.	150 페이지 “LDAP에 대한 클라이언트 프로파일 및 기본 속성 값 계획”
데이터 채우기를 계획합니다.	151 페이지 “LDAP 데이터 채우기 계획”

작업	지침
LDAP 이름 지정 서비스와 함께 사용하기 전에 Oracle Directory Server Enterprise Edition을 구성합니다.	**Oracle Directory Server Enterprise Edition**
LDAP 이름 지정 클라이언트와 함께 사용하기 위해 Oracle Directory Server Enterprise Edition을 설정합니다.	11 장, “LDAP 클라이언트를 사용하여 Oracle Directory Server Enterprise Edition 설정(작업)”
LDAP 클라이언트를 초기화합니다.	171 페이지 “LDAP 클라이언트 초기화”
프로파일을 사용하여 클라이언트를 초기화합니다.	172 페이지 “프로파일을 사용하여 LDAP 클라이언트를 초기화하는 방법”
수동으로 클라이언트를 초기화합니다.	176 페이지 “수동으로 LDAP 클라이언트를 초기화하는 방법”
클라이언트를 초기화 해제합니다.	177 페이지 “LDAP 클라이언트 초기화를 해제하는 방법”
서비스 검색 설명자를 사용하여 클라이언트 프로파일을 수정합니다.	156 페이지 “서비스 검색 설명자를 사용하여 다양한 서비스에 대한 클라이언트 액세스 수정”
이름 지정 서비스 정보를 검색합니다.	180 페이지 “LDAP 이름 지정 서비스 정보 검색”
클라이언트 환경을 사용자 정의합니다.	181 페이지 “LDAP 클라이언트 환경 사용자 정의”

LDAP 데이터 교환 형식

LDIF(LDAP 데이터 교환 형식)는 `ldapadd`, `ldapmodify` 등의 많은 LDAP 도구 간에 공통 텍스트 기반 교환 형식으로 사용됩니다. LDIF는 LDIF RFC 2849에서 자세히 설명합니다. 다음은 `ldapadd` 명령으로 생성되는 LDIF 출력의 두 가지 예입니다. `ldaplist(1)`에 `-l` 옵션을 사용하여 다음 정보를 표시합니다.

```
% ldaplist -l hosts myhost
hosts

dn: cn=myhost+ipHostNumber=7.7.7.115,ou=Hosts,dc=mydc,dc=mycom,dc=com
cn: myhost
iphostnumber: 7.7.7.115
objectclass: top
objectclass: device
objectclass: ipHost
description: host 1 - floor 1 - Lab a - building b
% ldaplist -l passwd user1
passwd

dn: uid=user1,ou=People,dc=mydc,dc=mycom,dc=com
uid: user1
cn: user1
userpassword: {crypt}duTx91g7PoNzE
uidnumber: 199995
```

```
gidnumber: 20
gecos: Joe Smith [New York]
homedirectory: /home/user1
loginshell: /bin/csh
objectclass: top
objectclass: shadowAccount
objectclass: account
objectclass: posixAccount
```

LDAP에 정규화된 도메인 이름 사용

LDAP을 사용하여 호스트 이름을 확인하는 경우 LDAP 클라이언트는 호스트 이름에 대해 항상 FQDN(정규화된 도메인 이름)을 반환합니다. LDAP FQDN은 DNS에서 반환되는 FQDN과 유사합니다. 예를 들어, 도메인 이름이 다음과 같다고 가정합니다.

```
west.example.net
```

호스트 이름 *server*를 조회할 때 `gethostbyname()`과 `getnameinfo()`는 모두 FQDN 버전을 반환합니다.

```
server.west.example.net
```

기본 디렉토리 정보 트리

기본적으로 LDAP 클라이언트는 DIT(디렉토리 정보 트리)에 특정 구조가 있다는 가정하에 정보에 액세스합니다. LDAP 서버에서 지원되는 각 도메인에 대해 가정된 구조의 하위 트리가 있습니다. 그러나 SSD(서비스 검색 설명자)를 지정하여 이 기본 구조를 대체할 수 있습니다. 특정 도메인의 기본 DIT에는 특정 정보 유형의 항목이 있는 잘 알려진 여러 컨테이너를 포함하는 기본 컨테이너가 있습니다. 이러한 하위 트리의 이름은 다음 표를 참조하십시오. 이 정보는 RFC 2307 등에서 확인할 수 있습니다.

표 9–1 DIT 기본 위치

기본 컨테이너	정보 유형
`ou=Ethers`	bootparams, ethers
`ou=Group`	group
`ou=Hosts`	hosts, ipnodes, publickey for hosts
`ou=Aliases`	aliases
`ou=Netgroup`	netgroup
`ou=Networks`	networks, netmasks
`ou=People`	passwd, shadow, user_attr, audit_user, publickey for users

표 9–1 DIT 기본 위치 (계속)

기본 컨테이너	정보 유형
ou=Protocols	protocols
ou=Rpc	rpc
ou=Services	services
ou=SolarisAuthAttr	auth_attr
ou=SolarisProfAttr	prof_attr, exec_attr
ou=projects	project
automountMap=auto_*	auto_*

기본 LDAP 스키마

스키마는 LDAP 디렉토리에 항목으로 저장될 수 있는 정보 유형을 설명하는 정의입니다. LDAP 이름 지정 클라이언트를 지원하기 위해 디렉토리 서버의 스키마를 확장해야 할 수도 있습니다. IETF 및 Oracle Solaris 관련 스키마에 대한 자세한 내용은 14 장, “LDAP 이름 지정 서비스(참조)”를 참조하십시오. IETF 웹 사이트(http://www.ietf.org)에서 다양한 RFC에 액세스할 수도 있습니다.

서비스 검색 설명자 및 스키마 매핑

주 – 스키마 매핑을 사용하는 경우 신중하고 일관된 방식으로 사용해야 합니다. 매핑된 속성의 구문이 매핑 대상 속성과 일치하는지 확인하십시오. 즉, 단일 값 속성이 단일 값 속성에 매핑되고, 속성 구문이 일치하고, 매핑된 객체 클래스에 올바른 필수(매핑되었을 수 있음) 속성이 있는지 확인하십시오.

앞에서 설명했듯이 LDAP 이름 지정 서비스에서는 기본적으로 DIT가 특정 방식으로 구성되어 있어야 합니다. 원하는 경우 SSD(서비스 검색 설명자)를 사용하여 DIT의 기본 위치가 아닌 다른 위치에서 검색하도록 LDAP 이름 지정 서비스에 지시할 수 있습니다. 기본 스키마에 의해 지정된 속성 및 객체 클래스 대신 다른 속성 및 객체 클래스를 사용하도록 지정할 수도 있습니다. 기본 필터 목록은 211 페이지 “LDAP 이름 지정 서비스에 사용되는 기본 필터”를 참조하십시오.

SSD에 대한 설명

serviceSearchDescriptor 속성은 LDAP 이름 지정 서비스 클라이언트가 특정 서비스에 대한 정보를 검색하는 방법과 위치를 정의합니다. serviceSearchDescriptor에는 서비스 이름과 세미콜론으로 구분된 기본-범위-필터로 구성된 세 쌍 하나 이상이 차례로

포함됩니다. 기본-범위-필터로 구성된 이러한 세 쌍은 특정 서비스에 대한 검색을 정의하는 데에만 사용되며 순서대로 검색됩니다. 특정 서비스에 대해 기본-범위-필터를 여러 개 지정하면 서비스가 특정 항목을 찾을 때 지정된 범위와 필터를 사용하여 각 기본에서 검색을 수행합니다.

주 – SSD에 포함되어 있지 않을 경우 SSD가 있는 서비스(데이터베이스)는 기본 위치에서 검색되지 않습니다. 서비스에 대해 SSD를 여러 개 지정하면 예측할 수 없는 동작이 발생합니다.

다음 예에서 LDAP 이름 지정 서비스 클라이언트는 `passwd` 서비스에 대해 `ou=west,dc=example,dc=com`에서 단일 레벨 검색을 수행한 후 `ou=east,dc=example,dc=com`에서 단일 레벨 검색을 수행합니다. 사용자 `username`의 `passwd` 데이터를 조회하기 위해 각 `BaseDN`에 대해 기본 LDAP 필터 `(&(objectClass=posixAccount)(uid=username))`이 사용됩니다.

```
serviceSearchDescriptor: passwd:ou=west,dc=example,dc=com;ou=east,
dc=example,dc=com
```

다음 예에서 LDAP 이름 지정 서비스 클라이언트는 `passwd` 서비스에 대해 `ou=west,dc=example,dc=com`에서 하위 트리 검색을 수행합니다. 사용자 `username`의 `passwd` 데이터를 조회하기 위해 LDAP 필터 `(&(fulltimeEmployee=TRUE)(uid=username))`을 사용하여 하위 트리 `ou=west,dc=example,dc=com`을 검색합니다.

```
serviceSearchDescriptor: passwd:ou=west,dc=example,
dc=com?sub?fulltimeEmployee=TRUE
```

특정 서비스 유형에 다중 컨테이너를 연결할 수도 있습니다. 다음 예에서 서비스 검색 설명자는 컨테이너 3개에서 암호 항목을 검색하도록 지정합니다.

```
ou=myuser,dc=example,dc=com
ou=newuser,dc=example,dc=com
ou=extuser,dc=example,dc=com
```

예에서 후행 ','는 `defaultSearchBase`가 SSD의 상대 기본에 추가되었음을 의미합니다.

```
defaultSearchBase: dc=example,dc=com
serviceSearchDescriptor: \
passwd:ou=myuser,;ou=newuser,;ou=extuser,dc=example,dc=com
```

attributeMap 속성

LDAP 이름 지정 서비스를 사용하면 모든 서비스에 대해 하나 이상의 속성 이름을 다시 매핑할 수 있습니다. LDAP 클라이언트는 14 장, “LDAP 이름 지정 서비스(참조)”에

문서화된 잘 알려진 속성을 사용합니다. 속성을 매핑하는 경우 속성이 원래 속성과 동일한 의미와 구문을 갖도록 해야 합니다. userPassword 속성을 매핑하면 문제가 발생할 수도 있습니다.

스키마 매핑을 사용하는 데에는 몇 가지 이유가 있습니다.

- 기존 디렉토리 서버의 속성을 매핑하려고 합니다.
- 대소문자만 다른 사용자 이름이 있는 경우 대소문자를 무시하는 uid 속성을 대소문자를 무시하지 않는 속성에 매핑해야 합니다.

이 속성의 형식은 service:attribute-name=mapped-attribute-name입니다.

특정 서비스에 대해 속성을 2개 이상 매핑하려는 경우 다중 attributeMap 속성을 정의합니다.

다음 예에서 employeeName 및 home 속성은 uid 및 homeDirectory 속성이 passwd 서비스에 사용될 때마다 사용됩니다.

```
attributeMap: passwd:uid=employeeName
attributeMap: passwd:homeDirectory=home
```

passwd 서비스의 gecos 속성을 여러 속성에 매핑할 수 있는 특별한 경우가 있습니다. 예를 들면 다음과 같습니다.

```
attributeMap: gecos=cn sn title
```

이 경우 gecos 값이 공백으로 구분된 cn, sn 및 title 속성 값 목록에 매핑됩니다.

objectclassMap 속성

LDAP 이름 지정 서비스를 사용하면 모든 서비스에 대해 객체 클래스를 다시 매핑할 수 있습니다. 특정 서비스에 대해 객체 클래스를 2개 이상 매핑하려는 경우 다중 objectclassMap 속성을 정의합니다. 다음 예에서 myUnixAccount 객체 클래스는 posixAccount 객체 클래스가 사용될 때마다 사용됩니다.

```
objectclassMap: passwd:posixAccount=myUnixAccount
```

LDAP 클라이언트 프로파일

클라이언트 설정을 간소화하고 각 클라이언트에 대해 동일한 정보를 다시 입력할 필요가 없게 하려면 디렉토리 서버에 단일 클라이언트 프로파일을 만듭니다. 이렇게 하면 단일 프로파일이 이 프로파일을 사용하도록 구성된 모든 클라이언트의 구성을 정의합니다. 프로파일 속성에 대한 이후 변경 사항은 새로 고침 간격으로 정의된 속도로 클라이언트에 전파됩니다.

svc:/network/ldap/client 서비스를 시작하면 LDAP 클라이언트 프로파일에 지정된 구성 정보가 SMF 저장소로 자동으로 가져와집니다.

모든 클라이언트 프로파일은 LDAP 서버에서 잘 알려진 위치에 저장되어야 합니다. 특정 도메인의 루트 DN에는 클라이언트 도메인을 포함하는 `nisDomainObject` 및 `nisDomain` 속성의 객체 클래스가 있어야 합니다. 모든 프로파일은 이 컨테이너에 상대적인 `ou=profile` 컨테이너에 있습니다. 이러한 프로파일을 익명으로 읽을 수 있어야 합니다.

LDAP 클라이언트 프로파일 속성

다음 표에서는 `idsconfig`를 실행할 때 자동으로 설정할 수 있는 LDAP 클라이언트의 프로파일 속성을 보여 줍니다. 수동으로 클라이언트 프로파일을 설정하는 방법에 대한 자세한 내용은 176 페이지 "수동으로 LDAP 클라이언트를 초기화하는 방법" 및 `idsconfig(1M)` 매뉴얼 페이지를 참조하십시오.

표 9–2 LDAP 클라이언트 프로파일 속성

속성	설명
`cn`	프로파일 이름입니다. 이 속성에는 기본값이 없습니다. 값을 지정해야 합니다.
`preferredServerList`	기본 서버의 호스트 주소는 공백으로 구분된 서버 주소 목록입니다. 호스트 이름은 사용하지 마십시오. 이 목록의 서버는 성공적으로 연결될 때까지 `defaultServerList`의 서버보다 **먼저** 순서대로 시도됩니다. 이 속성에는 기본값이 없습니다. `preferredServerList` 또는 `defaultServerList`에 서버를 하나 이상 지정해야 합니다.
`defaultServerList`	기본 서버의 호스트 주소는 공백으로 구분된 서버 주소 목록입니다. 호스트 이름은 사용하지 마십시오. `preferredServerlist`의 서버가 시도된 후 연결될 때까지 클라이언트 서브넷의 기본 서버와 나머지 기본 서버가 차례로 시도됩니다. `preferredServerList` 또는 `defaultServerList`에 서버를 하나 이상 지정해야 합니다. 이 목록의 서버는 기본 서버 목록의 서버 다음에 시도됩니다. 이 속성에는 기본값이 없습니다.
`defaultSearchBase`	잘 알려진 컨테이너 위치에 상대적인 DN입니다. 이 속성에는 기본값이 없습니다. 그러나 특정 서비스에 대해 `serviceSearchDescriptor` 속성이 이 속성을 대체할 수 있습니다.
`defaultSearchScope`	클라이언트에 의한 데이터베이스 검색 범위를 정의합니다. `serviceSearchDescriptor` 속성으로 대체할 수 있습니다. 가능한 값은 `one` 또는 `sub`입니다. 기본값은 `one` 레벨 검색입니다.
`authenticationMethod`	클라이언트에 사용되는 인증 방법을 식별합니다. 기본값은 none(익명)입니다. 자세한 내용은 133 페이지 "LDAP 이름 지정 서비스에 대한 인증 방법 선택"을 참조하십시오.
`credentialLevel`	클라이언트가 인증 시 사용해야 하는 자격 증명 유형을 식별합니다. 선택 항목은 `anonymous`, `proxy` 또는 `self`(per-user라고도 함)입니다. 기본값은 `anonymous`입니다.

표 9–2 LDAP 클라이언트 프로파일 속성 *(계속)*

속성	설명
serviceSearchDescriptor	클라이언트가 DIT의 지점을 하나 이상 확인해야 하는 경우 등에 클라이언트가 이름 지정 데이터베이스를 검색하는 방법과 위치를 정의합니다. 기본적으로 SSD는 정의되어 있지 않습니다.
serviceAuthenticationMethod	클라이언트가 지정된 서비스에 사용하는 인증 방법입니다. 기본적으로 서비스 인증 방법은 정의되어 있지 않습니다. 서비스에 serviceAuthenticationMethod가 정의되어 있지 않으면 기본적으로 authenticationMethod 값으로 설정됩니다.
attributeMap	클라이언트에 사용되는 속성 매핑입니다. 기본적으로 attributeMap은 정의되어 있지 않습니다.
objectclassMap	클라이언트에 사용되는 객체 클래스 매핑입니다. 기본적으로 objectclassMap은 정의되어 있지 않습니다.
searchTimeLimit	시간 초과 전에 클라이언트가 검색이 완료되도록 허용해야 하는 최대 시간(초)입니다. 이는 LDAP 서버가 검색이 완료되도록 허용하는 시간에 영향을 주지 않습니다. 기본값은 30초입니다.
bindTimeLimit	시간 초과 전에 클라이언트가 서버에 바인딩하도록 허용해야 하는 최대 시간(초)입니다. 기본값은 30초입니다.
followReferrals	클라이언트가 LDAP 참조를 따라야 하는지 여부를 지정합니다. 가능한 값은 TRUE 또는 FALSE입니다. 기본값은 TRUE입니다.
profileTTL	ldap_cachemgr(1M)에 의한 LDAP 서버의 클라이언트 프로파일 새로 고침 간격입니다. 기본값은 43200초 또는 12시간입니다. 값 0을 지정하면 프로파일이 새로 고쳐지지 않습니다.

로컬 LDAP 클라이언트 속성

다음 표에서는 ldapclient 명령을 사용하여 로컬로 설정할 수 있는 LDAP 클라이언트 속성을 나열합니다. 자세한 내용은 ldapclient(1M) 매뉴얼 페이지를 참조하십시오.

표 9–3 로컬 LDAP 클라이언트 속성

속성	설명
adminDN	관리자 자격 증명에 대한 관리자 항목의 식별 이름을 지정합니다. 클라이언트 시스템에서 enableShadowUpdate 스위치의 값이 true이고 credentialLevel의 값이 self가 아니면 adminDN을 지정해야 합니다.
adminPassword	관리자 자격 증명에 대한 관리자 항목의 암호를 지정합니다. 클라이언트 시스템에서 enableShadowUpdate 스위치의 값이 true이고 credentialLevel의 값이 self가 아니면 adminPassword를 정의해야 합니다.

표 9–3 로컬 LDAP 클라이언트 속성 *(계속)*

속성	설명
domainName	클라이언트 시스템의 기본 도메인이 되는 클라이언트 도메인 이름을 지정합니다. 이 속성에는 기본값이 없으며 지정해야 합니다.
proxyDN	프록시의 식별 이름입니다. 클라이언트 시스템이 proxy의 credentialLevel로 구성된 경우 proxyDN을 지정해야 합니다.
proxyPassword	프록시의 암호입니다. 클라이언트 시스템이 프록시의 credentialLevel로 구성된 경우 proxyPassword를 정의해야 합니다.
certificatePath	인증서 데이터베이스가 포함된 로컬 파일 시스템의 디렉토리입니다. 클라이언트 시스템이 TLS를 사용하여 authenticationMethod 또는 serviceAuthenticationMethod로 구성된 경우 이 속성이 사용됩니다. 기본값은 /var/ldap입니다.

주 – SSD의 BaseDN에 **후행 쉼표가 포함**된 경우 defaultSearchBase의 상대 값으로 처리됩니다. 검색을 수행하기 전에 defaultSearchBase의 값이 BaseDN에 추가됩니다.

ldap_cachemgr 데몬

ldap_cachemgr은 LDAP 클라이언트 시스템에서 실행되는 데몬입니다. svc:/network/ldap/client 서비스는 ldap_cachemgr 데몬을 관리하므로 데몬이 제대로 실행되려면 해당 서비스를 사용으로 설정해야 합니다. 데몬은 다음과 같은 주요 기능을 수행합니다.

- root로 실행되며 구성 데이터에 대한 액세스 권한을 획득합니다.
- 서버의 프로파일에 저장된 클라이언트 구성 정보를 새로 고치고 이 데이터를 클라이언트에서 가져옵니다.
- 사용할 활성 LDAP 서버의 정렬된 목록을 유지 관리합니다.
- 다양한 클라이언트가 제출한 일반적인 조회 요청을 일부 캐시하여 조회 효율성을 향상시킵니다.
- 호스트 조회 효율성을 향상시킵니다.
- enableShadowUpdate 스위치가 true로 설정된 경우 구성된 관리자 자격 증명에 대한 액세스 권한을 획득하고 shadow 데이터를 업데이트합니다.

주 – LDAP 이름 지정 서비스가 작동하려면 ldap_cachemgr이 항상 실행되고 있어야 합니다.

자세한 내용은 ldap_cachemgr(1M) 매뉴얼 페이지를 참조하십시오.

LDAP 이름 지정 서비스 보안 모델

LDAP 이름 지정 서비스는 두 가지 방법으로 LDAP 저장소를 사용할 수 있습니다. 한 가지 방법은 이름 지정 서비스와 인증 서비스 둘 다의 소스로 사용하는 것입니다. 다른 방법은 이름 지정 데이터의 소스로만 사용하는 것입니다. 이 절에서는 클라이언트 ID의 개념, 인증 방법, `pam_ldap` 및 `pam_unix_*` 모듈 및 LDAP 저장소가 이름 지정 서비스와 인증 서비스 둘 다로 사용되는 경우의 계정 관리에 대해 설명합니다. 또한 이 절에서는 Kerberos 환경(**Oracle Solaris 11.1 관리: 보안 서비스**의 제VI부, "Kerberos 서비스") 및 `pam_krb5(5)` 모듈과 함께 LDAP 이름 지정 서비스를 사용하는 방법에 대해 설명합니다.

주 – 이전에는 `pam_ldap` 계정 관리를 사용으로 설정한 경우 모든 사용자가 시스템에 로그인할 때마다 인증을 위해 로그인 암호를 제공해야 했습니다. 따라서 `ssh` 등의 도구를 사용하여 암호 기반이 아닌 로그인을 시도하면 실패했습니다.

사용자가 로그인할 때 디렉토리 서버에 인증하지 않고 계정 관리를 수행하고 사용자의 계정 상태를 검색합니다. 디렉토리 서버의 새 컨트롤은 기본적으로 사용으로 설정되는 `1.3.6.1.4.1.42.2.27.9.5.8`입니다.

기본값이 아닌 다른 값에 대해 이 컨트롤을 수정하려면 디렉토리 서버에 ACI(액세스 제어 명령)를 추가합니다.

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

주 – Kerberos를 인증 시스템으로 사용하고 LDAP 이름 지정 시스템과 통합하면 Kerberos를 통해 기업의 SSO(Single Sign-On) 환경을 지원할 수 있습니다. 사용자 또는 호스트 단위로 LDAP 이름 지정 데이터를 질의할 때도 동일한 ID 시스템을 사용할 수 있습니다.

LDAP 저장소의 정보에 액세스하기 위해 클라이언트는 먼저 ID를 디렉토리 서버에 증명합니다. 이 ID는 익명이거나 LDAP 서버에서 인식되는 호스트 또는 사용자일 수 있습니다. LDAP 서버는 클라이언트 ID와 서버의 ACI(액세스 제어 정보)를 기반으로 클라이언트가 디렉토리 정보를 읽을 수 있도록 합니다. ACI에 대한 자세한 내용은 사용 중인 Oracle Directory Server Enterprise Edition 버전에 대한 **관리 설명서**를 참조하십시오.

ID가 요청을 보내는 호스트를 기반으로 하는 경우 proxy 인증을 사용하는 것입니다. 호스트가 인증되면 해당 호스트의 모든 사용자에게 액세스 권한이 부여됩니다. ID가

사용자를 기반으로 하는 경우 per-user 인증을 사용하는 것입니다. 호스트의 각 사용자를 인증해야 해당 사용자에게 액세스 권한이 부여됩니다.

클라이언트가 특정 요청에 대해 익명이 아닌 사용자로 연결하는 경우 클라이언트와 서버 둘 다에서 지원되는 인증 방법을 사용하여 ID를 서버에 증명해야 합니다. 클라이언트가 ID를 증명하면 다양한 LDAP 요청을 실행할 수 있습니다.

시스템에 로그인할 때 PAM 서비스가 로컬 시스템, LDAP 서비스, Kerberos 서버 또는 이 세 가지 소스 조합에 있는 정보를 사용하여 로그인 시도가 성공할지 여부를 확인할 수도 있습니다. `pam_kerb` 모듈을 사용하는 경우 Kerberos 서버가 액세스 허용 여부를 결정합니다. `pam_ldap` 모듈을 사용하는 경우에는 LDAP 서버가 이러한 결정의 절반을 담당하고 로컬 호스트가 나머지 절반을 담당해야 합니다. 로컬 호스트의 정보와 `pam_unix_*` 모듈을 사용하는 경우 로컬에서 결정됩니다.

`pam_ldap`을 사용하여 LDAP 서비스를 통해 로그인하는 경우 이름 지정 서비스와 인증 서비스(`pam_ldap`)가 디렉토리에 액세스하는 방법에 차이가 있습니다. 이름 지정 서비스는 사전 정의된 ID를 기반으로 디렉토리에서 다양한 항목과 해당 속성을 읽습니다. 인증 서비스는 사용자 이름과 암호로 LDAP 서버에 대해 인증을 수행하여 사용자가 올바른 암호를 입력했는지 여부를 증명합니다. 인증 서비스에 대한 자세한 내용은 `pam_ldap(5)` 매뉴얼 페이지를 참조하십시오.

Kerberos를 사용하여 인증하고 LDAP 이름 지정 서비스의 인증도 사용으로 설정된 경우(per-user 모드에 필요) Kerberos가 이중 기능을 제공할 수 있습니다. Kerberos는 서버에 대해 인증을 수행하고, 주체(사용자 또는 호스트)의 Kerberos ID를 사용하여 디렉토리에 대해 인증을 수행합니다. 이렇게 하면 시스템에 대해 인증을 수행하는 데 사용되는 것과 동일한 사용자 ID가 조회 및 업데이트를 위해 디렉토리에 대해 인증을 수행하는 데에도 사용됩니다. 원하는 경우 관리자는 디렉토리의 ACI(액세스 제어 정보)를 사용하여 이름 지정 서비스에서 반환되는 결과를 제한할 수 있습니다.

전송 계층 보안

TLS(전송 계층 보안)를 사용하여 LDAP 클라이언트와 디렉토리 서버 간의 통신 보안을 유지하고 프라이버시 및 데이터 무결성을 제공할 수 있습니다. TLS 프로토콜은 SSL(Secure Sockets Layer) 프로토콜의 수퍼 세트입니다. LDAP 이름 지정 서비스는 TLS 연결을 지원합니다. SSL을 사용하면 디렉토리 서버와 클라이언트에 로드가 추가됩니다.

SSL용 디렉토리 서버를 설정해야 합니다. SSL용 Oracle Directory Server Enterprise Edition을 설정하는 방법에 대한 자세한 내용은 사용 중인 Oracle Directory Server Enterprise Edition 버전에 대한 관리 설명서를 참조하십시오. SSL용 LDAP 클라이언트도 설정해야 합니다.

TLS를 사용하는 경우 필요한 보안 데이터베이스를 설치해야 합니다. 특히 인증서와 키 데이터베이스 파일이 필요합니다. 예를 들어, Netscape Communicator의 이전 데이터베이스 형식을 사용하는 경우 `cert7.db` 및 `key3.db`라는 2개 파일이 필요합니다. Mozilla의 새 데이터베이스 형식을 사용하는 경우에는 `cert8.db`, `key3.db` 및

secmod.db라는 3개 파일이 필요합니다. cert7.db 또는 cert8.db 파일에 인증된 인증서가 포함되어 있으며, key3.db 파일에 클라이언트의 키가 포함되어 있습니다. LDAP 이름 지정 서비스 클라이언트가 클라이언트 키를 사용하지 않는 경우에도 이 파일은 있어야 합니다. secmod.db 파일에는 PKCS#11 모듈 등의 보안 모듈이 포함되어 있습니다. 이전 형식을 사용하는 경우에는 이 파일이 필요 없습니다.

자세한 내용은 177 페이지 “TLS 보안 설정”을 참조하십시오.

클라이언트 자격 증명 레벨 지정

LDAP 이름 지정 서비스 클라이언트는 클라이언트의 자격 증명 레벨에 따라 LDAP 서버에 대해 인증을 수행합니다. LDAP 클라이언트에는 디렉토리 서버에 대해 인증을 수행할 때 사용되는 여러 레벨을 지정할 수 있습니다.

- anonymous
- proxy
- proxy anonymous
- self(이 문서에서는 per-user라고 함)

LDAP anonymous 자격 증명 레벨

anonymous 액세스를 사용하는 경우 모든 사용자가 사용할 수 있는 데이터에만 액세스할 수 있습니다. 익명 모드에서는 LDAP BIND 작업이 수행되지 않습니다. 또한 보안에 미치는 영향을 고려해야 합니다. 특정 디렉토리 부분에 대해 anonymous 액세스를 허용하면 해당 디렉토리에 액세스할 수 있는 모든 사용자가 읽기 권한을 갖습니다. anonymous 자격 증명 레벨을 사용하는 경우 모든 LDAP 이름 지정 항목과 속성에 대해 읽기 권한을 허용해야 합니다.

주의 – 디렉토리에 대해 anonymous 쓰기를 허용하면 다른 사용자의 암호나 ID를 비롯하여 쓰기 권한이 있는 DIT의 정보를 모든 사용자가 변경할 수 있게 되므로 이렇게 하면 안됩니다.

주 – Oracle Directory Server Enterprise Edition을 사용하면 IP 주소, DNS 이름, 인증 방법 및 시간을 기반으로 액세스를 제한할 수 있습니다. 추가 제한을 적용하여 액세스를 제한할 수도 있습니다. 자세한 내용은 사용 중인 Oracle Directory Server Enterprise Edition 버전에 대한 **관리 설명서**의 “액세스 제어 관리”를 참조하십시오.

LDAP proxy 자격 증명 레벨

클라이언트가 LDAP 바인드 자격 증명(프록시 계정이라고도 함)의 단일 공유 세트에 대해 인증을 수행하거나 이 세트에 바인딩됩니다. 이 프록시 계정은 디렉토리에 바인딩할 수 있는 모든 항목일 수 있습니다. 이 프록시 계정에 LDAP 서버에서 이름 지정

서비스 기능을 수행할 수 있는 권한이 충분해야 합니다. 프록시 계정은 시스템별 공유 리소스입니다. 즉, 루트 사용자를 포함하여 프록시 액세스를 사용하여 시스템에 로그인한 각 사용자는 해당 시스템의 다른 모든 사용자와 동일한 결과를 보게 됩니다. proxy 자격 증명 레벨을 사용하는 모든 클라이언트에서 proxyDN과 proxyPassword를 구성해야 합니다. 암호화된 proxyPassword는 클라이언트에 로컬로 저장됩니다. 각 클라이언트 그룹에 대해 다른 프록시를 설정할 수 있습니다. 예를 들어, 영업 클라이언트가 급여 정보를 포함하는 HR 디렉토리에 액세스할 수 없도록 하는 동시에 모든 영업 클라이언트가 회사 전체의 액세스 가능 디렉토리와 영업 디렉토리에 모두 액세스할 수 있도록 프록시를 구성할 수 있습니다. 극단적인 경우 각 클라이언트에 다른 프록시를 지정하거나 모든 클라이언트에 프록시를 1개만 지정할 수도 있습니다. 일반적인 LDAP 배포는 두 극단 사이에 있습니다. 주의해서 원하는 사항을 선택하십시오. 프록시 에이전트가 너무 적으면 리소스에 대한 사용자 액세스를 제대로 제어하지 못하게 될 수 있습니다. 그러나 프록시가 너무 많으면 시스템 설정과 유지 관리가 복잡해집니다. 환경에 따라 프록시 사용자에게 적절한 권한을 부여해야 합니다. 구성에 가장 적합한 인증 방법을 결정하는 방법에 대한 자세한 내용은 132 페이지 “LDAP 클라이언트에 대한 자격 증명 저장소”를 참조하십시오.

프록시 사용자의 암호가 변경되는 경우 해당 프록시 사용자를 사용하는 모든 클라이언트에서 암호를 업데이트해야 합니다. LDAP 계정에 암호 에이징을 사용하는 경우 프록시 사용자에 대해 이를 해제해야 합니다.

주 – proxy 자격 증명 레벨은 특정 시스템의 모든 사용자와 프로세스에 적용됩니다. 두 사용자가 서로 다른 이름 지정 정책을 사용해야 하는 경우 서로 다른 시스템을 사용하거나 per-user 인증 모델을 사용해야 합니다.

또한 클라이언트가 proxy 자격 증명을 사용하여 인증하는 경우 모든 서버에서 proxyDN의 proxyPassword가 동일해야 합니다.

LDAP proxy anonymous 자격 증명 레벨

proxy anonymous는 자격 증명 레벨이 2개 이상 정의된다는 점에서 다중 값 항목입니다. proxy anonymous 레벨이 지정된 클라이언트는 먼저 프록시 ID를 사용하여 인증을 시도합니다. 어떤 이유로든(사용자 잠금, 암호 만료 등) 클라이언트가 프록시 사용자로 인증할 수 없는 경우 익명 액세스를 사용합니다. 이 경우 디렉토리 구성 방법에 따라 다른 서비스 레벨이 발생할 수 있습니다.

LDAP per-user 인증

per-user(self) 인증은 디렉토리 서버에 대해 인증을 수행할 때 Kerberos ID(주체)를 사용하여 각 사용자나 각 시스템에 대해 조회를 수행합니다. per-user 인증을 사용하는 경우 시스템 관리자가 ACI(액세스 제어 명령), ACL(액세스 제어 목록), 역할, 그룹 또는 기타 디렉토리 액세스 제어 방식을 사용하여 특정 사용자나 시스템에 대해 특정 이름 지정 서비스 데이터 액세스를 허용하거나 거부할 수 있습니다.

주 – per-user 모드를 구성하는 경우 이 모드를 사용으로 설정하기 위한 구성 값은 per-user 모드를 나타내는 "self"입니다.

per-user 인증 모델을 사용하려면 Kerberos SSO(Single Sign-On) 서비스를 배포해야 합니다. 또한 배포에 사용된 디렉토리 서버 중 하나 이상이 SASL 및 SASL/GSSAPI 인증 방식을 지원해야 합니다. Kerberos는 호스트 이름 조회 시 LDAP 대신 파일과 DNS를 사용하기 때문에 이 환경에는 DNS를 배포해야 합니다. 또한 per-user 인증을 사용하려면 `nscd`를 사용으로 설정해야 합니다. 이 구성에서 `nscd` 데몬은 선택적 구성 요소가 아닙니다.

enableShadowUpdate 스위치

클라이언트에서 `enableShadowUpdate` 스위치가 `true`로 설정된 경우 관리자 자격 증명을 사용하여 섀도우 데이터를 업데이트합니다. 섀도우 데이터는 디렉토리 서버의 `shadowAccount` 객체 클래스에 저장됩니다. 126 페이지 “로컬 LDAP 클라이언트 속성”에 설명된 대로 관리자 자격 증명은 `adminDN` 및 `adminPassword` 속성의 값으로 정의됩니다. 이러한 관리자 자격 증명은 다른 용도로 사용되지 않습니다.

관리자 자격 증명에는 `Proxy` 자격 증명과 유사한 등록 정보가 있습니다. 예외적으로, 관리자 자격 증명의 경우 사용자가 섀도우 데이터를 읽거나 업데이트하려면 영역에 대한 모든 권한이 있거나 유효 UID `root`가 있어야 합니다. 디렉토리에 바인딩할 수 있는 모든 항목에 관리자 자격 증명을 지정할 수 있습니다. 그러나 LDAP 서버의 동일한 디렉토리 관리자 ID(`cn=Directory Manager`)를 사용하지 **마십시오**.

관리자 자격 증명을 가진 이 항목에는 디렉토리의 섀도우 데이터를 읽고 쓸 수 있는 권한이 충분해야 합니다. 항목은 시스템별 공유 리소스이므로 모든 클라이언트에서 `adminDN` 및 `adminPassword` 속성을 구성해야 합니다. 암호화된 `adminPassword`는 클라이언트에 로컬로 저장됩니다. 암호는 클라이언트에 대해 구성된 것과 동일한 인증 방법을 사용합니다. 관리자 자격 증명은 특정 시스템의 모든 사용자와 프로세스가 섀도우 데이터를 읽고 업데이트하는 데 사용됩니다.

LDAP 클라이언트에 대한 자격 증명 저장소

프록시 ID를 사용하도록 클라이언트를 구성하면 클라이언트가 `svc:/network/ldap/client` 서비스에 프록시 정보를 저장합니다. 현재 LDAP 구현에서는 proxy 자격 증명이 클라이언트 프로파일에 저장되지 않습니다. 초기화 중에 `ldapclient`를 사용하여 설정된 proxy 자격 증명은 모두 SMF 저장소에 저장됩니다. 이로 인해 프록시의 DN 및 암호 정보에 대한 보안이 향상됩니다. 클라이언트 프로파일 설정에 대한 자세한 내용은 12 장, “LDAP 클라이언트 설정(작업)”을 참조하십시오.

마찬가지로, 섀도우 데이터 업데이트가 가능하도록 클라이언트를 구성하는 경우 클라이언트 자격 증명 레벨이 `self`가 아니면 클라이언트는 `svc:/network/ldap/client` 서비스에 해당 정보를 저장합니다.

per-user 인증을 사용하도록 클라이언트를 구성하는 경우 각 주체(각 사용자나 호스트)에 대한 Kerberos ID와 Kerberos 티켓 정보가 인증 중에 사용됩니다. 이 환경에서 디렉토리 서버는 Kerberos 주체를 DN에 매핑하고, Kerberos 자격 증명이 해당 DN에 대해 인증을 수행하는 데 사용됩니다. 그런 다음 디렉토리 서버는 ACI(액세스 제어 명령) 방식을 사용하여 필요에 따라 이름 지정 서비스 데이터 액세스를 허용하거나 거부합니다. 이 경우 Kerberos 티켓 정보가 디렉토리 서버에 대해 인증을 수행하는 데 사용되며, 인증 DN 또는 암호가 시스템에 저장되지 않습니다. 따라서 이 유형의 구성에서는 클라이언트가 `ldapclient` 명령으로 초기화된 경우 `adminDN` 및 `adminPassword` 속성을 지정할 필요가 없습니다.

LDAP 이름 지정 서비스에 대한 인증 방법 선택

`proxy` 또는 `proxy-anonymous` 자격 증명 레벨을 클라이언트에 지정할 때는 프록시가 디렉토리 서버에 대해 인증되는 방법도 선택해야 합니다. 기본적으로 인증 방법은 익명 액세스를 의미하는 `none`입니다. 인증 방법에 전송 보안 옵션이 연관될 수도 있습니다.

자격 증명 레벨과 마찬가지로 인증 방법에는 다중 값이 있을 수 있습니다. 예를 들어, 클라이언트 프로파일에서 클라이언트가 먼저 TLS로 보안된 `simple` 방법을 사용하여 바인딩하도록 지정할 수 있습니다. 실패할 경우 클라이언트는 `sasl/digest-MD5` 방법을 사용하여 바인딩합니다. 이 경우 `authenticationMethod`는 `tls:simple;sasl/digest-MD5`가 됩니다.

LDAP 이름 지정 서비스는 일부 SASL(Simple Authentication and Security Layer) 방식을 지원합니다. 이러한 방식을 사용하면 TLS 없이도 안전하게 암호를 교환할 수 있습니다. 그러나 이러한 방식은 데이터 무결성이나 프라이버시를 제공하지 않습니다. SASL에 대한 자세한 내용은 RFC 2222를 참조하십시오.

지원되는 인증 방식은 다음과 같습니다.

- `none`

  클라이언트가 디렉토리에 대해 인증을 수행하지 않습니다. 이는 `anonymous` 자격 증명 레벨과 같습니다.

- `simple`

  클라이언트 시스템이 `simple` 인증 방법을 사용하는 경우 사용자 암호를 일반 텍스트로 보내 서버에 바인딩됩니다. 따라서 세션을 IPsec로 보호하지 않으면 암호가 스누핑에 노출될 수 있습니다. `simple` 인증 방법을 사용할 경우의 주요 장점은 모든 디렉토리 서버가 이를 지원하며 설정하기가 쉽다는 것입니다.

- `sasl/digest-MD5`

  클라이언트 암호가 인증 중에 보호되지만 세션은 암호화되지 않습니다. Oracle Directory Server Enterprise Edition을 비롯한 일부 디렉토리 서버는 `sasl/digest-MD5` 인증 방법도 지원합니다. `digest-MD5`의 주요 장점은 인증 중에 암호가 일반 텍스트로 전송되지 않으므로 `simple` 인증 방법보다 더 안전하다는 것입니다. `digest-MD5`에 대한 자세한 내용은 RFC 2831을 참조하십시오. `digest-MD5`는 보안이 향상되어 `cram-MD5`보다 나은 방법입니다.

sasl/digest-MD5를 사용하는 경우 인증 보안이 유지되지만 세션은 보호되지 않습니다.

주 – Oracle Directory Server Enterprise Edition을 사용 중인 경우 암호를 디렉토리에 **일반 텍스트로 저장해야 합니다**.

- sasl/cram-MD5

  이 경우 LDAP 세션이 암호화되지 않지만 sasl/cram-MD5를 사용하여 인증이 수행되기 때문에 클라이언트 암호는 인증 중에 보호됩니다. 이는 오래된 인증 방법이므로 사용하면 안됩니다.

- sasl/GSSAPI

  이 인증 방법은 self 자격 증명 모드와 함께 사용되어 사용자별 조회를 가능하게 합니다. 클라이언트 자격 증명을 사용하도록 지정된 사용자별 nscd는 sasl/GSSAPI 방법과 클라이언트의 Kerberos 자격 증명을 사용하여 디렉토리 서버에 바인딩됩니다. 디렉토리 서버에서 사용자 단위로 액세스를 제어할 수 있습니다.

- tls:simple

  클라이언트가 simple 방법을 사용하여 바인딩하며 세션이 암호화됩니다. 암호가 보호됩니다.

- tls:sasl/cram-MD5

  LDAP 세션이 암호화되며 클라이언트가 sasl/cram-MD5를 사용하여 디렉토리 서버에 대해 인증을 수행합니다.

- tls:sasl/digest-MD5

  LDAP 세션이 암호화되며 클라이언트가 sasl/digest-MD5를 사용하여 디렉토리 서버에 대해 인증을 수행합니다.

주의 – Oracle Directory Server Enterprise Edition에서 digest-MD5를 사용하려면 암호를 일반 텍스트로 저장해야 합니다. 인증 방법이 sasl/digest-MD5 또는 tls:sasl/digest-MD5로 설정된 경우 프록시 사용자의 암호를 일반 텍스트로 저장해야 합니다. 암호를 일반 텍스트로 저장하는 경우 읽을 수 없도록 userPassword 속성에 올바른 ACI가 있는지 확인하십시오.

다음 표에는 다양한 인증 방법과 해당 특징이 요약되어 있습니다.

표 9–4 인증 방법

	바인딩	전송 시 암호	Oracle Directory Server Enterprise Edition의 암호	세션
none	아니오	해당 없음	해당 없음	암호화 안함

표 9–4 인증 방법 (계속)

	바인딩	전송 시 암호	Oracle Directory Server Enterprise Edition의 암호	세션
simple	예	일반 텍스트	모두	암호화 안함
sasl/digest-MD5	예	암호화	일반 텍스트	암호화 안함
sasl/cram-MD5	예	암호화	해당 없음	암호화 안함
sasl/GSSAPI	예	Kerberos	Kerberos	암호화
tls:simple	예	암호화	모두	암호화
tls:sasl/cram-MD5	예	암호화	해당 없음	암호화
tls:sasl/digest-MD5	예	암호화	일반 텍스트	암호화

LDAP의 특정 서비스에 대한 인증 방법 지정

serviceAuthenticationMethod 속성에서 특정 서비스에 대한 인증 방법을 지정할 수 있습니다. 다음 서비스에 대해 인증 방법을 선택할 수 있습니다.

- passwd-cmd

  이 서비스는 passwd(1)에서 로그인 암호와 암호 속성을 변경하는 데 사용됩니다.

- keyserv

  이 서비스는 chkey(1) 및 newkey(1M) 유틸리티에서 사용자의 Diffie-Hellman 키 쌍을 만들고 변경하는 데 사용됩니다.

- pam_ldap

  이 서비스는 pam_ldap(5)로 사용자를 인증하는 데 사용됩니다.

  pam_ldap은 계정 관리를 지원합니다.

주 – 서비스에 serviceAuthenticationMethod가 설정되어 있지 않으면 기본적으로 authenticationMethod 속성 값으로 설정됩니다.

주 – per-user 모드에서는 137 페이지 “Kerberos 서비스 모듈”(pam Kerberos)이 인증 서비스로 사용됩니다. 이 작업 모드에서는 ServiceAuthenticationMethod가 필요 없습니다.

주 – enableShadowUpdate 스위치를 true로 설정하면 방법이 정의된 경우 ldap_cachemgr 데몬이 passwd-cmd의 serviceAuthenticationMethod 매개변수에 정의된 인증 방법을 사용하여 LDAP 서버에 바인딩됩니다. 그렇지 않으면 authenticationMethod가 사용됩니다. 이 데몬은 none 인증 방법을 사용하지 않습니다.

다음 예에서는 사용자가 sasl/digest-MD5를 사용하여 디렉토리 서버에 대해 인증을 수행하지만 SSL 세션을 사용하여 암호를 변경하는 클라이언트 프로파일의 섹션을 보여 줍니다.

```
serviceAuthenticationMethod=pam_ldap:sasl/digest-MD5
serviceAuthenticationMethod=passwd-cmd:tls:simple
```

플러그 가능 인증 방법

PAM 프레임워크를 사용하면 pam_unix_*, pam_krb5 및 pam_ldap_* 모듈을 포함하여 여러 인증 서비스 중에서 선택할 수 있습니다.

per-user 인증 방법을 사용하는 경우 위에 나열된 세 가지 방법 중 가장 강력한 인증 서비스인 pam_krb5를 사용으로 설정해야 합니다. pam_krb5(5) 및 **Oracle Solaris 11.1 관리: 보안 서비스**를 참조하십시오.

pam_krb5 인증 시스템은 per-user 인증이 사용으로 설정되지 않은 경우에도 사용할 수 있습니다. proxy 또는 anonymous 자격 증명 레벨을 사용하여 디렉토리 서버 데이터에 액세스하는 경우에는 사용자 단위로 디렉토리 데이터에 대한 액세스를 제한할 수 없습니다.

유연성 증가, 더 강력한 인증 방법 지원 및 계정 관리 사용 가능성 때문에 anonymous 또는 proxy 인증 방법을 사용하는 경우 pam_unix_* 모듈보다 pam_ldap 모듈을 사용하는 것이 좋습니다.

pam_unix_* 서비스 모듈

/etc/pam.conf 파일을 변경하지 않은 경우 기본적으로 UNIX 인증이 사용으로 설정됩니다.

주 – Oracle Solaris 릴리스에서는 pam_unix 모듈이 제거되었으며 더 이상 지원되지 않습니다. 다른 서비스 모듈 세트를 통해 상응하는 기능이나 더 나은 기능을 사용할 수 있습니다. 따라서 본 설명서에서 pam_unix는 pam_unix 모듈 자체가 아니라 이에 상응하는 기능을 나타냅니다.

다음은 원래 pam_unix 모듈에 상응하는 기능을 제공하는 모듈의 목록입니다.

pam_authtok_check(5)

pam_authtok_get(5)
pam_authtok_store(5)
pam_dhkeys(5)
pam_passwd_auth(5)
pam_unix_account(5)
pam_unix_auth(5)
pam_unix_cred(5)
pam_unix_session(5)

pam_unix_* 모듈은 다음 목록에 설명된 대로 기존 UNIX 인증 모델을 따릅니다.

1. 클라이언트가 이름 서비스에서 사용자의 암호화된 암호를 검색합니다.
2. 사용자에게 사용자 암호를 묻는 메시지가 표시됩니다.
3. 사용자 암호가 암호화됩니다.
4. 클라이언트가 암호화된 두 암호를 비교하여 사용자 인증 여부를 결정합니다.

pam_unix_* 모듈을 사용할 때는 다음과 같은 두 가지 제한 사항이 적용됩니다.

- 암호가 UNIX crypt 형식으로 저장되어야 하며 일반 텍스트를 비롯한 다른 암호화 방법으로 저장되면 안됩니다.
- 이름 서비스가 userPassword 속성을 읽을 수 있어야 합니다.

  예를 들어, 자격 증명 레벨을 anonymous로 설정하면 모든 사용자가 userPassword 속성을 읽을 수 있어야 합니다. 마찬가지로, 자격 증명 레벨을 proxy로 설정하면 프록시 사용자가 userPassword 속성을 읽을 수 있어야 합니다.

주 – Oracle Directory Server Enterprise Edition에서 digest-MD5를 사용하려면 암호를 일반 텍스트로 저장해야 하므로 UNIX 인증은 sasl 인증 방법 digest-MD5와 호환되지 않습니다. UNIX 인증에서는 crypt 형식으로 암호를 저장해야 합니다.

주 – pam_unix_account 모듈은 enableShadowUpdate 스위치가 true로 설정된 경우 계정 관리를 지원합니다. 원격 LDAP 사용자 계정 컨트롤은 passwd 및 shadow 파일에 정의된 로컬 사용자 계정에 컨트롤이 적용되는 것과 동일한 방식으로 적용됩니다. enableShadowUpdate 모드에서 시스템은 암호 에이징 및 계정 잠금을 위해 LDAP 계정에 대해 LDAP 서버의 섀도우 데이터를 업데이트하고 사용합니다. 물론 로컬 계정의 섀도우 데이터는 로컬 클라이언트 시스템에만 적용되고 LDAP 사용자 계정의 섀도우 데이터는 모든 클라이언트 시스템의 사용자에게 적용됩니다.

암호 기록 검사는 로컬 클라이언트에 대해서만 지원되고 LDAP 사용자 계정에 대해서는 지원되지 않습니다.

Kerberos 서비스 모듈

pam_krb5(5) 매뉴얼 페이지와 **Oracle Solaris 11.1 관리: 보안 서비스**를 참조하십시오.

LDAP 서비스 모듈

LDAP 인증을 구현할 때 사용자는 pam_ldap의 serviceAuthenticationMethod 매개변수에 정의된 인증 방법(있는 경우)을 사용하여 LDAP 서버에 바인딩됩니다. 그렇지 않으면 authenticationMethod가 사용됩니다.

pam_ldap이 사용자 ID 및 제공된 암호로 서버에 바인딩될 수 있으면 사용자를 인증합니다.

주 – 이전에는 pam_ldap 계정 관리를 사용으로 설정한 경우 모든 사용자가 시스템에 로그인할 때마다 인증을 위해 로그인 암호를 제공해야 했습니다. 따라서 ssh 등의 도구를 사용하여 암호 기반이 아닌 로그인을 시도하면 실패했습니다.

사용자가 로그인할 때 디렉토리 서버에 인증하지 않고 계정 관리를 수행하고 사용자의 계정 상태를 검색합니다. 디렉토리 서버의 새 컨트롤은 기본적으로 사용으로 설정되는 1.3.6.1.4.1.42.2.27.9.5.8입니다.

기본값이 아닌 다른 값에 대해 이 컨트롤을 수정하려면 디렉토리 서버에 ACI(액세스 제어 명령)를 추가합니다.

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

---

pam_ldap은 userPassword 속성을 읽지 않습니다. 따라서 UNIX 인증을 사용하는 다른 클라이언트가 없는 경우 userPassword 속성을 읽기 위한 권한을 부여할 필요가 없습니다. 또한 pam_ldap은 none 인증 방법을 지원하지 않습니다. 따라서 클라이언트가 pam_ldap을 사용할 수 있도록 serviceAuthenticationMethod 또는 authenticationMethod 속성을 정의해야 합니다. 자세한 내용은 pam_ldap(5) 매뉴얼 페이지를 참조하십시오.

주의 – simple 인증 방법을 사용하면 전송 중인 userPassword 속성을 제3자가 읽을 수 있습니다.

다음 표에는 인증 방식 간의 주요 차이점이 요약되어 있습니다.

표 9–5 LDAP의 인증 동작

이벤트	pam_unix_*	pam_ldap	pam_krb5
암호 전송됨	passwd 서비스 인증 방법 사용	passwd 서비스 인증 방법 사용	암호가 아니라 Kerberos SSO(Single Sign-On) 기술 사용
새 암호 전송됨	암호화됨	TLS를 사용하지 않는 한 암호화 안함	Kerberos 사용, 암호가 전송되지 않음
새 암호 저장됨	crypt 형식	Oracle Directory Server Enterprise Edition에서 암호 저장 체계가 정의됨	암호가 Kerberos에 의해 관리됨
암호 읽기 필요?	예	아니오	아니오
암호 변경 후의 sasl/digest-MD5 호환성	아니오. 암호가 clear로 저장되지 않습니다. 사용자가 인증할 수 없습니다.	예. 기본 저장 체계가 clear로 설정되어 있는 한 사용자가 인증할 수 있습니다.	아니오. sasl/GSSAPI가 사용됩니다. LDAP 디렉토리 서버에서 해당 암호 데이터베이스를 관리하는 Kerberos kdc를 사용하는 경우를 제외하고 디렉토리 서버에 암호가 저장되지 않으며 암호가 전송되지도 않습니다.
암호 정책 지원?	예. enableShadowUpdate를 true로 설정해야 합니다.	예(그렇게 구성된 경우).	pam_krb5(5), Kerberos V5 계정 관리 모듈을 참조하십시오.

PAM 및 암호 변경

passwd 명령을 사용하여 암호를 변경합니다. enableShadowUpdate 스위치가 true로 설정되지 않은 경우 사용자가 userPassword 속성을 쓸 수 있어야 합니다. enableShadowUpdate 스위치가 true로 설정된 경우 관리자 자격 증명이 userPassword 속성을 업데이트할 수 있어야 합니다. passwd-cmd에 대한 serviceAuthenticationMethod가 이 작업에 대한 authenticationMethod를 대체합니다. 사용되는 인증 방법에 따라 현재 암호가 전송 중에 암호화 해제될 수 있습니다.

UNIX 인증의 경우 새 userPassword 속성은 UNIX crypt 형식으로 암호화되며 LDAP에 기록되기 전에 태그가 지정됩니다. 따라서 서버에 바인딩되는 데 사용되는 인증 방법에 관계없이 새 암호가 전송 중에 암호화됩니다. 자세한 내용은 pam_authtok_store(5) 매뉴얼 페이지를 참조하십시오.

enableShadowUpdate 스위치가 true로 설정된 경우 사용자 암호가 변경되면 pam_unix_* 모듈이 관련 섀도우 정보도 업데이트합니다. pam_unix_* 모듈은 로컬 사용자 암호가 변경될 때 모듈이 업데이트하는 것과 동일한 shadow 필드를 로컬 shadow 파일에서 업데이트합니다.

pam_ldap은 암호 업데이트를 더 이상 지원하지 않습니다. 이제 server_policy 옵션을 사용하는 pam_authtok_store가 pam_ldap 암호 업데이트 기능을 대체합니다. pam_authtok_store를 사용하면 새 암호가 일반 텍스트로 LDAP 서버에 전송됩니다. 따라서 프라이버시를 유지하려면 TLS를 사용합니다. TLS를 사용하지 않으면 새 userPassword가 스누핑에 노출됩니다. Oracle Directory Server Enterprise Edition에 태그가 지정되지 않은 암호를 설정하면 소프트웨어가 passwordStorageScheme 속성을 사용하여 암호를 암호화합니다. passwordStorageScheme에 대한 자세한 내용은 사용 중인 Oracle Directory Server Enterprise Edition 버전에 대한 **관리 설명서**의 사용자 계정 관리 절을 참조하십시오.

주 – passwordStorageScheme 속성을 설정하는 경우 다음 구성 문제를 고려해야 합니다. NIS 또는 UNIX 인증을 사용하는 다른 클라이언트가 LDAP을 저장소로 사용하는 경우 passwordStorageScheme은 crypt여야 합니다. 또한 Oracle Directory Server Enterprise Edition에 sasl/digest-MD5와 함께 LDAP 인증을 사용하는 경우에는 passwordStorageScheme을 clear로 설정해야 합니다.

LDAP 계정 관리

계정 및 암호 관리 시스템으로 pam_krb5를 선택하면 Kerberos 환경에서 모든 계정, 암호, 계정 잠금 및 기타 계정 관리 세부 사항이 관리됩니다. pam_krb5(5) 및 **Oracle Solaris 11.1 관리: 보안 서비스**를 참조하십시오.

pam_krb5를 사용하지 않는 경우 Oracle Directory Server Enterprise Edition의 암호 및 계정 잠금 정책 지원을 활용하도록 LDAP 이름 지정 서비스를 구성할 수 있습니다. 사용자 계정 관리를 지원하도록 pam_ldap(5)를 구성할 수 있습니다. passwd(1)은 올바른 PAM 구성과 함께 사용할 경우 Oracle Directory Server Enterprise Edition 암호 정책에 의해 설정된 암호 구문 규칙 세트를 적용합니다.

다음 계정 관리 기능은 pam_ldap(5)를 통해 지원됩니다. 이러한 기능은 Oracle Directory Server Enterprise Edition의 암호 및 계정 잠금 정책 구성에 따라 달라집니다. 원하는 개수만큼 기능을 사용으로 설정할 수 있습니다.

- 암호 에이징 및 만료 알림

  사용자는 일정에 따라 암호를 변경해야 합니다. 구성된 시간 내에 암호를 변경하지 않으면 해당 암호가 만료됩니다. 암호가 만료되면 사용자 인증이 실패합니다.

  사용자가 만료 경고 기간 내에 로그인하면 항상 경고 메시지가 표시됩니다. 이 메시지는 암호가 만료되기 전까지 남은 시간 또는 일 수를 명시해 줍니다.

- 암호 구문 검사

새 암호는 최소 암호 길이 요구 사항을 충족해야 합니다. 또한 암호는 사용자 디렉토리 항목의 uid, cn, sn 또는 mail 속성 값과 일치할 수 없습니다.

- 암호 기록 검사

  사용자는 암호를 다시 사용할 수 없습니다. 사용자가 암호를 이전에 사용한 암호로 변경하려고 하면 passwd(1)가 실패합니다. LDAP 관리자는 서버의 기록 목록에 유지되는 암호 수를 구성할 수 있습니다.

- 사용자 계정 잠금

  지정된 횟수만큼 인증 시도가 반복해서 실패하면 사용자 계정이 잠길 수 있습니다. 관리자가 계정을 비활성화하는 경우에도 사용자가 잠길 수 있습니다. 계정 잠금 시간이 경과하거나 관리자가 계정을 다시 활성화할 때까지 인증이 계속해서 실패합니다.

주 – 앞의 계정 관리 기능은 Oracle Directory Server Enterprise Edition에서만 작동합니다. 서버에서 암호 및 계정 잠금 정책을 구성하는 방법에 대한 자세한 내용은 사용 중인 Oracle Directory Server Enterprise Edition 버전에 대한 관리 설명서의 "사용자 계정 관리" 장을 참조하십시오. 191 페이지 "계정 관리에 pam_ldap 모듈을 사용하는 pam_conf 파일 예"도 참조하십시오. proxy 계정에 대해 계정 관리를 사용으로 설정하지 마십시오.

Oracle Directory Server Enterprise Edition에서 암호 및 계정 잠금 정책을 구성하기 전에 모든 호스트가 pam_ldap 계정 관리에 "최신" LDAP 클라이언트를 사용하는지 확인합니다.

또한 클라이언트에 올바르게 구성된 pam.conf(4) 파일이 있는지 확인합니다. 그렇지 않으면 proxy 또는 사용자 암호가 만료될 경우 LDAP 이름 지정 서비스가 작동하지 않습니다.

주 – 이전에는 pam_ldap 계정 관리를 사용으로 설정한 경우 모든 사용자가 시스템에 로그인할 때마다 인증을 위해 로그인 암호를 제공해야 했습니다. 따라서 ssh 등의 도구를 사용하여 암호 기반이 아닌 로그인을 시도하면 실패했습니다.

사용자가 로그인할 때 디렉토리 서버에 인증하지 않고 계정 관리를 수행하고 사용자의 계정 상태를 검색합니다. 디렉토리 서버의 새 컨트롤은 기본적으로 사용으로 설정되는 1.3.6.1.4.1.42.2.27.9.5.8입니다.

기본값이 아닌 다른 값에 대해 이 컨트롤을 수정하려면 디렉토리 서버에 ACI(액세스 제어 명령)를 추가합니다.

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

pam_unix_* 모듈을 사용한 LDAP 계정 관리

클라이언트에서 enableShadowUpdate 스위치가 true로 설정된 경우 로컬 계정이 사용할 수 있는 계정 관리 기능을 LDAP 계정도 사용할 수 있습니다. 기능에는 암호 에이징, 계정 만료 및 알림, 실패한 로그인 계정 잠금 등이 포함됩니다. 또한 이제 LDAP에서 passwd 명령에 대한 -dluNfnwx 옵션이 지원됩니다. 따라서 파일 이름 지정 서비스에 있는 pam_unix_* 모듈과 passwd 명령의 전체 기능이 LDAP 이름 지정 서비스에서 지원됩니다. enableShadowUpdate 스위치는 파일과 LDAP 범위 둘 다에 정의된 사용자에게 일관된 계정 관리를 구현하는 방법을 제공합니다.

사용자가 자신의 계정 관리 데이터를 수정하여 암호 정책을 우회하는 것을 방지하기 위해 LDAP 서버는 사용자가 서버에 있는 자신의 섀도우 데이터에 대해 쓰기 작업을 수행하지 못하도록 구성됩니다. 관리자 자격 증명이 있는 관리자가 클라이언트 시스템에 대해 섀도우 데이터 업데이트를 수행합니다. 그러나 이러한 구성은 사용자가 암호를 수정할 수 있어야 하는 pam_ldap 모듈과 충돌합니다. 따라서 pam_ldap 및 pam_unix_* 모듈에 의한 계정 관리는 호환되지 않습니다.

주의 – 동일한 LDAP 이름 지정 도메인에서 pam_ldap 모듈과 pam_unix_* 모듈을 함께 사용하지 마십시오. 모든 클라이언트가 pam_ldap 모듈을 사용하거나 모든 클라이언트가 pam_unix_* 모듈을 사용해야 합니다. 이 제한은 전용 LDAP 서버가 필요함을 나타낼 수 있습니다. 예를 들어, 웹 또는 전자 메일 응용 프로그램에서 사용자가 LDAP 서버의 해당 암호를 변경할 수 있어야 할 수 있습니다.

또한 enableShadowUpdate를 구현하려면 관리자 자격 증명(adminDN 및 adminPassword)을 모든 클라이언트에 로컬로 저장해야 합니다. 이 정보는 svc:/network/ldap/client 서비스에 저장됩니다.

계정 관리에 pam_ldap을 사용하는 경우와 달리 계정 관리에 pam_unix_* 모듈을 사용할 때는 /etc/pam.conf 파일을 변경할 필요가 없습니다. 기본 /etc/pam.conf 파일을 사용해도 됩니다.

◆ ◆ ◆ 10장

10 LDAP 이름 지정 서비스에 대한 계획 요구 사항(작업)

이 장에서는 서버와 클라이언트 설정 및 설치 프로세스를 시작하기 전에 수립해야 하는 고급 계획에 대해 설명합니다.

이 장에서는 다음 내용을 다룹니다.

LDAP 계획 개요

LDAP 클라이언트 프로파일은 LDAP 클라이언트가 지원 LDAP 서버에 대한 LDAP 이름 지정 서비스 정보에 액세스할 때 사용하는 구성 정보 모음입니다. 이 장에서는 LDAP 이름 지정 서비스의 다양한 측면에 대한 계획 수립에 대해 설명합니다. 여기에는 네트워크 모델, 디렉토리 정보 트리, 보안 모델, 다양한 프로파일 속성의 기본값, 데이터 채우기 준비 등이 포함됩니다.

LDAP 네트워크 모델 계획

가용성 및 성능을 위해 회사 전체 네트워크의 각 서브넷에는 서브넷의 모든 LDAP 클라이언트에 서비스를 제공할 고유한 LDAP 서버가 있어야 합니다. 이러한 서버 중 하나만 마스터 LDAP 서버로 만들면 됩니다. 나머지는 모두 마스터 서버의 복제본일 수 있습니다.

네트워크 구성을 계획하려면 가용 서버 개수, 클라이언트가 서버에 연결할 수 있는 방법 및 서버 액세스 순서를 고려하십시오. 서브넷당 서버가 1개 있는 경우 `defaultServerList`

속성을 사용하여 모든 서버를 나열하고 LDAP 클라이언트가 액세스 순서를 정렬 및 조작하도록 할 수 있습니다. 속도 또는 데이터 관리 때문에 특정 순서대로 서버에 액세스해야 하는 경우 preferredServerList 속성을 사용하여 고정된 서버 액세스 순서를 정의해야 합니다. defaultServerList는 목록의 모든 서버를 동일하게 처리하는 반면, preferredServerList의 서버는 우선 순위대로 나열되며 목록의 첫번째 서버가 사용하기에 가장 적합한 서버입니다. 주요 차이점은 preferredServerList를 사용할 경우 사용 가능한 서버 중 우선 순위가 가장 높은 서버가 우선 순위가 낮은 다른 가용 서버보다 먼저 사용된다는 점입니다. 우선 순위가 높은 서버를 사용할 수 있게 되면 클라이언트 시스템이 우선 순위가 낮은 서버에서 연결을 끊습니다. defaultServerList를 사용하면 모든 서버의 우선 순위가 같으며 온라인으로 전환되는 서버가 기존 서버를 대체하지 않습니다. 두 목록을 구성에 함께 사용할 수 있습니다. 마스터 서버의 로드를 줄이기 위해 이러한 목록에 마스터 서버를 포함해서는 안됩니다.

서버 및 네트워크 구성을 계획할 때는 다음과 같은 세 가지 추가 속성도 고려하면 좋습니다. bindTimeLimit 속성은 TCP 연결 요청의 시간 초과 값을 설정하는 데 사용할 수 있습니다. searchTimeLimit 속성은 LDAP 검색 작업의 시간 초과 값을 설정하는 데 사용할 수 있습니다. profileTTL 속성은 LDAP 클라이언트가 서버에서 프로파일을 다운로드해야 하는 빈도를 제어하는 데 사용할 수 있습니다. 느리거나 불안정한 네트워크의 경우 bindTimeLimit 및 searchTimeLimit 속성에 기본값보다 더 큰 값이 필요할 수 있습니다. 배포의 조기 단계 테스트를 위해 profileTTL 속성 값을 줄여 클라이언트가 LDAP 서버에 저장된 프로파일의 잦은 변경 사항을 인식하게 만들 수 있습니다.

디렉토리 정보 트리 계획

LDAP 이름 지정 서비스에는 기본 DIT(디렉토리 정보 트리) 및 연관된 기본 스키마가 있습니다. 예를 들어, ou=people 컨테이너에는 사용자 계정, 암호 및 섀도우 정보가 들어 있습니다. ou=hosts 컨테이너에는 네트워크 시스템에 대한 정보가 들어 있습니다. ou=people 컨테이너의 각 항목은 objectclass posixAccount 및 shadowAccount입니다.

기본 DIT는 잘 구성된 디렉토리 구조이며 개방형 표준을 기반으로 합니다. 자세한 내용은 RFC 2307bis 및 RFC 4876을 참조하십시오. 기본 DIT는 대부분의 이름 지정 서비스 요구를 만족시키기에 충분하며 변경하지 않고 사용하는 것이 좋습니다. 기본 DIT를 사용하는 경우 특정 도메인에 대해 이름 지정 서비스 정보를 검색할 디렉토리 트리 노드(기본 DN)만 결정하면 됩니다. 이 노드는 defaultSearchBase 속성으로 지정합니다. defaultSearchScope 속성을 설정하여 이름 지정 서비스 조회에서 수행해야 하는 검색 범위를 클라이언트에 알릴 수도 있습니다. DN 아래의 한 레벨만 검색합니까(one), 아니면 DN 아래의 전체 하위 트리를 검색합니까(sub)?

그러나 LDAP 이름 지정 서비스가 기존 DIT로 작업하거나 이름 지정 서비스 데이터가 디렉토리 트리에 분산된 더 복잡한 DIT를 처리하기 위해 유연성이 더 필요한 경우도 있습니다. 예를 들어, 사용자 계정 항목이 트리의 여러 부분에 있을 수 있습니다. 클라이언트 프로파일의 serviceSearchDescriptor, attributeMap 및 objectclassMap 속성은 이러한 경우를 처리하도록 설계되었습니다.

서비스 검색 설명자를 사용하여 특정 서비스에 대한 기본 검색 기준, 검색 범위 및 검색 필터를 대체할 수 있습니다. 122 페이지 “서비스 검색 설명자 및 스키마 매핑”을 참조하십시오.

`attributeMap` 및 `objectclassMap` 속성은 스키마 매핑 방법을 제공합니다. 두 속성을 사용하면 LDAP 이름 지정 서비스가 기존 DIT에서 작동할 수 있습니다. 예를 들어, `posixAccount` 객체 클래스를 기존 객체 클래스 `myAccount`에 매핑할 수 있습니다. `posixAccount` 객체 클래스의 속성을 `myAccount` 객체 클래스의 속성에 매핑할 수 있습니다.

다중 디렉토리 서버

다중 LDAP 서버가 DIT 1개에 서비스를 제공할 수 있습니다. 예를 들어, DIT의 일부 하위 트리가 다른 LDAP 서버에 상주할 경우 LDAP 서버는 알고는 있지만 자체 데이터베이스에 없는 이름 지정 데이터를 위해 LDAP 클라이언트를 다른 서버로 안내할 수 있습니다. 이러한 DIT 구성을 계획하는 경우 클라이언트의 프로파일 속성 `followReferrals`를 설정하여 이름 지정 서비스 조회를 계속하려면 서버 참조를 따르도록 LDAP 이름 지정 서비스에 지시할 수 있습니다. 그러나 가능한 경우 특정 도메인의 모든 이름 지정 데이터가 단일 디렉토리 서버에 상주하는 것이 가장 좋습니다.

클라이언트가 대부분 읽기 전용 복제본에 액세스하고 필요한 경우에만 참조를 따라 읽기/쓰기 마스터 서버에 액세스하게 하려는 경우 참조가 유용할 수 있습니다. 이렇게 하면 복제본에서 처리될 수 있는 요청으로 인해 마스터 서버에 과부하가 발생하지 않습니다.

다른 응용 프로그램과 데이터 공유

LDAP을 최대한 활용하려면 각 논리 항목에 대해 단일 LDAP 항목이 있어야 합니다. 예를 들어, 사용자의 경우 회사 화이트 페이지 정보뿐 아니라 계정 정보와 응용 프로그램별 데이터도 사용할 수 있습니다. `posixAccount` 및 `shadowAccount`는 보조 객체 클래스이므로 디렉토리의 모든 항목에 추가할 수 있습니다. 이 경우 신중한 계획, 설정 및 관리가 필요합니다.

디렉토리 접미어 선택

적절한 디렉토리 접미어를 선택하는 방법에 대한 자세한 내용은 Oracle Directory Server Enterprise Edition 설명서를 참조하십시오.

LDAP 및 복제 서버

복제 서버를 설정할 때는 다음과 같은 3가지 전략을 활용할 수 있습니다.

- 단일 마스터 복제
- 부동 마스터 복제
- 다중 마스터 복제

단일 마스터

단일 마스터 복제를 사용할 경우 특정 분할 영역 또는 분할되지 않은 네트워크에 대한 마스터 서버 1개에만 디렉토리 항목의 쓰기 가능 복사본이 보관됩니다. 모든 복제 서버에 디렉토리 항목의 읽기 전용 복사본이 있습니다. 복제본과 마스터 둘 다 검색, 비교 및 바인딩 작업을 수행할 수 있지만 마스터 서버만 쓰기 작업을 수행할 수 있습니다.

단일 마스터 복제 전략에는 마스터 서버가 단일 오류 지점이 될 수 있다는 단점이 있습니다. 마스터 서버의 작동이 중지되면 모든 복제본이 쓰기 작업을 처리할 수 없게 됩니다.

부동 마스터

부동 마스터 전략은 특정 분할 영역 또는 분할되지 않은 네트워크에 대해 항상 하나의 마스터 서버만 쓰기 권한을 가진다는 점에서 단일 마스터 전략과 유사합니다. 그러나 부동 마스터 전략을 구현할 경우 마스터 서버의 작동이 중지되면 복제본이 알고리즘을 통해 마스터 서버로 자동 변환됩니다.

부동 마스터 복제 전략에는 네트워크가 분할되고 분할 영역 한쪽의 복제본이 마스터가 될 경우 네트워크를 다시 결합할 때 새 마스터를 조정하는 프로세스가 매우 복잡해질 수 있다는 단점이 하나 있습니다.

다중 마스터

다중 마스터 복제에서는 디렉토리 항목 데이터에 대한 자체 읽기-쓰기 복사본이 있는 마스터 서버가 여러 개 있습니다. 다중 마스터 전략을 사용하면 단일 오류 지점이 생기는 문제가 없지만 서버 간에 업데이트 충돌이 발생할 수 있습니다. 즉, 항목의 속성이 두 마스터에서 거의 동시에 수정될 경우 "최종 작성자 인정"과 같은 업데이트 충돌 해결 정책을 구현해야 합니다.

복제 서버를 설정하는 방법에 대한 자세한 내용은 사용 중인 Oracle Directory Server Enterprise Edition 버전에 대한 **관리 설명서**를 참조하십시오. 일반적으로 대규모 엔터프라이즈 배포의 경우 다중 마스터 복제가 권장 옵션입니다.

LDAP 보안 모델 계획

보안 모델을 계획하려면 LDAP 클라이언트가 LDAP 서버와 통신할 때 사용해야 하는 ID를 먼저 고려해야 합니다. 예를 들어, 암호가 전송되지 않는 엔터프라이즈 수준의 Single Sign-On 솔루션을 원하는지, 아니면 데이터 전송 암호화 및 사용자 단위로 디렉토리 서버의 제어 데이터 결과에 액세스하는 기능을 원하는지 결정해야 합니다. 또한 전송 시 사용자 암호 플로우를 보호할 강력한 인증을 구현할지 여부 및/또는 LDAP 클라이언트와 LDAP 서버 간의 세션을 암호화하여 전송되는 LDAP 데이터를 보호해야 하는지 결정해야 합니다.

이 작업을 위해 프로파일의 `credentialLevel` 및 `authenticationMethod` 속성이 사용됩니다. `credentialLevel`에는 `anonymous`, `proxy`, `proxy anonymous` 및 `self`라는 4가지 자격 증명 레벨이 있습니다. LDAP 이름 지정 서비스 보안 개념에 대한 자세한 내용은 128 페이지 “LDAP 이름 지정 서비스 보안 모델”을 참조하십시오.

주 – 이전에는 `pam_ldap` 계정 관리를 사용으로 설정한 경우 모든 사용자가 시스템에 로그인할 때마다 인증을 위해 로그인 암호를 제공해야 했습니다. 따라서 `ssh` 등의 도구를 사용하여 암호 기반이 아닌 로그인을 시도하면 실패했습니다.

사용자가 로그인할 때 디렉토리 서버에 인증하지 않고 계정 관리를 수행하고 사용자의 계정 상태를 검색합니다. 디렉토리 서버의 새 컨트롤은 기본적으로 사용으로 설정되는 `1.3.6.1.4.1.42.2.27.9.5.8`입니다.

기본값이 아닌 다른 값에 대해 이 컨트롤을 수정하려면 디렉토리 서버에 ACI(액세스 제어 명령)를 추가합니다.

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

주 – 엔터프라이즈 수준의 Single Sign-On 솔루션으로 `pam_krb5` 및 Kerberos를 사용으로 설정하면 세션을 시작할 때 로그인 암호가 한 번만 필요한 시스템을 설계할 수 있습니다. 자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**를 참조하십시오. Kerberos를 사용으로 설정하는 경우 일반적으로 DNS도 사용으로 설정해야 합니다. 자세한 내용은 이 매뉴얼의 DNS 관련 장을 참조하십시오.

보안 모델을 계획할 때 필요한 주요 결정 사항은 다음과 같습니다.

- Kerberos 및 per-user 인증을 사용하겠습니까?
- LDAP 클라이언트에서 어떤 자격 증명 레벨과 인증 방법을 사용하겠습니까?
- TLS를 사용하겠습니까?
- NIS와 역방향 호환이 가능해야 합니까? 즉, 클라이언트에서 `pam_unix_*` 또는 `pam_ldap` 모듈을 사용하겠습니까?
- 서버의 `passwordStorageScheme` 속성 설정은 어떻게 지정하겠습니까?
- 액세스 제어 정보는 어떻게 설정하겠습니까?

  ACI에 대한 자세한 내용은 사용 중인 Oracle Directory Server Enterprise Edition 버전에 대한 **관리 설명서**를 참조하십시오.
- 클라이언트에서 `pam_unix_*` 또는 `pam_ldap` 모듈을 사용하여 LDAP 계정 관리를 수행하겠습니까?

LDAP에 대한 클라이언트 프로파일 및 기본 속성 값 계획

이전 계획 단계(네트워크 모델, DIT 및 보안 모델)를 수행했다면 다음 프로파일 속성의 값을 이해할 수 있을 것입니다.

- `cn`
- `defaultServerList`
- `preferredServerList`
- `bindTimeLimit`
- `searchTimeLimit`
- `profileTTL`
- `defaultSearchBase`
- `defaultSearchScope`
- `serviceSearchDescriptor`
- `attributeMap`
- `objectclassMap`
- `followReferrals`
- `credentialLevel`
- `authenticationMethod`
- `serviceCredentialLevel`
- `serviceAuthenticationMethod`

앞의 속성 중에서 `cn`, `defaultServerList` 및 `defaultSearchBase`만 필수입니다. 이러한 속성에는 기본값이 없습니다. 나머지 속성은 선택 사항이며 일부 속성에 기본값이 있습니다.

LDAP 클라이언트 설정에 대한 자세한 내용은 12 장, “LDAP 클라이언트 설정(작업)”을 참조하십시오.

LDAP 데이터 채우기 계획

LDAP 서버에 데이터를 채우려면 LDAP 서버가 적절한 DIT 및 스키마로 구성된 후에 새 `ldapaddent` 도구를 사용합니다. 이 도구는 해당 `/etc` 파일에서 LDAP 컨테이너의 항목을 만듭니다. 이 도구를 사용하면 다음 데이터 유형에 대해 컨테이너에 데이터를 채울 수 있습니다. `aliases`, `auto_*`, `bootparams`, `ethers`, `group`, `hosts`(IPv6 주소 포함), `netgroup`, `netmasks`, `networks`, `passwd`, `shadow`, `protocols`, `publickey`, `rpc` 및 `services`. 또한 `/etc/user_attr`, `/etc/security/auth_attr`, `/etc/security/prof_attr`, `/etc/security/exec_attr` 등의 RBAC 관련 파일을 추가할 수 있습니다.

기본적으로 `ldapaddent`는 표준 입력을 읽고 이 데이터를 명령줄에 지정된 데이터베이스와 연관된 LDAP 컨테이너에 추가합니다. 그러나 `-f` 옵션을 사용하여 데이터를 읽을 입력 파일을 지정할 수 있습니다.

클라이언트 구성에 따라 항목이 디렉토리에 저장되기 때문에 LDAP 이름 지정 서비스를 사용하도록 클라이언트를 구성해야 합니다.

성능을 향상시키려면 다음 순서대로 데이터베이스를 로드합니다.

1. `passwd` 데이터베이스, `shadow` 데이터베이스 순
2. `networks` 데이터베이스, `netmasks` 데이터베이스 순
3. `bootparams` 데이터베이스, `ethers` 데이터베이스 순

자동 마운트 항목을 추가하는 경우 데이터베이스 이름은 `auto_*` 형식입니다(예: `auto_home`).

LDAP 서버에 추가할 여러 호스트의 `/etc` 파일이 있는 경우 모든 파일을 동일한 `/etc` 파일에 병합한 다음 한 호스트에서 `ldapaddent` 명령을 사용하여 파일을 추가하거나, 각 호스트가 이미 LDAP 클라이언트로 구성되었다는 가정하에 각 호스트에서 `ldapaddent` 명령을 실행할 수 있습니다.

이름 지정 서비스 데이터가 이미 NIS 서버에 있고 LDAP 이름 지정 서비스에 대한 LDAP 서버로 데이터를 이동하려는 경우 `ypcat` 명령을 사용하여 NIS 맵을 파일로 덤프합니다. 그런 다음 이러한 파일에 대해 `ldapaddent` 명령을 실행하여 LDAP 서버에 데이터를 추가합니다.

다음 절차에서는 `yp` 클라이언트에서 테이블을 추출해야 한다고 가정합니다.

▼ `ldapaddent` 명령을 사용하여 서버에 host 항목을 채우는 방법

1 Oracle Directory Server Enterprise Edition이 `idsconfig` 명령을 사용하여 설정되었는지 확인합니다.

2 **클라이언트 시스템에서 수퍼유저가 되거나 이에 상응하는 역할을 맡습니다.**

역할에는 권한 부여 및 권한이 있는 명령이 포함됩니다. 역할에 대한 자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 9 장, “역할 기반 액세스 제어 사용(작업)”을 참조하십시오.

3 **시스템을 LDAP 클라이언트로 설정합니다.**

```
# ldapclient init -a profileName=new -a domainName=west.example.com 192.168.0.1
```

4 **서버에 데이터를 채웁니다.**

```
# ldapaddent -D “cn=directory manager” -f /etc/hosts hosts
```

암호를 묻는 메시지가 표시됩니다.

이 예에서 `ldapaddent` 명령은 new 프로파일에 구성된 인증 방법을 사용합니다. simple을 선택하면 암호가 일반 텍스트로 전송됩니다. 자세한 내용은 `ldapaddent(1M)` 매뉴얼 페이지를 참조하십시오.

독립형 모드에서 이 명령은 다음과 유사합니다.

```
# ldapaddent -h 192.168.0.1 -N new -M west.example.com -a simple-D “cn=directory manager” -f /etc/hosts hosts
```

◆ ◆ ◆ 11장

11 LDAP 클라이언트를 사용하여 Oracle Directory Server Enterprise Edition 설정(작업)

이 장에서는 LDAP 이름 지정 서비스 클라이언트 네트워크를 지원하도록 Oracle Directory Server Enterprise Edition을 구성하는 방법에 대해 설명합니다. 이 정보는 Oracle Directory Server Enterprise Edition과 관련이 있습니다. 디렉토리 서버 설치 및 구성에 대한 자세한 내용은 Oracle Directory Server Enterprise Edition 설명서를 참조하십시오.

주 – Oracle Directory Server Enterprise Edition과 함께 제공된 설치 및 구성 설명서에 있는 절차를 모두 수행한 후에만 LDAP 클라이언트에서 작동하도록 Oracle Directory Server Enterprise Edition을 구성할 수 있습니다.

주 – 디렉토리 서버(LDAP 서버)는 자신의 클라이언트가 될 수 **없습니다**.

이 장에서는 다음 내용을 다룹니다.

idsconfig 명령을 사용하여 Oracle Directory Server Enterprise Edition 구성

서버 설치를 기준으로 점검 목록 만들기

서버 설치 프로세스 중에 중요한 변수를 정의해야 하므로 idsconfig를 시작하기 전에 이러한 변수를 사용하여 아래와 유사한 점검 목록을 만들어야 합니다. 189 페이지 "LDAP 구성을 위한 빈 점검 목록"에 제공된 빈 점검 목록을 사용할 수 있습니다.

주 – 아래에 포함된 정보는 LDAP 관련 장에 있는 모든 예의 기본 사항입니다. 예제 도메인은 전국에 매장이 있는 위젯 회사인 Example, Inc.입니다. 예에서는 도메인 이름이 west.example.com인 West Coast Division을 처리합니다.

표 11–1 example.com 네트워크에 대해 정의된 서버 변수

변수	예제 네트워크에 대한 정의
디렉토리 서버 인스턴스가 설치된 포트 번호	389(기본값)
서버 이름	myserver(FQDN myserver.west.example.com 또는 192.168.0.1의 호스트 이름)
복제 서버(IP 번호:포트 번호)	192.168.0.2[myreplica.west.example.com]
디렉토리 관리자	cn=directory manager(기본값)
제공할 도메인 이름	west.example.com
시간 초과 전까지 클라이언트 요청을 처리할 최대 시간(초)	1
각 검색 요청에 대해 반환되는 최대 항목 수	1

주 – defaultServerList 또는 preferredServerList 정의에 호스트 이름을 사용 중인 경우 **반드시** 호스트 조회에 LDAP이 사용되지 않도록 해야 합니다. 즉, svc:/network/name-service/switch 서비스의 config/host 등록 정보에서 ldap을 구성하지 않아야 합니다.

표 11–2 example.com 네트워크에 대해 정의된 클라이언트 프로파일 변수

변수	예제 네트워크에 대한 정의
프로파일 이름(기본 이름은 default임)	WestUserProfile

표 11–2 example.com 네트워크에 대해 정의된 클라이언트 프로파일 변수 *(계속)*

변수	예제 네트워크에 대한 정의
서버 목록(기본적으로 로컬 서브넷으로 지정됨)	192.168.0.1
기본 서버 목록(첫번째, 두번째 등으로 시도할 서버 순서대로 나열됨)	none
검색 범위(디렉토리 트리 아래의 레벨 수. 'One'(기본값) 또는 'Sub')	one(기본값)
서버에 액세스하는 데 사용되는 자격 증명. 기본값은 anonymous입니다.	proxy
참조 따름?(주 서버를 사용할 수 없는 경우 다른 서버에 대한 포인터) 기본값은 no입니다.	Y
서버가 정보를 반환하도록 기다리는 검색 시간 제한(기본값은 30초임)	default
서버에 연결하기 위한 바인드 시간 제한(기본값은 10초임)	default
인증 방법. 기본값은 none입니다.	simple

주 – 클라이언트 프로파일은 도메인별로 정의됩니다. 특정 도메인에 대해 프로파일을 하나 이상 정의해야 합니다.

속성 색인

idsconfig 명령은 성능 향상을 위해 다음 속성 목록을 색인화합니다.

```
membernisnetgroup    pres,eq,sub
nisnetgrouptriple    pres,eq,sub
ipHostNumber         pres,eq,sub
uidNumber            pres,eq
gidNumber            pres,eq
ipNetworkNumber      pres,eq
automountkey         pres,eq
oncRpcNumber         pres,eq
```

스키마 정의

idsconfig(1M)는 필요한 스키마 정의를 자동으로 추가합니다. LDAP 관리에 익숙하지 않은 경우 서버 스키마를 수동으로 수정하지 마십시오. LDAP 이름 지정 서비스에서 사용하는 스키마의 확장 목록은 14 장, “LDAP 이름 지정 서비스(참조)”를 참조하십시오.

검색 색인 사용

VLV(가상 목록 보기)라고도 하는 Oracle Directory Server Enterprise Edition의 검색 색인 기능을 사용하면 클라이언트가 선택한 그룹이나 매우 긴 목록의 항목 수를 볼 수 있으므로 각 클라이언트에 대한 검색 프로세스 시간을 줄일 수 있습니다. 검색 색인은 최적화되고 사전 정의된 검색 매개변수를 제공하며, LDAP 이름 지정 클라이언트는 이러한 매개변수를 사용하여 다양한 서비스의 특정 정보에 보다 신속하게 액세스할 수 있습니다. 검색 색인을 만들지 않을 경우 서버 제한을 초과하면 클라이언트가 특정 유형의 모든 항목에 액세스하지 못합니다. 예를 들어, 암호 항목이 5000개 있지만 1000개 항목으로 크기 제한이 설정된 경우 일부 조회 작업 중에 4000개 항목은 반환되지 않습니다. 이 경우 클라이언트 시스템에서 로그인 및 기타 심각한 오류가 자주 발생할 수 있습니다.

VLV 색인은 디렉토리 서버에 구성되며 프록시 사용자는 이러한 색인에 대해 읽기 권한을 갖습니다.

Oracle Directory Server Enterprise Edition에서 검색 색인을 구성하기 전에 이러한 색인 사용 시 발생하는 성능 저하를 고려합니다. 자세한 내용은 사용 중인 Oracle Directory Server Enterprise Edition 버전에 대한 **관리 설명서**를 참조하십시오.

`idsconfig`는 여러 VLV 색인에 대한 항목을 만듭니다. 자세한 내용은 `idsconfig(1M)` 매뉴얼 페이지를 참조하십시오. `idsconfig`에서 생성된 VLV 항목을 확인하려면 `idsconfig` 명령의 출력을 참조하십시오. 샘플 `idsconfig` 출력은 159 페이지 “idsconfig 설정 예”을 참조하십시오.

서비스 검색 설명자를 사용하여 다양한 서비스에 대한 클라이언트 액세스 수정

SSD(서비스 검색 설명자)는 LDAP의 특정 작업에 대한 기본 검색 요청을 정의한 검색으로 변경합니다. SSD는 사용자 정의 컨테이너 정의나 다른 운영 체제와 함께 LDAP을 사용했으며 이제 최신 Oracle Solaris 릴리스로 전환 중인 경우에 특히 유용합니다. SSD를 사용하면 기존 LDAP 데이터베이스와 데이터를 변경하지 않고도 LDAP 이름 지정 서비스를 구성할 수 있습니다.

idsconfig 명령을 사용하여 SSD 설정

Example, Inc.의 선임자가 LDAP을 구성하고 사용자를 `ou=Users` 컨테이너에 저장했다고 가정합니다. 이제 최신 Oracle Solaris 릴리스로 업그레이드 중입니다. 정의에 따라 LDAP 클라이언트는 사용자 항목이 `ou=People` 컨테이너에 저장되어 있다고 가정합니다. 따라서 `passwd` 서비스 검색 시 LDAP 클라이언트는 DIT의 `ou=people` 레벨을 검색하지만 올바른 값을 찾지 못합니다.

Example, Inc.의 기존 DIT를 완전히 덮어쓰고 새 LDAP 이름 지정 서비스와 호환되도록 Example, Inc. 네트워크의 기존 응용 프로그램을 모두 재작성하면 이 문제를 해결할 수 있지만 이것은 너무 힘든 방법입니다. 이보다 훨씬 효율적인 두번째 방법은 SSD를 사용하여 LDAP 클라이언트에 기본 `ou=people` 컨테이너 대신 `ou=Users` 컨테이너에서 사용자 정보를 찾도록 지정하는 것입니다.

`idsconfig`를 사용하여 Oracle Directory Server Enterprise Edition을 구성하는 동안 필요한 SSD를 정의합니다. 프롬프트 라인은 다음과 같이 표시됩니다.

```
Do you wish to setup Service Search Descriptors (y/n/h? y
  A  Add a Service Search Descriptor
  D  Delete a SSD
  M  Modify a SSD
  P  Display all SSD's
  H  Help
  X  Clear all SSD's

  Q  Exit menu
Enter menu choice: [Quit] a
Enter the service id: passwd
Enter the base: service ou=user,dc=west,dc=example,dc=com
Enter the scope: one[default]
  A  Add a Service Search Descriptor
  D  Delete a SSD
  M  Modify a SSD
  P  Display all SSD's
  H  Help
  X  Clear all SSD's

  Q  Exit menu
Enter menu choice: [Quit] p

Current Service Search Descriptors:
==================================
Passwd:ou=Users,ou=west,ou=example,ou=com?

Hit return to continue.

  A  Add a Service Search Descriptor
  D  Delete a SSD
  M  Modify a SSD
  P  Display all SSD's
  H  Help
  X  Clear all SSD's

  Q  Exit menu
Enter menu choice: [Quit] q
```

idsconfig 명령 실행

주 – idsconfig를 실행하기 위해 특별한 권한이 필요하지는 않으며 LDAP 이름 지정 클라이언트가 아니어도 됩니다. idsconfig 실행 준비를 위해 154 페이지 "서버 설치를 기준으로 점검 목록 만들기"에 설명된 대로 점검 목록을 만들어야 합니다. 서버나 LDAP 이름 지정 서비스 클라이언트 시스템에서 idsconfig를 실행할 필요가 없습니다. 네트워크상의 모든 Oracle Solaris 시스템에서 idsconfig를 실행할 수 있습니다.

주의 – idsconfig는 디렉토리 관리자의 암호를 일반 텍스트로 보냅니다. 일반 텍스트로 보내지 않으려면 클라이언트가 아니라 디렉토리 서버 자체에서 idsconfig를 실행해야 합니다.

▼ idsconfig 명령을 사용하여 Oracle Directory Server Enterprise Edition을 구성하는 방법

1. **대상 Oracle Directory Server Enterprise Edition이 작동하고 실행 중인지 확인합니다.**

2. **idsconfig 명령을 실행합니다.**

   ```
   # /usr/lib/ldap/idsconfig
   ```

   이 장의 시작 부분(154 페이지 "서버 설치를 기준으로 점검 목록 만들기")에 있는 서버 및 클라이언트 점검 목록에 나열된 정의를 사용한 idsconfig의 예제 실행은 예 11–1을 참조하십시오.

3. **메시지가 표시되면 질문에 대답합니다.**

   기본 사용자 입력은 'no'[n]입니다. 특정 질문에 대한 설명이 필요한 경우 다음을 입력합니다.

   ```
   h
   ```

   그러면 간단한 도움말 단락이 나타납니다.

   idsconfig가 디렉토리 설정을 완료한 후 서버에서 지정된 명령을 실행해야 서버 설정이 완료되고 서버에서 클라이언트에 서비스를 제공할 수 있습니다.

idsconfig 설정 예

이 절에서는 대체로 기본값을 사용하는 기본 idsconfig 설정의 예를 제공합니다. 클라이언트 프로파일을 수정하는 가장 복잡한 방법은 SSD를 만드는 것입니다. 자세한 내용은 156 페이지 "서비스 검색 설명자를 사용하여 다양한 서비스에 대한 클라이언트 액세스 수정"을 참조하십시오.

프롬프트 뒤의 대괄호 안에 포함된 데이터는 해당 프롬프트의 기본값을 나타냅니다. 기본값을 적용하려면 Return을 누릅니다.

주 – 요약 화면에서 비어 있는 매개변수는 설정되지 않았습니다.

---

idsconfig가 디렉토리 설정을 완료한 후 서버에서 지정된 명령을 실행해야 서버 설정이 완료되고 서버에서 클라이언트에 서비스를 제공할 수 있습니다.

예 11–1 Example, Inc. 네트워크에 대해 idsconfig 명령 실행

다음 예에서 idsconfig 유틸리티는 LDAP 서버에 서버 인스턴스가 생성된 후 즉시 실행됩니다.

```
# usr/lib/ldap/idsconfig
It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.

Do you wish to continue with server setup (y/n/h)? [n] y
Enter the JES Directory Server's  hostname to setup: myserver
Enter the port number for DSEE (h=help): [389]
Enter the directory manager DN: [cn=Directory Manager]
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [west.example.com]
Enter LDAP Base DN (h=help): [dc=west,dc=example,dc=com]
  Checking LDAP Base DN ...
  Validating LDAP Base DN and Suffix ...
  No valid suffixes were found for Base DN dc=west,dc=example,dc=com
Enter suffix to be created (b=back/h=help): [dc=west,dc=example,dc=com]
Enter ldbm database name (b=back/h=help): [west]
  sasl/GSSAPI is not supported by this LDAP server
Enter the profile name (h=help): [default] WestUserProfile
Default server list (h=help): [192.168.0.1]
Preferred server list (h=help):
Choose desired search scope (one, sub, h=help):  [one]
The following are the supported credential levels:
  1  anonymous
  2  proxy
  3  proxy anonymous
  4  self
Choose Credential level [h=help]: [1] 2
The following are the supported Authentication Methods:
  1  none
```

예 11–1 Example, Inc. 네트워크에 대해 idsconfig 명령 실행 (계속)

```
  2  simple
  3  sasl/DIGEST-MD5
  4  tls:simple
  5  tls:sasl/DIGEST-MD5
  6  sasl/GSSAPI
Choose Authentication Method (h=help): [1] 2


Current authenticationMethod: simple
Do you want to add another Authentication Method? n
Do you want the clients to follow referrals (y/n/h)? [n]
Do you want to modify the server timelimit value (y/n/h)? [n] y
Enter the time limit for DSEE (current=3600): [-1]
Do you want to modify the server sizelimit value (y/n/h)? [n] y
Enter the size limit for DSEE (current=2000): [-1]
Do you want to store passwords in "crypt" format (y/n/h)? [n] y
Do you want to setup a Service Authentication Methods (y/n/h)? [n]
Client search time limit in seconds (h=help): [30]
Profile Time To Live in seconds (h=help): [43200]
Bind time limit in seconds (h=help): [10]
Do you want to enable shadow update (y/n/h)? [n]
Do you wish to setup Service Search Descriptors (y/n/h)? [n]

             Summary of Configuration

  1  Domain to serve               : west.example.com
  2  Base DN to setup              : dc=west,dc=example,dc=com
        Suffix to create           : dc=west,dc=example,dc=com
        Database to create         : west
  3  Profile name to create        : WestUserProfile
  4  Default Server List           : 192.168.0.1
  5  Preferred Server List         :
  6  Default Search Scope          : one
  7  Credential Level              : proxy
  8  Authentication Method         : simple
  9  Enable Follow Referrals       : FALSE
 10  DSEE Time Limit                : -1
 11  DSEE Size Limit                : -1
 12  Enable crypt password storage : TRUE
 13  Service Auth Method pam_ldap  :
 14  Service Auth Method keyserv   :
 15  Service Auth Method passwd-cmd:
 16  Search Time Limit             : 30
 17  Profile Time to Live          : 43200
 18  Bind Limit                    : 10
 19  Enable shadow update          : FALSE
 20  Service Search Descriptors Menu

Enter config value to change: (1-20 0=commit changes) [0]
Enter DN for proxy agent: [cn=proxyagent,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for proxyagent:
Re-enter passwd:

WARNING: About to start committing changes. (y=continue, n=EXIT) y
```

예 11–1 Example, Inc. 네트워크에 대해 idsconfig 명령 실행 *(계속)*

```
  1. Changed timelimit to -1 in cn=config.
  2. Changed sizelimit to -1 in cn=config.
  3. Changed passwordstoragescheme to "crypt" in cn=config.
  4. Schema attributes have been updated.
  5. Schema objectclass definitions have been added.
  6. Database west successfully created.
  7. Suffix dc=west,dc=example,dc=com successfully created.
  8. NisDomainObject added to dc=west,dc=example,dc=com.
  9. Top level "ou" containers complete.
  10. automount maps: auto_home auto_direct auto_master auto_shared processed.
  11. ACI for dc=west,dc=example,dc=com modified to disable self modify.
  12. Add of VLV Access Control Information (ACI).
  13. Proxy Agent cn=proxyagent,ou=profile,dc=west,dc=example,dc=com added.
  14. Give cn=proxyagent,ou=profile,dc=west,dc=example,dc=com read permission
      for password.
  15. Generated client profile and loaded on server.
  16. Processing eq,pres indexes:
      uidNumber (eq,pres)   Finished indexing.
      ipNetworkNumber (eq,pres)   Finished indexing.
      gidnumber (eq,pres)   Finished indexing.
      oncrpcnumber (eq,pres)   Finished indexing.
      automountKey (eq,pres)   Finished indexing.
  17. Processing eq,pres,sub indexes:
      ipHostNumber (eq,pres,sub)   Finished indexing.
      membernisnetgroup (eq,pres,sub)   Finished indexing.
      nisnetgrouptriple (eq,pres,sub)   Finished indexing.
  18. Processing VLV indexes:
      west.example.com.getgrent vlv_index   Entry created
      west.example.com.gethostent vlv_index   Entry created
      west.example.com.getnetent vlv_index   Entry created
      west.example.com.getpwent vlv_index   Entry created
      west.example.com.getrpcent vlv_index   Entry created
      west.example.com.getspent vlv_index   Entry created
      west.example.com.getauhoent vlv_index   Entry created
      west.example.com.getsoluent vlv_index   Entry created
      west.example.com.getauduent vlv_index   Entry created
      west.example.com.getauthent vlv_index   Entry created
      west.example.com.getexecent vlv_index   Entry created
      west.example.com.getprofent vlv_index   Entry created
      west.example.com.getmailent vlv_index   Entry created
      west.example.com.getbootent vlv_index   Entry created
      west.example.com.getethent vlv_index   Entry created
      west.example.com.getngrpent vlv_index   Entry created
      west.example.com.getipnent vlv_index   Entry created
      west.example.com.getmaskent vlv_index   Entry created
      west.example.com.getprent vlv_index   Entry created
      west.example.com.getip4ent vlv_index   Entry created
      west.example.com.getip6ent vlv_index   Entry created

idsconfig: Setup of DSEE server myserver is complete.


Note: idsconfig has created entries for VLV indexes.

      For DS5.x, use the directoryserver(1m) script on myserver
```

예 11–1 Example, Inc. 네트워크에 대해 idsconfig 명령 실행 (계속)

```
        to stop the server.  Then, using directoryserver, follow the
        directoryserver examples below to create the actual VLV indexes.

        For DSEE6.x, use dsadm command delivered with DS on myserver
        to stop the server.  Then, using dsadm, follow the
        dsadm examples below to create the actual VLV indexes.

      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getgrent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.gethostent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getnetent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getpwent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getrpcent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getspent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getauhoent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getsoluent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getauduent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getauthent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getexecent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getprofent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getmailent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getbootent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getethent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getngrpent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getipnent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getmaskent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getprent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getip4ent
      directoryserver -s <server-instance> vlvindex -n west -T west.example.com.getip6ent

<install-path>/bin/dsadm reindex -l -t west.example.com.getgrent <directory-instance-path>
 dc=west,dc=example,dc=com
<install-path>/bin/dsadm reindex -l -t west.example.com.gethostent <directory-instance-path>
 dc=west,dc=example,dc=com
.
.
.
<install-path>/bin/dsadm reindex -l -t west.example.com.getip6ent <directory-instance-path>
 dc=west,dc=example,dc=com
```

ldapaddent 명령을 사용하여 디렉토리 서버 채우기

주 – pam_unix_* 모듈을 사용 중인 경우 디렉토리 서버에 데이터를 채우기 전에 UNIX Crypt 형식으로 암호를 저장하도록 서버를 구성해야 합니다. pam_ldap을 사용 중인 경우 모든 형식으로 암호를 저장할 수 있습니다. UNIX crypt 형식으로 암호를 설정하는 방법에 대한 자세한 내용은 Oracle Directory Server Enterprise Edition 문서를 참조하십시오.

ldapaddent는 표준 입력(passwd 같은 /etc/filename)을 읽고 이 데이터를 서비스와 연관된 컨테이너에 넣습니다. 클라이언트 구성에 따라 기본적으로 데이터를 쓰는 방법이 결정됩니다.

▼ ldapaddent 명령을 사용하여 Oracle Directory Server Enterprise Edition에 사용자 암호 데이터를 채우는 방법

- **ldapaddent 명령을 사용하여 /etc/passwd 항목을 서버에 추가합니다.**

```
# ldapaddent -D "cn=directory manager" -f /etc/passwd passwd
```

ldapaddent(1M) 매뉴얼 페이지를 참조하십시오. 디렉토리 서버에 대한 쓰기 권한과 LDAP 보안에 대한 자세한 내용은 9 장, “LDAP 이름 지정 서비스 소개(개요)”를 참조하십시오.

member 속성을 사용하여 그룹 구성원 지정

Internet-Draft rfc2307bis는 groupOfMembers 객체 클래스를 그룹 서비스의 LDAP 항목에 대한 편리한 구조 클래스로도 사용할 수 있다고 지정합니다. 이러한 그룹 항목은 DN(식별 이름)으로 그룹 구성원을 지정하는 member 속성 값을 가질 수 있습니다. Oracle Solaris LDAP 클라이언트는 이러한 그룹 항목을 지원하고 그룹 구성원 확인 시 member 속성 값을 사용합니다.

LDAP 클라이언트는 groupOfUniqueNames 객체 클래스와 uniqueMember 속성을 사용하는 그룹 항목도 지원합니다. 그러나 이 객체 클래스와 속성은 사용하지 않는 것이 좋습니다.

posixGroup 객체 클래스와 memberUid 속성을 사용하여 그룹 항목을 정의하는 기존 방법이 계속 지원됩니다. ldapaddent 명령이 그룹 서비스에 대한 LDAP 서버를 채울 때 만드는 항목은 여전히 이 유형의 그룹 항목입니다. 따라서 그룹 항목에 member 속성을 추가하지 않습니다.

groupOfMembers 객체 클래스와 member 속성 값을 사용하여 그룹 항목을 추가하려면 ldapadd 도구 및 다음과 유사한 입력 파일을 사용합니다.

```
dn: cn=group1,ou=group,dc=mkg,dc=example,dc=com
objectClass: posixGroup
objectClass: groupOfNames
objectClass: top
cn: group1
gidNumber: 1234
member: uid=user1,ou=people,dc=mkg,dc=example,dc=com
member: uid=user2,ou=people,dc=mkg,dc=example,dc=com
member: cn=group2,ou=group,dc=mkg,dc=example,dc=com
```

LDAP 클라이언트는 memberUid, member 및 uniqueMember 속성이 없거나 일부 또는 모두 포함된 그룹 항목을 처리합니다. 구성원 평가 결과는 중복 항목이 제거된 세 속성의 합집합인 구성원이 그룹에 포함되어 있다는 것입니다. 즉, 그룹 항목 G에 사용자 U1과 U2를 나타내는 memberUid 값, 사용자 U2를 나타내는 member 값, 사용자 U3을 나타내는 uniqueMember 값이 있을 경우 그룹 G는 U1, U2 및 U3의 세 구성원을 포함합니다. 중첩 그룹도 지원됩니다. 즉, member 속성이 다른 그룹을 가리키는 값을 가질 수 있습니다.

그룹 구성원을 효율적으로 평가하여 사용자의 소속 그룹(중첩 그룹 포함)을 결정하려면 LDAP 서버에서 memberOf 플러그인을 구성하고 사용으로 설정해야 합니다. 그렇지 않으면 포함 그룹만 확인되고 중첩 그룹은 확인되지 않습니다. 기본적으로 memberOf 플러그인은 ODSEE 서버에 의해 사용으로 설정됩니다. 플러그인이 사용으로 설정되지 않은 경우 ODSEE의 dsconf 도구로 사용으로 설정합니다.

디렉토리 서버에 추가 프로파일 채우기

ldapclient 명령에 genprofile 옵션을 사용하여 지정된 속성을 기준으로 구성 프로파일의 LDIF 표현을 만듭니다. 그런 다음 생성된 프로파일을 LDAP 서버에 로드하여 클라이언트 프로파일로 사용할 수 있습니다. 클라이언트는 ldapclient init를 사용하여 클라이언트 프로파일을 다운로드할 수 있습니다.

ldapclient genprofile 사용에 대한 자세한 내용은 ldapclient(1M)를 참조하십시오.

▼ ldapclient 명령을 사용하여 디렉토리 서버에 추가 프로파일을 채우는 방법

1 관리자로 전환합니다.

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 genprofile 명령과 함께 ldapclient를 사용합니다.

```
# ldapclient genprofile \
-a profileName=myprofile \
-a defaultSearchBase=dc=west,dc=example,dc=com \
-a "defaultServerList=192.168.0.1 192.168.0.2:386" \> myprofile.ldif
```

3 새 프로파일을 서버에 업로드합니다.

```
# ldapadd -h 192.168.0.1 -D "cn=directory manager" -f myprofile.ldif
```

계정 관리를 사용으로 설정하도록 디렉토리 서버 구성

pam_ldap을 사용하는 클라이언트와 pam_unix_* 모듈을 사용하는 클라이언트에 대해 계정 관리를 구현할 수 있습니다.

주의 – 동일한 LDAP 이름 지정 도메인에 pam_ldap 및 pam_unix_* 모듈을 함께 사용하지 마십시오. 모든 클라이언트가 pam_ldap을 사용하거나 모든 클라이언트가 pam_unix_* 모듈을 사용합니다. 이 제한은 전용 LDAP 서버가 필요함을 나타낼 수 있습니다.

pam_ldap 모듈을 사용하는 클라이언트의 경우

pam_ldap이 제대로 작동하려면 서버에서 암호 및 계정 잠금 정책을 올바르게 구성해야 합니다. 디렉토리 서버 콘솔 또는 ldapmodify를 사용하여 LDAP 디렉토리에 대한 계정 관리 정책을 구성할 수 있습니다. 절차와 자세한 내용은 사용 중인 Oracle Directory Server Enterprise Edition 버전에 대한 **관리 설명서**의 "사용자 계정 관리" 장을 참조하십시오.

주 – 이전에는 pam_ldap 계정 관리를 사용으로 설정한 경우 모든 사용자가 시스템에 로그인할 때마다 인증을 위해 로그인 암호를 제공해야 했습니다. 따라서 ssh 등의 도구를 사용하여 암호 기반이 아닌 로그인을 시도하면 실패했습니다.

사용자가 로그인할 때 디렉토리 서버에 인증하지 않고 계정 관리를 수행하고 사용자의 계정 상태를 검색합니다. 디렉토리 서버의 새 컨트롤은 기본적으로 사용으로 설정되는 1.3.6.1.4.1.42.2.27.9.5.8입니다.

기본값이 아닌 다른 값에 대해 이 컨트롤을 수정하려면 디렉토리 서버에 ACI(액세스 제어 명령)를 추가합니다.

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

proxy 사용자의 암호는 **절대** 만료되지 않아야 합니다. 프록시 암호가 만료되면 proxy 자격 증명 레벨을 사용하는 클라이언트는 서버에서 이름 지정 서비스 정보를 검색할 수 없습니다. 프록시 사용자의 암호가 만료되지 않도록 하려면 다음 스크립트를 사용하여 프록시 계정을 수정합니다.

```
# ldapmodify -h ldapserver -D administrator DN \
-w administrator password <<EOF
dn: proxy user DN
DNchangetype: modify
replace: passwordexpirationtime
passwordexpirationtime: 20380119031407Z
EOF
```

주 – pam_ldap 계정 관리는 Oracle Directory Server Enterprise Edition을 사용하여 암호 에이징 및 계정 만료 정보를 유지 관리하고 사용자에게 제공합니다. 디렉토리 서버는 사용자 계정을 검증하기 위해 섀도우 항목의 해당 데이터를 해석하지 않습니다. 그러나 pam_unix_* 모듈은 섀도우 데이터를 검사하여 계정이 잠겼는지 또는 암호가 에이징되었는지 확인합니다. LDAP 이름 지정 서비스나 디렉토리 서버는 섀도우 데이터를 최신 상태로 유지하지 않으므로 모듈에서 섀도우 데이터를 기준으로 액세스 권한을 부여하면 안됩니다. 섀도우 데이터는 proxy ID를 사용하여 검색합니다. 따라서 proxy 사용자에게 userPassword 속성에 대한 읽기 권한을 부여하지 마십시오. proxy 사용자에게 userPassword에 대한 읽기 권한을 부여하지 않으면 PAM 서비스에서 잘못된 계정 검증을 하지 않습니다.

pam_unix_* 모듈을 사용하는 클라이언트의 경우

LDAP 클라이언트가 계정 관리에 pam_unix_* 모듈을 사용할 수 있게 하려면 섀도우 데이터를 업데이트할 수 있도록 서버를 설정해야 합니다. pam_ldap 계정 관리와 달리 pam_unix_* 모듈은 추가 구성 단계가 필요 없습니다. idsconfig 유틸리티를 실행하여 모든 구성을 수행할 수 있습니다. 기본 idsconfig 실행의 경우 예 11–1을 참조하십시오.

다음은 두 idsconfig 실행의 출력입니다.

첫번째 idsconfig 실행은 기존 클라이언트 프로파일을 사용합니다.

```
# /usr/lib/ldap/idsconfig

It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.

Do you wish to continue with server setup (y/n/h)? [n] y
Enter the JES Directory Server's  hostname to setup: myserver
Enter the port number for DSEE (h=help): [389]
Enter the directory manager DN: [cn=Directory Manager]
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [west.example.com]
Enter LDAP Base DN (h=help): [dc=west,dc=example,dc=com]
  Checking LDAP Base DN ...
  Validating LDAP Base DN and Suffix ...
  sasl/GSSAPI is not supported by this LDAP server
```

```
Enter the profile name (h=help): [default] WestUserProfile

Profile 'WestUserProfile' already exists, it is possible to enable
shadow update now. idsconfig will exit after shadow update
is enabled. You can also continue to overwrite the profile
or create a new one and be given the chance to enable
shadow update later.


Just enable shadow update (y/n/h)? [n] y
Add the administrator identity (y/n/h)? [y]
Enter DN for the administrator: [cn=admin,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for the administrator:
Re-enter passwd:
  ADDED: Administrator identity cn=admin,ou=profile,dc=west,dc=example,dc=com.
         Proxy ACI LDAP_Naming_Services_proxy_password_read does not
         exist for dc=west,dc=example,dc=com.
  ACI SET: Give cn=admin,ou=profile,dc=west,dc=example,dc=com read/write access
           to shadow data.
  ACI SET: Non-Admin access to shadow data denied.

  Shadow update has been enabled.
```

두번째 `idsconfig` 실행은 나중에 사용하기 위해 새 프로파일을 만듭니다. 부분 출력만 표시됩니다.

```
# /usr/lib/ldap/idsconfig

It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.

Do you wish to continue with server setup (y/n/h)? [n] y
Enter the JES Directory Server's  hostname to setup: myserver
Enter the port number for DSEE (h=help): [389]
Enter the directory manager DN: [cn=Directory Manager]
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [west.example.com]
Enter LDAP Base DN (h=help): [dc=west,dc=example,dc=com]
  Checking LDAP Base DN ...
  Validating LDAP Base DN and Suffix ...
  sasl/GSSAPI is not supported by this LDAP server

Enter the profile name (h=help): [default] WestUserProfile-new
Default server list (h=help): [192.168.0.1]
.
.
.
Do you want to enable shadow update (y/n/h)? [n] y

              Summary of Configuration

  1  Domain to serve              : west.example.com
  2  Base DN to setup             : dc=west,dc=example,dc=com
       Suffix to create           : dc=west,dc=example,dc=com
  3  Profile name to create       : WestUserProfile-new
```

```
.
.
.
 19  Enable shadow update          : TRUE
.
.
.
Enter DN for the administrator: [cn=admin,ou=profile,dc=west,dc=example,dc=com]
Enter passwd for the administrator:
Re-enter passwd:


WARNING: About to start committing changes. (y=continue, n=EXIT) y

  1. Changed timelimit to -1 in cn=config.
  2. Changed sizelimit to -1 in cn=config.
.
.
.
  11. ACI for dc=test1,dc=mpklab,dc=sfbay,dc=sun,dc=com modified to
      disable self modify.
.
.
.
  15. Give cn=admin,ou=profile,dc=west,dc=example,dc=com write permission for shadow.
...
```

◆ ◆ ◆ 12 장

12 LDAP 클라이언트 설정(작업)

이 장에서는 LDAP 이름 지정 서비스 클라이언트를 설정하는 방법에 대해 설명합니다. 이 장에서는 다음 내용을 다룹니다.

LDAP 클라이언트 설정을 위한 필수 조건

Oracle Solaris 클라이언트가 LDAP을 이름 지정 서비스로 사용하려면 다음 요구 사항을 충족해야 합니다.

- LDAP 서버가 클라이언트의 도메인 이름을 제공해야 합니다.
- 이름 서비스 스위치는 필수 서비스의 LDAP을 가리켜야 합니다.
- 동작을 정의하는 모든 특정 매개변수를 사용하여 클라이언트를 구성해야 합니다.
- `ldap_cachemgr`이 클라이언트에서 실행되고 있어야 합니다.
- 클라이언트가 구성된 서버가 하나 이상 작동되어 실행 중이어야 합니다.

`ldapclient` 유틸리티는 서버 시작을 제외한 위 단계를 모두 수행하므로 LDAP 클라이언트 설정에 중요합니다. 이 장의 나머지 내용은 `ldapclient` 유틸리티를 사용하여 LDAP 클라이언트를 설정하고 다른 여러 LDAP 유틸리티를 사용하여 LDAP 클라이언트에 대한 정보를 가져오고 상태를 확인하는 방법의 예를 보여 줍니다.

LDAP 및 서비스 관리 기능

LDAP 클라이언트 서비스는 서비스 관리 기능을 사용하여 관리됩니다. SMF 개요는 **Oracle Solaris 11.1에서 서비스 및 결함 관리**의 1 장, "서비스 관리(개요)"를 참조하십시오. 자세한 내용은 svcadm(1M) 및 svcs(1) 매뉴얼 페이지를 참조하십시오.

다음 목록에서는 SMF 서비스를 사용하여 LDAP 클라이언트 서비스를 관리하는 데 필요한 중요한 정보를 간단하게 설명합니다.

- svcadm 명령을 사용하여 사용으로 설정, 사용 안함으로 설정, 다시 시작 등 LDAP 클라이언트 서비스에 대한 관리 작업을 수행할 수 있습니다.

  참고 – -t 옵션을 사용하여 서비스를 일시적으로 사용 안함으로 설정하면 서비스 구성이 보호됩니다. -t 옵션을 사용하여 서비스를 사용 안함으로 설정하면 재부트 후 서비스에 대한 원래 설정이 복원됩니다. -t를 사용하지 않고 서비스를 사용 안함으로 설정하면 재부트 후에도 서비스가 사용 안함으로 유지됩니다.

- LDAP 클라이언트 서비스의 FMRI(오류 관리 리소스 식별자)는 svc:/network/ldap/client입니다.
- 구성 프로세스 중에 network/nis/domain 서비스도 사용으로 설정되어 network/ldap/client 서비스에서 사용되는 도메인 이름을 제공합니다.
- svcs 명령을 사용하여 LDAP 클라이언트 및 ldap_cachemgr 데몬의 상태를 질의할 수 있습니다.
  - 다음은 svcs 명령과 해당 출력의 예입니다.

    ```
    # svcs \*ldap\*
    STATE          STIME    FMRI
    online         15:43:46 svc:/network/ldap/client:default
    ```

  - svcs -l 명령과 해당 출력의 예입니다. 아래 표시된 출력을 얻으려면 FMRI에 인스턴스 이름을 사용해야 합니다.

    ```
    # svcs -l network/ldap/client:default
    fmri         svc:/network/ldap/client:default
    name         LDAP Name Service Client
    enabled      true
    state        online
    next_state   none
    restarter    svc:/system/svc/restarter:default
    manifest     /lib/svc/manifest/network/ldap/client.xml
    manifest     /lib/svc/manifest/network/network-location.xml
    manifest     /lib/svc/manifest/system/name-service/upgrade.xml
    manifest     /lib/svc/manifest/milestone/config.xml
    dependency   require_all/none svc:/system/filesystem/minimal (online)
    dependency   require_all/none svc:/network/initial (online)
    dependency   optional_all/none svc:/network/location:default (online)
    dependency   require_all/restart svc:/network/nis/domain (online)
    dependency   optional_all/none svc:/system/name-service/upgrade (online)
    dependency   optional_all/none svc:/milestone/config (online)
    ```

```
dependency    optional_all/none svc:/system/manifest-import (online)
dependency    require_all/none svc:/milestone/unconfig (online)
```

- 다음 명령을 사용하여 데몬의 존재를 확인할 수 있습니다.
  - 서버에서는 ptree 명령을 사용합니다.

    ```
    # ptree 'pgrep slapd'
    6410 zsched
    11565 /export/dsee/dsee6/ds6/lib/64/ns-slapd -D /export/dsee/test1 -i /export
    ```
  - 클라이언트에서는 다음 명령을 사용합니다.

    ```
    # ldapsearch -h server-name -b "" -s base "objectclass=*" |grep -i context
    namingContexts: dc=example,dc=com
    ```

LDAP 클라이언트 초기화

ldapclient 명령은 Oracle Solaris 시스템에서 LDAP 클라이언트를 설정하는 데 사용됩니다. 이 명령은 서버가 적절한 클라이언트 프로파일로 이미 구성되었다고 가정합니다. 클라이언트를 설정하려면 먼저 서버를 설치하고 적절한 프로파일로 구성해야 합니다.

주 – LDAP과 NIS는 network/nis/domain 서비스에서 정의된 동일한 도메인 이름 구성 요소를 사용하기 때문에 Oracle Solaris OS는 NIS 클라이언트와 고유 LDAP 클라이언트가 동일한 클라이언트 시스템에서 함께 사용되는 구성을 지원하지 않습니다.

---

ldapclient를 사용하여 클라이언트를 설정하는 두 가지 기본 방법이 있습니다.

- **프로파일**

  최소한 사용하려는 프로파일과 도메인은 포함된 서버 주소를 지정해야 합니다. 프로파일을 지정하지 않으면 "기본" 프로파일이 사용됩니다. 서버는 프록시 및 인증서 데이터베이스 정보를 제외하고 나머지 필요한 정보를 제공합니다. 클라이언트의 자격 증명 레벨이 proxy 또는 proxy anonymous인 경우 프록시 바인드 DN과 암호를 제공해야 합니다. 자세한 내용은 130 페이지 "클라이언트 자격 증명 레벨 지정"을 참조하십시오.

  새도우 데이터 업데이트를 사용으로 설정하려면 관리자 자격 증명(adminDN 및 adminPassword)을 제공해야 합니다.

- **설명서**

  클라이언트 자체에 프로파일을 구성하여 명령줄에서 모든 매개변수를 정의합니다. 따라서 프로파일 정보는 캐시 파일에 저장되며 서버에서 새로 고치지 않습니다.

주 – 엔터프라이즈 환경에서 LDAP 구성 프로파일을 사용하면 시스템 간에 프로파일이 공유되는 경우 복잡성을 줄일 수 있습니다.

▼ 프로파일을 사용하여 LDAP 클라이언트를 초기화하는 방법

1 **관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **`init` 옵션을 사용하여 `ldapclient` 명령을 실행합니다.**

```
# ldapclient init -a profileName=new \
-a domainName=west.example.com 192.168.0.1
System successfully configured
```

▼ Per-User 자격 증명을 사용하여 LDAP 클라이언트를 초기화하는 방법

시작하기 전에 per-user 자격 증명을 사용하여 LDAP 클라이언트를 설정하기 전에 다음 항목이 이미 구성되어 있어야 합니다.

- Kerberos KDC(키 배포 센터) 서버가 하나 이상 구성되어 실행 중이어야 합니다.
- DNS, DNS 서버에 대한 클라이언트 액세스 및 하나 이상의 DNS 서버가 구성되어 실행 중이어야 합니다.
- 클라이언트 시스템의 Kerberos가 구성되고 사용으로 설정되어 있어야 합니다.
- 다음과 같은 Kerberos 클라이언트 설치 프로파일이 있어야 합니다.

```
# cat /usr/tmp/krb5.profile
REALM EXAMPLE.COM
KDC kdc.example.com
ADMIN super/admin
FILEPATH /usr/tmp/krb5.conf
NFS 1
DNSLOOKUP none
```

- LDAP 서버가 설치되고 `sasl/GSSAPI`를 지원하도록 구성되어 있어야 합니다.
- 적절한 ID 매핑 구성이 있어야 합니다.
- 디렉토리 서버 및 KDC에 대한 Kerberos 호스트 주체가 KDC에 설정되어 있어야 합니다.
- 사용할 디렉토리 서버 DIT에서 `idsconfig` 명령이 실행된 상태여야 합니다.
- 적절한 per-user `gssapi` 프로파일(예: `gssapi_EXAMPLE.COM`)이 만들어져 있어야 합니다.

`idsconfig` 명령의 per-user 프로파일에 대한 설명은 다음 부분 예에서 보여 줍니다.

```
# /usr/lib/ldap/idsconfig
Do you wish to continue with server setup (y/n/h)? [n] y
Enter the Directory Server's hostname to setup: kdc.example.com
Enter the port number for DSEE (h=help): [389] <Enter your port>
```

```
Enter the directory manager DN: [cn=Directory Manager] <Enter your DN>
Enter passwd for cn=Directory Manager : <Enter your password>
Enter the domainname to be served (h=help): [example.com] <Enter your domain>
Enter LDAP Base DN (h=help): [dc=example,dc=com] <Enter your DN>
GSSAPI is supported. Do you want to set up gssapi:(y/n) [n] y
Enter Kerberos Realm: [EXAMPLE.COM] EXAMPLE.COM
```

주 – 또한 `gssapi` 프로파일의 경우 4 `self` 자격 증명 레벨과 6 `sasl/GSSAPI` 인증 방법을 제공해야 합니다.

- 필요한 사용자 주체가 KDC에 있어야 합니다.
- 클라이언트 시스템에서 Kerberos가 다음과 같은 명령과 클라이언트 프로파일을 사용하여 초기화되어 있어야 합니다.

  ```
  # /usr/sbin/kclient -p /usr/tmp/krb5.profile
  ```
- 이름 서비스 스위치가 `hosts`에 대해 `dns`를 사용하도록 구성되어 있어야 합니다. 다음 명령은 현재 저장소 값을 확인합니다.

  ```
  % svcprop -p config/host system/name-service/switch
  files\ dns\ nis
  ```
- DNS가 구성되어 있어야 하고, DNS 서비스가 실행 중이어야 합니다. 자세한 내용은 본 문서의 DNS 장을 참조하십시오.
- 디렉토리 서버 DIT에 최소한 이 클라이언트 시스템의 사용자, 클라이언트 호스트 및 필요한 `auto_home` LDAP 항목이 미리 로드되어 있어야 합니다. `ldapaddent` 명령을 사용하여 항목을 추가하는 방법에 대한 자세한 내용은 본 설명서의 다른 절을 참조하십시오.

주 – 클라이언트 구성 파일을 직접 편집하지 마십시오. `ldapclient` 명령을 사용하여 이러한 파일의 내용을 만들거나 수정합니다.

1 ldapclient init를 실행하여 gssapi 프로파일을 통해 클라이언트를 초기화합니다.

```
# /usr/sbin/ldapclient init -a profilename=gssapi_EXAMPLE.COM -a \
domainname=example.com 9.9.9.50
```

2 사용자로 로그인합니다.

- **kinit -p** *user***를 실행합니다.**
- **사용자의 로그인 세션에서 ldaplist -l passwd** *user***를 실행합니다. userpassword가 표시되어야 합니다.**
- **ldaplist -l passwd bar를 실행하면 userpassword 없이 항목을 가져올 수 있습니다. 기본적으로 root는 계속해서 모든 사용자의 userpassword를 볼 수 있습니다.**

자세한 정보 **per-user 자격 증명 사용 정보**

- `syslog` 파일에 `libsldap: Status: 7 Mesg: openConnection: GSSAPI bind failed - 82 Local error` 메시지가 표시되는 경우 Kerberos가 초기화되지 않았거나 티켓이 만료된 것입니다. `klist` 명령을 실행하여 찾습니다. 예를 들어, `kinit -p foo` 또는 `kinit -R -p foo`를 실행하고 다시 시도합니다.
- 원하는 경우 로그인할 때 `kinit` 명령이 자동으로 실행되도록 `/etc/pam.conf`에 `pam_krb5.so.1`을 추가할 수 있습니다.

  예를 들면 다음과 같습니다.

  ```
  login   auth optional pam_krb5.so.1
  rlogin  auth optional pam_krb5.so.1
  other   auth optional pam_krb5.so.1
  ```
- 사용자가 `kinit` 명령을 실행했으며 `syslog` 메시지에 `Invalid credential`이 표시되는 경우 `root` 호스트 항목이나 사용자 항목이 LDAP 디렉토리에 없거나 매핑 규칙이 잘못된 것일 수 있습니다.
- `ldapclient init` 명령을 실행하면 LDAP 프로파일에 self/sasl/GSSAPI 구성이 포함되어 있는지 확인합니다. 스위치 검사에 실패할 경우 일반적으로 DNS가 호스트 데이터베이스에 대한 검색 조건이 아니기 때문입니다.
  - DNS 클라이언트 ID가 사용으로 설정되지 않아 검사에 실패할 경우 `svcs -l dns/client`를 실행하여 서비스가 사용 안함으로 설정되었는지 확인합니다. `svcadm enable dns/client`를 실행하여 서비스를 사용으로 설정합니다.
  - sasl/GSSAPI 바인드 때문에 검사에 실패할 경우 `syslog`를 검사하여 문제를 확인합니다.

자세한 내용은 본 설명서와 **Oracle Solaris 11.1 관리: 보안 서비스**의 다른 참조를 참조하십시오.

▼ proxy 자격 증명을 사용하여 LDAP 클라이언트를 초기화하는 방법

주 – 클라이언트 구성 파일을 직접 편집하지 마십시오. `ldapclient` 명령을 사용하여 이러한 파일의 내용을 만들거나 수정합니다.

---

1 관리자로 전환합니다.

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 프록시 값을 정의합니다.

```
# ldapclient init \
-a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
-a domainName=west.example.com \
```

```
-a profileName=pit1 \
-a proxyPassword=test1234 192.168.0.1
System successfully configured
```

사용할 프로파일에 proxy가 설정된 경우 -a proxyDN 및 -a proxyPassword가 **필요합니다**. 서버에 저장된 프로파일에 자격 증명이 저장되어 있지 않으므로 클라이언트를 초기화할 때 정보를 제공해야 합니다. 이 방법은 proxy 자격 증명을 서버에 저장하는 이전 방법보다 더 안전합니다.

프록시 정보는 config 및 cred 등록 정보 그룹의 svc:/network/ldap/client 서비스에 저장됩니다.

▼ LDAP 클라이언트를 초기화하여 섀도우 데이터 업데이트를 사용으로 설정하는 방법

1 관리자로 전환합니다.

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 enableShadowUpdate 스위치를 설정하고 관리자 자격 증명을 정의하려면 ldapclient 명령을 실행합니다.

- **이미 실행 중인 LDAP 클라이언트를 업데이트하려면 다음 명령을 실행합니다.**

```
# ldapclient mod -a enableShadowUpdate=TRUE \
-a adminDN=cn=admin,ou=profile,dc=west,dc=example,dc=com \
-a adminPassword=admin-password
System successfully configured
```

- **LDAP 클라이언트를 초기화하려면 다음 명령을 실행합니다.**

```
# ldapclient init \
-a adminDN=cn=admin,ou=profile,dc=west,dc=example,dc=com \
-a adminPassword=admin-password
-a domainName=west.example.com \
-a profileName=WestUserProfile \
-a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
-a proxyPassword=<proxy_password> \
192.168.0.1
System successfully configured
```

3 구성을 확인하려면 network/ldap/client 서비스의 cred 등록 정보 내용을 표시합니다.

출력은 다음과 유사하게 나타납니다.

```
# svcprop -p cred svc:/network/ldap/client
cred/read_authorization astring solaris.smf.value.name-service.ldap.client
cred/value_authorization astring solaris.smf.value.name-service.ldap.client
cred/bind_dn astring cn=proxyagent,ou=profile,dc=west,dc=example,dc=com
cred/bind_passwd astring {NS1}4a3788f8eb85de11
cred/enable_shadow_update boolean true
```

```
cred/admin_bind_dn astring cn=admin,ou=profile,dc=west,dc=example,dc=com
cred/admin_bind_passwd astring {NS1}4a3788f8c053434f
```

▼ 수동으로 LDAP 클라이언트를 초기화하는 방법

루트 사용자나 이에 상응하는 역할을 가진 관리자는 수동 LDAP 클라이언트 구성을 수행할 수 있습니다. 그러나 많은 검사는 프로세스 중에 생략되므로 시스템을 잘못 구성하기 쉽습니다. 또한 프로파일을 사용할 때와 같이 단일 중앙 장소가 아니라 **모든 시스템**에서 설정을 변경해야 합니다.

1. **관리자로 전환합니다.**

   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2. **클라이언트를 초기화합니다.**

   ```
   # ldapclient manual \
   -a domainName=dc=west.example.com -a credentialLevel=proxy \
   -a defaultSearchBase=dc=west,dc=example,dc=com \
   -a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
   -a proxyPassword=testtest 192.168.0.1
   ```

3. **LDAP 클라이언트 구성을 확인합니다.**

   ```
   # ldapclient list
   NS_LDAP_FILE_VERSION= 2.0
   NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=west,dc=example,dc=com
   NS_LDAP_BINDPASSWD= {NS1}4a3788e8c053424f
   NS_LDAP_SERVERS= 192.168.0.1
   NS_LDAP_SEARCH_BASEDN= dc=west,dc=example,dc=com
   NS_LDAP_CREDENTIAL_LEVEL= proxy
   ```

▼ 수동 LDAP 클라이언트 구성을 수정하는 방법

1. **관리자로 전환합니다.**

   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2. **`ldapclient mod` 명령을 사용하여 인증 방법을 `simple`로 변경합니다.**

   ```
   # ldapclient mod -a authenticationMethod=simple
   ```

3. **LDAP 클라이언트 구성이 변경되었는지 확인합니다.**

   ```
   # ldapclient list
   NS_LDAP_FILE_VERSION= 2.0
   NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=west,dc=example,dc=com
   NS_LDAP_BINDPASSWD= {NS1}4a3788e8c053424f
   NS_LDAP_SERVERS= 192.168.0.1
   ```

```
NS_LDAP_SEARCH_BASEDN= dc=west,dc=example,dc=com
NS_LDAP_AUTH= simple
NS_LDAP_CREDENTIAL_LEVEL= proxy
```

일반 오류 mod 하위 명령을 사용하여 LDAP 클라이언트 구성의 일부 속성을 변경할 수 없습니다. 예를 들어, profileName 및 profileTTL 속성을 변경할 수 없습니다. 이러한 속성을 변경하려면 172 페이지 "프로파일을 사용하여 LDAP 클라이언트를 초기화하는 방법"에 설명된 대로 ldapclient init 명령을 사용하여 새 프로파일을 만듭니다. 또는 176 페이지 "수동으로 LDAP 클라이언트를 초기화하는 방법"에 설명된 대로 ldapclient manual 명령을 실행합니다.

▼ LDAP 클라이언트 초기화를 해제하는 방법

ldapclient uninit 명령은 최근 init, modify 또는 manual 작업 이전의 상태로 클라이언트 이름 서비스를 복원합니다. 즉, 이 명령은 마지막으로 수행된 단계에 대해 "실행 취소"를 수행합니다. 예를 들어, 클라이언트가 profile1을 사용하도록 구성된 다음 profile2를 사용하도록 변경된 경우 ldapclient uninit를 사용하면 클라이언트가 다시 profile1을 사용합니다.

1 관리자로 전환합니다.

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 LDAP 클라이언트의 초기화를 해제합니다.

```
# ldapclient uninit
System successfully recovered
```

TLS 보안 설정

주 – 모든 사용자가 보안 데이터베이스 파일을 읽을 수 있어야 합니다. key3.db 파일에 개인 키를 포함하지 마십시오.

TLS(전송 계층 보안)를 사용하는 경우 필요한 보안 데이터베이스를 설치해야 합니다. 특히 인증서와 키 데이터베이스 파일이 필요합니다. 예를 들어, Mozilla Firefox의 최신 데이터베이스 형식을 사용하는 경우 3개의 파일인 cert8.db, key3.db 및 secmod.db가 필요합니다. cert8.db 파일에 인증된 인증서가 포함되어 있으며, key3.db 파일에 클라이언트의 키가 포함되어 있습니다. LDAP 이름 지정 서비스 클라이언트가 클라이언트 키를 사용하지 않는 경우에도 이 파일은 있어야 합니다. secmod.db 파일에는 PKCS#11 모듈 등의 보안 모듈이 들어 있습니다. 이전 형식을 사용하는 경우에는 이 파일이 필요 없습니다.

주 – ldapclient를 실행하기 전에 이 절에 설명된 필요한 보안 데이터베이스 파일을 설정하고 설치해야 합니다.

사용 중인 Oracle Directory Server Enterprise Edition 버전의 관리자 설명서, "SSL 관리"에서 SSL 사용을 위해 LDAP 클라이언트 구성 절을 참조하십시오. 이러한 파일을 만들고 관리하는 방법에 대해 자세한 내용을 참조하십시오. 구성한 후에는 LDAP 이름 지정 서비스 클라이언트에 필요한 위치에 이러한 파일을 저장해야 합니다. certificatePath 속성은 이 위치를 결정하는 데 사용됩니다. 기본 위치는 /var/ldap입니다.

예를 들어, Mozilla Firefox를 사용하여 필요한 cert8.db, key3.db 및 secmod.db 파일을 설정한 후 다음과 같이 이 파일을 기본 위치에 복사합니다.

```
# cp $HOME/.mozilla/firefox/*.default/cert8.db /var/ldap
# cp $HOME/.mozilla/firefox/*.default/key3.db /var/ldap
# cp $HOME/.mozilla/firefox/*.default/secmod.db /var/ldap
```

모든 사용자에게 읽기 권한을 부여합니다.

```
# chmod 444 /var/ldap/cert8.db
# chmod 444 /var/ldap/key3.db
# chmod 444 /var/ldap/secmod.db
```

주 – Mozilla Firefox의 cert8.db, key3.db 및 secmod.db 파일은 $HOME/.mozilla의 하위 디렉토리에서 관리됩니다. 이러한 보안 데이터베이스의 복사본을 LDAP 이름 지정 서비스 클라이언트에 사용하는 경우 복사본이 로컬 파일 시스템에 저장되어 있어야 합니다.

PAM 구성

pam_ldap 모듈은 LDAP에 대한 인증 및 계정 관리 PAM 모듈 옵션 중 하나입니다. 현재 pam_ldap에서 지원되는 기능에 대한 자세한 내용은 pam_ldap(5) 매뉴얼 페이지를 참조하십시오.

per-user 모드와 self 자격 증명 옵션을 모두 선택한 경우 PAM Kerberos pam_krb5 모듈도 사용으로 설정해야 합니다. 자세한 내용은 pam_krb5(5) 매뉴얼 페이지와 **Oracle Solaris 11.1 관리: 보안 서비스** 설명서를 참조하십시오.

UNIX policy를 사용하도록 PAM 구성

UNIX policy를 사용하도록 PAM을 구성하려면 기본 /etc/pam.conf 파일을 사용합니다. 변경할 필요가 없습니다. 자세한 내용은 pam.conf(4) 매뉴얼 페이지를 참조하십시오.

그러나 shadow 데이터로 제어되는 암호 에이징 및 암호 정책이 필요한 경우 enableShadowUpdate 스위치를 사용하여 클라이언트를 구성하고 실행해야 합니다. 자세한 내용은 175 페이지 "LDAP 클라이언트를 초기화하여 섀도우 데이터 업데이트를 사용으로 설정하는 방법"을 참조하십시오.

LDAP server_policy를 사용하도록 PAM 구성

LDAP server_policy를 사용하도록 PAM을 구성하려면 191 페이지 "계정 관리에 pam_ldap 모듈을 사용하는 pam_conf 파일 예"의 샘플을 따르십시오. pam_ldap.so.1이 포함된 라인을 클라이언트의 /etc/pam.conf 파일에 추가합니다. 또한 샘플 pam.conf 파일의 PAM 모듈에 binding 플래그와 server_policy 옵션을 지정하는 경우 클라이언트의 /etc/pam.conf 파일에서 해당 모듈에 대해 동일한 플래그와 옵션을 사용합니다. 또한 서비스 모듈 pam_authtok_store.so.1이 포함된 라인에 server_policy 옵션을 추가합니다.

주 – 이전에는 pam_ldap 계정 관리를 사용으로 설정한 경우 모든 사용자가 시스템에 로그인할 때마다 인증을 위해 로그인 암호를 제공해야 했습니다. 따라서 ssh 등의 도구를 사용하여 암호 기반이 아닌 로그인을 시도하면 실패했습니다.

사용자가 로그인할 때 디렉토리 서버에 인증하지 않고 계정 관리를 수행하고 사용자의 계정 상태를 검색합니다. 디렉토리 서버의 새 컨트롤은 기본적으로 사용으로 설정되는 1.3.6.1.4.1.42.2.27.9.5.8입니다.

기본값이 아닌 다른 값에 대해 이 컨트롤을 수정하려면 디렉토리 서버에 ACI(액세스 제어 명령)를 추가합니다.

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

- binding 제어 플래그

  binding 제어 플래그를 사용하면 원격(LDAP) 암호의 로컬 암호 대체가 가능합니다. 예를 들어, 로컬 파일과 LDAP 이름 공간 둘 다에 사용자 계정이 있는 경우 로컬 계정과 연관된 암호가 원격 암호보다 우선 적용됩니다. 따라서 로컬 암호가 만료되면 원격 LDAP 암호가 유효해도 인증에 실패합니다.

- server_policy 옵션

  server_policy 옵션을 사용하면 pam_unix_auth, pam_unix_account 및 pam_passwd_auth가 LDAP 이름 공간에서 찾은 사용자를 무시하고 pam_ldap에서 인증 또는 계정 검증을 수행할 수 있게 합니다. pam_authtok_store의 경우 새 암호가 암호화

없이 LDAP 서버로 전달됩니다. 따라서 암호가 서버에 구성된 암호 보안 처리 체계에 따라 디렉토리에 저장됩니다. 자세한 내용은 pam.conf(4) 및 pam_ldap(5)를 참조하십시오.

LDAP 이름 지정 서비스 정보 검색

ldaplist 유틸리티를 사용하여 LDAP 이름 지정 서비스에 대한 정보를 검색할 수 있습니다. 이 LDAP 유틸리티는 LDAP 서버의 이름 지정 정보를 LDIF 형식으로 나열합니다. 문제 해결에 유용할 수 있습니다. 자세한 내용은ldaplist(1)을 참조하십시오.

모든 LDAP 컨테이너 나열

ldaplist는 빈 라인으로 레코드를 구분하여 출력을 표시하며 큰 다중 라인 레코드에 유용합니다.

주 – ldaplist 출력은 클라이언트 구성에 따라 달라집니다. 예를 들어, ns_ldap_search 값이 one이 아니라 sub이면 ldaplist는 현재 검색 baseDN 아래의 모든 항목을 나열합니다.

다음은 ldaplist 출력의 예입니다.

```
# ldaplist
dn: ou=people,dc=west,dc=example,dc=com

dn: ou=group,dc=west,dc=example,dc=com

dn: ou=rpc,dc=west,dc=example,dc=com

dn: ou=protocols,dc=west,dc=example,dc=com

dn: ou=networks,dc=west,dc=example,dc=com

dn: ou=netgroup,dc=west,dc=example,dc=com

dn: ou=aliases,dc=west,dc=example,dc=com

dn: ou=hosts,dc=west,dc=example,dc=com

dn: ou=services,dc=west,dc=example,dc=com

dn: ou=ethers,dc=west,dc=example,dc=com

dn: ou=profile,dc=west,dc=example,dc=com

dn: automountmap=auto_home,dc=west,dc=example,dc=com
```

```
dn: automountmap=auto_direct,dc=west,dc=example,dc=com

dn: automountmap=auto_master,dc=west,dc=example,dc=com

dn: automountmap=auto_shared,dc=west,dc=example,dc=com
```

모든 사용자 항목 속성 나열

사용자의 passwd 항목 등 특정 정보를 나열하려면 다음과 같이 getent를 사용합니다.

```
# getent passwd user1
user1::30641:10:Joe Q. User:/home/user1:/bin/csh
```

모든 속성을 나열하려는 경우 ldaplist에 -l 옵션을 사용합니다.

```
# ldaplist -l passwd user1
        dn: uid=user1,ou=People,dc=west,dc=example,dc=com
        uid: user1
        cn: user1
        uidNumber: 30641
        gidNumber: 10
        gecos: Joe Q. User
        homeDirectory: /home/user1
        loginShell: /bin/csh
        objectClass: top
        objectClass: shadowAccount
        objectClass: account
        objectClass: posixAccount
        shadowLastChange: 6445
```

LDAP 클라이언트 환경 사용자 정의

다음 절에서는 LDAP 클라이언트 환경을 사용자 정의할 수 있는 방법에 대해 설명합니다.

모든 서비스를 변경할 수 있지만 지정한 서비스에 대한 데이터가 서버에 채워져 있지 않으면 작동이 중지되므로 주의해야 합니다. 또한 기본적으로 파일을 설정할 수 없는 경우도 있습니다.

LDAP에 대한 이름 서비스 스위치 수정

이름 서비스 스위치를 수정하여 각 이름 지정 서비스가 정보에 액세스하는 위치를 사용자 정의할 수 있습니다. 36 페이지 “이름 서비스 스위치 관리”를 참조하십시오.

LDAP을 통해 DNS를 사용으로 설정

DNS를 사용으로 설정하려는 경우 44 페이지 “DNS 클라이언트를 사용으로 설정하는 방법”을 참조하십시오. per-user 인증을 사용하는 경우 sasl/GSSAPI 및 Kerberos 방식을 위해 DNS 이름 지정 서비스를 구성하고 사용으로 설정해야 합니다.

◆ ◆ ◆ 13장

13 LDAP 문제 해결(참조)

이 장에서는 LDAP 구성 문제에 대해 설명하고 해결 방법을 제안합니다.

LDAP 클라이언트 상태 모니터링

다음 절에서는 LDAP 클라이언트 환경의 상태를 확인하는 데 도움이 되는 다양한 명령을 보여 줍니다. 사용할 수 있는 옵션에 대한 자세한 내용은 매뉴얼 페이지를 참조하십시오.

SMF(서비스 관리 기능) 개요는 **Oracle Solaris 11.1에서 서비스 및 결함 관리**의 1 장, "서비스 관리(개요)"를 참조하십시오. 자세한 내용은 svcadm(1M) 및 svcs(1) 매뉴얼 페이지를 참조하십시오.

ldap_cachemgr 데몬이 실행 중인지 확인

항상 ldap_cachemgr 데몬이 올바르게 실행되고 작동해야 합니다. 그렇지 않으면 시스템이 작동하지 않습니다. LDAP 클라이언트 서비스인 svc:/network/ldap/client를 설정하고 시작하면 클라이언트 SMF 메소드가 자동으로 ldap_cachemgr 데몬을 시작합니다. 다음 메소드는 LDAP 클라이언트 서비스가 온라인 상태인지 확인합니다.

- svcs 명령을 사용하여 서비스가 사용으로 설정되었는지 확인합니다.

```
# svcs \*ldap\*
STATE          STIME    FMRI
disabled       Aug_24   svc:/network/ldap/client:default
```

- 이 명령을 사용하여 서비스에 대한 모든 정보를 확인합니다.

```
# svcs -l network/ldap/client:default
fmri svc:/network/ldap/client:default
name LDAP Name Service Client
enabled false
state disabled
next_state none
state_time Thu Oct 20 23:04:11 2011
```

```
logfile /var/svc/log/network-ldap-client:default.log
restarter svc:/system/svc/restarter:default
contract_id
manifest /lib/svc/manifest/network/ldap/client.xml
manifest /lib/svc/manifest/milestone/config.xml
manifest /lib/svc/manifest/network/network-location.xml
manifest /lib/svc/manifest/system/name-service/upgrade.xml
dependency optional_all/none svc:/milestone/config (online)
dependency optional_all/none svc:/network/location:default (online)
dependency require_all/none svc:/system/filesystem/minimal (online)
dependency require_all/none svc:/network/initial (online)
dependency require_all/restart svc:/network/nis/domain (online)
dependency optional_all/none svc:/system/manifest-import (online)
dependency require_all/none svc:/milestone/unconfig (online)
dependency optional_all/none svc:/system/name-service/upgrade (online)
```

- `-g` 옵션을 `ldap_cachemgr`에 전달합니다.

  이 옵션은 문제를 진단할 때 유용한 보다 광범위한 상태 정보를 제공합니다.

```
# /usr/lib/ldap/ldap_cachemgr -g
cachemgr configuration:
server debug level          0
server log file "/var/ldap/cachemgr.log"
number of calls to ldapcachemgr         19

cachemgr cache data statistics:
Configuration refresh information:
  Previous refresh time: 2010/11/16 18:33:28
  Next refresh time:     2010/11/16 18:43:28
Server information:
  Previous refresh time: 2010/11/16 18:33:28
  Next refresh time:     2010/11/16 18:36:08
  server: 192.168.0.0, status: UP
  server: 192.168.0.1, status: ERROR
    error message: Can't connect to the LDAP server
Cache data information:
  Maximum cache entries:          256
  Number of cache entries:          2
```

`ldap_cachemgr` 데몬에 대한 자세한 내용은 `ldap_cachemgr(1M)` 매뉴얼 페이지를 참조하십시오.

현재 프로파일 정보 확인

수퍼유저가 되거나 이에 상응하는 역할을 맡고 `list` 옵션을 사용하여 `ldapclient`를 실행합니다.

```
# ldapclient list
NS_LDAP_FILE_VERSION= 2.0
NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=west,dc=example,dc=com
NS_LDAP_BINDPASSWD= {NS1}4a3788e8c053424f
NS_LDAP_SERVERS= 192.168.0.1, 192.168.0.10
NS_LDAP_SEARCH_BASEDN= dc=west,dc=example,dc=com
NS_LDAP_AUTH= simple
```

```
NS_LDAP_SEARCH_REF= TRUE
NS_LDAP_SEARCH_SCOPE= one
NS_LDAP_SEARCH_TIME= 30
NS_LDAP_SERVER_PREF= 192.168.0.1
NS_LDAP_PROFILE= pit1
NS_LDAP_CREDENTIAL_LEVEL= proxy
NS_LDAP_SERVICE_SEARCH_DESC= passwd:ou=people,?sub
NS_LDAP_SERVICE_SEARCH_DESC= group:ou=group,dc=west,dc=example,dc=com?one
NS_LDAP_BIND_TIME= 5
```

svccfg 또는 svcprop 명령을 사용하거나 ldapclient 명령에 list 옵션을 사용하여 현재 프로파일 정보를 볼 수 있습니다. 사용 가능한 모든 등록 정보 설정에 대한 자세한 내용은 ldapclient(1M) 매뉴얼 페이지를 참조하십시오.

기본 클라이언트-서버 통신 확인

클라이언트가 LDAP 서버와 통신 중임을 보여 주는 최상의 방법은 ldaplist 명령을 사용하는 것입니다. 인수 없이 ldaplist를 사용하면 서버의 모든 컨테이너가 덤프됩니다. 이 기능은 컨테이너가 있으며 이를 채울 필요가 없는 한 작동합니다. 자세한 내용은 ldaplist(1) 매뉴얼 페이지를 참조하십시오.

첫번째 단계가 작동하면 ldaplist passwd *username* 또는 ldaplist hosts *hostname*을 시도할 수 있지만 많은 데이터가 포함된 경우 덜 채워진 서비스를 선택하거나 head 또는 more로 파이프할 수도 있습니다.

비클라이언트 시스템에서 서버 데이터 확인

앞 절에 나와 있는 대부분의 명령은 사용자가 LDAP 클라이언트를 이미 만들었다고 가정합니다. 클라이언트를 만들지 않았으며 서버의 데이터를 확인하려는 경우에는 ldapsearch 명령을 사용합니다. 다음 예에서는 모든 컨테이너를 나열합니다.

```
# ldapsearch -h server1 -b "dc=west,dc=example,dc=com" -s one "objectclass=*"
```

ldapsearch 명령의 기본 출력은 RFC-2849에 정의된 산업 표준화된 LDIF 형식입니다. 모든 버전의 ldapsearch가 -L 옵션을 사용하여 LDIF 형식을 출력할 수 있습니다.

LDAP 구성 문제 및 해결 방법

다음 절에서는 LDAP 구성 문제에 대해 설명하고 문제 해결 방법을 제안합니다.

확인되지 않은 호스트 이름

LDAP 클라이언트 백엔드는 호스트 조회에 대해 정규화된 호스트 이름(예: gethostbyname() 및 getaddrinfo()에 의해 반환되는 호스트 이름)을 반환합니다. 저장된

이름이 정규화된 경우, 즉 점이 하나 이상 포함된 경우 클라이언트는 이름을 있는 그대로 반환합니다. 예를 들어, 저장된 이름이 hostB.eng이면 반환되는 이름은 hostB.eng입니다.

LDAP 디렉토리에 저장된 이름이 정규화되지 않은 경우(점을 포함하지 않음) 클라이언트 백엔드가 이름에 도메인 부분을 추가합니다. 예를 들어, 저장된 이름이 hostA이면 반환되는 이름은 hostA.domainname입니다.

LDAP 도메인의 시스템에 원격으로 연결할 수 없음

DNS 도메인 이름이 LDAP 도메인 이름과 다른 경우 호스트 이름이 정규화된 상태로 저장되어 있지 않으면 LDAP 이름 지정 서비스를 사용하여 호스트 이름을 제공할 수 없습니다.

로그인이 작동하지 않음

LDAP 클라이언트는 로그인 중에 PAM 모듈을 사용자 인증에 사용합니다. 표준 UNIX PAM 모듈을 사용하는 경우 암호가 서버에서 읽혀 클라이언트측에서 확인됩니다. 이 프로세스는 다음 이유 중 하나로 인해 실패할 수 있습니다.

1. ldap이 이름 서비스 스위치의 passwd 데이터베이스와 연관되어 있지 않습니다.
2. 프록시 에이전트가 서버 목록의 사용자 userPassword 속성을 읽을 수 없습니다. 프록시 에이전트가 비교를 위해 암호를 클라이언트로 반환하기 때문에 최소한 프록시 에이전트가 암호를 읽을 수 있도록 해야 합니다. pam_ldap에는 암호에 대한 읽기 권한이 필요하지 않습니다.
3. 프록시 에이전트에 올바른 암호가 없을 수도 있습니다.
4. 항목에 shadowAccount 객체 클래스가 없습니다.
5. 사용자의 암호가 정의되어 있지 않습니다.

   ldapaddent를 사용하는 경우 -p 옵션을 사용하여 사용자 항목에 암호가 추가되도록 해야 합니다. -p 옵션 없이 ldapaddent를 사용하는 경우 ldapaddent를 사용하여 /etc/shadow 파일도 추가하지 않으면 사용자 암호가 디렉토리에 저장되지 않습니다.
6. 연결할 수 있는 LDAP 서버가 없습니다.

   서버의 상태를 확인합니다.

   ```
   # /usr/lib/ldap/ldap_cachemgr -g
   ```
7. pam.conf가 잘못 구성되었습니다.
8. LDAP 이름 공간에 사용자가 정의되어 있지 않습니다.
9. pam_unix_* 모듈에 대해 NS_LDAP_CREDENTIAL_LEVEL이 anonymous로 설정되었는데 익명 사용자는 userPassword를 사용할 수 없습니다.
10. 암호가 crypt 형식으로 저장되어 있지 않습니다.
11. pam_ldap이 계정 관리를 지원하도록 구성된 경우 로그인 실패는 다음 중 하나의 결과일 수 있습니다.

- 사용자 암호가 만료되었습니다.
- 실패한 로그인 시도 횟수가 너무 많아서 사용자 계정이 잠겼습니다.
- 관리자가 사용자 계정을 비활성화했습니다.
- 사용자가 `ssh` 또는 `sftp`와 같은 비암호 기반 프로그램을 사용하여 로그인을 시도했습니다.

12. per-user 인증 및 sasl/GSSAPI를 사용 중인 경우 Kerberos의 일부 구성 요소나 `pam_krb5` 구성이 잘못 설정된 것입니다. 이러한 문제 해결에 대한 자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**를 참조하십시오.

조회 속도가 너무 느림

LDAP 데이터베이스는 색인을 사용하여 검색 성능을 향상시킵니다. 색인이 잘못 구성된 경우 성능이 심각하게 저하됩니다. 본 설명서에는 색인화해야 하는 일반적인 속성 세트가 포함되어 있습니다. 고유한 색인을 추가하여 사이트의 성능을 향상시킬 수도 있습니다.

`ldapclient` 명령이 서버에 바인딩될 수 없음

`ldapclient` 명령이 지정된 `profileName` 속성과 함께 `init` 옵션을 사용할 때 클라이언트를 초기화하지 못했습니다. 가능한 실패 이유는 다음과 같습니다.

1. 명령줄에서 잘못된 도메인 이름을 지정했습니다.
2. 지정된 클라이언트 도메인의 시작점을 나타내는 `nisDomain` 속성이 DIT에 설정되어 있지 않습니다.
3. 서버에 액세스 제어 정보가 제대로 설정되지 않아 LDAP 데이터베이스에서 익명 검색을 사용할 수 없습니다.
4. 잘못된 서버 주소가 `ldapclient` 명령에 전달되었습니다. `ldapsearch` 명령을 사용하여 서버 주소를 확인합니다.
5. 잘못된 프로파일 이름이 `ldapclient` 명령에 전달되었습니다. `ldapsearch` 명령을 사용하여 DIT의 프로파일 이름을 확인합니다.
6. 클라이언트 네트워크 인터페이스의 `snoop`를 사용하여 나가는 트래픽 종류와 통신 중인 서버를 확인합니다.

디버깅에 `ldap_cachemgr` 데몬 사용

`-g` 옵션을 사용하여 `ldap_cachemgr` 데몬을 실행하면 현재 클라이언트 구성과 통계를 볼 수 있으므로 디버깅에 유용할 수 있습니다. 예를 들어,

```
# ldap_cachemgr -g
```

는 앞에서 설명한 대로 모든 LDAP 서버의 상태를 비롯한 현재 구성 및 통계를 표준 출력에 인쇄합니다. 이 명령을 실행하기 위해 수퍼유저가 될 필요는 **없습니다**.

`ldapclient` 명령이 설정 중에 중단됨

`ldapclient` 명령이 중단될 경우 Ctrl-C를 누르면 이전 환경을 복원한 후 종료됩니다. 이 경우 서버 관리자에게 문의하여 서버가 실행 중인지 확인하십시오.

또한 프로파일이나 명령줄에서 서버 목록 속성을 검사하고 서버 정보가 올바른지 확인하십시오.

◆ ◆ ◆ 14장

14 LDAP 이름 지정 서비스(참조)

이 장에서는 다음 내용을 다룹니다.

LDAP 구성을 위한 빈 점검 목록

표 14–1 서버 변수 정의를 위한 빈 점검 목록

변수	_____ 네트워크에 대한 정의
디렉토리 서버 인스턴스가 설치된 포트 번호(389)	
서버 이름	
복제 서버(IP 번호:포트 번호)	
디렉토리 관리자 [dn: cn=directory manager]	
제공할 도메인 이름	
시간 초과 전까지 클라이언트 요청을 처리할 최대 시간(초)	
각 검색 요청에 대해 반환되는 최대 항목 수	

표 14–2 클라이언트 프로파일 변수 정의를 위한 빈 점검 목록

변수	_____ 네트워크에 대한 정의
프로파일 이름	
서버 목록(기본적으로 로컬 서브넷으로 지정됨)	
기본 서버 목록(첫번째, 두번째 등으로 시도할 서버 순서대로 나열됨)	
검색 범위(디렉토리 트리 아래의 레벨 수. 'One' 또는 'Sub')	
서버에 액세스하는 데 사용되는 자격 증명. 기본값은 anonymous입니다.	
참조 따름?(주 서버를 사용할 수 없는 경우 다른 서버에 대한 포인터) 기본값은 no입니다.	
서버가 정보를 반환할 때까지 기다리는 검색 시간 제한(초). 기본값은 30초입니다.	
서버에 연결하기 위한 바인딩 시간 제한(초). 기본값은 30초입니다.	
인증 방법. 기본값은 none입니다.	

LDAP 명령

Oracle Solaris 시스템에는 LDAP 관련 명령 세트 2개가 있습니다. 한 세트는 일반적인 LDAP 도구로, LDAP 이름 지정 서비스를 사용하여 클라이언트를 구성할 필요가 없습니다. 두번째 세트는 클라이언트의 일반적인 LDAP 구성을 사용하며 LDAP 이름 지정 서비스를 사용하거나 사용하지 않고 구성된 클라이언트에서 실행될 수 있습니다.

일반적인 LDAP 도구

LDAP 명령줄 도구는 인증 및 바인딩 매개변수를 비롯한 일반적인 옵션 세트를 지원합니다. 다음 도구는 디렉토리 정보를 나타내기 위한 일반적인 텍스트 기반 형식인 LDIF(LDAP Data Interchange Format)를 지원합니다. 다음 명령을 사용하여 디렉토리 항목을 직접 조작할 수 있습니다.

ldapsearch(1)
ldapmodify(1)
ldapadd(1)
ldapdelete(1)

LDAP 이름 지정 서비스가 필요한 LDAP 도구

표 14–3 LDAP 도구

도구	기능
ldapaddent(1M)	해당 /etc 파일에서 LDAP 컨테이너의 항목을 만드는 데 사용됩니다. 이 도구를 사용하면 파일에서 디렉토리를 채울 수 있습니다. 예를 들어, 이 도구는 /etc/passwd 형식 파일을 읽고 디렉토리에 passwd 항목을 채웁니다.
ldaplist(1)	디렉토리에서 다양한 서비스의 내용을 나열하는 데 사용됩니다.
idsconfig(1M)	LDAP 이름 지정 서비스 클라이언트에 서비스를 제공하도록 Oracle Directory Server Enterprise Edition을 설정하는 데 사용됩니다.

계정 관리에 pam_ldap 모듈을 사용하는 pam_conf 파일 예

주 – 이전에는 pam_ldap 계정 관리를 사용으로 설정한 경우 모든 사용자가 시스템에 로그인할 때마다 인증을 위해 로그인 암호를 제공해야 했습니다. 따라서 ssh 등의 도구를 사용하여 암호 기반이 아닌 로그인을 시도하면 실패했습니다.

사용자가 로그인할 때 디렉토리 서버에 인증하지 않고 계정 관리를 수행하고 사용자의 계정 상태를 검색합니다. 디렉토리 서버의 새 컨트롤은 기본적으로 사용으로 설정되는 1.3.6.1.4.1.42.2.27.9.5.8입니다.

기본값이 아닌 다른 값에 대해 이 컨트롤을 수정하려면 디렉토리 서버에 ACI(액세스 제어 명령)를 추가합니다.

```
dn: oid=1.3.6.1.4.1.42.2.27.9.5.8,cn=features,cn=config
objectClass: top
objectClass: directoryServerFeature
oid:1.3.6.1.4.1.42.2.27.9.5.8
cn:Password Policy Account Usable Request Control
aci: (targetattr != "aci")(version 3.0; acl "Account Usable";
     allow (read, search, compare, proxy)
     (groupdn = "ldap:///cn=Administrators,cn=config");)
creatorsName: cn=server,cn=plugins,cn=config
modifiersName: cn=server,cn=plugins,cn=config
```

```
#
# Authentication management
#
# login service (explicit because of pam_dial_auth)
#
login   auth requisite         pam_authtok_get.so.1
login   auth required          pam_dhkeys.so.1
login   auth required          pam_unix_cred.so.1
```

```
login   auth required         pam_dial_auth.so.1
login   auth binding          pam_unix_auth.so.1 server_policy
login   auth required         pam_ldap.so.1
#
# rlogin service (explicit because of pam_rhost_auth)
#
rlogin  auth sufficient       pam_rhosts_auth.so.1
rlogin  auth requisite        pam_authtok_get.so.1
rlogin  auth required         pam_dhkeys.so.1
rlogin  auth required         pam_unix_cred.so.1
rlogin  auth binding          pam_unix_auth.so.1 server_policy
rlogin  auth required         pam_ldap.so.1
#
# rsh service (explicit because of pam_rhost_auth,
# and pam_unix_auth for meaningful pam_setcred)
#
rsh     auth sufficient       pam_rhosts_auth.so.1
rsh     auth required         pam_unix_cred.so.1
rsh     auth binding          pam_unix_auth.so.1 server_policy
rsh     auth required         pam_ldap.so.1
#
# PPP service (explicit because of pam_dial_auth)
#
ppp     auth requisite        pam_authtok_get.so.1
ppp     auth required         pam_dhkeys.so.1
ppp     auth required         pam_dial_auth.so.1
ppp     auth binding          pam_unix_auth.so.1 server_policy
ppp     auth required         pam_ldap.so.1
#
# Default definitions for Authentication management
# Used when service name is not explicitly mentioned for authentication
#
other   auth requisite        pam_authtok_get.so.1
other   auth required         pam_dhkeys.so.1
other   auth required         pam_unix_cred.so.1
other   auth binding          pam_unix_auth.so.1 server_policy
other   auth required         pam_ldap.so.1
#
# passwd command (explicit because of a different authentication module)
#
passwd  auth binding          pam_passwd_auth.so.1 server_policy
passwd  auth required         pam_ldap.so.1
#
# cron service (explicit because of non-usage of pam_roles.so.1)
#
cron    account required      pam_unix_account.so.1
#
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
#
other   account requisite     pam_roles.so.1
other   account binding       pam_unix_account.so.1 server_policy
other   account required      pam_ldap.so.1
#
# Default definition for Session management
# Used when service name is not explicitly mentioned for session management
#
other   session required      pam_unix_session.so.1
#
```

```
# Default definition for  Password management
# Used when service name is not explicitly mentioned for password management
#
other   password required     pam_dhkeys.so.1
other   password requisite    pam_authtok_get.so.1
other   password requisite    pam_authtok_check.so.1
other   password required     pam_authtok_store.so.1 server_policy
#
# Support for Kerberos V5 authentication and example configurations can
# be found in the pam_krb5(5) man page under the "EXAMPLES" section.
#
```

LDAP에 대한 IETF 스키마

스키마는 서버 디렉토리에 항목으로 저장될 수 있는 정보 유형을 설명하는 정의입니다.

디렉토리 서버에서 LDAP 이름 지정 클라이언트를 지원하려면 클라이언트의 스키마 매핑 기능을 사용하여 스키마가 매핑되지 않은 경우 서버에서 이 장에 정의된 스키마를 구성해야 합니다.

RFC 2307 네트워크 정보 서비스 스키마 및 RFC 2307bis, LDAP(Lightweight Directory Access Protocol) 기반 에이전트에 대한 구성 프로파일 스키마(RFC 4876), 프린터 서비스에 대한 LDAP 스키마 등 여러 필수 LDAP 스키마가 IETF에 의해 정의되었습니다. NIS를 지원하려면 이러한 스키마의 정의를 디렉토리 서버에 추가해야 합니다. IETF 웹 사이트(`http://www.ietf.org`)에서 다양한 RFC에 액세스할 수 있습니다.

주 – RFC 2307bis 등의 인터넷 초안은 최대 6개월 동안 유효한 초안 문서이며, 언제든지 다른 문서에 의해 업데이트되거나 무효화될 수 있습니다.

RFC 2307bis 네트워크 정보 서비스 스키마

수정된 RFC 2307bis를 지원하려면 LDAP 서버를 구성해야 합니다.

`nisSchema` OID는 `1.3.6.1.1`입니다. RFC 2307bis 속성은 다음과 같습니다.

```
( nisSchema.1.0 NAME 'uidNumber'
DESC 'An integer uniquely identifying a user in an
        administrative domain'
EQUALITY integerMatch SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.1 NAME 'gidNumber'
DESC 'An integer uniquely identifying a group in an
        administrative domain'
EQUALITY integerMatch SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.2 NAME 'gecos'
DESC 'The GECOS field; the common name'
```

```
EQUALITY caseIgnoreIA5Match
SUBSTRINGS caseIgnoreIA5SubstringsMatch
SYNTAX 'IA5String' SINGLE-VALUE )

( nisSchema.1.3 NAME 'homeDirectory'
DESC 'The absolute path to the home directory'
EQUALITY caseExactIA5Match
SYNTAX 'IA5String' SINGLE-VALUE )

( nisSchema.1.4 NAME 'loginShell'
DESC 'The path to the login shell'
EQUALITY caseExactIA5Match
SYNTAX 'IA5String' SINGLE-VALUE )

( nisSchema.1.5 NAME 'shadowLastChange'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.6 NAME 'shadowMin'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.7 NAME 'shadowMax'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.8 NAME 'shadowWarning'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.9 NAME 'shadowInactive'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.10 NAME 'shadowExpire'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.11 NAME 'shadowFlag'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.12 NAME 'memberUid'
EQUALITY caseExactIA5Match
SUBSTRINGS caseExactIA5SubstringsMatch
SYNTAX 'IA5String' )

( nisSchema.1.13 NAME 'memberNisNetgroup'
EQUALITY caseExactIA5Match
SUBSTRINGS caseExactIA5SubstringsMatch
SYNTAX 'IA5String' )

( nisSchema.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
SYNTAX 'nisNetgroupTripleSyntax' )

( nisSchema.1.15 NAME 'ipServicePort'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )
```

```
( nisSchema.1.16 NAME 'ipServiceProtocol'
SUP name )

( nisSchema.1.17 NAME 'ipProtocolNumber'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.18 NAME 'oncRpcNumber'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE )

( nisSchema.1.19 NAME 'ipHostNumber'
DESC 'IP address as a dotted decimal, eg. 192.168.1.1
        omitting leading zeros'
SUP name )

( nisSchema.1.20 NAME 'ipNetworkNumber'
DESC 'IP network as a dotted decimal, eg. 192.168,
        omitting leading zeros'
SUP name SINGLE-VALUE )

( nisSchema.1.21 NAME 'ipNetmaskNumber'
DESC 'IP netmask as a dotted decimal, eg. 255.255.255.0,
         omitting leading zeros'
EQUALITY caseIgnoreIA5Match
SYNTAX 'IA5String{128}' SINGLE-VALUE )

( nisSchema.1.22 NAME 'macAddress'
DESC 'MAC address in maximal, colon separated hex
      notation, eg. 00:00:92:90:ee:e2'
EQUALITY caseIgnoreIA5Match
SYNTAX 'IA5String{128}' )

( nisSchema.1.23 NAME 'bootParameter'
DESC 'rpc.bootparamd parameter'
SYNTAX 'bootParameterSyntax' )

( nisSchema.1.24 NAME 'bootFile'
DESC 'Boot image name'
EQUALITY caseExactIA5Match
SYNTAX 'IA5String' )

( nisSchema.1.26 NAME 'nisMapName'
SUP name )

( nisSchema.1.27 NAME 'nisMapEntry'
EQUALITY caseExactIA5Match
SUBSTRINGS caseExactIA5SubstringsMatch
SYNTAX 'IA5String{1024}' SINGLE-VALUE )

( nisSchema.1.28 NAME 'nisPublicKey'
DESC 'NIS public key'
SYNTAX 'nisPublicKeySyntax' )

( nisSchema.1.29 NAME 'nisSecretKey'
DESC 'NIS secret key'
SYNTAX 'nisSecretKeySyntax' )
```

```
( nisSchema.1.30 NAME 'nisDomain'
DESC 'NIS domain'
SYNTAX 'IA5String' )

( nisSchema.1.31 NAME 'automountMapName'
DESC 'automount Map Name'
EQUALITY caseExactIA5Match
SUBSTR caseExactIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )

( nisSchema.1.32 NAME 'automountKey'
DESC 'Automount Key value'
EQUALITY caseExactIA5Match
SUBSTR caseExactIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )

( nisSchema.1.33 NAME 'automountInformation'
DESC 'Automount information'
EQUALITY caseExactIA5Match
SUBSTR caseExactIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

nisSchema OID는 1.3.6.1.1입니다. RFC 2307 objectClasses는 다음과 같습니다.

```
( nisSchema.2.0 NAME 'posixAccount' SUP top AUXILIARY
  DESC 'Abstraction of an account with POSIX attributes'
  MUST ( cn $ uid $ uidNumber $ gidNumber $ homeDirectory )
  MAY ( userPassword $ loginShell $ gecos $ description ) )

( nisSchema.2.1 NAME 'shadowAccount' SUP top AUXILIARY
  DESC 'Additional attributes for shadow passwords'
  MUST uid
  MAY ( userPassword $ shadowLastChange $ shadowMin
        shadowMax $ shadowWarning $ shadowInactive $
        shadowExpire $ shadowFlag $ description ) )

( nisSchema.2.2 NAME 'posixGroup' SUP top STRUCTURAL
  DESC 'Abstraction of a group of accounts'
  MUST ( cn $ gidNumber )
  MAY ( userPassword $ memberUid $ description ) )

( nisSchema.2.3 NAME 'ipService' SUP top STRUCTURAL
  DESC 'Abstraction an Internet Protocol service.
        Maps an IP port and protocol (such as tcp or udp)
        to one or more names; the distinguished value of
        the cn attribute denotes the service's canonical
        name'
  MUST ( cn $ ipServicePort $ ipServiceProtocol )
  MAY ( description ) )

( nisSchema.2.4 NAME 'ipProtocol' SUP top STRUCTURAL
  DESC 'Abstraction of an IP protocol. Maps a protocol number
        to one or more names. The distinguished value of the cn
        attribute denotes the protocol's canonical name'
  MUST ( cn $ ipProtocolNumber )
  MAY  description )

( nisSchema.2.5 NAME 'oncRpc' SUP top STRUCTURAL
```

```
  DESC 'Abstraction of an Open Network Computing (ONC)
        [RFC1057] Remote Procedure Call (RPC) binding.
        This class maps an ONC RPC number to a name.
        The distinguished value of the cn attribute denotes
        the RPC service's canonical name'
  MUST ( cn $ oncRpcNumber $ description )
  MAY  description )

( nisSchema.2.6 NAME 'ipHost' SUP top AUXILIARY
  DESC 'Abstraction of a host, an IP device. The distinguished
        value of the cn attribute denotes the host's canonical
        name. Device SHOULD be used as a structural class'
  MUST ( cn $ ipHostNumber )
  MAY ( l $ description $ manager $ userPassword ) )

( nisSchema.2.7 NAME 'ipNetwork' SUP top STRUCTURAL
  DESC 'Abstraction of a network. The distinguished value of
        the cn attribute denotes the network's canonical name'
  MUST ipNetworkNumber
  MAY ( cn $ ipNetmaskNumber $ l $ description $ manager ) )

( nisSchema.2.8 NAME 'nisNetgroup' SUP top STRUCTURAL
  DESC 'Abstraction of a netgroup. May refer to other netgroups'
  MUST cn
  MAY ( nisNetgroupTriple $ memberNisNetgroup $ description ) )

( nisSchema.2.9 NAME 'nisMap' SUP top STRUCTURAL
  DESC 'A generic abstraction of a NIS map'
  MUST nisMapName
  MAY description )

( nisSchema.2.10 NAME 'nisObject' SUP top STRUCTURAL
  DESC 'An entry in a NIS map'
  MUST ( cn $ nisMapEntry $ nisMapName )
  MAY description )

( nisSchema.2.11 NAME 'ieee802Device' SUP top AUXILIARY
  DESC 'A device with a MAC address; device SHOULD be
        used as a structural class'
  MAY macAddress )

( nisSchema.2.12 NAME 'bootableDevice' SUP top AUXILIARY
  DESC 'A device with boot parameters; device SHOULD be
  used as a structural class'
  MAY ( bootFile $ bootParameter ) )

( nisSchema.2.14 NAME 'nisKeyObject' SUP top AUXILIARY
  DESC 'An object with a public and secret key'
  MUST ( cn $ nisPublicKey $ nisSecretKey )
  MAY ( uidNumber $ description ) )

( nisSchema.2.15 NAME 'nisDomainObject' SUP top AUXILIARY
  DESC 'Associates a NIS domain with a naming context'
  MUST nisDomain )

( nisSchema.2.16 NAME 'automountMap' SUP top STRUCTURAL
  MUST ( automountMapName )
  MAY description )
```

```
( nisSchema.2.17 NAME 'automount' SUP top STRUCTURAL
  DESC 'Automount information'
  MUST ( automountKey $ automountInformation )
  MAY description )

( nisSchema.2.18 NAME 'groupOfMembers' SUP top STRUCTURAL
  DESC 'A group with members (DNs)'
  MUST cn
  MAY ( businessCategory $ seeAlso $ owner $ ou $ o $
        description $ member ) )
```

메일 별칭 스키마

메일 별칭 정보는 이 인터넷 초안에 정의된 스키마를 사용합니다. 새 스키마를 사용할 수 있을 때까지 LDAP 클라이언트는 계속해서 메일 별칭 정보에 이 스키마를 사용합니다.

원래 LDAP 메일 그룹 스키마에는 많은 속성과 객체 클래스가 포함되어 있습니다. LDAP 클라이언트는 속성 2개와 단일 객체 클래스만 사용합니다. 이러한 항목은 아래에 나열되어 있습니다.

메일 별칭 속성은 다음과 같습니다.

```
( 0.9.2342.19200300.100.1.3
  NAME 'mail'
  DESC 'RFC822 email address for this person'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String(256)'
  SINGLE-VALUE )

( 2.16.840.1.113730.3.1.30
  NAME 'mgrpRFC822MailMember'
  DESC 'RFC822 mail address of email only member of group'
  EQUALITY CaseIgnoreIA5Match
  SYNTAX 'IA5String(256)' )
```

`mailGroup` 객체 클래스에 대한 스키마는 다음과 같습니다.

```
( 2.16.840.1.113730.3.2.4
  NAME 'mailGroup'
  SUP top
  STRUCTURAL
  MUST mail
  MAY ( cn $ mailAlternateAddress $ mailHost $ mailRequireAuth $
   mgrpAddHeader $ mgrpAllowedBroadcaster $ mgrpAllowedDomain $
   mgrpApprovePassword $ mgrpBroadcasterModeration $ mgrpDeliverTo $
   mgrpErrorsTo $ mgrpModerator $ mgrpMsgMaxSize $
   mgrpMsgRejectAction $ mgrpMsgRejectText $ mgrpNoMatchAddrs $
   mgrpRemoveHeader $ mgrpRFC822MailMember ))
```

디렉토리 사용자 에이전트 프로파일(DUAProfile) 스키마

DUAConfSchemaOID는 1.3.6.1.4.1.11.1.3.1입니다.

```
DESC 'Default LDAP server host address used by a DUA'
            EQUALITY caseIgnoreMatch
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
            SINGLE-VALUE )

          ( DUAConfSchemaOID.1.0 NAME 'defaultServerList'
            DESC 'Default LDAP server host address used by a DUAList'
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
            SINGLE-VALUE )

          ( DUAConfSchemaOID.1.1 NAME 'defaultSearchBase'
            DESC 'Default LDAP base DN used by a DUA'
            EQUALITY distinguishedNameMatch
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
            SINGLE-VALUE )

          ( DUAConfSchemaOID.1.2 NAME 'preferredServerList'
            DESC 'Preferred LDAP server host addresses to be used by a
            DUA'
            EQUALITY caseIgnoreMatch
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
            SINGLE-VALUE )

          ( DUAConfSchemaOID.1.3 NAME 'searchTimeLimit'
            DESC 'Maximum time in seconds a DUA should allow for a
            search to complete'
            EQUALITY integerMatch
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
            SINGLE-VALUE )

          ( DUAConfSchemaOID.1.4 NAME 'bindTimeLimit'
            DESC 'Maximum time in seconds a DUA should allow for the
            bind operation to complete'
            EQUALITY integerMatch
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
            SINGLE-VALUE )

          ( DUAConfSchemaOID.1.5 NAME 'followReferrals'
            DESC 'Tells DUA if it should follow referrals
            returned by a DSA search result'
            EQUALITY caseIgnoreIA5Match
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
            SINGLE-VALUE )

          ( DUAConfSchemaOID.1.6 NAME 'authenticationMethod'
            DESC 'A keystring which identifies the type of
            authentication method used to contact the DSA'
            EQUALITY caseIgnoreMatch
            SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
            SINGLE-VALUE )

          ( DUAConfSchemaOID.1.7 NAME 'profileTTL'
            DESC 'Time to live before a client DUA
```

```
  should re-read this configuration profile'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
  SINGLE-VALUE )

( DUAConfSchemaOID.1.9 NAME 'attributeMap'
  DESC 'Attribute mappings used by a DUA'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

( DUAConfSchemaOID.1.10 NAME 'credentialLevel'
  DESC 'Identifies type of credentials a DUA should
  use when binding to the LDAP server'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
  SINGLE-VALUE )

( DUAConfSchemaOID.1.11 NAME 'objectclassMap'
  DESC 'Objectclass mappings used by a DUA'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

( DUAConfSchemaOID.1.12 NAME 'defaultSearchScope'
  DESC 'Default search scope used by a DUA'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE )

( DUAConfSchemaOID.1.13 NAME 'serviceCredentialLevel'
  DESC 'Identifies type of credentials a DUA
  should use when binding to the LDAP server for a
  specific service'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

( DUAConfSchemaOID.1.14 NAME 'serviceSearchDescriptor'
  DESC 'LDAP search descriptor list used by Naming-DUA'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

( DUAConfSchemaOID.1.15 NAME 'serviceAuthenticationMethod'
  DESC 'Authentication Method used by a service of the DUA'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

    ( DUAConfSchemaOID.2.4 NAME 'DUAConfigProfile'
        SUP top STRUCTURAL
       DESC 'Abstraction of a base configuration for a DUA'
       MUST ( cn )
       MAY ( defaultServerList $ preferredServerList $
      defaultSearchBase $ defaultSearchScope $
      searchTimeLimit $ bindTimeLimit $
      credentialLevel $ authenticationMethod $
      followReferrals $ serviceSearchDescriptor $
      serviceCredentialLevel $ serviceAuthenticationMethod $
      objectclassMap $ attributeMap $
      profileTTL ) )
```

Oracle Solaris 스키마

Oracle Solaris 플랫폼에 필요한 스키마는 다음과 같습니다.

- 프로젝트 스키마
- 역할 기반 액세스 제어 및 실행 프로파일 스키마
- 프린터 스키마

프로젝트 스키마

/etc/project 파일은 프로젝트와 연관된 속성의 로컬 소스입니다. 자세한 내용은 user_attr(4) 매뉴얼 페이지를 참조하십시오.

프로젝트 속성은 다음과 같습니다.

```
( 1.3.6.1.4.1.42.2.27.5.1.1 NAME 'SolarisProjectID'
  DESC 'Unique ID for a Solaris Project entry'
  EQUALITY integerMatch
  SYNTAX INTEGER SINGLE )

( 1.3.6.1.4.1.42.2.27.5.1.2 NAME 'SolarisProjectName'
  DESC 'Name of a Solaris Project entry'
  EQUALITY caseExactIA5Match
  SYNTAX IA5String SINGLE )

( 1.3.6.1.4.1.42.2.27.5.1.3 NAME 'SolarisProjectAttr'
  DESC 'Attributes of a Solaris Project entry'
  EQUALITY caseExactIA5Match
  SYNTAX IA5String )

( 1.3.6.1.4.1.42.2.27.5.1.30 NAME 'memberGid'
  DESC 'Posix Group Name'
  EQUALITY caseExactIA5Match
  SYNTAX 'IA5String' )
```

프로젝트 objectClass는 다음과 같습니다.

```
( 1.3.6.1.4.1.42.2.27.5.2.1 NAME 'SolarisProject'
  SUP top STRUCTURAL
  MUST ( SolarisProjectID $ SolarisProjectName )
  MAY ( memberUid $ memberGid $ description $ SolarisProjectAttr ) )
```

역할 기반 액세스 제어 및 실행 프로파일 스키마

/etc/user_attr 파일은 사용자 및 역할과 연관된 확장 속성의 로컬 소스입니다. 자세한 내용은 user_attr(4) 매뉴얼 페이지를 참조하십시오.

역할 기반 액세스 제어 속성은 다음과 같습니다.

```
( 1.3.6.1.4.1.42.2.27.5.1.4 NAME 'SolarisAttrKeyValue'
  DESC 'Semi-colon separated key=value pairs of attributes'
  EQUALITY caseIgnoreIA5Match
  SUBSTRINGS caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.7 NAME 'SolarisAttrShortDesc'
  DESC 'Short description about an entry, used by GUIs'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.8 NAME 'SolarisAttrLongDesc'
  DESC 'Detail description about an entry'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.9 NAME 'SolarisKernelSecurityPolicy'
  DESC 'Solaris  kernel security policy'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.10 NAME 'SolarisProfileType'
  DESC 'Type of object defined in profile'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.11 NAME 'SolarisProfileId'
  DESC 'Identifier of object defined in profile'
  EQUALITY caseExactIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.12 NAME 'SolarisUserQualifier'
  DESC 'Per-user login attributes'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.13 NAME 'SolarisReserved1'
  DESC 'Reserved for future use'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.14 NAME 'SolarisReserved2'
  DESC 'Reserved for future use'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 'IA5String' SINGLE-VALUE )
```

역할 기반 액세스 제어 `objectClassses`는 다음과 같습니다.

```
( 1.3.6.1.4.1.42.2.27.5.2.3 NAME 'SolarisUserAttr' SUP top AUXILIARY
  DESC 'User attributes'
  MAY ( SolarisUserQualifier $ SolarisAttrReserved1 $ \
        SolarisAttrReserved2 $ SolarisAttrKeyValue ) )

( 1.3.6.1.4.1.42.2.27.5.2.4 NAME 'SolarisAuthAttr' SUP top STRUCTURAL
  DESC 'Authorizations data'
  MUST cn
  MAY ( SolarisAttrReserved1 $ SolarisAttrReserved2 $ \
        SolarisAttrShortDesc $ SolarisAttrLongDesc $ \
```

```
        SolarisAttrKeyValue ) )

( 1.3.6.1.4.1.42.2.27.5.2.5 NAME 'SolarisProfAttr' SUP top STRUCTURAL
  DESC 'Profiles data'
  MUST cn
  MAY ( SolarisAttrReserved1 $ SolarisAttrReserved2 $ \
        SolarisAttrLongDesc $ SolarisAttrKeyValue ) )

( 1.3.6.1.4.1.42.2.27.5.2.6 NAME 'SolarisExecAttr' SUP top AUXILIARY
  DESC 'Profiles execution attributes'
  MAY ( SolarisKernelSecurityPolicy $ SolarisProfileType $ \
        SolarisAttrReserved1 $ SolarisAttrReserved2 $ \
        SolarisProfileId $ SolarisAttrKeyValue ) )
```

LDAP에 대한 인터넷 인쇄 프로토콜 정보

다음 절에서는 인터넷 인쇄 프로토콜 및 프린터의 속성과 ObjectClasses에 대한 정보를 제공합니다.

인터넷 인쇄 프로토콜 속성

```
( 1.3.18.0.2.4.1140
NAME 'printer-uri'
DESC 'A URI supported by this printer.
This URI SHOULD be used as a relative distinguished name (RDN).
If printer-xri-supported is implemented, then this URI value
MUST be listed in a member value of printer-xri-supported.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )

( 1.3.18.0.2.4.1107
NAME 'printer-xri-supported'
DESC 'The unordered list of XRI (extended resource identifiers) supported
by this printer.
Each member of the list consists of a URI (uniform resource identifier)
followed by optional authentication and security metaparameters.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

( 1.3.18.0.2.4.1135
NAME 'printer-name'
DESC 'The site-specific administrative name of this printer, more end-user
friendly than a URI.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127}  SINGLE-VALUE )

( 1.3.18.0.2.4.1119
NAME 'printer-natural-language-configured'
```

```
DESC 'The configured language in which error and status messages will be
generated (by default) by this printer.
Also, a possible language for printer string attributes set by operator,
system administrator, or manufacturer.
Also, the (declared) language of the "printer-name", "printer-location",
"printer-info", and "printer-make-and-model" attributes of this printer.
For example: "en-us" (US English) or "fr-fr" (French in France) Legal values of
language tags conform to [RFC3066] "Tags for the Identification of Languages".'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127}  SINGLE-VALUE )

( 1.3.18.0.2.4.1136
NAME 'printer-location'
DESC 'Identifies the location of the printer. This could include
things like: "in Room 123A", "second floor of building XYZ".'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} SINGLE-VALUE )

( 1.3.18.0.2.4.1139
NAME 'printer-info'
DESC 'Identifies the descriptive information about this printer.
This could include things like: "This printer can be used for
printing color transparencies for HR presentations", or
"Out of courtesy for others, please print only small (1-5 page)
jobs at this printer", or even "This printer is going away on July 1, 1997,
please find a new printer".'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127}
SINGLE-VALUE )

( 1.3.18.0.2.4.1134
NAME 'printer-more-info'
DESC 'A URI used to obtain more information about this specific printer.
For example, this could be an HTTP type URI referencing an HTML page
accessible to a Web Browser.
The information obtained from this URI is intended for end user consumption.'
EQUALITY caseIgnoreMatch ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )

( 1.3.18.0.2.4.1138
NAME 'printer-make-and-model'
DESC 'Identifies the make and model of the device.
The device manufacturer MAY initially populate this attribute.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{127}  SINGLE-VALUE )

( 1.3.18.0.2.4.1133
NAME 'printer-ipp-versions-supported'
DESC 'Identifies the IPP protocol version(s) that this printer supports,
```

```
including major and minor versions,
i.e., the version numbers for which this Printer implementation meets
the conformance requirements.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1132
NAME 'printer-multiple-document-jobs-supported'
DESC 'Indicates whether or not the printer supports more than one
document per job, i.e., more than one Send-Document or Send-Data
operation with document data.'
EQUALITY booleanMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )

( 1.3.18.0.2.4.1109
NAME 'printer-charset-configured'
DESC 'The configured charset in which error and status messages will be
generated (by default) by this printer.
Also, a possible charset for printer string attributes set by operator,
system administrator, or manufacturer.
For example: "utf-8" (ISO 10646/Unicode) or "iso-8859-1" (Latin1).
Legal values are defined by the IANA Registry of Coded Character Sets and
the "(preferred MIME name)" SHALL be used as the tag.
For coherence with IPP Model, charset tags in this attribute SHALL be
lowercase normalized.
This attribute SHOULD be static (time of registration) and SHOULD NOT be
dynamically refreshed attributetypes: (subsequently).'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{63} SINGLE-VALUE )

( 1.3.18.0.2.4.1131
NAME 'printer-charset-supported'
DESC 'Identifies the set of charsets supported for attribute type values of
type Directory String for this directory entry.
For example: "utf-8" (ISO 10646/Unicode) or "iso-8859-1" (Latin1).
Legal values are defined by the IANA Registry of Coded Character Sets and
the preferred MIME name.'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{63} )

( 1.3.18.0.2.4.1137
NAME 'printer-generated-natural-language-supported'
DESC 'Identifies the natural language(s) supported for this directory entry.
For example: "en-us" (US English) or "fr-fr" (French in France).
Legal values conform to [RFC3066], Tags for the Identification of Languages.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{63} )

( 1.3.18.0.2.4.1130
NAME 'printer-document-format-supported'
DESC 'The possible document formats in which data may be interpreted
and printed by this printer.
Legal values are MIME types come from the IANA Registry of Internet Media Types.'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )
```

```
( 1.3.18.0.2.4.1129
NAME 'printer-color-supported'
DESC 'Indicates whether this printer is capable of any type of color printing
at all, including highlight color.'
EQUALITY booleanMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.7  SINGLE-VALUE )

( 1.3.18.0.2.4.1128
NAME 'printer-compression-supported'
DESC 'Compression algorithms supported by this printer.
For example: "deflate, gzip".  Legal values include; "none", "deflate"
attributetypes: (public domain ZIP), "gzip" (GNU ZIP), "compress" (UNIX).'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1127
NAME 'printer-pages-per-minute'
DESC 'The nominal number of pages per minute which may be output by this
printer (e.g., a simplex or black-and-white printer).
This attribute is informative, NOT a service guarantee.
Typically, it is the value used in marketing literature to describe this printer.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1126 NAME 'printer-pages-per-minute-color'
DESC 'The nominal number of color pages per minute which may be output by this
printer (e.g., a simplex or color printer).
This attribute is informative, NOT a service guarantee.
Typically, it is the value used in marketing literature to describe this printer.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1125 NAME 'printer-finishings-supported'
DESC 'The possible finishing operations supported by this printer.
Legal values include; "none", "staple", "punch", "cover", "bind", "saddle-stitch",
"edge-stitch", "staple-top-left", "staple-bottom-left", "staple-top-right",
"staple-bottom-right", "edge-stitch-left", "edge-stitch-top", "edge-stitch-right",
"edge-stitch-bottom", "staple-dual-left", "staple-dual-top", "staple-dual-right",
"staple-dual-bottom".'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1124 NAME 'printer-number-up-supported'
DESC 'The possible numbers of print-stream pages to impose upon a single side of
an instance of a selected medium. Legal values include; 1, 2, and 4.
Implementations may support other values.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27 )

( 1.3.18.0.2.4.1123 NAME 'printer-sides-supported'
DESC 'The number of impression sides (one or two) and the two-sided impression
rotations supported by this printer.
Legal values include; "one-sided", "two-sided-long-edge", "two-sided-short-edge".'
```

```
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1122 NAME 'printer-media-supported'
DESC 'The standard names/types/sizes (and optional color suffixes) of the media
supported by this printer.
For example: "iso-a4",  "envelope", or "na-letter-white".
Legal values  conform to ISO 10175, Document Printing Application (DPA), and any
IANA registered extensions.'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1117 NAME 'printer-media-local-supported'
DESC 'Site-specific names of media supported by this printer, in the language in
"printer-natural-language-configured".
For example: "purchasing-form" (site-specific name) as opposed to
(in "printer-media-supported"): "na-letter" (standard keyword from ISO 10175).'
EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1121 NAME 'printer-resolution-supported'
DESC 'List of resolutions supported for printing documents by this printer.
Each resolution value is a string with 3 fields:
1) Cross feed direction resolution (positive integer), 2) Feed direction
resolution (positive integer), 3) Resolution unit.
Legal values are "dpi" (dots per inch) and "dpcm" (dots per centimeter).
Each resolution field is delimited by ">".  For example:  "300> 300> dpi>".'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{255} )

( 1.3.18.0.2.4.1120 NAME 'printer-print-quality-supported'
DESC 'List of print qualities supported for printing documents on this printer.
For example: "draft, normal".  Legal values include; "unknown", "draft", "normal",
"high".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1110 NAME 'printer-job-priority-supported'
DESC 'Indicates the number of job priority levels supported.
An IPP conformant printer which supports job priority must always support a
full range of priorities from "1" to "100"
(to ensure consistent behavior), therefore this attribute describes the
"granularity".
 Legal values of this attribute are from "1" to "100".'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1118
NAME 'printer-copies-supported'
DESC 'The maximum number of copies of a document that may be printed as a single job.
A value of "0" indicates no maximum limit.
A value of "-1" indicates unknown.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )
```

```
( 1.3.18.0.2.4.1111
NAME 'printer-job-k-octets-supported'
DESC 'The maximum size in kilobytes (1,024 octets actually) incoming print job that
this printer will accept.
A value of "0" indicates no maximum limit.  A value of "-1" indicates unknown.'
EQUALITY integerMatch
ORDERING integerOrderingMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.27  SINGLE-VALUE )

( 1.3.18.0.2.4.1113
NAME 'printer-service-person'
DESC 'The name of the current human service person responsible for servicing this
printer.
It is suggested that this string include information that would enable other humans
to reach the service person, such as a phone number.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127}
SINGLE-VALUE )

( 1.3.18.0.2.4.1114
NAME 'printer-delivery-orientation-supported'
DESC 'The possible delivery orientations of pages as they are printed and ejected
from this printer.
Legal values include; "unknown", "face-up", and "face-down".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1115
NAME 'printer-stacking-order-supported'
DESC 'The possible stacking order of pages as they are printed and ejected from
this printer.
Legal values include; "unknown", "first-to-last", "last-to-first".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1116
NAME 'printer-output-features-supported'
DESC 'The possible output features supported by this printer.
Legal values include; "unknown", "bursting", "decollating", "page-collating",
"offset-stacking".'
EQUALITY caseIgnoreMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.18.0.2.4.1108
NAME 'printer-aliases'
DESC 'Site-specific administrative names of this printer in addition the printer
name specified for printer-name.'
EQUALITY caseIgnoreMatch
ORDERING caseIgnoreOrderingMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15{127} )

( 1.3.6.1.4.1.42.2.27.5.1.63
NAME 'sun-printer-bsdaddr'
DESC 'Sets the server, print queue destination name and whether the client generates
protocol extensions.
```

```
"Solaris" specifies a Solaris print server extension. The value is represented b the
following value: server "," destination ", Solaris".'
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.5.1.64
NAME 'sun-printer-kvp'
DESC 'This attribute contains a set of key value pairs which may have meaning to the
print subsystem or may be user defined.
Each value is represented by the following: key "=" value.'
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

인터넷 인쇄 프로토콜 ObjectClasses

```
objectclasses: ( 1.3.18.0.2.6.2549
NAME 'slpService'
DESC 'DUMMY definition'
SUP 'top' MUST (objectclass) MAY ())

objectclasses: ( 1.3.18.0.2.6.254
NAME 'slpServicePrinter'
DESC 'Service Location Protocol (SLP) information.'
AUXILIARY SUP 'slpService')

objectclasses: ( 1.3.18.0.2.6.258
NAME 'printerAbstract'
DESC 'Printer related information.'
ABSTRACT SUP 'top' MAY ( printer-name
$ printer-natural-language-configured
$ printer-location
$ printer-info
$ printer-more-info
$ printer-make-and-model
$ printer-multiple-document-jobs-supported
$ printer-charset-configured
$ printer-charset-supported
$ printer-generated-natural-language-supported
$ printer-document-format-supported
$ printer-color-supported
$ printer-compression-supported
$ printer-pages-per-minute
$ printer-pages-per-minute-color
$ printer-finishings-supported
$ printer-number-up-supported
$ printer-sides-supported
$ printer-media-supported
$ printer-media-local-supported
$ printer-resolution-supported
$ printer-print-quality-supported
$ printer-job-priority-supported
$ printer-copies-supported
$ printer-job-k-octets-supported
$ printer-current-operator
$ printer-service-person
$ printer-delivery-orientation-supported
$ printer-stacking-order-supported $ printer! -output-features-supported ))
```

```
objectclasses: ( 1.3.18.0.2.6.255
NAME 'printerService'
DESC 'Printer information.'
STRUCTURAL SUP 'printerAbstract' MAY ( printer-uri
$ printer-xri-supported ))

objectclasses: ( 1.3.18.0.2.6.257
NAME 'printerServiceAuxClass'
DESC 'Printer information.'
AUXILIARY SUP 'printerAbstract' MAY ( printer-uri $ printer-xri-supported ))

objectclasses: ( 1.3.18.0.2.6.256
NAME 'printerIPP'
DESC 'Internet Printing Protocol (IPP) information.'
AUXILIARY SUP 'top' MAY   ( printer-ipp-versions-supported $
printer-multiple-document-jobs-supported ))

objectclasses: ( 1.3.18.0.2.6.253
NAME 'printerLPR'
DESC 'LPR information.'
AUXILIARY SUP 'top' MUST ( printer-name ) MAY ( printer-aliases))

objectclasses: ( 1.3.6.1.4.1.42.2.27.5.2.14
NAME 'sunPrinter'
DESC 'Sun printer information'
SUP 'top' AUXILIARY MUST (objectclass $ printer-name)  MAY
(sun-printer-bsdaddr $ sun-printer-kvp))
```

프린터 속성

```
ATTRIBUTE ( 1.3.6.1.4.1.42.2.27.5.1.63
NAME sun-printer-bsdaddr
DESC 'Sets the server, print queue destination name and whether the
     client generates protocol extensions. "Solaris" specifies a
     Solaris print server extension.  The value is represented by
     the following value: server "," destination ", Solaris".'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE
)


ATTRIBUTE ( 1.3.6.1.4.1.42.2.27.5.1.64
NAME sun-printer-kvp
DESC 'This attribute contains a set of key value pairs which may have
      meaning to the print subsystem or may be user defined.  Each
      value is represented by the following: key "=" value.'
EQUALITY caseIgnoreIA5Match
SYNTAX  1.3.6.1.4.1.1466.115.121.1.15  )
```

Sun 프린터 ObjectClasses

```
OBJECTCLASS ( 1.3.6.1.4.1.42.2.27.5.2.14
NAME sunPrinter
DESC 'Sun printer information'
SUP  top
AUXILIARY
MUST ( printer-name )
MAY  ( sun-printer-bsdaddr $ sun-printer-kvp ))
```

LDAP에 대한 일반 디렉토리 서버 요구 사항

LDAP 클라이언트를 지원하려면 모든 서버가 LDAP v3 프로토콜과 복합 이름 지정 및 보조 객체 클래스를 지원해야 합니다. 또한 다음 컨트롤 중 하나 이상을 지원해야 합니다.

- Simple 페이징 모드(RFC 2696)
- 가상 목록 보기 컨트롤

서버는 다음 인증 방법 중 하나 이상을 지원해야 합니다.

```
anonymous
simple
sasl/cram-MD5
sasl/digest-MD5
sasl/GSSAPI
```

LDAP 클라이언트가 `pam_unix_*` 모듈을 사용 중인 경우 서버가 암호를 UNIX crypt 형식으로 저장하는 기능을 지원해야 합니다.

LDAP 클라이언트가 TLS를 사용 중인 경우 서버가 SSL 또는 TLS를 지원해야 합니다.

LDAP 클라이언트가 `sasl/GSSAPI`를 사용 중인 경우 서버가 SASL, GSSAPI, Kerberos 5 인증을 지원해야 합니다. 전송 시 GSS 암호화에 대한 지원은 선택 사항입니다.

LDAP 이름 지정 서비스에 사용되는 기본 필터

SSD를 사용하여 특정 서비스에 대한 매개변수를 수동으로 지정하지 않으면 기본 필터가 사용됩니다. 특정 서비스에 대한 기본 필터를 나열하려면 `ldaplist`에 `-v` 옵션을 사용합니다.

다음 예에서 `filter=(&(objectclass=iphost)(cn=abcde)`는 기본 필터를 정의합니다.

```
database=hosts
filter=(&(objectclass=iphost)(cn=abcde)
user data=(&(%s) (cn=abcde))
```

ldaplist는 다음과 같은 기본 필터 목록을 생성합니다. 여기서 %s는 문자열을 나타내고 %d는 숫자를 나타냅니다.

```
hosts
(&(objectclass=iphost)(cn=%s))
--------------
passwd
(&(objectclass=posixaccount)(uid=%s))
--------------
services
(&(objectclass=ipservice)(cn=%s))
--------------
group
(&(objectclass=posixgroup)(cn=%s))
--------------
netgroup
(&(objectclass=nisnetgroup)(cn=%s))
--------------
networks
(&(objectclass=ipnetwork)(ipnetworknumber=%s))
--------------
netmasks
(&(objectclass=ipnetwork)(ipnetworknumber=%s))
--------------
rpc
(&(objectclass=oncrpc)(cn=%s))
--------------
protocols
(&(objectclass=ipprotocol)(cn=%s))
--------------
bootparams
(&(objectclass=bootableDevice)(cn=%s))
--------------
ethers
(&(objectclass=ieee802Device)(cn=%s))
--------------
publickey
(&(objectclass=niskeyobject)(cn=%s))
or
(&(objectclass=niskeyobject)(uidnumber=%d))
--------------
aliases
(&(objectclass=mailGroup)(cn=%s))
--------------
```

표 14–4 getXbyY 호출에서 사용되는 LDAP 필터

필터	정의
bootparamByName	(&(objectClass=bootableDevice)(cn=%s))
etherByHost	(&(objectClass=ieee802Device)(cn=%s))
etherByEther	(&(objectClass=ieee802Device)(macAddress=%s))
groupByName	(&(objectClass=posixGroup)(cn=%s))

표 14–4 getXbyY 호출에서 사용되는 LDAP 필터 *(계속)*

필터	정의
groupByGID	(&(objectClass=posixGroup)(gidNumber=%ld))
groupByMember	(&(objectClass=posixGroup)(memberUid=%s))
hostsByName	(&(objectClass=ipHost)(cn=%s))
hostsByAddr	(&(objectClass=ipHost)(ipHostNumber=%s))
keyByUID	(&(objectClass=nisKeyObject)(uidNumber=%s))
keyByHost	(&(objectClass=nisKeyObject)(cn=%s))
netByName	(&(objectClass=ipNetwork)(cn=%s))
netByAddr	(&(objectClass=ipNetwork)(ipNetworkNumber=%s))
nisgroupMember	(membernisnetgroup=%s)
maskByNet	(&(objectClass=ipNetwork)(ipNetworkNumber=%s))
printerByName	(&(objectClass=sunPrinter)(|(printer-name=%s) (printer-aliases=%s)))
projectByName	(&(objectClass=SolarisProject)(SolarisProjectName=%s))
projectByID	(&(objectClass=SolarisProject)(SolarisProjectID=%ld))
protoByName	(&(objectClass=ipProtocol)(cn=%s))
protoByNumber	(&(objectClass=ipProtocol)(ipProtocolNumber=%d))
passwordByName	(&(objectClass=posixAccount)(uid=%s))
passwordByNumber	(&(objectClass=posixAccount)(uidNumber=%ld))
rpcByName	(&(objectClass=oncRpc)(cn=%s))
rpcByNumber	(&(objectClass=oncRpc)(oncRpcNumber=%d))
serverByName	(&(objectClass=ipService)(cn=%s))
serverByPort	(&(objectClass=ipService)(ipServicePort=%ld))
serverByNameAndProto	(&(objectClass=ipService)(cn=%s)(ipServiceProtocol=%s))
specialByNameserver	(ipServiceProtocol=%s))
ByPortAndProto	(&(objectClass=shadowAccount)(uid=%s))
netgroupByTriple	(&(objectClass=nisNetGroup)(cn=%s))
netgroupByMember	(&(objectClass=nisNetGroup)(cn=%s))
authName	(&(objectClass=SolarisAuthAttr)(cn=%s))

표 14–4 getXbyY 호출에서 사용되는 LDAP 필터 *(계속)*

필터	정의
auditUserByName	(&(objectClass=SolarisAuditUser)(uid=%s))
execByName	(&(objectClass=SolarisExecAttr)(cn=%s) (SolarisKernelSecurityPolicy=%s)(SolarisProfileType=%s))
execByPolicy	(&(objectClass=SolarisExecAttr)(SolarisProfileId=%s) (SolarisKernelSecurityPolicy=%s)(SolarisProfileType=%s))
profileByName	(&(objectClass=SolarisProfAttr)(cn=%s))
userByName	(&(objectClass=SolarisUserAttr)(uid=%s))

다음 표에서는 getent 속성 필터를 나열합니다.

표 14–5 getent 속성 필터

필터	정의
aliases	(objectClass=rfc822MailGroup)
auth_attr	(objectClass=SolarisAuthAttr)
audit_user	(objectClass=SolarisAuditUser)
exec_attr	(objectClass=SolarisExecAttr)
group	(objectClass=posixGroup)
hosts	(objectClass=ipHost)
networks	(objectClass=ipNetwork)
prof_attr	(objectClass=SolarisProfAttr)
protocols	(objectClass=ipProtocol)
passwd	(objectClass=posixAccount)
printers	(objectClass=sunPrinter)
rpc	(objectClass=oncRpc)
services	(objectClass=ipService)
shadow	(objectclass=shadowAccount)
project	(objectClass=SolarisProject)
usr_attr	(objectClass=SolarisUserAttr)

◆ ◆ ◆ 15장

15 NIS에서 LDAP으로 전환(작업)

이 장에서는 LDAP 디렉토리에 저장된 이름 지정 정보를 사용하는 NIS 클라이언트를 지원하도록 설정하는 방법에 대해 설명합니다. 이 장의 절차를 따르면 NIS 이름 지정 서비스 사용에서 LDAP 이름 지정 서비스 사용으로 전환할 수 있습니다.

LDAP으로 전환할 경우의 이점을 확인하려면 118 페이지 “LDAP 이름 지정 서비스와 다른 이름 지정 서비스 비교”를 참조하십시오.

이 장의 내용은 다음과 같습니다.

NIS-to-LDAP 서비스 개요

NIS-to-LDAP 전환 서비스(*N2L* **서비스**)는 NIS 마스터 서버의 기존 NIS 데몬을 NIS-to-LDAP 전환 데몬으로 대체합니다. N2L 서비스는 해당 서버에 NIS-to-LDAP 매핑 파일도 만듭니다. 매핑 파일에서는 NIS 맵 항목과 LDAP에 있는 그에 상응하는 DIT(디렉토리 정보 트리) 항목 간의 매핑을 지정합니다. 이 전환을 완료한 NIS 마스터 서버를 *N2L* **서버**라고 합니다. 슬레이브 서버에는 `NISLDAPmapping` 파일이 없으므로 계속 평상시처럼 작동합니다. 슬레이브 서버는 정규 NIS 마스터인 것처럼 N2L 서버에서 주기적으로 데이터를 업데이트합니다.

N2L 서비스의 동작은 ypserv 및 NISLDAPmapping 구성 파일로 제어됩니다. 스크립트인 inityp2l은 이러한 구성 파일의 초기 설정을 지원합니다. N2L 서버가 설정된 후에는 구성 파일을 직접 편집하여 N2L을 유지 관리할 수 있습니다.

N2L 서비스는 다음을 지원합니다.

- LDAP DIT(디렉토리 정보 트리)로 NIS 맵 가져오기
- NIS의 속도와 확장성으로 DIT 정보에 대한 클라이언트 액세스

모든 이름 지정 시스템에서는 정보 소스 1개만 권한 있는 소스가 될 수 있습니다. 기존 NIS에서는 NIS 소스가 권한 있는 정보입니다. N2L 서비스를 사용하는 경우 권한 있는 데이터 소스는 LDAP 디렉토리입니다. 9 장, "LDAP 이름 지정 서비스 소개(개요)"에 설명된 대로 디렉토리는 디렉토리 관리 도구를 통해 관리됩니다.

NIS 소스는 비상 백업이나 백아웃 전용으로 유지됩니다. N2L 서비스를 사용한 후에는 NIS 클라이언트를 단계적으로 제거해야 합니다. 최종적으로 모든 NIS 클라이언트가 LDAP 이름 지정 서비스 클라이언트로 대체되어야 합니다.

다음 하위 절에서는 추가 개요 정보를 제공합니다.

- 216 페이지 "NIS-to-LDAP 대상 가정"
- 217 페이지 "NIS-to-LDAP 서비스를 사용하지 않는 경우"
- 217 페이지 "NIS-to-LDAP 서비스가 사용자에게 미치는 영향"
- 218 페이지 "NIS-to-LDAP 전환 용어"
- 219 페이지 "NIS-to-LDAP 명령, 파일 및 맵"
- 219 페이지 "지원되는 표준 매핑"

NIS-to-LDAP 도구 및 서비스 관리 기능

NIS 및 LDAP 서비스는 서비스 관리 기능을 통해 관리됩니다. svcadm 명령을 사용하여 사용으로 설정, 사용 안함으로 설정, 다시 시작 등 이러한 서비스에 대한 관리 작업을 수행할 수 있습니다. svcs 명령을 사용하여 서비스 상태를 질의할 수 있습니다. LDAP 및 NIS와 함께 SMF를 사용하는 방법에 대한 자세한 내용은 170 페이지 "LDAP 및 서비스 관리 기능" 및 72 페이지 "NIS 및 서비스 관리 기능"을 참조하십시오. SMF 개요는 **Oracle Solaris 11.1에서 서비스 및 결함 관리**의 1 장, "서비스 관리(개요)"를 참조하십시오. 자세한 내용은 svcadm(1M) 및 svcs(1) 매뉴얼 페이지를 참조하십시오.

NIS-to-LDAP 대상 가정

이 장의 절차를 수행하려면 NIS 및 LDAP 개념, 용어, ID 등을 잘 알고 있어야 합니다. NIS 및 LDAP 이름 지정 서비스에 대한 자세한 내용은 본 설명서의 다음 절을 참조하십시오.

- 5 장, "네트워크 정보 서비스(개요)" - NIS 개요
- 9 장, "LDAP 이름 지정 서비스 소개(개요)" - LDAP 개요

NIS-to-LDAP 서비스를 사용하지 않는 경우

N2L 서비스는 NIS 사용에서 LDAP 사용으로의 전환 도구 역할을 수행하는 데 사용됩니다. 다음과 같은 경우에는 N2L 서비스를 사용하지 마십시오.

- NIS 및 LDAP 이름 지정 서비스 클라이언트 간에 데이터를 공유할 계획이 없는 환경

  이러한 환경의 N2L 서버는 지나치게 복잡한 NIS 마스터 서버 역할을 수행하게 됩니다.
- NIS 맵이 NIS 소스 파일을 수정하는 도구(`yppasswd` 제외)로 관리되는 환경

  DIT 맵에서 NIS 소스를 재생성하는 작업은 부정확한 작업이므로 결과 맵을 수동으로 검사해야 합니다. N2L 서비스를 사용한 후에는 백아웃 또는 NIS로 되돌리는 경우에만 NIS 소스 재생성 기능이 제공됩니다.
- NIS 클라이언트가 없는 환경

  이러한 환경에서는 LDAP 이름 지정 서비스 클라이언트와 해당 도구를 사용합니다.

NIS-to-LDAP 서비스가 사용자에게 미치는 영향

N2L 서비스와 관련된 파일을 설치만 하는 경우 NIS 서버의 기본 동작이 변경되지 않습니다. 설치 시 서버에서 NIS 매뉴얼 페이지가 일부 변경된 것과 N2L 도우미 스크립트 `inityp2l` 및 `ypmap2src`가 추가된 것이 관리자에게 표시됩니다. 그러나 NIS 서버에서 `inityp2l`을 실행하지 않았거나 N2L 구성 파일을 수동으로 만들지 않은 경우 NIS 구성 요소는 계속해서 기존 NIS 모드에서 시작되고 평상시처럼 작동합니다.

`inityp2l`을 실행한 후에는 서버 및 클라이언트 동작이 일부 변경된 것이 사용자에게 표시됩니다. 다음은 NIS 및 LDAP 사용자 유형 목록과 N2L 서비스가 배포된 후 각 사용자 유형에 표시되는 사항에 대한 설명입니다.

사용자 유형	N2L 서비스의 영향
NIS 마스터 서버 관리자	NIS 마스터 서버가 N2L 서버로 변환됩니다. `NISLDAPmapping` 및 `ypserv` 구성 파일이 N2L 서버에 설치됩니다. N2L 서버가 설정된 후에는 LDAP 명령을 사용하여 이름 지정 정보를 관리할 수 있습니다.
NIS 슬레이브 서버 관리자	N2L 전환 후에도 NIS 슬레이브 서버는 계속 NIS를 평상시처럼 실행합니다. `yppush`가 `ypmake`에 의해 호출되면 N2L 서버가 업데이트된 NIS 맵을 슬레이브 서버로 푸시합니다. `ypmake(1M)` 매뉴얼 페이지를 참조하십시오.

사용자 유형	N2L 서비스의 영향
NIS 클라이언트	NIS 읽기 작업은 기존 NIS와 다르지 않습니다. LDAP 이름 지정 서비스 클라이언트가 DIT의 정보를 변경하면 해당 정보가 NIS 맵에 복사됩니다. 구성 가능한 시간 제한이 만료되면 복사 작업이 완료됩니다. 이러한 동작은 클라이언트가 NIS 슬레이브 서버에 연결된 경우의 일반 NIS 클라이언트 동작과 유사합니다. N2L 서버가 읽기를 위해 LDAP 서버에 바인딩할 수 없는 경우 N2L 서버에서 캐시된 복사본의 정보를 반환합니다. 또는 N2L 서버에서 내부 서버 오류를 반환할 수 있습니다. 두 방법 중 하나로 응답하도록 N2L 서버를 구성할 수 있습니다. 자세한 내용은 ypserv(1M) 매뉴얼 페이지를 참조하십시오.
모든 사용자	NIS 클라이언트가 암호 변경 요청을 적용하면 변경 사항이 N2L 마스터 서버와 고유 LDAP 클라이언트에 즉시 표시됩니다. NIS 클라이언트에서 암호를 변경하려고 했는데 LDAP 서버를 사용할 수 없으면 변경 사항이 거부되고 N2L 서버에서 내부 서버 오류를 반환합니다. 이 동작은 잘못된 정보가 캐시에 기록되지 않도록 방지합니다.

NIS-to-LDAP 전환 용어

다음 용어는 N2L 서비스 구현과 관련이 있습니다.

표 15–1 N2L 전환과 관련된 용어

용어	설명
N2L 구성 파일	ypserv 데몬이 마스터 서버를 N2L 모드로 시작하는 데 사용하는 /var/yp/NISLDAPmapping 및 /var/yp/ypserv 파일입니다. 자세한 내용은 NISLDAPmapping(4) 및 ypserv(4) 매뉴얼 페이지를 참조하십시오.
맵	N2L 서비스 컨텍스트에서 맵 용어는 다음 두 가지 방법으로 사용됩니다. ■ NIS에서 특정 유형의 정보를 저장하는 데이터베이스 파일을 나타냅니다. ■ NIS 정보를 LDAP DIT와 매핑하는 프로세스에 대해 설명합니다.
매핑	NIS 항목을 LDAP DIT 항목으로 변환하거나 그 반대로 변환하는 프로세스입니다.
매핑 파일	NIS 및 LDAP 파일 간에 항목을 매핑하는 방법을 설정하는 NISLDAPmapping 파일입니다.
표준 맵	매핑 파일에 대한 수동 수정을 요구하지 않고 N2L 서비스에서 지원되는, 자주 사용하는 NIS 맵입니다. 지원되는 표준 맵 목록은 219 페이지 “지원되는 표준 매핑”을 참조하십시오.
비표준 맵	NIS 및 LDAP DIT 간에 RFC 2307 또는 이후 버전에서 식별된 매핑 이외의 매핑을 사용하기 위해 사용자 정의된 표준 NIS 맵입니다.
사용자 정의 맵	표준 맵이 아니므로 NIS에서 LDAP으로 전환할 때 매핑 파일을 수동으로 수정해야 하는 맵입니다.
LDAP 클라이언트	LDAP 서버를 읽고 쓰는 기존 LDAP 클라이언트입니다. 기존 LDAP 클라이언트는 LDAP 서버를 읽고 쓰는 시스템입니다. LDAP 이름 지정 서비스 클라이언트는 이름 지정 정보의 사용자 정의 하위 세트를 처리합니다.

표 15–1 N2L 전환과 관련된 용어 (계속)

용어	설명
LDAP 이름 지정 서비스 클라이언트	이름 지정 정보의 사용자 정의 하위 세트를 처리하는 LDAP 클라이언트입니다.
N2L 서버	N2L 서비스를 사용하여 N2L 서버로 재구성된 NIS 마스터 서버입니다. 재구성에는 NIS 데몬 대체, 새 구성 파일 추가 등이 포함됩니다.

NIS-to-LDAP 명령, 파일 및 맵

N2L 전환과 연관된 유틸리티 2개, 구성 파일 2개 및 매핑이 있습니다.

표 15–2 N2L 명령, 파일 및 맵에 대한 설명

명령/파일/맵	설명
/usr/lib/netsvc/yp/inityp2l	NISLDAPmapping 및 ypserv 구성 파일 생성을 지원하는 유틸리티입니다. 이 유틸리티는 이러한 파일의 관리에 사용되는 범용 도구가 아닙니다. 고급 사용자는 N2L 구성 파일을 유지 관리하거나, 텍스트 편집기로 사용자 정의 매핑을 만들어 inityp2l 출력을 검사하고 사용자 정의할 수 있습니다. inityp2l(1M) 매뉴얼 페이지를 참조하십시오.
/usr/lib/netsvc/yp/ypmap2src	표준 NIS 맵을 이에 상응하는 NIS 소스 파일의 근사값으로 변환하는 유틸리티입니다. ypmap2src는 주로 N2L 전환 서버에서 기존 NIS로 변환하는 데 사용됩니다. ypmap2src(1M) 매뉴얼 페이지를 참조하십시오.
/var/yp/NISLDAPmapping	NIS 맵 항목과 LDAP에 있는 이에 상응하는 DIT(디렉토리 정보 트리) 항목 간의 매핑을 지정하는 구성 파일입니다. NISLDAPmapping(4) 매뉴얼 페이지를 참조하십시오.
/var/yp/ypserv	NIS-to-LDAP 전환 데몬에 대한 구성 정보를 지정하는 파일입니다. ypserv(4) 매뉴얼 페이지를 참조하십시오.
ageing.byname	NIS-to-LDAP 전환이 구현된 경우 yppasswdd에서 암호 에이징 정보를 읽고 DIT에 쓰는 데 사용하는 매핑입니다.

지원되는 표준 매핑

기본적으로 N2L 서비스는 다음 맵 목록과 RFC 2307, RFC 2307bis 및 이후 버전의 LDAP 항목 간 매핑을 지원합니다. 이러한 표준 맵은 매핑 파일에 대한 수동 수정을 요구하지 않습니다. 다음 목록에 없는 시스템의 모든 맵은 사용자 정의 맵으로 간주되며 수동 수정이 필요합니다.

N2L 서비스는 auto.* 맵의 자동 매핑도 지원합니다. 그러나 대부분의 auto.* 파일 이름과 내용은 각 네트워크 구성과 관련이 있으므로 해당 파일은 이 목록에 지정되지 않습니다. 단, 표준 맵으로 지원되는 auto.home 및 auto.master 맵은 예외입니다.

```
audit_user
auth_attr
auto.home
```

```
auto.master
bootparams
ethers.byaddr ethers.byname
exec_attr
group.bygid group.byname group.adjunct.byname
hosts.byaddr hosts.byname
ipnodes.byaddr ipnodes.byname
mail.byaddr mail.aliases
netgroup netgroup.byprojid netgroup.byuser netgroup.byhost
netid.byname
netmasks.byaddr
networks.byaddr networks.byname
passwd.byname passwd.byuid passwd.adjunct.byname
prof_attr
project.byname project.byprojectid
protocols.byname protocols.bynumber
publickey.byname
rpc.bynumber
services.byname services.byservicename
timezone.byname
user_attr
```

NIS-to-LDAP 전환 중에 `yppasswdd` 데몬은 N2L 관련 맵인 `ageing.byname`을 사용하여 암호 에이징 정보를 읽고 DIT에 씁니다. 암호 에이징을 사용하지 않는 경우 `ageing.byname` 매핑은 무시됩니다.

NIS에서 LDAP으로 전환(작업 맵)

다음 표에서는 표준 및 사용자 정의 NIS-to-LDAP 매핑을 사용하여 N2L 서비스를 설치하고 관리하는 데 필요한 절차를 식별합니다.

작업	설명	지침
모든 필수 조건을 완료합니다.	NIS 서버와 Oracle Directory Server Enterprise Edition(LDAP 서버)을 올바르게 구성했는지 확인합니다.	221 페이지 “NIS-to-LDAP 전환에 대한 필수 조건”
N2L 서비스를 설정합니다.	NIS 마스터 서버에서 `inityp2l`을 실행하여 다음 매핑 중 하나를 설정합니다.	
	표준 매핑	223 페이지 “표준 매핑을 사용하여 N2L 서비스를 설정하는 방법”
	사용자 정의 또는 비표준 매핑	224 페이지 “사용자 정의 매핑 또는 비표준 매핑을 사용하여 N2L 서비스를 설정하는 방법”
맵을 사용자 정의합니다.	N2L 전환에 대한 사용자 정의 맵을 만드는 방법의 예를 봅니다.	227 페이지 “사용자 정의 맵의 예”

작업	설명	지침
N2L을 사용하여 Oracle Directory Server Enterprise Edition을 구성합니다.	N2L 전환에 대한 LDAP 서버로 Oracle Directory Server Enterprise Edition을 구성하고 조정합니다.	228 페이지 “Oracle Directory Server Enterprise Edition에서의 NIS-to-LDAP 최적 사용법”
시스템 문제를 해결합니다.	일반적인 N2L 문제를 식별하고 해결합니다.	231 페이지 “NIS-to-LDAP 문제 해결”
NIS로 되돌립니다.	적절한 맵을 사용하여 NIS로 되돌립니다.	
	이전 NIS 소스 파일을 기반으로 하는 맵	236 페이지 “이전 소스 파일 기반 맵으로 되돌리는 방법”
	현재 DIT를 기반으로 하는 맵	237 페이지 “현재 DIT 내용 기반 맵으로 되돌리는 방법”

NIS-to-LDAP 전환에 대한 필수 조건

N2L 서비스를 구현하기 전에 다음 항목을 확인하거나 완료해야 합니다.

- `inityp2l` 스크립트를 실행하여 N2L 모드를 사용으로 설정하기 전에 시스템이 작동하는 기존 NIS 서버로 설정되었는지 확인합니다.
- 시스템에서 LDAP 디렉토리 서버를 구성합니다.

  Oracle Directory Server Enterprise Edition 및 Oracle에서 제공하는 호환되는 디렉토리 서버 버전은 NIS-to-LDAP 마이그레이션 도구에서 지원됩니다. Oracle Directory Server Enterprise Edition을 사용하는 경우 N2L 서비스를 설정하기 **전에** `idsconfig` 명령을 사용하여 서버를 구성합니다. `idsconfig`에 대한 자세한 내용은 11 장, “LDAP 클라이언트를 사용하여 Oracle Directory Server Enterprise Edition 설정(작업)” 및 `idsconfig(1M)` 매뉴얼 페이지를 참조하십시오.

  다른 타사 LDAP 서버는 N2L 서비스에서 작동할 수도 있지만 Oracle에서 지원되지 않습니다. Oracle Directory Server Enterprise Edition 이외의 LDAP 서버나 호환되는 Oracle 서버를 사용 중인 경우 N2L을 설정하기 **전에** RFC 2307bis, RFC 4876 또는 이후 버전의 스키마를 지원하도록 서버를 수동으로 구성해야 합니다.
- `config/host` 등록 정보에 대해 `files`를 `dns` 이전에 사용합니다.
- N2L 마스터 서버와 LDAP 서버의 주소가 N2L 마스터 서버의 `hosts` 파일에 있는지 확인합니다.

  대체 해결 방법은 호스트 이름이 아니라 LDAP 서버 주소를 `ypserv`에 나열하는 것입니다. 이렇게 하면 LDAP 서버 주소가 다른 장소에 나열되므로 LDAP 서버나 N2L 마스터 서버의 주소를 변경할 경우 추가 파일 수정이 필요합니다.

NIS-to-LDAP 서비스 설정

다음 두 절차에 설명된 대로 표준 매핑을 사용하거나 사용자 정의 매핑을 사용하여 N2L 서비스를 설정할 수 있습니다.

NIS-to-LDAP 변환의 일부로 `inityp2l` 명령을 실행해야 합니다. 이 명령은 구성 정보를 제공해야 하는 대화식 스크립트를 실행합니다. 다음 목록에서는 제공해야 하는 정보 유형을 보여 줍니다. 이러한 속성에 대한 설명은 ypserv(1M) 매뉴얼 페이지를 참조하십시오.

- 생성되는 구성 파일의 이름(기본값 = `/etc/default/ypserv`)
- 구성 정보를 LDAP에 저장하는 DN(기본값 = `/etc/default/ypserv`)
- LDAP과 데이터 매핑에 사용되는 기본 서버 목록
- LDAP과 데이터 매핑에 사용되는 인증 방법
- LDAP과 데이터 매핑에 사용되는 TLS(전송 계층 보안) 방법
- LDAP에서 데이터 읽기/쓰기를 수행할 프록시 사용자 바인드 DN
- LDAP에서 데이터 읽기/쓰기를 수행할 프록시 사용자 암호
- LDAP 바인드 작업의 시간 초과 값(초)
- LDAP 검색 작업의 시간 초과 값(초)
- LDAP 수정 작업의 시간 초과 값(초)
- LDAP 추가 작업의 시간 초과 값(초)
- LDAP 삭제 작업의 시간 초과 값(초)
- LDAP 서버의 검색 작업에 대한 시간 제한(초)
- LDAP 서버의 검색 작업에 대한 크기 제한(바이트)
- N2L이 LDAP 참조를 따라야 하는지 여부
- LDAP 검색 오류 작업, 검색 시도 횟수 및 각 시도 사이의 시간 초과(초)
- 저장 오류 작업, 시도 횟수 및 각 시도 사이의 시간 초과(초)
- 매핑 파일 이름
- `auto_direct` 맵에 대한 매핑 정보를 생성할지 여부

  이 스크립트는 매핑 파일의 적절한 위치에 사용자 정의 맵과 관련된 정보를 배치합니다.
- 이름 지정 컨텍스트
- 암호 변경을 사용으로 설정할지 여부
- 모든 맵의 기본 TTL 값을 변경할지 여부

주 – `sasl/cram-md5` 인증은 Oracle Directory Server Enterprise Edition을 비롯한 대부분의 LDAP 서버에서 지원되지 **않습니다**.

▼ 표준 매핑을 사용하여 N2L 서비스를 설정하는 방법

219 페이지 "지원되는 표준 매핑"에 나열된 맵을 전환 중인 경우 이 절차를 사용합니다. 사용자 정의 맵이나 비표준 맵을 사용 중인 경우 224 페이지 "사용자 정의 매핑 또는 비표준 매핑을 사용하여 N2L 서비스를 설정하는 방법"을 참조하십시오.

LDAP 서버가 설정된 경우 `inityp2l` 스크립트를 실행하고 메시지가 표시되면 구성 정보를 제공합니다. `inityp2l`은 표준 및 `auto.*` 맵에 대한 구성 파일과 매핑 파일을 설정합니다.

1 **221 페이지 "NIS-to-LDAP 전환에 대한 필수 조건"에 나열된 필수 조건 단계를 완료합니다.**

2 **NIS 마스터 서버의 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

3 **NIS 마스터 서버를 N2L 서버로 변환합니다.**

```
# inityp2l
```

NIS 마스터 서버에서 `inityp2l` 스크립트를 실행하고 프롬프트를 따릅니다. 제공해야 하는 정보 목록은 222 페이지 "NIS-to-LDAP 서비스 설정"을 참조하십시오.

자세한 내용은 `inityp2l(1M)` 매뉴얼 페이지를 참조하십시오.

4 **LDAP DIT(디렉토리 정보 트리)가 완전히 초기화되었는지 확인합니다.**

`NISLDAPmapping` 파일에 나열된 모든 맵을 채우는 데 필요한 정보가 DIT에 이미 포함되어 있으면 DIT가 완전히 초기화됩니다.

- DIT가 완전히 초기화되지 않은 경우 단계 5를 계속하고 6단계를 건너뜁니다.
- 완전히 초기화된 경우 5단계를 건너뛰고 단계 6로 이동합니다.

5 **NIS 소스 파일에서 전환하기 위해 DIT를 초기화합니다.**

DIT가 완전히 초기화되지 **않은** 경우에만 이러한 단계를 수행합니다.

a. **이전 NIS 맵이 최신 상태인지 확인합니다.**

```
# cd /var/yp
# make
```

자세한 내용은 `ypmake(1M)` 매뉴얼 페이지를 참조하십시오.

b. NIS 서비스를 중지합니다.

```
# svcadm disable network/nis/server:default
```

c. 이전 맵을 DIT에 복사한 다음 맵에 대해 N2L 지원을 초기화합니다.

```
# ypserv -IR
```

ypserv가 종료될 때까지 기다립니다.

참고 – 원본 NIS dbm 파일은 덮어쓰지 않습니다. 필요한 경우 이러한 파일을 복구할 수 있습니다.

---

d. DNS 및 NIS 서비스를 시작하여 새 맵을 사용하는지 확인합니다.

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

이제 표준 맵을 사용한 N2L 서비스 설정이 완료되었습니다. 6단계를 완료하지 않아도 됩니다.

6 NIS 맵을 초기화합니다.

DIT가 완전히 초기화되었으며 5단계를 건너뛴 경우에만 이러한 단계를 수행합니다.

a. NIS 서비스를 중지합니다.

```
# svcadm disable network/nis/server:default
```

b. DIT의 정보를 사용하여 NIS 맵을 초기화합니다.

```
# ypserv -r
```

ypserv가 종료될 때까지 기다립니다.

참고 – 원본 NIS dbm 파일은 덮어쓰지 않습니다. 필요한 경우 이러한 파일을 복구할 수 있습니다.

---

c. DNS 및 NIS 서비스를 시작하여 새 맵을 사용하는지 확인합니다.

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

▼ 사용자 정의 매핑 또는 비표준 매핑을 사용하여 N2L 서비스를 설정하는 방법

다음 조건이 적용되는 경우 이 절차를 사용합니다.

- 219 페이지 “지원되는 표준 매핑”에 나열되지 않은 맵이 있습니다.
- 비-RFC 2307 LDAP 매핑에 매핑하려는 표준 NIS 맵이 있습니다.

1 **221 페이지 "NIS-to-LDAP 전환에 대한 필수 조건"에 나열된 필수 조건 단계를 완료합니다.**

2 **NIS 마스터 서버의 관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

역할에는 권한 부여 및 권한이 있는 명령이 포함됩니다. 역할에 대한 자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 9 장, "역할 기반 액세스 제어 사용(작업)"을 참조하십시오.

3 **NIS 마스터 서버를 N2L 서버로 구성합니다.**

```
# inityp2l
```

NIS 마스터 서버에서 `inityp2l` 스크립트를 실행하고 프롬프트를 따릅니다. 제공해야 하는 정보 목록은 222 페이지 "NIS-to-LDAP 서비스 설정"을 참조하십시오.

자세한 내용은 `inityp2l`(1M) 매뉴얼 페이지를 참조하십시오.

4 **/var/yp/NISLDAPmapping 파일을 수정합니다.**

매핑 파일을 수정하는 방법의 예는 227 페이지 "사용자 정의 맵의 예"를 참조하십시오.

5 **LDAP DIT(디렉토리 정보 트리)가 완전히 초기화되었는지 확인합니다.**

`NISLDAPmapping` 파일에 나열된 모든 맵을 채우는 데 필요한 정보가 DIT에 이미 포함되어 있으면 DIT가 완전히 초기화됩니다.

- 완전히 초기화되지 않은 경우 6단계, 8단계 및 9단계를 완료합니다.
- 완전히 초기화된 경우 6단계를 건너뛰고 단계 7, 8단계 및 9단계를 완료합니다.

6 **NIS 소스 파일에서 전환하기 위해 DIT를 초기화합니다.**

a. **이전 NIS 맵이 최신 상태인지 확인합니다.**

```
# cd /var/yp
# make
```

자세한 내용은 `ypmake`(1M) 매뉴얼 페이지를 참조하십시오.

b. **NIS 데몬을 중지합니다.**

```
# svcadm disable network/nis/server:default
```

c. **이전 맵을 DIT에 복사한 다음 맵에 대해 N2L 지원을 초기화합니다.**

```
# ypserv -Ir
```

`ypserv`가 종료될 때까지 기다립니다.

참고 – 원본 NIS dbm 파일은 덮어쓰지 않습니다. 필요한 경우 이러한 파일을 복구할 수 있습니다.

d. DNS 및 NIS 서비스를 시작하여 새 맵을 사용하는지 확인합니다.

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

e. 7단계를 건너뛰고 단계 8에서 계속합니다.

7 NIS 맵을 초기화합니다.

DIT가 완전히 초기화된 경우에만 이 단계를 수행합니다.

a. NIS 데몬을 중지합니다.

```
# svcadm disable network/nis/server:default
```

b. DIT의 정보를 사용하여 NIS 맵을 초기화합니다.

```
# ypserv -r
```

ypserv가 종료될 때까지 기다립니다.

참고 – 원본 NIS dbm 파일은 덮어쓰지 않습니다. 필요한 경우 이러한 파일을 복구할 수 있습니다.

c. DNS 및 NIS 서비스를 시작하여 새 맵을 사용하는지 확인합니다.

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

8 LDAP 항목이 올바른지 확인합니다.

항목이 올바르지 않으면 LDAP 이름 지정 서비스 클라이언트에서 항목을 찾을 수 없습니다.

```
# ldapsearch -h server -s sub -b "ou=servdates, dc=..." \ "objectclass=servDates"
```

9 LDAP_ 맵의 내용을 확인합니다.

다음 샘플 출력은 makedm 명령을 사용하여 hosts.byaddr 맵의 내용을 확인하는 방법을 보여 줍니다.

```
# makedbm -u LDAP_servdate.bynumber
plato: 1/3/2001
johnson: 2/4/2003,1/3/2001
yeats: 4/4/2002
poe: 3/3/2002,3/4/2000
```

내용이 예상과 같으면 NIS에서 LDAP으로 전환에 성공한 것입니다.

원본 NIS dbm 파일은 덮어쓰지 않으므로 언제든지 이러한 파일을 복구할 수 있습니다. 자세한 내용은 236 페이지 “NIS로 되돌리기”를 참조하십시오.

사용자 정의 맵의 예

다음 두 가지 예에서는 맵을 사용자 정의하는 방법을 보여 줍니다. 원하는 텍스트 편집기를 사용하여 필요에 따라 `/var/yp/NISLDAPmapping` 파일을 수정합니다. 파일 속성 및 구문에 대한 자세한 내용은 `NISLDAPmapping(4)` 매뉴얼 페이지와 9 장, "LDAP 이름 지정 서비스 소개(개요)"의 LDAP 이름 지정 서비스 정보를 참조하십시오.

예 15–1 호스트 항목 이동

이 예에서는 기본 위치에서 DIT의 다른 (비표준) 위치로 호스트 항목을 이동하는 방법을 보여 줍니다.

`NISLDAPmapping` 파일의 `nisLDAPobjectDN` 속성을 새 기본 LDAP DN(식별 이름)으로 변경합니다. 이 예에서는 LDAP 객체의 내부 구조가 변경되지 않으므로 `objectClass` 항목도 변경되지 않습니다.

변경 전:

```
nisLDAPobjectDN hosts: \
                        ou=hosts,?one?, \
                        objectClass=device, \
                        objectClass=ipHost
```

변경 후:

```
nisLDAPobjectDN hosts: \
                        ou=newHosts,?one?, \
                        objectClass=device, \
                        objectClass=ipHost
```

이렇게 변경하면 항목이 다음 위치가 아니라

```
dn: ou=newHosts, dom=domain1, dc=sun, dc=com
```

아래에 매핑됩니다.

```
dn: ou=hosts, dom=domain1, dc=sun, dc=com.
```

예 15–2 사용자 정의 맵 구현

이 예에서는 사용자 정의 맵을 구현하는 방법을 보여 줍니다.

가상 맵 *servdate.bynumber*에는 시스템 서비스 날짜에 대한 정보가 포함되어 있습니다. 이 맵은 시스템 일련 번호(이 예에서는 123)로 색인화되어 있습니다. 각 항목은 시스템 소유자 이름, 콜론 및 쉼표로 구분된 서비스 날짜 목록으로 구성됩니다(예: John Smith:1/3/2001,4/5/2003).

이전 맵 구조는 다음 형식과 같은 LDAP 항목에 매핑되어야 합니다.

```
dn: number=123,ou=servdates,dc=... \
                number: 123 \
                userName: John Smith \
```

예 15–2 사용자 정의 맵 구현 *(계속)*

```
                date: 1/3/2001 \
                date: 4/5/2003 \
                 .
                 .
                 .
                objectClass: servDates
```

NISLDAPmapping 파일을 검사하여 요청된 패턴에 가장 가까운 매핑이 group인 것을 확인할 수 있습니다. group 매핑에 사용자 정의 매핑을 모델링할 수 있습니다. 맵이 1개뿐이므로 nisLDAPdatabaseIdMapping 속성은 필요 없습니다. NISLDAPmapping에 추가할 속성은 다음과 같습니다.

```
nisLDAPentryTtl servdate.bynumber:1800:5400:3600

nisLDAPnameFields servdate.bynumber: \
                        ("%s:%s", uname, dates)

nisLDAPobjectDN servdate.bynumber: \
                        ou=servdates, ?one? \
                        objectClass=servDates:

nisLDAPattributeFromField servdate.bynumber: \
                        dn=("number=%s,", rf_key), \
                        number=rf_key, \
                        userName=uname, \
                        (date)=(dates, ",")

nisLDAPfieldFromAttribute servdate.bynumber: \
                        rf_key=number, \
                        uname=userName, \
                        dates=("%s,", (date), ",")
```

Oracle Directory Server Enterprise Edition에서의 NIS-to-LDAP 최적 사용법

N2L 서비스는 Oracle Directory Server Enterprise Edition을 지원합니다. 다른 타사 LDAP 서버는 N2L 서비스에서 작동할 수도 있지만 Oracle에서 지원되지 않습니다. Oracle Directory Server Enterprise Edition 서버 이외의 LDAP 서버나 호환되는 Oracle 서버를 사용 중인 경우 RFC 2307, RFC 2307bis, RFC 4876 또는 이후 버전의 스키마를 지원하도록 서버를 수동으로 구성해야 합니다.

Oracle Directory Server Enterprise Edition을 사용 중인 경우 디렉토리 서버를 개선하여 성능을 향상시킬 수 있습니다. 이러한 개선을 수행하려면 Oracle Directory Server Enterprise Edition에 LDAP 관리자 권한이 있어야 합니다. 디렉토리 서버를 재부트해야 할 수도 있습니다. 이 작업은 서버의 LDAP 클라이언트와 함께 조정해야 합니다. Oracle Directory Server Enterprise Edition 설명서는 Sun Java System Directory Server Enterprise Edition 6.2 웹 사이트에서 제공됩니다.

Oracle Directory Server Enterprise Edition을 사용하여 가상 목록 보기 색인 만들기

큰 맵의 경우 LDAP VLV(가상 목록 보기) 색인을 사용하여 LDAP 검색에서 전체 결과가 반환되도록 해야 합니다. Oracle Directory Server Enterprise Edition에서 VLV 색인을 설정하는 방법에 대한 자세한 내용은 Sun Java System Directory Server Enterprise Edition 6.2 설명서를 참조하십시오.

VLV 검색 결과는 고정 페이지 크기 50000을 사용합니다. Oracle Directory Server Enterprise Edition과 함께 VLV를 사용하는 경우 LDAP 서버와 N2L 서버 모두 이 크기의 전송을 처리할 수 있어야 합니다. 모든 맵이 이 제한보다 작은 경우 VLV 색인을 사용할 필요가 없습니다. 그러나 맵이 크기 제한보다 크거나 모든 맵의 크기를 잘 모르는 경우 VLV 색인을 사용하여 불완전한 반환을 방지합니다.

VLV 색인을 사용 중인 경우 다음과 같이 적절한 크기 제한을 설정합니다.

- Oracle Directory Server Enterprise Edition: `nsslapd-sizelimit` 속성이 50000보다 크거나 같은 값 또는 `-1`로 설정되어야 합니다. `idsconfig(1M)` 매뉴얼 페이지를 참조하십시오.
- N2L 서버: `nisLDAPsearchSizelimit` 속성이 50000보다 크거나 같은 값 또는 0으로 설정되어야 합니다. 자세한 내용은 `NISLDAPmapping(4)` 매뉴얼 페이지를 참조하십시오.

VLV 색인이 생성된 후 Oracle Directory Server Enterprise Edition 서버에서 `vlvindex` 옵션과 함께 `dsadm`을 실행하여 VLV 색인을 활성화합니다. 자세한 내용은 `dsadm`(1M) 매뉴얼 페이지를 참조하십시오.

표준 맵에 대한 VLV

다음 조건이 적용되는 경우 Oracle Directory Server Enterprise Edition `idsconfig` 명령을 사용하여 VLV를 설정합니다.

- Oracle Directory Server Enterprise Edition을 사용 중입니다.
- 표준 맵을 RFC 2307bis LDAP 항목에 매핑 중입니다.

VLV는 도메인과 관련이 있으므로 `idsconfig`를 실행할 때마다 특정 NIS 도메인에 대해 VLV가 생성됩니다. 따라서 NIS-to-LDAP 전환 중에 `NISLDAPmapping` 파일에 포함된 **각** `nisLDAPdomainContext` 속성에 대해 `idsconfig`를 한 번 실행해야 합니다.

사용자 정의 맵 및 비표준 맵에 대한 VLV

다음 조건이 적용되는 경우 맵에 대해 새 Oracle Directory Server Enterprise Edition VLV를 수동으로 만들거나 기존 VLV 색인을 복사하고 수정해야 합니다.

- Oracle Directory Server Enterprise Edition을 사용 중입니다.
- 큰 사용자 정의 맵이 있거나 비표준 DIT 위치에 매핑된 표준 맵이 있습니다.

기존 VLV 색인을 보려면 다음을 입력합니다.

```
% ldapsearch -h hostname -s sub -b "cn=ldbm database,cn=plugins,cn=config" "objectclass=vlvSearch"
```

Oracle Directory Server Enterprise Edition에서 서버 시간 초과 방지

N2L 서버가 맵을 새로 고치면 그 결과로 큰 LDAP 디렉토리에 액세스하게 될 수 있습니다. Oracle Directory Server Enterprise Edition이 올바르게 구성되지 않은 경우 새로 고침 작업이 완료되기 전에 시간 초과될 수 있습니다. 디렉토리 서버 시간 초과를 방지하려면 수동으로 또는 `idsconfig` 명령을 실행하여 다음 Oracle Directory Server Enterprise Edition 속성을 수정합니다.

예를 들어, 서버가 검색 요청을 수행하는 데 걸리는 최소 시간(초)을 늘리려면 다음 속성을 수정합니다.

```
dn: cn=config
nsslapd-timelimit: -1
```

테스트를 위해 제한 없음을 나타내는 속성 값 `-1`을 사용할 수 있습니다. 최적 제한 값을 확인했으면 속성 값을 변경합니다. 생산 서버에서는 속성 설정을 `-1`로 유지하지 **마십시오**. 제한이 없으면 서버가 서비스 거부 공격에 취약해질 수 있습니다.

LDAP을 사용하여 Oracle Directory Server Enterprise Edition을 구성하는 방법에 대한 자세한 내용은 본 설명서의 11 장, “LDAP 클라이언트를 사용하여 Oracle Directory Server Enterprise Edition 설정(작업)”을 참조하십시오.

Oracle Directory Server Enterprise Edition에서 버퍼 넘침 방지

버퍼 넘침을 방지하려면 수동으로 또는 `idsconfig` 명령을 실행하여 Oracle Directory Server Enterprise Edition 속성을 수정합니다.

1. 예를 들어, 클라이언트 검색 질의에 대해 반환되는 최대 항목 수를 늘리려면 다음 속성을 수정합니다.

   ```
   dn: cn=config
   nsslapd-sizelimit: -1
   ```

2. 클라이언트 검색 질의에 대해 확인되는 최대 항목 수를 늘리려면 다음 속성을 수정합니다.

   ```
   dn: cn=config, cn=ldbm database, cn=plugins, cn=config
   nsslapd-lookthroughlimit: -1
   ```

테스트를 위해 제한 없음을 나타내는 속성 값 -1을 사용할 수 있습니다. 최적 제한 값을 확인했으면 속성 값을 변경합니다. 생산 서버에서는 속성 설정을 -1로 유지하지 **마십시오**. 제한이 없으면 서버가 서비스 거부 공격에 취약해질 수 있습니다.

VLV를 사용 중인 경우 `sizelimit` 속성 값을 229 페이지 “Oracle Directory Server Enterprise Edition을 사용하여 가상 목록 보기 색인 만들기”에 정의된 대로 설정해야 합니다. VLV를 사용하지 않는 경우 가장 큰 컨테이너를 수용할 수 있는 크기로 크기 제한을 설정해야 합니다.

LDAP을 사용하여 Oracle Directory Server Enterprise Edition을 구성하는 방법에 대한 자세한 내용은 11 장, “LDAP 클라이언트를 사용하여 Oracle Directory Server Enterprise Edition 설정(작업)”을 참조하십시오.

NIS-to-LDAP 제한 사항

N2L 서버가 설정된 후에는 NIS 소스 파일이 더 이상 사용되지 않습니다. 따라서 N2L 서버에서 `ypmake`를 실행하지 마십시오. 기존 `cron` 작업 등에 대해 `ypmake`를 실수로 실행할 경우 N2L 서비스는 영향을 받지 않습니다. 그러나 `yppush`를 명시적으로 호출해야 함을 제안하는 경고가 기록됩니다.

NIS-to-LDAP 문제 해결

이 절에서는 다음 두 가지의 문제 해결에 대해 다룹니다.

일반 LDAP 오류 메시지

N2L 서버에서 내부 LDAP 문제와 관련된 오류를 기록하여 LDAP 관련 오류 메시지가 생성되는 경우가 있습니다. 치명적인 오류는 아니지만 오류 메시지의 문제를 조사해야 합니다. 예를 들어, N2L 서버가 계속 작동하지만 오래된 결과나 불완전한 결과를 제공할 수 있습니다.

다음 목록에서는 N2L 서비스를 구현할 때 발생할 수 있는 일반 LDAP 오류 메시지를 보여줍니다. 오류 설명과 가능한 오류 원인 및 해결 방법이 포함되어 있습니다.

`Administrative limit exceeded`

오류 번호: 11

원인: 디렉토리 서버의 `nsslapd-sizelimit` 속성에서 허용되는 것보다 큰 LDAP 검색이 수행되었습니다. 부분 정보만 반환됩니다.

해결책: nsslapd-sizelimit 속성의 값을 늘리거나 오류가 발생하는 검색에 대해 VLV 색인을 구현합니다.

Invalid DN Syntax

오류 번호: 34

원인: 잘못된 문자가 포함된 DN으로 LDAP 항목을 쓰려고 시도했습니다. N2L 서버가 DN에 생성된 + 기호 등의 잘못된 문자를 이스케이프하려고 합니다.

해결책: LDAP 서버 오류 로그를 검사하여 기록된 잘못된 DN을 확인한 다음 잘못된 DN을 생성한 NISLDAPmapping 파일을 수정합니다.

Object class violation

오류 번호: 65

원인: 잘못된 LDAP 항목을 쓰려고 시도했습니다. 일반적으로 이 오류는 MUST 속성의 누락으로 다음과 같은 경우에 발생할 수 있습니다.

- 속성이 누락된 항목을 만드는 NISLDAPmapping 파일의 버그
- 존재하지 않는 객체에 AUXILIARY 속성을 추가하려는 시도

  예를 들어, passwd.byxxx 맵에서 사용자 이름이 아직 생성되지 않은 경우 해당 사용자에게 보조 정보를 추가하려고 하면 실패합니다.

해결책: NISLDAPmapping 파일 버그의 경우 서버 오류 로그에 기록된 내용을 검사하여 문제의 특성을 확인합니다.

Can’t contact LDAP server

오류 번호: 81

원인: ypserv 파일이 잘못된 LDAP 디렉토리 서버를 가리키도록 잘못 구성되었을 수 있습니다. 또는 디렉토리 서버가 실행되고 있지 않을 수 있습니다.

해결책: 재구성하고 확인합니다.

- 올바른 LDAP 디렉토리 서버를 가리키도록 ypserv 파일을 재구성합니다.
- LDAP 서버가 실행 중인지 확인하려면 다음을 입력합니다.

```
% ping hostname 5 | grep "no answer" || \
      (ldapsearch -h hostname -s base -b ""  \
      "objectclass=*" >/dev/null && echo Directory accessible)
```

  서버를 사용할 수 없는 경우 no answer from *hostname* 메시지가 표시됩니다. LDAP 서버에 문제가 있는 경우 ldap_search: Can’t connect to the LDAP server - Connection refused 메시지가 표시됩니다. 마지막으로, 정상적으로 작동 중인 경우 Directory accessible 메시지가 표시됩니다.

`Timeout`

오류 번호: 85

원인: 일반적으로 DIT에서 맵을 업데이트하는 동안 LDAP 작업이 시간 초과되었습니다. 이제 맵에 오래된 정보가 들어 있을 수 있습니다.

해결책: `ypserv` 구성 파일에서 `nisLDAPxxxTimeout` 속성을 늘립니다.

NIS-to-LDAP 문제

N2L 서버를 실행하는 동안 다음 문제가 발생할 수 있습니다. 가능한 원인 및 해결 방법이 제공됩니다.

`NISLDAPmapping` 파일 디버깅

매핑 파일 `NISLDAPmapping`은 복잡합니다. 많은 잠재적 오류로 인해 매핑이 예기치 않은 방식으로 작동할 수 있습니다. 다음 방법을 사용하여 이러한 문제를 해결합니다.

`Console Message Displays When ypserv -ir (or - Ir) Runs`

설명: 간단한 메시지가 콘솔에 표시되고 서버가 종료됩니다(자세한 설명이 `syslog`에 기록됨).

원인: 매핑 파일의 구문이 잘못되었을 수 있습니다.

해결책: `NISLDAPmapping` 파일의 구문을 확인하고 수정합니다.

`NIS Daemon Exits at Startup`

설명: `ypserv` 또는 다른 NIS 데몬을 실행하면 LDAP 관련 오류 메시지가 기록되고 데몬이 종료됩니다.

원인: 원인은 다음 중 하나일 수 있습니다.

- LDAP 서버에 연결할 수 없습니다.
- NIS 맵 또는 DIT의 항목이 지정한 매핑과 호환되지 않습니다.
- LDAP 서버를 읽거나 쓰려고 하면 오류가 반환됩니다.

해결책: LDAP 서버의 오류 로그를 검사합니다. 231 페이지 “일반 LDAP 오류 메시지”에 나열된 LDAP 오류를 참조하십시오.

`Unexpected Results From NIS Operations`

설명: NIS 작업에서 예상 결과가 반환되지 않지만 오류는 기록되지 않습니다.

원인: LDAP 또는 NIS 맵에 잘못된 항목이 있어서 매핑이 의도대로 완료되지 않았을 수 있습니다.

해결책: NIS 맵의 N2L 버전 및 LDAP DIT의 항목을 확인하고 수정합니다.

1. LDAP DIT에 올바른 항목이 있는지 확인하고 필요에 따라 항목을 수정합니다.

Oracle Directory Server Enterprise Edition을 사용 중인 경우 `dsadm startconsole` 명령을 실행하여 관리 콘솔을 시작합니다.

2. 새로 생성된 맵을 원래 맵과 비교하여 `/var/yp` 디렉토리에 있는 NIS 맵의 N2L 버전에 예상 항목이 있는지 확인합니다. 필요에 따라 항목을 수정합니다.

   ```
   # cd /var/yp/domainname
   # makedbm -u test.byname
   # makedbm -u test.byname
   ```

   맵의 출력을 확인할 때 다음 사항에 주의합니다.

   - 두 파일에서 항목 순서가 동일하지 않을 수 있습니다.

     출력을 비교하기 전에 `sort` 명령을 사용합니다.
   - 두 파일에서 공백 사용이 동일하지 않을 수 있습니다.

     출력을 비교할 때 `diff -b` 명령을 사용합니다.

`Processing Order of NIS Maps`

설명: 객체 클래스 위반이 발생합니다.

원인: `ypserv -i` 명령을 실행하면 각 NIS 맵을 읽고 해당 내용이 DIT에 기록됩니다. 여러 맵이 동일한 DIT 객체에 속성을 제공할 수 있습니다. 일반적으로 하나의 맵이 객체의 모든 `MUST` 속성을 비롯하여 객체의 대부분을 만듭니다. 다른 맵은 추가 `MAY` 속성을 제공합니다.

맵은 `NISLDAPmapping` 파일에서 `nisLDAPobjectDN` 속성의 표시 순서와 동일한 순서로 처리됩니다. `MAY` 속성을 포함하는 맵이 `MUST` 속성을 포함하는 맵보다 먼저 처리되는 경우 객체 클래스 위반이 발생합니다. 이 오류에 대한 자세한 내용은 231 페이지 "일반 LDAP 오류 메시지"의 오류 65를 참조하십시오.

해결책: 맵이 올바른 순서대로 처리되도록 `nisLDAPobjectDN` 속성의 순서를 재지정합니다.

임시 해결 방법으로, `ypserv -i` 명령을 여러 번 다시 실행합니다. 이 명령을 실행할 때마다 LDAP 항목이 더 작성됩니다.

주 – 객체의 모든 `MUST` 속성이 적어도 하나의 맵에서 생성될 수 없도록 매핑할 수 **없습니다**.

N2L 서버 시간 초과 문제

`The server times out.`

원인: N2L 서버가 맵을 새로 고치면 그 결과로 큰 LDAP 디렉토리에 액세스하게 될 수 있습니다. Oracle Directory Server Enterprise Edition이 올바르게 구성되지 않은 경우 이 작업이 완료되기 전에 시간 초과될 수 있습니다.

해결책: 디렉토리 서버 시간 초과를 방지하려면 수동으로 또는 `idsconfig` 명령을 실행하여 Oracle Directory Server Enterprise Edition 속성을 수정합니다. 자세한 내용은 231 페이지 "일반 LDAP 오류 메시지" 및 228 페이지 "Oracle Directory Server Enterprise Edition에서의 NIS-to-LDAP 최적 사용법"을 참조하십시오.

N2L 잠금 파일 문제

`The ypserv command starts but does not respond to NIS requests.`

원인: N2L 서버 잠금 파일이 NIS 맵에 대한 액세스를 올바르게 동기화하고 있지 않습니다. 이 문제는 절대 발생해서는 안됩니다.

해결책: N2L 서버에서 다음 명령을 입력합니다.

```
# svcadm disable network/nis/server:default
# rm /var/run/yp_maplock /var/run/yp_mapupdate
# svcadm enable network/nis/server:default
```

N2L 교착 상태 문제

`The N2L server deadlocks.`

원인: N2L 마스터 서버와 LDAP 서버의 주소가 `hosts`, `ipnodes` 또는 `ypserv` 파일에 제대로 나열되어 있지 않으면 교착 상태가 발생할 수 있습니다. N2L의 올바른 주소 구성에 대한 자세한 내용은 221 페이지 "NIS-to-LDAP 전환에 대한 필수 조건"을 참조하십시오.

교착 상태 시나리오의 예를 보려면 다음 이벤트 시퀀스를 고려합니다.

1. NIS 클라이언트가 IP 주소를 조회하려고 합니다.
2. N2L 서버에서 `hosts` 항목이 오래된 것을 발견합니다.
3. N2L 서버가 LDAP에서 `hosts` 항목을 업데이트하려고 합니다.
4. N2L 서버가 `ypserv`에서 LDAP 서버 이름을 가져온 다음 `libldap`을 사용하여 검색합니다.
5. `libldap`이 이름 서비스 스위치를 호출하여 LDAP 서버 이름을 IP 주소로 변환하려고 합니다.
6. 이름 서비스 스위치가 N2L 서버에 대해 NIS 호출을 수행하여 교착 상태가 발생할 수 있습니다.

해결책: N2L 마스터 서버와 LDAP의 서버의 주소를 N2L 마스터 서버의 `hosts` 또는 `ipnodes` 파일에 나열합니다. 서버 주소가 `hosts`, `ipnodes` 또는 두 파일에 모두 나열되어야 하는지는 로컬 호스트 이름 확인을 위해 이러한 파일이 구성된 방식에 따라 달라집니다. 또한 `svc:/network/name-service/switch` 서비스에 대한 `config/hosts` 등록 정보의 조회 순서에서 `files`가 `nis` 앞에 나열되는지 확인합니다.

이 교착 상태 문제를 해결하는 대체 방법은 ypserv 파일에 호스트 이름이 아니라 LDAP 서버 주소를 나열하는 것입니다. 이 경우 LDAP 서버 주소는 다른 위치에 나열됩니다. 따라서 LDAP 서버나 N2L 마스터 서버의 주소를 변경하려면 추가 작업이 필요합니다.

NIS로 되돌리기

N2L 서비스를 사용하여 NIS에서 LDAP으로 전환된 사이트는 점차적으로 모든 NIS 클라이언트를 LDAP 이름 지정 서비스 클라이언트로 대체해야 합니다. 결국 NIS 클라이언트 지원이 중복됩니다. 그러나 필요한 경우 N2L 서비스는 다음 두 절차에 설명된 대로 기존 NIS로 되돌리는 두 가지 방법을 제공합니다.

참고 – 기존 NIS는 해당 맵이 있는 경우 NIS 맵의 N2L 버전을 무시합니다. NIS로 되돌린 후 맵의 N2L 버전을 서버에 그대로 유지해도 N2L 맵에서 문제가 발생하지는 않습니다. 따라서 나중에 N2L을 다시 사용으로 설정할 경우를 위해 N2L 맵을 유지하는 것이 유용할 수도 있습니다. 그러나 맵은 디스크 공간을 차지합니다.

▼ 이전 소스 파일 기반 맵으로 되돌리는 방법

1. **관리자로 전환합니다.**

   자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2. **NIS 데몬을 중지합니다.**

   ```
   # svcadm disable network/nis/server:default
   ```

3. **N2L을 사용 안함으로 설정합니다.**

   이 명령은 N2L 매핑 파일을 백업하고 이동합니다.

   ```
   # mv /var/yp/NISLDAPmapping backup_filename
   ```

4. **새 맵이 ypmake에 의해 푸시되지 않도록 NOPUSH 환경 변수를 설정합니다.**

   ```
   # NOPUSH=1
   ```

5. **이전 소스를 기반으로 하는 새로운 NIS 맵 세트를 만듭니다.**

   ```
   # cd /var/yp
   # make
   ```

6. **(선택 사항) NIS 맵의 N2L 버전을 제거합니다.**

   ```
   # rm /var/yp/domainname/LDAP_*
   ```

7 **DNS 및 NIS 서비스를 시작합니다.**

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

▼ 현재 DIT 내용 기반 맵으로 되돌리는 방법

이 절차를 수행하기 전에 이전 NIS 소스 파일을 백업합니다.

1 **관리자로 전환합니다.**

자세한 내용은 **Oracle Solaris 11.1 관리: 보안 서비스**의 "지정된 관리 권한을 사용하는 방법"을 참조하십시오.

2 **NIS 데몬을 중지합니다.**

```
# svcadm disable network/nis/server:default
```

3 **DIT에서 맵을 업데이트합니다.**

```
# ypserv -r
```

ypserv가 종료될 때까지 기다립니다.

4 **N2L을 사용 안함으로 설정합니다.**

이 명령은 N2L 매핑 파일을 백업하고 이동합니다.

```
# mv /var/yp/NISLDAPmapping backup_filename
```

5 **NIS 소스 파일을 재생성합니다.**

```
# ypmap2src
```

6 **재생성된 NIS 소스 파일에 올바른 내용과 구조가 있는지 수동으로 확인합니다.**

7 **재생성된 NIS 소스 파일을 적절한 디렉토리로 이동합니다.**

8 **(선택 사항) 매핑 파일의 N2L 버전을 제거합니다.**

```
# rm /var/yp/domainname/LDAP_*
```

9 **DNS 및 NIS 서비스를 시작합니다.**

```
# svcadm enable network/dns/client:default
# svcadm enable network/nis/server:default
```

용어집

baseDN DIT의 일부가 루트 지정된 DN입니다. NIS 도메인 항목의 baseDN인 경우 **컨텍스트**라고도 합니다.

databaseID N2L 서비스의 경우 databaseID는 동일한 형식의 NIS 항목이 포함된 맵 그룹의 별칭입니다(LDAP에 대한 동일한 매핑 사용). 맵에 다양한 키가 포함될 수 있습니다.

DBM DBM은 원래 NIS 맵을 저장하는 데 사용되는 데이터베이스입니다.

DES *DES(***데이터 암호화 표준***)*를 참조하십시오.

DES (데이터 암호화 표준) 데이터를 암호화하고 암호 해독하기 위해 미국 연방 표준국(U.S. National Bureau of Standards)에서 개발되었으며, 일반적으로 사용되는 정교한 알고리즘입니다. SUN-DES-1을 참조하십시오.

DIT 디렉토리 정보 트리를 참조하십시오.

DN LDAP의 식별 이름입니다. 각 LDAP 항목에 고유한 이름을 지정하는, 트리와 유사한 구조의 LDAP 디렉토리 주소 지정 체계입니다.

DNS *Domain Name System*을 참조하십시오.

DNS (도메인 이름 지정 서비스) 도메인 및 시스템 이름을 엔터프라이즈 외부 주소(예: 인터넷상의 주소)에 매핑하기 위한 이름 지정 정책과 방식을 제공하는 서비스입니다. DNS는 인터넷에서 사용되는 네트워크 정보 서비스입니다.

DNS 영역 네트워크 도메인 내의 관리 경계로, 대체로 1개 이상의 하위 도메인으로 구성됩니다.

DNS 영역 파일 DNS 소프트웨어가 도메인에 있는 모든 워크스테이션의 이름과 IP 주소를 저장하는 파일 세트입니다.

DNS 전달 NIS 서버는 응답할 수 없는 요청을 DNS 서버로 전달합니다.

GID **그룹** *ID*를 참조하십시오.

IP 인터넷 프로토콜입니다. 인터넷 프로토콜 제품군에 대한 **네트워크 계층** 프로토콜입니다.

IP 주소 네트워크에서 각 호스트를 식별하는 고유한 숫자입니다.

LAN (Local Area Network) 데이터와 소프트웨어를 공유하고 교환하기 위해 함께 연결된 단일 지역 사이트의 다중 시스템입니다.

LDAP Lightweight Directory Access Protocol은 LDAP 이름 지정 클라이언트와 서버가 서로 통신하는 데 사용하는 확장 가능한 표준 디렉토리 액세스 프로토콜입니다.

MIS 관리 정보 시스템(또는 서비스)입니다.

N2L 서버 NIS-to-LDAP 서버입니다. N2L 서비스를 사용하여 N2L 서버로 재구성된 NIS 마스터 서버입니다. 재구성에는 NIS 데몬 대체, 새 구성 파일 추가 등이 포함됩니다.

NDBM NDBM은 향상된 버전의 DBM입니다.

NIS 네트워크의 시스템 및 사용자에 대한 주요 정보가 포함된 분산 네트워크 정보 서비스입니다. NIS 데이터베이스는 **마스터 서버**와 모든 **복제본** 또는 **슬레이브 서버**에 저장됩니다.

NIS 맵 NIS에서 사용되며, 특정 유형의 정보(예: 네트워크상의 모든 사용자의 암호 항목 또는 네트워크상의 모든 호스트 시스템의 이름)를 포함하는 파일입니다. NIS 서비스에 속하는 프로그램은 이러한 맵을 질의합니다. *NIS*를 참조하십시오.

RDN Relative Distinguished Name의 머리글자어로, 상대 식별 이름입니다. DN의 한 부분입니다.

RFC 2307 표준 NIS 맵의 정보와 DIT 항목 간의 매핑을 지정하는 RFC입니다. 기본적으로 N2L 서비스는 업데이트된 버전 RFC 2307bis에 지정된 매핑을 구현합니다.

RPC RPC(원격 프로시저 호출)를 참조하십시오.

RPC (원격 프로시저 호출) 분산 컴퓨팅의 클라이언트-서버 모델을 구현하기 위한 쉽고 널리 사용되는 패러다임입니다. 제공된 인자를 사용하여 지정된 프로시저를 실행하기 위해 원격 시스템으로 요청이 전송되고 결과가 호출자에게 반환됩니다.

SASL Simple Authentication and Security Layer의 머리글자어입니다. 응용 프로그램 계층 프로토콜에서 인증 및 보안 계층 의미를 협상하기 위한 프레임워크입니다.

searchTriple DIT에서 특정 속성을 찾을 위치에 대한 설명입니다. searchTriple은 '기본 dn', '범위' 및 '필터'로 구성됩니다. RFC 2255에서 정의된 LDAP URL 형식의 일부입니다.

SSL SSL은 Secure Sockets Layer 프로토콜입니다. LDAP 등의 응용 프로그램 프로토콜 보안을 유지하기 위해 설계된 일반 전송 계층 보안 방식입니다.

TCP *TCP(**전송 제어 프로토콜**)*를 참조하십시오.

TCP/IP Transport Control Protocol/Interface Program의 머리글자어입니다. 원래 인터넷용으로 개발된 프로토콜 제품군입니다. **인터넷** 프로토콜 제품군이라고도 합니다. Oracle Solaris 네트워크는 기본적으로 TCP/IP에서 실행됩니다.

TCP (전송 제어 프로토콜) 안정적이고 연결 지향 전이중 스트림을 제공하는 인터넷 프로토콜 제품군의 주요 전송 프로토콜입니다. 배달 시 IP를 사용합니다. TCP/IP를 참조하십시오.

TLS (전송 계층 보안) TLS는 LDAP 클라이언트와 디렉토리 서버 간의 통신 보안을 유지하고 프라이버시 및 데이터 무결성을 제공합니다. TLS 프로토콜은 SSL(Secure Sockets Layer) 프로토콜의 수퍼세트입니다.

WAN (Wide Area Network) 전화, 광섬유 또는 위성 링크로 여러 지역 사이트의 시스템이나 여러 LAN(Local Area Network)을 연결하는 네트워크입니다.

X.500 OSI(Open Systems Interconnection) 표준에서 정의된 전역 레벨 디렉토리 서비스입니다. LDAP의 이전 형태입니다.

yp Yellow Pages입니다. NIS의 이전 이름으로, NIS 코드에서 여전히 사용됩니다.

개인 키 수학적으로 생성된 숫자 쌍의 개인 구성 요소로, 개인 키와 결합될 경우 DES 키를 생성합니다. DES 키는 다시 정보를 인코딩 및 디코딩하는 데 사용됩니다. 발신자의 개인 키는 키의 소유자만 사용할 수 있습니다. 각 사용자 또는 시스템에 고유한 공개 키와 개인 키 쌍이 있습니다.

공개 키 수학적으로 생성된 숫자 쌍의 공개 구성 요소로, 개인 키와 결합될 경우 DES 키를 생성합니다. DES 키는 다시 정보를 인코딩 및 디코딩하는 데 사용됩니다. 공개 키는 모든 사용자와 시스템이 사용할 수 있습니다. 각 사용자 또는 시스템에 고유한 공개 키와 개인 키 쌍이 있습니다.

그룹 ID 사용자의 기본 **그룹**을 식별하는 번호입니다.

기본 서버 목록 `client_info` 테이블 또는 `client_info` 파일입니다. 기본 서버 목록은 클라이언트 또는 도메인의 기본 서버를 지정합니다.

네트워크 마스크 소프트웨어가 특정 인터넷 프로토콜 주소의 나머지 부분에서 로컬 서브넷 주소를 구분하는 데 사용하는 숫자입니다.

네트워크 암호 보안 RPC 암호를 참조하십시오.

데이터 암호화 키 암호화를 수행하는 프로그램의 데이터를 암호화하고 암호 해독하는 데 사용되는 키입니다. **키 암호화 키**와 대조됩니다.

도메인 (1) 인터넷에서 대체로 LAN(Local Area Network), WAN(Wide Area Network) 또는 이러한 네트워크의 일부에 해당하는 이름 지정 계층의 일부입니다. 구문상, 인터넷 도메인 이름은 마침표(점)로 구분된 이름 시퀀스(레이블)로 구성됩니다. 예를 들어, `sales.example.com`입니다.

(2) 국제 표준화 기구(International Organization for Standardization)의 OSI(Open Systems Interconnection)에서 "도메인"은 일반적으로 PRMD(MHS Private Management Domain) 및 DMD(Directory Management Domain) 같은 복잡한 분산 시스템의 관리 파티션으로 사용됩니다.

도메인 이름 로컬 네트워크에서 DNS 관리 파일을 공유하는 시스템 그룹에 지정되는 이름입니다. 네트워크 정보 서비스 데이터베이스가 제대로 작동하려면 도메인 이름이 필요합니다. **도메인**을 참조하십시오.

디렉토리 (1) LDAP 디렉토리는 LDAP 객체의 컨테이너입니다. UNIX에서는 파일과 하위 디렉토리의 컨테이너입니다.

디렉토리 정보 트리 DIT는 특정 네트워크의 분산 디렉토리 구조입니다. 기본적으로 클라이언트는 DIT에 특정 구조가 있다고 가정하여 정보에 액세스합니다. LDAP 서버에서 지원되는 각 도메인에 대해 가정된 구조의 하위 트리가 있다고 가정됩니다.

디렉토리 캐시 디렉토리 객체와 연관된 데이터를 저장하는 데 사용되는 로컬 파일입니다.

레코드 **항목**을 참조하십시오.

마스터 서버 특정 도메인에 대한 네트워크 정보 서비스 데이터베이스의 마스터 복사본을 유지 관리하는 서버입니다. 이름 공간 변경은 항상 도메인의 마스터 서버가 유지하는 이름 지정 서비스 데이터베이스에 대해 수행됩니다. 각 도메인에는 마스터 서버가 ***1*개만** 있습니다.

매핑 NIS 항목을 DIT 항목으로 변환하거나 그 반대로 변환하는 프로세스입니다. 이 프로세스는 **매핑** 파일에 의해 제어됩니다.

메일 교환 레코드 DNS 도메인 이름과 해당 메일 호스트 목록을 포함하는 파일입니다.

메일 호스트 사이트에 대해 전자 메일 라우터 및 수신자 역할을 하는 워크스테이션입니다.

보안 RPC 암호 보안 RPC 프로토콜에 필요한 암호입니다. 이 암호는 개인 키를 암호화하는 데 사용됩니다. 이 암호는 항상 사용자의 로그인 암호와 동일해야 합니다.

색인화된 이름 테이블의 항목을 식별하는 데 사용되는 이름 지정 형식입니다.

서버 (1) NIS, DNS 및 LDAP에서는 네트워크에 이름 지정 서비스를 제공하는 호스트 시스템입니다.

(2) 파일 시스템의 **클라이언트-서버 모델**에서 서버는 계산 리소스(계산 서버라고도 불림) 및 큰 메모리 용량을 포함하는 시스템입니다. 클라이언트 시스템은 원격으로 이러한 리소스에 액세스하고 사용할 수 있습니다. 윈도우 시스템의 클라이언트-서버 모델에서 서버는 응용 프로그램 또는 "클라이언트 프로세스"에 윈도우화 서비스를 제공하는 프로세스입니다. 이 모델에서는 클라이언트와 서버가 동일한 시스템에서 실행되거나 별도의 시스템에서 실행될 수 있습니다.

(3) 실제로 제공된 파일을 처리하는 **데몬**입니다.

서버 목록 **기본 서버 목록**을 참조하십시오.

서브넷 경로 지정을 간소화하기 위해 단일 논리적 네트워크를 더 작은 물리적 네트워크로 나누는 작업 체계입니다.

소스 NIS 소스 파일입니다.

속성 각 LDAP 항목은 값이 1개 이상인 많은 **속성**으로 구성되어 있습니다.

또한 N2L 서비스 매핑 및 구성 파일은 각각 많은 **속성**으로 구성되어 있습니다. 각 속성에는 값이 1개 이상 있습니다.

스키마 특정 LDAP DIT에 저장할 수 있는 데이터 유형을 정의하는 규칙 세트입니다.

슬레이브 서버 NIS 데이터베이스의 복사본을 유지 관리하는 서버 시스템입니다. 운영 환경의 전체 복사본과 디스크가 있습니다.

식별 이름 식별 이름은 루트에서 명명된 항목까지의 경로를 따라 트리의 각 항목에서 선택된 속성으로 구성된 X.500 DIB(Directory Information Base)의 항목입니다.

암호화 데이터의 프라이버시를 보호하는 수단입니다.

암호화 키 **데이터 암호화 키**를 참조하십시오.

엔터프라이즈 레벨 네트워크 "엔터프라이즈 레벨" 네트워크는 케이블, 적외선 빔 또는 라디오 브로드캐스트를 통한 단일 LAN(Local Area Network) 통신이거나 케이블 또는 직접 전화 연결을 통해 연결된 둘 이상의 LAN 클러스터일 수 있습니다. 엔터프라이즈 레벨 네트워크 내의 각 시스템은 DNS 또는 X.500/LDAP 같은 전역 이름 지정 서비스를 참조하지 않고 다른 모든 시스템과 통신할 수 있습니다.

역방향 풀기 DNS 소프트웨어를 사용하여 워크스테이션 IP 주소를 워크스테이션 이름으로 변환하는 프로세스입니다.

응용 프로그램 레벨 이름 지정 서비스 응용 프로그램 레벨 이름 지정 서비스는 파일, 메일, 인쇄 등의 서비스를 제공하는 응용 프로그램에 통합되어 있습니다. 응용 프로그램 레벨 이름 지정 서비스는 엔터프라이즈 레벨 이름 지정 서비스에 바인딩되어 있습니다. 엔터프라이즈 레벨 이름 지정 서비스는 응용 프로그램 레벨 이름 지정 서비스의 컨텍스트가 바인딩될 수 있는 컨텍스트를 제공합니다.

이름 공간 (1) 이름 공간은 사용자, 워크스테이션 및 응용 프로그램이 네트워크를 통해 전달해야 하는 정보를 저장합니다.

(2) 이름 지정 시스템에 있는 모든 이름 세트입니다.

이름 서버 네트워크 이름 지정 서비스를 1개 이상 실행하는 서버입니다.

이름 서비스 스위치 이름 지정 클라이언트가 네트워크 정보를 가져올 수 있는 소스를 정의하는 `svc:/system/name-service/switch` 서비스입니다.

이름 지정 서비스 시스템, 사용자, 프린터, 도메인, 라우터, 기타 네트워크 이름과 주소를 처리하는 네트워크 서비스입니다.

이름 풀기 (name resolution) 워크스테이션 또는 사용자 이름을 주소로 변환하는 프로세스입니다.

인증 서버가 클라이언트 ID를 확인할 수 있는 수단입니다.

인터넷 주소 *TCP/IP*를 사용하는 호스트에 지정되는 32비트 주소입니다. **점으로 구분된 십진수 표기법**을 참조하십시오.

자격 증명 클라이언트 소프트웨어가 각 요청과 함께 이름 지정 서버로 보내는 인증 정보입니다. 이 정보는 사용자 또는 시스템의 ID를 확인합니다.

전역 이름 지정 서비스 전역 이름 지정 서비스는 전화, 위성 또는 다른 통신 시스템을 통해 연결되는 전세계 엔터프라이즈 레벨 네트워크(이름)를 식별합니다. 전세계에 연결된 이 네트워크 컬렉션을 "인터넷"이라고 합니다. 이름 지정 네트워크뿐 아니라 전역 이름 지정 서비스는 특정 네트워크상의 개별 시스템과 사용자도 식별합니다.

점으로 구분된 십진수 표기법 밑 10으로 작성된 8비트 숫자 4개와 숫자를 구분하는 마침표(점)로 구성된 32비트 정수의 구문 표현입니다. 인터넷에서 IP 주소를 나타내는 데 사용됩니다(예: 192.67.67.20).

접미어 LDAP에서 DIT의 DN(식별 이름)입니다.

컨텍스트 N2L 서비스의 경우 컨텍스트는 NIS 도메인이 일반적으로 매핑되는 환경입니다. baseDN을 참조하십시오.

클라이언트

(1) 클라이언트는 이름 지정 서버의 이름 지정 서비스를 요청하는 주체(시스템 또는 사용자)입니다.

(2) 파일 시스템의 클라이언트-서버 모델에서 클라이언트는 계산 능력, 큰 메모리 용량 등 계산 서버의 리소스에 원격으로 액세스하는 시스템입니다.

(3) 클라이언트-서버 모델에서 클라이언트는 "서버 프로세스"의 서비스에 액세스하는 **응용 프로그램**입니다. 이 모델에서는 클라이언트와 서버가 동일한 시스템에서 실행되거나 별도의 시스템에서 실행될 수 있습니다.

클라이언트-서버 모델

네트워크 서비스와 해당 서비스의 모델 사용자 프로세스(프로그램)를 설명하는 일반적인 방법입니다. 예를 들어, *DNS(Domain Name System)*의 이름 서버/이름 분석기 패러다임입니다. **클라이언트**를 참조하십시오.

키 서버

개인 키를 저장하는 Oracle Solaris 운영 환경 프로세스입니다.

키 (암호화)

키 관리 및 배포 시스템의 일부로 다른 키를 암호화하고 암호 해독하는 데 사용되는 키입니다. **데이터 암호화 키**와 대조됩니다.

필드

NIS 맵 항목은 많은 구성 요소와 구분자 문자로 구성될 수 있습니다. N2L 서비스 매핑 프로세스의 일부로, 항목은 먼저 명명된 많은 **필드**로 구분됩니다.

항목

DIT의 LDAP 요소 같은 데이터베이스 테이블의 단일 데이터 행입니다.

색인

E

F

G

H

N

W

X

Y

가