IBM® SecureWay® Policy Director

시작에서 수행까지

버전 3 릴리스 0

IBM® SecureWay® Policy Director

시작에서 수행까지

버전 3 릴리스 0

주

본 정보와 해당 지원 제품을 사용하기 전에 101 페이지의 『부록. 주의사항』에 나오는 일반 정보를 읽도록 하십시오.

제1판 (1999년 10월)

본 제판은 IBM SecureWay Policy Director 제품(SCT6-3KNA-00)과 신판에서 특별히 명시하기 전까지는 모든 후속 릴리스와 수정 제품에 적용됩니다.

본 제판은 IBM SecureWay Global Sign-On, 버전 2.0.200을 대체합니다.

목차

이 책에 관해

이 책은 IBM® SecureWay® Policy Director(Policy Director)의 설치 및 구성에 관한 정보를 제공합니다. Policy Director 서버는 다음 운영체제에 설치할 수 있습니다.

- Microsoft® Windows NT®
- AIX®
- Solaris®

NetSEAT 클라이언트는 다음 운영체제에 설치할 수 있습니다.

- Windows® 95
- Windows 98
- Windows NT

이 책의 사용자

이 책은 Policy Director의 계획 및 설치를 담당할 관리자를 위한 것입니다.

관리자는 IBM DCE(분산 컴퓨팅 환경)와 LDAP(Lightweight Directory Access Protocol)의 설치 및 구성을 잘 알아야 합니다. Policy Director는 IBM SecureWay Directory와 IBM 분산 컴퓨팅 환경 서버를 사용하며, Policy Director 제품 안에 포함되어 있습니다.

이 책의 구성

이 책은 다음과 같은 장들로 이루어져 있습니다.

- 1 페이지의 『제1장 Policy Director의 이해』에서는 Policy Director 및 그 구성요소의 개요를 제공합니다.
- 15 페이지의 『제2장 시스템 요구사항』에서는 사용자 운영체제 환경에 적합한 소프트웨어 및 하드웨어 요구사항에 관한 정보를 제공합니다.

- 19 페이지의 『제3장 Policy Director 계획』에서는 Policy Director의 계획, 구성, 관리 정보를 제공합니다.
- 29 페이지의 『제4장 IBM SecureWay Directory 설치 및 구성』에서는 LDAP 사용자 레지스트리를 선택할 경우 IBM SecureWay Directory 버전 3.1.1(LDAP) 클라이언트 SDK와 서버의 설치 및 구성 정보를 제공합니다. Policy Director의 설치 전 반드시 LDAP 서버를 설치 및 구성해야 합니다. 또한 Policy Director의 설치 전 반드시 LDAP 서버를 실행시켜야 합니다.
- 45 페이지의 『제5장 Windows용 Policy Director 설치』에서는 Windows NT 운영체제에서의 Policy Director의 설치 및 구성을 설명합니다.
- 61 페이지의 『제6장 AIX용 Policy Director 설치』에서는 IBM AIX 운영체제에서의 Policy Director의 설치 및 구성을 설명합니다.
- 79 페이지의 『제7장 Solaris용 Policy Director 설치』에서는 Sun Solaris 운영체제에서의 Policy Director의 설치 및 구성을 설명합니다.
- 95 페이지의 『제8장 관련 문서』에서는 그 밖의 Policy Director용 문서 및 관련 자료를 찾을 수 있는 곳을 알려줍니다.

본 릴리스의 새로운 기능

본 릴리스의 Policy Director에는 다음과 같은 새로운 기능이 포함되어 있습니다.

- 사용자 및 그룹 인증사항 정보를 저장하기 위한 IBM SecureWay Directory 지원
- 열기 그룹으로부터의 권한 부여 API 스펙에 대한 최신 갱신사항
- Policy Director 관리 콘솔을 사용한 IBM 방화벽 프록시 사용자 인증사항 정의 및 편집 기능
- 외부 인증 서비스 사용에 대한 지원을 제공하는 Policy Director CAS(Credentials Acquisition Service)
- 새로운 Policy Director CAS를 사용한 클라이언트측의 공인된 인증 지원
- WebSEAL과 Policy Director CAS 간의 IDL(인터페이스 정의 언어) 인터페이스를 사용한 사용자 자신의 사용자 정의 CAS 작성 기능. 또한 Policy Director는 시동, 서버 등록 및 신호 처리 등 Policy Director CAS 서버 기능을 처리하는 일반 서버 프레임워크를 제공합니다.

- GSS(Generic Security Services) 이외의 SSL(Secure Sockets Layer) 터널링 메커니즘 사용의 선택
- 로그인 및 암호 정책을 관리하기 위한 Policy Director CLI(Command Line Interface) 사용
- 단일 사인온 사용자, 그룹, 자원(목표)을 관리하기 위한 Policy Director 관리 콘솔 또는 CLI(Command Line Interface) 사용
- 웹 기반 단일 사인온 자원 암호 관리 툴
- 통합된 설치 처리

2000년 대응

이 제품은 2000년에 대응합니다. 관련 문서에 따라 사용될 때 본 제품과 함께 사용되는 모든 제품(예를 들어, 하드웨어, 소프트웨어, 펌웨어)들이 정확한 날짜 데이터를 본 제품과 원할히 교환할 수 있을 경우, 20세기와 21세기 내의 그리고 20세기와 21세기간의 날짜 데이터를 정확히 처리하고 주고 받을 수 있음을 의미합니다.

서비스 및 지원

IBM SecureWay FirstSecure 제공품에 포함된 모든 제품의 서비스 및 지원에 관해서는 IBM으로 문의하십시오. 이 제품의 일부에는 IBM이 아닌 타사의 지원이 관련될 수 있습니다. FirstSecure 제공품의 일부로 이와 같은 제품을 구입했을 경우에도 IBM으로 서비스 및 지원에 관해 문의하실 수 있습니다.

용례

이 책에서는 다음과 같은 활자상의 용례를 사용합니다.

용례	의미
굵은체	선택란, 단추 및 목록 상자 안의 항목과 같은 사용자 인터페이스 요소
단칸체	구문, 샘플 코드 및 사용자가 반드시 입력해야 하는 텍스트
이탤릭체	Policy Director에 관한 특별한 용어의 강조 및 처음 사용
→	메뉴로부터 선택 항목의 시리즈를 표시할 때. 예를 들어, **파일 → 실행** 누르기는 **파일**을 누른 다음에 **실행**을 누르는 것을 의미합니다.

웹 정보

Policy Director의 최신 갱신사항에 관한 정보는 다음 웹 주소에서 구할 수 있습니다.

http://www.ibm.com/software/security/policy/library

그 밖의 IBM SecureWay FirstSecure 제품의 갱신사항에 관한 정보는 다음 웹 주소에서 구할 수 있습니다.

http://www.ibm.com/software/security/firstsecure/library

제1장 Policy Director의 이해

IBM SecureWay Policy Director(Policy Director)는 IBM SecureWay FirstSecure의 구성요소 또는 독립 제품으로 사용이 가능합니다.

IBM SecureWay FirstSecure란?

IBM SecureWay FirstSecure(FirstSecure)는 IBM 통합 보안 솔루션의 일부입니다. FirstSecure는 다음과 같은 도움을 제공하는 포괄적인 통합 제품 세트입니다.

- 보안 e-business 환경을 설정합니다.
- 보안 계획을 단순화하여 보안 소유권의 총 비용을 축소시킵니다.
- 보안 정책을 구현합니다.
- 효과적인 e-business 환경을 작성합니다.

IBM SecureWay 제품에는 다음 구성요소가 포함되어 있습니다.

Policy Director

IBM SecureWay Policy Director(Policy Director)는 인증, 권한 부여, 데이터 보안 및 웹 자원 관리를 제공합니다.

Boundary Server

IBM SecureWay Boundary Server(Boundary Server)는 다음 기능을 제공합니다.

- 필터링, 프록시 및 회로 레벨 게이트웨이의 중요한 방화벽 기능
- IBM 방화벽과의 VPN(virtual private network) 연결
- 인터넷 보안용 구성요소
- 모빌 코드 보안 솔루션

구성 GUI는 Policy Director의 프록시 사용자 기능을 Boundary Server의 방화벽 제품과 결합시킵니다.

Intrusion Immunity

Intrusion Immunity는 침입자 감지와 항바이러스 보호를 제공합니다.

Trust Authority

IBM SecureWay Trust Authority(Trust Authority)는 암호화 및 상호 조작 가능성을 위한 공용 키 하부구조(PKI) 표준을 지원합니다. Trust Authority는 디지털 인증서의 발행, 갱신 및 취소에 대한 지원을 제공합니다. 이 인증서가 사용자를 인증하고 신뢰되는 통신을 보증하기 위한 방법을 제공합니다.

Toolbox

IBM SecureWay Toolbox(Toolbox)는 응용 프로그램 프로그래머가 자신의 소프트웨어 안으로 보안을 통합하기 위해 사용하는 API 세트입니다. FirstSecure의 일부로 Toolbos를 구할 수 있습니다. Policy Director와 Toolbox 모두에 Policy Director API 라이브러리와 문서가 있습니다.

각 IBM SecureWay FirstSecure 제품을 독립적으로 설치할 수 있으므로 보안 환경으로의 제어된 이동을 계획할 수 있습니다. 이 기능은 사용자 환경 보안의 복잡성과 비용을 축소시키고 웹 응용 프로그램과 자원의 전개를 가속화시킵니다.

FirstSecure 구성요소에 관한 자세한 정보와 IBM SecureWay 제품 문서 목록은 FirstSecure *계획 및 통합* 문서를 참조하십시오.

IBM SecureWay Policy Director란?

Policy Director는 지리적으로 분산된 인트라넷과 *엑스트라넷*에 있어서 자원의 전체적인 보안을 제공하는 독립적 권한 부여 및 보안 관리 솔루션입니다. *엑스트라넷*은 선택된 이용자들이 인터넷과 접속된 하나 이상의 인트라넷을 사용하지 못하도록 제한하기 위해 액세스 제어와 보안 기능을 사용하는 VPN(virtual private network)입니다.

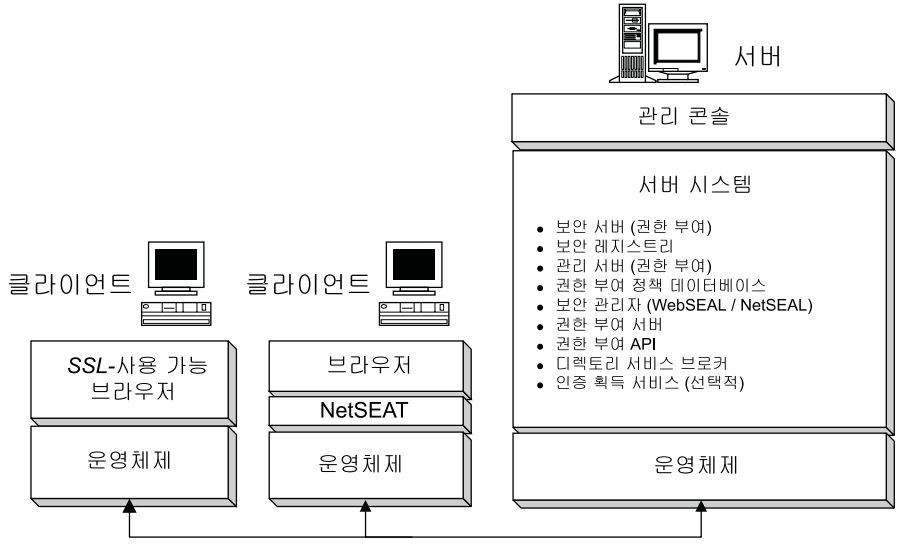
Policy Director는 인증, 권한 부여, 데이터 보안 및 자원 관리 서비스를 제공합니다. 보안 및 제대로 관리되는 인트라넷과 엑스트라넷을 빌드하려는 경우, 표준 인터넷용 응용 프로그램을 Policy Director와 함께 사용할 수 있습니다.

Policy Director는 Windows NT, AIX 및 Solaris 운영체제에서 실행됩니다.

Policy Director 구성요소

Policy Director에는 다음 구성요소가 포함되어 있습니다.

- IBM SecureWay Directory의 LDAP(Lightweight Directory Access Protocol)와 IBM DCE 클라이언트 및 서버
- Policy Director 기본
- 관리 서버
- WebSEAL 및 NetSEAL로 구성된 보안 관리자
- CAS(Credential Acquisition Service)
- 권한 부여 서버
- 권한 부여 API(Application Programming Interface)
- NetSEAT 클라이언트
- 관리 콘솔
- DSB(디렉토리 서비스 브로커)



Policy Director를 설치하기 전에 먼저 사용자 네트워크에 필요한 보안 및 관리 기능을 반드시 결정해야 합니다. 다음 섹션을 사용하여 필요한 Policy Director 구성요소를 결정하십시오.

IBM SecureWay Directory 및 DCE 서버

Policy Director는 IBM SecureWay Directory와 IBM 분산 컴퓨팅 환경 서버를 사용하며 Policy Director 제품 안에 포함되어 있습니다.

Policy Director는 LDAP 사용자 레지스트리 또는 DCE 사용자 레지스트리를 사용할 수 있습니다. Policy Director 설치시 사용자 레지스트리를 선택하도록 프롬프트가 표시됩니다.

LDAP 사용자 레지스트리를 사용할 계획이면, Policy Director를 설치하기 전에 반드시 LDAP 클라이언트를 설치하고 LDAP 서버를 구성해야 합니다. 29 페이지의 『제4장 IBM SecureWay Directory 설치 및 구성』에 나오는 지시사항을 따르십시오. DCE 사용자 레지스트리를 사용할 계획이면, LDAP 설치 및 구성 섹션을 건너뛸 수 있습니다.

IBM SecureWay Directory 서버

SecureWay Directory는 저장, 갱신, 검색 및 교환을 위해 중앙의 디렉토리 정보를 유지보수하는 LDAP(Lightweight Directory Access Protocol)를 제공합니다. 사용자 레지스트리를 위해 LDAP를 사용하는 경우, Policy Director가 LDAP를 사용해 사용자들에게 권한을 부여합니다.

IBM 분산 컴퓨팅 환경 서버

DCE(분산 컴퓨팅 환경)에는 이종 컴퓨팅 환경에 있어서 분산 응용 프로그램의 작성, 사용 및 유지보수를 지원하는 서비스와 툴이 포함되어 있습니다. DCE는 Policy Director 서버들이 사용자를 상호 인증하고 안전하게 통신할 수 있는 보안 도메인을 구성합니다. Windows NT 운영체제에서는 NetSEAT 클라이언트가 DCE 클라이언트로 기능합니다.

Policy Director 기본

Policy Director 기본(IVBase) 구성요소는 모든 Policy Director 구성요소가 사용하는 공통 참조 소프트웨어입니다. 이 구성요소는 Windows에 관리 콘솔을 설치할 경우를 제외하고 그 밖의 Policy Director 구성요소를 설치할 때 자동으로 설치됩니다.

AIX의 경우 SMIT 설정(IV.Smit) 구성요소가 IV.Base 패키지의 일부로 포함되어 있습니다. 이 패키지에는 SMIT가 사용하는 구성 정보가 있습니다. 이 패키지를 모든 AIX 서버에 반드시 설치해야 합니다.

관리 서버

관리 서버(IVMgr)는 전체 보안 도메인을 위한 1차 권한 부여 서버입니다. 관리 서버는 마스터 권한 부여 정책 데이터베이스를 제어하고 유지보수합니다. 모든 데이터는 관리 서버를 통해 이동합니다.

보안 관리자나 권한 부여 서버를 설치하기 전에 반드시 보안 도메인의 컴퓨터에 관리 서버를 설치해야 하지만 같은 컴퓨터에서는 필요하지 않습니다. 주어진 하나의 보안 도메인에 반드시 하나의 관리 서버 인스턴스만 있어야 합니다.

관리 서버의 각 인스턴스에는 관리 서버와 동일한 컴퓨터에 다음 구성요소를 설치해야 합니다.

- DCE 클라이언트
- LDAP 클라이언트(사용자 레지스트리로 LDAP를 사용할 경우)
- Policy Director 기본
- 관리 서버

보안 관리자

보안 관리자(IVNet)는 복제 권한 부여 정책 데이터베이스로부터 나오는 정보를 기반으로 액세스 제어 정책을 적용합니다. 보안 관리자에는 다음과 같은 구성요소가 포함되어 있습니다.

- 정교한 HTTP(Hypertext Transfer Protocol) 및 HTTPS(Secure Sockets Layer Interface) 액세스 제어용 WebSEAL
- 비정교한 TCP/IP(Transmission Control Protocol/Internet Protocol) 액세스 제어용 NetSEAL

NetSEAL과 WebSEAL 구성요소에는 이 기능들을 구성 및 사용 가능하게 만들 필요가 있으며, 기본값으로는 사용 불가능합니다.

WebSEAL

WebSEAL(IVWeb)은 보안 관리자의 HTTP 서버 구성요소입니다. WebSEAL은 HTTP, HTTPS 및 NetSEAT 클라이언트를 지원하는 보안 웹 서버입니다. WebSEAL은 Policy Director CAS(Credential Acquisition Service)를 Policy Director 사용자와 결합시켜 X.509 공인된 인증을 지원합니다.

NetSEAL

NetSEAL(IVTrap)는 TCP/IP 서버를 위해 비정교한 액세스 제어를 제공합니다. NetSEAL은 TCP/IP 서버에 구성 포트 세트로의 액세스를 제어합니다.

Policy Director 제품군은 인터넷 및 개인용 인트라넷에 걸쳐 클라이언트/서버 데이터 교환용 보안을 제공합니다. Policy Director NetSEAL과 Policy Director WebSEAL은 DCE가 정의한 보안 도메인 간의 네트워크 데이터를 제어하고 관리하는 서버측 제품입니다.

권한 부여 서버

권한 부여 서버(IVAcld)는 원격 모드에서 Policy Director 권한 부여 API를 사용하는 써드 파티 응용 프로그램으로부터의 권한 부여 요청을 처리합니다. 써드 파티 응용 프로그램용 보안 도메인에 있는 적어도 하나의 컴퓨터에 권한 부여 서버를 설치해야 합니다.

권한 부여 API

Policy Director 권한 부여 응용 프로그램 개발 킷이 ADK(IVAuthADK) 구성요소에는 Policy Director 권한 부여 API(Application Programming Interface)가 포함되어 있습니다. API를 통해 사용자들은 Policy Director 권한 부여를 사용하는 응용 프로그램을 작성할 수 있습니다.

Policy Director ADK(Application Development Kit)에는 개발자들이 Policy Director 보안과 권한 부여를 전사적 응용 프로그램에 직접 구축할 수 있도록 해주는 권한 부여 API 서버(AuthAPI™)가 포함되어 있습니다. Policy Director 권한 부여 API는 Policy Director 권한 부여 서비스로 직접 액세스합니다. 이 권한 부여 API를 사용함으로써 개발자들은 더 이상 각 응용 프로그램에 대한 권한 부여를 작성할 필요가 없습니다.

ADK에는 C 예제 프로그램이 포함되어 있습니다.

또한 ADK에는 Policy Director CAS(Credential Acquisition Service) 데모 서버와 외부 권한 부여 서비스 데모 서버가 들어 있습니다.

NetSEAT 클라이언트

Policy Director NetSEAT 클라이언트는 Windows 95, Windows 98 또는 Windows NT용의 간단한 클라이언트입니다. NetSEAT는 Policy Director 서버에 보안 통신 채널을 제공합니다.

NetSEAT 클라이언트 소프트웨어는 클라이언트들이 보안 도메인을 결합하여 WebSEAL과 NetSEAL이 제공하는 고급 보안 서비스를 사용할 수 있도록 해줍니다. NetSEAT는 모든 웹 및 클라이언트/서버 트래픽의 전체적인 암호화를 허용하는 동시에 모든 클라이언트의 네트워크 통신을 보안합니다.

NetSEAT는 Telnet과 POP3 등의 서비스가 생성한 것과 같은 클라이언트의 TCP/IP 트래픽을 보안하는 기능을 제공합니다. NetSEAT는 시스템 관리자가 워크스테이션의 네트워크 활동에 있어서 비정교한 제어를 실행할 수 있도록 해줍니다. 이와 같은 제어로 인해 인증된 사용자들이 보안 도메인을 사용할 수 있고 권한 부여 권한을 사용자 및 자원으로 연결시킵니다.

관리 콘솔

관리 콘솔(IVConsole)은 Policy Director 보안 도메인용 보안 정책을 관리하기 위해 사용되는 Java 기반의 그래픽 응용 프로그램입니다. 관리 콘솔을 사용하면 계정 레지스트리와 1차 권한 부여 정책 데이터베이스에서 관리 작업을 수행할 수 있습니다. 관리 콘솔의 경우 보안 도메인에 로그인하고 Policy Director 관리 서버에 보안 관리 원격 프로시듀어 호출(RPC)을 수행하는 데 DCE가 필요합니다. Windows 95, Windows 98 또는 Windows NT에서 관리 콘솔은 NetSEAT가 제공하는 간단한 DCE 서비스(런타임 서비스)를 사용합니다.

디렉토리 서비스 브로커

디렉토리 서비스 브로커(DSB)는 관리 서버 구성요소의 일부로 분배됩니다. 관리 콘솔과 NetSEAT 클라이언트의 경우 Windows 95, Windows 98 또는 Windows

NT 워크스테이션에서 실행할 때 보안 도메인에 DSB가 필요합니다. DSB의 경우 보통 초기 설치 후에는 관리나 구성이 필요하지 않습니다.

인증 획득 서비스(선택 사항)

Policy Director CAS는 선택적으로 구성하는 구성요소입니다.

*인증 획득*이란 전 도메인에 걸친 공통의 클라이언트 식별 표현에 인증 메커니즘이 제공하는 특정 식별 정보를 변환 또는 맵핑하는 처리입니다. 이와 같은 공통의 표현 방식을 *클라이언트 인증*이라 합니다.

인증 획득 또는 맵핑이 필요할 경우, 반드시 Policy Director WebSEAL 서버와 함께 사용할 수 있도록 Policy Director 인증 획득 서비스를 구성해야 합니다. WebSEAL가 Policy Director 사용자들을 자동으로 인증사항에 대응시킵니다.

클라이언트측 X.509 인증서를 사용하여 Policy Director에 액세스하는 클라이언트는 Policy Director 인증 획득 서비스 또는 자신만의 인증 획득 서비스를 작성하여 Policy Director ID에 대응시키는 *인증서* 정보를 가질 수 있습니다.

만일 다른 외부 레지스트리에 정의된 사용자라면, 사용자 이름을 사용자 정의 CAS 서버를 사용하여 Policy Director ID와 대응시킬 수 있습니다. 자신만의 CAS 서버를 작성하고 사용자 정의하여 보안 도메인을 위한 특정 솔루션을 제공하고 클라이언트 인증사항, 사용자 이름, 토큰 등을 처리할 수 있습니다. Policy Director 인증 획득 서비스 개발자나 설계자가 이와 같은 인증 및 서비스 맵핑의 자세한 정보를 전체적으로 결정합니다. Policy Director는 Policy Director 외부의 데이터베이스에 맵핑 규칙들을 저장합니다. Policy Director는 WebSEAL과 Policy Director 인증 획득 서비스 간의 IDL(인터페이스 정의 언어) 인터페이스를 제공합니다. 또한 Policy Director는 시동, 서버 등록 및 신호 처리 등의 Policy Director 인증 획득 서비스 서버 기능들을 처리하는 일반적인 서버 프레임워크를 제공합니다. 인증사항 획득 서비스 프레임워크를 확장시켜 특정 응용 프로그램에 필요한 ID 맵핑 기능을 수행하는 것은 Policy Director 인증 획득 서비스 개발자의 책임사항입니다.

각 Policy Director 구성요소에 관한 자세한 정보는 *Policy Director 관리 안내서*를 참조하십시오.

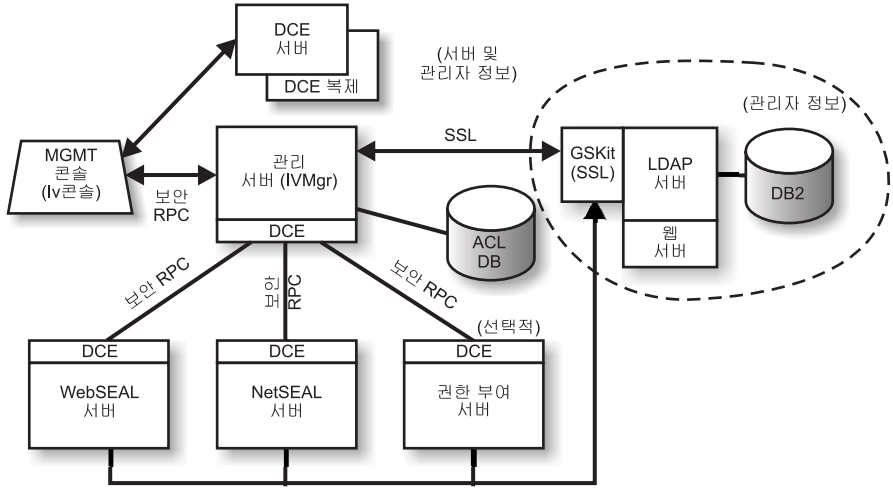
Policy Director의 작업 방식

다음 섹션에는 Policy Director의 일반적인 사용법을 보여주는 네 가지 시나리오가 나옵니다.

- 관리 콘솔을 사용하는 관리자
- 웹 브라우저로부터 보호된 웹 자원에 액세스하는 사용자
- NetSEAT 클라이언트를 사용하여 보호된 TCP/IP 서버에 액세스하는 사용자
- 보호된 써드 파티 서버에 액세스하는 사용자

관리 콘솔을 사용한 관리

다음 그림은 관리자가 Policy Director 관리에 관리 콘솔을 사용할 때의 데이터 흐름을 보여줍니다. 점선에 표시된 LDAP 구성요소들은 사용자 레지스트리로 LDAP를 사용할 경우에만 필요합니다.



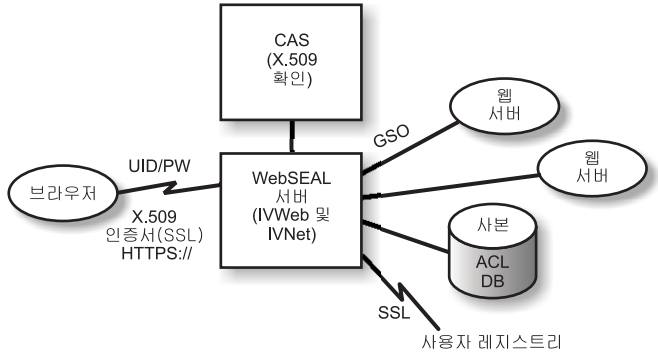
관리 콘솔의 관리자가 보안 도메인에 대해 인증하고 인증사항을 수신합니다.

관리자가 관리 콘솔로부터 사용자나 그룹을 관리할 때, 관리 콘솔이 보안 RPC상의 요청을 관리 서버로 전송합니다. 관리 서버에서는 해당 변경사항을 관리 서버의 DN(Ditinguished Name) 및 암호를 사용하여 이전에 설정했던 SSL 연결 상의 LDAP 서버로 전송합니다.

관리자가 ACL(액세스 제어 목록)을 추가, 수정 또는 적용할 때, 관리 콘솔에서는 보안 RPC 상의 데이터를 관리 서버로 전송합니다. 그런 다음, 관리 서버는 ACL 데이터베이스의 로컬 사본에 변경사항을 저장합니다. 필요한 ACL 데이터베이스가 수정되면, 관리 서버에서는 보안 RPC를 통해 ACL 데이터베이스가 변경되었음을 모든 다른 서버에 통지합니다. 또한 WebSEAL, NetSEAL 및 권한 부여 서버는 ACL 데이터베이스에서의 갱신사항에 대해 관리 서버를 정기적으로 확인합니다.

웹 브라우저를 사용하여 보호된 웹 자원에 액세스하는 사용자

다음 그림은 사용자가 웹 브라우저를 사용하여 보호된 웹 자원에 액세스할 때의 데이터 흐름을 보여줍니다.



사용자가 보호된 웹 페이지에 액세스를 시도할 때, SSL 사용 가능 브라우저에서는 WebSEAL 서버와의 접속을 시도합니다. WebSEAL이 클라이언트 공인된 인증을 위해 구성된 경우, WebSEAL이 브라우저로부터 X.509 인증서를 요청합니다. WebSEAL이 브라우저로부터 인증서를 수신하면 그 인증서를 CAS 서버로 전달합니다. CAS에서는 Policy Director가 인식하는 사용자 ID와 수신한 인증서를 대응시키려고 시도합니다. CAS 구성 파일 안에서 Policy Director 관리자는 Policy Director 사용자의 DN과 인증서 DN을 연관시키는 데 사용할 표를 작성할 수 있습니다. CAS가 인증서를 가진 WebSEAL에 의해 호출될 때, 맨 먼저 CAS는 인증서로부터 DN을 발췌하여 일치하는 표를 찾습니다. 일치하는 표를 찾으면 CAS는 연관된 Policy Director 사용자 DN을 WebSEAL로 리턴합니다. 그런 다음 WebSEAL는 이 DN을 사용하여 Policy Director 사용자를 식별합니다. 그러나 일치하는 표를 찾지 못한 경우에는 CAS가 인증서에서 나온 DN을 WebSEAL로

리턴합니다. 이 경우 인증서의 DN이 Policy Director 사용자를 식별하는 데 사용됩니다. WebSEAL 서버는 리턴된 DN을 사용하여 사용자의 인증사항을 검색합니다.

X.509 인증사항에 관한 자세한 정보는 아래 웹 주소를 참조하십시오.

`http://www.ietf.org`

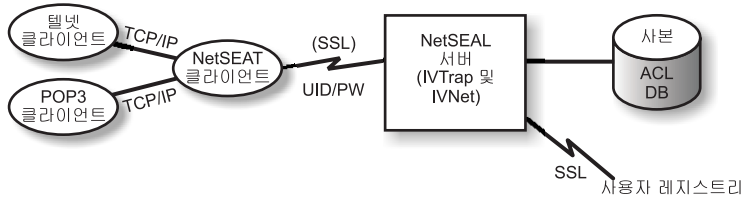
WebSEAL이 성공적으로 사용자 인증을 완료하면, WebSEAL은 ACL 데이터베이스의 로컬 복사본을 사용하여 요청된 방식으로 사용자가 웹 오브젝트에 액세스할 권한이 있는지를 결정합니다.

WebSEAL 서버와 액세스 중인 웹 자원을 포함한 벡엔드(back-end) 서버 간의 연결이 글로벌 사인온(GSO) 중계일 경우, WebSEAL이 LDAP의 해당 중계에 대해 GSO 인증사항을 찾아 웹 서버로 사용자 이름과 암호를 전달합니다.

관리 GSO 자원과 GSO 자원 그룹에 관한 정보는 *Policy Director 관리 안내서*의 관리 콘솔 정보를 참조하십시오.

NetSEAT 클라이언트를 사용하여 보호된 TCP/IP 서버에 액세스하는 사용자

다음 그림은 사용자가 NetSEAT 클라이언트를 사용하는 보호된 TCP/IP 서버에 액세스할 때의 데이터 흐름을 보여줍니다.



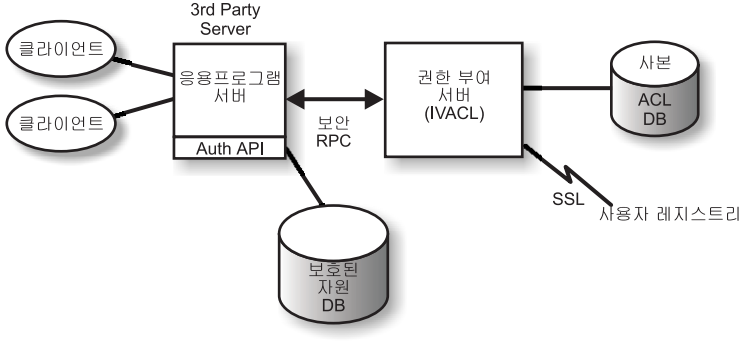
텔넷 클라이언트의 사용자는 NetSEAL 보호 서버와의 텔넷을 통해 사용자의 액세스 요청을 식별합니다. NetSEAL은 사용자 이름과 암호를 요청하고 사용자 정보를 제공하여 그 정보를 사용자 레지스트리에 저장된 값과 비교함으로써 사용자의 ID를 확인합니다. NetSEAL은 사용자가 지정 포트상의 컴퓨터에 액세스할 수 있는지를 확인합니다.

NetSEAT은 Policy Director 서버를 보안하기 위한 요청을 투명하게 재설정하여 보안 SSL 터널을 통해 정보를 전송합니다. NetSEAT은 그 구성 정보를 사용하여 텔넷, POP3 또는 HTTP 등 일반적인 TCP/IP 응용 프로그램에서 보안 서버로의 요청을 인식합니다. NetSEAT은 SSL의 기본적인 인증을 사용하여 NetSEAT 사용자의 ID와 인증사항을 설정합니다. 권한이 설정되었으면 보안 SSL을 캡슐화하여 요청된 트랜잭션을 적절한 보안 설정값에 따라 완료하십시오.

예를 들어, 웹 브라우저 요청이 Policy Director 보안 관리자에 의해 보안된 서비스나 자원에 액세스할 때, NetSEAT에서는 투명하게 요청을 간섭하여 적절한 서버로 그 요청을 라우트합니다. 이것이 Policy Director에 대한 첫번째 요청으로서 인증을 필요로 할 경우, NetSEAT에서 사용자에게 로그인 대화 상자를 프롬프트합니다. 사용자가 인증되고 나면, Policy Director는 정보용으로 각각의 예상 요청에 적절한 인증사항들을 첨부합니다. 이 처리는 Policy Director가 관리하는 모든 Winsock 응용 프로그램에 대해 단일 사인온 환경을 사용 가능하게 합니다. 또한 Policy Director는 이 인증사항들을 사용하여 요청된 Policy Director 보호 자원에 사용자가 액세스할 수 있는지의 여부를 결정합니다.

보호된 써드 파티 서버에 액세스하는 사용자

다음 그림은 사용자가 보호된 써드 파티 서버에 액세스할 때의 데이터 흐름을 보여줍니다.



클라이언트가 써드 파티 보호 서버상의 보호된 데이터에 액세스를 시도할 때 써드 파티 서버에서는 사용자를 인증하고 그 사용자와 Policy Director 사용자를 대응시킵니다. 응용 프로그램 서버는 Policy Director 사용자 정보를 권한 부여 서버

로 전달하여 LDAP(또는 DCE와 같이 사용자 레지스트리에 사용될 다른 제품)와 접속한 다음 사용자의 인증사항들을 검색합니다. 그리고 응용 프로그램 서버에서는 인증사항, 사용자가 액세스하려는 오브젝트의 이름 및 사용자가 수행하려는 조작을 권한 부여 서버로 전달하여 조작 허용 여부 등을 리턴합니다. 그런 후에 응용 프로그램 서버에서 액세스를 허용하거나 거부합니다.

Policy Director 패키지의 포함 제품

IBM SecureWay Policy Director 제품, 버전 3.0은 다섯 장의 CD로 제공됩니다. 다음 표에는 CD 제목과 내용이 있습니다.

CD 제목	**내용**
IBM SecureWay Policy Director 버전 3.0	• IBM Policy Director 버전 3.0
IBM SecureWay Policy Director 보안 서비스	• AIX용 IBM DCE 버전 2.2 • Windows NT용 IBM DCE 버전 2.2 • Solaris용 Transarc DCE 버전 2.0
AIX용 IBM SecureWay Directory 버전 3.1.1	• IBM SecureWay Directory 버전 3.1.1 • IBM DB2 버전 5.2(수정 팩 7 포함) • IBM Global Security Kit SSL Runtime Toolkit 버전 3.0.1(GSKit)
NT용 IBM SecureWay Directory 버전 3.1.1	• IBM SecureWay Directory 버전 3.1.1 • IBM DB2 버전 5.2(수정 팩 7 포함) • IBM Global Security Kit SSL Runtime Toolkit 버전 3.0.1(GSKit)
Solaris용 IBM SecureWay Directory 버전 3.1.1	• IBM SecureWay Directory 버전 3.1.1 • IBM DB2 버전 5.2(수정 팩 8 포함) • IBM Global Security Kit SSL Runtime Toolkit 버전 3.0.1(GSKit)

제2장 시스템 요구사항

사용자의 운영체제 환경이 다음 섹션에서 설명하는 소프트웨어 및 하드웨어 요구사항을 반드시 만족시켜야 합니다. 시스템 요구사항에 관한 최신 정보는 Policy Director README 파일을 참조하십시오. README 파일에는 제품 관련 서적의 교체에 관한 정보가 있습니다.

최신 README 파일은 IBM SecureWay Policy Director 웹 사이트의 라이브러리 페이지에 액세스해 구할 수 있습니다.

`http://www.ibm.com/software/security/policy/library`

Policy Director DCE, LDAP, NetSEAT 및 서버 구성요소를 설치하기 전에, 다음 섹션에 나오는 필수 하드웨어와 소프트웨어를 준비했는지 먼저 확인하십시오.

하드웨어 요구사항

메모리 사용, 버퍼 및 캐쉬 관리, 제어 구조는 규모 조정이 가능합니다. 그러나 기본 운영체제의 기초적인 요구사항, 전제되는 DCE 및 LDAP 클라이언트 요구사항, 사용자 클라이언트 요구사항은 사용자 구성을 위한 디스크 공간 및 메모리의 최소 요구사항을 나타냅니다.

Policy Director 서버를 위한 하드웨어 요구사항은 다음과 같습니다.

플랫폼	최소 디스크 공간	최소 메모리
Intel 또는 Intel 호환용 80486 133 MHz 이상의 Windows NT 서버	16MB	64MB
AIX 4.3.1 실행 하드웨어의 AIX 서버	16MB	64MB
Solaris 2.6 실행 하드웨어의 Solaris 서버	16MB	64MB

Policy Director 클라이언트를 위한 하드웨어 요구사항은 다음과 같습니다.

플랫폼	최소 디스크 공간	최소 메모리
Intel 또는 Intel 호환용 80486 133 MHz 이상의 Windows NT 클라이언트	16MB	32MB

AIX 4.3.1 실행 하드웨어의 AIX 서버	16MB	32MB
Solaris 2.6 실행 하드웨어의 Solaris 서버	16MB	24MB

소프트웨어 요구사항

Policy Director 설치를 계획할 경우, 다음 섹션에 나오는 올바른 운영체제 버전과 기타 전제되는 소프트웨어를 준비했는지 반드시 확인하십시오. 다음은 Policy Director 서버, NetSEAT 클라이언트 및 관리 콘솔을 위한 운영체제 요구사항입니다.

Policy Director 서버

Policy Director 서버는 다음 운영체제에 설치할 수 있습니다.

- Windows NT Server 버전 4.0(서비스 팩 4 이상 포함)
- AIX 버전 4.3.1 이상
- Sun Solaris 버전 2.6

NetSEAT 클라이언트

Policy Director NetSEAT 클라이언트는 다음 운영체제에 설치할 수 있습니다.

- Windows NT 버전 4.0(서비스 팩 4 이상 포함)
- Windows 98
- Windows 95

관리 콘솔

Policy Director 관리 콘솔은 다음 운영체제에 설치할 수 있습니다.

- Windows NT 서버 버전 4.0(서비스 팩 4 이상 포함)
- Windows NT, Windows 95 또는 Windows 98
- AIX 버전 4.3.1 이상(Java Runtime 1.1.6 이상 포함)
- Sun Solaris 버전 2.6

기타 소프트웨어 요구사항

Policy Director에는 DCE 서버와 LDAP 서버(사용자 레지스트리로 LDAP를 사용할 경우)가 필요합니다. 보안 도메인에 있는 최소한 하나의 컴퓨터에 반드시 하

나의 서버(LDAP 또는 DCE)가 있어야 합니다. DCE 및 LDAP 클라이언트와 서버는 Policy Director 제품의 일부로 제공됩니다. 이 제품들을 Policy Director를 설치하기 전에 설치하거나 기존에 설치되어 있던 올바른 레벨의 DCE 및 LDAP를 사용할 수 있습니다.

Windows NT 및 AIX

Windows NT 및 AIX 플랫폼에서는 Policy Director 서버에 다음 소프트웨어가 필요합니다.

- Windows NT 서버의 경우 Windows NT용 IBM DCE 버전 2.2 이상이나 AIX 서버의 경우 AIX용 IBM DCE 버전 2.2 이상
- DB2® 버전 5.2, 수정 팩 7이 포함된 IBM SecureWay Directory 버전 3.1.1(LDAP). LDAP는 사용자 레지스트리로 LDAP를 사용할 경우에만 필요합니다.
- SSL(Secure Sockets Layer) 버전 3.0 이상
- Policy Director CAS(Credentials Acquisition Service)와 WebSEAL에는 다음 웹 브라우저 중 하나가 필요합니다.
  - Microsoft Internet Explorer 버전 4 이상
  - Netscape Communicator 버전 4.5 이상
  - Netscape Navigator 버전 4.5 이상
- Windows 95 전용의 Policy Director 클라이언트에는 반드시 Winsock 버전 2.0 이상이 필요합니다.

Solaris

Solaris 플랫폼에서는 Policy Director 서버에 다음 소프트웨어가 필요합니다.

- Transarc DCE 버전 2.0.
- DB2 버전 5.2 수정 팩 8이 포함된 IBM SecureWay Directory(LDAP) 버전 3.1.1. LDAP는 사용자 레지스트리로 LDAP를 사용할 경우에만 필요합니다.
- SSL(Secure Sockets Layer) 버전 3.0 이상
- Policy Director CAS 및 WebSEAL에는 다음 웹 브라우저가 필요합니다.

- Microsoft Internet Explorer 버전 4 이상
- Netscape Communicator 버전 4.5 이상
- Netscape Navigator 버전 4.5 이상

제3장 Policy Director 계획

다음 섹션에서는 Policy Director의 설치 및 구성을 준비하고 계획하는 데 필요한 정보가 제공됩니다. 계획에 앞서 반드시 1 페이지의 『제1장 Policy Director의 이해』 부분을 읽은 다음 설치에 필요한 Policy Director 구성요소를 결정하십시오.

공통 구성

이 섹션에 나오는 구성은 사용자 네트워크를 위한 적절한 구성을 판별하는 데 도움이 됩니다. 20 페이지의 『일반적인 구성에 필요한 구성요소』에 있는 표를 사용하여 사용자 구성에 필요한 구성요소를 판별하십시오. 그런 다음 Policy Director 설치시 각 구성요소를 선택하십시오. WebSEAL과 NetSEAL은 모든 컴퓨터에서 설치가 가능하다는 것에 주의하십시오. 다음 목록에는 몇 가지 일반적인 Policy Director 구성요소 구성이 나옵니다.

관리 서버 전용

보안 도메인을 위한 단일 인스턴스의 관리 서버를 실행하는 서버. 이 시나리오에서 관리 서버는 자체 시스템에 상주합니다. 관리 서버는 보안 도메인용 마스터 권한 부여 데이터베이스를 유지보수하고, 보안 도메인 전체에 걸쳐 이 데이터베이스를 복사하며, 보안 도메인에 있는 기타 Policy Director 서버 컴퓨터에 관한 위치 정보를 유지보수합니다.

WebSEAL 서버를 사용하는 보안 관리자

두 가지 구성요소 형식의 WebSEAL—보안 관리자(IVNet) 및 WebSEAL(IVWeb). WebSEAL 서버가 웹 공간을 보호합니다. WebSEAL은 *스마트 중계*나 중계를 통해 높은 가용성과 고장 방지를 위한 백엔드(back-end) 서버를 지원합니다.

NetSEAL 서버를 사용하는 보안 관리자

두 가지 구성요소 형식의 NetSEAL—보안 관리자(IVNet) 및 NetSEAL(IVTrap). NetSEAL 서버가 VPN(virtual private network)을 보안하고 레거시 및 써드 파티 네트워크 서비스를 위한 액세스 제어를 제공합니다.

WebSEAL 및 NetSEAL 서버를 사용하는 보안 관리자

WebSEAL과 NetSEAL 서버의 조합.

권한 부여 서버

Policy Director 권한 부여 API를 사용하는 써드 파티 응용 프로그램으로 Policy Director 권한 부여 서비스에 대한 액세스를 제공하는 서버.

권한 부여 서버 및 ADK

권한 부여 서비스를 호출하기 위해 Policy Director 권한 부여 API를 사용하는 써드 파티 응용 프로그램을 작성하려는 개발자용 개발 환경을 제공하는 서버.

관리 콘솔

Policy Director 보안 도메인용 보안 정책을 관리하기 위해 사용되는 Java용 그래픽 응용 프로그램. Windows의 관리 콘솔에는 IVBase가 필요없습니다.

모든 구성요소

위에 나오는 모든 구성을 결합한 서비스를 제공하는 서버.

일반적인 구성에 필요한 구성요소

19 페이지의 『공통 구성』에서 설명한 Policy Director 구성이 다음 표에 나옵니다. 표에서 각 구성에 반드시 설치해야 하는 구성요소가 어느 것인지를 알 수 있습니다. 왼쪽에서 오른쪽으로 읽을 경우, 표시된 구성요소들은 올바른 설치 순서로 되어 있습니다.

두 가지 형식의 구성요소인 WebSEAL과 NetSEAL에 주의하십시오.

WebSEAL 보안 관리자(IVNet) 및 WebSEAL(IVWeb)

NetSEAL 보안 관리자(IVNet) 및 NetSEAL(IVTrap)

IVBase 관련 주:

- Windows의 관리 콘솔에는 IVBase가 필요없습니다.
- AIX에서는 IV.Smit가 IV.Base와 함께 자동으로 설치됩니다.

시나리오	설치 패키지							
	IVBase	**IVMgr**	**IVNet**	**IVWeb**	**IVTrap**	**IVAcld**	**IVAuthADK**	**IVConsole**
관리 서버 전용의 단일 인스턴스	**X**	**X**						
WebSEAL을 사용하는 보안 관리자	**X**	**X*** **	**X**	**X**				
NetSEAL을 사용하는 보안 관리자	**X**	**X*** **	**X**		**X**			
WebSEAL 및 NetSEAL을 사용하는 보안 관리자	**X**	**X*** **	**X**	**X**	**X**			
권한 부여 서버	**X**	**X*** **				**X**		
권한 부여 서버 및 ADK	**X**	**X*** **				**X**	**X**	
관리 콘솔	**X**							**X**
모든 구성요소	**X**	**X*** **	**X**	**X**	**X**	**X**	**X**	**X**

******* 이것이 보안 도메인에 있는 첫번째 컴퓨터이거나 유일한 컴퓨터일 경우, 반드시 관리 서버(IVMgr)를 설치해야 합니다. 이것이 기존의 관리 서버를 사용하는 기존의 보안 도메인에 있는 추가 컴퓨터일 경우에는 그 밖의 다른 관리 서버를 설치하지 마십시오. 주어진 보안 도메인에 반드시 하나의 관리 서버만 있어야 합니다.

설치 전 필수 정보

Policy Director를 설치하기 전에 먼저 Policy Director 소프트웨어 설치에 필요한 시스템 정보를 적어두십시오.

Policy Director 서버

- 셀 관리자용 사용자 이름(cell_admin)
- 셀 관리자용 암호(cell_admin)
- WebSEAL: HTTP 포트(기본값)
- WebSEAL: 웹 문서 루트 디렉토리

NetSEAT 클라이언트(Windows 전용)

- 셀 이름
- 보안 서버 호스트 이름
- 시간 서버 호스트 이름
- 디렉토리 서비스 브로커 호스트 이름

터널 메커니즘

Policy Director는 암호화 데이터를 전송하는 데 있어서 다음 프로토콜을 지원합니다.

- SSL(Secure Sockets Layer) 터널링
- GSS(Generic Security Services) 터널링

WebSEAL은 SSL 암호화 터널이 제공하는 데이터 통합성과 데이터 프라이버시를 지원합니다. WebSEAL과 NetSEAL은 RPC를 지원합니다. RPC와 함께 통합성과 시간소인을 사용함으로써 *재생 개시(playback attacks)*에 대한 보호를 제공받을 수 있습니다. 재생 개시는 사용자 데이터가 해당 사용자 클라이언트와 서버 간에 이동할 때 캡처되면서 발생합니다. 이렇게 하면 해당 데이터가 처음 사용자를 구현하는 수단으로서 서버에 역으로 재생 또는 제공됩니다.

SSL 터널링: SSL 프로토콜은 신호 교환이 두 워크스테이션 간의 통신을 설정하는 것을 허용합니다. 이 프로토콜이 인터넷에서의 보안과 프라이버시를 제공합니다. SSL은 인증을 위한 공용 키를 사용하고 SSL 연결에서 전송되는 데이터 암호화에는 암호 키를 사용합니다.

Policy Director NetSEAL 서버에 대해 SSL 터널링을 사용할 때 SSL을 사용하는 것이 가능해집니다. 이 구성은 NetSEAT 클라이언트가 특정 포트를 보안하는 Policy Director NetSEAL 서버에 대해 SSL 클라이언트로서 제공될 때 사용됩니다(예를 들어, Telnet이 사용하는 포트).

Policy Director WebSEAL은 SSL 버전 2와 3을 지원합니다.

GSS 터널링: GSS API(GSS 인터페이스)는 응용 프로그램이 보안 서비스에 액세스할 수 있도록 해 주는 표준 방식입니다. GSS 터널링은 보안 RPC에서 사용

됩니다. Microsoft® Windows NT®용 Policy Director 또는 Policy Director 관리 콘솔에 대한 지원 모듈로 NetSEAT 클라이언트를 설치할 경우, 이 옵션을 사용하는 것이 가능합니다.

GSS 터널링은 일반적인 방식으로 호출자에게 보안 서비스를 제공합니다. 이것은 기초적인 메커니즘과 기술 범위로 지원이 가능합니다. 그리고 다른 환경으로 응용 프로그램의 소스 레벨을 이식하는 것을 허용합니다. GSS 터널링은 방향과 무관하게 양방향 트래픽에서 보호 레벨에 대한 제어를 가능하게 만듭니다. 예를 들어 서버로부터 클라이언트로의 데이터 이동이 보안되지 않더라도 클라이언트로부터 서버로의 데이터 이동을 일괄 데이터 암호화를 사용하여 완전하게 보호할 수 있습니다.

보안 도메인을 위한 설치 요구사항

Policy Director는 그 구성요소를 하나 이상의 컴퓨터에 다양한 구성으로 설치할 수 있는 고도의 분산 보안 시스템입니다. 다음 표에는 보안 도메인에 반드시 설치해야 하는 구성요소가 나옵니다.

- DCE 서비스
- 사용자 레지스트리(IBM SecureWay Directory는 사용자 레지스트리로 LDAP를 사용할 경우에만 필요합니다.)
- Policy Director 서버
- Policy Director 관리 콘솔
- Policy Director 권한 부여 ADK

기존의 DCE 또는 LDAP 설치를 사용할 경우에는 기존 설치가 올바른 레벨에 있는지를 확인해야 합니다. 올바른 레벨에 관해서는 16 페이지의 『기타 소프트웨어 요구사항』을 참조하십시오. Policy Director 제품을 설치하기 전에 다음의 상호 의존성을 알아보십시오.

분산 컴퓨팅 환경 서비스

각 Policy Director 보안 도메인(DCE 셀)에는 Policy Director 서버 간의 통신을 보안하기 위해 적어도 하나의 컴퓨터에 완전한 DCE 서비스를 설치해야 합니

다. DCE 서비스를 Policy Director 서버와 동일한 호스트에 상주시키거나 네트워크상의 원격 호스트에 배치할 수 있습니다.

DCE 설치에 관한 정보는 설치 및 관리 매뉴얼과 필요한 플랫폼을 위한 기술 지원 자원을 참조하십시오. DCD 문서 목록은 96 페이지의 『IBM DCE 문서』를 참조하십시오.

DCE 설치시 다음 지침을 참고하십시오.

- 단일 호스트 시스템에 새 Policy Director 보안 도메인을 작성하는 경우, 완전한 DCE 서버 설치를 수행하십시오.
- DCE 서버가 원격 호스트에 있으면 로컬 호스트에 Policy Director를 설치하여 새 보안 도메인을 작성하십시오.
- 기존 Policy Director 보안 도메인에 Windows NT용 Policy Director를 설치하는 경우, NetSEAT 클라이언트를 사용하여 필요한 DCE 서비스에 대한 액세스를 제공하십시오. Windows NT용 Policy Director 서버와 동일한 호스트에 NetSEAT 클라이언트를 설치하십시오.

사용자 레지스트리

Policy Director는 사용자 레지스트리로서 IBM SecureWay Directory(LDAP) 사용자 레지스트리나 DCE 사용자 레지스트리를 사용할 수 있습니다.

사용자 레지스트리로 LDAP를 사용할 경우, Policy Director를 설치하기 전에 반드시 LDAP 서버를 설치하고 구성해야 하며, 각 Policy Director 컴퓨터에도 LDAP 클라이언트를 설치해야 합니다.

LDAP 설치 정보는 *IBM SecureWay Directory 설치 및 구성, 버전 3.1.1*을 참조하십시오. 이 LDAP 문서 위치는 98 페이지의 『IBM SecureWay Directory 문서』를 참조하십시오.

또한 DCE 설치에 관한 정보는 96 페이지의 『IBM DCE 문서』에 나오는 DCE 제품 정보를 참조하십시오.

Policy Director 서버

다음은 Policy Director 서버 설치에 적용되는 요구사항입니다.

- 올바른 통신을 위해서는 모든 Policy Director Windows NT 서버에 Policy Director NetSEAT 클라이언트가 필요합니다.
- 모든 Policy Director 서버 설치에는 자동으로 설치가 이루어지는 기본 구성요소가 필요합니다.
- 보안 도메인에 *첫 컴퓨터*나 *하나의 컴퓨터만* 설치할 경우에는 컴퓨터에 반드시 관리 서버를 설치해야 합니다.
- 기존의 관리 서버를 가진 기존의 보안 도메인에 *추가* 컴퓨터를 설치할 경우에는 다른 관리 서버를 설치하지 마십시오. 주어진 보안 도메인에 반드시 하나의 관리 서버 인스턴스만 있어야 합니다.
- WebSEAL, NetSEAL, 써드 파티 권한 부여 서버 구성요소는 선택사항입니다.
- 보안 관리자는 WebSEAL과 결합하여 WebSEAL HTTP 서버 구성요소 및 정교한 HTTP 액세스 제어를 제공하고, NetSEAL과 결합하여 NetSEAL 비정교한 TCP/IP 액세스 제어 구성요소를 제공합니다.
- AIX 및 Solaris의 모든 Policy Director 서버에는 완전한 DCE 클라이언트와 (사용자 레지스트리로 LDAP를 사용할 경우에) LDAP 클라이언트가 필요합니다.

관리 콘솔

관리 콘솔에는 보안 도메인과 관리 서버를 설치 및 구성하는 것이 필요합니다. 또한 관리 콘솔에는 DCE 클라이언트와(관리 콘솔이 Windows 컴퓨터에 있는 경우에) NetSEAT 클라이언트가 필요합니다.

권한 부여 ADK

응용 프로그램 개발 컴퓨터에 Policy Director 권한 부여 ADK를 설치하십시오. 권한 부여 ADK는 보호된 써드 파티 서버에 사용자들이 액세스하는 것을 허용하는 응용 프로그램 개발에 사용됩니다. 권한 부여 ADK에는 권한 부여 ADK를 설치할 때 자동으로 설치되는 기본 구성요소가 필요합니다.

응용 프로그램을 실행하는 보안 도메인의 경우 최소한 하나의 컴퓨터에 반드시 권한 부여 서버를 설치해야 합니다. 일반적인 개발 환경에는 권한 부여 ADK와 동일한 시스템에 권한 부여 서버가 포함되어 있습니다.

단계별 Policy Director 설치 개요

Policy Director 설치에는 다음 단계가 필요합니다.

1. 이전 버전의 IBM SecureWay Policy Director가 설치되어 있으며, 현재의 설치를 이주시키려 할 때에는 Policy Director 웹 페이지에 있는 이주 정보를 참조하십시오(x 페이지의 『웹 정보』 참조).
2. 사용자의 운영체제에서 Policy Director의 지원 여부를 확인하십시오.

   지원 운영체제에 관한 정보는 16 페이지의 『Policy Director 서버』를 참조하십시오.
3. 사용자 요구사항에 적합한 서버 구성요소와 이 구성요소를 설치할 컴퓨터를 결정하십시오.

   지원 정보에 관해서는 19 페이지의 『공통 구성』을 참조하십시오.
4. 보안 도메인에서 SSL 터널링이나 GSS 터널링을 사용할 것인지 결정하십시오.

   자세한 정보는 22 페이지의 『터널 메커니즘』을 참조하십시오.
5. DCE 하부구조가 없으면 설치 및 구성하십시오.

   필수 DCE 서비스의 개요에 관해서는 23 페이지의 『분산 컴퓨팅 환경 서비스』를 참조하십시오.
6. 보안 도메인에서 LDAP 사용자 레지스트리나 DCE 사용자 레지스트리를 사용할 것인지 결정하십시오. 사용자 레지스트리에 IBM SecureWay Directory(LDAP)를 사용하고, 기존의 LDAP를 사용하지 않을 경우 LDAP를 설치 및 구성하십시오.

   LDAP 설치에 관한 하부구조 정보는 29 페이지의 『제4장 IBM SecureWay Directory 설치 및 구성』을 참조하십시오.
7. Policy Director 서버로 사용될 컴퓨터에 DCE와 LDAP 클라이언트를 설치하십시오.

   DCE 설치에 관한 정보는 96 페이지의 『IBM DCE 문서』에 나오는 DCE 제품 정보를 참조하십시오.
8. Policy Director 서버 구성요소를 설치하십시오.

사용할 운영체제 플랫폼에 관해서는 설치 장을 참조하십시오. 다음 중 하나를 사용할 수 있습니다.

- 45 페이지의 『제5장 Windows용 Policy Director 설치』
- 61 페이지의 『제6장 AIX용 Policy Director 설치』
- 79 페이지의 『제7장 Solaris용 Policy Director 설치』

9. 클라이언트 인증서 인증에 대해 Policy Director CAS를 사용하는 경우, Policy Director CAS를 구성하십시오.

   Policy Director CAS에 관한 정보는 『인증 획득 서비스 구성』을 참조하십시오.

10. 관리 콘솔을 설치하십시오.

    사용할 운영체제 플랫폼에 관해서는 설치 장을 참조하십시오. 다음 중 하나를 사용할 수 있습니다.

    - Windows NT의 경우 55 페이지의 『Windows에서 관리 콘솔 설치』를 참조하십시오.
    - AIX의 경우 DCE 사용자 레지스트리를 사용할 때에는 75 페이지의 『관리 콘솔 설치』, LDAP 사용자 레지스트리를 사용할 때에는 66 페이지의 『관리 콘솔 구성 및 시작』을 참조하십시오.
    - Solaris의 경우 91 페이지의 『관리 콘솔 설치』를 참조하십시오.

Policy Director 재설치

패키지를 다시 설치해야 할 경우에는 먼저 기존의 패키지를 제거한 다음 원하는 패키지를 다시 설치해야 합니다. 그 방법은 76 페이지의 『Policy Director 제거』를 참조하십시오.

인증 획득 서비스 구성

Policy Director CAS(인증 획득 서비스)는 사용자 조정이 가능한 Policy Director의 구성요소로서 WebSEAL이 지원하는 표준 인증 메커니즘의 확장에 사용할 수 있습니다.

Policy Director CAS는 자동으로 설치됩니다. Policy Director CAS를 인증 획득 서비스로 사용하려 할 때에는 반드시 구성해야 합니다. Policy Director CAS의 이해 및 구성에 관한 정보는 *Policy Director Administration Guide*의 2장과 12장을 참조하십시오.

제4장 IBM SecureWay Directory 설치 및 구성

DCE 사용자 레지스트리를 사용할 계획이면 IBM SecureWay Directory(LDAP) 설치 및 구성 섹션을 건너뛸 수 있습니다.

Policy Director 설치시 LDAP 사용자 레지스트리나 DCE 사용자 레지스트리 중 선택할 것을 요구받습니다.

- LDAP를 선택할 경우에는 반드시 IBM SecureWay Directory 버전 3.1.1(LDAP) Client SDK와 서버를 설치한 다음, Policy Director를 설치하기 전에 LDAP 서버를 구성해야 합니다.
- SSL을 사용하여 LDAP 서버에 액세스할 경우에는 LDAP 클라이언트도 반드시 구성해야 합니다.

LDAP 서버 및 클라이언트 설치

LDAP를 사용자 레지스트리로 사용할 경우, Policy Director에 LDAP 서버와 클라이언트가 필요합니다.

보안 도메인의 적어도 한 컴퓨터에는 반드시 LDAP 서버가 있어야 합니다. LDAP 클라이언트와 서버는 Policy Director 제품의 일부로 제공됩니다. 이 제품들을 Policy Director 설치 전에 반드시 설치하거나 기존에 설치되어 있던 올바른 레벨의 LDAP를 사용할 수 있습니다.

LDAP를 설치할 때 **SecureWay Directory와 Client SDK** 설치를 선택하십시오.

LDAP 설치 및 구성에 관한 자세한 정보는 *IBM SecureWay Directory 설치 및 구성, 버전 3.1.1* 서적을 참조하십시오. 해당 CD마다 지원되는 각 운영체제별로 이 책에 대한 별도의 버전이 HTML 형식으로 준비되어 있습니다. 액세스 방법에 관한 정보는 98 페이지의 『IBM SecureWay Directory 문서』를 참조하십시오.

LDAP 클라이언트만 설치

사용자 레지스트리로 LDAP를 사용할 경우, Policy Director를 실행할 각 시스템에 반드시 LDAP 클라이언트를 설치해야 합니다. LDAP 클라이언트는 Policy Director 제품의 일부로 제공됩니다. Policy Director를 설치하기 전에 LDAP 클라이언트를 설치하십시오.

LDAP를 설치할 때 이미 Policy Director에 대해 설치 및 구성된 올바른 레벨에서 LDAP 서버를 기존에 설치했다면, **SecureWay Client SDK**만 설치하도록 선택하십시오.

LDAP 서버 구성

사용자 레지스트리로 LDAP를 사용할 경우, 첫 Policy Director 서버를 설치하기 전에 반드시 LDAP 서버를 구성해야 합니다. 첫 Policy Director 시스템에 대해 LDAP 서버를 구성했으면, 추가적인 Policy Director 서버를 추가할 때 LDAP 서버를 다시 구성하지 않아도 됩니다.

LDAP 서버 구성시 SSL이 LDAP 서버에 액세스하는 것이 가능하다면 SSL 액세스를 사용하는 추가의 각 컴퓨터에 클라이언트 및 서버 키 링 쌍을 복사해야 합니다. 자세한 정보는 34 페이지의 『SSL 액세스 사용 가능(선택사항)』을 참조하십시오.

LDAP 서버를 구성하기 위해서는 다음 목록에 나오는 구성 단계를 각 보안 도메인에 대해 한 번만 완료해야 합니다.

1. 필요한 접미어를 추가하십시오. 그 방법은 31 페이지의 『접미어 추가』를 참조하십시오.
2. 보안 스키마 오브젝트와 속성을 설치하십시오. 32 페이지의 『보안 스키마 오브젝트 및 속성 설치』를 참조하십시오.
3. LDAP 액세스 제어를 사용 가능하게 만드십시오. 그 방법은 43 페이지의 『LDAP 액세스 제어 사용 가능』을 참조하십시오.
4. SSL 액세스를 사용 가능하게 만드십시오. 그 방법은 34 페이지의 『SSL 액세스 사용 가능(선택사항)』을 참조하십시오.

SSL 액세스를 사용 가능하게 했으면, SSL을 사용하여 LDAP 서버에 액세스하는 LDAP 클라이언트(Policy Director 서버)를 추가할 때마다 40 페이지의 『SSL 액세스를 위한 LDAP 클라이언트 설정』에 나오는 단계를 완료하십시오.

주: LDAP 관리자가 LDAP 데이터베이스에 있는 암호의 암호화 설정값을 지정할 수 있습니다. LDAP는 암호를 명확한 텍스트로 저장하도록 허용함으로써 이것이 보안 노출의 원인이 될 수 있습니다. 적절한 암호화 레벨로 사용자 암호 속성을 설정하는 것에 관한 설명은 LDAP 문서를 참조하십시오.

접미어 추가

IBM SecureWay Directory에서 다음 단계를 완료해 새로운 접미어를 작성하십시오.

1. 웹 브라우저를 사용하여 아래 웹 주소에서 IBM SecureWay Directory Server 웹 관리 툴에 액세스하십시오.

   `http://servername/ldap`

   LDAP 관리자로서 웹 인터페이스를 통해 로그인하십시오(예를 들어, `cn=root`).
2. 누르기: **접미어 → 접미어 추가**.
3. **접미어 DN** 필드에는 반드시 접미어를 추가시켜야 합니다.

   `secAuthority=Default`

   관리 서버를 구성하는 중 `secAuthority=Default`에 대한 오브젝트가 작성됩니다.
4. **새로운 접미어 추가** 단추를 누르십시오.
5. 다른 접미어를 추가하려면 **접미어 추가** 링크를 눌러 이전 창으로 가십시오.
6. 필요하다면 Policy Director 사용자 및 글로벌 사인온(GSO) 데이터에 대한 접미어를 추가하십시오. 예를 들면, 다음과 같습니다.

   `o=IBM,c=US`

   사용자 설치에 적합한 방식으로 마음대로 접미어를 지정할 수 있으며, `o=`는 사용자 조직의 약식 이름, `c=`는 국가별 정보입니다.

이 단계는 GSO 데이터와 사용자 및 그룹에 대한 접미어를 작성합니다. 이 접미어들은 LDAP 웹 관리 툴로 작성됩니다.

7. **새로운 접미어 추가** 단추를 누르십시오.
8. 추가를 원하거나 조직에 필요한 각각의 새로운 접미어에 대해 절차를 반복하십시오.
9. 현재 LDAP 관리 툴 웹 페이지에 있는 **서버 재시작** 링크를 눌러 접미어를 모두 추가한 후 LDAP 서버를 재시작하십시오.

보안 스키마 오브젝트 및 속성 설치

Policy Director는 LDAP 오브젝트 및 속성 세트를 사용하여 LDAP 서버 안에 있는 사용자 인증사항을 유지보수합니다.

보안 오브젝트와 속성이 설치되었는지 알아보려면 IBM SecureWay Directory Management Tool(DMT)을 사용하십시오. 오브젝트와 속성이 나오지 않으면 설치하십시오. DMT는 IBM SecureWay Directory 패키지의 일부로 설치됩니다.

Policy Director 보안 오브젝트와 속성이 설치되었는지 알아보려면 다음 단계를 완료하십시오.

1. LDAP 클라이언트에서 Directory Management 툴을 시작하십시오.

   주: secAuthority=Default 접미어 항목이 없다는 메시지를 수신할 경우 그대로 진행할 수 있습니다. 관리 서버를 구성하는 중 secAuthority=Default에 대한 오브젝트가 작성됩니다.

2. **스키마 → 오브젝트 클래스 → 오브젝트 클래스 보기**를 누르십시오.
3. 다음의 모든 Policy Director 오브젝트와 속성이 나오는지 확인하십시오.

   오브젝트 클래스
   secAuthorityInfo
   secGroup
   secMap
   secPolicy
   secPolicyData
   secUser

4. **스키마 → 속성 → 속성 보기**를 누르십시오.
5. 다음의 모든 Policy Director 오브젝트와 속성이 나오는지 확인하십시오.

속성
secUUID
secLoginType
secAuthority
secAcctValid
secPwdValid
secDN
secPwdMgmtBind
secAcctExpires
secAcctInactivity
secAcctLife
secPwdAlpha
secPwdSpaces
secPwdFailures
secPwdLastChanged
secPwdLastUsed

6. 32 페이지의 3 단계와 32 페이지의 5 단계에서 찾은 값에 기초하여 다음 중 하나를 수행하십시오.
   - 모든 오브젝트가 나올 경우에는 더 이상의 조치가 필요 없습니다. 34 페이지의 『SSL 액세스 사용 가능(선택사항)』으로 계속하십시오.
   - 오브젝트의 전부는 아니더라도 *일부*가 나올 경우에는 7단계로 가십시오.
   - 오브젝트가 *하나*도 나오지 않을 경우에는 8단계로 가십시오.
7. Policy Director 오브젝트와 속성의 전부는 아니더라도 일부를 찾은 경우에는 기존의 Policy Director 오브젝트와 속성을 제거하십시오.

   DMT에서 다음과 같이 누르십시오.

   스키마 → 오브젝트 클래스 → 오브젝트 클래스 삭제를 눌러 오브젝트 클래스를 제거하십시오.

   다음에는 **스키마 → 속성 → 속성 삭제**를 눌러 속성을 제거하십시오.
8. Policy Director 오브젝트와 속성을 하나도 찾지 못한 경우에는 *IBM SecureWay Policy Director 버전 3.0* CD를 넣으십시오.
9. 명령 프롬프트에서 **ldapmodify**를 사용하여 스키마 파일을 로드하십시오. 예를 들어, 다음과 같이 입력할 수 있습니다.

   UNIX:

   ```
   ldapmodify -h hostname -p 389 -D cn=root -w password -f /schema/secschema.def
   ```

   Windows:

```
ldapmodify -h hostname -p 389 -D cn=root -w password -f x:\schema\secschema.def
```

*x:*는 사용자의 Windows CD-ROM 드라이브의 드라이브 문자입니다.

10. Policy Director를 사용하여 SecureWay Boundary Server 사용자들을 관리할 계획이면, Policy Director 스키마 파일에서 나온 오브젝트와 속성도 반드시 추가해야 합니다.

    명령 프롬프트에서 **ldapmodify** 명령으로 스키마 파일을 로드하십시오. 예를 들어, 다음과 같이 입력할 수 있습니다.

    Windows:

    ```
    ldapmodify -h hostname -p 389 -D cn=root -w password -f x:\schema\puschema.def
    ```

    UNIX:

    ```
    ldapmodify -h hostname -p 389 -D cn=root -w password -f /schema/puschema.def
    ```

    *x:*는 사용자의 CD-ROM 드라이브의 드라이브 문자입니다.

SSL 액세스 사용 가능(선택사항)

LDAP 서버로의 SSL 액세스가 필요 없으면 이 섹션을 건너뛸 수 있습니다. 43 페이지의 『LDAP 액세스 제어 사용 가능』으로 가십시오.

LDAP 서버에 SSL 액세스가 필요하면 이 섹션을 계속하십시오. 이 절차는 LDAP 서버와 LDAP 클라이언트 간에 처음으로 SSL 통신을 설정할 때만 수행하면 됩니다.

Policy Director 서버와 LDAP 서버 간의 통신 보안을 위해 선택적으로 SSL을 사용 가능하게 만들 수 있습니다.

GSKit(IBM Global Security Kit) SSL Runtime Toolkit 버전 3.0.1은 LDAP를 설치하는 중에 설치됩니다. GSKit는 두 개의 Key Management Tool—한 버전은 창을 사용하는 버전인 **ikmguiw**이고, 다른 하나는 창을 사용하지 않는 버전인 **ikmgui**입니다. 다음 절차를 통해 **ikmguiw**가 호출될 때마다 각 버전을 사용할 수 있습니다.

LDAP 문서에서 나오는 툴 사용법에 따라 작업하십시오. 자세한 정보는 98 페이지의 『IBM SecureWay Directory 문서』를 참조하십시오.

또는 특별히 SSL 액세스를 위해 Policy Director를 사용 가능하게 만드는 약식 절차를 사용할 수 있습니다.

키 데이터베이스 파일 및 인증서 작성

LDAP 서버에서 SSL 지원을 사용할 수 있도록 하려면 서버에 인증서를 식별하고 *개인용 인증서*로 사용할 수 있는 인증서가 반드시 있어야 합니다. 이 개인용 인증서는 클라이언트가 서버를 인증할 수 있도록 허용하기 위해 서버가 클라이언트로 전송한 인증서입니다. 키 데이터베이스 파일에는 인증서와 공용 및 개인용 키 쌍이 저장되어 있습니다. 일반적으로 사용자들은 Verisign과 같은 CA(Certificate Authority)로부터 *서명된 인증서*를 확보합니다.

그러나, *자체 서명* 인증서를 사용할 수도 있습니다. 자체 서명 인증서를 사용할 경우 인증서를 생성한 시스템이 CA입니다.

키 데이터베이스 파일과 인증서를 작성할 경우, GSKit Key Management Tool(**ikmguiw**)을 사용할 수 있습니다. 키 데이터베이스 파일과 인증서(자체 서명 또는 서명된)를 작성하려면, 다음과 같이 하십시오.

1. IBM Global Security Kit(GSKit) SSL Runtime Toolkit 버전 3.0.1과 Java용 Key Management Tool이 SSL을 사용할 LDAP 서버와 LDAP 클라이언트 모두에 설치되었는지 확인하십시오.

   Windows: `C:\Program Files\IBM\GSK\bin\ikmguiw.exe`

   Solaris: `/opt/IBM/GSK/bin/ikmguiw`

   AIX: `/usr/lpp/ibm/gsk/bin/ikmguiw`
2. IBM Key Management 툴(**ikmguiw**)을 시작하십시오.
3. **키 데이터베이스 파일 → 신규**를 누르십시오.
4. **CMS 키 데이터베이스 파일**이 선택한 키 데이터베이스 유형인지 확인하십시오.
5. 키 데이터베이스 파일이 위치할 **파일 이름**과 **위치** 필드에 정보를 입력하십시오. 키 데이터베이스 파일 확장자는 *.kdb*입니다.
6. **확인**을 누르십시오.
7. 키 데이터베이스 파일 암호를 입력한 후 확인하십시오.

이 암호는 키 데이터베이스 파일을 편집할 때 필요하므로 반드시 기억하십시오.

8. 기본 만기 시간을 허용하거나 사용자 부서의 요구사항에 따라 변경하십시오.
9. 암호를 마스크하여 은닉(stash) 파일에 저장하려는 경우 **파일로 암호 은닉**을 누르십시오.

   은닉 파일이 일부 응용 프로그램에 의해 사용될 수 있으므로, 응용 프로그램이 키 데이터베이스 파일을 사용하기 위한 암호를 알아서는 안됩니다. 은닉 파일에는 키 데이터베이스 파일과 동일한 위치 및 이름이 있으며, *.sth* 확장자가 있습니다.
10. **확인**을 누르십시오.

이로써 키 데이터베이스 파일 작성을 완료했습니다. 그리고 설정 서명자 인증서 세트가 준비되었습니다. 이 서명자 인증서가 바로 인식된 기본 인증 권한입니다.

개인용 인증서 작성

CA(예를 들어, VeriSign)로부터의 인증서를 사용할 계획이면, 반드시 CA(Certificate Authority)로부터 인증서를 요청하고 요청이 완료된 다음에 수신해야 합니다. 『인증서 수신』에 나오는 단계를 완료하십시오.

인증서 수신: 자체 서명 인증서 대신 CA(예를 들어, VeriSign)로부터의 인증서를 사용 중이면 다음 단계를 완료하십시오.

1. **ikmguiw**를 사용하여 CA로부터 인증서를 요청한 다음 키 데이터베이스 파일에 새로운 인증서를 수신하십시오.
2. 키 데이터베이스 파일의 **개인용 인증서 요청** 섹션을 누르십시오.
3. **신규**를 누르십시오.
4. 모든 정보를 입력하여 인증 권한으로 송신할 수 있는 요청을 작성하십시오.
5. **확인**을 누르십시오.
6. CA가 인증서를 리턴했으면 **개인용 인증서** 섹션과 **수신**을 차례로 눌러 키 데이터베이스 파일 안으로 설치할 수 있습니다.
7. 키 데이터베이스 파일에 LDAP 서버의 인증서가 작성되었으면 SSL 서버를 사용 가능하게 만들 LDAP 서버를 구성할 수 있습니다.

사용자의 인증서가 아직 인식되지 않은 경우에는 CA(Certificate Authority) 인증서를 클라이언트 시스템으로 복사하십시오.

사용자 인증서를 이미 인식된 CA(예를 들어, VeriSign)가 생성한 경우에는 더 이상의 조치가 필요 없습니다. 39 페이지의 『SSL이 사용 가능하도록 LDAP 서버 구성』으로 가십시오.

자체 서명 인증서 작성: 자체 서명 인증서 대신 CA(예를 들어, VeriSign)으로부터의 인증서를 사용할 계획이면 다음 단계를 완료하십시오. 36 페이지의 『인증서 수신』을 참조하십시오.

새로운 자체 서명 인증서를 작성하여 키 데이터베이스에 저장하려면 다음과 같이 하십시오.

1. **작성 → 새로운 자체 서명 인증서**를 누르십시오.
2. 이 신규 인증서를 키 데이터베이스 파일에서 식별하기 위해 사용할 수 있는 **키 레이블** 필드에 이름을 입력하십시오.

   예를 들면, LDAP 서버의 시스템 이름이 레이블일 수 있습니다.
3. **버전** 필드의 기본값인 X509 V3과 **키 크기** 필드의 기본값을 허용하십시오.
4. 기본 시스템 이름을 허용하거나 이 인증서에 대한 **공통 이름** 필드에 다른 DN(distinguished name)을 입력하십시오.
5. **조직** 필드에 회사 이름을 입력하십시오.
6. 선택적 필드를 완성하거나 공백으로 남겨 두십시오.
7. **국가별 정보** 필드의 기본값 및 **유효 기간** 필드의 365를 허용하거나 사용자 조직에 맞게 변경하십시오.
8. **확인**을 누르십시오.

   GSKit이 신규 공용 및 개인용 키 쌍을 생성하고 인증서를 작성합니다.

   GSKit는 키 데이터베이스 파일에 하나 이상의 개인용 인증서가 있을 경우, 사용자가 이 키를 데이터베이스의 기본 키로 사용할 것인지 조회합니다. 기본값으로 그 가운데 하나를 허용할 수 있습니다. 사용자 인증서를 선택하기 위한 레이블이 제공되지 않을 경우에는 기본 인증서가 런타임에 사용됩니다.

이로써 LDAP 서버의 개인용 인증서 작성을 완료했습니다. 따라서 인증서가 키 데이터베이스의 개인용 인증서 섹션에 표시되어야 합니다. 키 데이터베이스 파일에서 보유하고 있는 인증서 유형 중 선택하려면 Key Management Tool의 중간 막대를 사용하십시오.

다음에는 LDAP 서버의 인증서를 Base64 암호화 ASCII 데이터 파일로 발췌해야 합니다.

자체 서명 인증서 발췌

사용자의 인증서가 자체 서명 인증서인 경우에는 키 데이터베이스 파일로부터 서명자 인증서를 반드시 발췌해야 합니다. 발췌 절차를 진행하십시오.

발췌는 클라이언트 시스템을 설정하는 데 사용됩니다. 37 페이지의 『자체 서명 인증서 작성』에서 자체 서명 인증서를 작성했다면 발췌 또한 키 데이터베이스 파일의 서명자 인증서 섹션에 표시되어야 합니다(발췌는 자체 서명 인증서입니다). 사용자가 키 데이터베이스의 서명자 인증서 섹션에 있을 경우, 그 곳에 신규 인증서가 있는지 확인하십시오.

서명자 인증서를 발췌하려면 다음과 같이 하십시오.

1. **ikmguiw**를 사용하여 LDAP 서버의 인증서를 Base64 암호화 ASCII 데이터 파일로 발췌하십시오. 이 파일이 40 페이지의 『SSL 액세스를 위한 LDAP 클라이언트 설정』에 나오는 절차에 사용됩니다.
2. 37 페이지의 『자체 서명 인증서 작성』에 추가한 자체 서명 인증서를 강조표시하십시오.
3. **인증서 발췌**를 누르십시오.
4. 데이터 유형으로 **Base64 암호화 ASCII 데이터**를 누르십시오.
5. 새로 발췌한 인증서에 대해 인증서 파일 이름을 입력하십시오. 인증서 파일의 확장자는 *.arm*입니다.
6. 발췌한 인증서를 저장할 위치를 입력하십시오.
7. **확인**을 누르십시오.
8. 발췌한 인증서를 LDAP 클라이언트 시스템에 복사하십시오.
9. SSL이 사용되도록 LDAP 서버를 구성할 수 있습니다.

SSL이 사용 가능하도록 LDAP 서버 구성

SSL이 사용 가능하도록 LDAP 서버를 구성하려면 다음과 같이 하십시오.

1. 사용자 레지스트리로 LDAP를 사용할 경우, LDAP 서버가 설치되어 실행 중인지 확인하십시오. 자세한 정보는 29 페이지의 『제4장 IBM SecureWay Directory 설치 및 구성』을 참조하십시오.
2. 다음 URL과 함께 웹 기반 LDAP 관리 툴을 사용하십시오.

   `http://`*servername*`/ldap`

   *servername*은 LDAP 서버 시스템의 이름입니다.
3. 아직 로그온하지 않았으면 LDAP 관리자(예를 들어, cn=root)로 로그온하십시오.
4. **서버 → SSL**을 누르십시오.
5. SSL과 비 SSL 모두에 대해 **SSL 작동**을 누르거나 설정하려는 SSL 상태에 대해 **SSL만**을 누르십시오.
6. 인증 메소드의 유형에 대해 **서버 인증**을 누르십시오.
7. 포트 번호를 입력하거나 기본 포트 번호인 636을 허용하십시오.
8. 키 데이터베이스 파일 및 인증서 작성에 나오는 5단계에서 지정했던 키 데이터베이스 경로 및 파일 이름을 입력하십시오.

   키 데이터베이스 파일 확장자는 *.kdb*입니다.
9. LDAP 서버 인증서를 키 데이터베이스에 저장할 때 식별을 위해 사용한 **키 레이블** 필드에 이름을 입력하십시오. 예를 들면, LDAP 서버의 시스템 이름이 레이블일 수 있습니다.
10. 키 데이터베이스 파일 암호를 입력한 후 확인하십시오. 또한 LDAP 서버가 은닉 파일을 사용하도록 할 경우에는 암호 필드를 공백으로 남겨둘 수 있습니다.
11. **적용**을 누르십시오.
12. **서버 재시작** 링크를 눌러 LDAP 서버를 다시 시작하고 변경사항을 유효하게 만들 수 있습니다.

SSL 액세스 테스트: SSL이 사용 가능한지를 검사하려면 LDAP 서버 명령줄로부터 다음 명령을 입력하십시오.

```
ldapsearch -h servername -Z -K keyfile -P key_pw -b "" -s base \
objectclass=*
```

이 명령에서 역슬래쉬(\)는 명령이 한 줄에 들어가지 않을 때에만 필요합니다.

다음은 각 항목에 대한 설명입니다.

옵션	설명
servername	LDAP 서버의 DNS 호스트 이름
keyfile	생성된 키 링의 완전한 경로
key_pw	생성된 키 링의 암호

이 명령은 LDAP 서버상의 접미어를 포함하고 있는 LDAP 기본 정보를 리턴합니다.

이로써 서버 SSL 설정을 완료했습니다. 다음에는 SSL 액세스를 위한 LDAP 클라이언트를 설정하십시오.

SSL 액세스를 위한 LDAP 클라이언트 설정

SSL 액세스를 위한 LDAP 서버를 설정했으면 SSL 액세스를 위한 LDAP 클라이언트를 설정해야 합니다.

키 데이터베이스 파일 작성: 클라이언트에 GSKit이 설치되었는지 확인한 다음 35 페이지의 『키 데이터베이스 파일 및 인증서 작성』에서 설명한 IBM Key Management Tool을 사용하여 신규 키 데이터베이스 파일을 작성하십시오.

클라이언트가 LDAP 서버를 인증하도록 하기 위해서는 클라이언트가 LDAP 서버의 인증서를 작성한 CA(서명자)을 반드시 인식해야 합니다. LDAP 서버가 자체 서명 인증서를 사용 중이면, 클라이언트가 신뢰할 수 있는 루트로서 LDAP 서버 인증서를 생성한 시스템을 알 수 있어야 합니다(CA).

서명자 인증서 추가: 키 데이터베이스 파일 작성 후 서명자 인증서를 추가하려면 다음과 같이 하십시오.

1. 38 페이지의 『자체 서명 인증서 발췌』의 키 데이터베이스 파일로부터 발췌한 인증서를 클라이언트 시스템으로 복사했는지 확인하십시오. 복사하지 않았다면 지금 복사하십시오.
2. 클라이언트 CMS 키 데이터베이스 파일의 **서명자 인증서** 섹션을 누르십시오.

3. **추가**를 누르십시오.
4. **Base64 암호화 ASCII 데이터**를 눌러 데이터 유형을 설정하십시오.
5. 인증서의 파일 이름과 위치를 나타내십시오. 인증서 파일의 확장자는 *.arm*입니다.
6. **확인**을 누르십시오.
7. 추가하려는 서명자 인증서에 대해 레이블을 입력하십시오. 예를 들면, LDAP 서버의 시스템 이름을 레이블로 사용할 수 있습니다.
8. **확인**을 누르십시오.

   자체 서명 인증서가 서명자 인증서로서 클라이언트의 키 데이터베이스에 표시됩니다.
9. 새로 추가한 서명자 인증서를 강조표시하고 **보기/편집**을 누르십시오.
10. **신뢰할 수 있는 루트로서 인증서 설정**이 선택되었는지 확인하여 신뢰할 수 있는 루트로 표시되도록 하십시오.

    일반적인 인증 권한에 의해 LDAP 서버의 인증서가 생성된 경우에는 인증 권한이 서명자 인증서로서 목록에 나오고 신뢰할 수 있는 루트로 표시되어 있는지 확인하십시오. 그렇지 않은 경우에는 서명자 인증서로서 인증 권한의 인증서를 추가한 다음 그것이 신뢰할 수 있는 루트임을 나타내십시오.

이 때 클라이언트가 LDAP 서버를 사용하여 SSL 세션을 설정할 수 있어야 합니다.

SSL 사용 가능 테스트: SSL이 사용 가능한지를 검사하려면 LDAP 클라이언트 명령줄로부터 다음 명령을 입력하십시오.

```
ldapsearch -h servername -Z -K client_keyfile -P key_pw -b "" \
-s base objectclass=*
```

이 명령에서 역슬래쉬(\)는 명령이 한 줄에 들어가지 않을 때에만 필요합니다.

다음은 각 항목에 대한 설명입니다.

옵션	설명
servername	LDAP 서버의 DNS 호스트 이름
client_keyfile	생성된 키 링의 완전한 경로
key_pw	생성된 키 링의 암호

이 명령은 LDAP 서버상의 접미어를 포함하고 있는 LDAP 기본 정보를 리턴합니다.

이로써 SSL 설정을 완료했습니다.

LDAP 서버 및 클라이언트 인증 유형 사용(선택사항)

이 구성 섹션은 선택사항입니다.

1. 39 페이지의 『SSL이 사용 가능하도록 LDAP 서버 구성』에서 설명한 절차를 완료하십시오. 그러나 **서버 인증**을 위해 LDAP 서버를 구성하는 대신 **서버 및 클라이언트 인증** 둘 다 수행하도록 선택하십시오.

   이 경우 서버가 그 인증서를 클라이언트로 전송하고 클라이언트가 인증하면, 서버가 클라이언트의 인증서를 요청합니다. LDAP 서버가 둘 다를 위해 구성된 경우에는 클라이언트 시스템을 위해서도 인증서를 설정해야 합니다.
2. 클라이언트 시스템에서는 클라이언트 시스템을 위한 인증서 설정 작업이 다음 절차에 나오는 설명에 따라 이루어집니다.
   - 35 페이지의 『키 데이터베이스 파일 및 인증서 작성』
   - 인증서가 자체 서명 인증서인 경우는 37 페이지의 『자체 서명 인증서 작성』, 인증서가 서명자 인증서인 경우는 36 페이지의 『인증서 수신』
   - 38 페이지의 『자체 서명 인증서 발췌』
   - 39 페이지의 『SSL이 사용 가능하도록 LDAP 서버 구성』
3. LDAP 서버에서 클라이언트의 개인용 인증서를 작성하여 키 데이터베이스 파일에 추가한 후에는 해당 클라이언트 인증서를 작성한 CA(Certificate Authority)가 서명자 인증서(신뢰할 수 있는 루트)로서 반드시 인식되어야 합니다. 인증 권한은 40 페이지의 『서명자 인증서 추가』에 나오는 설명과 같이 LDAP 서버의 키 데이터베이스에 추가됩니다.

SSL 액세스 테스트: 클라이언트의 개인용 인증서를 작성한 인증 권한을 LDAP 서버가 인식하면 다음 명령을 사용하여 설정을 검사할 수 있습니다.

```
ldapsearch -h servername -Z -K client_keyfile -P key_pw -N client_label \
-b "" \ -s base objectclass=*
```

이 명령에서 역슬래쉬(\)는 명령이 한 줄에 들어가지 않을 때에만 필요합니다.

다음은 각 항목에 대한 설명입니다.

옵션	설명
servername	LDAP 서버의 DNS 호스트 이름
client_keyfile	생성된 클라이언트 키 링의 완전한 경로
key_pw	생성된 키 링의 암호
client_label	키와 연관된 레이블(있을 경우). 이 필드는 선택적 필드로서 LDAP 서버가 서버와 클라이언트 인증 모두를 수행하도록 구성된 경우에만 필요합니다.

이 명령은 LDAP 서버의 접미어를 포함하고 있는 LDAP 기본 정보를 리턴합니다. **-N** 매개변수는 클라이언트의 개인용 인증서가 클라이언트의 키 데이터베이스 파일에 추가되었을 때 지정된 레이블을 나타낸다는 점에 유의하십시오.

LDAP 서버의 서명자 인증서 레이블은 지정하지 마십시오. **-N** 매개변수는 요청이 있을 때 서버로 전송되는 클라이언트 인증서를 GSKit에 나타냅니다. 지정된 레이블이 없으면 서버가 클라이언트의 인증서를 요청할 때 기본 개인용 인증서가 전송됩니다.

이로써 SSL 설정을 완료했습니다.

LDAP 액세스 제어 사용 가능

LDAP 사용자 레지스트리로 Policy Director 보안을 통합하려면, 다음 단계를 완료하여 사용자 레지스트리를 제어하는 LDAP ACL을 갱신하십시오.

1. **시작 → 프로그램 → IBM SecureWay Directory → Directory Management Tool**을 눌러 LDAP 클라이언트나 LDAP 서버로부터 Directory Management Tool을 시작하십시오.
2. 다음과 같이 서버를 리바인드하십시오.
   a. **서버 → 리바인드**를 누르십시오.
   b. **인증**을 누르십시오.
   c. 사용자 DN(예를 들어, cn=root)을 입력하십시오.
   d. 암호를 입력하십시오.
   e. **확인**을 누르십시오.

3. 표시되는 각각의 경고 메시지에 대해 **확인**을 누르거나 경고 메시지 창을 닫으십시오.
4. 31 페이지의 『접미어 추가』에서 작성한 접미어에 Policy Director 보안 디먼 그룹 제어를 부여하십시오.
   a. **항목 → 항목 추가**를 누르십시오.
   b. **항목 RDN**에 Policy Director 사용자와 GSO 사용자 데이터베이스를 위한 접미어를 입력하십시오. 예를 들면, 다음과 같이 할 수 있습니다.

      ```
      o=IBM,c=US
      ```

   c. **조직**을 누르십시오.
   d. **다음**을 누르십시오.

      LDAP 항목 작성 창이 나옵니다.
   e. 사용자 조직에 대한 적절한 정보를 추가한 다음 **작성** 단추를 누르십시오.
   f. **트리 → 트리 최신 정보로 고침**을 누르면 찾아보기 디렉토리 트리에 새 항목이 나옵니다.
5. 제어 중인 각 LDAP ACL의 소유자 목록에 다음을 추가하여 Policy Director 보안 디먼 그룹에 완전한 제어를 부여하십시오.

   ```
   cn=SecurityGroup,secAuthority=Default
   ```

   이는 **ACL** 탭을 눌러 작업할 수 있습니다.

   LDAP ACL 편집 창이 나옵니다.
   a. DN 필드에 `cn=SecurityGroup,secAuthority=Default`를 입력한 다음, 드롭다운 목록으로부터 **그룹**을 누르십시오.
   b. **추가** 단추를 누르십시오.
   c. 추가, 삭제, 클래스에 부여된 권한에서 모든 선택란을 선택하십시오.
   d. 완료했을 때 **변경**을 누르면 `cn=SecurityGroup,secAuthority=Default`가 접미어 DN에 대한 ACL 목록에 나옵니다.
   e. 소유자 목록에 추가할 것이 여러 개일 경우, 접미어 각각에 대해 절차를 반복하십시오.

이로써 LDAP 구성을 완료했습니다.

제5장 Windows용 Policy Director 설치

이 장의 각 섹션에서는 지원되는 Windows와 Windows NT 플랫폼에 Policy Director를 설치 및 구성하는 방법을 설명합니다.

Policy Director 설치를 시작할 때에는 먼저 『Windows용 Policy Director를 설치하기 전에』에 나오는 정보를 검토했는지 확인하십시오.

Windows용 Policy Director를 설치하기 전에

NetSEAT와 Policy Director를 설치할 때에는 먼저 다음 정보를 읽어보십시오.

- NetSEAT와 Policy Director를 설치하기 위해서는 먼저 Windows NT 서버를 설치하고 구성해야 합니다.
- Windows NT 도메인 관리자와 보안 도메인 관리자의 암호를 알아야 합니다 (예를 들어, cell_admin account). 관리자 권한을 확보하도록 하십시오.
- Windows NT 운영체제에 Policy Director 서버를 설치할 때, 신규 DCE 셀을 작성하는 중이면 다음을 참조하십시오.
  - DCE 서버 또한 설치 및 구성해야 합니다.
  - 사용자 레지스트리에 LDAP를 사용 중이면, LDAP 서버 또한 설치 및 구성해야 합니다.
- 23 페이지의 『보안 도메인을 위한 설치 요구사항』에 나오는 Policy Director 전개에 관한 모든 정보를 잘 이해하고 있어야 합니다.

NetSEAT 및 Policy Director 설치

Policy Director 설치를 시작할 때에는 먼저 모든 응용 프로그램을 닫았는지 확인하십시오. Policy Director 설치를 완료했으면 컴퓨터를 껐다가 다시 켜십시오.

보안 도메인 인벤토리 완성

설치 중에는 사용자 보안 도메인 구성에 고유한 다음의 정보를 제공해야 합니다.

- cell_admin과 같은 사용자의 보안 도메인 이름(DCE 셀)
- 다음의 서비스를 제공하는 컴퓨터의 이름
  - 보안
  - 시간
  - CDS(Cell Directory Services)
  - DSB(디렉토리 서비스 브로커)

NetSEAT 설치

Policy Director NetSEAT 설정 파일이 NetSEAT 파일을 사용자의 하드 디스크로 복사한 후에는 NetSEAT 구성 유틸리티가 자동으로 시작됩니다.

NetSEAT를 설치하려면 다음과 같이 하십시오.

1. 관리자 권한의 사용자로 로그인하십시오.
2. *IBM SecureWay Policy Director 버전 3.0* CD를 CD-ROM 드라이브에 넣으십시오.
3. CD의 \win32\client 디렉토리로 변경하십시오.
4. Setup.exe 파일을 두 번 클릭한 다음 InstallShield 프로그램을 시작하십시오.
5. 설치 언어 선택 창이 나오면 적절한 언어를 선택하십시오.
6. **다음**을 누르면 Policy Director 환영 창이 나옵니다.
7. **다음**을 누르십시오.
8. 설치할 구성요소 선택 창이 나오면 **Policy Director용 클라이언트 서버 제품**을 누르십시오.
9. **다음**을 누르십시오.
10. 설정 유형 선택 창이 나오면 **일반 설치**를 누르십시오.

    일반 설치를 위한 기본 위치는 다음과 같습니다.

    ```
    c:\Program Files\ibm\netseat\
    ```

또한 **사용자 설치**를 지정했으면 NetSEAT를 설치할 드라이브와 디렉토리를 지정하십시오.

대상 위치 창 선택이 나옵니다.

11. **다음**을 누르십시오.

    NetSEAT 파일이 하드 디스크의 기본 NetSEAT 위치로 복사됩니다. NetSEAT 구성 창이 나옵니다.

NetSEAT 구성

NetSEAT 구성 작업이 NetSEAT에 DCE 서버 이름, 위치 및 서비스 등 보안 도메인에 관한 정보를 제공합니다.

하드 드라이브에 모든 NetSEAT 파일이 복사된 후, **보안 도메인** 탭)이 나옵니다.

NetSEAT를 구성하려면 다음과 같이 하십시오.

1. 새 보안 도메인을 위한 항목을 추가하려면 **추가**를 누르십시오.

   새 보안 도메인 창이 나옵니다.
2. cell_admin과 같이 NetSEAT이 속하게 될 보안 도메인(DCE 셀)의 이름을 입력하십시오.
3. **GSS 사용 가능** 또는 **SSL 사용 가능** 선택란을 선택하십시오.
4. **확인**을 누르십시오.

   보안 도메인 등록 정보 창이 나옵니다.
5. 제공할 DCE 서버와 서비스를 추가하려면 **추가**를 누르십시오.

   DCE 서버 추가 창이 나옵니다.

   이 창을 사용하여 각각에서 제공하는 보안 도메인과 서비스에 있는 기존 DCE 서버를 NetSEAT에 알리십시오. 하나 이상의 DCE 서버가 필요한 경우도 있습니다. 모든 서비스들이 한 컴퓨터에 있거나 아니면 여러 컴퓨터에 나뉘어 있을 수 있습니다.

   다음은 발생할 가능성이 있는 시나리오입니다.

   - **새 보안 도메인(하나의 호스트 시스템)**

하나의 호스트 시스템만으로 이루어진 새 보안 도메인을 작성할 경우 호스트 시스템이 모든 DCE 서비스를 제공합니다. **시스템 이름** 필드에 호스트 시스템의 이름을 입력하십시오. 하나 이상의 서비스를 선택하십시오. DSB를 아직 설치하지 않았더라도 DSB를 선택하십시오.

- **새 보안 도메인(둘 이상의 호스트)**

  새 보안 도메인을 작성하며 DCE 서비스가 다른 호스트에 있을 경우에는 로컬 호스트가 DSB 서비스만 제공합니다. 이 경우 먼저 DCE 서비스(보안, 시간, CDS)를 제공하는 DCE 서버를 추가하십시오. 다음에 로컬 시스템을 나타내는 `localhost`라는 이름의 다른 DCE 서버를 추가하고 DSB 선택란을 선택하십시오. DSB를 아직 설치하지 않았더라도 DSB를 선택할 수 있습니다.

- **기존 보안 도메인**

  기존 보안 도메인에 Policy Director를 추가할 경우 보안, 시간, CDS를 제공하는 DCE 서버의 이름을 추가하십시오. 그리고나서 자동으로 DSB를 설치한 Policy Director 관리 서버를 포함하고 있는 DSB 서버의 이름을 추가하십시오. 이 시스템에 대해 DSB 선택란을 선택하십시오. 이 시나리오에서는 DSB를 포함하여 모든 서비스가 같은 호스트 시스템에 있을 수 있습니다.

6. 각 서버의 경우 보안 도메인에 있는 기존 서버의 완전한 DN 시스템 이름을 입력하십시오(예를 들어, SFF98732.austin.ibm.com).
7. 각 서버의 경우 서버에 대해 다음 중 하나 이상의 서비스를 선택하십시오.
   - 보안
   - DSB
   - 시간
   - CDS
8. **확인**을 누르십시오.

   보안 도메인 등록 정보 창이 새 항목을 표시합니다.
9. 필요에 따라 47 페이지의 5 단계에서 8 단계를 반복하여 추가 서버와 서비스를 추가하십시오.

10. 보안 도메인 등록 정보 창으로부터 기본 고급 로그인 구성인 **DCE 로그인만**을 허용하십시오.

    보안 도메인 등록 정보 창의 통합된 로그인 영역은 NetSEAT 설치에 사용되지 않습니다.

11. **확인**을 누르십시오.

    NetSEAT 구성 창이 나옵니다.

12. **확인**을 누르십시오.

    시스템 재시작이 필요함 창이 나옵니다.

13. **예**를 눌러 컴퓨터를 재시작하십시오.

14. **확인**을 누르십시오.

    컴퓨터가 재시작할 때 NetSEAT가 자동으로 시작합니다. Windows의 작업 표시줄에 NetSEAT 아이콘이 나옵니다.

    이로써 NetSEAT 설치와 구성을 완료했습니다.

NetSEAT 클라이언트 구성 확인

Policy Director 서버를 설치할 때에는 먼저 지정된 보안 도메인에 NetSEAT 클라이언트가 성공적으로 구성되었는지 확인하십시오. **netseat_ping** 명령을 사용하여 다음 서비스의 사용 가능 여부를 알아 볼 수 있습니다.

- 보안 서비스
- 시간 서비스
- 셀 디렉토리 서비스
- DSB(디렉토리 서비스 브로커)

필요한 서비스와 NetSEAT 클라이언트가 통신할 수 있는지 확인하려면 다음 단계를 완료하십시오.

1. **시작 → 프로그램 → NetSEAT → NetSEAT 로그인**을 눌러 cell_admin으로서 로그인하십시오.

   또는 명령줄에서 **netseat_login** 명령을 사용하여 로그인할 수 있습니다.

2. 사용자 구성에 반드시 필요한 경우가 아니면 PKI 로그인을 선택하지 마십시오.

3. Policy Director 관리자의 사용자 이름과 암호를 입력하십시오.
4. **확인**을 누르십시오.
5. 명령줄에서 **netseat_ping** 명령을 사용하여 구성 상태를 확보할 수 있습니다.

   예를 들어, NetSEAT 클라이언트가 ″redback″이라는 보안 도메인으로 구성된 경우, DOS 프롬프트에 이 명령을 입력하여 상태를 확보할 수 있습니다.

   ```
   netseat_ping -C redback
   ```

   다음 출력과 유사한 정보가 나옵니다.

   ```
   /.../redback:
          SecurityServers:
                       ncacn_ip_tcp:redback[ ] is available
                       ncadg_ip_udp:redback[ ] is available
          CdsServers:
                       ncacn_ip_tcp:redback[ ] is available
                       ncadg_ip_udp:redback[ ] is available
          TimeServers:
                       ncacn_ip_tcp:redback[ ] is available
                       ncadg_ip_udp:redback[ ] is available
          DsbServers:
                       ncacn_ip_tcp:redback[ ] not available
                       ncacn_ip_udp:redback[ ] not available
   ```

   하지만 새 보안 도메인 작성을 계획했다면 DSB가 실행되지 않는다는 점에 유의하십시오. 이 경우 DSB에 대한 **netseat_ping** 출력이 사용 가능하지 않음을 읽습니다. 이 시나리오에서는 읽을 수 있는 것으로 되어 있습니다. Policy Director 관리 서버 구성요소의 설치, 구성, DSB 시작은 모두 자동으로 이루어지므로 안전하게 Policy Director 설치를 진행할 수 있습니다. DSB가 이미 실행되고 있으면, DSB에 대한 출력이 사용 가능함을 읽습니다(v3.1).
6. DSB를 제외한 다른 서비스가 사용 가능하지 않다면, Policy Director 서버를 설치하기 전에 문제점을 해결하십시오.

Policy Director 서버 설치

Policy Director 서버를 설치할 경우, 먼저 관리자의 사용자 이름과 암호를 반드시 알고 있어야 합니다.

Policy Director 서버 구성요소를 설치하려면 다음과 같이 하십시오.

1. 사용자 레지스트리로 LDAP를 사용할 경우, LDAP 서버가 설치되어 실행 중인지 확인하십시오. 자세한 정보는 29 페이지의 『제4장 IBM SecureWay Directory 설치 및 구성』을 참조하십시오.
2. *IBM SecureWay Policy Director 버전 3.0* CD를 CD-ROM 드라이브에 넣으십시오.
3. CD의 \win32\server 디렉토리로 변경하십시오.
4. Setup.exe 파일을 누른 다음 InstallShield 프로그램을 시작하십시오.
5. 설치 언어 선택 창이 나오면 적절한 언어를 선택하십시오.
6. **다음**을 누르면 Policy Director 환영 창이 나옵니다.
7. **다음**을 누르십시오.

   대상 위치 창 선택이 나옵니다.
8. 프로그램 파일에 대한 기본 디렉토리 위치를 허용하거나 **찾아보기** 단추를 눌러 다른 위치를 작성하거나 선택하십시오.

   기본 위치는 `C:\Program Files\IBM\`입니다.

   기본 위치가 아닌 곳에 NetSEAT를 설치할 경우, 같은 위치에 Policy Director 서버를 설치하십시오.
9. **다음**을 누르십시오.

   구성요소 선택 창이 나옵니다.
10. 적절한 Policy Director 서버 구성요소를 선택하십시오. 선택과 관련된 정보는 19 페이지의 『공통 구성』을 참조하십시오.

    보안 도메인에는 한 인스턴스의 Policy Director 관리 서버(IVMgr)만 있어야 합니다.
11. **다음**을 누르십시오.
12. WebSEAL을 선택하지 않았으면 52 페이지의 14단계로 가십시오.

    WebSEAL(IVWeb) 구성요소를 선택했으면 웹 문서 루트 위치 선택 창이 나옵니다. 이 창에서 사용자 웹 공간의 루트 디렉토리 위치를 묻습니다. 웹 사이트에 속한 모든 자원들은 이 디렉토리 아래 상주합니다.
13. 루트 디렉토리 위치를 허용하거나 **찾아보기** 단추를 눌러 다른 위치를 작성하거나 선택하십시오. 기본 위치는 다음과 같습니다.

```
C:\...\IBM\Policy Director\www\docs
```

이제 Policy Director 파일이 CD에서 하드 디스크로 복사됩니다. 보안 도메인 관리자 로그인 창이 나옵니다. 이 단계는 보안 인증사항을 설정하고 구성 처리를 완료하는 데 필요합니다.

14. DCE 셀 관리자 이름과 암호를 완성하십시오.
15. 관리 서버 구성요소(IVMgr)를 선택한 경우, **LDAP 레지스트리**나 **DCE 레지스트리**를 선택하도록 프롬프트가 표시됩니다.

    관리 서버를 선택하지 않은 경우에는 기존 보안 도메인의 사용자 레지스트리 유형이 자동으로 발견됩니다.

    - LDAP 사용자 레지스트리가 발견되면, 『LDAP 사용자 레지스트리 사용』에 나오는 설명과 같이 설치가 계속됩니다.
    - DCE 사용자 레지스트리가 발견되면, 54 페이지의 『DCE 사용자 레지스트리 사용』에 나오는 설명과 같이 설치가 계속됩니다.
16. 사용자 레지스트리에 대해 다음 중 하나를 누르십시오.
    - **LDAP 사용자 레지스트리**를 선택한 경우, 『LDAP 사용자 레지스트리 사용』으로 가십시오.
    - **DCE 사용자 레지스트리**를 선택한 경우, 54 페이지의 『DCE 사용자 레지스트리 사용』으로 가십시오.

LDAP 사용자 레지스트리 사용

Policy Director 보안 도메인이 LDAP 사용자 레지스트리를 사용하거나 IVMgr를 설치하여 **LDAP 레지스트리**를 선택한 경우, LDAP 서버 정보 창이 나옵니다.

1. LDAP 서버 구성에 필요한 정보를 입력하십시오.
    - LDAP 호스트 이름
    - 포트 번호
    - SSL 포트 번호(LDAP 서버 액세스에 SSL을 사용할 경우에만)
    - GSO 데이터베이스를 위한 LDAP DN(예를 들어, o=ibm,c=us)
2. **다음**을 누르십시오.

    LDAP 서버와 통신 창이 나옵니다.

3. Policy Director와 LDAP 서버 간에 SSL 통신의 사용 가능 또는 사용 불가능 여부를 선택하십시오. SSL 통신을 사용 가능하게 하려면 **예**를 누르고, 사용 불가능하게 하려면 **아니오**를 누르십시오.

   Windows NT에서는 SSL 통신이 호스트 시스템과 LDAP 서버의 모든 Policy Director 서버 간에 한 번만 사용 가능합니다.

   SSL 통신을 사용 가능하게 한 경우, 4단계로 가십시오.

   SSL 통신을 사용 불가능하게 한 경우, 5단계로 가십시오.

4. 다음 프롬프트에 대해 값을 제공하십시오.
   - SSL 키 파일 위치
   - SSL 파일 DN(키 레이블)
   - SSL 키 파일 암호

   자세한 정보는 35 페이지의 『키 데이터베이스 파일 및 인증서 작성』을 참조하십시오.

5. **다음**을 누르십시오.

   LDAP 관리자 로그인 창이 나옵니다.

6. LDAP 관리자 이름(예를 들어, cn=root)과 암호 정보를 완성하고 **확인**을 누르십시오.

   서버가 구성되어 시작합니다. 이 작업에는 몇 분이 소요됩니다. 시스템 정보 창이 나오고 등록 정보를 포함한 서버 상태를 표시합니다.

7. **다음**을 누르십시오.

   Policy Director 설정 완료 창이 나옵니다.

8. **예**를 눌러 재시작하십시오.

   재시작 옵션에 **아니오**로 체크 표시한 경우에는 후에 Windows NT를 반드시 재시작하여 구성 처리를 완료해야 합니다. 이로써 Policy Director 설치를 완료했습니다.

9. **완료**를 누르십시오.

   시스템을 재시작하도록 프롬프트가 표시됩니다.

DCE 사용자 레지스트리 사용

Policy Director 보안 도메인이 DCE 사용자 레지스트리를 사용하거나 IVMgr를 설치하여 **DCE 사용자 레지스트리**를 선택한 경우, 다음과 같이 설치가 진행됩니다.

1. WebSEAL(IVWeb) 구성요소를 선택했으면 웹 문서 루트 위치 창이 나옵니다. 이 창에서 사용자 웹 공간의 루트 디렉토리 위치를 묻습니다. 웹 사이트에 속한 모든 자원들은 이 디렉토리 아래 상주합니다.

   WebSEAL을 선택하지 않았으면 3단계로 가십시오.

2. 기본 루트 디렉토리 위치를 허용하거나 **찾아보기** 단추를 눌러 다른 위치를 작성하거나 선택하십시오. 기본 위치는 다음과 같습니다.

   ```
   C:\Program Files\IBM\Policy Director\www\docs
   ```

3. **다음**을 누르십시오.

   이제 Policy Director 파일이 CD에서 하드 디스크로 복사됩니다. 보안 도메인 관리자 로그인 창이 나옵니다.

4. LDAP 관리자 이름과 암호 정보를 완성한 다음 **확인**을 누르십시오.

   서버가 구성되어 시작합니다. 이 작업에는 몇 분이 소요됩니다. 시스템 정보 창이 나오고 등록 정보를 포함한 서버 상태를 표시합니다.

5. **다음**을 누르십시오.

   Policy Director 설정 완료 창이 나옵니다.

6. **완료**를 누르십시오.

   시스템을 재시작하도록 프롬프트가 표시됩니다.

7. **예**를 눌러 재시작하십시오.

   재시작 옵션에 **아니오**로 체크 표시한 경우에는 후에 Windows NT를 반드시 재시작하여 구성 처리를 완료해야 합니다. 이로써 Policy Director 설치를 완료했습니다.

인증 획득 서비스 구성

Policy Director CAS는 자동으로 설치됩니다. CAS를 인증 획득 서비스로 사용하려 할 경우 반드시 구성해야 합니다. *Policy Director Administration Guide*의 인증 획득 서비스 구성에 관한 정보를 참조하십시오.

Windows NT에서 NetSEAL 트랩 사용

Policy Director NetSEAL(IVTrap)이 특정 포트에 이루어진 요청들을 트랩합니다. NetSEAL 트랩을 사용하기 위해서는 지정된 포트를 사용하는 모든 응용 프로그램을 중단하고 다시 시작해야 합니다.

특정 포트의 트랩을 위해 Policy Director NetSEAL을 구성하는 것에 관한 정보는 *Policy Director Administration Guide*에서 NetSEAL에 관한 개요 정보를 참조하십시오.

Windows에서 관리 콘솔 설치

Policy Director는 Windows 클라이언트 데스크탑으로부터 Policy Director 보안 시스템의 많은 구성요소를 관리하는 관리 콘솔을 제공합니다. 관리 콘솔은 다음 운영체제 중 어느 것에나 설치할 수 있습니다.

- Windows 95
- Windows 98
- Windows NT 버전 4.0(서비스 팩 4 이상 포함)

Policy Director를 실행하는 각 Windows 운영체제에는 Policy Director NetSEAT 클라이언트가 필요합니다.

NetSEAT 클라이언트는 DCE 런타임 클라이언트나 Policy Director 서버에 대한 클라이언트로서 구성할 수 있습니다. 관리 콘솔이 두 가지 구성 모두를 허용하더라도, Policy Director 서버에는 Policy Director 서버에 대해 완전한 클라이언트가 필요합니다.

구성요소를 재설치해야 할 경우에는 설치 전에 기존 구성요소를 반드시 제거해야 합니다.

서버 구성요소와 함께 관리 콘솔 설치

50 페이지의 『Policy Director 서버 설치』에서 Policy Director 서버 구성요소를 설치하고 구성했으면 다음 단계를 완료하십시오.

1. *IBM SecureWay Policy Director 버전 3.0* CD를 CD-ROM 드라이브에 넣으십시오.
2. \win32\Console 디렉토리로 변경하십시오.
3. Setup.exe 파일을 두 번 클릭한 다음, InstallShield 프로그램을 시작하십시오.
4. 설치 언어 선택 창이 나오면 적절한 언어를 선택하십시오.
5. **다음**을 누르면 Policy Director 환영 창이 나옵니다.
6. **다음**을 누르면 대상 위치 선택 창이 나옵니다.
7. 파일을 설치할 위치를 나타내십시오.

   파일들이 Windows 컴퓨터의 적절한 위치에 복사됩니다. 성공적인 설치를 나타내는 정보 창이 나옵니다.
8. Windows 재시작 여부를 조회할 경우, **예**를 누르십시오.
9. **확인**을 누르십시오.
10. 57 페이지의 『관리 콘솔 시작』으로 가십시오.

서버 구성요소 없이 관리 콘솔 설치

추가 Windows 시스템으로부터 Policy Director 보안 관리를 가능하게 하려면, Policy Director 서버 구성요소를 설치하지 않은 Windows 시스템에 관리 콘솔을 설치하십시오. 이 방식으로 관리 콘솔을 설치할 경우, NetSEAT 클라이언트를 DCE 런타임 클라이언트나 Policy Director 서버에 대한 클라이언트로서 구성할 수 있습니다.

서버 구성요소 없이 관리 콘솔을 설치하려면 Windows 데스크탑 시스템으로 가서 다음 단계를 완료하십시오.

1. Windows 운영체제가 지원되는 플랫폼인지 확인하십시오. 자세한 정보는 16 페이지의 『Policy Director 서버』를 참조하십시오.

2. Policy Director NetSEAT 클라이언트를 설치하십시오. 46 페이지의 『NetSEAT 설치』의 지시사항을 따르십시오.
3. 관리 콘솔을 실행할 보안 도메인에 NetSEAT 클라이언트가 제대로 구성되었는지 확인하십시오. 자세한 정보는 49 페이지의 『NetSEAT 클라이언트 구성 확인』을 참조하십시오.
4. *IBM SecureWay Policy Director 버전 3.0* CD를 CD-ROM 드라이브에 넣으십시오.
5. \win32\Console 디렉토리로 변경하십시오.
6. Setup.exe 파일을 두 번 클릭한 다음, InstallShield 프로그램을 시작하십시오.
7. 설치 언어 선택 창이 나오면 적절한 언어를 선택하십시오.
8. **다음**을 누르면 Policy Director 환영 창이 나옵니다.
9. **다음**을 누르면 대상 위치 선택 창이 나옵니다.
10. 파일을 설치할 위치를 나타내십시오.

    파일들이 Windows 컴퓨터의 적절한 위치에 복사됩니다. 성공적인 설치를 나타내는 정보 창이 나옵니다.
11. **확인**을 눌러 설치를 완료하십시오.
12. 관리 콘솔을 시작하려면 『관리 콘솔 시작』으로 가십시오.

관리 콘솔 시작

관리 콘솔을 시작하려면 다음과 같이 하십시오.

1. Policy Director 서버가 설치되어 실행되고 있는지 확인하십시오.
2. **시작 → 프로그램 → Policy Director → 관리 콘솔**을 누르십시오.

   Policy Director 관리 콘솔 창이 나옵니다.
3. cell_admin과 같은 관리자 권한의 사용자로서 관리 콘솔을 로그인하십시오.

Policy Director 제거

Policy Director 구성요소를 제거하기 위해서는 관리자로서 로그온해야 합니다. 관리자 인증사항을 가진 사용자로서 Windows 도메인에 로그인하십시오. 예를 들면, 다음과 같습니다.

```
dce_login cell_admin password
```

적절한 보안 도메인 인증사항 없이 구성요소 제거를 시도하면, 권한 부여 실패 메시지 창이 나옵니다.

설치할 때와 정확히 반대 순서로 Policy Director 구성요소를 제거해야 합니다. Policy Director를 제거하려면 제어판에서**프로그램 추가/제거** 아이콘을 사용하십시오.

설치된 전체 Policy Director를 설치 제거하려면 순서에 따라 다음 절차를 수행하십시오.

1. 관리 콘솔 제거
2. 서버 구성요소 제거
3. NetSEAT 클라이언트 제거

관리 콘솔 제거

관리 콘솔을 제거하려면 다음과 같이 하십시오.

1. 관리 콘솔이 실행되고 있으면 닫으십시오.
2. 제어판의 **프로그램 추가/제거**로 가서 **Policy Director 관리 콘솔**을 누르십시오.
3. **추가/제거** 단추를 누르십시오.
4. 조회 후에는 **예**를 눌러 제거할 프로그램을 확인하십시오.
5. **확인**을 누르십시오.

서버 구성요소 제거

Policy Director 서버 구성요소를 제거하기 위해서는 반드시 권한과 인증사항을 확보한 다음에 구성요소를 제거해야 합니다.

서버 구성요소를 제거하려면 다음과 같이 하십시오.

1. Policy Director 서버가 설치되어 실행되고 있는지 확인하십시오.
2. 제어판의 **프로그램 추가/제거**로 가서 제거할 첫번째 Policy Director 서버 구성요소를 선택하십시오.
3. Policy Director 서버 구성요소를 설치할 때와 정확히 반대 순서로 제거하십시오.

   예를 들어, 모든 구성요소를 설치한 경우 다음 순서로 제거할 수 있습니다.

   - 권한 부여 ADK(IVAuthADK)
   - 권한 부여 서버(IVAcld)
   - NetSEAL(IVTrap)
   - WebSEAL(IVWeb)
   - 보안 관리자(IVNet)
   - 관리 서버(IVMgr)
   - 기본(IVBase). 이 구성요소는 항상 자동으로 설치됩니다.

   Policy Director 관리 콘솔은 아무 때나 제거할 수 있습니다. 구성요소의 설치 순서에 관한 자세한 정보는 26 페이지의『단계별 Policy Director 설치 개요』를 참조하십시오.
4. **추가/제거** 단추를 누르십시오.
5. 요청이 있을 때 LDAP 관리자 사용자 이름과 암호를 입력하십시오.
6. 각 Policy Director 서버 구성요소에 대해 2단계에서 5단계를 반복하십시오.
7. 완료했으면 **확인**을 누르십시오.

NetSEAT 클라이언트 제거

Policy Director NetSEAT 구성요소를 제거하기 위해서는 Windows NT 관리자 권한이 반드시 있어야 합니다.

1. 제어판의 **프로그램 추가/제거**로 가서 **설치/제거** 탭을 누르십시오.
2. 탭의 목록 창으로부터 **Policy Director NetSEAT 클라이언트**를 누르십시오.
3. **추가/제거**를 누르십시오.
4. **확인**을 누르십시오.

제6장 AIX용 Policy Director 설치

이 장의 각 섹션에서는 AIX 운영체제에 Policy Director를 설치 및 구성하는 방법을 설명합니다.

Policy Director 설치를 시작할 때에는 먼저 『AIX용 Policy Director를 설치하기 전에』에 나오는 정보를 검토했는지 확인하십시오.

AIX용 Policy Director를 설치하기 전에

NetSEAT와 Policy Director를 설치할 때에는 먼저 다음 정보를 읽어보십시오.

- Policy Director 서버를 설치할 때 신규 DCE 셀을 작성하는 중이면 다음을 참조하십시오.
  - DCE 서버 또한 설치 및 구성해야 합니다.
  - 사용자 레지스트리에 LDAP를 사용 중이면, LDAP 서버 또한 설치 및 구성해야 합니다.
- 23 페이지의 『보안 도메인을 위한 설치 요구사항』에 나오는 Policy Director 전개에 관한 모든 정보를 잘 이해하고 있어야 합니다.

관리 콘솔 설치

Policy Director가 Policy Director 시스템의 모든 구성요소를 관리하는 데 사용되는 관리 콘솔을 제공합니다. 관리자가 AIX 시스템, Windows 시스템 또는 둘 다 설치하도록 선택할 수 있습니다.

AIX용 관리 콘솔은 IV.Console라는 이름의 패키지로 분배됩니다. 패키지를 설치 및 구성하려면 SMIT를 사용하십시오.

Policy Director 설치

AIX에 Policy Director를 설치하려면 다음 지시사항에 따라 작업하십시오.

1. 사용자 레지스트리로 LDAP를 사용할 경우, LDAP 서버가 설치되어 실행 중인지 확인하십시오. 자세한 정보는 29 페이지의 『제4장 IBM SecureWay Directory 설치 및 구성』 부분을 참조하십시오.
2. 루트로서 로그인하십시오.
3. *IBM SecureWay Policy Director 버전 3.0* CD를 CD-ROM 드라이브에 넣으십시오.
4. SMIT를 시작하십시오.
5. **소프트웨어 설치 및 유지보수**를 누르십시오.

   소프트웨어 설치 및 유지보수 메뉴가 나옵니다.
6. **소프트웨어 설치 및 갱신**을 누르십시오.

   소프트웨어 설치 및 갱신 메뉴가 나옵니다.
7. **패키지 이름별 소프트웨어 설치 및 갱신**을 누르십시오.

   패키지 이름별 소프트웨어 설치 및 갱신 창이 나옵니다.
8. 소프트웨어를 설치할 장치의 이름을 입력하십시오.

   예를 들면, 다음과 같습니다.

   - CD 장치로부터 설치하면 `/dev/cd0`을 입력합니다.
   - 마운트된 서버의 디렉토리로부터 설치하면 `/mnt/user/lpp/IV`를 입력합니다.

     장치 이름을 입력하면 복수 선택 목록 창이 나옵니다.
9. **IV**를 누르십시오.

   복수 선택 목록 창에 Policy Director 소프트웨어 패키지 목록이 나옵니다.
10. 설치할 패키지를 선택하십시오.

    - 모든 Policy Director 패키지를 설치하려면 **IV** 항목을 누르십시오.
    - 일부 Policy Director 패키지만 설치하려면 23 페이지의 『보안 도메인을 위한 설치 요구사항』에 나오는 설치 종속성을 살펴보십시오.
11. **확인**을 누르십시오.

SMIT 메뉴인 패키지 이름별 소프트웨어 설치 및 갱신 창이 나옵니다.

12. 다음과 같이 레이블된 필드에 대해 **예**를 누르십시오.

    자동 설치 필수 소프트웨어?

    이 단계에서 Policy Director 기본(IV.Base) 및 SMIT 설정(IV.smit) 패키지가 설치된 것을 확인합니다. 이 패키지들은 기타 Policy Director 패키지를 위한 전제 소프트웨어입니다. 이 필드를 **아니오**로 설정하도록 선택한 경우 패키지 선택 메뉴로 갑니다. IV.Base와 IV.Smit를 선택했는지 확인하십시오.

13. 사용자 설치에 적합한 값으로 기타 필드를 설정하십시오.

14. **확인**을 누르십시오.

    SMIT가 다음이 포함된 상태 메시지를 표시합니다.

    - Policy Director 소프트웨어 패키지의 사전 설치 확인
    - 패키지 파일 발췌 중 각 패키지 이름
    - 각 패키지를 위한 구성 메뉴 작성
    - 파일 발췌 완료시 성공을 나타내는 상태 메시지

15. 파일 발췌를 완료했으면 『LDAP 사용자 레지스트리를 사용하는 Policy Director 구성』의 설명에 따라 Policy Director 패키지를 구성하십시오. 또한 DCE 레지스트리를 사용 중이면 71 페이지의 『DCE 사용자 레지스트리를 사용하는 Policy Director 구성』을 참조하십시오.

LDAP 사용자 레지스트리를 사용하는 Policy Director 구성

구성을 완료하기 위해서는 먼저 Policy Director 소프트웨어 패키지를 반드시 설치해야 합니다. Policy Director 패키지를 아직 설치하지 않았으면 62 페이지의 『Policy Director 설치』를 참조하십시오.

DCE 사용자 레지스트리를 사용하는 Policy Director를 설치할 경우 71 페이지의 『DCE 사용자 레지스트리를 사용하는 Policy Director 구성』으로 가십시오.

SMIT 설정을 제외한 설치된 각각의 Policy Director 패키지를 반드시 구성해야 합니다. 한 번에 하나씩 패키지를 구성하십시오. 일부 Policy Director 패키지에는 구성 중에 화면 프롬프트에 응답할 관리자가 필요합니다.

Policy Director 패키지를 구성하려면 다음과 같이 하십시오.

1. SMIT를 시작하십시오.

   시스템 관리 메뉴가 나옵니다.

2. **통신 응용 프로그램 및 서비스**를 누르십시오.

   설치된 소프트웨어 패키지의 목록이 나옵니다. 예를 들면, 다음과 같습니다.

   - TCP/IP
   - NFS
   - DCE(분산 컴퓨팅 환경)
   - Policy Director

3. **Policy Director**를 누르십시오.

   다음 옵션을 가진 Policy Director 메뉴가 나옵니다.

   - Policy Director 구성
   - Policy Director 구성 해제

4. **Policy Director 구성**을 누르십시오.

   다음과 같은 설치된 Policy Director 패키지 목록이 나옵니다.

   - Policy Director 기본 구성
   - Policy Director 관리 서버 구성
   - Policy Director 관리 콘솔 구성
   - Policy Director 보안 관리자 구성
   - Policy Director WebSEAL 구성
   - Policy Director 권한 부여 서버 구성
   - Policy Director NetSEAL 구성
   - Policy Director 권한 부여 ADK 구성

5. 구성할 각 패키지를 한 번에 하나씩 누르십시오.

   반드시 Policy Director 구성 목록에 나오는 순서대로 Policy Director 패키지를 구성해야 합니다. 맨 위 항목에서 맨 아래 항목으로 차례대로 각 패키지를 선택하십시오.

이제 다음 섹션에 있는 적절한 구성 지시사항을 사용하여 선택한 Policy Director 패키지를 구성해야 합니다.

기본 패키지 구성

기본 패키지는 기타 패키지를 설치할 때마다 컴퓨터에 설치됩니다. 기본 패키지를 구성하려면, Policy Director 구성 목록에서 **Policy Director 기본**을 누르십시오.

Policy Director 기본 패키지 구성은 사용자 입력 없이 이루어집니다.

관리 서버 구성

관리 서버를 구성하려면 다음과 같이 하십시오.

1. Policy Director 구성 목록에서 **Policy Director 관리 서버**를 누르십시오.

   사용자 레지스트리 유형을 선택하도록 프롬프트가 표시됩니다.
2. 사용자 레지스트리로 LDAP를 사용할 경우, LDAP 사용자 레지스트리에 2를 입력하십시오.

   DCE 셀 관리자 이름과 암호를 요청하는 프롬프트가 나옵니다.
3. 프롬프트가 표시될 때 DCE 셀 관리자 계정 이름과 암호를 입력하십시오.

   사용자 레지스트리로 LDAP를 사용할 경우, 관리 서버와 LDAP 서버 간에 통신을 구성하기 위한 일련의 프롬프트가 나옵니다.
4. LDAP 서버 구성에 필요한 정보를 입력하십시오.
   - LDAP 서버 호스트 이름
   - LDAP 서버 포트 번호
   - LDAP 서버 SSL 포트 번호(선택사항)
5. LDAP 관리 사용자를 위한 사용자 이름과 암호를 입력하십시오(예를 들어, `cn=root`). 이제 Policy Director 보안 정보가 LDAP 서버에 등록됩니다.
6. 관리 서버와 LDAP 서버 간에 SSL 통신의 사용 가능 또는 사용 불가능 여부를 선택하십시오.

   주: 각 서버와 LDAP 서버 간에 SSL 통신을 개별적으로 사용 가능 또는 사용 불가능하게 만들 수 있습니다. 이 경우 관리 서버(IVMgr)와 LDAP 서버 간에 사용자가 SSL 통신을 설정합니다.

7. SSL 통신을 사용 불가능하게 한 경우, 8단계로 가십시오. SSL 통신을 사용 가능하게 한 경우, 다음 프롬프트에 값을 제공하십시오.
   - SSL 키 링 파일 위치
   - SSL 키 레이블
   - SSL 키용 암호
8. 31 페이지의 『접미어 추가』에서 추가한 GSO 데이터베이스 접미어에 DN을 제공하여 GSO 데이터베이스 액세스를 사용 가능하게 만드십시오.

   예를 들면, 다음과 같습니다.

   ```
   o=IBM,c=US
   ```

   GSO 데이터베이스 액세스가 구성되면 Policy Director 구성 관리자가 자동으로 DSB(디렉토리 서비스 브로커)를 구성합니다. 완료할 때마다 일련의 메시지가 각각의 자동화 단계를 나열합니다.

   IVMgr 패키지 설치가 성공한 것을 나타내는 메시지가 나타납니다.

   사용 가능한 패키지의 목록이 다시 나옵니다.

관리 콘솔 구성 및 시작

관리 콘솔을 구성하려면 Policy Director 구성 목록에서 **Policy Director 관리 콘솔**을 누르십시오.

Policy Director 관리 콘솔은 사용자 입력 없이 이루어집니다.

AIX 버전의 관리 콘솔을 시작하려면 다음과 같이 하십시오.

1. Policy Director 서버가 설치되어 실행되고 있는지 확인하십시오.
2. 다음 명령을 입력하십시오.

```
$ /opt/intraverse/bin/ivconsole
```

또한 Windows 클라이언트 버전의 관리 콘솔을 사용할 경우, 57 페이지의 『관리 콘솔 시작』의 지시사항에 따라 작업하십시오.

보안 관리자 구성

보안 관리자(IVNet)를 구성하려면 다음과 같이 하십시오.

1. Policy Director 구성 목록에서 **Policy Director 보안 관리자**를 누르십시오.

   보안 관리자를 LDAP 서버로 통합하기 위해 여러 프롬프트가 시리즈로 나옵니다.

2. 프롬프트가 표시될 경우, LDAP 서버 구성에 필요한 정보를 입력하십시오.

   - LDAP 서버 호스트 이름
   - LDAP 서버 포트 번호
   - LDAP 서버 SSL 포트 번호(선택사항)

   Policy Director 관리 서버나 권한 부여 서버를 이미 구성했을 경우, 이 프롬프트가 표시되지 않습니다.

3. LDAP 관리 사용자를 위한 사용자 이름과 암호를 입력하십시오. 이제 Policy Director 보안 정보가 LDAP 서버에 등록됩니다.

4. 보안 관리자와 LDAP 서버 간에 SSL 통신의 사용 가능 또는 사용 불가능 여부를 선택하십시오.

   주: 각 Policy Director 서버와 LDAP 서버 간에 SSL 통신을 개별적으로 사용 가능 또는 사용 불가능하게 만들 수 있습니다. 이 경우 보안 관리자(WebSEAL과 NetSEAL이 사용할 경우 IVNet)와 LDAP 서버 간에 사용자가 SSL 통신을 설정합니다.

5. SSL 통신을 사용 불가능하게 한 경우 6단계로 가십시오 SSL 통신을 사용 가능하게 한 경우, 다음 프롬프트에 값을 제공하십시오.

   - SSL 키 링 파일 위치
   - SSL 키 레이블
   - SSL 키용 암호

6. 31 페이지의 『접미어 추가』에서 추가한 GSO 데이터베이스 접미어에 DN을 제공하여 GSO 데이터베이스 액세스를 사용 가능하게 만드십시오.

   예를 들면, 다음과 같습니다.

   ```
   o=IBM,c=US
   ```

Policy Director 관리 서버나 권한 부여 서버를 이미 구성했을 경우, 이 프롬프트가 표시되지 않습니다.

DCE 셀 관리자 이름과 암호를 요청하는 프롬프트가 나옵니다.

7. 프롬프트가 표시될 때, DCE 셀 관리자 계정 이름과 암호를 입력하십시오.

   보안 관리자가 구성되어 시작됩니다. 또한 CAS 서버도 시작됩니다.

   보안 관리자 패키지 설치가 성공한 것을 나타내는 메시지가 표시됩니다.

Policy Director WebSEAL 구성

Policy Director WebSEAL(IVWeb)를 구성하려면 다음과 같이 하십시오.

1. Policy Director 구성 목록에서 **Policy Director WebSEAL**를 누르십시오.

   다음을 확인하는 값과 함께 Policy Director WebSEAL 구성 메뉴가 나옵니다.

   - HTTP 및 HTTPS 클라이언트 액세스
   - 필수 TCP(Transmission Control Protocol) 포트
   - 기본 웹 문서 루트 디렉토리

2. 현재 구성 값을 확인하십시오.

```
웹 서버 구성을 확인하십시오.
1. TCP HTTP 사용 가능?                예
2. HTTP 포트                          80
3. HTTPS 사용 가능?                   예
4. HTTPS 포트                         443
5. 웹 문서 루트 디렉토리              /opt/Policy Director/www/docs
a. 구성 허용 후 설치 계속
x. 설치 종료

변경 항목 선택: a
```

3. 구성을 허용하고 설치를 계속하려면 a를 입력하거나 변경할 값의 수를 입력하십시오.

   Policy Director 보안 관리자 구성이 DCE 셀 관리자 이름과 암호를 프롬프트합니다.

4. DCE 셀 관리자 계정 이름과 암호를 입력하십시오.

   Policy Director 보안 관리자가 재시작합니다.

이 설치는 Policy Director WebSEAL을 구성하고 사용 가능하게 만듭니다.

Policy Director 권한 부여 서버 구성

Policy Director 권한 부여 서버(IVAcld)를 구성하려면 다음과 같이 하십시오.

1. Policy Director 구성 목록에서 **Policy Director 권한 부여 서버**를 누르십시오.

   LDAP 서버로 Policy Director 권한 부여 서버를 통합하기 위해 여러 프롬프트가 나옵니다.

2. 프롬프트가 표시될 경우, LDAP 서버 구성에 필요한 정보를 입력하십시오.
   - LDAP 서버 호스트 이름
   - LDAP 서버 포트 번호
   - LDAP 서버 SSL 포트 번호(선택사항)

   Policy Director 관리 서버나 권한 부여 서버를 이미 구성했을 경우, 이 프롬프트가 표시되지 않습니다.

3. LDAP 관리 사용자를 위한 사용자 이름과 암호를 입력하십시오. 이제 Policy Director 보안 정보가 LDAP 서버에 등록됩니다.

4. 보안 관리자와 LDAP 서버 간에 SSL 통신의 사용 가능 또는 사용 불가능 여부를 선택하십시오.

   주: 각 Policy Director 서버와 LDAP 서버 간에 SSL 통신을 개별적으로 사용 가능 또는 사용 불가능하게 만들 수 있습니다. 이 경우 권한 부여 서버(IVAcld)와 LDAP 서버 간에 사용자가 SSL 통신을 설정합니다.

5. SSL 통신을 사용 불가능하게 한 경우, 6단계로 가십시오. SSL 통신을 사용 가능하게 한 경우, 다음 프롬프트에 값을 제공하십시오.
   - SSL 키 링 파일 위치
   - SSL 키 레이블
   - SSL 키용 암호

6. 31 페이지의 『접미어 추가』에서 추가한 GSO 데이터베이스 접미어에 DN을 제공하여 GSO 데이터베이스 액세스를 사용 가능하게 만드십시오.

   예를 들면, 다음과 같습니다.

```
o=IBM,c=US
```

Policy Director 관리 서버나 권한 부여 서버를 이미 구성했을 경우, 이 프롬프트가 표시되지 않습니다.

DCE 셀 관리자 이름과 암호를 요청하는 프롬프트가 나옵니다.

7. 프롬프트가 표시될 때 DCE 셀 관리자 계정 이름과 암호를 입력하십시오.

   권한 부여 서버가 구성되어 시작됩니다.

   권한 부여 서버 패키지 설치가 성공한 것을 나타내는 메시지가 표시됩니다.

Policy Director NetSEAL 구성

Policy Director NetSEAL을 구성하려면 다음과 같이 하십시오.

1. Policy Director 구성 목록에서 **Policy Director NetSEAL**을 누르십시오.

   DCE 셀 관리자 이름과 암호를 요청하는 프롬프트가 나옵니다.

2. LDAP 관리 사용자를 위한 사용자 이름과 암호를 입력하십시오. 이제 Policy Director 보안 정보가 LDAP 서버에 등록됩니다.

   이로써 Policy Director NetSEAL 패키지 구성을 완료했습니다.

Policy Director NetSEAL이 특정 포트에 이루어진 요청을 트랩합니다. NetSEAL 트랩을 사용하기 위해서는 지정된 포트를 사용하는 모든 응용 프로그램을 중단하고 다시 시작해야 합니다. Policy Director NetSEAL을 사용하는 것에 관한 자세한 정보는 76 페이지의 『AIX에서 NetSEAL 트랩 사용』을 참조하십시오.

Policy Director 권한 부여 ADK 구성

Policy Director 권한 부여 ADK를 구성하려면, Policy Director 구성 목록에서 **Policy Director 권한 부여 ADK**를 누르십시오.

Policy Director 권한 부여 패키지 구성은 사용자 입력 없이 완료됩니다.

Policy Director 인증 획득 서비스 구성

Policy Director CAS는 자동으로 설치됩니다. Policy Director CAS를 인증 획득 서비스로 사용할 경우, 반드시 구성해야 합니다. *Policy Director Administration Guide*에서 Policy Director CAS에 관한 정보와 WebSEAL 서버를 위한 구성 방법을 참조하십시오.

DCE 사용자 레지스트리를 사용하는 Policy Director 구성

구성을 완료하기 위해서는 먼저 Policy Director 소프트웨어 패키지를 반드시 설치해야 합니다. Policy Director 패키지를 아직 설치하지 않았으면 먼저 62 페이지의 『Policy Director 설치』를 참조하십시오.

LDAP 사용자 레지스트리를 사용하는 Policy Director를 설치할 경우 63 페이지의 『LDAP 사용자 레지스트리를 사용하는 Policy Director 구성』으로 가십시오.

SMIT 설정을 제외한 설치된 각각의 Policy Director 패키지를 반드시 구성해야 합니다. 한 번에 하나씩 패키지를 구성하십시오. 일부 Policy Director 패키지에는 구성 중에 화면 프롬프트에 응답할 관리자가 필요합니다.

Policy Director 패키지를 구성하려면 다음과 같이 하십시오.

1. SMIT를 시작하십시오.

   시스템 관리 메뉴가 나옵니다.
2. **통신 응용 프로그램 및 서비스**를 누르십시오.

   설치된 소프트웨어 패키지의 목록이 나옵니다. 예를 들면, 다음과 같습니다.
   - TCP/IP
   - NFS
   - DCE(분산 컴퓨팅 환경)
   - Policy Director
3. **Policy Director**를 누르십시오.

   다음 옵션을 가진 Policy Director 메뉴가 나옵니다.
   - Policy Director 구성
   - Policy Director 구성 해제

4. **Policy Director 구성**을 누르십시오.

   다음과 같은 설치된 Policy Director 패키지 목록이 나옵니다.

   - Policy Director 기본 구성
   - Policy Director 관리 서버 구성
   - Policy Director 관리 콘솔 구성
   - Policy Director 보안 관리자 구성
   - Policy Director WebSEAL 구성
   - Policy Director 권한 부여 서버 구성
   - Policy Director NetSEAL 구성
   - Policy Director 권한 부여 ADK 구성

5. 구성할 각 패키지를 한 번에 하나씩 누르십시오.

   반드시 Policy Director 구성 목록에 나오는 순서대로 Policy Director 패키지를 구성해야 합니다. 맨 위 항목에서 맨 아래 항목으로 차례대로 각 패키지를 선택하십시오.

이제 다음 섹션에 있는 적절한 구성 지시사항을 사용하여 선택한 Policy Director 패키지를 구성해야 합니다.

기본 패키지 구성

기본 패키지는 기타 다른 패키지를 설치할 때마다 컴퓨터에 설치됩니다. 기본 패키지를 구성하려면 Policy Director 구성 목록에서 **Policy Director 기본**을 누르십시오.

Policy Director 기본 패키지 구성은 사용자 입력 없이 완료됩니다.

관리 서버 구성

관리 서버를 구성하려면 다음과 같이 하십시오.

1. Policy Director 구성 목록에서 **Policy Director 관리 서버**를 누르십시오.

   DCE 셀 관리자 이름과 암호를 요청하는 프롬프트가 나옵니다.

2. 프롬프트가 표시될 때 DCE 셀 관리자 계정 이름과 암호를 입력하십시오.

   설치가 구성되고 관리 서버가 시작됩니다.

관리 콘솔 구성 및 시작

관리 콘솔을 구성하려면 Policy Director 구성 목록에서 **Policy Director 관리 콘솔**을 누르십시오.

Policy Director 관리 콘솔 구성은 사용자 입력 없이 완료됩니다.

AIX 버전의 관리 콘솔을 시작하려면 다음과 같이 하십시오.

1. Policy Director 서버가 설치되어 실행되고 있는지 확인하십시오.
2. 다음 명령을 입력하십시오.

```
$ /opt/intraverse/bin/ivconsole
```

보안 관리자 구성

보안 관리자(IVNet)를 구성하려면 다음과 같이 하십시오.

1. Policy Director 구성 목록에서 **Policy Director 보안 관리자**를 누르십시오.
2. 프롬프트가 표시될 때 DCE 셀 관리자 계정 이름과 암호를 입력하십시오.

설치가 구성되어 보안 관리자가 시작됩니다.

Policy Director WebSEAL 구성

Policy Director WebSEAL(IVWeb)를 구성하려면 다음과 같이 하십시오.

1. Policy Director 구성 목록에서 **Policy Director WebSEAL**을 누르십시오.

   다음을 확인하는 값과 함께 Policy Director WebSEAL 구성 메뉴가 나옵니다.

   - HTTP 및 HTTPS 클라이언트 액세스
   - 필수 TCP(Transmission Control Protocol) 포트
   - 기본 웹 문서 루트 디렉토리
2. 현재 구성 값을 확인하십시오.

```
웹 서버 구성을 확인하십시오.
1. TCP HTTP 사용 가능?                  예
2. HTTP 포트                            80
3. HTTPS 사용 가능?                     예
4. HTTPS 포트                           443
5. 웹 문서 루트 디렉토리                /opt/Policy Director/www/docs
```

```
a. 구성 허용 후 설치 계속
x. 설치 종료

변경 항목 선택: a
```

3. 구성을 허용하고 설치를 계속하려면 a를 입력하거나 변경할 값의 수를 입력하십시오.

   Policy Director 보안 관리자 구성이 DCE 셀 관리자 이름과 암호를 프롬프트합니다.

4. DCE 셀 관리자 계정 이름과 암호를 입력하십시오.

   Policy Director 보안 관리자가 재시작합니다.

   이 설치는 Policy Director WebSEAL을 구성하고 사용 가능하게 만듭니다.

Policy Director 권한 부여 서버 구성

Policy Director 권한 부여 서버(IVAcld)를 구성하려면 다음과 같이 하십시오.

1. Policy Director 구성 목록에서 **Policy Director 권한 부여 서버**를 누르십시오.

   DCE 셀 관리자 이름과 암호를 요청하는 프롬프트가 나옵니다.

2. DCE 셀 관리자 계정 이름과 암호를 입력하십시오.

   권한 부여 서버가 구성되어 시작합니다.

Policy Director NetSEAL 구성

Policy Director NetSEAL을 구성하려면 다음과 같이 하십시오.

1. Policy Director 구성 목록에서 **Policy Director NetSEAL**를 누르십시오.

   DCE 셀 관리자 이름과 암호를 요청하는 프롬프트가 나옵니다.

2. LDAP 관리 사용자를 위한 사용자 이름과 암호를 입력하십시오. 이제 Policy Director 보안 정보가 LDAP 서버에 등록됩니다.

   이로써 Policy Director NetSEAL 구성을 완료했습니다.

Policy Director NetSEAL이 특정 포트에 이루어진 요청을 트랩합니다. NetSEAL 트랩을 사용하기 위해서는 지정된 포트를 사용하는 모든 응용 프로그램을 중단하고 다시 시작해야 합니다. Policy Director NetSEAL을 사용하는 것에 관한 자세한 정보는 76 페이지의 『AIX에서 NetSEAL 트랩 사용』을 참조하십시오.

Policy Director 권한 부여 ADK 구성

Policy Director 권한 부여 ADK를 구성하려면 Policy Director 구성 목록에서 **Policy Director 권한 부여 ADK**를 누르십시오.

Policy Director 권한 부여 패키지 구성은 사용자 입력 없이 완료됩니다.

Policy Director 인증 획득 서비스 구성

Policy Director CAS는 자동으로 설치됩니다. Policy Director CAS를 인증 획득 서비스로 사용할 경우, 반드시 구성해야 합니다. *Policy Director Administration Guide*에서 Policy Director CAS에 관한 정보와 WebSEAL 서버를 위한 구성 방법을 참조하십시오.

관리 콘솔 설치

Policy Director는 Windows 클라이언트 데스크탑으로부터 Policy Director 보안 시스템의 많은 구성요소를 관리하는 관리 콘솔을 제공합니다. 관리 콘솔은 다음 운영체제 중 어느 것에나 설치할 수 있습니다.

- Windows 95
- Windows 98
- Windows NT 버전 4.0(서비스 팩 4 이상 포함)
- AIX 버전 4.3.1.0 이상

Policy Director를 실행하는 각 Windows 운영체제에는 Policy Director NetSEAT 클라이언트가 필요합니다.

NetSEAT 클라이언트는 DCE 런타임 클라이언트나 Policy Director 서버에 대한 클라이언트로서 구성할 수 있습니다. 관리 콘솔이 두 가지 구성 모두를 허용하더라도 Policy Director 서버에는 Policy Director 서버에 대해 완전한 클라이언트가 필요합니다.

구성요소를 재설치해야 할 경우에는 설치 전에 기존 구성요소를 반드시 제거해야 합니다.

AIX에서 NetSEAL 트랩 사용

Policy Director NetSEAL 트랩을 사용하려면 응용 프로그램이 보안된(트랩된) 포트에 액세스하기 전에 NetSEAL 디먼 보안 관리자(secmgrd)를 반드시 시작해야 합니다. 시동 처리 중에 응용 프로그램에 앞서 secmgrd가 시작하는지 확인하려면, /etc/inittab 항목을 사용하십시오.

텔넷, RLOGIN, POP3 등과 같은 네트워킹 응용 프로그램과 함께 NetSEAL 트랩을 사용하십시오. **inetd** 디먼이 이 응용 프로그램을 제어합니다. Policy Director 시동 스크립트인 /etc/iv/iv가 secmgrd를 시작한 다음 inetd 디먼을 중지시키고 재시작하십시오. 이 절차는 시스템 시동 후 이 응용 프로그램들의 성공적인 트랩 활동을 보장합니다.

Policy Director를 중지시켰다가 재시작할 경우, 트랩된 포트를 요청하는 모든 응용 프로그램들도 중지했다가 다시 시작해야 합니다. 이 처리를 자동화하기 위해 /etc/iv/iv에 코드를 추가하여 secmgrd가 시작한 후 응용 프로그램이 중지했다가 시작하도록 만들 수 있습니다. 기타 응용 프로그램의 중지 및 시작 방법에 대한 템플리트로 **inetd**를 중지 및 재시작하는 데 /etc/iv/iv 스크립트 기술을 사용하십시오.

특정 포트의 트랩을 위한 Policy Director NetSEAL 구성에 관한 정보는 *Policy Director Administration Guide*에서 NetSEAL에 관한 정보를 참조하십시오.

Policy Director 제거

Policy Director를 제거하기 위해서는 먼저 AIX용 Policy Director를 구성 해제해야 합니다.

- Policy Director의 구성 해제에 관한 정보는 77 페이지의 『Policy Director 패키지 구성 해제』를 참조하십시오.
- Policy Director 제거에 관한 정보는 78 페이지의 『Policy Director 패키지 제거』를 참조하십시오.

Windows 버전의 관리 콘솔을 제거하려면 부분을 참조하십시오.

Policy Director 패키지 구성 해제

Policy Director 서버를 구성 해제하려면 다음 단계를 완료하십시오.

1. SMIT를 시작하십시오.
2. **통신 응용 프로그램 및 서비스**를 누르십시오.

   통신 응용 프로그램 및 서비스 메뉴가 나옵니다.
3. **Policy Director**를 누르십시오.

   Policy Director 메뉴가 나옵니다.
4. 메뉴로부터 **Policy Director 구성 해제**를 누르십시오.

   구성된 Policy Director 패키지 목록이 나옵니다.

   구성 해제할 패키지를 선택하십시오. 다음과 같은 패키지가 표시됩니다.

   - Policy Director 권한 부여 서버 구성 해제
   - Policy Director 권한 부여 ADK 구성 해제
   - Policy Director NetSEAL 구성 해제
   - Policy Director WebSEAL 구성 해제
   - Policy Director 보안 관리자 구성 해제
   - Policy Director 관리 서버 구성 해제
   - Policy Director 관리 콘솔 구성 해제
   - Policy Director 기본 구성 해제
   - IV Smit 메뉴 구성 해제
5. 한 번에 하나씩 패키지를 구성 해제하십시오.

   주: 패키지를 설치한 것과 정확히 반대 순서로 패키지를 구성 해제하십시오. 확실한 순서를 위해 메뉴의 맨 위에서부터 메뉴의 맨 아래로 패키지를 구성 해제하십시오.
6. 컴퓨터에서 모든 Policy Director를 제거하려는 이유로 Policy Director 패키지를 구성 해제할 경우, 다른 모든 Policy Director 패키지를 구성 해제한 후 **Policy Director Smit 메뉴 구성 해제**를 누르십시오.

   이 단계는 SMIT 데이터베이스로부터 Policy Director 패키지 정보를 제거합니다.

7. Policy Director를 제거하려면 『Policy Director 패키지 제거』를 참조하십시오.

Policy Director 패키지 제거

Policy Director를 제거하기 위해서는 먼저 Policy Director 소프트웨어가 구성 해제되었는지 확인해야 합니다. 구성 해제에 관한 지시사항은 77 페이지의 『Policy Director 패키지 구성 해제』를 참조하십시오.

Policy Director를 제거하려면 다음과 같이 하십시오.

1. SMIT를 시작하십시오.
2. **소프트웨어 설치 및 유지보수**를 누르십시오.

   소프트웨어 설치 및 유지보수 메뉴가 나옵니다.
3. **소프트웨어 유지보수 및 유틸리티**를 누르십시오.

   소프트웨어 유지보수 및 유틸리티 메뉴가 나옵니다.
4. **설치된 소프트웨어 제거**를 누르십시오.

   설치된 소프트웨어 제거 창이 나옵니다.
5. 제거할 Policy Director 패키지를 선택하십시오. 한 번에 여러 패키지를 선택할 수 있습니다.

   모든 Policy Director 패키지를 제거하려면 `IV`를 입력하십시오.

Policy Director 소프트웨어가 제거됩니다.

관리 콘솔 및 NetSEAT 제거

Windows의 관리 콘솔과 NetSEAT 클라이언트는 InstallShield 설치 제거 기능을 사용하여 제거할 수 있습니다.

- 관리 콘솔을 제거하십시오. 58 페이지의 『관리 콘솔 제거』에 나오는 지시사항을 참조하십시오.
- NetSEAT 클라이언트를 제거하십시오. 59 페이지의 『NetSEAT 클라이언트 제거』에 나오는 지시사항을 참조하십시오.

제7장 Solaris용 Policy Director 설치

이 장의 각 섹션에서는 Solaris 운영체제에 Policy Director를 설치 및 구성하는 방법을 설명합니다.

Policy Director 설치를 시작할 때에는 먼저 『Solaris용 Policy Director를 설치하기 전에』에 나오는 정보를 검토했는지 확인하십시오.

Solaris용 Policy Director를 설치하기 전에

Policy Director를 설치할 때에는 먼저 다음 정보를 읽어보십시오.

이 릴리스의 Policy Director를 위한 설치 절차에는 **pkgadd** 명령이 필요합니다. **pkgadd** 명령을 실행하려면 명령 프롬프트에 다음 명령을 입력하십시오.

```
# pkgadd -d /cdrom/cdrom0/solaris
```

Policy Director 소프트웨어를 설치하려면 **pkgadd** 명령을 사용하십시오. 때로는 **pkgadd** 명령이 표준 절차 지시사항에는 나오지 않는 보충 프롬프트를 표시하는 경우가 있습니다. 이 프롬프트들은 사용자 시스템 설정 및 구성의 고유한 상황에 따라 표시되는 것입니다. 표준 절차의 외부에서 발생하는 이러한 프롬프트에 대해서는 항상 y로 응답하십시오.

Policy Director를 설치하기 전에 다음과 같이 하십시오.

- 반드시 DCE 클라이언트를 설치해야 합니다.
- 사용자 레지스트리를 위해 LDAP를 사용하면, LDAP 클라이언트도 반드시 설치해야 합니다.

Policy Director를 설치하기 위해서는 먼저 Transarc DCE 원격 관리 기능을 반드시 사용 가능하게 만들어야 합니다. 원격 관리 기능이 사용 가능하지 않을 경우, Policy Director 설치를 완료할 수 없습니다.

일부 원격 관리 기능들을 사용하게 되면 셀 관리자가 로컬 루트 계정에 본질적으로 동등하게 됩니다. 보통 Transarc DCE가 이 원격 관리 기능을 사용 불가능하게 만듭니다. 하지만 Policy Director 소프트웨어에는 이 기능이 필요합니다.

원격 관리 기능을 사용 가능하게 하는 방법은 *Transarc Release Notes, 릴리즈 1.1*(DCE-D1002-01)의 4.2.1 섹션을 참조하십시오.

설치 화면 출력

본 문서의 표준 절차가 **pkgadd** 명령으로 나올 수 있는 모든 화면 출력을 나타내지는 않습니다. 문서화되지 않은 대부분의 화면 출력들은 사용자가 수행하는 조작에 관한 추가 정보를 제공합니다. 일반적으로 본 문서의 표준 절차들은 사용자 응답이 필요한 메시지들만을 표시합니다.

LDAP 사용자 레지스트리를 사용하는 Policy Director 서버 설치

DCE 사용자 레지스트리를 사용하는 Policy Director를 설치할 경우 87 페이지의 『DCE 사용자 레지스트리를 사용하는 Policy Director 서버 설치』으로 가십시오.

서버 패키지들은 *IBM SecureWay Policy Director 버전 3.0* CD의 /solaris 디렉토리에 있습니다.

Policy Director 패키지를 설치하기 위해서는 사용자 루트로서 로그온해야 합니다.

패키지를 다시 설치해야 할 경우에는 먼저 기존의 패키지(**pkgrm**)를 제거한 다음 원하는 패키지를 다시 설치해야 합니다.

관리 서버를 설치하는 방법은 다음과 같습니다.

1. 사용자 레지스트리로 LDAP를 사용할 경우, LDAP 서버가 설치되어 실행 중인지 확인하십시오. 자세한 정보는 29 페이지의 『제4장 IBM SecureWay Directory 설치 및 구성』을 참조하십시오.
2. **pkgadd** 명령을 입력하여 CD로부터 사용 가능한 패키지들을 나열하십시오.

   ```
   # pkgadd -d /cdrom/cdrom0/solaris
   ```

   사용 가능한 패키지의 목록이 화면에 나옵니다.

다른 CD-ROM 마운트 포인트를 사용 중이면, 위의 명령에 나오는 것으로 대체하십시오.

3. IVBase에 대한 선택 번호를 입력하여 Policy Director 기본 파일을 설치한 다음 Enter 키를 누르십시오.

   이 명령이 CD로부터 파일들을 발췌하여 사용자가 지정한 하드 디스크에 파일들을 설치합니다.

   IVBase 패키지 설치가 성공한 것을 나타내는 프롬프트가 표시됩니다. 사용 가능한 패키지의 목록이 다시 나옵니다.

   다음 단계로 계속하기 전에 보안 도메인에는 한 인스턴스의 관리 서버(IVMgr)만 있어야 한다는 점을 기억하십시오. 독립형 시스템 설치를 진행 중이면, 다음 단계를 계속하십시오. 2차 서버에 설치하는 중이면, 23 페이지의 『보안 도메인을 위한 설치 요구사항』을 반드시 검토하십시오.

4. IVMgr에 대한 선택 번호를 입력하여 Policy Director 관리 서버 파일을 설치하십시오. Enter 키를 누르십시오.

   이 명령이 CD로부터 파일들을 발췌하여 사용자가 지정한 하드 디스크에 파일들을 설치합니다.

   사용자 레지스트리 유형을 선택하도록 프롬프트가 표시됩니다.

5. 사용자 레지스트리를 위해 LDAP를 사용할 경우, LDAP 사용자 레지스트리에 2를 입력하십시오.

   DCE 셀 관리자 이름과 암호를 요청하는 프롬프트가 나옵니다.

6. DCE 셀 관리자 계정에 액세스하기 위해 필요한 정보를 입력하십시오.

   ```
   셀 관리자 [cell_admin]의 사용자 이름 입력:
   셀 관리자의 암호 입력:
   ```

   관리 서버와 LDAP 서버 간에 통신을 구성하기 위한 일련의 프롬프트가 나옵니다.

7. LDAP 서버 구성에 필요한 정보를 입력하십시오.
   - LDAP 서버 호스트 이름
   - LDAP 서버 포트 번호
   - LDAP 서버 SSL 포트 번호

8. LDAP 관리 사용자를 위한 DN과 암호를 입력하십시오(예를 들어, cn=root). 이제 LDAP 서버에 Policy Director 암호 정보가 포함되었습니다.
9. 관리 서버와 LDAP 서버 간에 SSL 통신의 사용 가능 또는 사용 불가능 여부를 선택하십시오.

   각 Policy Director 서버와 LDAP 서버 간에 SSL 통신을 개별적으로 사용 가능 또는 사용 불가능하게 만들 수 있습니다. 이 경우 관리 서버와 LDAP 서버 간에 사용자가 SSL 통신을 설정합니다.
10. SSL 통신을 사용 불가능하게 한 경우, 이 단계를 건너뛰십시오. SSL 통신을 사용 가능하게 한 경우, 다음 프롬프트에 값을 제공하십시오.
    - SSL 키 링 파일 위치
    - SSL 키 레이블
    - SSL 키용 암호
11. 31 페이지의 『접미어 추가』에서 추가한 GSO 데이터베이스 접미어에 DN을 제공하여 GSO 데이터베이스 액세스를 사용 가능하게 만드십시오.

    예를 들면, 다음과 같습니다.

    ```
    o=IBM,c=US
    ```

    GSO 데이터베이스 액세스가 구성되면 Policy Director 구성 관리자가 자동으로 DSB를 구성합니다. 완료할 때마다 일련의 메시지가 자동화 단계를 나열합니다.

    IVMgr 패키지 설치가 성공한 것을 나타내는 메시지가 표시됩니다. 사용 가능한 패키지의 목록이 다시 나옵니다.

WebSEAL 및 NetSEAL을 위한 보안 관리자 설치

보안 관리자 패키지(IVNet)에는 기본 패키지로부터의 자원이 필요합니다. IVNet를 설치하기 전에 기본 구성요소를 설치했는지 확인하십시오.

1. IVNet에 대한 선택 번호를 입력하여 Policy Director 보안 관리자 파일을 설치한 다음 Enter 키를 누르십시오.

   CD로부터 파일이 발췌되어 하드 디스크의 기본 디렉토리에 설치됩니다.

사용자 레지스트리로 LDAP를 사용할 경우, 보안 관리자를 LDAP 서버에 통합하기 위한 일련의 프롬프트가 나옵니다.

2. 프롬프트가 표시될 경우, LDAP 서버 구성에 필요한 정보를 입력하십시오.
   - LDAP 서버 호스트 이름
   - LDAP 서버 포트 번호
   - LDAP 서버 SSL 포트 번호

   위에 있는 LDAP 서버 구성 프롬프트는 LDAP 서버와의 통신이 이 시스템의 기타 Policy Director 패키지에 대해 이전에 구성되지 않은 경우에만 나옵니다. 관리 서버(IVMgr)나 권한 부여 서버(IVAcld)가 이 시스템에 구성된 경우, 이 단계에서는 앞에서 언급한 프롬프트들이 나오지 않습니다.
3. LDAP 관리 사용자를 위한 DN과 암호를 입력하십시오.

   이제 LDAP 서버에 Policy Director 보안 정보가 포함되었습니다.
4. 보안 관리자와 LDAP 서버 간에 SSL 통신의 사용 가능 또는 사용 불가능 여부를 선택하십시오.

   각 Policy Director 서버와 LDAP 서버 간에 SSL 통신을 개별적으로 사용 가능 또는 사용 불가능하게 만들 수 있습니다. 이 경우 보안 관리자와 LDAP 서버 간에 사용자가 SSL 통신을 설정합니다.
5. SSL 통신을 사용 불가능하게 한 경우, 이 단계를 건너뛰십시오. SSL 통신을 사용 가능하게 한 경우, 다음 프롬프트에 값을 제공하십시오.
   - SSL 키 링 파일 위치
   - SSL 키 레이블
   - SSL 키용 암호
6. 31 페이지의 『접미어 추가』에서 추가한 GSO 데이터베이스 접미어에 DN을 제공하여 GSO 데이터베이스 액세스를 사용 가능하게 만드십시오.

   예를 들면, 다음과 같습니다.

   ```
   o=IBM,c=US
   ```

   DCE 셀 관리자 이름과 암호를 요청하는 프롬프트가 나옵니다.
7. DCE 셀 관리자 계정에 액세스하기 위해 필요한 정보를 입력하십시오.

```
셀 관리자 [cell_admin]의 사용자 이름 입력:
셀 관리자의 암호 입력:
```

보안 관리자가 구성되어 시작됩니다.

CAS 서버가 구성되어 시작됩니다.

IVNet 패키지 설치가 성공한 것을 나타내는 프롬프트가 나옵니다. 사용 가능한 패키지의 목록이 다시 나옵니다.

WebSEAL 구성요소 사용 가능

WebSEAL 구성요소를 사용 가능하게 하려면, WebSEAL(IVWeb) 패키지를 설치하십시오.

1. IVWeb에 대한 선택 번호를 입력하여 WebSEAL HTTP 서버 구성요소를 사용 가능하게 만드는 데 필요한 파일들을 설치하십시오.
2. 계속하려면 Enter 키를 누르십시오.

   CD로부터 파일이 발췌되어 하드 디스크에 설치됩니다.

   구성 목록은 HTTP 및 HTTPS 클라이언트 액세스, 필요한 TCP 포트, 기본 웹 문서 루트 디렉토리를 확인하는 값과 함께 나옵니다.
3. 현재 구성 값을 확인하십시오.

   ```
   웹 서버 구성을 확인하십시오.
   1. Enable TCP HTTP?     예
   2. HTTP 포트    80
   3. HTTPS 사용 가능?     예
   4. HTTPS 포트   443
   5. 웹 문서 루트 디렉토리 /opt/Policy Director/www/docs

   a. 구성 허용 후 설치 계속
   x. 설치 종료

   변경 항목 선택: a
   ```
4. 구성을 허용하고 설치를 계속하려면 a를 입력한 다음 Enter 키를 누르십시오.
5. DCE 셀 관리자 계정에 액세스하기 위해 필요한 정보를 입력하십시오.

   ```
   셀 관리자 [cell_admin]의 사용자 이름 입력:
   셀 관리자의 암호 입력:
   ```

컴퓨터에 설치를 구성하고 WebSEAL을 사용 가능하게 만드십시오. 보안 관리자가 자동으로 재시작합니다.

NetSEAL 구성요소 사용 가능

NetSEAL 구성요소를 사용 가능하게 하려면, NetSEAL(IVTrap) 패키지를 설치하십시오.

1. IVTrap에 대한 선택 번호를 입력하여 NetSEAL의 비정교한 TCP/IP 액세스 제어 구성요소를 사용 가능하게 만드는 데 필요한 파일들을 설치한 다음 Enter 키를 누르십시오.

   NetSEAL이 구성 및 사용 가능하게 되었습니다.

   DCE 셀 관리자의 이름과 암호를 요청하는 프롬프트가 나옵니다.

2. DCE 셀 관리자 계정에 액세스하기 위해 필요한 정보를 입력하십시오.

   ivadmin 명령을 사용하여 보호된 포트를 지정하는 것이 필요함을 나타내는 메시지가 나옵니다.

   보호된 모든 포트가 NetSEAL 제어하에 있음을 확인하기 위해서 시스템을 재시작(재부트)하는 것이 필요함을 나타내는 다른 메시지가 나옵니다.

   IVTrap 패키지 설치가 성공한 것을 나타내는 프롬프트가 표시됩니다. 사용 가능한 패키지의 목록이 다시 나옵니다.

Policy Director NetSEAL이 특정 포트에 이루어진 요청을 트랩합니다. NetSEAL 트랩을 사용하기 위해서는 지정된 포트를 사용하는 모든 응용 프로그램을 중단하고 다시 시작해야 합니다. Policy Director NetSEAL 구성에 관한 자세한 정보는 *Policy Director Administration Guide*에서 NetSEAL에 관한 개요 정보를 참조하십시오.

권한 부여 서버 설치

권한 부여 서버를 설치하려면 다음과 같이 하십시오.

1. IVAcld에 대한 선택 번호를 입력하여 Policy Director 권한 부여 서버 파일을 설치한 다음 Enter 키를 누르십시오.

   CD로부터 파일이 발췌되어 하드 디스크의 기본 디렉토리에 설치됩니다.

   사용자 레지스트리로 LDAP를 사용할 경우, 권한 부여 서버를 LDAP 서버에 통합하기 위한 일련의 프롬프트가 나옵니다.

2. 프롬프트가 표시될 경우, LDAP 서버 구성에 필요한 정보를 입력하십시오.
   - LDAP 서버 호스트 이름
   - LDAP 서버 포트 번호
   - LDAP 서버 SSL 포트 번호

   위에 있는 LDAP 서버 구성 프롬프트는 이 시스템에 LDAP 서버와의 통신이 기타 Policy Director 패키지에 대해 이전에 구성되지 않은 경우에만 나옵니다. 관리 서버(IVMgr)나 보안 관리자(IVNet)가 이 시스템에 구성된 경우, 이 단계에서는 앞에서 언급한 프롬프트들이 나오지 않습니다.
3. LDAP 관리 사용자를 위한 DN과 암호를 입력하십시오.

   이제 LDAP 서버에 Policy Director 암호 정보가 포함되었습니다.
4. 관리 서버와 LDAP 서버 간에 SSL 통신의 사용 가능 또는 사용 불가능 여부를 선택하십시오.

   각 Policy Director 서버와 LDAP 서버 간에 SSL 통신을 개별적으로 사용 가능 또는 사용 불가능하게 만들 수 있습니다. 이 경우 관리 서버와 LDAP 서버 간에 사용자가 SSL 통신을 설정합니다.
5. SSL 통신을 사용 불가능하게 한 경우, 이 단계를 건너뛰십시오. SSL 통신을 사용 가능하게 한 경우, 다음 프롬프트에 값을 제공하십시오.
   - SSL 키 링 파일 위치
   - SSL 키 레이블
   - SSL 키용 암호
6. 31 페이지의 『접미어 추가』에서, 추가한 GSO 데이터베이스 접미어에 DN을 제공하여 GSO 데이터베이스 액세스를 사용 가능하게 만드십시오.

   예를 들면, 다음과 같습니다.

   ```
   o=IBM,c=US
   ```

   DCE 셀 관리자 이름과 암호를 요청하는 프롬프트가 나옵니다.
7. DCE 셀 관리자 계정에 액세스하기 위해 필요한 정보를 입력하십시오.

   ```
   셀 관리자 [cell_admin]의 사용자 이름 입력:
   셀 관리자의 암호 입력:
   ```

   권한 부여 서버가 구성되어 시작됩니다.

IVAcld 패키지 설치가 성공한 것을 나타내는 프롬프트가 표시됩니다. 사용 가능한 패키지의 목록이 다시 나옵니다.

권한 부여 API 구성요소 설치

C 파일용 권한 부여 API를 설치하려면 IVAuthADK를 위한 선택 번호를 입력한 다음 Enter 키를 누르십시오.

CD로부터 파일이 발췌되어 하드 디스크의 기본 디렉토리에 설치됩니다.

IVAuthADK 패키지 설치가 성공한 것을 나타내는 프롬프트가 표시됩니다. 사용 가능한 패키지의 목록이 다시 나옵니다.

DCE 사용자 레지스트리를 사용하는 Policy Director 서버 설치

LDAP 사용자 레지스트리를 사용하는 Policy Director를 설치할 경우, 80 페이지의 『LDAP 사용자 레지스트리를 사용하는 Policy Director 서버 설치』로 가십시오.

서버 패키지들은 *IBM SecureWay Policy Director 버전 3.0* CD의 /solaris 디렉토리에 있습니다.

Policy Director 패키지를 설치하기 위해서는 사용자 루트로서 로그온해야 합니다.

패키지를 다시 설치해야 할 경우에는 먼저 기존의 패키지(**pkgrm**)를 제거한 다음 원하는 패키지를 다시 설치해야 합니다.

관리 서버를 설치하는 방법은 다음과 같습니다.

1. **pkgadd** 명령을 입력하여 CD로부터 사용 가능한 패키지들을 나열하십시오.

   ```
   # pkgadd -d /cdrom/cdrom0/solaris
   ```

   사용 가능한 패키지의 목록이 화면에 나옵니다.

   다른 CD-ROM 마운트 포인트를 사용 중이면, 위의 명령에 나오는 것으로 대체하십시오.
2. IVBase에 대한 선택 번호를 입력하여 Policy Director 기본 파일을 설치한 다음 Enter 키를 누르십시오.

이 명령이 CD로부터 파일들을 발췌하여 사용자가 지정한 하드 디스크에 파일들을 설치합니다.

IVBase 패키지 설치가 성공한 것을 나타내는 프롬프트가 표시됩니다. 사용 가능한 패키지의 목록이 다시 나옵니다.

다음 단계를 계속하기 전에, 보안 도메인에는 한 인스턴스의 관리 서버(IVMgr)만 있어야 한다는 점을 기억하십시오. 현재 독립형 시스템 설치를 진행 중이면 다음 단계를 계속하십시오. 2차 서버에 설치하는 중이면, 23 페이지의 『보안 도메인을 위한 설치 요구사항』을 반드시 검토하십시오.

3. IVMgr에 대한 선택 번호를 입력하여 Policy Director 관리 서버 파일을 설치하십시오. Enter 키를 누르십시오.

   이 명령이 CD로부터 파일들을 발췌하여 사용자가 지정한 하드 디스크에 파일을 설치합니다.

   사용자 레지스트리 유형을 선택하도록 프롬프트가 표시됩니다.

4. 사용자 레지스트리로 DCE를 사용할 경우, 1을 입력하십시오.

   DCE 셀 관리자 이름과 암호를 요청하는 프롬프트가 나옵니다.

5. DCE 셀 관리자 계정에 액세스하기 위해 필요한 정보를 입력하십시오.

   ```
   셀 관리자 [cell_admin]의 사용자 이름 입력:
   셀 관리자의 암호 입력:
   ```

   IVMgr 패키지 설치가 성공한 것을 나타내는 메시지가 표시됩니다. 사용 가능한 패키지의 목록이 다시 나옵니다.

WebSEAL 및 NetSEAL을 위한 보안 관리자 설치

보안 관리자 패키지(IVNet)에는 기본 패키지로부터의 자원이 필요합니다. IVNet를 설치하기 전에 기본 구성요소를 설치했는지 확인하십시오.

1. IVNet에 대한 선택 번호를 입력하여 Policy Director 보안 관리자 파일을 설치한 다음 Enter 키를 누르십시오.

   CD로부터 파일이 발췌되어 하드 디스크의 기본 디렉토리에 설치됩니다. DCE 셀 관리자 이름과 암호를 요청하는 프롬프트가 나옵니다.

2. DCE 셀 관리자 계정에 액세스하기 위해 필요한 정보를 입력하십시오.

```
셀 관리자 [cell_admin]의 사용자 이름 입력:
셀 관리자의 암호 입력:
```

보안 관리자가 구성되어 시작됩니다.

IVNet 패키지 설치가 성공한 것을 나타내는 프롬프트가 나옵니다. 사용 가능한 패키지의 목록이 다시 나옵니다.

WebSEAL 구성요소 사용 가능

WebSEAL 구성요소를 사용 가능하게 하려면 WebSEAL(IVWeb) 패키지를 설치하십시오.

1. IVWeb에 대한 선택 번호를 입력하여 WebSEAL HTTP 서버 구성요소를 사용 가능하게 만드는 데 필요한 파일들을 설치하십시오.
2. 계속하려면 Enter 키를 누르십시오.

   CD로부터 파일이 발췌되어 하드 디스크에 설치됩니다.

   구성 목록은 HTTP 및 HTTPS 클라이언트 액세스, 필요한 TCP 포트 및 기본 웹 문서 루트 디렉토리를 확인하는 값과 함께 나옵니다.
3. 현재 구성 값을 확인하십시오.

```
웹 서버 구성을 확인하십시오.
1. Enable TCP HTTP?     예
2. HTTP 포트    80
3. HTTPS 사용 가능?     예
4. HTTPS 포트   443
5. 웹 문서 루트 디렉토리 /opt/Policy Director/www/docs

a. 구성 허용 후 설치 계속
x. 설치 종료

변경 항목 선택: a
```

4. 구성을 허용하고 설치를 계속하려면 a를 입력한 다음 Enter 키를 누르십시오.
5. DCE 셀 관리자 계정에 액세스하기 위해 필요한 정보를 입력하십시오.

```
셀 관리자 [cell_admin]의 사용자 이름 입력:
셀 관리자의 암호 입력:
```

컴퓨터에 설치를 구성하고 WebSEAL을 사용 가능하게 만드십시오. 보안 관리자가 자동으로 재시작합니다.

NetSEAL 구성요소 사용 가능

NetSEAL 구성요소를 사용 가능하게 하려면 NetSEAL(IVTrap) 패키지를 설치하십시오.

1. IVTrap에 대한 선택 번호를 입력하여 NetSEAL 비정교한 TCP/IP 액세스 제어 구성요소를 사용 가능하게 만드는 데 필요한 파일들을 설치한 다음 Enter 키를 누르십시오.

   NetSEAL이 구성 및 사용 가능하게 되었습니다.

   DCE 셀 관리자의 이름과 암호를 요청하는 프롬프트가 나옵니다.

2. DCE 셀 관리자 계정에 액세스하기 위해 필요한 정보를 입력하십시오.

   ivadmin 명령을 사용하여 보호된 포트를 지정하는 것이 필요함을 나타내는 메시지가 나옵니다.

   보호된 모든 포트가 NetSEAL 제어하에 있음을 확인하기 위해서 시스템을 재시작(재부트)하는 것이 필요함을 나타내는 다른 메시지가 나옵니다.

   IVTrap 패키지 설치가 성공한 것을 나타내는 프롬프트가 표시됩니다. 사용 가능한 패키지의 목록이 다시 나옵니다.

Policy Director NetSEAL이 특정 포트에 이루어진 요청을 트랩합니다. NetSEAL 트랩을 사용하기 위해서는 지정된 포트를 사용하는 모든 응용 프로그램을 중단하고 다시 시작해야 합니다. Policy Director NetSEAL 구성에 관한 자세한 정보는 *Policy Director Administration Guide*에서 NetSEAL에 관한 개요 정보를 참조하십시오.

권한 부여 서버 설치

권한 부여 서버를 설치하려면 다음과 같이 하십시오.

1. IVAcld에 대한 선택 번호를 입력하여 Policy Director 권한 부여 서버 파일을 설치한 다음 Enter 키를 누르십시오.

   CD로부터 파일이 발췌되어 하드 디스크의 기본 디렉토리에 설치됩니다. DCE 셀 관리자 이름과 암호를 요청하는 프롬프트가 나옵니다.

2. DCE 셀 관리자 계정에 액세스하기 위해 필요한 정보를 입력하십시오.

   ```
   셀 관리자 [cell_admin]의 사용자 이름 입력:
   셀 관리자의 암호 입력:
   ```

권한 부여 서버가 구성되어 시작됩니다.

IVAcld 패키지 설치가 성공한 것을 나타내는 프롬프트가 표시됩니다. 사용 가능한 패키지의 목록이 다시 나옵니다.

권한 부여 API 구성요소 설치

C 파일용 권한 부여 API를 설치하려면 IVAuthADK를 위한 선택 번호를 입력한 다음 Enter 키를 누르십시오.

CD로부터 파일이 발췌되어 하드 디스크의 기본 디렉토리에 설치됩니다.

IVAuthADK 패키지 설치가 성공한 것을 나타내는 프롬프트가 표시됩니다. 사용 가능한 패키지의 목록이 다시 나옵니다.

인증 획득 서비스 구성

Policy Director CAS는 자동으로 설치됩니다. Policy Director CAS를 인증 획득 서비스로 사용할 경우, 반드시 구성해야 합니다. *Policy Director Administration Guide*의 인증 획득 서비스 구성에 관한 정보를 참조하십시오.

관리 콘솔 설치

Policy Director는 많은 Policy Director 구성요소를 관리하는 관리 콘솔을 제공합니다.

Solaris용 관리 콘솔는 IVConsole 설치 패키지를 사용하여 설치됩니다. 패키지를 설치 및 구성하려면 **pkgadd**를 사용하십시오.

1. 루트로서 로그인하십시오.
2. *IBM SecureWay Policy Director 버전 3.0* CD를 Policy Director 서버 시스템의 CD-ROM 드라이브에 넣으십시오.
3. 사용 가능한 패키지의 목록을 다음과 같이 표시하십시오.

   ```
   # pkgadd -d /cdrom/cdrom0/solaris
   ```

4. 아직 설치되지 않은 경우, IVBase에 대한 선택 번호를 입력하십시오. IVBase가 이미 설치되었으면 92 페이지의 6단계로 가십시오.

5. 계속하려면 y를 누르십시오.

   패키지 목록이 나옵니다.

6. IVConsole을 위한 선택 번호를 입력하십시오.
7. 계속하려면 y를 누르십시오.

   성공적인 설치를 나타내는 프롬프트가 나옵니다. 이제 관리 콘솔을 시작할 준비가 되었습니다.

관리 콘솔 시작

관리 콘솔을 시작하려면 다음과 같이 하십시오.

1. Policy Director 서버가 설치되어 실행되고 있는지 확인하십시오.
2. 다음 명령을 입력하십시오.

```
$ /opt/intraverse/bin/ivconsole
```

Policy Director 제거

컴퓨터에서 Policy Director 서버를 제거할 때에는 **pkgrm** 유틸리티를 사용하십시오. 설치시 순서와 반대로 패키지를 제거해야 합니다. **pkgrm**과 **pkgadd** 명령은 같은 유틸리티 계열의 멤버들이고 같은 사용자 인터페이스를 가집니다. 루트 사용자가 **pkgrm** 유틸리티를 실행합니다.

이 명령을 사용하는 방법에는 여러 가지가 있습니다.

- 인수 없이 **pkgrm** 명령을 시작하십시오.

  시스템에 있는 현재 패키지 목록이 번호와 함께 나옵니다. 제거할 패키지에 대해 하나의 선택 번호를 입력하십시오.

- **pkgrm** 명령을 시작하고 명령에 대한 인수로서 하나의 패키지 이름을 지정하십시오. 예를 들면, 다음과 같이 할 수 있습니다.

  ```
  # pkgrm IVBase
  ```

- **pkgrm** 명령을 시작하고 명령에 대한 여러 인수로서 패키지 이름들을 차례로 지정하십시오. 예를 들면, 다음과 같이 할 수 있습니다.

  ```
  # pkgrm IVAuthADK IVAcld IVTrap IVWeb IVNet IVMgr IVBase
  ```

pkgrm 명령에 관한 자세한 정보는 Solaris 운영체제 문서를 참조하십시오.

주: 반드시 설치에 요구되는 것과 정확히 반대 순서로 Policy Director 패키지를 제거해야 합니다.

Policy Director를 제거하려면 다음과 같이 하십시오.

1. 루트로서 Solaris 운영체제에 로그인하십시오.

   앞에 나오는 **pkgrm** 명령을 시작하는 방법 중 하나를 사용하십시오.

2. Policy Director 구성요소는 반드시 다음 순서로 제거해야 합니다.
   - IVTrap
   - IVWeb
   - IVNet
   - IVAuthADK
   - IVAcld
   - IVMgr
   - IVBase

   사용자의 컴퓨터 시스템 구성이 위에 있는 패키지를 모두 가지지 않을 수도 있습니다. IVBase에 앞서 Policy Director 관리 콘솔(IVConsole)을 제거할 수 있습니다.

관리 콘솔 제거

관리 콘솔을 제거하려면 다음과 같이 하십시오.

1. 사용자 루트로서 로그인하십시오.
2. 다음 명령을 입력하십시오.

   ```
   # pkgrm ivconsole
   ```

제8장 관련 문서

이 장에 나오는 문서들을 사용하여 Policy Director 버전 3.0과 관련 제품에 관한 자세한 정보를 찾아 볼 수 있습니다.

Policy Director 문서

Policy Director 제품과 함께 제공되는 *IBM SecureWay Policy Director 시작 및 실행, 버전 3.0*은 문서 팩에서도 구할 수 있습니다. Policy Director 문서 팩에는 이 책과 Policy Director 사용권 정보가 포함되어 있습니다.

이 책외에 다음 문서에도 Policy Director에 관한 정보가 포함되어 있으며, 각 문서들은 *IBM SecureWay Policy Director 버전 3.0* CD의 /doc 서브디렉토리에서 PDF(PostScript Document Format) 형식으로 구할 수 있습니다.

- *IBM SecureWay Policy Director Administration Guide, 버전 3.0*

  이 책은 Policy Director 관리에 관한 세부사항을 제공합니다. 이 책은 다음과 같은 IBM SecureWay Policy Director에 관한 정보를 제공합니다.

  – 인증, 권한 부여, 인증 획득과 같은 Policy Director 개념
  – 관리 콘솔을 사용하는 일반 관리 작업
  – WebSEAL 관리
  – NetSEAL 관리
  – NetSEAT 관리
  – 관리 자원(**ivadmin** 명령)

- *IBM SecureWay Policy Director Programming Guide and Reference, 버전 3.0*

  이 책은 권한 부여 API 구성요소와 그 작업 수행 방법을 설명합니다.
  – 권한 부여 API를 사용하여 응용 프로그램 작성
  – Policy Director 권한 부여 서비스 초기화
  – 응용 프로그램 서버나 클라이언트 인증

- 사용자 인증 확보
- 권한 부여 결정
- 선택적 작업 수행
- 정리 및 종료
- 권한 부여 API를 사용하여 응용 프로그램 전개

Policy Director README 파일에는 출판된 제품 서적을 교체시킨 Policy Director 정보에 관한 최신 정보가 있습니다.

최신 README 파일은 IBM SecureWay Policy Director 웹 사이트에서 구할 수 있습니다.

`http://www.ibm.com/software/security/policy/library`

IBM SecureWay FirstSecure 문서

다음 책에는 FirstSecure에 관한 정보가 있습니다.

- *IBM SecureWay FirstSecure Planning and Integration, Version 2.0 (S564-8D11–00)*

  이 책은 FirstSecure와 FirstSecure를 구성하는 제품에 관해 설명하며 모든 IBM SecureWay 제품 사용 계획에 도움을 줍니다.

IBM SecureWay Policy Director(Policy Director)는 IBM SecureWay FirstSecure의 구성요소 또는 독립 제품으로 사용이 가능합니다. 사용 중인 Policy Director 버전이 FirstSecure 제공품에 포함된 경우, FirstSecure와 함께 이 책을 제공받습니다. 독립 제품으로 Policy Director 버전을 구입한 경우에는 FirstSecure 웹 페이지에서 이 책을 찾을 수 있습니다.

`http://www.ibm.com/software/security/firstsecure/library`

IBM DCE 문서

다음 문서들은 DCE를 설치하는 방법을 설명하는 것으로서 *IBM SecureWay Policy Director 보안 서비스* CD의 /doc에서 PDF 형식으로 또는 DCE 웹 사이트에서 구할 수 있습니다.

`http://www.ibm.com/network/dce/library/`

Windows NT용 IBM DCE

*Windows NT용 IBM 분산 컴퓨팅 환경 빠른 시작, 버전 2.2*는 다음 웹 주소에서 구할 수 있습니다.

`http://www.software.ibm.com/network/dce/library/publications/dcent.html`

이 책은 Distributed Computing Environment (DCE) for Windows NT, Version 2.2와 제품을 계획, 설치 및 구성하는 방법에 관해 설명합니다.

IBM Distributed Computing Environment for Windows NT Quick Beginnings Version 2.2 책은 또한 *IBM SecureWay Policy Director 보안 서비스* CD의 /doc/DCE22_QuickBeginnings_NT.pdf에서도 구할 수 있습니다.

AIX용 IBM DCE

*IBM Distributed Computing for AIX Quick Beginnings Version 2.2*는 다음 웹 주소에서 구할 수 있습니다.

`http://www.software.ibm.com/network/dce/library/publications/dceaix.html`

이 책은 IBM Distributed Computing Environment for AIX, Version 2.2(AIX용 DCE 2.2)와 제품을 계획, 설치 및 구성하는 방법에 관해 설명합니다.

*IBM Distributed Computing Environment for AIX Quick Beginnings Version 2.2*는 또한 *IBM SecureWay Policy Director 보안 서비스* CD의 /doc/DCE22_QuickBeginnings_AIX.pdf에서도 구할 수 있습니다.

Solaris용 Transarc DCE

*Transarc DCE 버전 2.0 설치하기 전에*와 *설치 및 구성 안내서*는 다음 웹 주소에서 구할 수 있습니다.

`http://www.transarc.com/Library/documentation/dce/2.0/index.html`

Transarc DCE 버전 2.0 설치하기 전에 문서에는 Transarc DCE 소프트웨어 및 문서에 관한 다음 정보들이 수록되어 있습니다.

- OSF DCE와 DCE * DFS 제품 간의 차이점
- DCE * DFS 버전 2.0과 버전 1.1 간의 차이점

- DCE * DFS와 연관된 알려진 결함 및 제한점

Transarc DCE 버전 2.0 시작하기 전에 문서는 또한 *IBM SecureWay Policy Director 보안 서비스* CD의 /doc/DCE20_ReleaseNotes_Solaris.pdf에서도 구할 수 있습니다.

*설치 및 구성 안내서*는 DCE DFS 2.0 제품의 설치, 구성, 이주에 관한 지시사항을 제공합니다.

*설치 및 구성 안내서*는 *IBM SecureWay Policy Director 보안 서비스* CD의 /doc/DCE20_InstallGuide_Solaris.pdf에서도 구할 수 있습니다.

IBM SecureWay Directory 문서

다음 책에는 IBM SecureWay Directory(LDAP)를 위한 설치 및 구성 정보가 있습니다.

- *IBM SecureWay Directory Installation and Configuration, Version 3.1.1*

  지원되는 각 운영체제별로 이 책에 대한 별도의 버전이 HTML 형식으로 준비되어 있습니다. 해당 CD의 /doc/wparent.htm에 각 운영체제에 대한 책이 있습니다. 다음과 같은 CD가 있습니다.

  – *NT용 IBM SecureWay Directory 버전 3.1.1*

  – *AIX용 IBM SecureWay Directory 버전 3.1.1*

  – *Solaris용 IBM SecureWay Directory 버전 3.1.1*

  LDAP 설치 후 설치 및 구성 .HTM 문서 파일의 위치는 다음과 같습니다.

  ```
  C:\Program Files\IBM\LDAP\nls\html\enUS1252\config\wparent.htm
  ```

HTML 파일로 된 다음 책에는 IBM SecureWay를 관리하는 방법에 관한 정보가 포함되어 있습니다.

- *IBM SecureWay Directory Administration Guide, Version 3.1.1*

  1. LDAP의 기본 설치 후 다음 웹 주소에서 찾을 수 있는 문서에 웹 브라우저를 사용하여 액세스하십시오.

     ```
     C:\Program Files\IBM\LDAP\nls\html\enUS1252\config\wparent.ht
     ```

HTML 형식으로 된 다음 책에는 IBM SecureWay Directory 클라이언트에 관한 정보가 포함되어 있습니다.

- *IBM SecureWay Directory Client SDK Programming Reference, Version 3.1.1*

  이 책에는 다음 LDAP 정보에 대한 링크가 포함되어 있습니다.

  – LDAP 클라이언트 SDK 플러그인 프로그래밍 참조서 정보

    1. LDAP의 기본 설치 후 다음 웹 주소에서 찾을 수 있는 문서에 웹 브라우저를 사용하여 액세스하십시오.

       `C:\Program Files\IBM\doc\progref.htm`

    2. *IBM SecureWay Directory 클라이언트 SDK 프로그래밍 참조서*를 여십시오.
    3. **부록**을 누르십시오.
    4. **LDAP Client SDK 플러그인 프로그래밍 참조서**를 누르십시오.

  – GSKit 및 키 관리 툴 **ikmguiw**의 사용법과 SSL 액세스를 지원하는 LDAP 서버 구성법에 관한 정보

    1. *IBM SecureWay Directory 클라이언트 SDK 프로그래밍 참조서*를 아직 열지 않았으면 여십시오.
    2. **API 범주**를 누르십시오.
    3. **SSL**을 누르십시오.
    4. **LDAP_SSL API**를 누르십시오.
    5. 적절한 HTML 파일을 열려면 **IKMGUI 사용** 링크를 찾아서 누르십시오.

또한 다음 문서들도 IBM SecureWay Directory 서버에 사용할 수 있습니다.

- *IBM SecureWay Directory Server Plug-ins Reference*

부록. 주의사항

이 정보는 미국내에서 제공되는 제품 및 서비스를 위해 개발되었습니다. 다른 나라에서는 본 문서에 나오는 제품, 서비스 또는 기타 기능들이 IBM에 의해 제공되지 않을 수 있습니다. 귀하께서 현재 사용할 수 있는 제품 및 서비스에 관한 자세한 정보는 귀사를 담당하는 IBM 영업대표에게 문의하십시오. IBM 제품, 프로그램 또는 서비스에 대한 어떠한 언급도 IBM 제품, 프로그램 또는 서비스만 사용해야 한다는 것을 의미하지는 않습니다. IBM의 지적재산권을 침해하지 않는 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수 있습니다. 그러나 IBM 제품이 아닌 타사의 제품, 프로그램 또는 서비스와 함께 수행된 작동의 평가 및 검증은 사용자의 책임사항입니다.

IBM은 본 문서에서 다루는 주제와 관련하여 특허를 보유하거나 출원중인 응용 프로그램을 소유하고 있을 수 있습니다. 이 문서를 제공한다고 해서 그러한 특허에 대한 사용권까지 부여하는 것은 아닙니다. 특허 사용권에 대한 문의는 다음 주소로 하십시오.

150-010
서울특별시 영등포구 여의도동 25-11, 한진해운빌딩
한국아이.비.엠주식회사
지적재산권부

다음 내용은 영국 및 해당 지역 법규에 일치하지 않는 국가에는 적용되지 않습니다. IBM은 본 출판물을 어떠한 종류의 보증도 없이『현상대로』제공하며 달리 법에 규정되어 있지 않은 한, 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 비롯하여 어떠한 형태의 묵시적 혹은 명시적 보증을 하지 않습니다. 일부 주에서는 특정 거래에 있어서 명시적 또는 묵시적 보증의 포기가 허용되지 않을 수도 있습니다. 따라서 이 내용이 사용자에게 적용되지 않을 수도 있습니다.

이 정보에는 기술상으로 정확하지 않거나 인쇄상의 오류가 있을 수 있습니다. 본 정보는 정기적으로 변경되며, 변경사항은 개정판에 통합됩니다. IBM은 이 정보에 설명된 제품 및/또는 프로그램을 사전 통보 없이 언제라도 개선 및/또는 수정할 수 있습니다.

이 정보에서 언급된 IBM 이외의 웹 사이트는 단지 사용자의 이해를 돕기 위한 것이며, 이러한 웹 사이트를 보증하는 것은 아닙니다. 이 웹 사이트에 있는 자료는 IBM 제품 자료의 일부가 아니며, 이 웹 사이트의 사용에 대한 책임은 사용자에게 있습니다.

IBM은 독자가 보낸 정보가 타당한 경우 적절한 방식으로 이를 사용하거나 배포할 수 있으며, 정보를 제공한 독자는 이에 대해 책임을 지거나 사용에 제한을 받지 않습니다.

(i) 독립적으로 작성한 프로그램 및 다른 프로그램(이 프로그램 포함) 간의 정보 교환과 (ii) 교환된 정보의 상호 사용을 목적으로 그 프로그램 정보를 필요로 하는 사용권자는 다음 주소로 문의하십시오.

150-010
서울특별시 영등포구 여의도동 25-11, 한진해운빌딩
한국아이.비.엠주식회사
소프트웨어 사업본부

그러한 정보는 일부 경우에 따라 수수료를 지불하여 적절한 조항과 조건에 따라 사용 가능합니다.

IBM은 본 문서에서 설명하는 사용권 프로그램과 그러한 프로그램을 사용할 수 있는 모든 사용권 자료들은 IBM 고객 계약서, IBM 프로그램 사용권 계약 또는 이와 동등한 계약 조건하에서 IBM에 의해 제공됩니다.

여기에 포함된 성능 자료는 제어 환경하에서 측정된 것입니다. 따라서 기타 운영 환경에서의 결과와는 크게 다를 수 있습니다. 일부 측정값은 개발 단계 시스템에서 얻은 것일 수 있으며, 이러한 측정값이 일반적으로 사용할 수 있는 시스템에서도 같을 것이라고 보장할 수 없습니다. 뿐만 아니라 일부 측정치는 추정을 통해 얻은 것이므로 실제값과 다를 수 있습니다. 이 문서의 사용자는 특정 환경에 해당되는 자료를 확인해야 합니다.

IBM 제품 이외의 것에 관한 정보는 해당 제품의 제조업체, 출간물 또는 그 외 사용가능한 공식 소스를 통해 구한 것입니다. IBM은 IBM 제품이 아닌 것과 관련된 불만 사항이나 성능 및 호환성 문제에 대해서는 보장하지 않으며 그와 같은 제품은 테스트하지 않았습니다. IBM 제품이 아닌 제품의 성능에 대한 문의는 해당 제조업체로 하십시오.

IBM의 향후 방향이나 의도에 관한 공고는 사전 통지 없이 변경되거나 철회될 수 있으며 이는 단지 목적이나 목표를 제시하는 것에 지나지 않습니다.

표시된 모든 IBM 가격은 IBM에서 제안하는 현재의 소매가로서 사전 통지 없이 변경될 수 있습니다. 딜러 가격과는 다를 수 있습니다.

본 정보에는 일상적인 업무에서 사용되는 자료 및 보고서의 견본이 들어 있습니다. 그러한 자료를 최대한 구체적으로 설명하기 위해 특정 개인, 회사, 상표 및 제품명이 언급되는 경우가 있습니다. 그러나 이러한 모든 이름은 가공의 것이며 실제 사용되는 이름 및 주소와 유사한 경우 전적으로 우연의 일치입니다.

등록상표

다음에 나오는 용어는 IBM사의 등록상표입니다.

AIX
DB2
FirstSecure
IBM
Policy Director
SecureWay

그 밖의 기타 회사, 제품 또는 서비스명은 다른 회사의 등록상표나 서비스 상표입니다.

AuthAPI	DASCOM, Inc.
DASCOM	DASCOM, Inc.
Internet Explorer	Microsoft Corporation
Netscape 및 Netscape 로고	Netscape Communications Corporation
Netscape Communicator	Netscape Communications Corporation
Netscape Navigator	Netscape Communications Corporation

NetSEAL	DASCOM, Inc.
NetSEAT	DASCOM, Inc.
Solaris	Sun Microsystems, Inc.
WebSEAL	DASCOM, Inc.

Java 및 모든 Java 기반 등록상표와 로고는 미국과 다른 나라에서 Sun Microsystems, Inc.의 등록상표입니다.

Microsoft, Windows, Windows NT 및 Windows 로고는 미국과 다른 나라에서 Microsoft Corporation의 등록상표입니다.

UNIX는 미국과 다른 나라에서 X/Open Company Limited가 독점권을 갖는 등록상표입니다.

색인

[가]

[다]

[마]

[바]

[사]

[아]

[자]

[차]

[카]

[타]

[파]

[하]

[숫자]

A

B

C

IBM 한글 지원에 관한 설문

FAX : (02) 781-7778

보내 주시는 의견은 더 나은 고객 지원 체제를 위한 귀중한 자료가 됩니다.
독자 여러분의 좋은 의견을 기다립니다.

책 제목: IBM® SecureWay® Policy Directory
시작에서 수행까지
버전 3 릴리스 0

성 명		직위/담당업무	
회 사 명		부 서 명	
주 소			
전화번호		팩스번호	
전자우편 주소			
사용중인 시스템	☐ 중대형 서버 ☐ UNIX 서버 ☐ PC 및 PC 서버		

1. IBM에서 제공하는 한글 책자와 영문 책자 중 어느 것을 더 좋아하십니까? 그 이유는 무엇입니까?
   ☐ 한글 책자 ☐ 영문 책자
   (이유:)

2. 본 책자와 해당 소프트웨어에서 사용된 한글 용어에 대한 귀하의 평가 점수는?
   ☐ 수 ☐ 우 ☐ 미 ☐ 양 ☐ 가

3. 본 책자와 해당 소프트웨어에서 번역 품질에 대한 귀하의 평가 점수는?
   ☐ 수 ☐ 우 ☐ 미 ☐ 양 ☐ 가

4. 본 책자의 인쇄 상태에 대한 귀하의 평가 점수는?
   ☐ 수 ☐ 우 ☐ 미 ☐ 양 ☐ 가

5. 한글 소프트웨어 및 책자가 지원되는 분야에 대해 귀하는 어떻게 생각하십니까?
   ☐ 한글 책자를 늘려야 함 ☐ 현재 수준으로 만족
   ☐ 그다지 필요성을 느끼지 않음

6. IBM은 인쇄물 형식(hardcopy)과 화면 형식(softcopy)의 두 종류로 책자를 제공합니다. 어느 형식을 더 좋아하십니까?
   ☐ 인쇄물 형식(hardcopy) ☐ 화면 형식(softcopy) ☐ 둘 다

☞ IBM 한글 지원 서비스에 대해 기타 제안사항이 있으시면 적어주십시오.

☺ 설문에 답해 주셔서 감사합니다.
귀하의 의견은 저희에게 매우 소중한 것이며, 고객 여러분들께 보다 좋은 제품을 제공해 드리기 위해 최선을 다하겠습니다.

부품 번호: CT63KKO

Printed in Singapore

CT63KKO