Tivoli® SecureWay®
Policy Director for Operating Systems
설치 안내서
버전 3 릴리스 7
Tivoli® SecureWay®
Policy Director for Operating Systems
설치 안내서
버전 3 릴리스 7
Policy Director for Operating Systems 설치 안내서(2000년 12월)
저작권 표시

© Copyright IBM Corporation 2000 All rights reserved. IBM 소프트웨어 사용권 협정이나 IBM 고객 또는 사용권 협정에 대한 Tivoli 제품 추가 협정에 준하여 사용해야 합니다. IBM Corporation의 사전 서면 승인 없이 본 출판물의 어떤 부분도 전자, 기계, 자료, 공학, 화학, 매뉴얼 등 그 밖의 다른 방법이나 형식으로 재생, 전송, 복사하거나 검색 시스템에 저장할 수 없으며 컴퓨터 언어로 옮길 수 없습니다. IBM Corporation은 IBM Corporation의 저작권 표시를 수반하는 경우에 한해서 제한적으로 개인 사용 목적으로 하드카피를 작성하거나 기계로 읽을 수 있는 다른 형태의 문서를 작성할 수 있는 권한을 부여합니다. IBM Corporation의 사전 서면 협정 없는 저작권에서 어떠한 권한도 부여되지 않습니다. 이 문서는 출판을 목적으로 하지 않으므로 어떠한 보증 없이 “현상태로도” 제공됩니다. 이에 따라, 특정 목적을 위한 상업성과 합작성의 보증뿐만 아니라 이 책에 대한 어떠한 보증도 제공하지 않습니다.

등록상표


UNIX는 미국과 기타 국가에서 Open Group을 통해 독점적으로 사용권을 부여받은 등록상표입니다.

기타 회사, 제품 및 서비스 이름은 기타 회사의 등록상표 또는 서비스 상표입니다.

주의사항

본 출판물에서 Tivoli Systems나 IBM 제품, 프로그램 또는 서비스를 언급한다고 해서 Tivoli Systems나 IBM이 활동하고 있는 모든 국가에서 이를 사용할 수 있다는 것을 의미하지는 않습니다. 이러한 제품, 프로그램 또는 서비스의 언급이 Tivoli Systems나 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있음을 나타내지는 않습니다. 저작 재산권 또는 다른 법적으로 보호받을 수 있는 권한에 따라, 가능성이 동일한 어떤 제품, 프로그램 또는 서비스를 언급된 제품, 프로그램 또는 서비스 대신에 사용할 수 있습니다. Tivoli Systems나 IBM이 명시적으로 지정한 경우를 제외하고 다른 제품과 관련된 운영의 평가 및 검증은 사용자의 책임입니다. Tivoli Systems나 IBM은 이 문서의 주된 내용을 다루는 아플리케이션의 특허를 보유하거나 특히 출원중일 수 있습니다. 이책을 제공한다고 해서 특허에 대한 사용권을 제공하는 것은 아닙니다. 134-270, 서울특별시 강남구 도곡동 467-12, 군인공제회관 빌딩, 한국 아이비.컴. 주식회사 고객사무센터에 사전으로 사용권에 대한 문의를 할 수 있습니다.
## 목차

서문 .................................................................................................................. vii
  이 책의 사용자 .................................................................................................. vii
  제반 사항 및 관련 서적 ................................................................................... vii
  이 책의 내용 ..................................................................................................... vii
  이 책에 사용된 규약 ........................................................................................ viii
  플랫폼 특정 정보 ............................................................................................ viii
  피드백 및 서적 제공 ....................................................................................... ix
  고객 지원 문의 ................................................................................................ ix

제1장 PDOS 이해하기 ......................................................................................... 1
  PDOS란? ............................................................................................................. 1
  PDOS의 특성 ...................................................................................................... 1
  PDOS 작동 방법 ............................................................................................... 2
  PDOS 페키지 내용 ............................................................................................ 3
  추가 정보 .......................................................................................................... 4

제2장 PDOS 설치 계획 ......................................................................................... 5
  PDOS로 마이그레이션 ........................................................................................ 5
  AIX, HP-UX 및 Solaris에서의 PDOS 설치에 대한 하드웨어 요구사항 .......... 5
  AIX에서의 PDOS 설치에 대한 소프트웨어 요구사항 .................................. 5
    AIX 4.3.3 이상 .............................................................................................. 5
    AIX 4.3.1 및 AIX 4.3.2 ................................................................................ 6
  HP-UX에서의 PDOS 설치에 대한 소프트웨어 요구사항 ............................... 6
  Solaris에서의 PDOS 설치에 대한 소프트웨어 요구사항 .............................. 6

제3장 PDOS 설치 .................................................................................................. 7
  AIX에 PDOS 설치 ............................................................................................. 7
    SMIT를 사용하여 AIX에 설치 ...................................................................... 7
    명령행을 사용하여 AIX에 설치 ................................................................. 8
  HP-UX에 PDOS 설치 ....................................................................................... 8
    SWinstall을 사용하여 HP-UX에 설치 ....................................................... 8
    명령행을 사용하여 HP-UX에 설치 ............................................................ 9
  Solaris에서 PDOS 설치 .................................................................................... 9
    Admintool을 사용하여 Solaris에 설치 ..................................................... 9
    명령행을 사용하여 Solaris에 설치 ............................................................ 10

제4장 PDOS 구성 ................................................................................................ 11
<table>
<thead>
<tr>
<th>제목</th>
<th>페이지</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDOS 구성 계획</td>
<td>11</td>
</tr>
<tr>
<td>PDOS 구성 명령 읽기 사용법</td>
<td>12</td>
</tr>
<tr>
<td>PDOS 구성 읽기</td>
<td>13</td>
</tr>
<tr>
<td>명령행에서 PDOS 구성</td>
<td>15</td>
</tr>
<tr>
<td>응답 파일을 사용하여 PDOS 구성</td>
<td>16</td>
</tr>
<tr>
<td>응답 파일 작성</td>
<td>16</td>
</tr>
<tr>
<td>응답 파일 사용</td>
<td>16</td>
</tr>
<tr>
<td>응답 파일의 속성에 명령행 읽기 사용</td>
<td>17</td>
</tr>
<tr>
<td>제5장 PDOS 시작 및 종지</td>
<td>19</td>
</tr>
<tr>
<td>PDOS 시작</td>
<td>19</td>
</tr>
<tr>
<td>명령행</td>
<td>19</td>
</tr>
<tr>
<td>자동 시작</td>
<td>19</td>
</tr>
<tr>
<td>PDOS가 실행 중인지 확인</td>
<td>19</td>
</tr>
<tr>
<td>PDOS 종지</td>
<td>19</td>
</tr>
<tr>
<td>제6장 PDOS 구성 해제</td>
<td>21</td>
</tr>
<tr>
<td>PDOS 구성 해제 계획</td>
<td>21</td>
</tr>
<tr>
<td>PDOS 구성 해제 명령 읽기 사용법</td>
<td>21</td>
</tr>
<tr>
<td>PDOS 구성 해제 읽기</td>
<td>22</td>
</tr>
<tr>
<td>구성 해제에 대한 응답 파일 사용</td>
<td>22</td>
</tr>
<tr>
<td>응답 파일 작성</td>
<td>22</td>
</tr>
<tr>
<td>응답 파일 사용</td>
<td>23</td>
</tr>
<tr>
<td>응답 파일의 속성에 명령행 읽기 사용</td>
<td>23</td>
</tr>
<tr>
<td>제7장 PDOS 설치 제거</td>
<td>25</td>
</tr>
<tr>
<td>AIX에서 PDOS 설치 제거</td>
<td>25</td>
</tr>
<tr>
<td>SMIT를 사용하여 AIX에서 설치 제거</td>
<td>25</td>
</tr>
<tr>
<td>명령행을 사용하여 AIX에서 설치 제거</td>
<td>26</td>
</tr>
<tr>
<td>HP-UX에서 Policy Director for Operating Systems 설치 제거</td>
<td>26</td>
</tr>
<tr>
<td>SWRemovable 사용하여 HP-UX에서 설치 제거</td>
<td>26</td>
</tr>
<tr>
<td>명령행을 사용하여 HP-UX에서 설치 제거</td>
<td>27</td>
</tr>
<tr>
<td>Solaris에서 Policy Director for Operating Systems 설치 제거</td>
<td>27</td>
</tr>
<tr>
<td>ADMINTOOL을 사용하여 Solaris에서 설치 제거</td>
<td>27</td>
</tr>
<tr>
<td>명령행을 사용하여 Solaris에서 설치 제거</td>
<td>28</td>
</tr>
<tr>
<td>부록A. PDOS 구성 읽기</td>
<td>29</td>
</tr>
<tr>
<td>부록B. PDOS 구성 해제 읽기</td>
<td>33</td>
</tr>
</tbody>
</table>
부록C. TACF에서 PDOS로 마이그레이트 .................................................. 35
  마이그레이션 프로세스의 개요 .................................................. 35
  PDOS로의 마이그레이트 계획 .................................................. 36
    계승된 ACL 모델과 계승되지 않은 ACL 모델 .................................. 36
    중앙집중화된 policy와 분산 policy ........................................ 36
  마이그레이션 프로세스 ......................................................... 37
    사전 마이그레이션 테스크 .................................................. 37
    마이그레이션 단계 .......................................................... 37
  se2pdos 변환 유털리티 ......................................................... 40
    사용법 ........................................................................... 40
    옵션 ............................................................................. 40
    예제 ............................................................................. 41
  ACL 허용 및 Namespace ......................................................... 41
  스크립트 맵핑 ..................................................................... 44
색인 .................................................................................. 47
서문

Policy Director for Operating Systems 설치 안내서는 Policy Director for Operating Systems(PDOS) 계획, 설치 및 구성에 대한 정보를 제공합니다.

이 책의 사용자
이 책은 다음을 어느 정도 알고 있는 시스템 관리자를 위한 것입니다.
- UNIX® 운영체제
- 인터넷 프로토콜(HTTP, TCP/IP, FTP, TELNET, SSL)
- 보안 관리
- 다역토리 서비스
- 인증
- 권한
- Tivoli SecureWay Policy Director

시스템 관리자에게 유용한 보조 정보로는 다음이 있습니다.
- Tivoli Management Environment Framework
- Tivoli Distributed Monitoring
- Tivoli Enterprise Console®
- Tivoli SecureWay Security Manager
- Tivoli User Administration

제반 사항 및 관련 서적
유용한 관련 정보를 포함하는 문서는 다음과 같습니다.
- Tivoli SecureWay Policy Director for Operating Systems 관리 안내서 버전 3.7.1
- Tivoli SecureWay Policy Director 관리 안내서 버전 3.7.1
- AIX®용 Tivoli SecureWay Policy Director Base 설치 안내서 버전 3.7.1
- HP-UX용 Tivoli SecureWay Policy Director Base 설치 안내서 버전 3.7.1
- Solaris용 Tivoli SecureWay Policy Director Base 설치 안내서 버전 3.7.1
- Tivoli SecureWay Policy Director 설치하기 전에 버전 3.7.1

이 책의 내용
Policy Director for Operating Systems 설치 안내서에는 다음과 같은 절이 있습니다.
- 1. 페이지의 [PDOS 이해하기]
  PDOS의 개요, 수반하는 기능 및 PDOS 페이지 내용을 제공합니다.
- 5. 페이지의 [PDOS 설치 계획]
  설치에 대한 하드웨어 및 소프트웨어 요구사항을 자세히 설명합니다.
- 7. 페이지의 [PDOS 설치]
원래의 설치 유튜리티와 명령행을 사용하여, AIX, HP-UX 및 Solaris에서 PDOS를 설치하는 방법에 대해 설명합니다.

- **11 페이지의『PDOS 구성』**
  PDOS 구성 계획, 구성 옵션 및 명령행과 응답 파일을 통한 구성에 대해 설명합니다.

- **19 페이지의『PDOS 시작 및 종지』**
  PDOS를 시작 및 중지하는 방법 및 PDOS가 실행 중인지 판별하는 방법에 대해 설명합니다.

- **21 페이지의『PDOS 구성 해제』**
  PDOS 구성 해제 계획, 구성 해제 옵션 및 명령행과 응답 파일을 통한 구성 해제에 대해 설명합니다.

- **25 페이지의『PDOS 설치 제거』**
  원래의 설치 제거 유튜리티와 명령행을 사용하여, AIX, HP-UX 및 Solaris에서 PDOS를 설치 제거하는 방법에 대해 설명합니다.

- **29 페이지의『PDOS 구성 옵션』**
  구성 옵션을 정의하고 최소, 최대 및 기본 값을 제공합니다.

- **33 페이지의『PDOS 구성 해제 옵션』**
  구성 해제 옵션을 정의하고 최소, 최대 및 기본 값을 제공합니다.

- **35 페이지의『TACF에서 PDOS로 마이그레이트』**
  마이그레이션 계획, 마이그레이션 프로세스, 변환 유튜리티, TACF 클래스 및 허용 PDOS policy 및 허용에 맵핑되는 방식 및 TACF 및 PDOS 해당 명령에 대해 설명합니다.

이 책에 사용된 규약

이 책에서는 특수 용어와 조치에 대해 및 가자의 규약을 사용합니다. 규칙은 다음과 같습니다.

- **글씨**
  문자 그대로 사용해야 하는 명령, 키워드, 파일 이름, 권한 역할, URL 또는 기타 정보는 이것처럼 글씨 글씨로 표시합니다. 장, 대화 상자 및 기타 제어 이룹도 이것처럼 글씨 글씨로 표시합니다.

- **기울임체**
  제공해야 하는 변수와 값은 이것처럼 기울임체로 표시합니다. 강조되는 단어와 절도 이것처럼 기울임체로 표시합니다.

- **굵은 기울임체**
  새 용어는 텍스트에 정의된 때 이것처럼 굵은 기울임체로 표시합니다.

모노스페이스 코드, 예제, 출력 및 시스템 메세지는 이것처럼 모노스페이스 글꼴로 표시되다.

플랫폼 특정 정보

다음 표는 출판시 알려져 있는 지원되는 플랫폼 버전을표시한 것입니다. 자세한 최근 정보에 대해서는 ‘설치하기 전에’를 참조하십시오.

### 표 1. PDOS 지원 플랫폼 및 버전

<table>
<thead>
<tr>
<th>플랫폼</th>
<th>지원되는 버전</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX 4.x</td>
<td>AIX, 버전 4.3.1, 4.3.2 및 4.3.3(PTF u470050 버전이 있는)을 실행하는 IBM® RS/6000® 시리즈</td>
</tr>
<tr>
<td>HP-UX</td>
<td>HP-UX, 버전 11.00.47을 실행하는 HP9000/700 및 800 시리즈</td>
</tr>
</tbody>
</table>
표 1. PDOS 지원 플랫폼 및 버전 (계속)

<table>
<thead>
<tr>
<th>플랫폼</th>
<th>지원되는 버전</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris</td>
<td>Solaris, 버전 2.6(105181-23 패치가 있는), 2.7 및 2.8을 실행하는 Sun SPARC 시리즈</td>
</tr>
</tbody>
</table>

피드백 및 서적 제공

Tivoli 제품이나 문서에 대한 사용자의 의견을 환영합니다. 제품 및 문서에 대한 의견이나 제안 사항이 있으면, 다음과으로 문의하시기 바랍니다.

■ 전자 우편을 tivoli@kr.ibm.com으로 보내주십시오.

고객 지원 문의

국내에서 본 제품이나 모든 Tivoli 제품에 대한 지원을 받으시려면 다음과 같은 방법으로 문의하십시오.

■ 웹사이트 방문: http://www.support.tivoli.com
■ Tivoli 고객 지원으로 전화: 02-3781-5243
■ 전자 우편 보내기: tivoli@kr.ibm.com

Tivoli 고객 지원에 문의하실 때는 지원 요원이 더욱 쉽게 도와드릴 수 있도록 사용자 정보를 제공해주십시오.
1

PDOS 이해하기

이 장에서는 다음 주제에 대한 정보를 포함하여, Policy Director for Operating Systems(PDOS)에 대한 간략한 개요를 제공합니다.

- PDOS란?
- PDOS의 특성
- PDOS의 작동 방법
- PDOS 패키지 내용

이 장에는 추가 정보를 얻을 수 있는 소스도 있습니다.

PDOS를 설치하기 전에 이 책과 Policy Director for Operating Systems 관리 안내서 버전 3.7.1을 읽도록 하십시오.

PDOS란?

Policy Director for Operating Systems(PDOS)는 원래의 운영체계에서 제공되는 것 외에 권한 policy 시행 중을 제공합니다. 관리자는 주요 시스템 자원에 대한 액세스를 제한하거나 허용하는 세부적인 액세스 제어사항을 적용하여 추가 권한 policy를 정의합니다. 제어사항은 신원, 그룹 구성원 지격, 조작 유형, 하루 중의 시간이나 그 주의 요일 및 액세스하는 어플리케이션에 따라 결정됩니다. 관리자는 특정 파일 자원, 로그인 및 네트워크 서비스 및 신원 변경사항에 대한 액세스를 제공할 수 있습니다. 이러한 제어사항을 사용하여 관리 절차의 실행을 관리하고 사용자 기준으로 관리 가능성을 제한할 수 있습니다. 권한 policy 시행 외에 PDOS는 정의된 policy와 감사 권한 결정을 검증할 수 있는 메커니즘도 제공합니다.

PDOS의 특성

PDOS는 Policy Director 핵심 기능을 사용하여 다음과 같이 UNIX 보안을 시행합니다.

- 네트워크 서비스에 대한 자세한 액세스 제어를 제공합니다.
- 파일 및 명령어에 대한 자세한 액세스 제어를 제공합니다.
- 로그인 서비스에 대한 자세한 액세스 제어를 제공합니다.
- 루트 사용자의 특권을 제한할 수 있습니다.
- 플랫폼에서 일정합니다.
- 중앙집중화된 권한 policy 관리가 제공됩니다.
PDOS 작동 방법

PDOS를 사용하려면, Policy Director Management Server가 초기에 사용가능해야 합니다. Policy Director는 시스템 관리자가 PDOS를 사용하여 정의하는 policy를 시행하기 때문입니다. 시스템 관리자는 시스템 자원과 서비스에 대한 policy를 설정합니다. PDOS는 커널을 입력할 때 관련 조작을 인터셉트하며 그 조작에 대한 정보와 Policy Director를 사용해서 권한을 결정하는 컨텍스트를 이용해서 작동합니다. 그림을 참조하십시오.

그림 1. PDOS 구성
## PDOS 패키지 내용

PDOS CD, Tivoli SecureWay Policy Director for Operating Systems 버전 3.7 (128-BIT) (원래 설치 패키지)에는 다음과 같은 패키지가 있습니다.

<table>
<thead>
<tr>
<th>플랫폼(디렉토리)</th>
<th>구성요소</th>
<th>패키지</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX (/usr/sys/)</td>
<td>IBM Global Security Toolkit 3.0.1.120</td>
<td>gskru301 및 gskrf301</td>
</tr>
<tr>
<td></td>
<td>IBM Global Security Toolkit 4.0.3.61</td>
<td>gskit.rte</td>
</tr>
<tr>
<td></td>
<td>IBM SecureWay Directory 3.1.1.5 Client</td>
<td>ldap.client</td>
</tr>
<tr>
<td></td>
<td>IBM SecureWay Directory 3.1.1.5 Max Crypto Client</td>
<td>ldap.max_crypto_client</td>
</tr>
<tr>
<td></td>
<td>IBM SecureWay Directory 3.1.1.5 Messages - U.S. English</td>
<td>ldap.msg.en_US</td>
</tr>
<tr>
<td></td>
<td>Tivoli SecureWay Policy Director 3.7.0 Runtime Environment</td>
<td>PD.RTE</td>
</tr>
<tr>
<td></td>
<td>Tivoli SecureWay Policy Director for Operating Systems 3.7.0 Runtime Environment</td>
<td>PDOS.rte</td>
</tr>
<tr>
<td></td>
<td>Tivoli SecureWay Policy Director for Operating Systems 3.7.0 Messages - U.S. English (en_US)</td>
<td>PDOS.msg.en_US</td>
</tr>
<tr>
<td>HP-UX (/hp)</td>
<td>IBM Global Security Toolkit 4.0.3.65</td>
<td>gsk4bas</td>
</tr>
<tr>
<td></td>
<td>IBM SecureWay Directory 3.2 Client</td>
<td>LDAP</td>
</tr>
<tr>
<td></td>
<td>Tivoli SecureWay Policy Director 3.7.0 Runtime Environment</td>
<td>PDRTE</td>
</tr>
<tr>
<td></td>
<td>Tivoli SecureWay Policy Director for Operating Systems 3.7.0 Runtime Environment</td>
<td>PDOSrte</td>
</tr>
<tr>
<td></td>
<td>Tivoli SecureWay Policy Director for Operating Systems 3.7.0 Messages - U.S. English (en_US.iso88591)</td>
<td>PDOSmsgen_US</td>
</tr>
<tr>
<td>Solaris (/solaris)</td>
<td>IBM Global Security Toolkit 4.0.3.65</td>
<td>gsk4bas</td>
</tr>
<tr>
<td></td>
<td>IBM SecureWay Directory 3.2 Client</td>
<td>IBMldapc</td>
</tr>
<tr>
<td></td>
<td>Tivoli SecureWay Policy Director 3.7.0 Runtime Environment</td>
<td>PDRTE</td>
</tr>
<tr>
<td></td>
<td>Tivoli SecureWay Policy Director for Operating Systems 3.7.0 Runtime Environment</td>
<td>PDOSrte</td>
</tr>
<tr>
<td></td>
<td>Tivoli SecureWay Policy Director for Operating Systems 3.7.0 Messages - U.S. English (en_US)</td>
<td>PDOSenUS</td>
</tr>
<tr>
<td>ALL (/docs)</td>
<td>Tivoli SecureWay Policy Director for Operating Systems Installation Guide Version 3.7.0 (PDF)</td>
<td>pdos37_install.pdf</td>
</tr>
<tr>
<td></td>
<td>Tivoli SecureWay Policy Director for Operating Systems Administration Guide Version 3.7.0 (PDF)</td>
<td>pdos37_admin.pdf</td>
</tr>
<tr>
<td></td>
<td>Tivoli SecureWay Policy Director for Operating Systems Release Notes Version 3.7.0 (HTML)</td>
<td>pdos37_relnotes.html</td>
</tr>
</tbody>
</table>
추가 정보

PDOS, PDOS 지원(포럼을 포함하여), 제품 뉴스 및 교육에 대한 일반 정보는 다음 웹 사이트를 참조하시오.

http://www.tivoli.com/products/index/
2

PDOS 설치 계획

이 장에서는 Policy Director for Operating Systems(PDOS)를 설치하는데 필요한 계획 및 제
반 사항에 대해 설명합니다.

PDOS로 마이그레이트

현재 policy 시행을 위해 TACF를 사용 중이며, Tivoli Security SecureWay Manager (TSSM)
환경 또는 TSSM 이외 환경 여부에 관계없이 이 장에 있는 PDOS 설치 계획 정보 외에 35 페이지
이치의『TACF에서 PDOS로 마이그레이트』에 있는 마이그레이션 부록을 읽어야 합니다.

AIX, HP-UX 및 Solaris에서의 PDOS 설치에 대한 하드웨어 요구사항

PDOS 기계에 대한 하드웨어 요구사항은 다음 표에 제공되어 있습니다.

표 2. PDOS 하드웨어 요구사항

<table>
<thead>
<tr>
<th>최소 RAM</th>
<th>64MB</th>
</tr>
</thead>
<tbody>
<tr>
<td>권장되는 RAM</td>
<td>128MB 이상</td>
</tr>
</tbody>
</table>

표 3. PDOS 설치에 필요한 디스크 공간

<table>
<thead>
<tr>
<th>플랫폼</th>
<th>필요한 공간</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>PDOS를 위한 /opt의 10MB</td>
</tr>
<tr>
<td></td>
<td>GSKit, LDAP 및 PD를 위한 /usr의 90MB</td>
</tr>
<tr>
<td>HP-UX</td>
<td>PDOS 런타임 파일을 위한 /var의 20MB</td>
</tr>
<tr>
<td></td>
<td>PDOS, GSKit, LDAP 및 PD를 위한 /opt의 100MB</td>
</tr>
<tr>
<td>Solaris</td>
<td>PDOS 런타임 파일을 위한 /var의 20MB</td>
</tr>
<tr>
<td></td>
<td>PDOS, GSKit, LDAP, PD를 위한 /opt의 100MB</td>
</tr>
<tr>
<td></td>
<td>PDOS 런타임 파일을 위한 /var의 20MB</td>
</tr>
</tbody>
</table>

 주: 모든 플랫폼에 대해 /var/pdos 아래에 필요한 공간은 policy와 감사 설정에 따라 결정되므로
 필요한 공간은 시스템이 changes하면서 증가할 수 있습니다.

AIX에서의 PDOS 설치에 대한 소프트웨어 요구사항

AIX에서의 PDOS 설치에 대한 소프트웨어 요구사항은 시스템에서 사용하는 AIX 버전에
따라 다릅니다. 필요한 대부분의 소프트웨어가 PDOS CD에서 사용가능합니다.

AIX 4.3.3 이상

시스템이 AIX 4.3.3 이상을 사용할 경우 PDOS 설치에 대한 최소 소프트웨어 요구사항은 실행
중인 IBM SecureWay Directory Client 버전에 따라 다릅니다.
IBM SecureWay Directory 3.1.1.5 Client
- Tivoli SecureWay Policy Director 3.7.0 Runtime Environment
- IBM SecureWay Directory 3.1.1.5 Max Crypto Client
- IBM Global Security Toolkit 3.0.1.120 및 4.0.3.61
- 볼치 u470050을 함께 사용가능한 bos.rte.libthreads 4.3.3.11(CD에 없음)

IBM SecureWay Directory 3.2 Client
- Tivoli SecureWay Policy Director 3.7.0 Runtime Environment
- IBM SecureWay Directory 3.2 Max Crypto Client(CD에 없음)
- IBM Global Security Toolkit 4.0.3.61
- 볼치 u470050을 함께 사용가능한 bos.rte.libthreads 4.3.3.11(CD에 없음)

AIX 4.3.1 및 AIX 4.3.2
AIX 4.3.1 및 4.3.2에서 PDOS 설치에 대한 소프트웨어 요구사항은 다음과 같습니다.
- Tivoli SecureWay Policy Director 3.7.0 Runtime Environment
- IBM SecureWay Directory 3.1.1.5 Client
- IBM SecureWay Directory 3.1.1.5 Max Crypto Client
- IBM Global Security Toolkit 3.0.1.120 및 4.0.3.61

주: IBM SecureWay Directory 3.2는 AIX 4.3.1 및 AIX 4.3.2를 지원하지 않습니다.

HP-UX에서의 PDOS 설치에 대한 소프트웨어 요구사항
HP-UX에서 PDOS를 설치하는데 필요한 최소 소프트웨어(대부분 PDOS CD에 있음)는 다음과 같습니다.
- HP-UX 11.00.47(CD에 없음)
- Tivoli SecureWay Policy Director 3.7.0 Runtime Environment
- IBM SecureWay Directory 3.2 Client
- IBM Global Security Toolkit 4.0.3.65

Solaris에서의 PDOS 설치에 대한 소프트웨어 요구사항
Solaris에서 PDOS를 설치하는데 필요한 최소 소프트웨어(대부분 PDOS CD에 있음)는 다음과 같습니다.
- 볼치 105181-23이 있는 Solaris 2.6(CD에 없음)
- Tivoli SecureWay Policy Director 3.7.0 Runtime Environment
- IBM SecureWay Directory 3.2 Client
- IBM Global Security Toolkit 4.0.3.57
3. PDOS 설치

이 장에서는 AIX, HP-UX 및 Solaris에서 Policy Director for Operating Systems(PDOS)를 설치하는 방법에 대해 설명합니다. PDOS를 설치하려고 하는 플랫폼에 대한 원래의 소프트웨어 설치 유달리터에 익숙해야 합니다.

PDOS를 설치하려면 다음을 만족해야 합니다.

- root 권한을 가지고 있어야 합니다.
- 다음 디렉토리에 파일들을 설치하고 그 위치를 변경하지 마십시오.
  
```bash
/opt/pdos
/var/pdos
```

런타임시 PDOS는 /var/pdos 아래의 여러 디렉토리에 권한 policy 정보, 감사 로그 및 오류 로그 를 저장합니다. /var이 전체가 될 수 있는 사용자 환경이 권한 policy를 시행하는 PDOS 능력에 영향을 주지 않게 하려면 /var/pdos를 별도의 파일 시스템으로 작성하는 것이 좋습니다. 또한 /var/pdos/log 및 /var/pdos/audit도 별도의 파일 시스템으로 작성하는 것이 바람직합니다. /var/pdos, /var/pdos/log 및 /var/pdos/audit 디렉토리의 공간 사용을 주의 깊게 모니터해야 합니다.

런타임시, PDOS는 시스템에서의 osseal 사용자 및 그룹 존재 여부에 영향을 받습니다. osseal 그룹 항목이 존재하지 않을 경우, PDOS 설치시 osseal 그룹 항목이 작성됩니다. osseal 사용자 항목이 존재하지 않을 경우, PDOS 설치시 osseal 사용자 항목이 작성됩니다. osseal 사용자는 1 차 osseal 그룹에서 작성됩니다.

AIX에 PDOS 설치

PDOS는 SMIT를 사용하여 AIX에 설치하거나, 명령행에서 설치할 수 있습니다.

SMIT를 사용하여 AIX에 설치

SMIT를 사용하여 AIX에 PDOS를 설치하려면 다음 단계를 사용하십시오.

1. PDOS CD-ROM을 넣으십시오.
2. root로 로그인하십시오.
3. 명령행에서 다음을 입력하십시오.
```bash
smit
```

Enter 키를 누르십시오. 시스템 관리 인터페이스 툴 창이 표시됩니다.
4. 시스템 관리 메뉴에서, 소프트웨어 설치 및 유지보수를 누르십시오.
5. 소프트웨어 설치 및 유지보수 메뉴에서, 소프트웨어 설치 및 개선을 누르십시오.
6. 소프트웨어 설치 및 개선 메뉴에서, 가장 최근의 사용 가능한 소프트웨어에서 설치 및 개선을 누르십시오. 가장 최근의 사용 가능한 소프트웨어에서 설치 및 개선 패널이 표시됩니다.
7. PDOS 패키지가 있는 다렉토리의 이름을 입력하여 소프트웨어에 대한 입력 디바이스/다렉토리를 지정하십시오(/dev/cd0). OK를 누르십시오.
8. 가장 최근의 사용가능한 소프트웨어에서 설치 및 런업 패널이 표시됩니다.
9. 설치할 소프트웨어에서, 목록을 누르십시오. 다중 선택 목록 패널이 표시됩니다. 3.7.0.0 Policy Director for Operating Systems Runtime을 강조표시하십시오. OK를 누르십시오.
10. 가장 최근의 사용가능한 소프트웨어에서 설치 및 런업 창이 다시 표시됩니다. OK를 누르십시오.
11. 설치 선택사항을 확인하도록 요청합니다. OK를 누르십시오.
12. 설치서 가장 최근의 사용가능한 소프트웨어에서 설치 및 런업 창은 설치 명령과 설치에 대한 출력 로그를 보여주는 분할 창을 표시합니다.
13. 설치가 완료되면, 완료를 누르십시오.
14. 가장 최근의 사용가능한 소프트웨어에서 설치 및 런업 패널을 닫으십시오. 시스템 관리 인터페이스 툴 창이 표시됩니다.
15. 시스템 관리 인터페이스 툴 창을 닫으십시오.

명령행을 사용하여 AIX에 설치
명령행에서 AIX에 PDOS를 설치하려면, 다음 단계를 사용하십시오.
1. PDOS CD-ROM을 넣으십시오.
2. root로 로그온하십시오.
3. 명령행에서 다음을 입력하십시오.

```
install -c -a -g -X -d /dev/cd0 PDOS.rte PDOS.msg.language
```

여기서 language는 설치되는 언어 버전에 대한 국가 코드이고, /dev/cd0은 디렉토리입니다. Enter 키를 누르십시오. 예를 들어, 영어 라틴phabet 영어 메시지를 설치하기 위한 명령은 다음과 같습니다.

```
install -c -a -g -X -d /dev/cd0 PDOS.rte PDOS.msg.en_US
```

HP-UX에 PDOS 설치
PDOS는 SWinstall을 사용하여 AIX에 설치하거나, 명령행에서 설치할 수 있습니다. 파일들은 /opt/pdos 및 /var/pdos 디렉토리에 설치해야 합니다. /로부터 대상을 변경하지 마십시오.

SWinstall을 사용하여 HP-UX에 설치
HP-UX에 PDOS를 설치하려면, 다음 단계를 완료하십시오.
1. PDOS CD-ROM을 넣으십시오.
2. root로 로그온하십시오.
3. 실행되지 않을 경우, pfs_mountd를 시작한 후 pfsd를 시작하십시오. pfs_mount 명령을 사용하여 CD를 마운트하십시오. 예를 들어, 명령행에서 다음을 입력하십시오.

```
pfs_mount /dev/dsk/c0t0d0 /cd-rom
```

여기서 /dev/dsk/c0t0d0은 CDROM 디바이스이고 /cd-rom은 마운트 포인트입니다. Enter 키를 누르십시오.
4. 명령행에서 다음을 입력하십시오.

```
swinstall
```
Enter 키를 누르십시오. SD 설치 - 소프트웨어 선택사항 창과 소스 저장 폴업 파일이 표시됩니다. 소스 저장소 유형 목록에서 국지 CD-rom을 선택하십시오. 소스 저장소 경로에 대해, /cd-rom/hp를 입력하십시오. 여기서 cd-rom은 CD에 대한 마운트 포인터입니다. 확인을 누르십시오. SD 설치 - 소프트웨어 선택사항 창이 표시됩니다.

5. SD 설치 - 소프트웨어 선택사항 창에서, PDOS 패키지 PDOSrte PDOSmsglanguage를 선택하여 설치할 소프트웨어를 표시하십시오. language는 설치할 안됩니다. 조차를 누르고 설치 표시를 선택하십시오.

6. 조치 메뉴를 누르고 설치(본체)를 선택하십시오. 설치 본체 팩업 파일이 표시됩니다. 상태가 준비되면, 확인을 누르십시오. 확인 팩업 창이 표시됩니다. 예를 누르십시오.

7. 설치 창 팩업 파일에 설치 프로세스의 상태가 표시됩니다. 상태가 완료되면, 완료를 누르십시오.

8. SD 설치 - 소프트웨어 선택사항 창을 닫으십시오.

명령행을 사용하여 HP-UX에 설치
명령행에서 HP-UX에 PDOS를 설치하려면, 다음 단계를 사용하십시오.

1. PDOS CD-ROM을 넣으십시오.
2. root로 로그온하십시오.
3. 실행되지 않을 경우, pfs_mount.t를 시작한 후 pfsd를 시작하십시오. pfs_mount 명령을 사용하여 CD를 마운트하십시오. 예를 들어, 명령행에서 다음을 입력하십시오.

pfs_mount /dev/dsk/c0t0d0 /cd-rom

여기서 /dev/dsk/c0t0d0는 CDROM 디바이스이고 /cd-rom은 마운트 포인트입니다. Enter 키를 누르십시오.

4. 명령행에서 다음을 입력하십시오.

swinstall -s /cd-rom/hp PDOSrte PDOSmsglanguage

여기서 language는 설치되는 언어 버전에 대한 국가 코드이고, /cd-rom/hp는 디렉토리입니다. Enter 키를 누르십시오. 예를 들어, 영어 선택어 영어 메세지를 설치하기 위한 명령은 다음과 같습니다.

swinstall -s /cd-rom/hp PDOSrte PDOSmsgen_US

Solaris에 PDOS 설치
PDOS는 Admintool을 사용하여 Solaris에 설치하거나, 명령행에서 설치할 수 있습니다.

Admintool을 사용하여 Solaris에 설치
Admintool을 사용하여 Solaris에 PDOS를 설치하려면 다음 단계를 사용하십시오.

1. PDOS CD-ROM을 넣으십시오.
2. root로 로그온하십시오.
3. 명령행에서 다음을 입력하십시오.

admintool

Return 키를 누르십시오. Admintool: 사용자 창이 표시됩니다.


5. 편집을 누르고 추가를 선택하십시오. Admintool: 소스 메체 설정 창이 표시됩니다.
6. 소프트웨어 위치 목록에서 볼륨 관리가 있는 CD를 선택하고 CD 경로 필드에 `/cdrom/cdrom0/solaris`를 입력하십시오. 확인을 누르십시오. Admintool: 소프트웨어 추가 창이 표시됩니다.

7. Admintool: 소프트웨어 추가 창에서, Policy Director for Operating Systems 컨테이너와 설치할 적절한 언어 패키지를 선택하십시오. 추가를 누르십시오.

8. 패키지가 설치되기 전에 확인 메세자가 표시됩니다. 표시되는 순서는 패키지가 설치되는 순서에 따라 다릅니다. 각 패키지마다 "이 패키지를 설치하시겠습니까?" 확인 메세지가 표시됩니다. 이 메시지가 표시되면 Yes를 입력하십시오. Return 키를 누르십시오.


13. 설치가 완료되면 Return 키를 누르십시오. Admintool: 소프트웨어 창이 표시됩니다. 이 창을 닫으십시오.

명령행을 사용하여 Solaris에 설치

명령행에서 Solaris에 PDOS를 설치하려면, 다음 단계를 사용하십시오.

1. PDOS CD-ROM을 넣으십시오.
2. root로 로그인하십시오.
3. 명령행에서 다음을 입력하십시오.

   pkgadd -d /cdrom/cdrom0/solaris -a /cdrom/cdrom0/solaris/pdosdefault PDOSrte PDOSlanguage

여기서 language는 설치되는 언어 버전에 대한 국가 코드이고, /cdrom/cdrom0/solaris는 디렉토리이며, /cdrom/cdrom0/solaris/pdosdefault는 PDOS 패키지와 같은 디렉토리에 있는 스크립트입니다. Return 키를 누르십시오.

을 들어, 영어 런타임과 영어 메세지를 설치하기 위한 명령은 다음과 같습니다.

   pkgadd -d /cdrom/cdrom0/solaris -a /cdrom/cdrom0/solaris/pdosdefault PDOSrte PDOSenUS

4. 각 패키지에 대해 설치 프로세스가 완료되면, "패키지 설치를 성공했습니다." 메시지가 표시됩니다.
PDOS 구성

이 장에서는 AIX, HP-UX 및 Solaris에서 Policy Director for Operating Systems(PDOS)를 구성하는 방법에 대해 설명합니다.

PDOS 구성 명령은 pdoscfg입니다. 몇몇 구성 옵션은 필수이며, 나머지는 선택적입니다. 이 명령은 또한 시스템에서 먼저 PDOS를 구성 해제하지 않고 특정 구성 옵션을 제거할 경우에도 사용됩니다.

다음과 같은 절들이 있으며 그 내용은 다음과 같습니다.
- PDOS 구성 계획
- PDOS 구성 명령 옵션 사용법
- PDOS 구성 옵션
- 명령행에서 PDOS 구성
- 응답 파일을 사용하여 PDOS 구성

PDOS 구성 계획

시스템에서 PDOS를 구성하고 실행하기 전에, 관리 policy를 설정하는 방법과 해당 기계에서 사용되도록 구성된 policy branch 이름을 주의하여 고려해야 합니다. 관리 policy가 올바르게 실행되도록 하려면, Policy Director 사용자 레지스트리 Namespace에 국지 사용자 Namespace를 매핑하는 방법에 대해 주의하여 고려해야 합니다. 자세한 정보는 Policy Director for Operating Systems 관리 안내서를 참조하십시오.

PDOS를 구성하기 전에, 사용자 환경은 특정 상태에 있어야 하며 사용자는 사용하는 시스템에 대한 정보를 알아야 합니다.

1. Policy Director Management Server는 LDAP 사용자 레지스트리를 사용하도록 구성해야 합니다.
2. Policy Director Runtime Environment는 PDOS가 설치된 기계에 설치되고 구성되어야 합니다.
3. base64가 LDAP 서버 기계로부터 LDAP SSL CA 인증서 파일을 암호화하도록 해야 합니다.
4. LDAP 사용자 레지스트리 접미사를 알아야 합니다.
5. 구성 중인 policy branch의 이름을 알아야 합니다.
6. Policy Director security master 암호를 알아야 합니다.

또한 구성 명령에서 사용할 수 있는 옵션들을 검토하여 특정 상황에 맞게 정의할 수 있는 옵션들은 관별해야 합니다.
정책 옵션은 초기 구성에서 지정해야 합니다. 이러한 필수 구성 옵션은 다음과 같습니다.

- branch
- suffix
- ldap_ssl_cacert

Policy Director security master 암호를 제공하지 않으면, 이에 대한 프롬프트가 표시됩니다. PDOS를 구성하고 나면, 이를 시작해야 합니다. PDOS를 시작하는 방법에 대해서는 19 페이지의 PDOS 시작 및 종지를 참조하십시오.

PDOS 구성 명령 옵션 사용법

PDOS 구성 명령 옵션은 구성 명령 pdoscfg와 함께 사용됩니다. 필수가 아닌 옵션은 대괄호로 묶여 있습니다. 대괄호가 없는 옵션은 처음 PDOS를 구성할 때 필요합니다.

-branch와 -suffix 옵션을 제거하여면, 먼저 PDOS 구성은 해제한 후 다시 구성 명령을 실행해야 합니다. -ssl_listening_port 및 -ldap_ssl_cacert 옵션을 제거하려면, 구성 명령을 실행하기 전에 PDOS를 중지해야 합니다.

pdoscfg

[—admin_cred_refresh number_of_minutes]
[—audit_level (all | none | permit | deny | admin | verbose | info)]
[—audit_log_entries number_of_log_entries]
[—audit_logflush number_of_seconds]
[—audit_logs number_of_logs]
[—audit_log_size number_of_bytes]
[—autostart (on | off)]
[—branch policy_branch_name]
[—cred_hold number_of_minutes]
[—delete (comma_delimited_list_of_options)]
[—dns (on | off)]
[—help]
[—kmsg_hnd_threads number_of_threads]
[—ldap_ssl_cacert ldap_certificate_file_name]
[—login_policy (on | off)]
[—operations]
[—pdosd_log_entries number_of_log_entries]
[—pdosd_logs number_of_logs]
[—pdoswdd_log_entries number_of_log_entries]
[—pdoswdd_logs number_of_logs]
[—refresh_interval number_of_minutes]
[—rspfile file_name]
[—sec_master_pwd security_master_password]
[—ssl_listening_port port_to_listen_for_notification]
[—suffix policy_director_suffix]
[—tcb_interval number_of_minutes]
PDOS 구성 옵션

구성 명령에 대한 옵션은 이 절에 설명되어 있습니다. 각 옵션마다 절의 및 기본값이 제공됩니다 (적용가능할 경우). 최소 및 최대 값에 대한 정보는 29 페이지의 [PDOS 구성 옵션]의 부록에 제공되어 있습니다.

- admin_cred_refresh
  관리자의 인증사항 간격을 분 단위로 갱신합니다.
  기본값: 360

- audit_level
  감사 로그들의 목록으로 표시로 구분됩니다. 헤더는 all, none, permit, deny, admin, verbose, info입니다.
  기본값: none

- audit_log_entries
  세 로그로 포함하기 이전의 pdosauditd 로그 항목 수. 기본값 0은 세 로그로 톨어버리지 않음을 의미합니다.
  기본값: 0

- audit_logflush
  감사 로그 버퍼를 삭제하기 위한 초 단위의 간격.
  기본값: 5

- audit_logs
  로그 파일을 제순환하기 전에 사용할 pdosauditd 로그 파일 수. 값 0은 로그 파일을 제순환하지 말아야 함을 나타냅니다. 로그 수를 0 이외의 값으로 설정하는 것은 audit_log_entries가 0이 아닐 경우에만 효과가 있습니다.
  기본값: 0

- audit_log_size
  로그가 새 로그로 톨어버리기 이전의 바이트 단위의 최대 로그 파일 크기.
  기본값: 1000000

- autostart
  시스템 제부트시 PDOS를 자동으로 시작합니다.
  기본값: on

- branch
  이 기계가 등록할 policy branch 이름.
-cred_hold
관리자가 아닌 인증사항이 액세스 없이 캐시되는 분 단위의 최대 시간. 이 값을
admin_credential refresh 값과 user_credential refresh 값 이상이어야 합니다.
기본값: 10080

-delete
구성 파일에서 제거할 옵션들의 목록으로 사용할 수 있습니다. 저장되는 옵션은
admin_credential refresh, audit_log, audit_log_entries, audit_logflush, audit_logs,
audit_log_size, cred_hold, dns, kmsg_hnd_threads, pdosd_log_entries, pdosd_logs,
pdoswdd_log_entries, pdoswdd_logs, refresh_interval, tcb_interval, tcb_max_file_size,
tcb_monitor_threads, uid, user_credential refresh, warning입니다.

-dns PDOS가 IP 주소를 호스 이름 맵핑 정보에 저장할 수 있도록 합니다.
기본값: on

-help 모든 옵션에 대한 도움말을 표시합니다. 하나의 옵션에 대한 도움말을 표시하려면, -help
-option>을 입력하십시오.

-kmsg_hnd_threads
권한 요청을 처리하기 위해 사용되는 스레드 수. 양의 정수여야 합니다.
기본값: 4

-ldap_ssl_cacert
Policy Director 사용자 레지스트리를 포함하는 LDAP 서버의 CA 인증서. 이 인증서는
PDOS 및 LDAP 서버 사이에 발생하는 비타동 인증에 필요합니다.

-login_policy
시스템 로그인 및 암호 제한사항을 사용가능하게 합니다.
기본값: on

-operations
지원되는 옵션을 나열합니다.

-pdosd_log_entries
세 로그로 통합되기 이전에 사용할 pdosd 로그 항목 수. 기본값 0은 세 로그로 통합
오버되지 않음을 의미합니다.
기본값: 0

-pdosd_logs
로그 파일을 재순환하기 전에 사용할 pdosd 파일 수. 값 0은로그 파일을 재순환하지 말
아야 함을 나타냅니다. 로그 수를 0 이외의 값으로 설정하는 것은
pdosd_log_entries가 0이 아닐 경우에만 효과가 있습니다.
기본값: 0

-pdoswdd_log_entries
세 로그로 통합하기 이전에 사용할 pdoswdd 로그 항목 수. 기본값 0은 세 로그로 통합
오버되지 않음을 의미합니다.
기본값: 0

-pdoswdd_logs
로그 파일을 재순환하기 전에 사용할 pdoswdd 로그 파일 수. 값 0은로그 파일을 재순
환하지 말아야 함을 나타냅니다. 로그 수를 0 이외의 값으로 설정하는 것은
pdoswdd_log_entries가 0이 아닐 경우에만 효과가 있습니다.
기본값: 0
-refresh_interval
Policy Director Management Server가 해당되는 간격 동안 수신되지 않은 경우, policy 갱신사항에 대해 풀링되는 분 단위의 간격. 0 값은 Policy 데이터베이스 갱신사항이 풀링에 의해 수신되지 않은 것을 나타냅니다. -ssl_listening_port와 비교해 보십시오.
기본값: 10분

-rspfile
구성에 대한 옵션 값을 포함하는 파일의 이름.

-sec_master_pwd
Policy Director security master 암호.

-ssl_listening_port
Policy 데이터베이스 갱신 공고에 대해 인식할 포트. 0 값은 policy 데이터베이스 갱신 사항이 공고에 의해 수신되지 않을음을 나타냅니다. -refresh_interval과 비교해 보십시오.
기본값: 0

-suffix
구성 동안 PDOS Policy Director 사용자 및 그룹이 작성되어야 하는 LDAP 입니다.

-tcb_interval
모든 TCB 파일이 서명 변경사항에 대해 점검되는 초 단위의 간격. 위크로드는 대략 이 간격에서 일정하게 분산됩니다.
기본값: 1800

-tcb_max_file_size
검사함계 계산에 대해 중요하게 고려되는 파일의 최대 메가바이트 수. 점검되는 바이트들 은 파일 전체적으로 분산됩니다.
기본값: 10

-tcb_monitor_threads
변경사항에 대해 TCB 파일을 모니터하기 위해 사용되는 스레드 수. 이 값을 두 개 이상으로 설정하는 것은 멀티포로세서 기계에서만 유효합니다. 양의 정수여야 합니다.
기본값: 1

-uid
uid/gid를 사용자/그룹 이름 매핑 정보에 캐시할 수 있게 합니다.
기본값: off

-usage
명령 사용에 대한 도움말을 표시합니다.

-user_cred_refresh
사용자의 인증사항 간격을 분 단위로 갱신합니다.
기본값: 720

-version
pdoscfg 유용성의 버전을 표시합니다.

-warning
글로벌 권한 경고 모드를 사용가능하게 합니다.
기본값: off

-?
명령 사용에 대한 도움말을 표시합니다.

명령행에서 PDOS 구성
명령행에서 처음 PDOS를 구성할 경우 다음 예를 사용하십시오.
응답 파일을 사용하여 PDOS 구성

PDOS는 응답 파일을 사용하여 구성할 수 있습니다. 응답 파일에는 보통 명령행에서 지정하는 정보가 들어 있습니다. 응답 파일을 사용하면 명령행에서 정보를 입력할 필요가 없어지므로 구성 프로세스가 자동화될 수 있습니다. 프로세스의 일부만 자동화하려면, 하나의 응선이나 몇몇 응선에 대한 정보를 포함하는 부분별 응답 파일을 작성하면 됩니다. 나머지 응선은 명령행에서 지정할 수 있습니다. 명령행에 지정된 응선은 응답 파일에 제공된 값에 대체됩니다.

응답 파일의 각 행에는 속성과 이에 연관되는 값이 있습니다. 값은 명령행에서 입력으로 사용된 것처럼 구성 프로그램에서 사용됩니다.

응답 패일 작성

응답 패일 형식은 구성 파일 형식과 같습니다. 응답 패일에는 속성=값 쌍으로 된 스탠자키가 있습니다. 스탠자는 대괄호로 묶어 있는 스탠자 이름을 포함하는 행에서 시작하여 또다른 행이 대괄호로 묶어 있는 또다른 스탠자 이름으로 시작될 때, 또는 파일 끝에 도달할 때 종료됩니다. 각 스탠자는 0개 이상의 속성=값 쌍이 있습니다. 스탠자 이름은 응답 파일에서 여러 번 반복될 수 없습니다. 주석은 앞에 # 문자를 사용하여 응답 파일에 추가될 수 있습니다.

응답 파일은 다음과 유사합니다.

```plaintext
[policy]
#Information about the policy.
branch=policy_branch_name
[ldap]
ssl-certificate=/tmp/ldapcacert.b64
[credentials]
admin-cred-refresh=30
[sec-master]
sec-master-pwd=cGo0sutbnielr
suffix=o=tivoli
[ssl]
ssl-listening-port=888
```

이 예에서, 스탠자 이름 행은 [policy], [ldap], [credentials], [pdoscfg], [ssl]입니다. policy 스탠자에는 속성=값 쌍이 branch=policy_branch_name이 있습니다. ldap 스탠자에는 속성=값 쌍인 ssl-certificate=/tmp/ldapcacert.b64가 있습니다. credentials 스탠자에는 속성=값 쌍인 admin-cred-refresh=30이 있습니다. pdoscfg 스탠자에는 속성=값 쌍인 sec-master-pwd=cGo0sutbnielr가 있습니다. ssl 스탠자에는 속성=값 쌍인 ssl-listening-port=888이 있습니다. 예제 응답 파일에는 하나의 주석인 "#Information about the policy."가 있습니다.

응답 파일은 구성 파일을 하나의 파일에 연결하여 작성할 수도 있습니다. 사용하는 구성 파일은 /opt/pdos/etc 디렉토리에 있으며, osseal.conf, pdosd.conf, pdosaududit.conf 및 pdoeswdd.conf를 포함합니다.

응답 파일 사용

응답 파일을 사용하여 PDOS를 구성하려면, 명령행에서 pdoscfg 명령 다음에 -rspfile 응선과 함께 응답 파일 이름을 입력하시시오. 예를 들면 다음과 같습니다.

```plaintext
pdoscfg -rspfile /opt/pdos/etc/config.rsp
```
응답 파일에서 항목을 대체하거나 응답 파일에 추가 항목을 제공하려면, 명령행에서 `pdoscfg` 명령 다음에 `-rspfile` 옵션과 대체 또는 구성에 추가할 각 항목에 대한 옵션을 응답 파일 이름과 함께 입력하십시오. 예를 들면, 다음과 같습니다.

```
pdoscfg -rspfile /opt/pdos/etc/config.rsp \
   -uid off \
   -audit_level all
```

응답 파일의 속성에 명령행 옵션 맵핑

응답 파일에는 속성 값 쌍 세트를 포함하는 스탠지가 있습니다. 스탠지 및 속성은 다음 표에 표시된 것처럼 명령행 옵션에 맵핑됩니다.

표 4. `pdoscfg` 옵션에 해당되는 속성

<table>
<thead>
<tr>
<th>스탠지</th>
<th>속성</th>
<th>옵션</th>
</tr>
</thead>
<tbody>
<tr>
<td>[audit]</td>
<td>level</td>
<td>-audit_level</td>
</tr>
<tr>
<td>[authorization]</td>
<td>warning</td>
<td>-warning</td>
</tr>
<tr>
<td>[cache]</td>
<td>dns</td>
<td>-dns</td>
</tr>
<tr>
<td></td>
<td>uid</td>
<td>-uid</td>
</tr>
<tr>
<td>[credentials]</td>
<td>admin-cred-refresh</td>
<td>-admin_cred_refresh</td>
</tr>
<tr>
<td></td>
<td>cred-hold</td>
<td>-cred_hold</td>
</tr>
<tr>
<td></td>
<td>user-cred-refresh</td>
<td>-user_cred_refresh</td>
</tr>
<tr>
<td>[ldap]</td>
<td>ssl-certificate</td>
<td>-ldap_ssl_cacert</td>
</tr>
<tr>
<td>[pdosaudid]</td>
<td>log-entries</td>
<td>-audit_log_entries</td>
</tr>
<tr>
<td></td>
<td>audit-logflush</td>
<td>-audit_logflush</td>
</tr>
<tr>
<td></td>
<td>logs</td>
<td>-audit_logs</td>
</tr>
<tr>
<td></td>
<td>audit-logsize</td>
<td>-audit_log_size</td>
</tr>
<tr>
<td>[pdoscfg]</td>
<td>sec-master-pwd</td>
<td>-sec_master_pwd</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>-delete</td>
</tr>
<tr>
<td></td>
<td>suffix</td>
<td>-suffix</td>
</tr>
<tr>
<td></td>
<td>autostart</td>
<td>-autostart</td>
</tr>
<tr>
<td></td>
<td>login-policy</td>
<td>-login_policy</td>
</tr>
<tr>
<td>[pdosd]</td>
<td>kmsg-handler-threads</td>
<td>-kmsg_hnd_threads</td>
</tr>
<tr>
<td></td>
<td>log-entries</td>
<td>-pdosd_log_entries</td>
</tr>
<tr>
<td></td>
<td>logs</td>
<td>-pdosd_logs</td>
</tr>
<tr>
<td>[pdoswdd]</td>
<td>log-entries</td>
<td>-pdoswdd_log_entries</td>
</tr>
<tr>
<td></td>
<td>logs</td>
<td>-pdoswdd_logs</td>
</tr>
<tr>
<td>[policy]</td>
<td>branch</td>
<td>-branch</td>
</tr>
<tr>
<td></td>
<td>refresh-interval</td>
<td>-refresh_interval</td>
</tr>
<tr>
<td>[ssl]</td>
<td>ssl-listening-port</td>
<td>-ssl_listening_port</td>
</tr>
<tr>
<td>[tcb]</td>
<td>interval</td>
<td>-tcb_interval</td>
</tr>
<tr>
<td></td>
<td>max-checksum-file-size</td>
<td>-tcb_max_file_size</td>
</tr>
<tr>
<td></td>
<td>monitor-threads</td>
<td>-monitor_threads</td>
</tr>
</tbody>
</table>
PDOS 시작 및 중지

이 장에서는 Policy Director for Operating Systems(PDOS)를 시작하고 중지하는 방법에 대해 설명합니다.

PDOS 시작

명령행

명령행에서 수동으로 PDOS를 시작하거나 자동 시작을 사용할 수 있습니다.

PDOS를 시작하려면, 명령행에 다음 명령을 입력하고 Enter 키를 누르십시오.

```
rc.osseal start
```

자동 시작

초기 구성에서 자동 시작을 사용할 수 없게 하였으면, PDOS는 기본적으로 시스템 재부팅 시 자동 시작됩니다.

PDOS가 시스템이 재시작될 때 자동으로 시작되도록 하려면, 명령행에 다음 명령을 입력하고 Enter 키를 누르십시오. 시스템이 다시 부트되면, PDOS는 자동으로 시작됩니다.

```
pdoscfg -autostart on
```

PDOS가 재부트 전에 시작되도록 하려면, 명령행에 다음 명령을 입력하고 Enter 키를 누르십시오.

```
rc.osseal start
```

PDOS가 실행 중인지 확인

PDOS가 실행 중인지 확인하려면, 명령행에 다음 명령을 입력하고 Enter 키를 누르십시오.

```
pdosctl -s
```

PDOS 중지

PDOS를 중지하려면, 명령행에 다음 명령을 입력하고 Enter 키를 누르십시오.

```
rc.osseal stop
```
6

PDOS 구성 해제

이 장에서는 AIX, HP-UX 및 Solaris에서 Policy Director for Operating Systems(PDOS)의 구성을 해제하는 방법에 대해 설명합니다.

PDOS 구성 해제 명령은 pdosucfg입니다. 이 명령은 PDOS 구성 파일들을 제거하고, 다만 및 커널이 자동 시작되지 않도록 하며, Policy Director에서의 PDOS 동록을 취소합니다.

다음과 같은 절들이 있으며 그 내용은 다음과 같습니다.

- PDOS 구성 해제 계획
- PDOS 구성 해제 명령 옵션 사용법
- PDOS 구성 해제 옵션
- 구성 해제에 대한 응답 파일 사용

PDOS 구성 해제 계획

PDOS를 구성 해제하기 전에, 사용자 환경이 특정 상태에 있어야 하고 사용자는 사용하는 시스템에 대한 정보를 알아야 합니다.

1. Policy Director Management Server와 LDAP 서버는 실행 중 상태여야 합니다.
2. Policy Director Runtime Environment는 PDOS가 설치된 기계에 설치하고 구성해야 합니다.
3. Policy Director security master 암호를 알아야 합니다.
4. PDOS를 중지하십시오. PDOS를 중지하는 방법에 대해서는 19 페이지의『PDOS 시작 및 중지』를 참조하십시오.

PDOS 구성 해제 명령 옵션 사용법

PDOS 구성 해제 옵션은 구성 해제 명령 pdosucfg와 함께 사용됩니다.

```bash
pdosucfg [-help] [-operations] [-remove_once_only (on | off)] [-remove_per_policy (on | off)] [-rspfile file_name] [-sec_master_pwd security_master_password] [-usage] [-version]
```
PDOS 구성 해제 옵션

구성 해제 명령에 대한 옵션은 이 절에 설명되어 있습니다. 각 옵션마다 정의 및 기본값이 제공 됩니다. 음성의 승인가능한 값에 대한 추가 정보는 33 페이지의 'PDOS 구성 해제 옵션'의 부록에 제공되어 있습니다.

-helper 모든 음성에 대한 도움말을 표시합니다. 하나의 음성에 대한 도움말을 표시하려면, -help -option을 입력하십시오.

-operations

지원되는 음션을 나열합니다.

-remove_once_only

PDOS 제품 policy를 등록 취소합니다. 다른 PDOS 기기가 이 Policy Director Management Server에 대해 구성된 경우에는 지정하지 마십시오. 다른 기기가 작동되지 않습니다. 추가 policy가 추가된 경우, 이를 수동으로 제거해야 할 수도 있습니다.

기본값: off

-remove_per_policy

이 기기가 사용되도록 구성된 policy branch에 고유한 PDOS 정보를 등록 취소합니다. 다른 PDOS 기기가 그 policy branch 밑에 구성된 경우에는 지정하지 마십시오. 다른 기기가 작동되지 않습니다. 그 policy branch 밑에 추가 policy가 추가된 경우, 이를 수동으로 제거해야 할 수도 있습니다.

기본값: off

-rspfile

구성 해제에 대한 음선 값을 포함하는 파일.

-sec_master_pwd

Policy Director security master 암호.

-usage

명령 사용에 대한 도움말을 표시합니다.

-version

버전을 표시합니다.

-? 명령 사용에 대한 도움말을 표시합니다.

구성 해제에 대한 응답 파일 사용

PDOS는 응답 파일을 사용하여 구성 해제할 수 있습니다.

응답 파일 작성

구성 해제 응답 파일의 형식은 구성 응답 파일의 형식과 같습니다.

PDOS를 구성 해제하기 위한 응답 파일의 내용은 다음 예와 유사합니다.

[pdoscfg]
sec-master-pwd=cGoOsutbnielr

여기서,

[pdoscfg]
sec-master-pwd=cGoosutbnielr

는 스탠자 이름이고,

을 사용하여 PDOS를 구성 해제하려면, 명령행에서 `pdosucfg` 명령 다음에 `-rspfile` 옵션과 함께 응답 파일 이름을 입력하십시오. 예를 들면 다음과 같습니다.

```
pdosucfg -rspfile /opt/pdos/etc/unconfig.rsp
```

여기서,
```
/opt/pdos/etc/unconfig.rsp
```

는 응답 파일 이름입니다.

응답 파일에서 항목을 대체하거나 구성 해제 명령에 추가 항목을 제공하려면, 명령행에서 `pdosucfg` 명령 다음에 `-rspfile` 옵션과, 대체하거나 구성 해제에 추가할 각 항목에 대한 옵션을 응답 파일 이름과 함께 입력하십시오. 예를 들면 다음과 같습니다.

```
pdosucfg -rspfile /opt/pdos/etc/unconfig.rsp -remove_per_policy off
```

응답 파일의 속성에 명령행 옵션 맵핑

응답 파일에는 속성=값 쌍 세트를 포함하는 스탠자가 있습니다. 스탠자 및 속성은 다음 표에 표시된 것처럼 명령행 옵션에 맵핑됩니다.

```
<table>
<thead>
<tr>
<th>스탠자</th>
<th>속성</th>
<th>옵션</th>
</tr>
</thead>
<tbody>
<tr>
<td>[pdoscfg]</td>
<td>remove-once-only</td>
<td>-remove_once_only</td>
</tr>
<tr>
<td></td>
<td>remove-per-policy</td>
<td>-remove_per_policy</td>
</tr>
<tr>
<td></td>
<td>sec-master-pwd</td>
<td>-sec_master_pwd</td>
</tr>
</tbody>
</table>
```

표 5. `pdosucfg` 옵션에 해당하는 속성
PDOS 설치 제거

이 장에서는 AIX, HP-UX 및 Solaris에서 Policy Director for Operating Systems(PDOS)의 설치를 제거하는 방법에 대해 설명합니다. PDOS를 설치한 플랫폼에 대한 원래 설치 및 설치 제거 유필리티에 의속해야 합니다.

PDOS를 설치 제거하려면 다음을 만족해야 합니다.
- root 권한을 가지고 있어야 합니다.
- PDOS를 설치 제거하기 전에 이를 구성 해제하십시오.
- 커널 환경을 제거하려면 PDOS를 설치 제거한 후에 시스템을 다시 부팅하십시오.

설치시 osseal 그룹 항목이나 osseal 사용자 항목이 작성되었으면, PDOS를 설치 제거할 때 삭제 됩니다.

AIX에서 PDOS 설치 제거

PDOS는 SMIT를 사용하여 AIX에서 설치 제거하거나, 명령행에서 설치 제거할 수 있습니다.

SMT를 사용하여 AIX에서 설치 제거

SMIT를 사용하여 AIX에서 PDOS를 설치 제거하려면 다음 단계를 사용하십시오.

1. root로 로그온하십시오.
2. 명령행에서 다음을 입력하십시오.

```
smitt
```

Enter 키를 누르십시오. 시스템 관리 인터페이스 툴 창이 표시됩니다.
3. 시스템 관리 메뉴에서, 소프트웨어 설치 및 유지 보수를 누르십시오.
4. 소프트웨어 설치 및 유지보수 메뉴에서, 소프트웨어 유지보수 및 유필리티를 누르십시오.
5. 소프트웨어 유지보수 및 유필리티 메뉴에서, 설치된 소프트웨어 제거를 누르십시오. 설치된 소프트웨어 제거 팝업 패널이 표시됩니다.
6. 소프트웨어 이름에 대한 입력 필드를 누르고 PDOS.rte와 PDOS.msg.language를 입력하십시오. language는 설치 제거될 언어 버전에 대한 국가 코드입니다. 예를 들어, 영어 언어 버전의 경우 다음을 입력하십시오.

```
PDOS.msg.en_US
```
7. 선택된 소프트웨어를 설치 제거하기 전에, SMIT는 설치 제거할 수 있는지 판별합니다. 사전 열람만 할 필요가 없고 예로 설정해야 합니다. OK를 누르십시오. 확인 창에서 예를 누르십시오.
8. 사전 열람하는 동안, 분할 화면에서 설치 제거 명령과 설치 제거 사전 열람에 대한 출력 로 그를 보여줍니다.
9. 사전 열람이 완료되면, 완료를 누르십시오.
10. 설치된 소프트웨어 제거 창이 표시됩니다. 사전 열람한 합니까?에서 아니오를 지정하십시오. OK를 누르십시오.
11. 확인 창에서 확인을 누르십시오.
12. 설치 제거 동안, 본관 화면에서 설치 제거 명령과 설치 제거에 대한 출력 로그를 보여줍니다.
13. 설치 제거가 완료되면, 설치된 소프트웨어 제거 창이 표시됩니다. 완료를 누르십시오.
14. 설치된 소프트웨어 제거 창을 닫으십시오.
15. 시스템 관리 인터페이스 툴 창을 닫으십시오.
16. 설치 제거가 완료되면 다시 부팅하십시오.

명령행을 사용하여 AIX에서 설치 제거

명령행을 통해 AIX에서 PDOS를 설치 제거하려면 다음 단계를 사용하십시오.
1. root로 로그온하십시오.
2. 명령행에 다음 명령을 입력하고 Enter 키를 누르십시오.
   ```
   installp -u -g PDOS.rte PDOS.msg.language
   ```
   여기서 language는 설치 제거되는 언어 버전에 대한 국가 코드입니다. 예를 들어, 영어 런타임과 영어 메시지를 설치 제거하기 위한 명령은 다음과 같습니다.
   ```
   installp -u -g PDOS.rte PDOS.msg.en_US
   ```
3. 설치 제거가 완료되면 다시 부팅하십시오.

HP-UX에서 Policy Director for Operating Systems 설치 제거

PDOS는 SWRemove를 사용하여 HP-UX에서 설치 제거하거나, 명령행에서 설치 제거할 수 있습니다.

SWRemove를 사용하여 HP-UX에서 설치 제거

SWRemove를 사용하여 HP-UX에서 PDOS를 설치 제거하려면 다음 단계를 사용하십시오.
1. root로 로그온하십시오.
2. 명령행에서 다음을 입력하십시오.
   ```
   swremove
   ```
   Enter 키를 누르십시오. SD 제거-소프트웨어 선택사항 창이 표시됩니다.
3. 설치 제거할 모든 PDOS 패키지를 선택하십시오.
4. 조치 메뉴에서, 제거 표시를 선택하십시오.
5. 조치 메뉴에서, 제거(백색)를 선택하십시오. 제거(백색) 팝업 패널이 표시됩니다. 상태가 준비되면, 확인을 누르십시오.
6. 확인 팝업 패널에서, 예를 누르십시오. 제거 창이 표시됩니다.
7. 상태가 완료되면, 완료를 누르십시오.
8. SD 제거-소프트웨어 선택사항 창을 닫으십시오.
9. 설치 제거가 완료되면 다시 부팅하십시오.
명령행을 사용하여 HP-UX에서 설치 제거
명령행을 통해 HP-UX에서 PDOS를 설치 제거하려면 다음 단계를 사용하십시오.
1. root로 로그온하십시오.
2. 명령행에 다음 명령을 입력하고 Enter 키를 누르십시오.
   swremove PDOSrte PDOSmsgen_US
   여기서 language는 설치 제거되는 언어 버전에 대한 국가 코드입니다. 예를 들어, 영어 런타임과 영어 메세지를 설치 제거하기 위한 명령은 다음과 같습니다.
   swremove PDOSrte PDOSmsgen_US
3. 설치 제거가 완료되면 다시 부팅하십시오.

Solaris에서 Policy Director for Operating Systems 설치 제거
PDOS는 Admintool을 사용하여 Solaris에서 설치 제거하나, 명령행에서 설치 제거할 수 있습니다.

ADMINTOOL을 사용하여 Solaris에서 설치 제거
Admintool을 사용하여 Solaris에서 PDOS를 설치 제거하려면 다음 단계를 사용하십시오.
1. root로 로그온하십시오.
2. 명령행에서 다음을 입력하십시오.
   admintool
   Return 키를 누르십시오. Admintool: 사용자 창이 표시됩니다.
   Policy Director for Operating Systems Messages - U.S. English (en_US)
5. 랜다임 메뉴에서 삭제를 선택하십시오.
7. 패키지가 제거되기 전에 확인 메세지들이 표시됩니다. 표시되는 순서는 패키지가 제거되는 순서에 따라 다릅니다. 각 패키지마다 "이 패키지를 제거하시겠습니까?" 확인 메세지가 표시됩니다. 이 메시지가 표시되면 Yes를 입력하십시오. Return 키를 누르십시오.
8. 랜다임 패키지에 대해 "이 패키지에는 이 패키지를 제거하는 프로세스 동안 super-user 권한으로 실행될 스크립트가 있습니다. 이 패키지 제거를 계속하시겠습니까?" 확인 메세지가 표시됩니다. Yes를 입력하십시오. Return 키를 누르십시오.
9. 완료되면 Return 키를 누르십시오.
10. Admintool: 소프트웨어 창을 닫으십시오.
11. 설치 제거가 완료되면 다시 부팅하십시오.
명령행을 사용하여 Solaris에서 설치 제거
명령행을 통해 Solaris에서 PDOS를 설치 제거하려면 다음 단계를 사용하십시오.

1. root로 로그온하십시오.
2. 명령행에 다음 명령을 입력하고 Return 키를 누르십시오.
   pkg rm PDOSrte PDOSlanguage
   여기서 language는 설치 제거되는 언어 버전에 대한 국가 코드입니다. 예를 들어, 영어 런타임과 영어 메시지를 설치 제거하기 위한 명령은 다음과 같습니다.
   pkg rm PDOSrte PDOSenUS
6. 설치 제거가 완료되면 다시 부팅하십시오.
Policy Director for Operating Systems (PDOS) 구성 명령에 대해 사용할 수 있는 옵션은 다음과 같습니다.

### 표 6. PDOS 구성 옵션

<table>
<thead>
<tr>
<th>옵션</th>
<th>설명</th>
<th>값</th>
</tr>
</thead>
<tbody>
<tr>
<td>-admin_credential</td>
<td>관리자의 인증사항 간격을 부 단위로 갱신합니다.</td>
<td>최소: 1, 최대: maxint, 기본값: 360(6시간)</td>
</tr>
<tr>
<td>-audit_level</td>
<td>클로벌 감사 레벨에 대한 값 목록으로, 설포로 구분됩니다.</td>
<td>all, none, permit, deny, admin, verbose, info</td>
</tr>
<tr>
<td>-audit_log_entries</td>
<td>세 로그로 시스템인정이 이전의 pdosaudit 표시 로그 항목 수. 기본값 0은 세로그로 시스템인정되지 않은 값을 의미합니다. 로그 수를 0 이상의 값으로 설정하는 것은 audit_log_entries가 0이 아닐 경우에만 효과가 있습니다.</td>
<td>최소: 0, 최대: maxint, 기본값: 0</td>
</tr>
<tr>
<td>-audit_logflush</td>
<td>감사 로그 버퍼를 삭제하기 위한 초 단위의 간격.</td>
<td>최소: 5, 최대: 9999, 기본값: 5</td>
</tr>
<tr>
<td>-audit_logs</td>
<td>로그 파일을 재생산하기 이전의 pdosaudit 파일 수. 값 0은 로그 파일을 재생산하지 말아야 한다. 로그 수를 0 이외의 값으로 설정하는 것은 audit_log_entries가 0이 아닐 경우에만 효과가 있습니다.</td>
<td>최소: 0, 최대: maxint, 기본값: 0</td>
</tr>
<tr>
<td>-audit_log_size</td>
<td>로그가 세 로그로 시스템인정이 이전의 바이트 단위의 최대 로그 파일 크기.</td>
<td>최소: 10000000, 최대: 1000000000, 기본값: 100000000</td>
</tr>
<tr>
<td>-autostart</td>
<td>시스템 재부팅시 PDOS를 자동으로 시작합니다.</td>
<td>on</td>
</tr>
<tr>
<td>-branch</td>
<td>이 기계가 등록한 policy branch 이름.</td>
<td></td>
</tr>
<tr>
<td>옵션</td>
<td>설명</td>
<td>값</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>-cred_hold</td>
<td>관리자가 아닌 인증사항이 액세스 없이 캐시되는 분 단위의 최대 시간. 이 값은 admin_cred_refresh 값과 user_cred_refresh 값 이상이어야 합니다.</td>
<td>최소: 1, 최대: maxint, 기본값: 10080(1주일)</td>
</tr>
<tr>
<td>-delete</td>
<td>구성 파일에서 제거할 옵션들의 목록으로 샘플로 구분됩니다.</td>
<td>admin_cred_refresh, audit_level, audit_log_entries, audit_logflush, audit_logs, audit_log_size, cred_hold, dns, kmsg_hnd_threads, pdosd_log_entries, pdosd_logs, pdoswdd_log_entries, pdoswdd_logs, refresh_interval, tcb_interval, tcb_max_file_size, tcb_monitor_threads, uid, user_cred_refresh, warning</td>
</tr>
<tr>
<td>-dns</td>
<td>PDOS가 IP 주소를 호스 이름 맵핑 정보에 저장할 수 있도록 합니다.</td>
<td>on</td>
</tr>
<tr>
<td>-help</td>
<td>모든 옵션에 대한 도움말을 표시합니다. 하나의 옵션에 대한 도움말 을 표시하려면, **-help -&lt;option&gt;**을 입력하십시오.</td>
<td>기본값: on</td>
</tr>
<tr>
<td>-kmsg_hnd_threads</td>
<td>컨버로부터 온한 요청을 처리하기 위해 사용되는 블록 수. 양의 정수여야 합니다.</td>
<td>최소: 1, 최대: maxint, 기본값: 4</td>
</tr>
<tr>
<td>-ldap_ssl_cacert</td>
<td>Policy Director 사용자 롤리스트를 포함하는 LDAP Server의 CA 인증서. 이 인증서는 PDOS과 LDAP Server 사이에 발생하는 매핑에 사용합니다.</td>
<td>파일을 제공해야 합니다.</td>
</tr>
<tr>
<td>-login_policy</td>
<td>시스템 로그인 및 암호 제한사항을 사용가능하게 합니다.</td>
<td>on</td>
</tr>
<tr>
<td>-operations</td>
<td>지원되는 옵션을 나열합니다.</td>
<td>기본값: on</td>
</tr>
<tr>
<td>-pdosd_log_entries</td>
<td>세 로그로 볼바로 이전에 사용할 pdosd 로그 항목 수. 기본값 0 온 세 로그로 볼바로 되지 않음을 의미합니다.</td>
<td>최소: 0, 최대: maxint, 기본값: 0</td>
</tr>
</tbody>
</table>
표 6. PDOS 구성 옵션 (계속)

<table>
<thead>
<tr>
<th>옵션</th>
<th>설명</th>
<th>값</th>
</tr>
</thead>
<tbody>
<tr>
<td>-pdosd_logs</td>
<td>로그 파일을 제출하기 전에 사용할 pdosd 파일 수. 값 0은 로그 파일을 제출하지 말아야 함을 나타냅니다. 로그 수를 0이외의 값으로 설정하는 것은 pdosd_log_entries가 0이 아닐 경우에만 효과가 있습니다.</td>
<td>최소: 0&lt;br&gt;최대: maxint&lt;br&gt;기본값: 0</td>
</tr>
<tr>
<td>-pdoswdd_log_entries</td>
<td>새 로그로 불러오기 이전에 사용할 pdoswdd 로그 항목 수. 기본값 0은 새 로그로 불러오지 않음을 의미합니다.</td>
<td>최소: 0&lt;br&gt;최대: maxint&lt;br&gt;기본값: 0</td>
</tr>
<tr>
<td>-pdoswdd_logs</td>
<td>로그 파일을 제출하기 전에 사용할 pdoswdd 로그 파일 수. 값 0은 로그 파일을 제출하지 말아야 함을 나타냅니다. 로그 수를 0이외의 값으로 설정하는 것은 pdoswdd_log_entries가 0이 아닐 경우에만 효과가 있습니다.</td>
<td>최소: 0&lt;br&gt;최대: maxint&lt;br&gt;기본값: 0</td>
</tr>
<tr>
<td>-refresh_interval</td>
<td>Policy Director Management Server가 해당되는 간격 동안 수신 되지 않은 경우, policy 경신사항에 대해 폴링되는 본 단위의 간격. 0 값은 policy 데이터베이스 경신 사항이 폴링에 의해 수신되지 않음을 나타냅니다. -ssl_listening_port와 비교해 보십시오.</td>
<td>최소: 0&lt;br&gt;최대: maxint/60&lt;br&gt;기본값: 10</td>
</tr>
<tr>
<td>-rspfile</td>
<td>구성에 대한 옵션 값을 포함하는 파일의 이름. 파일을 제공해야 합니다.</td>
<td></td>
</tr>
<tr>
<td>-sec_master_pwd</td>
<td>Policy Director security master 암호.</td>
<td></td>
</tr>
<tr>
<td>-ssl_listening_port</td>
<td>policy 데이터베이스 경신 공고에 대해 안식할 포트. 0 값은 policy 데이터베이스 경신사항이 공고에 의해 수신되지 않음을 나타냅니다. -refresh_interval과 비교해 보십시오.</td>
<td>최소: 0&lt;br&gt;최대: 65535&lt;br&gt;기본값: 0</td>
</tr>
<tr>
<td>-suffix</td>
<td>구성 동안 PDOS Policy Director 사용자 및 그룹이 작성되어야 하는 LDAP 캐피처.</td>
<td></td>
</tr>
<tr>
<td>-tcb_interval</td>
<td>모든 TCB 파일이 서명 변경사항에 대해 점검되는 초 단위의 간격. 웨크로드는 태스크가 간격에서 일정하게 분산됩니다.</td>
<td>최소: 1&lt;br&gt;최대: maxint&lt;br&gt;기본값: 1800</td>
</tr>
</tbody>
</table>
표 6. PDOS 구성 옵션 (계속)

<table>
<thead>
<tr>
<th>옵션</th>
<th>설명</th>
<th>값</th>
</tr>
</thead>
<tbody>
<tr>
<td>-tcb_max_file_size</td>
<td>검사함께 개선에 대해 중요하다고 알려지는 파일의 최대 메가바이트 수. 검사되는 파일들은 파일 전체적으로 분산됩니다.</td>
<td>최소: 1, 최대: ((2^{44} - 1)), 기본값: 10</td>
</tr>
<tr>
<td>-tcb_monitor_threads</td>
<td>변경사항에 대해 TCB 파일을 모니터링하기 위해 사용되는 스펙드 수. 이 값은 두 개 이상으로 설정하는 것은 멀티프로세서 기계에서만 유효합니다. 양의 정수여야 합니다.</td>
<td>최소: 1, 최대: maxint, 기본값: 1</td>
</tr>
<tr>
<td>-uid</td>
<td>uid/gid를 사용자/그룹 이름 맵핑 정보에 사용할 수 있게 합니다.</td>
<td>on</td>
</tr>
<tr>
<td>-usage</td>
<td>명령 사용에 대한 도움말을 표시합니다.</td>
<td></td>
</tr>
<tr>
<td>-user_cred_refresh</td>
<td>사용자의 인증사항 간격을 분 단위로 정산합니다.</td>
<td>최소: 1, 최대: maxint, 기본값: 720</td>
</tr>
<tr>
<td>-version</td>
<td>pdoscfg 유틸리티의 버전을 표시합니다.</td>
<td></td>
</tr>
<tr>
<td>-warning</td>
<td>글로벌 권한 경고 모드를 사용가능하게 합니다.</td>
<td>on</td>
</tr>
<tr>
<td>-?</td>
<td>명령 사용에 대한 도움말을 표시합니다.</td>
<td></td>
</tr>
</tbody>
</table>
표 7. PDOS 구성 해제 옵션

<table>
<thead>
<tr>
<th>옵션</th>
<th>설명</th>
<th>값</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help</td>
<td>모든 옵션에 대한 도움말을 표시합니다. 하나의 옵션에 대한 도움말을 표시하려면, -help -&lt;option&gt;을 입력하십시오.</td>
<td></td>
</tr>
<tr>
<td>-operations</td>
<td>지원되는 옵션을 나열합니다.</td>
<td></td>
</tr>
<tr>
<td>-remove_only_once</td>
<td>PDOS 제품 policy를 등록 취소합니다. 다른 PDOS 기체가 이 Policy Director Management Server에 대해 구성된 경우에는 지정하지 마십시오. 다른 기체가 작동되지 않습니다. 추가 policy가 추가된 경우, 이를 수동으로 제거해야 할 수도 있습니다.</td>
<td>on</td>
</tr>
<tr>
<td></td>
<td>기본값: off</td>
<td></td>
</tr>
<tr>
<td>-remove_per_policy</td>
<td>이 기체가 사용되도록 구성된 PDOS 정보에 고유한 policy branch을 등록 취소합니다. 다른 PDOS 기체가 그 policy branch 밑에 구성된 경우에는 지정하지 마십시오. 다른 기체가 작동되지 않습니다. 그 policy branch 밑에 추가 policy가 추가된 경우, 이를 수동으로 제거해야 할 수도 있습니다.</td>
<td>on</td>
</tr>
<tr>
<td></td>
<td>기본값: off</td>
<td></td>
</tr>
<tr>
<td>-rspfile file_name</td>
<td>구성 해제 프로세스에서 사용되는 값이 들어 있습니다.</td>
<td>파일을 제공해야 합니다.</td>
</tr>
<tr>
<td>-sec_master_pwd password</td>
<td>Policy Director에서 등록 취소하기 위해 사용되는 security master 암호.</td>
<td></td>
</tr>
<tr>
<td>-usage</td>
<td>명령 사용에 대한 도움말을 표시합니다.</td>
<td></td>
</tr>
<tr>
<td>-version</td>
<td>pdosuconf 유틸리티의 버전을 표시합니다.</td>
<td></td>
</tr>
<tr>
<td>-?</td>
<td>명령 사용에 대한 도움말을 표시합니다.</td>
<td></td>
</tr>
</tbody>
</table>
TACF에서 PDOS로 마이그레이트

이 장에서는 기존의 자원 보호를 기존 TACF 환경에서 Policy Director for Operating Systems(PDOS) 환경으로 전송할 수 있는 방법에 대해 설명합니다. 기존의 TACF 환경이 없으면 이 정보는 사용자에게 적용되지 않습니다. 이 장의 내용은 다음과 같습니다.

- 마이그레이션 프로세스의 개요
- PDOS로의 마이그레이션 계획
- 마이그레이션 프로세스
- 변환 유튜리티
- ACL 허용 및 Namespace
- 스크립트 맵핑

마이그레이션 프로세스의 개요

마이그레이션 프로세스는 PDOS가 설치되어 구성된 후, PDOS가 시작되기 전에 발생합니다. 마이그레이션 프로세스의 초점은 TACF 데이터베이스로부터 사용자를 Policy Director 사용자로 정의한 후 PDOS Namespace 향목, 액세스 제어 목록(ACL) 및 POP(Protected Object Policy) 측면에서, TACF 보호를 재정의하는 것입니다. 마이그레이션 프로세스는 TACF 명령을 PDOS 명령으로 변환하여 TACF 스크립트를 Policy Directory pdadmin 스크립트로 변환하는 작업이 포함됩니다. 그림2를 참조하십시오.

그림 2. PDOS 데이터의 초기 채우기
PDOS로의 마이그레이트 계획

PDOS로의 마이그레이트를 계획할 경우의 고려사항은 다음과 같습니다.

- TACF 제한되지 않은 ACL 모델과 Policy Director 계승 ACL 모델 사이의 차이점
- 분산 policy와 중앙집중화된 policy의 차이점

제계된 ACL 모델과 계승되지 않은 ACL 모델

TACF는 계승되지 않은 ACL 모델을 사용하고, PDOS는 계승된 ACL 모델을 사용합니다. PDOS로 마이그레이트하기 전에, 계승된 모델로 마이그레이트할 경우의 효과를 고려하고 계획해야 합니다. 계승된 모델 구현 투명에서 현재 TACF 보호 설정을 검토하십시오. 검토 후에는 PDOS로 보호를 변경하기 전에 갱신해야 합니다.

TACF는 계승되지 않은 ACL 모델을 사용하므로, 다렉토리에 있는 ACL은 포함된 파일이나 서브드렉토리에 적용되지 않습니다. TACF 관리자는 계승 파일을 마이그레이트하는 보호 설정의 구현에 익숙할 것입니다. 예를 들어 관리자는 /proj와 같은 최상위 디렉토리에 할당되는 기본 액세스를 놓고 사용자와 그룹에 대해 파일들에 대한 특정 액세스를 부여할 수 있습니다.

```
editres FILE ("/proj") defaccess(READ CHDIR)
editres FILE ("/proj/*") defaccess(READ CHDIR)
editres FILE ("/proj/proja/designs/projahld") comment ("Projecta Design") defaccess (READ)
owner ("projalead")
authorize FILE ("/proj/proja/designs/projahld") access (READ WRITE CREATE DELETE...) gid ("engineers")
```

PDOS는 Policy Director ACL 계승 모델을 사용합니다. 예제에서, "/proj/*"의 ACL은 불필요하게 됩니다. "proj"에서 READ 및 CHDIR 권한을 포함하는 ACL로도 충분하기 때문입니다. 다음 Policy Director padmin 명령으로 /projects 및 /proj/proja/designs/projahld에 대한 유사한 PDOS policy를 구성할 수 있습니다.

```
object create "/OSSEAL/mypolicy/File/proj" "" 0 ispolicyattachable yes
acl create proj_ac1
acl attach "/OSSEAL/mypolicy/File/proj"_ proj_ac1
acl modify proj_ac1 set any-other "T(OSSEALrlID"
object create "/OSSEAL/mypolicy/File/proj/proja/designs/projahld" "" 0 ispolicyattachable yes
object modify "/OSSEAL/mypolicy/File/proj/proja/designs/projahld"
set description "Projecta Design"
object create projA_projahld_ac1
acl attach "/OSSEAL/mypolicy/File/projA/projahd/designs/projahld" projA_projahld_ac1
acl create projAprojahd_ac1
acl attach "/OSSEAL/mypolicy/File/projA/designs/projahld" projA_projahld_ac1
acl modify projAprojahd_ac1 set any-other "projalead" "T(OSSEAL)cabvm"
object create projA_projahld_ac1
acl create projAprojahd_ac1
acl create projA_projahld_ac1 set any-other "T(OSSEAL)rlr1"
acl modify projAprojahd_ac1 set group "engineers" "T(OSSEAL)dr1wN...
```

TACF 표시에서, "/proj/*"에 대한 자원이 저장되지 않으면, 다렉토리 /proj/proja/designs/는 ACL과 연관되지 않습니다. PDOS 표시에서, /proj/proja/designs/와 해당되는 모든 서브디렉토리는 Policy Director 사용자 "any-other" 및 "unauthenticated"에 대해 T(OSSEAL)rlID의 효율적인 ACL을 갖습니다.

중앙집중화된 policy와 분산 policy

다중 TACF 시스템 환경은 분산 policy 모델의 인스턴스이고, PDOS는 중앙집중화된 policy 모델의 인스턴스입니다.

다중 TACF 시스템 환경에서, 각 TACF 시스템은 자체적으로 포함됩니다. 각 시스템은 고유한 사용자 및 그룹 레지스트리와 해당되는 고유 보호 policy를 유지 보수합니다. TSSM과 같은 중
양집중화된 관리 도구를 사용하지 않으면, 환경 사이의 일관성을 보장할 수 없습니다. 예를 들어, 하나의 시스템은 주어진 사용자 이름에 대해 파일의 READ 및 WRITE 허용을 부여하고, 다른 시스템은 같은 사용자 이름에 대해 같은 파일의 READ, WRITE, DELETE 허용을 부여할 수 있습니다. 사용자 이름이 실제로 같은 사람을 인급하지 않을 경우 추가로 복잡성과 비일관성이 존재할 수 있습니다.

PDOS는 양집중화된 policy 모델을 제공합니다. 사용자, 그룹 및 policy 정보(Policy Director 사용자, 그룹, 오브젝트, ACL, POP)는 여러 시스템에 대한 양집중화된 데이터베이스에 보유됩니다. ACL은 정의된 Protected Object에 첨부됩니다. /etc/passwd 파일을 보호하는 ACL은 한 번 정의되면 정의된 후에는 모든 등록PDOS 클라이언트에서 해석됩니다. ACL은 Protected Object를 포함하는 policy branch에 등록하는 PDOS 클라이언트에만 적용됩니다.

중앙집중화된 환경에 마이그레이션하기 전에, 충돌 및 비일관성에 대해 도메인에서 시스템을 검토하십시오. 이러한 문제점이 해결되었으며, 단일 시스템을 "모델" 대상으로 정하고 이 시스템을 사용하여 Policy Director 데이터베이스를 채우십시오. 그러나 중앙집중화된 관리 설계가 사용될 경우, 모든 TACF 시스템이 유사한 호보 성격을 갖는 동일한 자원들을 정의함으로 높은 충돌 요인이 발생합니다. 예를 들어 모든 TACF 시스템이 TACF 데이터베이스에서 /etc/passwd에 대해 FILE 자원을 포함할 수 있습니다. 중앙집중화된 관리 도구가 사용되므로, 도메인에서 이 자원들에 대한 비일관성이 최소화됩니다. 이 경우 도메인에 있는 기계로 "모델"로 선택할 수 있습니다.

마이그레이션 프로세스

PDOS로의 마이그레이션에는 몇 가지의 시점 마이그레이션 테스크와 실제 마이그레이션이 관련 됩니다.

사전 마이그레이션 테스크

TACF에서 PDOS로 워크스테이션을 마이그레이션하기 전에, 다음 테스크를 완료하십시오.

- Policy Director Server를 설치하고 구성하십시오. 서버를 PDOS 클라이언트가 사용할 수 있도록 만드십시오.
- PDOS가 Tivoli SecureWay Security Manager(TSSM)으로 관리될 경우 다음과 같이 하십시오.
  - TSSM 3.7.1을 설치하고 Policy Director policy branch 이름 구성할 편해하십시오.
  - PDOS 클라이언트의 제반 사항이 설치되었는지 확인하십시오. PDOS를 시작하십시오.

주: Policy branch 이름 구성 정보는 PDOS 구성 단계에서 사용됩니다.

- 계층 ACL 모델리의 마이그레이션에 대한 성과를 분석하십시오. 중앙집중화된 policy 시스템으로의 마이그레이션에 대한 TACF "모델" 시스템을 편해하십시오.

마이그레이션 단계

TACF에서 PDOS로 마이그레이션하려면 다음 단계를 사용하십시오.

1. TACF "모델" 기계를 선택하십시오.
2. 부팅시 TACF 자동 시작이 작동되지 않도록 하십시오.

AIX /etc/inittab에서 TACF 항목을 제거하십시오.
```
seos:2:once:/usr/seos/rc/SeOS.base
seolgrd:2:respawn:/usr/seos/bin/seolgrd=de/console 2>&1
seolgrcd:2:respawn:/usr/seos/bin/seolgrd >dev/console 2>&1
```

HP-UX
```
etc/rc*.d 디렉토리에서 SeOS 시작 파일을 제거하십시오.
```
Solaris

t/sdrc2.d 다택토리에서 SeOS 시작 파일을 제거하십시오.

3. TACF 데이터베이스 소스 스크립트를 작성하십시오. TACF sedb2scr 유필리터를 실행하여 TACF 데이터베이스를 스크립트 형식으로 저장하십시오.
   
   # /usr/seos/bin/sedb2scr -r > /outdirdir/sedb2scr.out

TACF가 종료되었으면, 국지 모드에서 sedb2scr을 실행할 수 있습니다.
   
   # cd /usr/seos/seosdb
   # /usr/seos/bin/sedb2scr -r > /outdirdir/sedb2scr.out

여기에 /outdirdir는 출력 파일을 포함할 수 있도록 충분히 큰 디렉토리입니다. 출력 파일의 크기는 TACF 데이터베이스 입력 수에 따라 다릅니다. Solaris와 같은 일부 시스템에서는 시스템이 다시 부팅될 때 자동으로 제거될 수 있으므로 /tmp 디렉토리를 사용하지 마십시오.

4. TACF *.ini 파일을 저장하십시오. TACF 로그인 및 암호 policy 정보는 /
   /var/TACF_install-dir/seos.ini 파일에 있습니다.
   
   # cp /var/TACF_install-dir/seos.ini /outdirdir

5. TACF 다이얼을 종료하고 시스템을 다시 부팅하십시오.
   
   # secons -s

AIX

   # shutdown -Fr

HP-UX

   # shutdown -r -y 10

Solaris

   # /usr/sbin/shutdown -y -g 10 -i6

6. PDOS를 설치하고 구성하십시오. PDOS를 시작하지 마십시오.

   a. TSSM을 사용하여 설치할 경우, Tivoli SecureWay Security Manager Supplement for Policy Director 및 Tivoli SecureWay Security Manager 설치하기 전에 버전 3.7.1에서 PDOS 분산 및 설치에 대해 참조하십시오. 또한 이 책에서 7 페이지의 PDOS 설치를 참조할 수 있습니다.

   b. PDOS 클라이언트가 TSSM 관리 환경의 일부로 구성될 경우, PDOS policy branch 이름에 대해 TSSM 설치 동안 정의된 해당되는 policy branch 이름을 사용하십시오. 예를 들면, 다음과 같습니다.
   
      pdoscfg -branch policy-branch

      그렇지 않음 경우, 5 페이지의 PDOS 설치 계획에서 policy branch 이름과 LDAP 접미어 정보를 패널하는 방법에 대해 살펴보십시오.

7. TACF 사용자 레지스트리로 Policy Directory 사용자 레지스트리를 채우십시오.

   ■ PDOS se2pdos 유필리터를 사용하여 TACF 사용자 및 그룹을 Policy Director 사용자 및 그룹으로 변환하십시오. 5 페이지의 PDOS 설치 계획에서 policy branch 이름과 LDAP 접미어 정보를 패널하는 방법에 대해 살펴보십시오.

   ■ Policy Director 사용자 및 그룹을 작성할 Policy Director 스크립트를 작성하십시오.

      # cd /outdirdir
      # se2pdos -i -u"suffix" -p policy-branch -n <sedb2scr.out > pdosusers.pd

      텍스트 편집기를 사용하여 출력 결과를 점검하십시오.

      # vi pdosusers.pd
Policy Director 보안 policy를 채워십시오.
주: 이 단계는 TSSM 이외 환경에 해당합니다. TSSM 관리 환경을 사용 중인 TSSM 프로파일 분배를 사용하여 policy를 채워십시오.

```
# cd /outdirectory
# se2pdos -i -p policy-branch -nr <sedb2scr.out pdospolicy.pd
```

a. 텍스트 편집기를 사용하여 출력 결과를 검증하십시오.
```
# vi pdospolicy.pd
```
b. pdadmin 유틸리티를 사용하여 Policy Director에 PDOS policy를 입력하십시오.
```
# pdadmin -a sec_master -p sec_master_password pdospolicy.pd
```
c. pdadmin 유틸리티를 사용하여 Policy Director에 로그인 및 암호 policy를 입력하십시오.
이 표를 사용하여, Policy Director 환경 속성 이름과 outdirectory/seos.ini 파일에 있는 [server] 스탠드의 적절한 값을 입력시킬 수 있습니다.

<table>
<thead>
<tr>
<th>Policy Director 확장 속성 이름</th>
<th>TACF/var/TACF/seos.ini 값</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login-LockMinutes</td>
<td>def_disable_time</td>
</tr>
<tr>
<td>Login-MaxFailedLogins</td>
<td>def_fail_count</td>
</tr>
<tr>
<td>Login-LockMinutes</td>
<td>def_diff_time</td>
</tr>
<tr>
<td>Login-MaxGraceLogins</td>
<td>def_fail_count</td>
</tr>
</tbody>
</table>

```
# pdadmin -a sec_master -p sec_master_password
```
```
pdadmin> object modify /OSSEAL/policy-branch/Login set attribute "Login-LockMinutes" "0"
pdadmin> object modify /OSSEAL/policy-branch/Login set attribute "Login-MaxGraceLogins" "0"
pdadmin> object modify /OSSEAL/policy-branch/Login set attribute "Login-MaxFailedLogins" "0"
pdadmin> object modify /OSSEAL/policy-branch/Login set attribute "Login-MaxPasswordDays" "0"
pdadmin> object modify /OSSEAL/policy-branch/Login set attribute "Login-MinPassswordDays" "0"
```

9. 시스템을 복원하고, PDOS를 시작한 후 마이그레이션을 검증하십시오.

a. HP-UX 전용
1) 다음 명령을 사용하여 TACF 드라이버가 구성되어 있지 않은지를 검증하십시오.
   ```
   kinstall -d SEOS
   ```
2) 다음 명령을 사용하여 SEOS가 존재하지 않는지를 검증하십시오.
   ```
   kmadmin -s SEOS
   ```
   SEOS에 대해 나타나는 정보가 없어야 합니다.

b. 자동 시작을 복원하십시오.
   ```
   # pdoscfg -autostart on
   ```
c. PDOS를 시작하십시오.
   ```
   # rc.osseal start
   ```
d. policy 마이그레이션이 완료된 후, policy를 생성 상태에 두기 전에 PDOS 감사 및 정고 모드 기능을 사용하여 결과로 발생하는 policy 작동을 검증하십시오.

10. TACF를 설치 제거하십시오.
관리 노드가 아니라 TSSM 앱드포트 환경에 있으면, wuninstalltacf 유틸리를 사용하여 TACF를 제거하십시오. Tivoli SecureWay Security Manager 사용자 안내서 버전 3.7.1 및 Tivoli SecureWay Security Manager 설치하기 전에 버전 3.7.1을 참조하십시오. 그렇지 않으면 TACF 제품 다이나토리의 내용을 제거할 수도 있습니다.

# rm -fr /var/TACF

**se2pdos 변환 유틸리티**

이 절에서는 변환 유틸리티 se2pdos에 대해 설명합니다. 대부분의 명령형 메개변수는 선택적입니다. 사용자나 그룹을 변환하고 있으며 집미어를 지정해야 합니다. 입력 파일을 지정하지 않으면, stdin으로 간주됩니다.

**사용법**


**옵션**

<table>
<thead>
<tr>
<th>옵션</th>
<th>설명</th>
<th>기본값</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f input file</td>
<td>입력 파일</td>
<td>stdin</td>
</tr>
<tr>
<td>-o output file</td>
<td>출력 파일</td>
<td>stdout</td>
</tr>
<tr>
<td>-e error file</td>
<td>오류/경고 로그</td>
<td>변환 출력의 주석</td>
</tr>
<tr>
<td>-nc</td>
<td>editres 또는 editfile 명령으로 작성된 자원에 대해 오브젝트와 템플릿을 작성하지 않음</td>
<td>editres 또는 editfile에 대한 오브젝트 및 템플릿 작성</td>
</tr>
<tr>
<td>-nr</td>
<td>레지스트리 명령(자원)을 변환하지 않음</td>
<td>자원 명령 처리</td>
</tr>
<tr>
<td>-na</td>
<td>레지스트리 명령(액세스)을 변환하지 않음</td>
<td>자원 명령 처리</td>
</tr>
<tr>
<td>-p branch</td>
<td>PDOS policy branch 이름</td>
<td>osseal.conf의 값, 설정하지 않을 경우 &quot;default&quot;</td>
</tr>
<tr>
<td>-s</td>
<td>자원 항목들과 별개의 레지스트리 항목</td>
<td>항목 구분 안함(-na 또는 -nr에 대해 무시됨)</td>
</tr>
<tr>
<td>-w #</td>
<td>경고 레벨</td>
<td>경고 레벨 1</td>
</tr>
<tr>
<td>0</td>
<td>모든 경고를 억제함</td>
<td>경고 레벨 1</td>
</tr>
<tr>
<td>1</td>
<td>가능한 시멘틱 차이 보고</td>
<td>경고 레벨 1</td>
</tr>
<tr>
<td>2</td>
<td>적용될 수 없는 항목 보고</td>
<td>경고 레벨 1</td>
</tr>
<tr>
<td>-l</td>
<td>원래 스크립트 맥락</td>
<td>맞추지 않음</td>
</tr>
<tr>
<td>-g suffix</td>
<td>그룹에 대한 접미어(-na 또는 -u를 지정하지 않을 경우 필수)</td>
<td>그룹에 대한 접미어(-na 또는 -u를 지정하지 않을 경우 필수)</td>
</tr>
<tr>
<td>-u suffix</td>
<td>사용자에 대한 접미어(-na 또는 -g를 지정하지 않을 경우 필수)</td>
<td>사용자에 대한 접미어(-na 또는 -g를 지정하지 않을 경우 필수)</td>
</tr>
<tr>
<td>-?</td>
<td>사용법</td>
<td>n/a</td>
</tr>
<tr>
<td>-V</td>
<td>버전</td>
<td>n/a</td>
</tr>
</tbody>
</table>
예제

이 절에는 변경 유필리티를 사용하는 방법에 대한 일부 예제가 있습니다. 예제에서 TACF 명령의 출력은 sedb2scr.out 파일입니다. 참조되는 LDAP 접미어가 작성되었습니다.

Policy Director 레지스터리 채우기
Policy Director 레지스터리를 초기에 TACF 사용자 및 그룹으로 채울 일련의 명령들을 생성하려면 명령행에 다음 명령을 입력하십시오.

```
se2pdos -nr -s "ou=users, o=IBM, c=US" -g "ou=groups, o=IBM, c=US" -f sedb2scr.out -o se2pdos.out
```

-s 옵션은 그룹 명령 이전에 사용자 명령이 생성되도록 하기 위해 사용됩니다.

그룹 접미어를 저장하지 않거나 사용자 접미어와 같지 않으면, 그룹 DN에 "group"이 추가됩니다. 예를 들면 다음과 같습니다.

```
editgrp ("mygroup") name('My group') owner('root')
```

그룹 DN은 유사한 이름이 저장된 사용자와 그룹 사이에 이름 충돌을 막기 위해 수정됩니다.

Policy Director Policy 정보 채우기
Policy Director policy 정보를 채울 일련의 명령들은 생성하려면, 명령행에 다음 명령을 입력하십시오.

```
se2pdos -na -i -f sedb2scr.out -o se2pdos.out
pdadmin -a sec-master -p password < se2pdos.out
```

-i 옵션은 se2pdos 명령과 함께 사용하면 TACF과 PDOS가 서로 맞춰져, 필요한 경우 pdadmin에 적용하기 전에 결과를 검사하고 수정할 수 있습니다.

TACF 쉐尔 스크립트 마이그레이트
TACF 쉐尔 스크립트 kevinc.se에 해당되는 PDOS를 생성하려면 명령행에 다음을 입력하십시오.

```
se2pdos -1 -f kevinc.se -o kevinc.pdos -u "ou=users, o=IBM, c=us"
```

여기서 kevinc.se 스크립트는 사용자를 작성하고 /home/kevinc/filea 파일에서 그 사용자에 대한 policy를 정의하는데 사용됩니다. -1 옵션은 쉐尔 스크립트를 변환할 때 권장됩니다. kevinc.se 스크립트는 다음으로 구성될 수 있습니다.

```
editusr ("kevinc") restrictions (days(AnyDay) time(AnyTime)) name('Kevin Cee') \
  grace(1) audit(FAILURE LOGINFAILURE) 
chusr ("kevinc") owner('root') 
join ("kevinc") group('staff') 
newres FILE ("/home/kevinc/filea") audit(FAILURE) defaccess(NONE) uid('kevinc') 
authorize FILE ("/home/kevinc/filea") audit(FAILURE) access(ALL) uid('kevinc') 
authorize FILE ("/home/kevinc/filea") audit(FAILURE) access(ALL) uid('root')
```

ACL 허용 및 Namespace
TACF 클래스 및 허용은 PDOS policy 및 허용에 매핑됩니다.
TACF _default 자원에 대한 허용은 PDOS Namespace 루트에 박령됩니다. 예를 들어, newres class ("_default")defaccess(READ)는 다른 인증되지 않은 /OSSEAL/policy-branch/class 루트에 대한 T(OSSEAL)r 허용 항목을 생성합니다. Policy Director 기본 허용 T(traverse)가 모든 허용 변환에 추가됩니다.

파일 클래스 루트에 대한 허용은 계승되지 않으므로, TACF FILE _default 자원에 대한 변환은 없습니다.

표 10. CONNECT PDOS 자원 및 허용 해당 사항

<table>
<thead>
<tr>
<th>TSSM/TACF 자원/클래스: CONNECT</th>
<th>PDOS 자원 Namespace</th>
<th>PDOS 허용</th>
</tr>
</thead>
<tbody>
<tr>
<td>all/read</td>
<td>NetOutgoing</td>
<td>C</td>
</tr>
<tr>
<td>none</td>
<td>NetOutgoing</td>
<td>없음</td>
</tr>
</tbody>
</table>

표 11. FILE PDOS 자원 및 허용 해당 사항

<table>
<thead>
<tr>
<th>TSSM/TACF 자원/클래스: FILE</th>
<th>PDOS 자원 Namespace</th>
<th>PDOS 허용</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>File</td>
<td>r, l, w, x, N, d, p, o, u, c, R, D</td>
</tr>
<tr>
<td>alter</td>
<td>File</td>
<td>r, l, w, x, N, d, p, o, u, c, R, D</td>
</tr>
<tr>
<td>chdir</td>
<td>File</td>
<td>D</td>
</tr>
<tr>
<td>chmod</td>
<td>File</td>
<td>p</td>
</tr>
<tr>
<td>chown</td>
<td>File</td>
<td>o</td>
</tr>
<tr>
<td>control</td>
<td>File</td>
<td>r, l, w, x, o, p, u, c, D</td>
</tr>
<tr>
<td>create</td>
<td>File</td>
<td>N</td>
</tr>
<tr>
<td>delete</td>
<td>File</td>
<td>d</td>
</tr>
<tr>
<td>none</td>
<td>File</td>
<td>없음</td>
</tr>
<tr>
<td>read</td>
<td>File</td>
<td>l, r</td>
</tr>
<tr>
<td>rename</td>
<td>File</td>
<td>R</td>
</tr>
<tr>
<td>sec(TSSM에서 ACL 변경)</td>
<td>File</td>
<td>p</td>
</tr>
<tr>
<td>update (r, w, x)</td>
<td>File</td>
<td>l, r, w, x</td>
</tr>
<tr>
<td>utime</td>
<td>File</td>
<td>U</td>
</tr>
<tr>
<td>write</td>
<td>File</td>
<td>w</td>
</tr>
<tr>
<td>execute</td>
<td>File</td>
<td>x</td>
</tr>
</tbody>
</table>

표 12. GRPSURROGATE = SURROGATE PDOS 자원 및 허용 해당 사항

<table>
<thead>
<tr>
<th>TSSM/TACF 자원/클래스: GRPSURROGATE = SURROGATE (&quot;GROUP.groupname&quot;)</th>
<th>PDOS 자원 Namespace</th>
<th>PDOS 허용</th>
</tr>
</thead>
<tbody>
<tr>
<td>all/read</td>
<td>Surrogate/Group</td>
<td>G</td>
</tr>
<tr>
<td>none</td>
<td>Surrogate/Group</td>
<td>없음</td>
</tr>
</tbody>
</table>
## 13. HOLIDAY PDOS 자원 및 허용 해당 사항

<table>
<thead>
<tr>
<th>TSSM/TACF 자원/클래스</th>
<th>HOLIDAY</th>
<th>PDOS 자원 Namespace</th>
<th>PDOS 허용</th>
</tr>
</thead>
<tbody>
<tr>
<td>all/read</td>
<td>Login/Holidays</td>
<td>L</td>
<td></td>
</tr>
<tr>
<td>none</td>
<td>Login/Holidays</td>
<td>없음</td>
<td></td>
</tr>
</tbody>
</table>

## 14. PROCESS PDOS 자원 및 허용 해당 사항

<table>
<thead>
<tr>
<th>TSSM/TACF 자원/클래스</th>
<th>PROCESS</th>
<th>PDOS 자원 Namespace</th>
<th>PDOS 허용</th>
</tr>
</thead>
<tbody>
<tr>
<td>all/read</td>
<td>File</td>
<td>K</td>
<td></td>
</tr>
<tr>
<td>none</td>
<td>File</td>
<td>없음</td>
<td></td>
</tr>
</tbody>
</table>

## 15. PROGRAM PDOS 자원 및 허용 해당 사항

<table>
<thead>
<tr>
<th>TSSM/TACF 자원/클래스</th>
<th>PROGRAM</th>
<th>PDOS 자원 Namespace</th>
<th>PDOS 허용</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>File</td>
<td>없음</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>File</td>
<td>r</td>
<td></td>
</tr>
<tr>
<td>none</td>
<td>File</td>
<td>없음</td>
<td></td>
</tr>
<tr>
<td>Trusted 랜덤</td>
<td>TCB/Secure-Programs</td>
<td>Namespace 허용만</td>
<td></td>
</tr>
</tbody>
</table>

## 16. SECFILE PDOS 자원 및 허용 해당 사항

<table>
<thead>
<tr>
<th>TSSM/TACF 자원/클래스</th>
<th>SECFILE</th>
<th>PDOS 자원 Namespace</th>
<th>PDOS 허용</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted 랜덤</td>
<td>TCB/Secure-Files</td>
<td>Namespace 허용만</td>
<td></td>
</tr>
<tr>
<td>SE FILE 허용</td>
<td>File</td>
<td>PDOS 파일 클래스 허용</td>
<td></td>
</tr>
</tbody>
</table>

## 17. SUDO PDOS 자원 및 허용 해당 사항

<table>
<thead>
<tr>
<th>TSSM/TACF 자원/클래스</th>
<th>SUDO</th>
<th>PDOS 자원 Namespace</th>
<th>PDOS 허용</th>
</tr>
</thead>
<tbody>
<tr>
<td>all/execute</td>
<td>Sudo/sudo-command</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sudo/sudo-command/Permitted</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sudo/sudo-command/Prohibited</td>
<td></td>
<td></td>
</tr>
<tr>
<td>none</td>
<td>Sudo/sudo-command</td>
<td>없음</td>
<td></td>
</tr>
</tbody>
</table>

## 18. SURROGATE SURROGATE PDOS 자원 및 허용 해당 사항

<table>
<thead>
<tr>
<th>TSSM/TACF 자원/클래스: SURROGATE SURROGATE (&quot;USER.username&quot;)</th>
<th>PDOS 자원 Namespace</th>
<th>PDOS 허용</th>
</tr>
</thead>
<tbody>
<tr>
<td>all/read</td>
<td>Surrogate/User</td>
<td>G</td>
</tr>
<tr>
<td>none</td>
<td>Surrogate/User</td>
<td>없음</td>
</tr>
</tbody>
</table>
표 19. TCP PDOS 자원 및 허용 해당 사항

<table>
<thead>
<tr>
<th>TSSM/TACF 자원/클래스 TCP</th>
<th>PDOS 자원 Namespace</th>
<th>PDOS 허용</th>
</tr>
</thead>
<tbody>
<tr>
<td>all, read, write</td>
<td>NetIncoming</td>
<td>C</td>
</tr>
<tr>
<td>none</td>
<td>NetIncoming</td>
<td>없음</td>
</tr>
</tbody>
</table>

표 20. TERMINAL PDOS 자원 및 허용 해당 사항

<table>
<thead>
<tr>
<th>TSSM/TACF 자원/클래스 TERMINAL</th>
<th>PDOS 자원 Namespace</th>
<th>PDOS 허용</th>
</tr>
</thead>
<tbody>
<tr>
<td>all, read, write</td>
<td>Login/Terminal/Local/Default/&lt;terminal&gt; 또는 Login/Terminal/Remote/Default/&lt;terminal&gt;</td>
<td>L</td>
</tr>
<tr>
<td>none</td>
<td>Login/Terminal/Local/Default/&lt;terminal&gt; 또는 Login/Terminal/Remote/Default/&lt;terminal&gt;</td>
<td>없음</td>
</tr>
</tbody>
</table>

표 21. GTERMINAL PDOS 자원 및 허용 해당 사항

<table>
<thead>
<tr>
<th>TSSM/TACF 자원/클래스 GTERMINAL</th>
<th>PDOS 자원 Namespace</th>
<th>PDOS 허용</th>
</tr>
</thead>
<tbody>
<tr>
<td>all, read, write</td>
<td>Login/Terminal/Local/&lt;group name&gt;/&lt;terminal&gt; 또는 Login/Terminal/Remote/&lt;group name&gt;/&lt;terminal&gt;</td>
<td>L</td>
</tr>
<tr>
<td>none</td>
<td>Login/Terminal/Local/&lt;group name&gt;/&lt;terminal&gt; 또는 Login/Terminal/Remote/&lt;group name&gt;/&lt;terminal&gt;</td>
<td>없음</td>
</tr>
</tbody>
</table>

스크립트 맵핑

TACF는 자원 허용을 기초로 하는 모델입니다. 자원 및 액세스는 별도로 정의된 후 허용 세트와 결합됩니다. PDOS 보호는 액세스(허용)에 있는 테이터 스트리 오브젝트의 콜렉션(ACL 템플릿)을 하나 이상의 시스템 자원에 바인딩하여 이루어집니다.

많은 TACF selang 명령이 PDOS pdadmin 명령에서 해당되는 사항을 수행하고 있습니다. 어떤 selang 명령에서는 pdadmin 해당 사항이 없습니다. 다음 표는 해당 사항이 있는 명령을 제 공합니다.

표 22. TACF 및 PDOS 해당 명령

<table>
<thead>
<tr>
<th>selang 명령</th>
<th>pdadmin 변환</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorize/authorize-</td>
<td>acl modify</td>
</tr>
<tr>
<td>access()</td>
<td>attach</td>
</tr>
<tr>
<td>uid()</td>
<td>set user</td>
</tr>
<tr>
<td>gid()</td>
<td>set group</td>
</tr>
<tr>
<td>via(pgm())</td>
<td>acl modify set attribute Access-Restrictions &quot;accessor:actions:filespec1,...:filespecn&quot;</td>
</tr>
<tr>
<td>newfile/chfile/editfile</td>
<td>object create</td>
</tr>
<tr>
<td></td>
<td>acl create</td>
</tr>
<tr>
<td>defaccess()</td>
<td>acl modify any-other</td>
</tr>
<tr>
<td></td>
<td>acl modify unauthenticated</td>
</tr>
</tbody>
</table>
표 22. TACF 및 PDOS 해당 명령 (계속)

<table>
<thead>
<tr>
<th>selang 명령</th>
<th>pdadmin 변환</th>
</tr>
</thead>
<tbody>
<tr>
<td>comment()</td>
<td>object modify descriptions</td>
</tr>
<tr>
<td>audit()</td>
<td>pop create</td>
</tr>
<tr>
<td></td>
<td>pop modify set audit-level all</td>
</tr>
<tr>
<td></td>
<td>pop attach</td>
</tr>
<tr>
<td>warning</td>
<td>pop create</td>
</tr>
<tr>
<td></td>
<td>pop modify set warning on</td>
</tr>
<tr>
<td></td>
<td>pop attach</td>
</tr>
<tr>
<td>restrictions()</td>
<td>pop create</td>
</tr>
<tr>
<td></td>
<td>pop modify set tod-access on</td>
</tr>
<tr>
<td></td>
<td>pop attach</td>
</tr>
<tr>
<td>newgrp/chgrp/editgrp</td>
<td>group create</td>
</tr>
<tr>
<td>comment()</td>
<td>group modify description</td>
</tr>
<tr>
<td>restrictions</td>
<td>pop create</td>
</tr>
<tr>
<td></td>
<td>pop modify set tod-access on</td>
</tr>
<tr>
<td></td>
<td>pop attach</td>
</tr>
<tr>
<td>newres/chres/editres</td>
<td>acl create</td>
</tr>
<tr>
<td>defaccess()</td>
<td>acl modify any-other</td>
</tr>
<tr>
<td></td>
<td>acl modify unauthenticated</td>
</tr>
<tr>
<td>comment()</td>
<td>object modify description</td>
</tr>
<tr>
<td>comment()(SUDO only)</td>
<td>object modify set attribute Sudo-Command</td>
</tr>
<tr>
<td></td>
<td>object modify set attribute Sudo-Target-User</td>
</tr>
<tr>
<td></td>
<td>object modify set attribute Sudo-Password</td>
</tr>
<tr>
<td></td>
<td>object modify set attribute Sudo-Arguments</td>
</tr>
<tr>
<td>audit()</td>
<td>pop create</td>
</tr>
<tr>
<td></td>
<td>pop modify set audit-level all</td>
</tr>
<tr>
<td></td>
<td>pop attach</td>
</tr>
<tr>
<td>warning</td>
<td>pop create</td>
</tr>
<tr>
<td></td>
<td>pop modify set warning on</td>
</tr>
<tr>
<td></td>
<td>pop attach</td>
</tr>
<tr>
<td>restrictions()</td>
<td>pop create</td>
</tr>
<tr>
<td></td>
<td>pop modify set tod-access on</td>
</tr>
<tr>
<td></td>
<td>pop attach</td>
</tr>
<tr>
<td>dates()(HOLIDAY only)</td>
<td>object create</td>
</tr>
<tr>
<td></td>
<td>object modify set attribute Holiday-Dates</td>
</tr>
<tr>
<td>targuid</td>
<td>object create</td>
</tr>
<tr>
<td></td>
<td>object modify set attribute Sudo-Target-User user</td>
</tr>
<tr>
<td>trust</td>
<td>object create TCB entry</td>
</tr>
<tr>
<td>newusr/chusr/editusr</td>
<td>create user</td>
</tr>
<tr>
<td>password()</td>
<td>user modify password</td>
</tr>
<tr>
<td>comment()</td>
<td>user modify description</td>
</tr>
<tr>
<td>restrictions()</td>
<td>policy set tod-access -user</td>
</tr>
<tr>
<td>selang 명령</td>
<td>pdadmin 변경</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>join</td>
<td>group modify add</td>
</tr>
<tr>
<td>join-</td>
<td>group modify remove</td>
</tr>
<tr>
<td>rmfile</td>
<td>acl delete object delete</td>
</tr>
<tr>
<td>rmgroup</td>
<td>group delete</td>
</tr>
<tr>
<td>rmres</td>
<td>acl delete object delete</td>
</tr>
<tr>
<td>rmusr</td>
<td>user delete</td>
</tr>
<tr>
<td>setoptions</td>
<td>inactive() object modify /OSSEAL/policy-branch/Login set attribute Login-MaxInactiveDays</td>
</tr>
<tr>
<td>showfile</td>
<td>acl show object show</td>
</tr>
<tr>
<td>showgrp</td>
<td>group show</td>
</tr>
<tr>
<td>showres</td>
<td>object show</td>
</tr>
<tr>
<td>showusr</td>
<td>user show</td>
</tr>
</tbody>
</table>

**PDOS** 해당 사항을 수반하지 않는 **TACF** 명령은 다음과 같습니다.

allow/allow-
chappl
chlogin/editlogin
newappl/chappl/editappl
environment
find
help
history
hosts
newlogin
rmappl
rmlogin
ruler
setoptions
showappl
source

**TACF** 명령 alias, unalias, source는 se2pdos 유틸리티에서 지원됩니다.
色彩

[ 가 ]
계층되지 않은 ACL 로열, 마이그레이션 36
계층된 ACL 로열, 마이그레이션 36
구문, 변환 유틸리티 40
구성
- 음성 13, 29
- 응답 파일 사용 16
- 응답 파일 작성 16
구성 자세, PDOS 11
구성 음성, PDOS 13, 29
구성 해제
- 음성 22, 33
- 응답 파일 사용 22, 23
- 응답 파일 작성 22
PDOS 21
구성 해제 자세, PDOS 21
구성 해제 명령 음성의 사용법, PDOS 21
구성 해제 음성
PDOS 33
구성 해제 음성, PDOS 22
구성 해제에 대한 응답 파일
- 속성 23
- 속성에 대한 명령행 음성 명령 23
구성에 대한 응답 파일
- 속성 17
- 속성에 대한 명령행 음성 명령 17
구성, PDOS 11

[ 마 ]
마이그레이션
개요 35
계층되지 않은 ACL 로열 36
계층된 ACL 로열 36
계획 36
마이그레이션 단계 37
변환 유틸리티 40
문서 policy 36
사전 마이그레이션 테스크 37
스크립트 명령 44
중형집중화된 policy 36
프로세스 37
ACL 파일 41
Namespace 41
PDOS 35
se2pdos 40
마이그레이션 계획 36
마이그레이션 단계 37
마이그레이트
PDOS 35
명령행에서 구성, PDOS 15

명령행에서 설치
AIX 8
HP-UX 9
Solaris 10
명령행에서 설치 제거
AIX 26
HP-UX 27
Solaris 28
명령행에서 시작
PDOS 19
Policy Director for Operating Systems 19

[ 바 ]
변환 유틸리티
구문 40
마이그레이션 40
사용법 40
예제 41
응선 40
문서 policy, 마이그레이션 36

[ 사 ]
사용법
- 구성 명령 음성 12
- 변환 유틸리티 40
사전 마이그레이션 테스크 37
설치
AIX 7
HP-UX 8
PDOS 7
Solaris 9
설치 계획, PDOS 5
설치 제거
AIX 25
HP-UX 26
PDOS 25
Smit 25
Solaris 27
SWRemove 26, 27
소프트웨어 요구사항
AIX 5
HP-UX 6
Solaris 6
속성
- 구성 해제에 대한 응답 파일 23
- 구성에 대한 응답 파일 17
속성에 대한 명령행 음성 명령
- 구성 해제에 대한 응답 파일 23
속성에 대한 명령행 음성 맵핑 (계속)
구성에 대한 응답 파일 17
스크립트 맵핑, 마이크로소프트 44
시작
PDOS 19
Policy Director for Operating Systems 19
실행 중, PDOS 19

[ 아 ]
에제, 변환 유필리티 41
음성
구성 13, 29
구성 해제 22, 33
변환 유필리티 40
se2pdos 40
응답 파일
응답 파일 사용 16, 23
응답 파일 작성 16, 22
응답 파일 사용
구성 16
구성 해제 22, 23
응답 파일 16, 23
응답 파일 작성
구성 16
구성 해제 22
응답 파일을 사용하여 구성, PDOS 16

[ 자 ]
자동 시작, PDOS 19
중앙집중화된 policy, 마이크로소프트 36
중지, PDOS 19

[ 타 ]
특성, PDOS 1

[ 과 ]
페키지 내용 3

[ 하 ]
하드웨어 요구사항 5

A
ACL 하용, 마이크로소프트 41
Admintooll 9
AIX
명령행에서 설치 8
명령행에서 설치 제거 26
설치 7
설치 제거 25
소프트웨어 요구사항 5
AIX에 설치, SMIT 7

H
HP-UX
명령행에서 설치 9
명령행에서 설치 제거 27
설치 8
설치 제거 26
소프트웨어 요구사항 6
HP-UX에 설치, SWinstall 8

N
Namespace, 마이크로소프트 41

P
PDOS
구성 11
구성 계획 11
구성 명령 음성 사용법 12
구성 음성 13, 29
구성 해제 21
구성 해제 계획 21
구성 해제 명령 음성 사용법 21
구성 해제 음성 22, 33
마이크로소프트 35
마이크로소프트 5
명령행에서 구성 15
명령행에서 시작 19
설치 7
설치 계획 5
설치 제거 25
시작 19
실행 중 19
응답 파일을 사용하여 구성 16
자동 시작 19
작동 방법 2
정보 1
조정 1
중지 19
특성 1
페키지 내용 3
하드웨어 요구사항 5
PDOS 정보 1
Policy Director for Operating Systems
  명령행에서 설치 19
  시작 19

S
sc2pdos
  마이크래이션 40
  음성 40
Smit 7, 25
Solaris
  명령행에서 설치 10
  명령행에서 설치 제거 28
  설치 9
  설치 제거 27
  소프트웨어 요구사항 6
Solaris에 설치, Admintool 9
SWinstall 8
SWRemove 26, 27
IBM 한글 지원에 관한 설문

FAX : (02) 3787-0123

보고 주시는 의견은 훨씬 고개 지원 체재를 위한 귀중한 자료가 됩니다.
독자 여러분의 좋은 의견을 기다립니다.

책 제목: Tivoli® SecureWay®
Policy Director for Operating Systems 설치 안내서
버전 3 팔리스 7

<table>
<thead>
<tr>
<th>성명</th>
<th>직위/담당업무</th>
</tr>
</thead>
<tbody>
<tr>
<td>회사명</td>
<td>부서명</td>
</tr>
<tr>
<td>주소</td>
<td></td>
</tr>
<tr>
<td>전화번호</td>
<td>팩스번호</td>
</tr>
<tr>
<td>전자우편주소</td>
<td></td>
</tr>
<tr>
<td>사용중인 시스템</td>
<td>○ 중대형 서버 ○ UNIX 서버 ○ PC 및 PC 서버</td>
</tr>
</tbody>
</table>

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 생각하셨습니까?
   □ 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) □ 모두

* IBM 한글 지원 서비스에 대해 기타 제안사항이 있으시면 적어주십시오.

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