SiteMinder

정책 서버 관리 안내서

12.52 SP1

ca technologies

CA Technologies 제품 참조

이 문서는 다음 CA Technologies 제품을 참조합니다 :

- SiteMinder
- eTrust SOA Security Manager(이전의 CA SOA Security Manager)
- CA IdentityMinder®(이전의 CA Identity Manager)
- CA Security Compliance Manager

CA 에 문의

기술 지원팀에 문의

온라인 기술 지원 및 지사 목록, 기본 서비스 시간, 전화 번호에 대해서는 http://www.ca.com/worldwide 에서 기술 지원팀에 문의하십시오.

설명서 변경 사항

이 설명서가 마지막으로 릴리스된 이후에 다음과 같이 업데이트되었습니다.

- CA SiteMinder 이벤트 관리자 구성 (페이지 214) - 이벤트 라이브러리 파일을 구성하는 방법에 대한 정보가 추가되었습니다(178452).
- LDAP 검색 시간 만료 문제 해결 (페이지 309) - SearchTimeout 레지스트리 설정을 설정하기 위한 또 다른 용례가 추가되었습니다. CQ169864 및 STAR Issue # 20130617 을 해결합니다.
- r12.x 정책 저장소 암호화 키 재설정 (페이지 127) - CQ171497 및 CQ171365 를 해결하기 위해 암호화 키를 재설정하기 전에 정책 서버를 중지하는 단계가 추가되었습니다.
- MySQL 세션 저장소 시간 만료 오류 해결 (페이지 313) - MySQL 데이터베이스에 대한 세션 저장소 시간 만료 오류 문제의 해결 방법을 설명하는 항목이 추가되었습니다. CQ 177929 를 해결합니다.
- 일부 LDAP 사용자 디렉터리에 대한 VLV 인덱싱으로 인해 SiteMinder 에이전트 그룹 조회가 실패함 (페이지 332) - VLV 인덱싱으로 인한 에이전트 그룹 조회 실패 문제의 해결 방법을 설명하는 항목이 추가되었습니다. CQ 176247 및 STAR 이슈 20397633-1 을 해결합니다.
- SM--관리 UI 가 응답하지 않음 (페이지 309) - 포함된 JBoss 응용 프로그램 서버가 있는 독립 실행형 관리 UI 설치 환경에서 관리 UI 가 응답하지 않는 문제의 해결 방법을 설명하는 항목이 추가되었습니다. CQ 175819 및 STAR 이슈 21529036-1 을 해결합니다.
- r12.x 정책 저장소 암호화 키 재설정 (페이지 127) - 지침이 업데이트되었고 CQ 171365/178999 를 해결합니다.
- ODBC 데이터베이스로 감사 데이터 가져오기 (페이지 55) - smauditimport 도구를 사용하여 -b 옵션을 통해 감사 데이터를 Oracle 데이터베이스로 가져올 때 "ODBC Oracle Wire Protocol Driver Setup"(ODBC Oracle 유선 프로토콜 드라이버 설정) 대화 상자에서 "Enable bulk load"(대량 로드 사용) 옵션을 설정하지 않도록 지시하는 참고가 추가되었습니다. CQ 159529 및 STAR 이슈 21045785-2 를 해결합니다.

목차

제 1 장: 정책 서버 관리

이 섹션은 다음 항목을 포함하고 있습니다.

정책 서버 관리 개요

정책 서버는 다음을 비롯한 다른 CA 제품과 함께 작동하는 액세스 제어용 플랫폼을 제공합니다.

- SiteMinder - 정책 서버와 SiteMinder 에이전트를 함께 사용하여 웹 서버에 대한 액세스 제어를 제공합니다.
- eTrust SOA Security Manager - 정책 서버와 [set AGENT value for your book]를 함께 사용하여 XML 기반 웹 서비스에 대한 액세스 제어를 제공합니다. 이 제품을 구입한 경우 자세한 내용은 *eTrust SOA Security Manager Policy Configuration Guide*(eTrust SOA Security Manager 정책 구성 안내서)를 참조하십시오.
- CA Identity Manager - 아이덴티티 관리 서비스를 제공합니다. 자세한 내용은 *CA Identity Manager Administration Guide*(CA Identity Manager 관리 안내서)를 참조하십시오.

참고: SiteMinder 및 정책 기반 리소스 관리에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

정책 서버 구성 요소

정책 서버 환경은 다음 두 개의 핵심 구성 요소로 구성됩니다.

- **정책 서버** - 정책 관리, 인증, 권한 부여 및 계정 서비스를 제공합니다.
- **정책 저장소** - 모든 정책 서버 데이터가 포함됩니다.

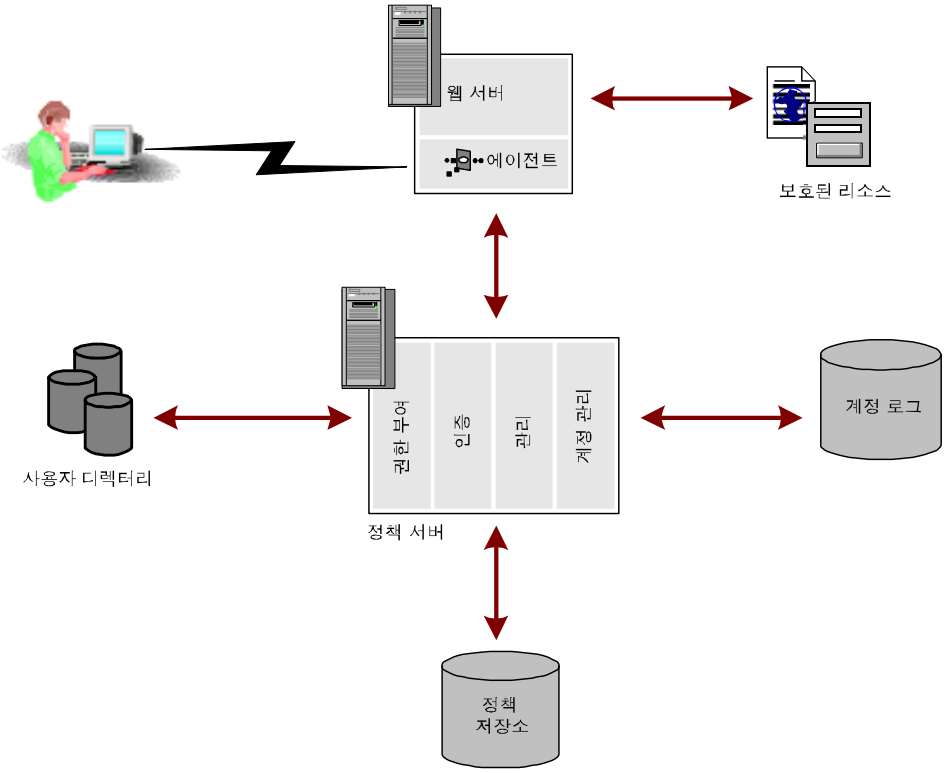
추가 구성 요소는 SiteMinder 에이전트 등의 다양한 CA 제품에 포함되어 있습니다. SiteMinder 에이전트는 표준 웹 서버 또는 응용 프로그램 서버와 통합되어 있으며, SiteMinder 에서 미리 정의된 보안 정책에 따라 웹 응용 프로그램 및 콘텐츠에 대한 액세스를 관리할 수 있도록 해 줍니다. 다른 유형의 SiteMinder 에이전트는 SiteMinder 에서 웹 엔터티가 아닌 다른 엔터티에 대한 액세스를 제어할 수 있도록 해 줍니다. 예를 들어 SiteMinder RADIUS 에이전트는 RADIUS 장치에 대한 액세스를 관리하는 반면 SiteMinder 가맹 에이전트는 포털 사이트에서 가맹의 웹 사이트에 전달되는 정보를 관리합니다.

정책 서버 작업

정책 서버는 액세스 제어 및 싱글 사인온 기능을 제공하며, 일반적으로 별도의 Windows 또는 UNIX 시스템에서 실행되어 다음과 같은 주요 보안 작업을 수행합니다.

- **인증** - 정책 서버는 다양한 인증 방법을 지원합니다. 즉, 토큰, 양식 기반 인증 및 공개 키 인증서를 사용하여 사용자 이름 및 암호를 기반으로 사용자를 인증할 수 있습니다.
- **권한 부여** - 정책 서버는 정책 서버 관리자가 설정한 액세스 제어 규칙을 관리하고 적용합니다. 이러한 규칙은 보호된 각 리소스에 대해 허용되는 작업을 정의합니다.
- **관리** - 정책 서버는 관리 UI 를 사용하여 구성할 수 있습니다. 관리 UI 는 정책 서버의 관리 서비스를 통해 정책 저장소에 구성 정보를 기록할 수 있습니다. 정책 저장소는 권한 정보를 포함하는 데이터베이스입니다.
- **계정** - 정책 서버는 시스템 내에서 발생하는 이벤트에 대한 감사 정보를 포함하는 로그 파일을 생성합니다. 이러한 로그는 미리 정의된 보고서 형식으로 인쇄할 수 있으므로 보안 이벤트나 잘못된 부분을 분석하는 데 유용합니다.
- **건전성 모니터링** - 정책 서버는 건전성 모니터링 구성 요소를 제공합니다.

다음 다이어그램에서는 단일 SiteMinder 웹 에이전트가 포함된 SiteMinder 환경에서의 간단한 정책 서버 구현을 보여 줍니다.

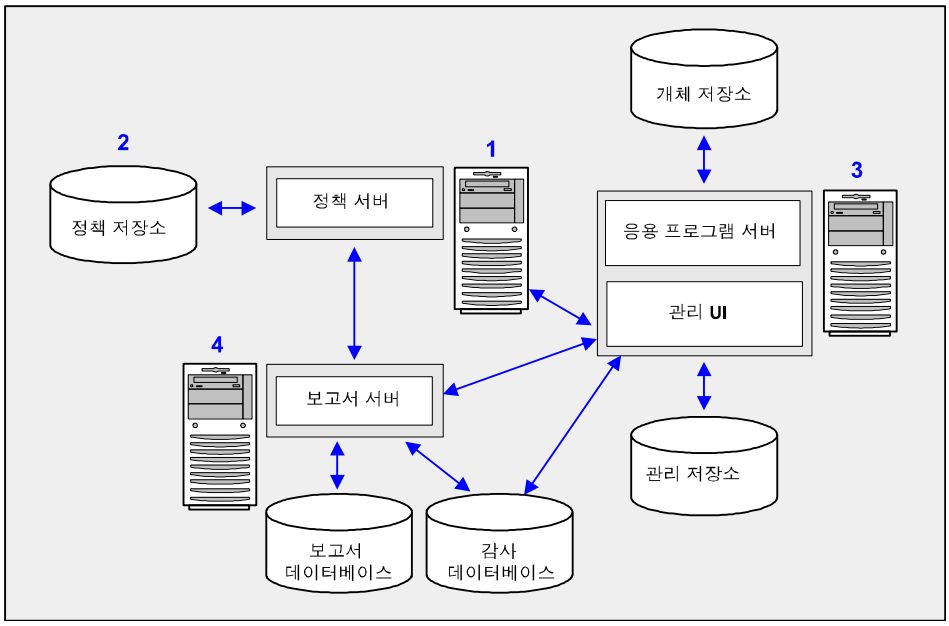


웹 구현에서 사용자는 브라우저를 통해 리소스를 요청합니다. 웹 서버가 해당 요청을 받으면 SiteMinder 웹 에이전트가 이를 가로챕니다. 웹 에이전트는 리소스가 보호되어 있는지 여부를 확인하고, 보호된 경우 사용자의 자격 증명을 수집하여 정책 서버로 전달합니다. 정책 서버는 네이티브 사용자 디렉터리에 대해 사용자를 인증한 다음, 정책 저장소에 포함된 규칙 및 정책을 기반으로 인증된 사용자에게 요청된 리소스에 대한 권한이 부여되었는지 확인합니다. 사용자가 인증되고 권한이 부여된 경우 정책 서버는 보호된 리소스에 대한 액세스 권한을 부여하고 권한 정보를 전송합니다.

참고: SiteMinder 에이전트 API 를 사용하여 사용자 지정 에이전트를 생성할 수 있습니다. 자세한 내용은 *Programming Guide for C*(C 프로그래밍 안내서)를 참조하십시오.

정책 서버 관리

다음 다이어그램에서는 정책 서버 관리 모델을 보여 줍니다.



1. **정책 서버** - 정책 서버는 정책 관리, 인증, 권한 부여 및 계정 서비스를 제공합니다.
2. **정책 저장소** - 정책 저장소에는 모든 정책 서버 데이터가 포함됩니다. 지원되는 LDAP 또는 관계형 데이터베이스에 정책 저장소를 구성할 수 있습니다.
3. **관리 UI** - 정책 서버를 통해 SiteMinder 관리자 계정, 개체 및 정책 데이터를 관리하려면 관리 UI 를 사용하십시오. 관리 UI 를 설치할 때 디렉터리 XML 파일, 관리자 사용자 저장소 및 개체 저장소를 구성합니다.
   - **개체 저장소** - 관리 UI 는 이벤트 및 태스크 기반의 비동기 응용 프로그램입니다. 개체 저장소에는 이 정보가 저장됩니다. Microsoft SQL Server 또는 Oracle 데이터베이스에 개체 저장소를 구성합니다.
   - **관리자 사용자 저장소** - 관리 UI 는 관리자 사용자 저장소를 사용하여 SiteMinder 관리자 계정을 인증합니다. 모든 관리자 계정은 단일 관리자 사용자 저장소에 저장해야 합니다. 관리 UI 를 설치할 때 지원되는 LDAP 디렉터리 서버나 ODBC 데이터베이스에 관리자 사용자 저장소를 구성합니다.

4. **보고서 서버 및 데이터베이스** - 관리 UI 에서 다양한 SiteMinder 정책 분석 및 감사 보고서를 생성하고 관리할 수 있습니다. 보고서 서버와 보고서 데이터베이스는 보고 기능을 사용하는 데 필요합니다. 정책 분석 보고서를 실행하려면 보고서 서버와 보고서 데이터베이스가 필요합니다. 감사 기반 보고서를 실행하려면 보고서 서버와 감사 데이터베이스가 필요합니다.

정책 서버 관리 태스크

정책 서버 관리자는 SiteMinder 환경의 시스템 수준 구성 및 조정과 성능 모니터링 및 유지 관리를 수행할 뿐 아니라 필요에 따라 사용자 및 사용자 세션 관리도 수행해야 합니다.

대부분의 기본적인 시스템 구성 및 관리 태스크는 정책 서버 관리 콘솔을 사용하여 수행합니다. 그 외의 다른 태스크는 관리 UI 를 사용하여 수행합니다.

정책 서버 관리 태스크에는 다음이 포함됩니다.

- 정책 서버 시작 및 중지
- 정책 서버 감독 기능 구성
- 캐시 관리
- 암호화 키 구성 및 관리
- 사용자 세션 및 계정 관리
- SiteMinder 환경의 건전성 모니터링
- 보고 실행

정책 서버 관리 콘솔

정책 서버 관리 콘솔(또는 관리 콘솔)에는 다양한 정책 서버 구성 및 시스템 관리 옵션이 있습니다. 관리 콘솔에서는 정보 및 컨트롤이 기능별로 그룹화되어 단일 창의 여러 탭에서 그룹별로 제공되는 탭 기반 사용자 인터페이스가 사용됩니다.

중요! 정책 서버 관리 콘솔은 Microsoft Windows 관리자 그룹의 구성원인 사용자만 실행해야 합니다.

관리 콘솔 시작

다음 단계를 수행하십시오.

- **Windows**

  SiteMinder 프로그램 그룹에서 정책 서버 관리 콘솔 아이콘을 선택합니다.

  중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하려면 관리자 권한으로 바로 가기를 열어야 합니다. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

- **UNIX**

  installation_directory/siteminder/bin/smconsole 을 실행합니다.

참고: UNIX 에서 정책 서버 관리 콘솔을 실행하려면 다음을 수행하십시오.

- X 디스플레이 서버가 실행 중인지 확인합니다.
- 다음을 실행하여 디스플레이가 사용되도록 설정합니다.

  `export DISPLAY=n.n.n.n:0.0`

  n.n.n.n

  정책 서버 호스트 시스템의 IP 주소를 지정합니다.

관리 콘솔 설정에 대한 변경 내용 저장

관리 콘솔의 아무 탭에서나 다음을 클릭하십시오.

- 설정을 저장하고 관리 콘솔을 열어 두려면 "적용"을 클릭합니다.
- 설정을 저장하고 관리 콘솔을 닫으려면 "확인"을 클릭합니다.

참고: 관리 콘솔 설정에 대한 변경 내용을 적용하려면 인증 및 권한 부여 프로세스를 중지했다가 다시 시작해야 합니다. 이러한 서비스를 다시 시작하기 전까지는 정책 서버에서 새 설정을 사용할 수 없습니다.

정책 서버 사용자 인터페이스

브라우저 기반 CA SiteMinder 관리 UI 는 기본적으로 정책 서버 개체에 대한 관리를 지원할 뿐 아니라 일부 시스템 관리 기능도 제공합니다.

관리 UI 에 액세스하려면

1. 다음 작업 중 하나를 수행하십시오.
   - 관리 UI 를 호스트하는 컴퓨터에서 "시작", "프로그램", "CA", "SiteMinder", "SiteMinder 관리 UI"를 차례로 클릭합니다.
   - 브라우저에서 다음 URL 을 엽니다.

     `http://fqdn:port/iam/siteminder/adminui`

     fqdn

     관리 UI 호스트 시스템의 정규화된 도메인 이름을 지정합니다.

     port

     관리 UI를 호스트하는 응용 프로그램 서버가 수신 대기하는 포트를 지정합니다. 독립 실행형 옵션으로 관리 UI를 설치한 경우 8080을 입력합니다.

     예: http://somehost@example.com:8080/iam/siteminder/adminui

     관리 UI 로그인 페이지가 표시됩니다.
2. 올바른 사용자 이름과 암호를 입력합니다.

   정책 서버에 처음으로 액세스하는 경우 정책 서버 설치 시 생성한 기본 슈퍼 사용자 관리자 계정을 사용합니다.

3. "로그인"을 클릭합니다.

   관리 UI 가 열립니다.

   창의 내용은 로그인하는 데 사용한 관리자 계정의 권한에 따라 달라집니다. 계정에서 액세스 권한을 가진 항목만 표시됩니다.

XPS 도구에 대한 액세스 권한 부여

SiteMinder 에 포함된 XPS 도구에 대한 액세스 권한은 관리자가 관리 UI 를 사용하여 각 사용자에게 부여해야 합니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "관리", "관리자", "관리자"를 차례로 클릭합니다.
3. 다음 작업 중 하나를 수행하십시오.
   - 새 관리자를 추가하려면 "관리자 만들기"를 클릭합니다.
   - 기존 관리자의 액세스 권한을 변경하려면 사용자를 검색하고 기록에 액세스할 사용자의 이름을 클릭합니다.
4. 각 필드에 이름을 입력하고 원하는 경우 설명을 입력합니다.
5. 사용자 경로를 입력하거나 "조회"를 클릭하여 기존 사용자 경로를 선택합니다.

   참고: XPS 도구에서 제어하는 모든 설정에 대한 쓰기 권한을 가지려면 사용자 경로(관리자가 관리 UI 에 지정하거나 XPSSecurity 도구를 사용하여 지정)가 필요합니다. 사용자 경로의 형식은 다음과 같습니다. *namespace*://*directory_server*/*DN* 또는 *Login_for_OS*
6. (선택 사항) 슈퍼 사용자 권한을 부여하려면 "슈퍼 사용자" 옵션을 선택하십시오.

7. "액세스 방법" 섹션에서 다음 명령줄 도구 중 하나를 선택합니다.

   XPSEvaluate 허용됨

   XPS 식 평가 도구에 대한 액세스를 허용합니다.

   XPSExplorer 허용됨

   XPS 데이터베이스를 편집하는 도구에 대한 액세스를 허용합니다.

   XPSRegClient 허용됨

   Web Access Manager 또는 보고서 서버를 권한 있는 클라이언트로 등록하는 XPS 도구에 대한 액세스를 허용합니다.

   XPSConfig 허용됨

   XPS 인식 제품의 XPS 설정을 검사하고 구성하는 도구에 대한 액세스를 허용합니다.XPSSecurity 허용됨

   XPS 사용자를 생성하고 해당 사용자의 XPS 관련 권한을 지정하는 보안 도구에 대한 액세스를 허용합니다.

8. 제출을 클릭합니다.

   관리자에게 선택된 XPS 도구를 사용할 권한이 부여됩니다.

추가 정보:

이벤트 처리기 라이브러리 추가 (페이지 144)

제 2 장: 정책 서버 시작 및 중지

이 섹션은 다음 항목을 포함하고 있습니다.

서비스 및 프로세스 개요

정책 서버는 Windows 에서 두 개의 서비스를 실행하고 UNIX 에서는 두 개의 프로세스를 실행합니다. 정책 서버 설치 프로세스는 정책 서버 및 모니터 프로세스를 시작하고, 나중에 시스템 시작 시 프로세스를 자동으로 실행하도록 감독 응용 프로그램을 구성합니다.

Windows 의 기본 정책 서버 프로세스는 다음과 같습니다.

정책 서버

인증, 권한 부여, 계정 설정, 로깅 및 관리(사용되도록 설정된 경우)를 위한 에이전트 요청을 처리합니다.

SiteMinder 건전성 모니터 서비스

OneView 모니터를 통해 인증 서버, 권한 부여 서버 및 웹 에이전트의 건전성과 성능을 모니터링합니다.

UNIX 의 기본 정책 서버 프로세스는 다음과 같습니다.

smpolicysrv

인증, 권한 부여, 계정 설정, 로깅 및 관리(사용되도록 설정된 경우)를 위한 에이전트 요청을 처리합니다.

smmon

OneView 모니터를 통해 인증 서버, 권한 부여 서버 및 웹 에이전트의 건전성과 성능을 모니터링합니다.

Windows 시스템에서 정책 서버 서비스 시작 및 중지

Windows 시스템에서 정책 서버 서비스를 시작하거나 중지하려면

- 관리 콘솔의 "상태" 탭에서 "시작" 또는 "중지" 단추를 클릭합니다.
- Windows "시작" 메뉴에서 "설정", "제어판", "서비스"를 사용하여 액세스할 수 있는 "Windows 서비스" 대화 상자를 사용합니다. 정책 서버 프로세스를 시작하거나 중지하면 관련 감독 기능도 시작되거나 중지됩니다.
- 명령줄에서 smpolicysrv 를 사용하여 정책 서버를 중지할 수 있습니다.

  ```
  installation_path\siteminder\bin\smpolicysrv -stop
  ```

참고: Windows 시스템의 경우 원격 데스크톱 또는 터미널 서비스 창에서 smpolicysrv 명령을 실행하지 *마십시오*. smpolicysrv 명령을 실행하려면 프로세스 간 통신이 필요하며 smpolicysrv 프로세스를 원격 데스크톱 또는 터미널 서비스 창에서 실행할 경우에는 프로세스 간 통신이 작동하지 않습니다.

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

UNIX 시스템에서 정책 서버 프로세스 시작 및 중지

UNIX 시스템에서 정책 서버 프로세스를 시작하거나 중지하려면 다음 작업 중 하나를 수행하십시오.

- 관리 콘솔의 "상태" 탭에서 해당하는 "시작" 또는 "중지" 단추를 클릭합니다.
- 제공된 스크립트를 사용합니다. 정책 서버 프로세스를 시작 및 중지할 수 있는 다음 두 개의 스크립트가 제공됩니다. 이러한 스크립트는 UNIX 감독 기능도 중지하므로 프로세스가 자동으로 다시 시작되지 않습니다.

  ```
  installation_path/siteminder/start-all
  installation_path/siteminder/stop-all
  ```

또한 다음 스크립트를 사용하여 정책 서버 프로세스를 시작 및 중지할 수도 있습니다. 스크립트를 실행할 때 UNIX 감독 기능이 실행되고 있지 않으면 프로세스와 함께 감독 기능이 시작됩니다. 이 스크립트는 다음과 같이 동일한 명령줄 옵션을 사용하여 호출할 수 있습니다.

installation_path/siteminder/smpolsrv

명령줄 옵션

-stop

프로세스를 중지합니다.

-start

프로세스를 시작합니다.

-status

프로세스가 실행 중인지 여부를 나타냅니다.

정책 서버는 모든 UNIX 감독 기능 작업을 *installation_directory*/log/smexec.log 파일에 로깅합니다. 로그 항목은 항상 기존 로그 파일에 추가됩니다.

추가 정보:

명령줄에서 정책 서버 문제 해결 (페이지 315)

정책 서버 종료 중 스레드 종료 시간

기본적으로 정책 서버는 모든 스레드가 종료될 때까지 3 분 동안 기다렸다가 종료됩니다. 이 시간이 지나면 종료되지 않은 스레드가 있더라도 정책 서버가 종료됩니다.

레지스트리 키를 생성하여 스레드가 종료될 때까지 정책 서버가 기다리는 최대 시간을 변경할 수 있습니다.

레지스트리 키를 생성하려면

1. 정책 서버 호스트 시스템에 액세스하여 다음 중 하나를 수행합니다.
   - Windows: 레지스트리 편집기를 열고 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\\Netegrity\SiteMinder\CurrentVersion\PolicyServer 로 이동합니다.
   - (UNIX) sm.registry 파일을 엽니다. 이 파일의 기본 위치는 *siteminder_home*/registry 입니다.

     siteminder_home

     정책 서버 설치 경로를 지정합니다.
2. 레지스트리 값 종류를 REG_DWORD 로 지정하여 MaxShutDownTime 을 생성합니다.

   측정 단위: 초

   기본값: 180

   최소값: 30

   최대값: 1800
3. 다음 작업 중 하나를 수행하십시오.
   - (Windows) 레지스트리 편집기를 종료합니다.
   - (UNIX) sm.registry 파일을 저장합니다.
4. 정책 서버를 다시 시작합니다.

중요! 종료 중 정책 서버 스레드가 제대로 종료되지 않으면 SiteMinder 지원부에 문의하십시오.

정책 서버 감독 기능 구성

정책 서버가 설치된 UNIX 및 Windows 에서는 하나 이상의 감독 기능 응용 프로그램이 정책 서버 프로세스의 상태를 모니터링하고 실패한 프로세스를 자동으로 다시 시작합니다. 다음 단원에서는 플랫폼별로 정책 서버 프로세스를 시작 및 중지하는 방법과 UNIX 및 Windows 감독 기능을 구성하고 사용 또는 사용하지 않도록 설정하는 방법에 대해 설명합니다.

Windows 감독 기능 구성

Windows 의 경우 각 정책 서버 프로세스는 별도의 감독 기능에 의해 모니터링됩니다. 이러한 각 감독 기능은 *Policy_Server_installation_path*\config\siteminder.conf 구성 파일에서 다음 임계값을 읽습니다.

SMEXEC_UPTIME_THRESHOLD

정책 서버 서비스가 시작된 후 관련 감독 기능이 빈번한 작동 중단에 대한 모니터링을 중지하기 전까지 정책 서버 서비스가 실행되어야 하는 최소 시간(초)을 나타냅니다. 이 매개 변수의 기본값은 60(초)입니다.

SMEXEC_RESTART_THRESHOLD

SMEXEC_UPTIME_THRESHOLD 매개 변수로 지정된 시간 내에 감독 기능이 서비스 재시작을 시도할 수 있는 최대 횟수를 나타납니다. 서비스가 이 매개 변수로 지정된 시도 횟수 이상 작동 중단될 경우 감독 기능은 서비스 재시작 시도를 중지합니다. 이 매개 변수의 기본값은 5(회)입니다.

임계값 매개 변수를 변경하려면 siteminder.conf 파일을 편집하고 정책 서버 프로세스를 다시 시작하십시오.

UNIX 감독 기능 구성

UNIX 의 경우 정책 서버 및 건전성 모니터 프로세스가 단일 감독 기능에 의해 모니터링됩니다. 감독 기능은 다음 구성 파일에서 해당 설정을 읽습니다.

installation_path/config/siteminder.conf

이 파일을 편집하여 다음 설정을 변경할 수 있습니다.

POLICYSERVER_ENABLED

감독 기능이 실행되기 시작할 때의 정책 서버 프로세스 상태를 나타냅니다. 감독 기능 시작 시 프로세스가 사용되도록 설정하려면 이 매개 변수를 YES 로 설정하십시오.

MONITOR_ENABLED

감독 기능이 실행되기 시작할 때의 건전성 모니터 프로세스 상태를 나타냅니다. 감독 기능 시작 시 프로세스가 사용되도록 설정하려면 이 매개 변수를 YES 로 설정하십시오.

SMEXEC_UPTIME_THRESHOLD

정책 서버 서비스가 시작된 후 관련 감독 기능이 빈번한 작동 중단에 대한 모니터링을 중지하기 전까지 정책 서버 서비스가 실행되어야 하는 최소 시간(초)을 나타냅니다. 이 매개 변수의 기본값은 60 입니다.

SMEXEC_RESTART_THRESHOLD

SMEXEC_UPTIME_THRESHOLD 매개 변수로 지정된 시간 내에 감독 기능이 서비스 재시작을 시도할 수 있는 최대 횟수를 나타납니다. 서비스가 이 매개 변수로 지정된 시도 횟수 이상 작동 중단될 경우 감독 기능은 서비스 재시작 시도를 중지합니다. 이 매개 변수의 기본값은 5(회)입니다.

UNIX 감독 기능 매개 변수를 변경하려면

1. *installation_path*/config/siteminder.conf 파일을 편집합니다.
2. 명령줄에서 다음 스크립트를 실행합니다.

   installation_path/siteminder/bin/stop-all

   정책 서버 프로세스가 중지됩니다.
3. 명령줄에서 다음 스크립트를 실행합니다.

   installation_path/siteminder/bin/start-all

   UNIX 감독 기능이 siteminder.conf 파일의 새 설정을 사용하여 다시 시작됩니다.

제 3 장: 정책 서버 데이터 저장소 옵션 구성

이 섹션은 다음 항목을 포함하고 있습니다.

데이터 저장소 옵션 구성 개요

정책 서버 관리 콘솔의 "데이터" 탭에서 SiteMinder 데이터 저장소의 저장소 위치를 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 시작합니다.

   중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "데이터" 탭을 클릭합니다.

   참고: 이 탭의 설정과 컨트롤에 대한 자세한 내용을 보려면 "도움말", "관리 콘솔 도움말"을 차례로 클릭하십시오.

3. "데이터베이스"에서 구성할 데이터 저장소를 선택합니다. 선택한 데이터 저장소에 따라 사용할 수 있는 저장소 기능이 달라집니다.

   참고: 다음 표에는 구성 가능한 데이터 저장소와 관련 저장소 옵션이 나와 있습니다. 설정을 어떻게 조합하는지에 따라 상황에 맞는 컨트롤에 표시되는 설정이 달라집니다.

4. "저장소"에서 선택된 데이터 저장소의 저장소 유형을 선택합니다.
5. 필수 정보를 구성합니다.
6. "확인"을 클릭하여 설정을 저장합니다.

다음 표에는 SiteMinder 데이터 저장소와 사용 가능한 저장소 옵션이 나와 있습니다. 이러한 저장소에 대한 자세한 내용은 *SiteMinder 구현 안내서*를 참조하십시오.

데이터베이스	사용 가능한 저장소
정책 저장소	LDAP ODBC
키 저장소	LDAP ODBC
감사 로그	ODBC 텍스트 파일
세션 저장소	ODBC CA Directory

정책 저장소 데이터베이스 구성

정책 저장소는 모든 정책 서버 개체가 저장되는 데이터베이스입니다.

정책 저장소 데이터베이스를 구성하려면

1. "데이터베이스" 드롭다운 목록에서 "정책 저장소"를 선택합니다.
2. "저장소" 드롭다운 목록에서 사용 가능한 저장소 유형("LDAP" 또는 "ODBC")을 선택합니다.
3. "Storage Options"(저장소 옵션)를 선택한 저장소 유형에 적절하게 지정합니다.

4. "적용"을 클릭하여 설정을 저장하거나, "확인"을 클릭하여 설정을 저장하고 콘솔을 종료합니다.
5. (선택 사항) 정책 저장소의 데이터베이스 저장소 유형을 "LDAP"으로 변경한 경우 해당 정책 저장소를 키 저장소로 사용하려면 정책 저장소 데이터베이스를 사용하도록 키 저장소 또는 감사 로그 구성 (페이지 35)에 설명된 단계를 완료합니다.

   참고: LDAP 사용 정책 저장소와 통신하는 정책 서버가 하나 이상 있는 경우 각 정책 서버 시스템의 관리 콘솔에서 동일한 설정을 구성하십시오.

정책 저장소 데이터베이스를 사용하도록 키 저장소 또는 감사 로그 구성

정책 저장소를 구성한 후 필요에 따라 데이터베이스를 구성할 수 있습니다. 정책 저장소가 호환되는 저장소 유형인 경우(즉, 정책 저장소를 저장하도록 구성된 데이터베이스가 다른 데이터베이스에도 유효한 저장소 옵션에 해당하는 경우) 정책 서버에서 정책 저장소 데이터베이스를 다음 중 하나 이상의 용도로 사용하도록 구성할 수 있습니다.

- 키 저장소
- 감사 로그

중요! LDAP 데이터베이스를 정책 저장소로 사용하는 경우에는 정책 저장소 데이터베이스를 감사 로그용으로 사용하지 *마십시오*. LDAP 데이터베이스에는 감사 로그를 기록할 수 없습니다. SiteMinder 샘플 데이터 원본(SmSampleUsers)을 정책 저장소로 사용하는 경우에는 정책 저장소 데이터베이스를 감사 로그용으로 사용하지 *마십시오*. 샘플 정책 저장소에서는 감사 로그가 지원되지 않습니다.

다른 데이터베이스를 정책 저장소 데이터베이스에 저장하도록 구성하려면 "데이터베이스" 드롭다운 목록에서 정책 저장소가 아닌 다른 데이터베이스를 선택할 때마다 "데이터베이스" 드롭다운 목록과 "Storage Options"(저장소 옵션) 영역 사이에 표시되는 "정책 저장소 데이터베이스 사용" 옵션을 설정하십시오.

"정책 저장소 데이터베이스 사용" 옵션이 선택되어 있으면 "저장소" 드롭다운 목록과 상황에 맞는 "Storage Options"(저장소 옵션)가 비활성화됩니다.

키 저장소를 위한 별도의 데이터베이스 구성

키 저장소는 정책 서버가 SiteMinder 에이전트에서 생성된 쿠키를 암호화하는 데 사용되는 키를 저장하는 위치입니다.

키 저장소를 위한 별도의 데이터베이스를 구성하려면

1. "데이터베이스" 드롭다운 목록에서 "키 저장소"를 선택합니다.
2. "저장소" 드롭다운 목록에서 사용 가능한 저장소 유형("LDAP" 또는 "ODBC")을 선택합니다.

   참고: 정책 서버에서는 정책 저장소와 키 저장소에 LDAP 및 ODBC 를 혼합하여 사용할 수 있습니다. 즉, 정책 저장소는 ODBC 데이터베이스에 있고 키 저장소는 LDAP 디렉터리 서버에 있거나, 그 반대일 수 있습니다. 지원되는 데이터베이스 목록은 기술 지원 사이트의 "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)를 참조하십시오.
3. "Storage Options"(저장소 옵션)를 선택한 저장소 유형에 적절하게 지정합니다.
4. "적용"을 클릭하여 설정을 저장하거나, "확인"을 클릭하여 설정을 저장하고 콘솔을 종료합니다.

감사 로그를 위한 별도의 데이터베이스 구성

감사 로그 데이터베이스는 정책 서버가 이벤트 정보가 포함된 감사 로그를 저장하는 위치입니다.

데이터베이스에 감사 로그를 저장하면 사용 중인 환경의 지연 시간이 늘어날 수 있습니다. 이 지연은 정책 서버와 데이터베이스 사이의 추가적인 트래픽으로 인해 발생합니다. 트랜잭션의 양이 늘어남에 따라 이 데이터베이스 지연 시간이 정책 서버의 성능에 영향을 줄 수 있습니다. 데이터베이스 속도가 느려지면 정책 서버도 느려집니다.

텍스트 파일에 로깅한 후 이러한 로그를 데이터베이스로 내보내는 방법은 데이터베이스의 성능이 허용할 수 없을 만큼 저하되는 경우 대안으로서 고려하십시오.

다음 단계를 수행하십시오.

1. "데이터베이스" 드롭다운 목록에서 "감사 로그"를 선택합니다.
2. "저장소" 드롭다운 목록에서 사용 가능한 저장소 유형을 선택합니다.

3. "Storage Options"(저장소 옵션)를 선택한 저장소 유형에 적절하게 지정합니다.
4. "적용"을 클릭하여 설정을 저장하거나, "확인"을 클릭하여 설정을 저장하고 콘솔을 종료합니다.

정책 서버 감사 로그를 ODBC 데이터베이스에 저장할지 텍스트 파일에 저장할지 결정할 때는 다음 요소를 고려하십시오.

- SiteMinder 보고 기능을 사용하려면 감사 로그를 ODBC 데이터베이스에 기록해야 합니다. 보고 기능은 텍스트 파일 로그를 지원하지 *않습니다*.
- SiteMinder 감사 로그를 ODBC 데이터베이스 및 텍스트 파일에 기록할 때는 다국어(I18N)가 지원됩니다.
- 기본적으로 SiteMinder 관리자가 정책 저장소 개체에 대해 변경한 내용은 감사 데이터베이스에 기록되지 않습니다. 이러한 개체 변경 사항은 *siteminder_home*\audit 디렉터리에 있는 텍스트 파일에 기록됩니다. 보고서에 이러한 이벤트를 포함하도록 SiteMinder 를 구성할 수 있습니다.
- 동기 로깅은 비동기 로깅보다 정책 서버의 성능에 더 큰 영향을 줍니다.
- ODBC 데이터베이스에 로깅하는 경우에는 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Database\ 레지스트리 위치에 있는 다음 레지스트리 키 값을 설정하십시오. 이러한 설정은 부하가 높을 경우 감사 데이터의 손실을 방지하는 데 유용합니다.

  ConnectionHangwaitTime

  부하가 높은 경우 60 초로 설정하는 것이 좋습니다. 기본값은 30 초입니다.

  QueryTimeout

  부하가 높은 경우 30 초로 설정하는 것이 좋습니다. 기본값은 15 초입니다.

  LoginTimeout

  부하가 높은 경우 30 초로 설정하는 것이 좋습니다. 기본값은 15 초입니다.

  참고: ConnectionHangwaitTime 값은 항상 QueryTimeout 및 LoginTimeout 값의 두 배 이상이어야 합니다.

추가 정보:

정책 저장소 개체에 대한 관리자 변경 내용 기록 (페이지 86)
보고서에 SiteMinder 관리 감사 이벤트를 포함하는 방법 (페이지 90)

세션 저장소 구성

세션 저장소는 정책 서버가 영구 세션 데이터를 저장하는 위치입니다.

다음 단계를 수행하십시오.

1. "데이터베이스"에서 "세션 서버"를 선택합니다.
2. "저장소"에서 사용 가능한 저장소 유형을 선택합니다.
3. "세션 서버 사용" 옵션을 설정합니다.

   하나 이상의 영역에서 영구 세션을 사용할 예정이라면 세션 저장소가 사용되도록 설정합니다. 세션 저장소를 사용하면 정책 서버 성능에 영향을 미칩니다.

   참고: 다음 옵션은 사용하지 않도록 설정됩니다.

   정책 저장소 데이터베이스 사용

   성능상의 이유로, 세션 저장소와 정책 저장소를 한 데이터베이스에서 실행할 수 없습니다.
4. 필수 저장소 옵션을 지정합니다.
5. "확인"을 클릭하여 설정을 저장하고 콘솔을 종료합니다.

부하가 높은 경우의 세션 저장소 시간 만료 구성

부하가 높은 경우에는 만료되거나 유휴 시간이 만료된 세션을 제거하는 등의 세션 저장소 유지 관리 태스크에 필요한 장기 실행 쿼리가 시간 만료될 수 있습니다. MaintenanceQueryTimeout 레지스트리 설정 값을 늘려 세션 저장소 유지 관리 태스크에 대한 만료 시간(기본값 60 초)을 조정하십시오. 유지 관리 스레드가 작업을 성공적으로 완료할 수 있도록 값을 늘리십시오.

MaintenanceQueryTimeout 레지스트리 설정은 다음 레지스트리 위치에서 찾을 수 있습니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\
SessionServer
```

LDAP 저장소 옵션 구성

LDAP 의 상황에 맞는 저장소 컨트롤을 사용하여 다음으로 구성된 LDAP 디렉터리 서버에 SiteMinder 를 연결할 수 있습니다.

- 정책 저장소
- 세션 저장소

다음 사항을 고려하십시오.

- SiteMinder 에서 세션 저장소로 지원하는 유일한 LDAP 디렉터리 서버는 CA Directory 입니다. 자세한 내용은 "12.52 SP1 SiteMinder Platform Support Matrix"(12.52 SP1 SiteMinder 플랫폼 지원표)를 참조하십시오.
- 정책 서버 관리 콘솔에서 LDAP 설정을 업데이트한 후 정책 서버를 다시 시작합니다. 정책 서버를 다시 시작해야 매개 변수가 적용됩니다.

LDAP 데이터베이스 구성

LDAP 데이터베이스를 구성하려면

1. "LDAP IP 주소" 필드에서 LDAP 서버의 서버 이름이나 IP 주소를 지정합니다. 성능상의 이유로 IP 주소를 사용하는 것이 좋습니다.

   참고: LDAP 서버 장애 조치를 허용하기 위해 이 필드에 여러 서버를 지정할 수 있습니다.

2. "루트 DN" 필드에서 SiteMinder 스키마가 있는 LDAP 분기를 지정합니다(예: o=myorg.org).

3. 정책 서버가 SSL 을 통해 LDAP 디렉터리와 통신하는 경우 "SSL 사용" 확인란을 선택합니다.

   참고: 이 옵션을 선택할 경우 "Netscape 인증서 데이터베이스 파일" 필드에서 인증서 데이터베이스를 지정해야 합니다.

4. "관리자 사용자 이름" 필드에서 LDAP 디렉터리 관리자의 DN(예: cn=Directory Manager)을 지정합니다.

5. "관리자 암호" 필드에 LDAP 디렉터리의 관리자 암호를 입력합니다.

6. 확인을 위해 "암호 확인" 필드에 LDAP 디렉터리의 관리자 암호를 다시 입력합니다.

7. "LDAP 연결 테스트"를 클릭하여 입력한 매개 변수가 올바르고 연결이 가능한지 확인합니다.

LDAP 장애 조치 구성

LDAP 디렉터리가 여러 개인 경우 장애 조치용 디렉터리를 구성할 수 있습니다. 장애 조치가 사용되도록 설정하려면 "LDAP 서버" 필드에 각 LDAP 서버의 IP 주소 및 포트 번호를 공백으로 구분하여 입력합니다. 각 서버에 대해 고유한 포트를 지정할 수 있습니다. LDAP 서버가 비표준 포트(비 SSL 의 경우 389, SSL 의 경우 636)에서 실행 중인 경우 구분 기호로 ':'을 사용하여 마지막 서버 IP 주소에 포트 번호를 추가합니다. 예를 들어 서버가 포트 511 및 512 에서 실행 중인 경우 다음과 같이 입력할 수 있습니다.

```
123.123.12.11:511 123.123.12.22:512
```

이 경우 포트 511 의 LDAP 서버 123.123.12.11 이 요청에 응답하지 않으면 요청은 자동으로 포트 512 의 123.123.12.22 로 전달됩니다.

모든 LDAP 서버가 동일한 포트에서 실행 중인 경우 마지막 서버에 포트 번호를 추가할 수 있습니다. 예를 들어 모든 서버가 포트 511 에서 실행 중인 경우 다음과 같이 입력할 수 있습니다.

```
123.123.12.11 123.123.12.22:511
```

향상된 LDAP 조회 처리 구성

SiteMinder 의 LDAP 조회 처리 기능이 개선되어 성능 및 중복성이 향상되었습니다. 이전 버전의 SiteMinder 에서는 LDAP SDK 계층을 통해 자동 LDAP 조회 처리 기능이 지원되었습니다. LDAP 조회가 발생하면 LDAP SDK 계층에서 정책 서버와의 상호 작용 없이 조회 대상 서버에 대한 요청 실행이 처리되었습니다.

이제 SiteMinder 에는 향상된 비자동 LDAP 조회 처리에 대한 지원이 포함되어 있습니다. 비자동 조회 처리 기능을 사용하면 LDAP 조회가 LDAP SDK 계층 대신 정책 서버로 반환됩니다. 조회에는 해당 조회를 처리하는 데 필요한 모든 정보가 포함됩니다. 정책 서버는 조회에 지정된 LDAP 디렉터리가 작동하는지 여부를 확인하며, 적절한 LDAP 디렉터리가 작동하지 않는 경우 요청을 종료할 수 있습니다. 이 기능은 오프라인 시스템에 대한 LDAP 조회로 인해 요청 대기 시간이 계속해서 증가할 경우 발생하는 성능 문제를 해결합니다. 이와 같이 대기 시간이 증가하면 SiteMinder 가 요청으로 포화 상태가 됩니다.

LDAP 조회 처리를 구성하려면

1. 정책 서버 관리 콘솔을 엽니다.

   중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "데이터" 탭을 선택합니다.

   향상된 조회 사용

   정책 서버가 LDAP SDK 계층에 의한 LDAP 조회 처리 대신 정책 서버의 향상된 LDAP 조회 처리를 사용할 수 있도록 하려면 이 확인란을 선택하십시오.

   최대 조회 홉 수

   원래 요청을 해결하려고 시도하는 동안 허용되는 최대 연속 조회 횟수를 나타냅니다. 조회는 추가 조회가 필요한 위치를 가리킬 수 있으므로 복제가 잘못 구성되어 조회 루프가 발생할 때 이 제한이 유용합니다.

3. 값을 필요한 대로 수정합니다.
4. 정책 서버를 다시 시작합니다.

큰 LDAP 정책 저장소에 대한 지원 구성

LDAP 정책 저장소의 크기가 클 경우 관리 UI 성능 문제가 발생할 수 있습니다.

이러한 문제를 방지하려면 다음 레지스트리 설정 값을 수정하면 됩니다.

Max AdmComm Buffer Size

관리 UI 버퍼 크기(한 패킷에서 정책 서버로부터 관리 UI 로 전달되는 총 데이터 바이트 크기)를 지정합니다.

다음 레지스트리 위치에서 이 설정을 구성하십시오.

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\PolicyServ\

이 값을 설정할 때는 주의해야 합니다. 더 큰 버퍼 크기를 할당하면 전체 성능이 저하됩니다.

범위: 256 KB~2,097,000 KB

기본값: 256 KB(이 레지스트리 설정이 없는 경우에도 적용됨)

SearchTimeout

LDAP 정책 저장소에 대한 검색 만료 시간(초)을 지정합니다.

다음 레지스트리 위치에서 이 설정을 구성하십시오.

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\LdapPolicyStore\SearchTimeout

이 설정의 적절한 값에 영향을 주는 요인의 예로는 다음이 포함됩니다(이 예에 국한되지 않음).

- 네트워크 속도
- LDAP 검색 쿼리 응답의 크기
- LDAP 연결 상태
- LDAP 서버의 부하

충분히 큰 값을 사용하면 많은 양의 정책 저장소 데이터를 가져올 때 LDAP 가 시간 만료되지 않습니다.

제한: 16 진수 숫자를 사용하십시오.

기본값: 0x14(20 초) 이 값은 또한 레지스트리 설정이 없는 경우에도 사용됩니다.

예: 0x78(120 초)

추가 정보:

정책 저장소 데이터베이스 구성 (페이지 34)
키 저장소를 위한 별도의 데이터베이스 구성 (페이지 36)

SSL 지원을 구성하는 방법

SSL 을 통한 LDAP 연결을 구성하려면 사용자의 인증서 데이터베이스 파일을 사용하도록 SiteMinder 를 구성해야 합니다.

SSL 을 통한 연결을 구성하려면 다음 단계를 완료하십시오.

1. SSL 연결 사전 요구 사항을 검토합니다.
2. NSS 유틸리티를 설치합니다.
3. 인증서 데이터베이스 파일을 생성합니다.
4. 인증서 데이터베이스에 루트 CA(인증 기관)를 추가합니다.
5. 인증서 데이터베이스에 서버 인증서를 추가합니다. 서버 인증서가 인증 기관에서 서명된 경우 각 인증 기관의 루트 인증서를 인증서 데이터베이스에도 추가하십시오.
6. 인증서 데이터베이스의 인증서 목록을 표시합니다.
7. 정책 서버를 인증서 데이터베이스에 연결합니다.

SSL 사전 요구 사항

다음 SSL 사전 요구 사항을 고려하십시오.

- 디렉터리 서버가 SSL 을 지원하는지 확인합니다.

  참고: 자세한 내용은 해당 공급업체의 설명서를 참조하십시오.

- SiteMinder 에서는 Mozilla LDAP SDK 를 사용하여 LDAP 디렉터리와 통신하므로 데이터베이스 파일이 Netscape 버전 파일 형식(cert8.db)이어야 합니다.

  중요! cert8.db 데이터베이스 파일에 인증서를 설치할 때 Microsoft Internet Explorer 를 사용하지 마십시오.

인증서 데이터베이스 파일 만들기

인증서 데이터베이스 파일을 만들려면 정책 서버에 포함된 Mozilla Network Security Services(NSS) certutil 응용 프로그램을 사용하십시오.

참고: 다음 절차에서는 태스크를 완료하는 데 필요한 옵션 및 인수에 대해 자세히 설명합니다. NSS 유틸리티 옵션 및 인수의 전체 목록은 NSS project page (NSS 프로젝트 페이지)에서 Mozilla 설명서를 참조하십시오.

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

다음 단계를 수행하십시오.

1. 명령 프롬프트에서 설치 bin 디렉터리로 이동합니다.

   예: C:\Program Files\CA\SiteMinder\bin

   참고: Windows 에는 네이티브 certutil 유틸리티가 있습니다. 정책 서버의 bin 디렉터리에서 작업 중인지 확인하십시오. 그렇지 않을 경우 실수로 Windows certutil 유틸리티를 실행할 수 있습니다.

2. 다음 명령을 입력합니다.

   `certutil -N -d certificate_database_directory`

   -N

   cert8.db, key3.db 및 secmod.db 인증서 데이터베이스 파일을 생성합니다.

   -d *certificate_database_directory*

   certutil 도구가 인증서 데이터베이스 파일을 생성할 디렉터리를 지정합니다.

   참고: 파일 경로에 공백이 있으면 경로를 따옴표로 묶으십시오.

   데이터베이스 키 암호화에 사용할 암호를 묻는 메시지가 표시됩니다.

3. 암호를 입력하고 확인합니다.

   필요한 다음 인증서 데이터베이스 파일이 생성됩니다.

   - cert8.db
   - key3.db
   - secmod.db

예: 인증서 데이터베이스 파일 만들기

```
certutil -N -d C:\certdatabase
```

인증서 데이터베이스에 루트 인증 기관 추가

루트 인증 기관(CA)을 추가하려면 정책 서버에 있는 Mozilla Network Security Services(NSS) certutil 응용 프로그램을 사용하십시오.

참고: 다음 절차에서는 태스크를 완료하는 데 필요한 옵션 및 인수에 대해 자세히 설명합니다. NSS 유틸리티 옵션 및 인수의 전체 목록은 NSS project page (NSS 프로젝트 페이지)에서 Mozilla 설명서를 참조하십시오.

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

다음 단계를 수행하십시오.

1. 명령 프롬프트에서 정책 서버 설치 bin 디렉터리로 이동합니다.

   예: C:\Program Files\CA\SiteMinder\bin

   참고: Windows 에는 네이티브 certutil 유틸리티가 있습니다. NSS 유틸리티의 bin 디렉터리에서 작업 중인지 확인하십시오. 그렇지 않을 경우 실수로 Windows certutil 유틸리티를 실행할 수 있습니다.

2. 다음 명령을 실행합니다.

   ```
   certutil -A -n alias -t trust_arguments -i root_CA_path -d
   certificate_database_directory
   ```

   -A

   인증서 데이터베이스에 인증서를 추가합니다.

   -n *alias*

   인증서의 별칭을 지정합니다.

   참고: 별칭에 공백이 있는 경우 별칭을 따옴표로 묶으십시오.

-t *trust_arguments*

인증서에 적용할 트러스트 특성을 지정합니다. 세 개의 사용 가능한 트러스트 범주는 다음 순서로 표시됩니다: "SSL, 전자 메일, 개체 서명". 각 범주 위치에서 다음 특성 인수를 0 개 이상 사용할 수 있습니다.

p

유효한 피어입니다.

P

트러스트된 피어입니다. 이 인수는 p 를 내포합니다.

c

유효한 CA 입니다.

T

클라이언트 인증서를 발급하도록 트러스트된 CA 입니다. 이 인수는 c 를 내포합니다.

C

서버 인증서를 발급하도록 트러스트된 CA 입니다(SSL 만 해당). 이 인수는 c 를 내포합니다.

중요! 이 인수는 SSL 트러스트 범주에 필요합니다.

u

인증 또는 서명에 인증서를 사용할 수 있습니다.

-i *root_CA_path*

루트 CA 파일의 경로를 지정합니다. 이 경로는 인증서 이름을 포함합니다. 인증서의 유효한 확장명에는 cert, .cer, .pem 이 포함됩니다.

참고: 파일 경로에 공백이 있으면 경로를 따옴표로 묶으십시오.

-d *certificate_database_directory*

인증서 데이터베이스가 포함된 디렉터리의 경로를 지정합니다.

참고: 파일 경로에 공백이 있으면 경로를 따옴표로 묶으십시오.

예: 인증서 데이터베이스에 루트 CA 추가

```
certutil -A -n "My Root CA"  -t "C,," -i C:\certificates\cacert.cer -d C:\certdatabase
```

인증서 데이터베이스에 서버 인증서 추가

SSL 을 통한 통신을 사용하려면 인증서에 서버 인증서를 추가하십시오. 정책 서버에 있는 Mozilla Network Security Services(NSS) certutil 응용 프로그램을 사용하십시오.

참고: 다음 절차에서는 태스크를 완료하는 데 필요한 옵션 및 인수에 대해 자세히 설명합니다. NSS 유틸리티 옵션 및 인수의 전체 목록은 NSS project page (NSS 프로젝트 페이지)에서 Mozilla 설명서를 참조하십시오.

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

다음 단계를 수행하십시오.

1. 명령 프롬프트에서 정책 서버 설치 bin 디렉터리로 이동합니다.

   예: C:\Program Files\CA\SiteMinder\bin

   참고: Windows 에는 네이티브 certutil 유틸리티가 있습니다. NSS 유틸리티의 bin 디렉터리에서 작업 중인지 확인하십시오. 그렇지 않을 경우 실수로 Windows certutil 유틸리티를 실행할 수 있습니다.

2. 다음 명령을 실행합니다.

   `certutil -A -n alias -t trust_arguments -i server_certificate_path -d certificate_database_directory`

   -A

   인증서 데이터베이스에 인증서를 추가합니다.

   -n *alias*

   인증서의 별칭을 지정합니다.

   참고: 별칭에 공백이 있는 경우 별칭을 따옴표로 묶으십시오.

-t *trust_arguments*

트러스트 인수를 지정합니다. 각 인증서에 대한 세 개의 사용 가능한 트러스트 범주는 다음 순서로 표시됩니다: "SSL, 전자 메일, 개체 서명". 각 범주 위치에서 다음 특성 인수를 0 개 이상 사용할 수 있습니다.

p

유효한 피어입니다.

P

트러스트된 피어입니다. 이 인수는 p 를 내포합니다.

중요! 이 인수는 SSL 트러스트 범주에 필요합니다.

-i *server_certificate_path*

서버 인증서의 경로를 지정합니다. 이 경로는 인증서 이름을 포함합니다. 인증서의 유효한 확장명에는 cert, .cer, .pem 이 포함됩니다.

참고: 파일 경로에 공백이 있으면 경로를 따옴표로 묶으십시오.

-d *certificate_database_directory*

인증서 데이터베이스가 포함된 디렉터리의 경로를 지정합니다.

참고: 파일 경로에 공백이 있으면 경로를 따옴표로 묶으십시오.

NSS 에서 인증서 데이터베이스에 서버 인증서를 추가합니다.

예: 인증서 데이터베이스에 서버 인증서 추가

```
certutil -A -n "My Server Certificate" -t "P,," -i C:\certificates\servercert.cer -d
C:\certdatabase
```

인증서 데이터베이스의 인증서 목록 표시

인증서가 인증서 데이터베이스에 있는지 확인하려면 Mozilla Network Security Services(NSS) certutil 응용 프로그램을 사용하십시오. 정책 서버에는 이 도구가 포함되어 있습니다.

참고: 다음 절차에서는 태스크를 완료하는 데 필요한 옵션 및 인수에 대해 자세히 설명합니다. NSS 유틸리티 옵션 및 인수의 전체 목록은 NSS project page (NSS 프로젝트 페이지)에서 Mozilla 설명서를 참조하십시오.

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

다음 단계를 수행하십시오.

1. 명령 프롬프트에서 정책 서버 설치 bin 디렉터리로 이동합니다.

   예: C:\Program Files\CA\SiteMinder\bin

   참고: Windows 에는 네이티브 certutil 유틸리티가 있습니다. NSS 유틸리티의 bin 디렉터리에서 작업 중인지 확인하십시오. 그렇지 않을 경우 실수로 Windows certutil 유틸리티를 실행할 수 있습니다.

2. 다음 명령을 실행합니다.

   `certutil -L -d certificate_database_directory`

   -L

   인증서 데이터베이스에 있는 모든 인증서의 목록을 표시합니다.

   -d *certificate_database_directory*

   인증서 데이터베이스가 포함된 디렉터리의 경로를 지정합니다.

   참고: 파일 경로에 공백이 있으면 경로를 따옴표로 묶으십시오.

   이 명령은 루트 CA 별칭, 서버 인증서 별칭, 그리고 인증서를 인증서 데이터베이스에 추가할 때 지정한 트러스트 특성을 표시합니다.

예: 인증서 데이터베이스의 인증서 목록 표시

```
certutil -L -d C:\certdatabase
```

정책 서버를 인증서 데이터베이스에 연결

SSL 을 통해 사용자 디렉터리와 통신하려면 정책 서버에서 인증서 데이터베이스를 지정해야 합니다.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 시작합니다.

   중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "데이터" 탭을 클릭합니다.

3. "Netscape 인증서 데이터베이스 파일" 필드에 인증서 데이터베이스 파일의 경로를 입력합니다.

   예: C:\certdatabase\cert8.db

   참고: key3.db 파일은 cert8.db 파일과 동일한 디렉터리에 있어야 합니다.

4. 정책 서버를 다시 시작합니다.

   정책 서버가 SSL 을 통하여 사용자 디렉터리와 통신할 수 있습니다.

ODBC 저장소 옵션 구성

다음 항목에 대한 ODBC 데이터 원본을 구성하려면 ODBC 의 상황에 맞는 저장소 컨트롤을 사용하십시오.

- 정책 저장소
- 키 저장소
- 감사 로그
- 세션 저장소

참고: ODBC 데이터 원본 구성에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

ODBC 데이터 원본 구성

ODBC 데이터 원본을 구성하려면

1. "데이터 원본 정보" 필드에 ODBC 데이터 원본 이름을 입력합니다. 이 필드에 여러 이름을 입력하여 ODBC 장애 조치가 사용되도록 설정할 수 있습니다.

   데이터 원본 정보

   ODBC 데이터 원본의 이름을 나타냅니다. 장애 조치가 가능하도록 이 필드에 여러 개의 이름을 입력할 수 있습니다.

   사용자 이름

   데이터베이스에 대한 모든 액세스 권한이 있는 데이터베이스 계정의 사용자 이름을 나타냅니다(필요한 경우).

   암호

   데이터베이스 계정의 암호를 포함합니다.

암호 확인

확인을 위해 데이터베이스 계정 암호를 중복해서 포함합니다.

최대 연결 수

동시에 허용되는 데이터베이스당 최대 ODBC 연결 수를 나타냅니다.

2. "ODBC 연결 테스트"를 클릭하여 입력한 매개 변수가 올바르고 연결이 가능한지 확인합니다.

ODBC 장애 조치 구성

ODBC 데이터 원본이 여러 개 있는 경우 장애 조치를 구성하려면 "데이터 원본 정보" 필드에 데이터 원본 이름을 쉼표로 구분된 목록으로 지정하십시오. 예를 들어 "SiteMinder Data Source1,SiteMinder Data Source2"를 입력하면 정책 서버는 Data Source1 을 먼저 찾습니다. SiteMinder Data Source1 이 응답하지 않으면 정책 서버는 자동으로 SiteMinder Data Source2 를 찾습니다.

참고: 위에 설명된 방법을 사용하면 정책 저장소, 키 저장소, 세션 저장소 및 감사 로그로 사용되는 데이터 원본에 대한 장애 조치를 구성할 수 있습니다.

SQL 쿼리에서 반환되는 레코드 수에 대한 제한 구성

많은 수의 레코드를 반환하는 SQL 쿼리로 인해 정책 서버가 중단되거나 작동 중단될 수 있습니다. 이러한 결과를 관리하기 위해 반환되는 레코드 수가 지정한 최대값을 초과할 경우 SMPS 로그에 경고 메시지를 출력할 수 있습니다.

최대값을 구성하려면 레지스트리 키 MaxResults 를 추가하고 해당 값을 1 이상으로 설정하십시오. 쿼리에서 반환되는 레코드 수가 MaxResults 로 지정된 제한과 같거나 이를 초과할 경우 정책 서버는 SMPS 로그에 경고를 출력합니다. MaxResults 가 0 으로 설정되어 있거나 정의되어 있지 않으면 경고 메시지가 출력되지 않습니다.

레지스트리 키 MaxResults 를 추가해도 반환되는 레코드 수는 변경되지 않습니다. 이 키를 추가하면 결과 수가 설정한 제한을 초과할 때 경고가 표시될 뿐입니다. 이 피드백을 사용하여 필요에 맞게 SQL 쿼리를 수정하고 반환되는 레코드 수를 세부적으로 조정할 수 있습니다.

SQL 쿼리에서 반환되는 레코드 수에 대한 제한을 구성하려면

1. 수동으로 레지스트리 키 MaxResults 를 추가합니다.

   Windows

   다음 위치에 레지스트리 키 MaxResults 를 추가합니다.

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersi
   on\Ds
   \ODBCProvider
   ```

   Solaris

   sm.registry 파일에 다음 행을 추가합니다.

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersi
   on\Ds
   \ODBCProvider=35921
   MaxResults=0x1; REG_DWORD
   ```

2. MaxResults 에 1 이상의 값을 할당합니다.

시간 만료에 대한 ODBC 레지스트리 설정 구성

아래에 나열된 매개 변수는 다양한 상황에서 ODBC 데이터베이스와 정책 서버 간의 연결에 대한 시간 만료를 제어합니다. 이 키는 Windows 및 UNIX 의 다음 위치에서 사용할 수 있습니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\Curre
ntVersion\Database
```

"LoginTimeout"

데이터베이스에 연결할 수 있는 시간입니다.

"QueryTimeout"

쿼리를 완료하기까지 30 초가 허용됩니다. 이 시간 내에 쿼리가 완료되지 않으면 데이터베이스에 취소 요청이 전송됩니다. ODBC 사용자 디렉터리의 경우 쿼리 만료 시간보다 사용자 디렉터리 개체의 Searchtimeout 이 우선합니다. 이 값은 XPSExplorer 를 사용하여 설정합니다.

"ConnectionHangWaitTime"

정책 서버가 연결을 응답 없음으로 표시할 때까지의 시간(초)입니다. 이 값은 QueryTimeout 또는 SearchTimeout 값보다 두 배 이상 커야 합니다.

"ConnectionTimeout"

연결의 최대 대기 시간입니다. 쿼리 만료 시간이나 로그인 만료 시간이 적용된 경우에는 이러한 값이 연결 만료 시간보다 우선합니다.

텍스트 파일 저장소 옵션 구성

텍스트 파일에 정책 저장소 감사 로그를 저장하도록 구성하려면 텍스트 파일 저장소 옵션을 사용하십시오.

텍스트 파일을 지정하려면"파일 이름" 필드에 파일의 전체 경로를 입력하거나, "찾아보기" 단추를 클릭하여 필요한 디렉터리로 이동한 다음 원하는 파일 이름을 클릭하거나 직접 입력하십시오.

ODBC 용 감사 데이터 가져오기 도구

정책 서버는 감사 데이터를 ODBC 데이터베이스에 저장하거나 텍스트 파일로 출력할 수 있습니다. smauditimport 도구는 SiteMinder 감사 데이터 텍스트 파일을 읽은 후 해당 데이터를 ODBC 데이터베이스로 가져옵니다. 이 데이터베이스는 5.x 또는 6.x 스키마를 사용하여 감사 저장소로 구성되어 있어야 합니다.

smauditimport 도구는 인증, 권한 부여 및 관리 데이터를 ODBC 데이터베이스의 해당하는 테이블로 가져옵니다. 이 도구는 ODBC 데이터베이스로 가져온 행 수를 로깅합니다. ODBC 데이터베이스로 가져올 수 없는 행의 경우네는 해당 행 번호를 로깅합니다.

정책 또는 사용자 저장소의 필드에 '[', ']' 또는 '\' 문자가 나타날 경우 앞에 이스케이프 문자 '\'(백슬래시)를 추가해야 합니다. 이러한 문자는 사용자 이름, 영역 이름 등의 필드에 해당 문자가 사용되었기 때문에 나타납니다.

이러한 문자를 자동으로 이스케이프 처리하려면 다음 레지스트리 키를 설정하십시오.
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\LogConfig]
값 종류: DWORD VALUE
값 이름: EscapeAuditFields
값 데이터: 1

값 데이터가 0 으로 설정되어 있거나 해당 키가 없으면 이스케이프 처리되지 않고 작업이 실패합니다.

참고: 일부 SiteMinder 설명서에서는 감사와 로깅이라는 용어가 같은 의미로 사용됩니다.

텍스트 파일에 더 많은 감사 데이터 로깅

기본적으로 정책 서버가 텍스트 파일에 로깅하는 감사 데이터의 양은 ODBC 데이터베이스에 로깅하는 양보다 적습니다. 텍스트 파일에 기본적으로 로깅되는 감사 데이터의 양을 늘려 ODBC 데이터베이스에 로깅되는 데이터 양과 맞출 수 있습니다. 이렇게 하려면 레지스트리 키 "Enable Enhance Tracing"을 수동으로 추가하고 해당 값을 1 로 설정하십시오. "Enable Enhance Tracing"이 사용되지 않도록 설정하려면 해당 값을 0(기본값)으로 설정하십시오.

텍스트 파일에 더 많은 감사 데이터를 로깅하려면

1. 레지스트리 키 "Enable Enhance Tracing"을 수동으로 추가합니다.

   Windows

   다음 키를 추가합니다.

   ```
   종류=DWORD
   \netegrity\SiteMinder\CurrentVersion\Reports
   \"Enable Enhance Tracing"
   ```

   Solaris

   다음 단계를 수행하십시오.

   a. .../siteminder/registry/sm.registry 파일을 엽니다.

   b. 다음 행을 찾습니다.

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder
   \CurrentVersion\Reports=25089
   ```

c. 이 행 아래에 다음을 추가합니다.

```
"Enable Enhance Tracing"=0x1;    REG_DWORD
```

d. 파일을 저장한 후 닫습니다.

2. "Enable Enhance Tracing"을 1 로 설정합니다.

참고: "Enable Enhance Tracing" 값은 EMS(Entitlement Management Services) 이벤트의 로깅에는 영향을 주지 않습니다.

ODBC 용 감사 데이터 가져오기 사전 요구 사항

smauditimport 도구를 실행하기 전에 다음 사전 요구 사항을 충족하는지 확인하십시오.

- 정책 서버가 Windows, Solaris 또는 Linux 운영 환경에 설치되어 있어야 합니다.

  참고: Solaris 및 Linux 플랫폼의 경우 smauditimport 도구를 실행하기 전에 nete_ps_env.ksh 를 실행하십시오.

- ODBC 데이터베이스가 5.x 또는 6.x 스키마를 사용하여 감사(로깅) 저장소로 구성되어 있어야 합니다.

  참고: ODBC 데이터베이스를 감사(로깅) 저장소로 구성하는 방법에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

- 레지스트리 키 "Enable Enhance Tracing"이 1 로 설정되어 있어야 합니다.

ODBC 데이터베이스로 감사 데이터 가져오기

smauditimport 도구는 SiteMinder 감사 데이터 텍스트 파일을 읽은 후 ODBC 데이터베이스로 가져옵니다. 이 도구는 정책 서버 설치 디렉터리의 \bin 디렉터리에 있습니다.

중요! 감사 데이터를 ODBC 데이터베이스로 가져오기 전에 SiteMinder 5.x 또는 6.x 스키마를 사용하여 데이터베이스를 감사 저장소로 구성하십시오. SiteMinder 스키마를 사용하여 ODBC 데이터베이스를 구성하는 방법에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

다음 단계를 수행하십시오.

1. 정책 서버가 설치된 컴퓨터에서 *siteminder_installation*\bin 으로 이동합니다.

   siteminder_installation

   정책 서버 설치 경로를 지정합니다.

2. 다음 명령을 실행합니다.

   smauditimport *audit_file dsn user_name user_password* -f -v -b*bulk_load_size* -s5 | -s6 -a*number*

   audit_file

   감사 데이터가 들어 있는 텍스트 파일의 경로와 이름을 지정합니다.

   참고: smauditimport 도구를 사용하려면 감사 데이터 텍스트 파일의 전체 경로 이름이 필요합니다.

   dsn

   ODBC 데이터베이스의 DSN(데이터 원본 이름)을 지정합니다.

   user_name

   ODBC 데이터베이스 관리자의 이름을 지정합니다.

   user_password

   ODBC 데이터베이스 관리자의 암호를 지정합니다.

   -a

   (필수) 정책 서버의 "Enable Enhance Tracing" 레지스트리 설정 값을 지정합니다. 이 설정은 HKEY_LOCAL_MACHINE\Software\Netegrity\SiteMinder\Currentversion\Reports 아래에 있습니다. Windows 운영 환경의 경우 이 설정은 Windows 레지스트리에 있습니다. UNIX 또는 Linux 운영 환경의 경우 이 설정은 sm.registry 파일에 있습니다. 이 설정 값이 이 옵션에 사용된 값과 일치해야 합니다.

   예: -a2("Enable Enhance Tracing" 레지스트리 설정이 2 임을 나타냄)

   -f

   (선택 사항) 감사 데이터를 가져오는 동안 오류가 발생할 경우 smauditimport 는 행 번호를 로깅하고 처리를 계속합니다.

   기본값: -f 옵션을 사용하지 않을 경우 오류가 발생하면 smauditimport 는 행 번호를 로깅하고 처리를 중지합니다.

-v

(선택 사항) 텍스트 파일에 있는 필드 수를 확인하고, 숫자 필드의 값이 지정된 범위 내에 있는지 확인하고, 데이터베이스에 대한 연결의 유효성을 검사하고, 오류를 출력합니다.

참고: smauditimport 가 유효성 검사 모드에서 실행되는 경우에는 데이터베이스로 데이터를 가져오지 않습니다.

-b *bulk_load_size*

(선택 사항) 읽은 후 ODBC 데이터베이스로 가져올 행 수를 지정합니다.

기본값: 100

참고: smauditimport 도구를 -b 옵션과 함께 사용하여 감사 데이터를 Oracle 데이터베이스로 가져오려면 "ODBC Oracle Wire Protocol Driver Setup"(ODBC Oracle 유선 프로토콜 드라이버 설정) 대화 상자에서 "Enable bulk load"(대량 로드 사용) 옵션을 설정하지 *마십시오*. "ODBC Oracle Wire Protocol Driver Setup"(ODBC Oracle 유선 프로토콜 드라이버 설정)의 "Enable bulk load"(대량 로드 사용) 옵션을 설정할 경우 대량 로드 중 예기치 않은 동작이 발생합니다.

-s5 | -s6

(선택 사항) 5.x 스키마나 6.x 스키마를 사용하여 감사 저장소로 구성된 ODBC 데이터베이스를 지원합니다.

기본값: 6.x 스키마를 사용하여 감사 저장소로 구성된 ODBC 데이터베이스를 지원합니다.

Netscape 인증서 데이터베이스 파일 지정

SSL 을 통해 정책 또는 사용자 정보를 저장하는 데 LDAP 디렉터리를 사용하려면 정책 서버를 Netscape 인증서 데이터베이스 파일이 들어 있는 디렉터리에 연결해야 합니다. 이 디렉터리에는 cert8.db 및 key3.db 파일이 있어야 합니다.

인증서 데이터베이스 파일을 설치하기 전에 이 파일의 복사본을 만드십시오. Netscape Communicator 에서 현재 인증서 데이터베이스를 사용하는 경우 인증서 데이터베이스 원본 대신 복사본을 사용하고 cert8.db 를 사용하지 마십시오.

"Netscape 인증서 데이터베이스 파일" 필드에 인증서 데이터베이스의 이름을 입력하거나 디렉터리 트리에서 데이터베이스를 찾아 선택하십시오. 이 필드에는 AD 네임스페이스를 사용하여 관리 UI 에 구성된 Active Directory 사용자 저장소의 값이 필요하지 않습니다. AD 사용자 저장소는 SSL 연결 설정 시 네이티브 Windows 인증서 리포지토리를 사용합니다.

추가 정보:

감사 로그를 위한 별도의 데이터베이스 구성 (페이지 36)

제 4 장: 일반 정책 서버 설정 구성

이 섹션은 다음 항목을 포함하고 있습니다.

정책 서버 설정 개요

정책 서버 관리 콘솔의 "설정" 탭에서 다음과 같이 정책 서버의 동작 및 작업 수행 방식을 결정하는 여러 일반 설정을 구성할 수 있습니다.

- 액세스 제어용 TCP 포트
- TCP 포트 및 비활성 시간 만료를 포함한 관리 설정
- 연결 설정
- RADIUS 설정
- 성능 설정
- OneView 모니터 설정

정책 서버 설정 구성

일반 정책 서버 설정을 구성하려면

1. 정책 서버 관리 콘솔을 시작합니다.

   중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "설정" 탭을 클릭합니다.

   참고: 이 탭의 설정과 컨트롤에 대한 자세한 내용을 보려면 "도움말", "관리 콘솔 도움말"을 차례로 클릭하십시오.

3. 원하는 설정을 조정합니다.
4. 작업을 마쳤으면 "적용"을 클릭하여 설정을 저장하거나, "확인"을 클릭하여 설정을 저장하고 관리 콘솔을 종료합니다.

액세스 제어 설정 구성

정책 서버는 인증, 권한 부여 및 계정 설정용으로 세 가지 개별 TCP 포트를 사용하여 SiteMinder 에이전트와 통신합니다.

이러한 에이전트 통신 포트를 사용하거나 사용하지 않도록 설정하고 각 기능에 사용되는 TCP 포트 번호를 변경하려면 관리 콘솔 "설정" 탭의 "액세스 제어" 그룹 상자에 있는 컨트롤을 사용하십시오.

정책 서버 관리 설정 구성

정책 서버는 TCP 포트를 통해 관리 UI 와 통신하여 브라우저 기반 정책 관리를 수행할 수 있도록 합니다.

관리 UI 와의 통신에 사용되는 TCP 포트 번호를 사용 또는 사용하지 않도록 설정하거나 변경하고 관리 비활성 상태에 대한 시간 만료 값을 지정하려면 관리 콘솔 "설정" 탭의 "관리" 그룹 상자에 있는 컨트롤을 사용하십시오.

정책 서버 연결 옵션 구성

최대 정책 서버 스레드 수와 정책 서버에 대한 연결의 유휴 만료 시간을 지정하려면 관리 콘솔 "설정" 탭의 "연결 옵션" 그룹 상자에 있는 컨트롤을 사용하십시오.

정책 서버 성능 설정 구성

캐시 및 스레드 설정을 구성하여 정책 서버 성능을 조정하려면 관리 콘솔 "설정" 탭의 "성능" 그룹 상자를 사용하십시오.

RADIUS 설정 구성

배포 환경에서 RADIUS 구성 요소를 지원하기 위한 설정을 지정하려면 관리 콘솔 "설정" 탭의 "RADIUS" 그룹 상자를 사용하십시오.

OneView 모니터 설정 구성

기본적으로 OneView 모니터는 모니터링 대상 정책 서버에서 로컬로 실행됩니다.

모니터가 다른 정책 서버에서의 연결을 원격으로 모니터링할 수 있도록 구성하거나 클러스터의 모든 정책 서버를 모니터링할 중앙 원격 정책 서버를 지정하려면 관리 콘솔 "설정" 탭의 "OneView 모니터" 그룹 상자를 사용하십시오.

SiteMinder 정책 데이터 동기화 다시 예약

SiteMinder 는 XPSSweeper 도구를 사용하여 정책 데이터를 자동으로 동기화합니다. 다음 매개 변수를 설정하여 이 도구가 실행되는 빈도를 변경할 수 있습니다.

AutosweepSchedule

XPSSweeper 프로세스가 실행되는 요일과 시간(시와 분)을 지정합니다.

기본값: 월요일마다 08:30

제한: 24 시간제를 사용하는 GMT 표준 시간대. 항목이 여러 개일 경우 쉼표 또는 공백으로 구분하십시오.

예: Mon@13:30,Tue@14:00

참고: 사용자에게 SiteMinder 바이너리 파일(XPS.dll, libXPS.so, libXPS.sl)에 대한 쓰기 액세스 권한이 *없다면* 관리자가 관리 UI 또는 XPSSecurity 도구를 사용하여 관련 XPS 명령줄 도구를 사용할 수 있는 권한을 사용자에게 부여해야 합니다.

다음 단계를 수행하십시오.

1. 정책 서버에서 명령줄을 열고 다음 명령을 입력합니다.

   ```
   xpsconfig
   ```

   이 도구가 시작되어 이 세션에 대한 로그 파일 이름이 표시되고 선택 메뉴가 열립니다.

2. 다음을 입력합니다.

   ```
   xps
   ```

   옵션 목록이 나타납니다.

3. 다음을 입력합니다.

   ```
   8 (AutosweepSchedule)
   ```

   XPSSweeper 도구에 대한 현재 일정이 표시됩니다.

4. C 를 입력하고 원하는 날짜와 시간을 입력합니다. 날짜 또는 시간을 여러 개 입력하려면 쉼표나 공백으로 구분합니다. 다음 형식을 사용합니다.

   ```
   Mon@13:30,Tue@14:00
   ```

   새 설정과 이전 설정이 표시됩니다. 추가한 값은 설정 맨 아래에 "보류 중인 값"으로 표시됩니다.

5. 다음 작업을 수행하십시오.

   a. Q 를 두 번 입력합니다.

   b. L 을 입력합니다.

   c. Q 를 입력하여 XPS 세션을 종료합니다.

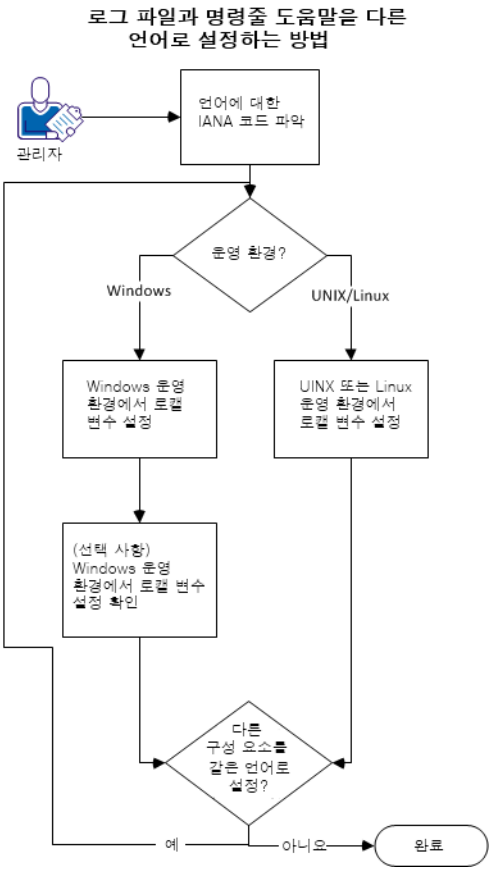
   변경 내용이 저장되고 명령 프롬프트가 표시됩니다.

다른 언어로 로그 파일 및 명령줄 도움말 설정

다음 구성 요소는 다른 언어로 로그 파일 및 명령줄 도움말을 설정할 수 있습니다.

- 정책 서버
- 웹 에이전트
- 보고서 서버
- CA SiteMinder Agent for SharePoint
- CA SiteMinder for Secure Proxy Server
- [set AGENT value for your book]
- SiteMinder SDK 로 만든 모든 사용자 지정 소프트웨어

다음 그래프는 다른 언어로 로그 파일 및 명령줄 도움말을 설정하기 위한 워크플로를 설명합니다.



다음 단계를 수행하십시오.

1. 언어의 IANA 코드를 파악합니다 (페이지 64).
2. 다음 절차 중 하나를 사용하여 운영 환경에 대한 환경 변수를 만듭니다.
   - Windows 운영 환경에서 로캘 변수를 설정합니다 (페이지 66).
   - UNIX 또는 Linux 운영 환경에서 로캘 변수를 설정합니다 (페이지 68).
3. (선택 사항) Windows 운영 환경에서 로캘 변수 설정을 확인합니다 (페이지 67).
4. (선택 사항) 1 - 3 단계를 반복하여 환경의 모든 다른 구성 요소를 동일한 언어로 설정합니다.

언어의 IANA 코드 파악

각 언어에는 고유 코드가 있습니다. IANA(Internet Assigned Numbers Authority)는 이러한 언어 코드를 할당합니다. 언어 코드를 로캘 변수에 추가하면 소프트웨어가 표시하는 언어가 변경됩니다. 로캘 변수를 만들기 전에 원하는 언어에 대한 올바른 코드를 파악하십시오.

다음 표에는 이 소프트웨어에서 지원되는 언어에 해당되는 IANA 코드가 수록되어 있습니다.

언어	IANA 코드
포르투갈어(브라질)	pt_BR
프랑스어	fr
독일어	de
이탈리아어	it
일본어	ja
한국어	ko
중국어 간체	zh-Hans
스페인어	es

참고: IANA 언어 코드의 목록은 이 타사 웹 사이트에서 볼 수 있습니다.

환경 변수

환경 변수는 사용자가 자신의 필요에 맞게 컴퓨터를 사용자 지정하기 위해 사용할 수 있는 설정입니다. 환경 변수의 예로는 다음과 같은 항목이 포함됩니다.

- 다운로드된 파일을 검색 또는 저장하기 위한 기본 디렉터리
- 사용자 이름
- 실행 파일을 검색하기 위한 위치의 목록(경로)

Windows 운영 환경에서는 컴퓨터의 모든 사용자에게 적용되는 글로벌 환경 변수를 사용할 수 있습니다. UNIX 또는 Linux 운영 환경의 환경 변수는 각 사용자 또는 프로그램에 대해 설정되어야 합니다.

로캘 변수를 설정하려면 다음 목록에서 운영 환경에 대한 절차를 선택하십시오.

- Windows 운영 환경에서 로캘 변수를 설정합니다 (페이지 66).
- UNIX 또는 Linux 운영 환경에서 로캘 변수를 설정합니다 (페이지 68).

Windows 운영 환경에서 로캘 변수 설정

다음 로캘 변수는 소프트웨어에 대한 언어 설정을 지정합니다.

SM_ADMIN_LOCALE

이 변수를 만들고 원하는 언어로 설정하십시오. 다른 언어를 사용할 *각* 구성 요소에서 이 변수를 설정하십시오. 예를 들어, 정책 서버와 에이전트를 프랑스어로 설정하려고 한다고 가정합니다. 이 경우, 이러한 두 구성 요소에서 이 변수를 프랑스어로 설정하십시오.

참고: 설치 관리자 또는 구성 프로그램은 이 변수를 설정하지 *않습니다.*

다음 단계를 수행하십시오.

1. "시작", "제어판", "시스템", "고급 시스템 설정"을 클릭합니다.

   "시스템 속성" 대화 상자가 나타납니다.

2. "고급" 탭을 클릭합니다.
3. "환경 변수"를 클릭합니다.
4. "시스템 변수" 섹션으로 이동하여 "새로 만들기"를 클릭합니다.

   "새 시스템 변수" 대화 상자가 열리고 그 안의 "변수 이름:" 필드에 커서가 위치합니다.

5. 다음 텍스트를 입력합니다.

   SM_ADMIN_LOCALE

6. "변수 이름:" 필드를 클릭한 다음 원하는 IANA 언어 코드 (페이지 64)를 입력합니다.
7. "확인"을 클릭합니다.

   "새 시스템 변수" 대화 상자가 닫히고 목록에서 SM_ADMIN_LOCALE 변수가 표시됩니다.

8. "확인"을 *두 번* 클릭합니다.

   로캘 변수가 설정되었습니다.

9. (선택 사항) 1 - 8 단계를 반복하여 동일한 언어로 다른 구성 요소를 설정합니다.

Windows 운영 환경에서 로캘 변수 값 확인

로캘 변수가 설정된 값을 언제든 확인할 수 있습니다. 이 절차는 변수를 설치한 후 올바로 설정되었는지 확인하기 위해 수행할 수 있습니다.

참고: UNIX 및 Linux 에서 변수 값을 확인하는 방법은 설정 절차 (페이지 68)에 설명되어 있습니다.

다음 단계를 수행하십시오.

1. 다음 단계를 사용하여 명령줄 창을 엽니다.
   a. "시작", "실행"을 차례로 클릭합니다.
   b. 다음 명령을 입력합니다.

      ```
      cmd
      ```

   c. "확인"을 클릭합니다.

      명령줄 창이 열립니다.
2. 다음 명령을 입력합니다.

   ```
   echo %SM_ADMIN_LOCALE%
   ```

   다음 줄에 로캘이 표시됩니다. 예를 들어, 언어가 독일어로 설정된 경우 다음 코드가 표시됩니다.

   ```
   de
   ```

   로캘 변수의 값이 확인되었습니다.

UNIX 또는 Linux 운영 환경에서 로캘 변수 설정

다음 로캘 변수는 소프트웨어에 대한 언어 설정을 지정합니다.

SM_ADMIN_LOCALE

이 변수를 만들고 원하는 언어로 설정하십시오. 다른 언어를 사용할 *각* 구성 요소에서 이 변수를 설정하십시오. 예를 들어, 정책 서버와 에이전트를 프랑스어로 설정하려고 한다고 가정합니다. 이 경우, 이러한 두 구성 요소에서 이 변수를 프랑스어로 설정하십시오.

참고: 설치 관리자 또는 구성 프로그램은 이 변수를 설정하지 *않습니다.*

다음 단계를 수행하십시오.

1. 원하는 구성 요소를 실행하는 컴퓨터에 로그인합니다.
2. 콘솔(명령줄) 창을 엽니다.
3. 다음 명령을 입력합니다.

   `export SM_ADMIN_LOCALE=IANA_language_code`

   다음 예의 명령은 언어를 프랑스어로 설정합니다.

   `export SM_ADMIN_LOCALE=fr`

   로캘 변수가 설정되었습니다.
4. (선택 사항) 다음 명령을 입력하여 로캘 변수가 올바로 설정되었는지 확인합니다.

   `echo $SM_ADMIN_LOCALE`

   다음 줄에 로캘이 표시됩니다. 예를 들어, 언어가 독일어로 설정된 경우 다음 코드가 표시됩니다.

   `de`
5. (선택 사항) 1 - 4 단계를 반복하여 동일한 언어로 다른 구성 요소를 설정합니다.

제 5 장: 인증서 데이터 저장소 관리

이 섹션은 다음 항목을 포함하고 있습니다.

인증서 해지 목록 업데이트

SiteMinder 는 인증서 데이터 저장소의 인증서에 대한 인증서 유효성 검사를 요구하는 기능을 제공합니다. 12.52 SP1 에서 페더레이션 기능은 인증서 데이터 저장소를 사용합니다. 이 기능에는 HTTP-아티팩트 백 채널 보호, SAML 메시지 확인 및 SAML 메시지 암호화가 포함됩니다. 인증서 데이터 저장소는 CRL(인증서 해지 목록)을 사용하여 유효성 검사를 구축할 수 있습니다.

인증서 데이터 저장소는 CRL 의 위치를 참조합니다. 기본적으로 SiteMinder 는 CRL 업데이트를 확인하지 않습니다. 업데이트를 확인하려면 CRL 업데이트 프로그램(CRLUpdater)이 사용되도록 설정하십시오.

다음 정보를 고려하십시오.

- SiteMinder 는 각 CRL 의 NextUpdate 날짜를 사용하여 저장된 위치를 참조할 시점과 CRL 을 다시 로드할 시점을 결정합니다. 또한 SiteMinder 는 날짜를 사용하여 인증서를 무효화할지 여부를 결정합니다.
- 기본적으로 SiteMinder 는 업데이트를 한 시간에 한 번 확인합니다. 기본 빈도를 늘릴 수 있습니다.
- CRL 업데이트 사용은 로컬 정책 서버 관리 설정입니다. 환경에서 하나의 정책 서버에 대해서만 CRL 업데이트가 사용되도록 설정하십시오.
- CRL 을 로드하지 못할 경우 CRL 이 성공적으로 로드되기 전에는 모든 인증서가 해지된 것으로 표시됩니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. XPSConfig 유틸리티를 시작합니다.
3. CDS 를 입력하고 Enter 키를 누릅니다.
4. EnableCRLUpdater 에 대한 숫자를 입력하고 Enter 키를 누릅니다.
5. C 를 입력하고 Enter 키를 누릅니다.
6. yes 를 입력하고 Enter 키를 누릅니다.
7. Q 를 입력합니다.
8. 다음 단계 중 하나를 완료합니다.
   - SiteMinder 에서 업데이트를 확인하는 빈도를 변경하려면
     a. DefaultCRLUpdaterSleepPeriod 에 대한 숫자를 입력하고 Enter 키를 누릅니다.
     b. C 를 입력하고 Enter 키를 누릅니다.
     c. 새 값을 입력하고 Enter 키를 누릅니다.
     d. 유틸리티를 종료합니다.
   - 기본 빈도를 그대로 두려면 유틸리티를 종료합니다.
9. 정책 서버를 다시 시작합니다.

   CRL 목록 업데이트가 예약됩니다.

기본 CRL 업데이트 간격 변경

업데이트 간격은 인증서 데이터 저장소가 CRL 을 다시 로드하는 빈도입니다. 저장된 CRL 파일에 NextUpdate 값이 포함되어 있지 않은 경우 업데이트 간격을 구성하십시오. 데이터 저장소는 SiteMinder 구성에 CRL 파일을 추가할 때 지정한 위치에서 업데이트된 CRL 을 찾습니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "X509 인증서 관리", "CDS 설정"을 선택합니다.
3. 업데이트 기간에 대한 새 값을 입력합니다. 기본값은 1 일입니다.
4. "저장"을 클릭합니다.

새 값은 업데이트 간의 간격입니다.

OCSP 업데이트

SiteMinder 는 인증서 데이터 저장소의 인증서에 대한 인증서 유효성 검사를 요구하는 기능을 제공합니다. 12.52 SP1 에서 페더레이션 기능은 인증서 데이터 저장소를 사용합니다. 이 기능에는 HTTP-아티팩트 백 채널 보호, SAML 메시지 확인 및 SAML 메시지 암호화가 포함됩니다.

인증서 데이터 저장소는 인증서의 유효성을 검사하기 위해 OCSP 서비스를 사용할 수 있습니다. OCSP 는 CA(인증 기관)가 필요 시 인증서 유효성 검사를 제공하기 위해 제공하는 HTTP 서비스를 사용합니다.

기본적으로 SiteMinder 는 인증서 데이터 저장소에서 인증서의 해지 상태를 확인하지 않습니다. OCSP 응답자를 통해 해지 상태를 확인하려면 OCSP 업데이트 유틸리티(OCSPUpdater)를 사용하십시오. OCSPUpdater 는 사용되도록 설정된 경우 구성된 OCSP 응답자에 대한 해지 상태를 5 분마다 확인합니다. 이 기본 주기는 구성할 수 있습니다.

OCSPUpdater 를 구성할 때는 다음 구성 요소를 사용합니다.

- SMocsp.conf 파일

  OCSPUpdater 는 OCSP 응답자 구성에 SMocsp.conf 파일을 사용합니다. 인증서를 발급하는 각 CA(인증 기관)마다 자체 OCSP 응답자가 있습니다. SMocsp.conf 파일에서 인증서 데이터 저장소의 각 CA 인증서에 대한 모든 OCSP 응답자를 포함하십시오.

  OCSPUpdater 를 사용하려면 SMocsp.conf 파일이 있어야 합니다.

  참고: SMocsp.conf 파일은 SiteMinder X.509 인증서 인증 체계가 자체 OCSP 구현을 구성하기 위해 사용하는 것과 동일한 파일입니다.

- XPSConfig 유틸리티

  XPSConfig 를 사용하면 OCSPUpdater 의 사용 여부 및 업데이트 빈도 설정과 같은 동작을 사용자 지정할 수 있습니다. 사용자 지정은 OCSPUpdater 를 실행 중인 정책 서버에 로컬로 적용됩니다. OCSPUpdater 는 SiteMinder 배포에서 하나의 정책 서버에서만 사용되도록 설정하십시오.

OCSP 및 CRL 검사 간 장애 조치

인증서 데이터 저장소는 OCSP 에서 CRL 유효성 검사로의 장애 조치를 지원합니다. CRL 및 OCSP 검사를 구성하면 둘 사이의 장애 조치를 사용할 수 있습니다.

SiteMinder 페더레이션 기능은 확장이 인증서에 있더라도 장애 조치가 구성된 인증서 배포 지점 확장을 지원하지 않습니다.

장애 조치에 대한 자세한 내용은 *정책 서버 구성 안내서*의 인증서 유효성 검사 단원을 참조하십시오.

OCSP 업데이트 예약

OCSP 업데이트는 XPSConfig 를 사용하여 예약합니다.

중요! OCSP 업데이트 사용은 로컬 정책 서버 관리 설정입니다. OCSPUpdater 는 SiteMinder 배포에서 하나의 정책 서버에서만 사용되도록 설정하십시오.

OCSP 업데이트를 예약하려면

1. 정책 서버 호스트 시스템에 로그인합니다.
2. XPSConfig 유틸리티를 시작합니다.
3. CDS 를 입력하고 Enter 키를 누릅니다.
4. EnableOCSPUpdater 에 대한 숫자를 입력하고 Enter 키를 누릅니다.
5. C 를 입력하고 Enter 키를 누릅니다.
6. yes 를 입력하고 Enter 키를 누릅니다.
7. Q 를 입력합니다.
8. 다음 태스크 중 하나를 수행합니다.
   - SiteMinder 의 업데이트 확인 빈도를 변경합니다.
     a. DefaultOCSPUpdaterSleepPeriod 에 대한 숫자를 입력하고 Enter 키를 누릅니다.
     b. C 를 입력하고 Enter 키를 누릅니다.
     c. 새 값을 입력하고 Enter 키를 누릅니다.
     d. 유틸리티를 종료합니다.
   - 유틸리티를 종료하여 기본값 빈도를 그대로 둡니다.
9. 정책 서버를 다시 시작합니다.

OCSP 해지 상태 업데이트가 예약됩니다. 업데이트가 초기화되려면 페더레이션 싱글 사인온 트랜잭션이 수행되어야 합니다. OCSPUpdater 가 사용되도록 설정된 정책 서버가 이 첫 번째 트랜잭션을 실행해야 합니다. 배포의 다른 정책 서버는 이후의 트랜잭션을 수행할 수 있습니다.

OCSP 업데이트에 맞게 SMocsp.conf 파일 수정

OCSPUpdater 는 응답자 구성 값에 대해 SMocsp.conf 파일을 사용합니다. 이 파일은 X.509 인증서 인증 체계가 OCSP 구현을 구성하기 위해 사용하는 것과 동일한 파일이지만, 인증 체계에 대한 모든 설정이 페더레이션에 적용되는 것은 아닙니다.

SMocsp.conf 파일은 *siteminder_home*/config 디렉터리에 있어야 합니다.

중요! SMocsp.conf 파일에 특정 CA 에 대한 항목이 있다고 해서 해당 OCSP 가 사용되도록 설정되었음을 의미하지는 않습니다. EnableOCSPUpdater 설정을 Yes 로 설정해야 합니다.

파일을 편집하려면

1. *siteminder_home*/config 로 이동합니다.
2. 텍스트 편집기에서 파일을 엽니다.
3. 다음 태스크 중 하나를 수행합니다.
   - 기존 OCSPResponder 항목을 수정합니다.
   - 인증서 매핑에서 IssuerDN 과 일치하는 각 IssuerDN 에 고유한 OCSPResponder 항목을 추가합니다.

     중요! 발급자 DN 에 응답자 레코드가 없거나 구성이 올바르지 않으면 정책 서버는 인증서의 유효성 검사를 확인하지 않고 인증서 작업을 수행합니다.
4. 업데이트에 영향을 미칠 수 있는 파일 설정을 편집합니다.

   중요! OCSP 가 사용되도록 설정된 정책 서버 하나에는 하나의 파일만 있을 수 있습니다.
5. 파일을 저장합니다.
6. OCSPUpdater 가 이미 사용되도록 설정된 경우에는 정책 서버를 다시 시작합니다. 그렇지 않은 경우에는 다음 smkeytool 명령을 사용하여 편집된 SMocsp.conf 파일을 로드할 수 있습니다.

   ```
   smkeytool -loadOCSPConfigFile
   ```

추가 정보:

페더레이션에서 사용되는 SMocsp.conf 설정 (페이지 75)

페더레이션에서 사용되는 SMocsp.conf 설정

SMocsp.conf 파일을 수정하기 위한 지침은 다음과 같습니다.

- 설정의 이름은 대/소문자가 구분되지 않는 경우도 있습니다. 항목의 대/소문자 구분 여부는 특정한 설정에 따라 다릅니다.
- 파일의 설정이 비어 있으면 정책 서버에서 오류 메시지를 보냅니다. 이 메시지는 항목이 올바르지 않음을 나타냅니다. 정책 서버는 이 설정을 무시합니다. 설정을 비워 두려면 메시지를 무시하십시오.
- 설정 이름 앞에 공백을 두지 마십시오.

SMocsp.conf 파일에서 페더레이션에 대한 다음 설정을 구성할 수 있습니다.

OCSPResponder

필수입니다. 항목이 OCSP 응답자 레코드임을 나타냅니다. 각 OCSP 응답자 레코드는 OCSPResponder 라는 이름으로 시작해야 합니다.

IssuerDN

필수입니다. 인증서 발급자의 DN 을 지정합니다. 이 값은 파일의 각 OCSP 응답자 레코드에 레이블을 지정합니다.

항목: 인증서의 발급자 DN 값입니다.

AlternateIssuerDN

선택 사항입니다. 보조 IssuerDN 또는 리버스 DN 을 지정합니다.

ResponderLocation

선택 사항입니다. OCSP 응답자 서버의 위치를 나타냅니다.

ResponderLocation 설정 또는 AIAExtension 설정을 사용할 수 있지만 다음 사항에 유의하십시오.

- ResponderLocation 설정이 비어 있거나 SMocsp.conf 파일에 없는 경우에는 AIAExtension 설정을 YES 로 설정하십시오. 또한 AIA 확장이 인증서에 있어야 합니다.
- ResponderLocation 설정에 값이 있고 AIAExtension 이 YES 로 설정된 경우 정책 서버는 유효성 검사에 ResponderLocation 을 사용합니다. ResponderLocation 설정은 AIAExtension 보다 우선 순위가 높습니다.
- 이 설정에 대해 지정된 OCSP 응답자가 중지되고 AIAExtension 이 YES 로 설정된 경우에는 인증이 실패합니다. 정책 서버는 인증서의 AIA 확장에 지정된 응답자를 시도하지 않습니다.

위치를 입력하는 경우 값을 *responder_server_url*:*port_number* 의 형식으로 입력하십시오.

응답자 서버의 URL 및 포트 번호를 입력하십시오.

AIAExtension

선택 사항입니다. 정책 서버가 유효성 검사 정보를 찾기 위해 인증서의 AIA(Authority Information Access) 확장을 사용하는지 여부를 지정합니다.

AIAExtension 또는 ResponderLocation 설정을 사용할 수 있지만 다음 조건을 참조하십시오.

- AIAExtension 이 YES 로 설정되고 ResponderLocation 이 구성되지 않은 경우 정책 서버는 인증서의 AIA 확장을 유효성 검사에 사용합니다. 확장은 인증서에 있어야 합니다.
- AIAExtension 이 YES 로 설정되고 ResponderLocation 설정에 값이 있는 경우 정책 서버는 ResponderLocation 을 유효성 검사에 사용합니다. ResponderLocation 설정은 AIAExtension 보다 우선 순위가 높습니다.
- AIAExtension 이 NO 로 설정된 경우 정책 서버는 ResponderLocation 설정을 사용합니다. AIAExtension 에 대한 값이 있으면 정책 서버는 이를 무시합니다.

YES 또는 NO 를 입력하십시오.

기본값: NO

HttpProxyEnabled

선택 사항입니다. OCSP 요청을 웹 서버가 아니라 프록시 서버로 전송하도록 정책 서버에 지시합니다.

YES 또는 NO 를 입력하십시오.

기본값: NO

HttpProxyLocation

선택 사항입니다. 프록시 서버의 URL 을 지정합니다. 이 값은 HttpProxyEnabled 가 YES 로 설정된 경우에만 필요합니다.

http://로 시작하는 URL 을 입력하십시오.

참고: https://로 시작하는 URL 을 입력하지 마십시오.

HttpProxyUserName

선택 사항입니다. 프록시 서버에 대한 로그인 자격 증명의 사용자 이름을 지정합니다. 이 사용자 이름은 유효한 프록시 서버 사용자의 이름이어야 합니다. 이 값은 HttpProxyEnabled 가 YES 로 설정된 경우에만 필요합니다.

영숫자 문자열을 입력하십시오.

HttpProxyPassword

선택 사항입니다. 프록시 서버 사용자 이름의 암호를 지정합니다. 이 값은 일반 텍스트로 표시됩니다. 이 값은 HttpProxyEnabled 가 YES 로 설정된 경우에만 필요합니다.

영숫자 문자열을 입력하십시오.

SignRequestEnabled

선택 사항입니다. 정책 서버에 생성된 OCSP 요청에 서명하도록 지시합니다. 서명 기능을 사용하려면 이 값을 Yes 로 설정하십시오.

이 값은 사용자 인증서 서명과 별개이며 OCSP 요청에만 사용됩니다.

참고: 이 설정은 OCSP 응답자가 서명된 요청을 요구하는 경우에만 필요합니다.

YES 또는 NO 를 입력하십시오.

기본값: NO

SignDigest

선택 사항입니다. 정책 서버가 OCSP 요청에 서명할 때 사용하는 알고리즘을 지정합니다. 이 설정은 대/소문자를 구분하지 않습니다. 이 설정은 SignRequestEnabled 설정을 YES 로 설정한 경우에만 필요합니다.

다음 옵션 중 하나를 입력하십시오. SHA1, SHA224, SHA256, SHA384, SHA512

기본값: SHA1

Alias

선택 사항입니다. OCSP 응답자에 전송되는 OCSP 요청에 서명하는 키/인증서 쌍의 별칭을 지정합니다. 이 키/인증서 쌍은 SiteMinder 인증서 데이터 저장소에 있어야 합니다.

참고: 별칭은 SignRequestEnabled 설정을 YES 로 설정한 경우에만 필요합니다.

소문자 ASCII 영숫자 문자를 사용하여 별칭을 입력하십시오.

IgnoreNonceExtension

선택 사항입니다. OCSP 요청에 nonce 를 포함하지 않도록 정책 서버에 지시합니다. nonce(한 번 사용되는 숫자)는 응답이 재사용되는 것을 방지하기 위해 인증 요청에 가끔 포함되는 고유한 숫자입니다. 이 매개변수를 Yes 로 설정하면 정책 서버는 OCSP 요청에 nonce 를 포함하지 *않습니다*.

YES 또는 NO 를 입력하십시오.

기본값: NO

PrimaryValidationMethod

선택 사항입니다. 정책 서버가 인증서의 유효성을 검사하기 위해 사용할 기본 방법을 OCSP 또는 CRL 중에서 지정합니다. 이 설정은 EnableFailover 설정을 Yes 로 설정한 경우에만 필요합니다.

OCSP 또는 CRL 을 입력하십시오.

기본값: OCSP

EnableFailover

OCSP 및 CRL 인증서 유효성 검사 방법 간에 장애 조치를 수행하도록 정책 서버에 지정합니다.

YES 또는 NO 를 입력하십시오.

기본값: NO

ResponderCertAlias

페더레이션에만 필요합니다. OCSP 응답의 서명을 확인하는 인증서의 별칭 이름을 지정합니다. 정책 서버가 응답 서명 유효성 검사를 수행하도록 하려면 이 설정에 대한 별칭을 지정하십시오. 그렇게 하지 않으면 CA 발급자가 사용할 수 있는 OCSP 구성이 없습니다.

참고: 정책 서버는 X.509 인증서 인증에 이 설정을 사용하지 않습니다.

별칭 이름을 지정하는 문자열을 입력하십시오.

SMocsp.conf 파일이 로드된 후 각 발급자에게 OCSP 구성이 있는지 여부를 확인할 수 있습니다. 다음은 샘플 상태 메시지입니다.

```
SMocsp.conf 파일이 로드되었습니다.
다음 발급자 별칭에 대해 OCSP 구성이 추가되었습니다:
ocspcacert
ocspcacert1
ocspcacert2
```

상태 메시지의 발급자 별칭은 데이터 저장소에 CA 인증서를 추가할 때 관리 UI 에서 지정한 별칭을 가리킵니다. 발급자 별칭이 목록에 없으면 SMocsp.conf 및 cds.log 파일을 확인하십시오. 로그 파일은 *siteminder_home*\log 에 있습니다.

RevocationGracePeriod

페더레이션의 경우에만 선택 사항입니다. 인증서가 해지된 후 인증서의 무효화를 지연할 기간(일)을 지정합니다. OCSP 유예 기간은 구성이 갑자기 중지되지 않도록 사용자에게 인증서를 업데이트할 시간을 부여합니다. 값이 0 이면 인증서가 해지될 때 즉시 무효화됩니다.

이 필드에 값을 지정하지 않으면 정책 서버는 관리 UI 의 기본 해지 유예 기간 설정을 사용합니다. "인프라" > "X509 인증서 관리" > "인증서 관리"로 이동하여 기본 설정을 확인할 수 있습니다.

기본값: 0

OCSP 가 사용되지 않도록 설정

SMocsp.conf 파일에서 발급자 항목을 제거하여 특정 CA 에 대한 OCSP 구성이 사용되지 않도록 설정할 수 있습니다. OCSPUpdater 가 사용되지 않도록 설정하려면 파일에서 이전에 사용되도록 설정한 모든 항목을 제거하십시오.

다음 단계를 수행하십시오.

1. SMocsp.conf 파일을 편집기에서 엽니다. SMocsp.conf 파일은 *siteminder_home*/config 디렉터리에 있습니다.
2. 연계된 발급자 항목을 SMocsp.conf 파일에서 삭제합니다.
3. smkeytool 유틸리티를 사용하여 다음 명령을 입력합니다.

   ```
   smkeytool -loadOCSPConfigFile
   ```

특정 CA 발급자에 대한 OCSP 가 사용되지 않도록 설정됩니다.

OCSP 가 사용되지 않도록 설정되었을 때 CA 인증서 추가

OCSPUpdater 가 사용되지 않도록 설정했지만 특정 발급자의 항목이 SMocsp.conf 파일에 있는 경우 정책 서버가 해당 발급자에 대한 인증서의 추가를 차단합니다. 인증서를 추가하려고 하면 정책 서버가 오류 메시지를 로깅합니다. OCSP 가 발급자에 대해 구성되었지만 OCSPUpdater 는 사용되도록 설정되지 않았기 때문에 오류가 발생합니다. 따라서 해지 상태 검사를 수행할 수 없습니다. 동일한 발급자를 사용하여 인증서를 추가하려고 하면 추가 작업이 실패합니다.

오류 없이 CA 인증서를 추가하려면

1. SMocsp.conf 파일을 편집기에서 엽니다. SMocsp.conf 파일은 *siteminder_home*/config 디렉터리에 있습니다.
2. 해당 CA 에 대한 구성을 제거합니다.
3. XPSConfig 를 사용하여 EnableOCSPUpdater 를 Yes 로 설정하여 OCSP 를 다시 사용되도록 설정합니다.
4. 명령줄에서 다음 명령을 입력하여 SMocsp.conf 파일을 로드합니다.

   ```
   smkeytool -loadOCSPConfigFile
   ```

5. EnableOCSPUpdater 매개 변수를 원래 의도한 대로 No 로 재설정합니다.

인증서 캐시 새로 고침 간격

인증서 캐시 새로 고침 간격은 인증서 데이터 저장소가 정책 저장소의 인증서 데이터를 업데이트하는 빈도를 가리킵니다. SiteMinder 성능 향상을 위해 인증서 데이터는 메모리에 캐시됩니다. 데이터가 최신 상태가 되도록 메모리의 정보를 새로 고치십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "X509 인증서 관리", "CDS 설정"을 선택합니다.
3. 인증서 캐시 새로 고침 간격에 대한 새 값을 초 단위로 입력합니다. 기본값은 300 초입니다.
4. "저장"을 클릭합니다.

새로 고침 간격이 구성됩니다.

기본 해지 유예 기간

기본 해지 유예 기간은 인증서가 해지되는 시점부터 인증서가 무효화되는 시점까지의 지연 시간(일)입니다. 유예 기간 동안 SiteMinder 는 해지된 인증서를 무효화되기 전까지 사용할 수 있습니다. 인증서가 무효화된 후에는 더 이상 활성화 상태가 아니며 SiteMinder 에서 이를 사용할 수 없습니다.

이 기본 유예 기간은 CRL 및 OCSP 응답자에 적용됩니다. CRL 을 시스템에 추가할 때 CRL 유예 기간에 대한 값을 지정하지 않으면 SiteMinder 는 기본 유예 기간을 사용합니다. SMocsp.conf 파일에 OCSP 유예 기간을 구성하지 않으면 SiteMinder 는 기본 유예 기간을 사용합니다. CRL 또는 OCSP 에 대한 개별 유예 기간 설정이 이 기본 유예 기간 값보다 높은 우선 순위를 가집니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "X509 인증서 관리", "CDS 설정"을 선택합니다.

3. 해지 유예 기간에 대한 새 값을 일 단위로 입력합니다. 기본값은 0 이며, 이는 인증서가 해지되면 바로 무효화됨을 의미합니다.
4. "저장"을 클릭합니다.

해지 유예 기간이 정의됩니다.

제 6 장: 정책 서버 슈퍼 사용자 암호 변경

이 섹션은 다음 항목을 포함하고 있습니다.

슈퍼 사용자 암호 개요

슈퍼 사용자는 정책 서버 설치 프로세스에 의해 자동으로 설정되는 정책 서버 관리자 계정입니다. 관리 콘솔의 "슈퍼 사용자" 탭에서 슈퍼 사용자 암호를 변경할 수 있습니다.

참고: 이전에 관리 UI 에서 슈퍼 사용자가 사용되지 않도록 설정한 경우 이 대화 상자에서 슈퍼 사용자 계정 암호를 변경해도 슈퍼 사용자가 다시 사용되도록 설정되지는 않습니다.

정책 서버 슈퍼 사용자 암호 변경

정책 서버 슈퍼 사용자 암호를 변경하려면

1. 정책 서버 관리 콘솔을 시작합니다.

   중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "슈퍼 사용자" 탭을 클릭합니다.

   참고: 이 탭의 설정과 컨트롤에 대한 자세한 내용을 보려면 "도움말", "관리 콘솔 도움말"을 차례로 클릭하십시오.

3. "이전 암호" 필드에 슈퍼 사용자의 현재 암호를 입력합니다.

4. "새 암호" 필드에 슈퍼 사용자의 새 암호를 입력합니다.

   참고: SiteMinder 슈퍼 사용자 관리자의 암호에는 파이프(|), 보다 큼(>) 또는 보다 작음(<) 문자를 포함할 수 없습니다.

5. "암호 확인" 필드에 새 암호를 다시 입력하여 확인합니다.

6. "적용"을 클릭하여 슈퍼 사용자 변경 내용을 저장하거나, "확인"을 클릭하여 설정을 저장하고 콘솔을 닫습니다.

   참고: 슈퍼 사용자 계정 암호에 대한 변경 내용은 정책 서버 프로세스를 다시 시작하지 않아도 적용됩니다.

제 7 장: 정책 서버 로깅 구성

이 섹션은 다음 항목을 포함하고 있습니다.

정책 서버 로깅 개요

정책 서버 로그 파일에는 정책 서버의 상태에 대한 정보가 기록되며, 필요할 경우 인증, 권한 부여 및 기타 이벤트에 대한 구성 가능한 수준의 감사 정보도 정책 서버 로그 파일에 기록됩니다. 정책 서버가 RADIUS 서버로 구성된 경우 RADIUS 작업은 RADIUS 로그 파일에 로깅됩니다.

이러한 로그는 관리 콘솔의 "로그" 탭에서 구성할 수 있습니다.

정책 서버 로그 구성

정책 서버 로그를 구성하려면

1. 정책 서버 관리 콘솔을 시작합니다.

   중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "로그" 탭을 클릭합니다.

   참고: 이 탭의 설정과 컨트롤에 대한 자세한 내용을 보려면 "도움말", "관리 콘솔 도움말"을 차례로 클릭하십시오.

3. "정책 서버 로그" 및 "정책 서버 감사 로그" 그룹 상자에 있는 설정을 조정하여 정책 서버 로그의 위치, 롤오버 특성 및 필요한 감사 로깅 수준을 구성합니다.
4. 정책 서버가 RADIUS 서버로 구성된 경우 "RADIUS 로그" 그룹 상자에 있는 설정을 조정합니다.
5. "적용"을 클릭하여 변경 내용을 저장합니다.

정책 저장소 개체에 대한 관리자 변경 내용 기록

기본적으로 정책 저장소 개체에 대한 SiteMinder 관리자 변경 내용은 *siteminder_home*\audit 에 있는 여러 개의 XPS 텍스트 파일에 기록됩니다.

감사 로그는 다음 예에서처럼 텍스트 파일로 저장됩니다.

policy_server_home/audit/xps-*process_id-start_time-audit_sequence.file_type*

각 감사 로그 파일의 이름에는 다음 정보가 포함됩니다.

process_id

감사된 이벤트와 관련된 프로세스의 번호를 나타냅니다.

start_time

트랜잭션이 *시작된* 시간을 다음 형식으로 나타냅니다.

YYYYMMDDHHMMSS

4 자리 연도와 24 시간제가 사용됩니다.

예: 20061204133000

audit_sequence

감사된 이벤트의 시퀀스 번호를 제공합니다.

file_type

다음 이벤트 유형 중 하나를 나타냅니다.

access

다음과 같은 액세스 이벤트가 포함된 감사 로그 파일을 나타냅니다.

- 관리 UI 또는 보고서 서버가 등록됨
- 관리 UI 또는 보고서 서버가 다른 사용자를 대신하여 프록시 역할을 함
- 관리자에게 요청된 작업에 대한 액세스가 거부됨

audit

다음과 같은 이벤트가 포함된 감사 로그 파일을 나타냅니다.

- 개체가 수정됨(XPS 도구 또는 관리 UI 사용)
- 관리자 레코드가 생성, 수정 또는 삭제됨

txn

다음과 같은 트랜잭션 이벤트가 포함된 감사 로그 파일을 나타냅니다.

- XPS 도구가 개체에 대한 변경을 시작, 커밋 또는 거부함

참고: 사용자에게 SiteMinder 바이너리 파일(XPS.dll, libXPS.so, libXPS.sl)에 대한 쓰기 액세스 권한이 *없다면* 관리자가 관리 UI 또는 XPSSecurity 도구를 사용하여 관련 XPS 명령줄 도구를 사용할 수 있는 권한을 사용자에게 부여해야 합니다.

기본 설정을 변경하려면

1. 정책 서버 호스트 시스템에 액세스합니다.

2. 명령줄을 열고 다음 명령을 입력합니다.

   ```
   xpsconfig
   ```

   이 도구가 시작되어 이 세션에 대한 로그 파일 이름이 표시되고 선택 메뉴가 열립니다.

3. 다음을 입력합니다.

   ```
   xps
   ```

   옵션 목록이 나타납니다.

4. 다음을 입력합니다.

   ```
   1
   ```

   현재 정책 저장소 감사 설정이 표시됩니다.

5. C 를 입력합니다.

   참고: 이 매개 변수는 TRUE 또는 FALSE 값을 사용합니다. 값을 변경하면 두 상태 간에 전환됩니다.

   업데이트된 정책 저장소 감사 설정이 표시됩니다. 새 값은 목록 맨 아래에 "pending value"(보류 중인 값)로 표시됩니다.

6. 다음 작업을 수행하십시오.

   a. Q 를 두 번 입력합니다.

   b. Q 를 입력하여 XPS 세션을 종료합니다.

   변경 내용이 저장되고 명령 프롬프트가 표시됩니다.

오래된 로그 파일을 자동으로 처리하는 방법

다음 스크립트 중 하나를 사용자 지정하여 SiteMinder 정책 서버에서 오래된 로그 파일이 자동으로 처리되도록 구성할 수 있습니다.

- Harvest.bat(Windows)
- Harvest.sh(UNIX 또는 Linux)

이러한 스크립트는 다음 이벤트 중 하나가 발생할 때 실행됩니다.

- 다음 옵션을 사용하여 XPSAudit 프로세스가 시작될 때

  CLEANUP

  디렉터리의 모든 로그 파일을 한 번에 처리합니다.

- 로그 파일이 롤오버될 때마다
- XPSAudit 프로세스가 종료될 때

  롤오버 또는 종료 중에는 로그 파일이 파일 이름별로 한 번에 하나씩 처리됩니다.

스크립트를 사용자 지정하여 원하는 방법으로 파일을 처리할 수 있습니다. 예를 들어 파일을 삭제하거나, 데이터베이스로 이동하거나, 다른 위치에 보관하도록 스크립트를 수정할 수 있습니다.

참고: 이 스크립트는 예제로만 제공됩니다. CA 에서는 지원되지 않습니다.

오래된 로그 파일을 자동으로 처리하려면 다음을 수행하십시오.

1. 정책 서버에서 다음 디렉터리를 엽니다.

   policy_server_home/audit/samples

2. 텍스트 편집기를 사용하여 운영 체제에 해당하는 스크립트를 열고 다음 디렉터리에 복사본을 저장합니다.

   policy_server_home/audit/Harvest.*extension*

   참고: 파일 이름을 바꾸거나 지정된 것과 다른 위치에 저장하지 *마십시오*.

3. 스크립트의 주석을 참조하여 필요에 따라 스크립트를 사용자 지정합니다.
4. 사용자 지정한 스크립트를 저장하고 텍스트 편집기를 닫습니다.

보고서에 SiteMinder 관리 감사 이벤트를 포함하는 방법

SiteMinder 보고서 서버와 감사 데이터베이스가 있는 경우 정책 서버에서 관리 감사 이벤트를 수집하도록 구성할 수 있습니다. 이 데이터를 감사 데이터베이스로 가져오면 생성하는 보고서에 이 데이터를 포함시킬 수 있습니다.

필요에 맞게 사용자 지정할 수 있는 샘플 Perl 스크립트가 SiteMinder 정책 서버와 함께 설치되어 있습니다.

SiteMinder 보고서에 관리 감사 이벤트를 포함하려면 다음 과정을 따르십시오.

1. 다음 작업을 수행하여 정책 서버의 샘플 스크립트를 복사합니다.
   a. 다음 디렉터리를 엽니다.

      policy_server_home\audit\samples

      참고: 다음 디렉터리가 *policy_server_home* 변수의 기본 위치입니다.

      - C:\Program Files\ca\siteminder(Windows)
      - /opt/ca/siteminder(UNIX, Linux)

   b. 다음 파일을 찾습니다.

      - Harvest.bat(Windows 의 경우)
      - Harvest.sh(UNIX 또는 Linux 의 경우)
      - ProcessAudit.pl
      - Categories.txt

   c. 앞의 파일을 다음 디렉터리에 복사합니다.

      policy_server_home\audit
2. (선택 사항) ProcessAudit.pl 스크립트를 사용자 지정합니다.

3. 다음에 예약된 XPSAudit 명령이 실행되고 나면 감사 로그의 복사본이 CSV(쉼표로 구분된 값) 형식으로 생성되어 다음 디렉터리에 .TMP 파일로 저장됩니다.

   policy_server_home\audit_R6tmp

   참고: 수동으로 .tmp 파일로 생성할 이벤트가 있는 경우에는 policy_server_home\audit 디렉터리에서 다음 명령을 실행하십시오.

   ```
   ProcessAudit.pl <Transaction id>
   ```

   smobjlog4 데이터베이스 테이블에 다음 11 개의 특성 및 값이 표시됩니다. .TMP 파일에는 처음 8 개만 생성됩니다.

   ```
   sm_timestamp        DATE DEFAULT SYSDATE NOT NULL,
   sm_categoryid       INTEGER DEFAULT 0 NOT NULL,
   sm_eventid          INTEGER DEFAULT 0 NOT NULL,
   sm_hostname         VARCHAR2(255) NULL,
   sm_sessionid        VARCHAR2(255) NULL,
   sm_username         VARCHAR2(512) NULL,
   sm_objname          VARCHAR2(512) NULL,
   sm_objoid           VARCHAR2(64) NULL,
   sm_fielddesc        VARCHAR2(1024) NULL,
   sm_domainoid        VARCHAR2(64) NULL,
   sm_status           VARCHAR2(1024) NULL
   ```

4. 정책 서버의 이전 디렉터리에 있는 .TMP 파일을 감사 데이터베이스를 호스트하는 서버로 복사합니다.

5. 다음 파일 중 하나를 생성하여 .TMP 파일의 CSV 형식 내용을 데이터베이스 스키마에 매핑합니다.

   - *control_file_name*.ctl(Oracle 데이터베이스용 제어 파일)
   - *format_file_name*.fmt(SQL Server 데이터베이스용 형식 파일)

   참고: 자세한 내용은 데이터베이스 공급업체에서 제공하는 설명서 또는 온라인 도움말을 참조하십시오.

6. 감사 데이터베이스를 호스트하는 서버에서 다음 중 데이터베이스 유형에 적절한 명령을 실행합니다.

   - sqlldr(Oracle 데이터베이스의 경우)
   - bcp(SQL Server 데이터베이스의 경우)

   참고: 자세한 내용은 데이터베이스 공급업체에서 제공하는 설명서 또는 온라인 도움말을 참조하십시오.

7. 명령이 완료된 후 보고서 서버를 사용하여 관리 이벤트의 보고서를 생성합니다.

   관리 감사 이벤트가 보고서에 표시됩니다.

Windows 에서 텍스트 기반 감사 로그에 ODBC 감사 로그 내용 미러

SiteMinder 감사 로그를 텍스트 파일로 저장하면 기본적으로 사용할 수 있는 필드 중 일부만 포함됩니다. ODBC 감사 데이터베이스처럼 감사 로그가 포함된 텍스트 파일에 사용할 수 있는 필드를 모두 넣으려면 레지스트리 키를 정책 서버에 추가할 수 있습니다.

텍스트 기반 감사 로그에 ODBC 감사 로그 내용을 미러하려면

1. 레지스트리 편집기를 엽니다.
2. 다음 위치를 확장합니다.

   `HKEY_LOCAL_MACHINE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Reports\`
3. 다음과 같은 이름으로 새 DWORD 값을 생성합니다.

   `Enable Enhance Tracing`
4. 값을 1 로 설정합니다. 나중에 이 설정이 사용되지 않도록 설정하려면 값을 다시 0 으로 변경하십시오.
5. 정책 서버를 다시 시작합니다.

   ODBC 감사 로그 내용이 텍스트 기반 감사 로그에 표시됩니다.

Solaris 에서 텍스트 기반 감사 로그에 ODBC 감사 로그 내용 미러

SiteMinder 감사 로그를 텍스트 파일로 저장하면 기본적으로 사용할 수 있는 필드 중 일부만 포함됩니다. ODBC 감사 데이터베이스처럼 감사 로그가 포함된 텍스트 파일에 사용할 수 있는 필드를 모두 넣으려면 레지스트리 키를 정책 서버에 추가할 수 있습니다.

텍스트 기반 감사 로그에 ODBC 감사 로그 내용을 미러하려면

1. 다음 파일을 엽니다.

   ```
   sm.registry
   ```

2. 다음 행을 찾습니다.

   ```
   -
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\R
   eports=25089
   ```

3. 이 행 아래에 다음 텍스트를 포함하는 새 행을 추가합니다.

   ```
   - Enable Enhance Tracing= 0x1; REG_DWORD
   ```

   참고: 나중에 이 기능이 사용되지 않도록 설정하려면 0x1 을 0x0 으로 변경하십시오.

4. 정책 서버를 다시 시작합니다.

   ODBC 감사 로그 내용이 텍스트 기반 감사 로그에 표시됩니다.

시스템 로그에 로깅 문제 보고

정책 서버에서 감사 로그를 준비하거나 실행하는 동안 발생할 수 있는 예외에 대한 정보가 Windows 이벤트 로그 뷰어에 로깅되도록 구성할 수 있습니다. 이렇게 구성하면 디버그 로그가 사용되지 않도록 설정된 프로덕션 환경에서 이 정보가 손실되지 않도록 할 수 있습니다. 이 기능을 구성하려면 CategoryCount 레지스트리 키의 값을 7 로 설정하십시오.

CategoryCount 레지스트리 키는 다음 레지스트리 위치에 있습니다.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application
\SiteMinder
```

이러한 이벤트는 이벤트 로그 범주 ObjAuditLog 및 AccessAuditLog 아래에 로깅됩니다.

SiteMinder 는 개체가 생성, 업데이트 또는 삭제될 때 개체 이벤트를 호출합니다. SiteMinder 개체 감사 로그를 준비/실행하는 중에 발생하는 예외는 Windows 이벤트 뷰어의 'ObjAuditLog' 범주 아래에 로깅됩니다.

액세스 이벤트는 사용자 관련 작업으로 인해 발생하며 인증, 권한 부여, 관리 및 가맹 작업의 컨텍스트에서 호출됩니다. SiteMinder 액세스 감사 로그를 준비/실행하는 중에 발생하는 예외는 Windows 이벤트 뷰어의 'AccessAuditLog' 범주 아래에 로깅됩니다.

인증서 데이터 저장소 로깅 구성

기본 설정을 변경하려면 인증서 데이터 저장소 로그를 구성하십시오. 기본적으로 로그는 다음과 같은 형태로 구성됩니다.

- 다음 파일에 정보를 로깅합니다.

  cds.log

  이 로그는 *siteminder_home*\log 에 있습니다.

  siteminder_home

  정책 서버 설치 경로를 지정합니다.
- 정보 및 오류 메시지를 포함합니다.
- 파일 크기가 500 KB 에 도달하면 롤오버하여 백업을 생성합니다.
- 10 개의 백업 사본이 생성되면 가장 오래된 사본을 삭제합니다.

다음 단계를 수행하십시오.

1. *siteminder_home*\config\properties 로 이동하고 다음 파일을 엽니다.

   cdslog4j.properties

   참고: log4j 에 대한 자세한 내용은 Apache 웹 사이트를 참조하십시오.
2. 다음 중 하나 이상을 수행합니다.
   - 로깅 수준을 변경하려면 다음 매개 변수 맨 뒤의 값을 업데이트합니다.

     `log4j.logger.com.ca.CertificateDataStore=`

     중요! 매개 변수에서 다음을 제거하지 마십시오. 그러지 않으면 로깅에 실패합니다.

     `, CertificateDataStore`

- 출력 위치나 로그 이름을 변경하려면 다음 매개 변수 맨 뒤의 파일 경로를 업데이트하십시오.

  ```
  log4j.appender.CertificateDataStore.File=
  ```

- 파일이 순환되고 백업이 생성되는 크기를 변경하려면 다음 매개 변수 맨 뒤의 값을 업데이트하십시오.

  ```
  log4j.appender.CertificateDataStore.MaxFileSize=
  ```

- 가장 오래된 백업 사본을 삭제할 때까지 유지되는 백업 사본 수를 변경하려면 다음 매개 변수 맨 뒤의 값을 업데이트하십시오.

  ```
  log4j.appender.CertificateDataStore.MaxBackupIndex=
  ```

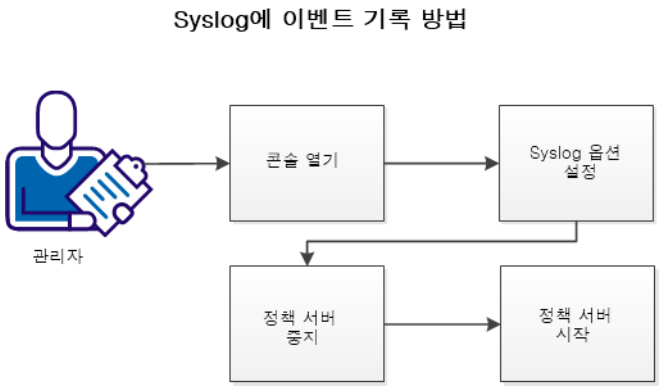
참고: SiteMinder 지원에서 요청하는 경우 외에는 ClientDispatcher 섹션의 설정을 수정하지 마십시오. 이 설정은 디버깅 전용입니다.

3. 파일을 저장합니다.

   인증서 데이터 저장소 로깅이 구성됩니다.

Syslog 에 이벤트를 기록하는 방법

관리자는 지원되는 운영 환경의 syslog 에 정책 서버 이벤트를 기록할 수 있습니다. 다음 그림에서는 syslog 에 이벤트를 기록하는 방법을 설명합니다.



다음 단계를 수행하십시오.

1. 콘솔을 엽니다 (페이지 96).
2. syslog 옵션을 설정합니다 (페이지 97).
3. 다음 단계를 수행하여 정책 서버를 다시 시작합니다.
   - 정책 서버를 중지합니다 (페이지 99).
   - 정책 서버를 시작합니다 (페이지 100).

콘솔 열기

설정을 변경하려면 콘솔을 여십시오.

다음 단계를 수행하십시오.

1. 시스템에서 X-windows 서버가 실행 중인지 확인합니다.
2. 터미널 창을 엽니다.
3. 다음 명령을 사용하여 DISPLAY 변수를 설정합니다.

   ```
   export DISPLAY=IP_address:0.0
   ```

   IP_address

   콘솔 창이 표시되는 위치의 IP 주소를 지정합니다. 콘솔에 *연결할* 시스템의 IP 주소를 사용합니다.

   예: (IPV4) 192.168.1.1

   예: (IPV6) 2001:DB8::/32
4. 콘솔을 호스트하는 시스템에 로그인합니다.
5. 다음 디렉터리로 이동합니다.

   ```
   installation_directory/siteminder/bin
   ```

   installation_directory

   정책 서버가 설치된 파일 시스템의 위치를 지정합니다.

   기본값: /opt/CA/siteminder
6. 다음 명령을 실행하여 콘솔을 엽니다.

   ```
   ./smconsole
   ```

Syslog 옵션 설정

콘솔의 syslog 옵션을 설정하여 syslog 에 기록할 이벤트를 지정할 수 있습니다.

참고: Syslog 및 해당 설정에 대한 자세한 내용은 이 웹 사이트를 참조하십시오.

다음 단계를 수행하십시오.

1. 다음 단계를 수행하여 syslog 기록을 사용하도록 설정합니다.
   a. "데이터" 탭을 클릭합니다.
   b. "데이터베이스" 드롭다운 목록을 클릭하고 "감사 로그"를 선택합니다.
   c. "저장소" 드롭다운 목록을 클릭하고 "Syslog"를 선택합니다.
2. "우선 순위" 필드에서 텍스트를 선택하고 다음 목록에서 원하는 값을 입력합니다.

   우선 순위

   syslog 에 기록되는 이벤트의 우선 순위를 지정합니다. 다음 값 중 *하나*를 선택하십시오.

   - LOG_EMERG
   - LOG_ALERT
   - LOG_CRIT
   - LOG_ERR
   - LOG_WARNING
   - LOG_NOTICE
   - LOG_INFO
   - LOG_DEBUG

   기본값: LOG_INFO

3. "기능" 필드에서 텍스트를 선택하고 다음 목록에서 원하는 값을 입력합니다.

   기능

   syslog 에 기록할 운영 환경의 이벤트를 지정합니다. 다음 값 중 *하나*를 선택하십시오.

   - LOG_AUTH
   - LOG_AUTHPRI
   - LOG_CRON
   - LOG_DAEMON
   - LOG_FTP
   - LOG_KERN
   - LOG_LPR
   - LOG_MAIL
   - LOG_NEWS
   - LOG_SYSLOG
   - LOG_USER
   - LOG_UUCP
   - LOG_LOCAL0
   - LOG_LOCAL1
   - LOG_LOCAL2
   - LOG_LOCAL3
   - LOG_LOCAL4
   - LOG_LOCAL5
   - LOG_LOCAL6
   - LOG_LOCAL7

   기본값: LOG_AUTH

4. (선택 사항) 다음 필드의 텍스트를 바꿉니다.

   텍스트

   syslog 에 기록할 이벤트의 텍스트를 지정합니다. 예를 들어 tiger 라는 단어를 지정할 경우 tiger 라는 단어가 포함된 모든 이벤트가 syslog 에 기록됩니다.

   기본값: Siteminder

5. "확인"을 클릭합니다.

   콘솔이 닫히고 syslog 옵션이 설정됩니다.

UNIX 정책 서버 중지

정책 서버를 중지하면 다음과 같은 결과가 발생합니다.

- 정책 서버가 사용 환경에서 일시적으로 제거됩니다.
- 권한 부여 또는 인증 결정이 필요한 에이전트가 중지된 정책 서버에 연결할 수 없게 됩니다. 이러한 에이전트는 사용 가능한 다른 정책 서버에 여전히 연결할 수 있습니다.
- 모든 로깅 작업이 중지됩니다.

다음 단계를 수행하십시오.

1. 정책 서버를 원래 설치한 사용자 계정으로 정책 서버를 호스트하는 시스템에 로그인합니다.
2. 다음 작업 중 *하나*를 수행하여 모든 정책 서버 프로세스를 중지합니다.
   - 관리 콘솔을 열고 "상태" 탭을 클릭한 다음 "중지" 단추를 클릭합니다.
   - 다음 스크립트를 사용합니다. 이 스크립트는 UNIX 감독 기능도 중지하므로 프로세스가 자동으로 다시 시작되지 않습니다.

     ```
     installation_path/siteminder/stop-all
     ```

     정책 서버는 모든 UNIX 감독 기능 작업을 installation_directory/log/smexec.log 파일에 로깅합니다. 로그 항목은 항상 기존 로그 파일에 추가됩니다.

UNIX 정책 서버 시작

정책 서버를 시작하면 다음과 같은 결과가 발생합니다.

- 에이전트는 권한 부여 또는 인증 결정을 위해 정책 서버에 연결합니다.
- 로깅이 시작됩니다.

다음 작업 중 *하나*를 수행하여 모든 정책 서버 프로세스를 시작합니다.

- 관리 콘솔을 열고 "상태" 탭을 클릭한 다음 "시작" 단추를 클릭합니다.
- 다음 스크립트를 사용합니다. 이 스크립트는 UNIX 감독 기능도 시작합니다.

  ```
  installation_path/siteminder/start-all
  ```

  정책 서버는 모든 UNIX 감독 기능 작업을 installation_directory/log/smexec.log 파일에 로깅합니다. 로그 항목은 항상 기존 로그 파일에 추가됩니다.

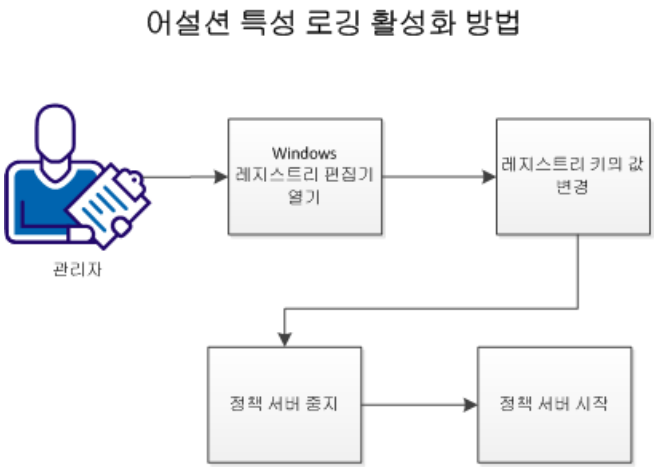
Windows 운영 환경에서 어설션 특성 로깅이 사용되도록 설정하는 방법

감사 로그에 어설션 특성에 대한 정보를 기록할 수 있습니다. 이러한 로그는 보안 감사에 사용하거나 조사 과정에서 사용하십시오. 이벤트 유형에 따라 로그에 기록되는 정보가 달라집니다. 어설션 특성을 로깅하도록 설정한 경우 다음 이벤트가 기록됩니다.

- 모든 어설션 생성
- 모든 어설션 소비
- 모든 인증 성공
- 모든 인증 실패
- 모든 인증 시도
- 모든 응용 프로그램 액세스

기본적으로는 어설션 특성이 로깅되지 않도록 설정됩니다. 정책 서버에서 어설션 특성을 로깅하도록 설정하십시오.

다음 그림에서는 어설션 특성 로깅이 사용되도록 설정하는 방법을 보여 줍니다.



다음 단계를 수행하십시오.

1. Windows 레지스트리 편집기를 엽니다 (페이지 101).
2. 레지스트리 키의 값을 변경합니다.
3. 다음 단계를 수행하여 정책 서버를 다시 시작합니다.
   a. 정책 서버를 중지합니다 (페이지 103).
   b. 정책 서버를 시작합니다 (페이지 103).

Windows 레지스트리 편집기 열기

정책 서버를 호스트하는 시스템에서 Windows 레지스트리 편집기를 열어 이 설정을 변경하십시오.

다음 단계를 수행하십시오.

1. "시작", "실행"을 차례로 클릭합니다.
2. "열기:" 필드에 다음 텍스트를 입력합니다.

   ```
   regedit
   ```

3. "확인"을 클릭합니다.

   Windows 레지스트리 편집기가 열립니다.

레지스트리 키 값 변경

다음 레지스트리 키는 특성 어설션 로깅을 제어합니다.

Enable Enhance Tracing

특성 어설션이 감사 로그에 기록되는지 여부를 나타냅니다. 값 2 는 로깅을 사용하도록 설정합니다. 값 3 은 로깅을 사용하도록 설정하고 사용자의 인증 방법을 기록합니다. 값 4 는 DeviceDNA™를 사용한 고급 세션 보증에 대해 로깅을 사용하도록 설정합니다.

제한: 0, 2, 3, 4

기본값: 0(로깅 사용 안 함)

다음 단계를 수행하십시오.

1. 레지스트리 편집기에서 다음 항목을 확장합니다.

   HKEY_LOCAL_MACHINE

2. "Software", "Netegrity", "SiteMinder", "Currentversion", "Reports"를 차례로 클릭합니다.
3. 다음 레지스트리 키를 찾습니다.

   Enable Enhance Tracing

4. 이 키를 마우스 오른쪽 단추로 클릭하고 "수정"을 선택합니다.
5. 다음 태스크 중 *하나*를 수행합니다.
   - 어설션 특성을 로깅하도록 설정하려면 값을 2 로 변경합니다.
   - 어설션 특성과 사용되는 인증 방법을 로깅하도록 설정하려면 값을 3 으로 변경합니다.
   - DeviceDNA™를 사용한 고급 세션 보증에 대한 로깅을 사용하도록 설정하려면 값을 4 로 변경합니다.
   - 어설션 특성을 로깅하지 않도록 설정하려면 값을 0 으로 변경합니다.
6. "확인"을 클릭합니다.
7. 레지스트리 편집기를 닫습니다.

"Enable Enhance Tracing" 레지스트리 값이 변경되었습니다.

Windows 정책 서버 중지

계속하기 전에 정책 서버를 중지하십시오. 정책 서버를 중지하면 다음과 같은 결과가 발생합니다.

- 정책 서버가 사용 환경에서 일시적으로 제거됩니다.
- 권한 부여 또는 인증 결정이 필요한 에이전트가 중지된 정책 서버에 연결할 수 없게 됩니다. 이러한 에이전트는 사용 가능한 다른 정책 서버에 여전히 연결할 수 있습니다.
- 모든 로깅 작업이 중지됩니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.

   참고: 관리자 권한이 있는 계정을 사용하십시오.

2. "시작", "프로그램", "SiteMinder", "SiteMinder 정책 서버 관리 콘솔"을 차례로 클릭합니다.
3. "중지" 단추를 클릭합니다.
4. "확인"을 클릭합니다.

   정책 서버가 중지되고 콘솔이 닫힙니다.

Windows 정책 서버 시작

정책 서버를 시작합니다. 정책 서버를 시작하면 다음과 같은 결과가 발생합니다.

- 에이전트는 권한 부여 또는 인증 결정을 위해 정책 서버에 연결합니다.
- 로깅이 시작됩니다.

다음 단계를 수행하십시오.

1. "시작", "프로그램", "SiteMinder", "SiteMinder 정책 서버 관리 콘솔"을 차례로 클릭합니다.

   "상태" 탭이 선택된 상태로 콘솔이 열립니다.

2. "시작" 단추를 클릭합니다.
3. "확인"을 클릭합니다.

   정책 서버가 시작됩니다.

UNIX 또는 Linux 운영 환경에서 어설션 특성을 로깅하도록 설정하는 방법

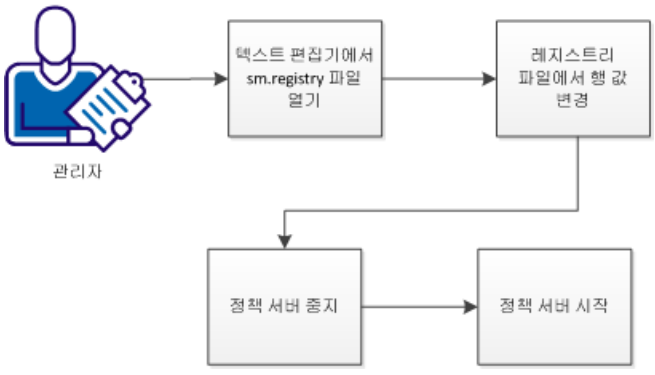
감사 로그에 어설션 특성에 대한 정보를 기록할 수 있습니다. 이러한 로그는 보안 감사에 사용하거나 조사 과정에서 사용하십시오. 이벤트 유형에 따라 로그에 기록되는 정보가 달라집니다. 어설션 특성을 로깅하도록 설정한 경우 다음 이벤트가 기록됩니다.

- 모든 어설션 생성
- 모든 어설션 소비
- 모든 인증 성공
- 모든 인증 실패
- 모든 인증 시도
- 모든 응용 프로그램 액세스

기본적으로는 어설션 특성이 로깅되지 않도록 설정됩니다. 정책 서버에서 어설션 특성을 로깅하도록 설정하십시오.

다음 그림에서는 어설션 특성 로깅이 사용되도록 설정하는 방법을 보여 줍니다.

어설션 특성 로깅 활성화



다음 단계를 수행하십시오.

1. 텍스트 편집기에서 sm.registry 파일을 엽니다 (페이지 105).
2. 레지스트리 파일의 행 값을 변경합니다.
3. 다음 단계를 수행하여 정책 서버를 다시 시작합니다.
   a. 정책 서버를 중지합니다 (페이지 99).
   b. 정책 서버를 시작합니다. (페이지 100)

텍스트 편집기에서 sm.registry 파일 열기

UNIX 또는 Linux 운영 환경의 경우 텍스트 편집기에서 sm.registry 파일을 열어 이 설정을 변경하십시오. sm.registry 파일은 정책 서버에 저장되어 있습니다.

다음 단계를 수행하십시오.

1. 다음 디렉터리로 이동합니다.

   Installation_Directory/registry

   installation_directory

   정책 서버가 설치된 파일 시스템의 위치를 지정합니다.

   기본값: /opt/CA/siteminder

2. 텍스트 편집기에서 다음 파일을 엽니다.

   sm.registry

   이제 설정을 변경할 수 있습니다.

레지스트리 파일의 행 값 변경

sm.registry 파일의 다음 항목은 특성 어설션 로깅을 제어합니다.

Enable Enhance Tracing

특성 어설션이 감사 로그에 기록되는지 여부를 나타냅니다. 값 2 는 로깅을 사용하도록 설정합니다. 값 3 은 로깅을 사용하도록 설정하고 사용자의 인증 방법을 기록합니다. 값 4 는 DeviceDNA™를 사용한 고급 세션 보증에 대해 로깅을 사용하도록 설정합니다.

제한: 0, 2, 3, 4

기본값: 0(로깅 사용 안 함)

다음 단계를 수행하십시오.

1. sm.registry 파일에서 다음 섹션을 찾습니다.

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Reports=
   ```

2. "Reports" 섹션에서 다음 행을 찾습니다.

   ```
   Enable Enhance Tracing=      0; REG_DWORD
   ```

3. 0 을 다음 값 중 *하나*로 변경합니다.
   - 2(로깅 사용)
   - 3(로깅 사용 및 인증 방법 기록)
   - 4(DeviceDNA™를 사용한 고급 세션 보증에 대한 로깅 사용)

4. sm.registry 파일의 이 행이 다음 예 중 *하나*와 일치하는지 확인합니다.

   ```
   Enable Enhance Tracing=      2; REG_DWORD
   Enable Enhance Tracing=      3; REG_DWORD
   Enable Enhance Tracing=      4; REG_DWORD
   ```

5. sm.registry 파일에 변경 내용을 저장하고 텍스트 편집기를 닫습니다.

   레지스트리 파일의 행 값이 변경되었습니다.

UNIX 정책 서버 중지

정책 서버를 중지하면 다음과 같은 결과가 발생합니다.

- 정책 서버가 사용 환경에서 일시적으로 제거됩니다.
- 권한 부여 또는 인증 결정이 필요한 에이전트가 중지된 정책 서버에 연결할 수 없게 됩니다. 이러한 에이전트는 사용 가능한 다른 정책 서버에 여전히 연결할 수 있습니다.
- 모든 로깅 작업이 중지됩니다.

다음 단계를 수행하십시오.

1. 정책 서버를 원래 설치한 사용자 계정으로 정책 서버를 호스트하는 시스템에 로그인합니다.
2. 다음 작업 중 *하나*를 수행하여 모든 정책 서버 프로세스를 중지합니다.
   - 관리 콘솔을 열고 "상태" 탭을 클릭한 다음 "중지" 단추를 클릭합니다.
   - 다음 스크립트를 사용합니다. 이 스크립트는 UNIX 감독 기능도 중지하므로 프로세스가 자동으로 다시 시작되지 않습니다.

     ```
     installation_path/siteminder/stop-all
     ```

     정책 서버는 모든 UNIX 감독 기능 작업을 installation_directory/log/smexec.log 파일에 로깅합니다. 로그 항목은 항상 기존 로그 파일에 추가됩니다.

UNIX 정책 서버 시작

정책 서버를 시작하면 다음과 같은 결과가 발생합니다.

- 에이전트는 권한 부여 또는 인증 결정을 위해 정책 서버에 연결합니다.
- 로깅이 시작됩니다.

다음 작업 중 *하나*를 수행하여 모든 정책 서버 프로세스를 시작합니다.

- 관리 콘솔을 열고 "상태" 탭을 클릭한 다음 "시작" 단추를 클릭합니다.
- 다음 스크립트를 사용합니다. 이 스크립트는 UNIX 감독 기능도 시작합니다.

  ```
  installation_path/siteminder/start-all
  ```

  정책 서버는 모든 UNIX 감독 기능 작업을 installation_directory/log/smexec.log 파일에 로깅합니다. 로그 항목은 항상 기존 로그 파일에 추가됩니다.

제 8 장: 암호화 키 구성 및 관리

이 섹션은 다음 항목을 포함하고 있습니다.

정책 서버 암호화 키 개요

정책 서버와 에이전트는 SiteMinder 환경의 정책 서버와 에이전트 간에 전달되는 중요한 데이터를 암호화하고 암호 해독하는 데 암호화 키를 사용합니다.

- 에이전트 키 - SiteMinder 쿠키를 암호화하는 데 사용됩니다. SiteMinder 쿠키는 싱글 사인온 환경의 모든 에이전트가 읽을 수 있으며, 각 에이전트가 다른 에이전트에 의해 암호화된 쿠키를 암해 해독할 수 있어야 하므로 싱글 사인온 환경의 모든 에이전트 간에 공유됩니다. 에이전트 키는 정책 서버에서 관리되며 에이전트에 정기적으로 배포됩니다.
- 세션 티켓 키 - 정책 서버가 세션 티켓을 암호화하는 데 사용됩니다. 세션 티켓에는 사용자 자격 증명을 비롯하여 세션과 관련된 자격 증명 및 기타 정보가 포함됩니다. 에이전트는 세션 티켓을 SiteMinder 쿠키에 포함하지만 세션 티켓 키에 대한 액세스 권한이 없으므로 해당 내용에 액세스할 수는 없습니다. 세션 티켓 키에 대한 액세스 권한은 정책 서버에만 있습니다.

두 키 유형 모두 정책 서버의 키 저장소에 보관되고 런타임에 에이전트에 배포됩니다. 기본적으로 키 저장소는 정책 저장소의 일부이지만 원하는 경우 별도의 키 저장소 데이터베이스를 생성할 수 있습니다.

그 밖의 특수 키는 다음과 같습니다.

- 정책 저장소 키 - 정책 저장소의 특정 데이터를 암호화하는 데 사용됩니다. 정책 저장소 키는 디스크에 있는 파일에 암호화된 상태로 저장됩니다. 정책 서버는 고유한 기술을 사용하여 정책 저장소 키를 암호화합니다. 정책 저장소 키는 정책 서버를 설치할 때 지정한 암호화 키에서 파생됩니다.
- 키 저장소 키 - 별도로 구성된 키 저장소의 에이전트 키와 세션 티켓 키를 암호화하는 데 사용됩니다. 키 저장소 키는 정책 저장소 키로 암호화되어 레지스트리(또는 UNIX 의 해당 위치)에 보관됩니다.

키 관리 개요

대규모 배포 환경에서 키 정보를 최신 상태로 유지하기 위해 정책 서버는 자동화된 키 롤오버 메커니즘을 제공합니다. 동일한 키 저장소를 공유하는 정책 서버 설치 환경에 대해 키를 자동으로 업데이트할 수 있습니다. 키 변경을 자동화하면 키의 무결성을 유지할 수 있습니다.

싱글 사인온이 구성된 SiteMinder 에이전트의 경우 다음과 같이 하십시오.

- 키 저장소를 복제합니다.
- 싱글 사인온 환경의 모든 SiteMinder 환경에서 복제된 저장소를 공유합니다.

정책 서버는 독립 실행형 키 저장소를 사용할 수 없는 것으로 확인될 경우 가용성을 확인하기 위해 키 저장소에 다시 연결하려고 시도합니다. 연결에 실패할 경우 정책 서버는 다음을 수행합니다.

- 일시 중단 상태로 전환하고 키 저장소가 다시 온라인 상태가 될 때까지 설정된 연결에서 모든 새 요청을 거부합니다.

  일시 중단 상태의 정책 서버는 SuspendTimeout 에 지정된 시간 동안 해당 상태로 유지되다가 정상적으로 종료됩니다. SuspendTimeout 이 0 인 경우 정책 서버는 키 저장소 연결이 다시 설정될 때까지 일시 중단된 상태로 유지됩니다.
- 오류 상태를 반환하여 웹 에이전트가 다른 정책 서버로 장애 조치될 수 있도록 합니다.
- 적절한 오류 메시지를 로깅합니다.

또한 정책 서버는 시작 시 키 저장소를 사용할 수 없는 경우에도 정상적으로 종료됩니다.

키를 관리하려면 관리 UI 를 사용하십시오.

FIPS 140-2 알고리즘

FIPS(Federal Information Processing Standard) 140-2 공표안에는 분류되지 않은 중요한 데이터를 보호하는 보안 시스템 내에서 암호화 알고리즘을 사용하기 위한 요구 사항이 지정되어 있습니다. SiteMinder 에는 FIPS 140-2 *Security Requirements for Cryptographic Modules*(암호화 모듈에 대한 보안 요구 사항)을 충족하는 것으로 확인된 RSA 의 Crypto-C ME v2.0 암호화 라이브러리가 포함되어 있습니다. 이 모듈에 대한 유효성 검사 인증서 번호는 608 입니다.

SiteMinder 의 Java 기반 API 는 FIPS 호환 버전의 Crypto-J 암호화 라이브러리를 사용합니다.

SiteMinder 는 사전 FIPS 모드나 FIPS 전용 모드에서 작동할 수 있습니다. 암호화 경계, 즉 SiteMinder 가 암호화를 적용하는 방식은 두 모드 모두에서 동일하지만 알고리즘은 서로 다릅니다.

FIPS 전용 모드에서 SiteMinder 가 사용하는 알고리즘은 다음과 같습니다.

- AES Key Wrap - 키 암호화
- OFB 모드의 AES(HMAC-SHA 256) - 채널 암호화
- CBC 모드의 AES(HMAC-SHA 224) - 싱글 사인온을 쉽게 하기 위해 사용되는 토큰 암호화

SiteMinder 핵심 구성 요소는 암호화된 데이터를 광범위하게 사용합니다.

- 웹 에이전트는 다음을 암호화합니다.
  - 쿠키 - 정책 서버에서 가져온 에이전트 키 사용
  - 정책 서버로 보내는 데이터 - 세션 키 사용
  - 공유 암호 - 호스트 키 사용 암호화된 공유 암호는 호스트 구성 파일에 저장됩니다.

- 정책 서버는 다음을 암호화합니다.
  - 웹 에이전트로 보내는 데이터 - 세션 키 사용
  - 정책 저장소 키 - 호스트 키 사용
  - 정책 저장소의 중요한 데이터 - 정책 저장소 키 사용
  - 세션 사양 - 세션 티켓 키 사용
  - 관리 UI 로 보내는 데이터 - 세션 키 사용
  - 사용자 디렉터리의 암호 서비스 데이터 - 세션 티켓 키 사용

정책 저장소 키는 정책 저장소에 저장된 중요한 데이터를 암호화하는 데 사용되며, 정책 저장소를 설치할 때 입력한 시드 문자열에서 파생됩니다. 또한 정책 저장소 키는 호스트 키를 사용하여 암호화되어 시스템 로컬 파일에 저장됩니다. 무인 작업을 지원하기 위해 호스트 키는 정책 저장소 코드에 포함된 고정 키로 사용됩니다. 에이전트는 이와 동일한 호스트 키 메커니즘을 사용하여 공유 암호의 복사본을 암호화하고 저장합니다.

정책 서버가 인증 토큰을 형성하는 데 사용하는 세션 티켓 키와 웹 에이전트가 쿠키 데이터를 암호화하는 데 주로 사용하는 에이전트 키는 정책 저장소(SiteMinder 구성 설정에 따라 키 저장소도 가능)에 암호화된 형식으로 저장되는 암호화 키입니다. 이러한 키는 정책 저장소 키와 키 저장소 키를 사용하여 암호화됩니다. 키 저장소 키는 정책 저장소에 암호화됩니다. 에이전트 인증 및 TLI 핸드셰이크에 사용되는 에이전트 공유 암호도 다른 중요한 데이터와 함께 정책 저장소 키로 암호화되어 정책 저장소에 저장됩니다.

도입된 에이전트 키

SiteMinder 웹 에이전트는 쿠키를 사용자의 브라우저로 전달하기 전에 에이전트 키를 사용하여 쿠키를 암호화합니다. 웹 에이전트가 SiteMinder 쿠키를 받은 경우 에이전트 키를 사용하여 쿠키의 내용을 암호 해독할 수 있습니다. 정책 서버와 통신하는 모든 웹 에이전트에 대해 키가 동일한 값으로 설정되어 있어야 합니다.

정책 서버는 다음과 같은 유형의 에이전트 키를 제공합니다.

- *동적 키* - 정책 서버 알고리즘에 의해 생성되며 연결된 정책 서버와 관련 SiteMinder 웹 에이전트에 배포됩니다. 동적 키는 정기적인 간격으로 롤오버하거나 관리 UI 의 "키 관리" 대화 상자를 사용하여 롤오버할 수 있습니다. 보안을 위해 에이전트 키 유형으로 동적 키를 사용하는 것이 좋습니다.
- *정적 키* - 무기한 동일하게 유지되며 정책 서버 알고리즘에 의해 생성되거나 수동으로 입력할 수 있습니다. SiteMinder 배포 환경에서는 정보를 오랜 기간 동안 사용자 컴퓨터의 쿠키에 저장해야 하는 일부 기능에 대해 이 유형의 키를 사용합니다.

  참고: 정적 에이전트 키는 항상 설치 시 생성됩니다. 정책 키를 에이전트 키로 사용하든 그렇지 않든 관계없이 이 정적 키는 사용자 관리 등의 일부 다른 제품 기능에 사용됩니다.

추가 정보:

동적 에이전트 키 롤오버 (페이지 114)

동적 에이전트 키 롤오버

동적 에이전트 키 롤오버는 FSS 관리 UI 의 "키 관리" 대화 상자에서 구성합니다. 웹 에이전트는 키 업데이트를 위해 정책 서버를 정기적으로 폴링합니다. 키가 업데이트된 경우 웹 에이전트는 폴링 중에 변경 내용을 가져옵니다. 기본 폴링 시간은 30 초이지만 웹 에이전트의 pspollinterval 매개 변수를 변경하여 원하는 시간을 구성할 수 있습니다.

참고: 웹 에이전트의 매개 변수 변경에 대한 자세한 내용은 *SiteMinder 웹 에이전트 구성 안내서*를 참조하십시오.

정책 서버는 알고리즘을 사용하여 동적 키를 정기적으로 생성합니다. 이러한 키는 키 저장소에 저장됩니다. 웹 에이전트는 새 키가 검색되면 키 저장소에서 이를 가져옵니다.

동적 에이전트 키 롤오버

동적 에이전트 키 롤오버는 관리 UI 에서 구성합니다. 웹 에이전트는 키 업데이트를 위해 정책 서버를 정기적으로 폴링합니다. 키가 업데이트된 경우 웹 에이전트는 폴링 중에 변경 내용을 가져옵니다. 기본 폴링 시간은 30 초이지만 웹 에이전트의 pspollinterval 매개 변수를 변경하여 기본값을 변경할 수 있습니다.

참고: 웹 에이전트의 매개 변수 변경에 대한 자세한 내용은 *SiteMinder 웹 에이전트 구성 안내서*를 참조하십시오.

정책 서버는 알고리즘을 사용하여 동적 키를 정기적으로 생성합니다. 이러한 키는 키 저장소에 저장됩니다. 웹 에이전트는 새 키가 검색되면 키 저장소에서 이를 가져옵니다.

동적 키 롤오버에 사용되는 에이전트 키

SiteMinder 배포 환경에서는 동적 키 롤오버에 다음 키를 사용하며 이러한 키를 키 저장소에 보관합니다.

- 이전 키 - 현재 값 이전에 에이전트 키에 사용된 마지막 값을 포함하는 동적 키입니다.
- 현재 키 - 현재 에이전트 키의 값을 포함하는 동적 키입니다.
- 이후 키 - 에이전트 키 롤오버에 현재 키로 사용될 다음 값을 포함하는 동적 키입니다.
- 정적 키

정책 서버가 동적 에이전트 키 롤오버를 처리할 경우 현재 키의 값이 이전 키의 값을 대체합니다. 이후 키의 값은 현재 키의 값을 대체하며, 정책 서버는 이후 키의 새 값을 생성합니다.

클라이언트 브라우저에서 쿠키를 받으면 웹 에이전트는 키 저장소의 현재 키를 사용하여 쿠키를 암호 해독합니다. 암호 해독된 값이 유효하지 않으면 웹 에이전트는 이전 키를 사용해 보고 필요한 경우 이후 키도 사용해 봅니다. 이전 키는 아직 업데이트되지 않은 에이전트의 쿠키를 암호 해독하거나 클라이언트 브라우저의 기존 쿠키를 암호 해독하는 데 필요할 수 있습니다. 이후 키는 업데이트된 에이전트에 의해 생성되었지만 키 저장소에서 업데이트된 키를 아직 폴링하지 않은 에이전트가 읽는 쿠키에 필요할 수 있습니다.

에이전트 키의 롤오버 간격

에이전트 키 롤오버 프로세스는 지정된 시간에 시작됩니다. 여러 정책 서버에서 여러 롤오버가 수행되는 것을 방지하기 위해 각 서버는 최대 30 분의 롤오버 대기 시간을 설정합니다. 대기 시간이 끝날 때까지 업데이트가 수행되지 않은 경우 정책 서버는 키를 업데이트합니다.

모든 정책 서버는 업데이트된 키를 기다린 다음 해당 에이전트에 대해 새 키를 처리합니다. 단일 정책 서버의 경우에도 업데이트 시간은 지정된 롤오버 시간을 초과하여 최대 30 분이 될 수 있습니다.

에이전트 키 롤오버 프로세스는 SiteMinder "에이전트 키 관리" 대화 상자에 지정된 시간에 시작됩니다. 이 프로세스에는 최대 3 분이 소요될 수 있습니다. 이 시간 동안 정책 서버에 연결된 모든 웹 에이전트가 업데이트된 키를 받습니다.

참고: 복제된 정책 서버가 여러 개 포함된 배포 환경에서 에이전트 키 배포 프로세스에는 최대 30 분이 소요될 수 있습니다.

정적 키

정적 키는 일관되게 유지되는 데이터를 암호화하는 데 사용되는 문자열입니다. 에이전트 키 롤오버 기능을 사용하는 SiteMinder 배포 환경에서 정적 키를 사용하면 오랜 기간 동안 사용자 정보를 보관할 수 있습니다.

다음과 같은 SiteMinder 기능 및 상황의 경우에 정적 키를 사용합니다.

- HTML 양식 인증을 위한 사용자 자격 증명 저장

  사용자가 자격 증명을 저장할 수 있도록 HTML 양식 인증 체계가 구성된 경우 정책 서버는 정적 키를 사용하여 사용자의 자격 증명을 암호화합니다.

- 사용자 추적

  사용자 추적이 설정된 경우 정책 서버는 정적 키를 사용하여 사용자 아이덴티티 정보를 암호화합니다.

- 여러 키 저장소의 싱글 사인온

  키 저장소가 여러 개 포함된 SiteMinder 배포 환경에서는 싱글 사인온에 정적 키가 사용될 수 있습니다. 이 경우 SiteMinder 에이전트는 모든 쿠키 암호화에 정적 키를 사용합니다.

  참고: 정적 키를 변경할 경우 이전 정적 키로 생성된 모든 쿠키가 무효화됩니다. 사용자는 다시 인증해야 할 수 있으며 사용자 추적 정보는 무효화됩니다. 또한 정적 키가 싱글 사인온에 사용되는 경우 사용자가 다른 쿠키 도메인의 리소스에 액세스하려고 하면 사용자에게 자격 증명이 요청됩니다.

추가 정보:

개별 키 저장소를 사용하는 여러 정책 저장소 (페이지 123)

세션 티켓 키

사용자가 보호된 리소스에 로그인하는 데 성공하면 정책 서버는 세션 티켓을 생성합니다. 세션 티켓은 정책 서버가 사용자 인증의 유효 기간을 확인하는 데 사용됩니다. 이 세션 티켓은 *세션 티켓 키*를 사용하여 암호화되고 에이전트 사용자 캐시에 캐시됩니다.

정책 서버가 알고리즘을 사용하여 세션 티켓 키를 생성하도록 선택하거나, SiteMinder "키 관리" 대화 상자에서 세션 티켓 키를 입력할 수 있습니다. 보안상 임의로 생성된 키를 사용하는 것이 좋습니다.

그러나 SiteMinder 구현에 싱글 사인온 환경의 여러 키 저장소가 포함되어 있는 경우에는 모든 키 저장소에 대해 동일한 세션 티켓 키를 사용해야 합니다.

추가 정보:

세션 티켓 키 관리 (페이지 132)
캐시 관리 개요 (페이지 153)

키 관리 시나리오

싱글 사인온 요구 사항과 정책 서버, 정책 저장소 및 키 저장소의 구현 방식에 따라 세 가지 유형의 키 관리 시나리오가 있습니다. 이러한 시나리오에는 다음이 포함됩니다.

- 공용 정책 저장소 및 키 저장소

  이 시나리오에서는 정책 서버 그룹이 단일 정책 저장소 및 키 저장소를 공유하며 단일 쿠키 도메인에서 액세스 제어 및 싱글 사인온을 제공합니다.

  정책 저장소 데이터는 단일 정책 저장소에 보관됩니다. 키 데이터는 단일 키 저장소에 보관됩니다. 키 저장소는 정책 저장소의 일부이거나 별도의 저장소일 수 있습니다.

  정책 저장소 데이터와 키 저장소 데이터는 모두 장애 조치를 위해 복제될 수 있습니다. 복제는 정책 저장소에 대해 선택된 데이터베이스 또는 디렉터리 유형에 따라 구성되어야 합니다. 복제 체계에 대한 자세한 내용은 데이터베이스 또는 디렉터리 공급업체에서 제공하는 설명서를 참조하십시오.

- 공용 키 저장소를 사용하는 여러 정책 저장소

  이 시나리오에서는 정책 서버 그룹이 개별 정책 저장소에 연결되어 있지만 공용 키 저장소를 공유하여 여러 쿠키 도메인에서 액세스 제어 및 싱글 사인온을 제공합니다.

  각 정책 서버 그룹의 정책 저장소 데이터는 단일 정책 저장소에 보관됩니다. 모든 정책 서버 그룹의 키 데이터는 단일 키 저장소에 보관됩니다. 개별 키 저장소를 사용하면 모든 정책 서버와 연결된 에이전트가 키를 공유하여 개별 쿠키 도메인에서 싱글 사인온을 사용할 수 있습니다.

  정책 저장소 데이터와 키 저장소 데이터는 모두 장애 조치를 위해 복제될 수 있습니다. 복제는 정책 저장소에 대해 선택된 데이터베이스 또는 디렉터리 유형에 따라 구성되어야 합니다. 복제 체계에 대한 자세한 내용은 데이터베이스 또는 디렉터리 공급업체에서 제공하는 설명서를 참조하십시오.

- 여러 정책 저장소 및 여러 키 저장소

  이 시나리오에서는 각 쿠키 도메인의 정책 서버가 개별 키 저장소를 갖는 것이 바람직한 여러 쿠키 도메인에서 각 정책 서버 그룹이 단일 정책 저장소 및 키 저장소를 공유하여 액세스 제어 및 싱글 사인온을 제공합니다.

  각 정책 서버 그룹의 정책 저장소 데이터는 단일 정책 저장소에 보관됩니다. 각 정책 서버 그룹의 키 데이터는 단일 키 저장소에 보관됩니다. 키 저장소는 정책 저장소의 일부이거나 별도의 저장소일 수 있습니다. 모든 웹 에이전트의 싱글 사인온에 동일한 정적 키 집합을 사용할 수 있습니다.

  정책 저장소 데이터와 키 저장소 데이터는 모두 장애 조치를 위해 복제될 수 있습니다. 복제는 정책 저장소에 대해 선택된 데이터베이스 또는 디렉터리 유형에 따라 구성되어야 합니다. 복제 체계에 대한 자세한 내용은 데이터베이스 또는 디렉터리 공급업체에서 제공하는 설명서를 참조하십시오.

추가 정보:

LDAP 장애 조치 구성 (페이지 40)
ODBC 장애 조치 구성 (페이지 51)

키 관리 고려 사항

회사에서 사용할 키 관리 시나리오를 결정할 때는 다음 사항을 고려하십시오.

- 공용 키 저장소를 공유하는 정책 서버가 여러 개 포함된 환경에서 동적 키를 구성하는 경우 에이전트 키 생성을 수행할 단일 정책 서버를 지정해야 합니다. 다른 모든 정책 서버에서는 키 생성이 사용되지 않도록 설정해야 합니다.
- 정책 서버가 여러 개 포함된 네트워크 구성에서는 정책 서버 관리 콘솔을 사용하여 각 정책 서버의 정책 저장소를 지정할 수 있습니다. 정책 저장소는 SiteMinder 개체 및 정책 정보를 저장하기 위한 기본 위치인 마스터 정책 저장소이거나, 마스터 정책 저장소에서 복사된 데이터를 사용하는 복제된 정책 저장소일 수 있습니다.

- 마스터/슬레이브 디렉터리 또는 데이터베이스는 해당 디렉터리 또는 데이터베이스 공급자의 사양에 따라 구성해야 합니다. 정책 서버에서는 정책 저장소의 장애 조치 순서를 지정할 수 있지만 정책 서버가 데이터 복제를 제어하지는 않습니다. 복제 체계에 대한 자세한 내용은 디렉터리 또는 데이터베이스 공급자의 설명서를 참조하십시오.
- 동적 키 롤오버를 사용하는 네트워크에서 정책 서버의 키 저장소는 마스터 키 저장소이거나 복제된 슬레이브 키 저장소일 수 있습니다. 마스터 키 저장소는 키를 생성하는 정책 서버 프로세스에서 직접 키를 받습니다. 슬레이브 키 저장소는 마스터 키 저장소에 있는 키의 복사본을 받습니다.
- 마스터/슬레이브 환경에서는 마스터 정책 저장소와 키 저장소에 연결된 정책 서버에서 키 생성을 구성해야 합니다. 그런 다음 마스터 정책 저장소와 키 저장소 데이터를 장애 조치 순서에 포함된 다른 모든 정책 저장소 및 키 저장소에 복제해야 합니다.
- 여러 쿠키 도메인에 대한 싱글 사인온 환경에서는 단일 마스터 키 저장소나 단일 마스터 키 저장소에서 복제된 키가 포함된 슬레이브 키 저장소가 있는 경우에만 동적 키를 사용할 수 있습니다.
- 정책 저장소와 키 저장소를 설치하는 데는 LDAP 디렉터리와 ODBC 디렉터리를 혼합하여 사용할 수 있습니다. 즉, 정책 저장소는 ODBC 데이터베이스에 있고 키 저장소는 LDAP 디렉터리 서버에 있거나, 그 반대일 수 있습니다. 지원되는 데이터베이스 목록을 보려면 기술 지원 사이트로 이동하여 "SiteMinder 12.52 SP1 Platform Support Matrix"(SiteMinder 12.52 SP1 플랫폼 지원표)를 검색하십시오.

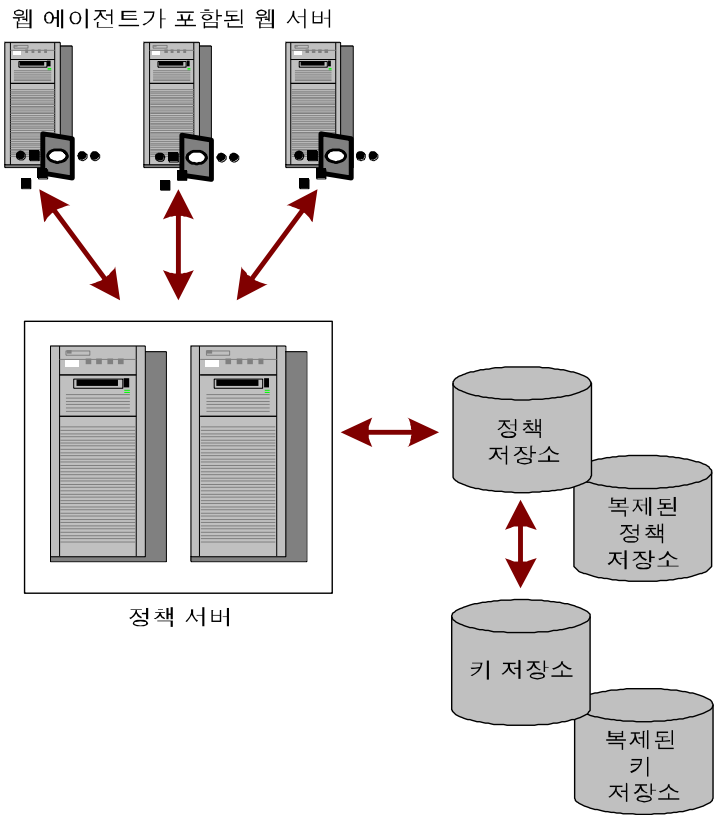
추가 정보:

에이전트 키 생성 구성 (페이지 128)
LDAP 장애 조치 구성 (페이지 40)
ODBC 장애 조치 구성 (페이지 51)

공용 정책 저장소 및 키 저장소

키 롤오버를 사용하는 SiteMinder 구성에 대한 가장 간단한 시나리오는 여러 정책 서버가 단일 키 저장소와 함께 단일 정책 저장소 및 관련 장애 조치 정책 저장소를 사용하는 경우입니다.

다음 그림에서는 단일 정책 저장소를 사용하는 여러 정책 서버를 보여 줍니다.



이 구성 유형에서는 정책 서버가 키 저장소에서 동적 키를 받습니다. 정책 서버와 연결된 웹 에이전트는 정책 서버에서 새 키를 수집합니다.

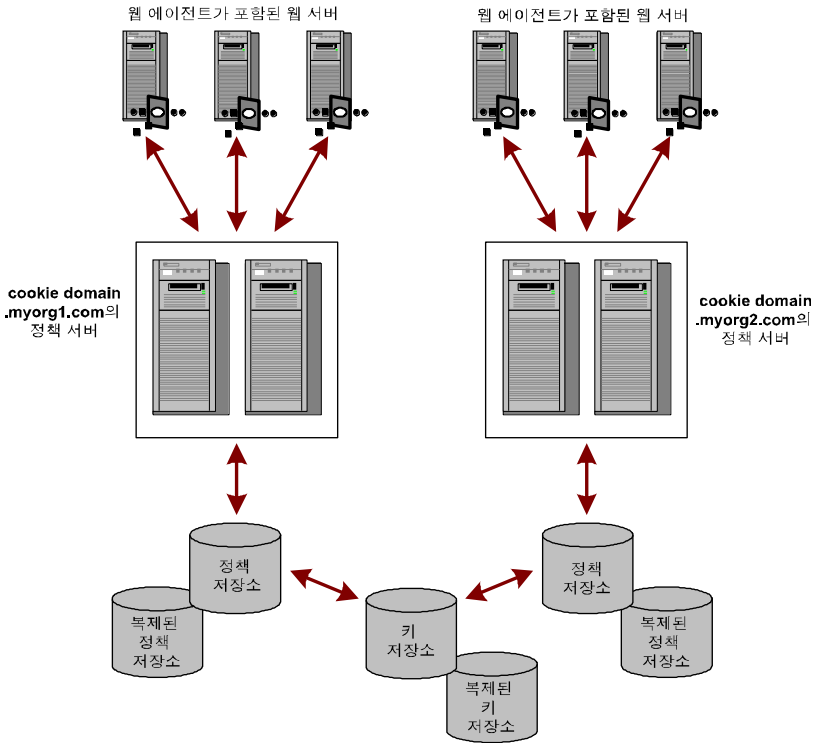
추가 정보:

키 관리 고려 사항 (페이지 119)

공용 키 저장소를 사용하는 여러 정책 저장소

네트워크 구성이 싱글 사인온 환경에서 개별 정책 저장소를 사용하는 여러 정책 서버로 이루어진 경우 모든 정책 서버가 키 롤오버에 공용 키 저장소를 사용하도록 할 수 있습니다.

다음 그림에서는 공용 키 저장소를 사용하는 여러 정책 서버를 보여 줍니다.



정책 서버 하나에서 동적 키를 생성하고 이를 중앙 키 저장소에 저장합니다. 정책 서버 관리 콘솔을 통해 각 정책 서버가 중앙 키 저장소를 사용하도록 구성되어 있으며 다른 모든 정책 서버에는 에이전트 키 생성이 사용되지 않도록 설정되어 있어야 합니다. 에이전트는 해당 정책 서버를 폴링하여 새 키를 검색합니다. 정책 서버는 공용 키 저장소에서 새 키를 검색하고 이를 SiteMinder 에이전트에 전달합니다.

참고: 이 시나리오에는 키를 생성하지 않는 정책 서버가 키 업그레이드를 위해 키 저장소를 폴링하도록 하는 추가 레지스트리 설정이 필요합니다.

추가 정보:

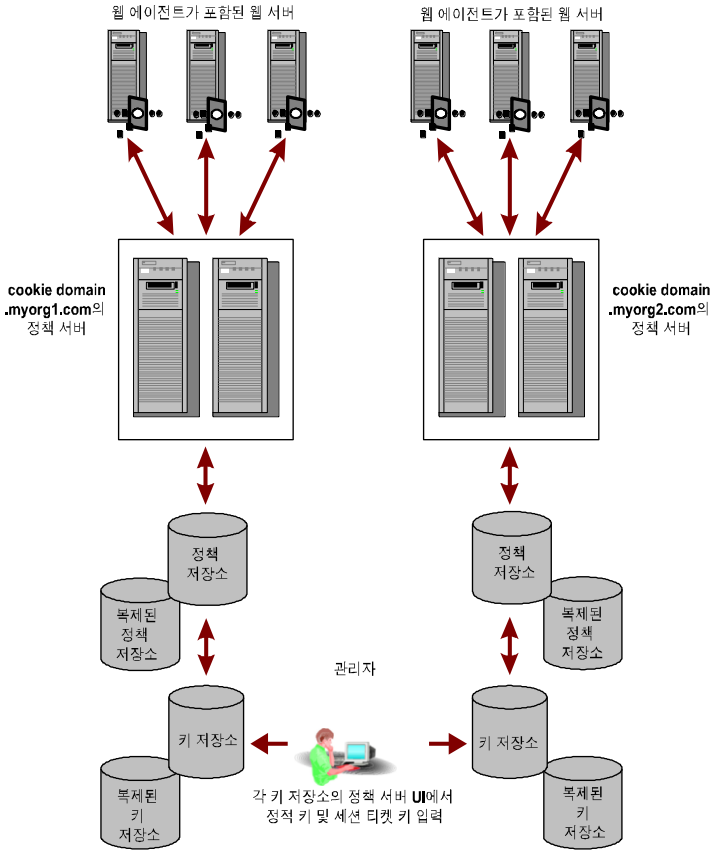
키 관리 고려 사항 (페이지 119)
EnableKeyUpdate 레지스트리 키 설정 (페이지 133)

개별 키 저장소를 사용하는 여러 정책 저장소

네트워크 구성이 여러 개의 정책 서버, 정책 저장소 및 마스터 키 저장소로 이루어진 경우 적절한 권한을 가진 관리자가 다음 중 하나 이상을 쉽게 수행할 수 있도록 각 정책 저장소에 대해 동일한 정적 키 및 세션 티켓 키를 지정할 수 있습니다.

- 모든 에이전트 간의 싱글 사인온
- 공용 사용자 디렉터리를 사용하는 암호 서비스

다음 그림에서는 여러 개의 정책 서버 및 저장소를 사용하는 환경을 보여 줍니다.



위 예에서는 SiteMinder 웹 에이전트가 생성한 모든 쿠키를 암호화하는 데 동일한 정적 키가 사용됩니다.

추가 정보:

키 관리 고려 사항 (페이지 119)

r6.x 정책 저장소 암호화 키 재설정

r6.x 정책 저장소 암호화 키를 재설정하려면

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행합니다.

   ```
   smobjexport -dsiteminder_administrator -wpassword -ofile_name -c
   ```

   -d*siteminder_administrator*

   SiteMinder 관리자 계정의 이름을 지정합니다.

   참고: 이 관리자는 모든 SiteMinder 도메인 개체를 관리할 수 있어야 합니다.

   -w*password*

   SiteMinder 관리자 계정의 암호를 지정합니다.

   -o*file_name*

   다음을 지정합니다.

   - 출력 위치의 경로
   - 유틸리티가 생성하는 smdif 파일의 이름

   참고: 이 인수를 지정하지 않을 경우 기본 출력 파일 이름은 stdout.smdif 및 stdout.cfg 입니다.

   -c

   중요한 데이터를 일반 텍스트로 내보냅니다.

   이 유틸리티는 정책 저장소 데이터를 smdif 파일로 내보냅니다.
3. smreg 유틸리티가 *policy_server_home*\bin 에 있는지 확인합니다.

   policy_server_home

   정책 서버 설치 경로를 지정합니다.

   참고: 이 유틸리티가 없는 경우 CA Support 사이트에서 제공되는 정책 서버 설치 미디어에서 이 유틸리티를 찾을 수 있습니다.

4. 다음 명령을 실행합니다.

   `smreg -key encryption_key`

   encryption_key

   새 암호화 키를 지정합니다.

   제한: 6 자~24 자

   정책 저장소 암호화 키가 변경됩니다.

5. 정책 서버 관리 콘솔을 시작하고 "데이터" 탭을 엽니다.
6. 정책 저장소 관리자 암호를 다시 입력하고 "업데이트"를 클릭합니다.

   관리자 암호가 새 암호화 키를 사용하여 다시 암호화됩니다.

7. 다음 명령을 실행합니다.

   `smreg -su password`

   암호

   SiteMinder 슈퍼 사용자 암호를 지정합니다.

   슈퍼 사용자 암호가 설정되고 새 암호화 키를 사용하여 암호화됩니다.

8. 다음 명령을 실행합니다.

   `smobjimport -dsiteminder_administrator -wpassword -ifile_name -r -f -c`

   -d*siteminder_administrator*

   SiteMinder 관리자 계정의 이름을 지정합니다.

   참고: 이 관리자는 모든 SiteMinder 도메인 개체를 관리할 수 있어야 합니다.

   -w*password*

   SiteMinder 관리자 계정의 암호를 지정합니다.

   -i*file_name*

   다음을 지정합니다.

   - smdif 파일의 경로
   - smdif 파일의 이름

   참고: 이 인수를 지정하지 않을 경우 기본 입력 파일 이름은 stdout.smdif 및 stdout.cfg 입니다.

-r

가져오는 중에 중복 정책 저장소 정보를 덮어쓸 수 있도록 지정합니다.

-f

개체의 자동 이름 변경을 해제합니다. 기본적으로 가져오려는 개체의 이름이 대상 정책 저장소에 이미 있을 경우 중복 개체가 생성됩니다. 개체의 이름은 *nameoid* 입니다.

name

개체의 이름을 지정합니다.

oid

새 중복 개체의 개체 ID 를 지정합니다.

이름 충돌로 인해 개체를 생성할 수 없을 경우 오류 메시지가 반환됩니다.

-c

입력 파일에 중요한 데이터가 일반 텍스트로 포함되어 있음을 나타냅니다.

9. 다음 명령을 실행합니다.

```
smreg -su password
```

password

SiteMinder 슈퍼 사용자 암호를 지정합니다.

슈퍼 사용자 암호가 설정됩니다.

정책 저장소 암호화 키가 재설정됩니다.

r12.x 정책 저장소 암호화 키 재설정

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 정책 서버를 중지합니다.

   참고: 암호화 키를 변경하기 전에 정책 저장소를 가리키는 모든 정책 서버를 중지하십시오.
3. XPSExport 를 사용하여 정책 저장소 콘텐츠의 전체 백업 내보내기

   xpsexport <filename> -xb –npass

   또는 (출력을 암호화하려면)

   xpsexport <filename> -xb –pass <password>
4. smkeyexport 를 사용하여 에이전트 내보내기(일반 텍스트 옵션이 필요)

   smkeyexport –o <filename> -d<sm admin name> -w<smadmin password> -c
5. 정책 저장소 암호화 키 변경

   smreg –key <new key>
6. SmConsole 을 사용하여 정책 저장소 암호 재설정 및 테스트

   SmConsole 의 "데이터" 탭을 사용하여 이전에 구성된 암호를 다시 입력하고, 변경 내용을 적용한 다음 "연결 테스트" 단추를 사용하여 확인합니다.
7. 3 단계의 내보내기 토큰과 함께 XPSImport 를 사용하여 정책 저장소 내용을 가져오십시오.

   xpsimport <filename> –fo –pass <password>

   또는 (내보내기 파일을 만들기 위해 암호가 사용되지 않은 경우)

   xpsimport <filename> –fo –npass
8. 4 단계의 내보내기 토큰과 함께 smkeyimport(clear-text 옵션)를 사용하여 에이전트 키를 가져오십시오.

   smkeyimport –i<filename> -d<sm admin name> -w<sm admin password> -c
9. 정책 서버를 다시 시작합니다.

정책 저장소 암호화 키가 재설정됩니다.

에이전트 키 생성 구성

정책 서버 관리 콘솔의 "키" 탭을 사용하여 정책 서버가 에이전트 키 생성을 처리하는 방식을 구성할 수 있습니다.

참고: 에이전트 키를 생성하려는 정책 서버에서만 키 생성이 사용되도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 시작합니다.

   중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "키" 탭을 클릭합니다.

   참고: 이 탭의 설정과 컨트롤에 대한 자세한 내용을 보려면 "도움말", "관리 콘솔 도움말"을 차례로 클릭하십시오.

3. "키" 탭의 필드 및 컨트롤을 적절하게 설정하여 에이전트 키 생성을 구성합니다.
4. 작업을 마쳤으면 "적용"을 클릭하여 변경 내용을 저장합니다.

에이전트 키 관리

관리 UI 에서 액세스하는 SiteMinder "키 관리" 대화 상자를 사용하여 정기적 에이전트 키 롤오버를 구성하고, 수동 롤오버를 실행하고, 정적 키를 변경할 수 있습니다. 세션 티켓 키를 관리할 수도 있습니다.

참고: 키를 관리하려면 "키 및 암호 정책 관리" 권한이 있는 계정을 사용하여 관리 UI 에 로그인해야 합니다. 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

추가 정보:

세션 티켓 키 관리 (페이지 132)

주기적 키 롤오버 구성

정책 서버는 다음 빈도의 주기적 에이전트 키 롤오버를 지원합니다.

- Weekly(주별)
- 일별
- 하루 중 지정된 간격

롤오버 간에 허용되는 가장 짧은 기간은 1 시간입니다.

참고: 운영 체제가 일광 절약 시간에 따라 시스템 시간을 조정하도록 구성되어 있는지 확인하십시오. 일광 절약 시간을 사용하도록 구성되지 않은 시스템에서는 키 롤오버 시 1 시간의 오차가 발생할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔에 액세스하고 "키" 탭을 엽니다.
2. "에이전트 키 생성 사용"을 선택하고 "확인"을 클릭합니다.
3. 관리 UI 에 로그인합니다.
4. "관리", "정책 서버"를 차례로 클릭합니다.
5. "키 관리", "에이전트 키 관리"를 차례로 클릭합니다.
6. "에이전트 키" 섹션에서 "동적 에이전트 키 사용"을 선택합니다.

   중요! "동적 에이전트 키 사용"을 선택한 후에는 주기적 키 롤오버 구성 설정을 저장하기 전까지 "지금 롤오버"를 클릭할 수 없습니다.
7. "동적 키 상세 정보" 섹션에서 "자동 키 롤오버"를 선택합니다.
8. "롤오버 빈도 설정"을 클릭합니다.
9. 롤오버가 발생할 빈도를 지정합니다.
10. "확인"을 클릭합니다.
11. "제출"을 클릭합니다.

    에이전트 키 롤오버가 구성됩니다.

수동으로 키 롤오버

동적 에이전트 키를 수동으로 롤오버할 수 있습니다. 이 기능의 특징은 다음과 같습니다.

- 보안이 더 강화됩니다. 언제라도 롤오버를 실행할 수 있습니다.
- 유연성이 높아집니다. 정책 서버가 동적 키를 생성하도록 구성할 수 있지만 반드시 롤오버 빈도를 지정할 필요는 없습니다.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔에 액세스하고 "키" 탭을 엽니다.
2. "에이전트 키 생성 사용"을 선택하고 "확인"을 클릭합니다.
3. 관리 UI 에 로그인합니다.
4. "관리", "정책 서버"를 차례로 클릭합니다.
5. "키 관리", "에이전트 키 관리"를 차례로 클릭합니다.
6. "에이전트 키" 섹션에서 "동적 에이전트 키 사용"을 선택합니다.
7. "동적 키 상세 정보" 섹션에서 "수동 키 롤오버"를 선택합니다.
8. "지금 롤오버"를 클릭합니다.

   정책 서버가 즉시 새 에이전트 키를 생성합니다. 에이전트 키 롤오버를 수동으로 실행하는 경우를 제외하고 정책 서버는 자동으로 새 동적 키를 생성하지 않습니다.

참고: 키를 두 번 이상 롤오버하려는 경우 이외에는 이 단추를 여러 번 클릭하지 마십시오.

웹 에이전트는 다음에 정책 서버를 폴링할 때 새 키를 가져옵니다. 캐시 동기화로 인해 이 작업에는 최대 3 분이 걸릴 수 있습니다. 보안상의 이유로 완전히 새로운 키 집합을 사용하려는 경우에는 동적 키를 두 번 롤오버하십시오. 이 작업은 키 저장소에서 현재 키와 이전 키를 제거합니다.

에이전트 키 관리 및 세션 시간 만료 조정

에이전트 키 업데이트와 세션 시간 만료를 조정해야 합니다. 그러지 않으면 세션 정보가 포함된 쿠키가 무효화될 수 있습니다. 조직에서 정책을 설계하는 사람과 동적 키 롤오버를 구성하는 사람이 다를 수 있기 때문에 이 조정은 중요합니다.

세션 만료 시간은 구성된 에이전트 키 롤오버 간격의 두 배 이하여야 합니다. 관리자가 세션 만료 전에 에이전트 키 롤오버가 두 번 발생하도록 구성할 경우 첫 번째 키 롤오버 이전에 웹 에이전트가 작성한 쿠키는 더 이상 유효하지 않으며 사용자는 해당 세션이 종료되기 *전에* 해당 ID 에 대해 다시 인증을 요청받습니다.

예를 들어 키 롤오버가 3 시간마다 발생하도록 구성할 경우 최대 세션 만료 시간을 6 시간 이하로 설정하여 여러 키 롤오버로 인해 세션 쿠키가 무효화되지 않도록 해야 합니다.

정적 키 변경

웹 에이전트가 특정 기능에 대한 아이덴티티 정보를 암호화하기 위해 사용하는 정적 에이전트 키를 변경할 수 있습니다.

중요! 정적 키를 변경하는 것은 권장되지 않습니다. 보안 위반과 같이 중대한 상황에서만 정적 키를 변경하십시오. 이 작업을 수행하면 일부 SiteMinder 기능의 정상 작동에 필요한 데이터가 손실될 수 있습니다. 영구 쿠키에 저장된 아이덴티티를 설정하고 사용하는 기능은 더 이상 작동하지 않습니다. 인증된 사용자의 경우 여러 SiteMinder 설치 간에 싱글 사인온이 작동하기 전에 강제로 다시 로그인해야 할 수 있습니다.

또한 정적 키는 여러 개의 정책 서버와 여러 개의 마스터 키 저장소가 필요한 싱글 사인온 환경을 유지하는 데 사용될 수도 있습니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "관리", "정책 서버"를 차례로 클릭합니다.
3. "키 관리", "에이전트 키 관리"를 차례로 클릭합니다.
4. "에이전트 키" 섹션에서 "정적 에이전트 키 사용"을 선택합니다.
5. 다음 작업 중 하나를 수행하십시오.
   - "임의 에이전트 키 생성" 섹션에서 "지금 롤오버"를 클릭합니다.

     정책 서버가 임의 정적 키를 새로 생성합니다.
   - "에이전트 키 지정" 섹션에 정적 에이전트 키를 입력합니다.

     두 개의 키 저장소가 싱글 사인온을 유지하기 위해 정적 키를 사용해야 하는 상황에서 이 옵션을 사용합니다.

6. "지금 롤오버"를 클릭합니다.
7. "제출"을 클릭합니다.

   정적 키가 3 분 내에 롤오버됩니다.

세션 티켓 키 관리

정책 서버가 알고리즘을 사용하여 세션 티켓 키를 생성하거나, 사용자가 수동으로 세션 티켓 키를 입력할 수 있습니다. 세션 티켓은 사용자가 성공적으로 인증될 때마다 설정되며 정책 서버는 세션 티켓을 통해 사용자의 세션이 계속될 수 있는 기간을 확인할 수 있습니다.

참고: 여러 개의 독립적 키 저장소가 포함된 구현에서만 수동으로 할당된 세션 티켓 키가 필요합니다. 정책 서버는 자동으로 생성된 키를 독립적 키 저장소에 전파할 수 없습니다. 그 밖의 다른 모든 경우에는 정책 서버 알고리즘을 통해 생성된 세션 티켓 키를 사용하는 것이 좋습니다.

세션 티켓 키 생성

정책 서버는 동적 에이전트 키를 생성하는 것과 비슷한 방법을 사용하여 세션 티켓 키를 생성할 수 있습니다. 세션 티켓 키를 임의로 생성하면 정책 서버는 알고리즘을 사용하여 암호화 및 암호 해독에 사용되는 키를 생성할 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "관리", "정책 서버"를 차례로 클릭합니다.
3. "키 관리", "세션 키 관리"를 차례로 클릭합니다.
4. 다음 작업 중 하나를 수행하십시오.
   - "임의 세션 티켓 키 생성" 섹션에서 "지금 롤오버"를 클릭합니다.

     정책 서버가 세션 티켓 키를 새로 생성합니다. 이 키는 세션 티켓의 암호화 및 암호 해독에 사용되는 키를 즉시 대체합니다.

- "세션 티켓 키 지정" 섹션에서 세션 티켓을 지정하고 "지금 롤오버"를 클릭합니다.

  정책 서버는 기존 세션 티켓 키를 즉시 새로 입력한 값으로 바꿉니다.

5. "제출"을 클릭합니다.

세션 티켓 키 수동 입력

정책 서버가 여러 키 저장소가 포함된 구현의 일부인 경우 세션 티켓 키를 수동으로 입력할 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "관리", "정책 서버"를 차례로 클릭합니다.
3. "키 관리", "세션 키 관리"를 차례로 클릭합니다.
4. "세션 티켓 키 지정" 섹션에서 키를 지정합니다.
5. "지금 롤오버"를 클릭합니다.

   정책 서버는 기존 세션 티켓 키를 즉시 새로 입력한 값으로 바꿉니다.
6. "제출"을 클릭합니다.

EnableKeyUpdate 레지스트리 키 설정

개별 정책 저장소에 연결하지만 중앙 키 저장소를 공유하는 여러 정책 서버가 있는 환경에서 단일 정책 서버가 암호화 키를 생성할 경우 추가 레지스트리 설정이 필요합니다. 이 레지스트리 설정은 각 정책 서버가 정기적으로 공용 키 저장소를 폴링하여 새 암호화 키를 검색하도록 구성합니다.

Windows 정책 서버에서 EnableKeyUpdate 레지스트리 키를 구성하려면

1. Windows "시작" 메뉴에서 "실행"을 선택합니다.
2. "실행" 대화 상자에 regedit 를 입력하고 "확인"을 클릭합니다.
3. 레지스트리 편집기에서 다음 위치로 이동합니다.

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\
   CurrentVersion\ObjectStore
   ```

4. 다음 레지스트리 값을 변경합니다.

   "EnableKeyUpdate"=0

   다음과 같이 변경합니다.

   "EnableKeyUpdate"=1

5. 정책 서버를 다시 시작합니다.

UNIX 정책 서버에서 EnableKeyUpdate 레지스트리 키를 구성하려면

1. 다음 위치로 이동합니다.

   install_directory/siteminder/registry

2. 텍스트 편집기에서 sm.registry 를 엽니다.
3. 파일에서 다음 텍스트를 찾습니다.

   HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\
   CurrentVersion\ObjectStore

4. 다음 레지스트리 값을 변경합니다.

   "EnableKeyUpdate"=0

   다음과 같이 변경합니다.

   "EnableKeyUpdate"=1

5. 정책 서버를 다시 시작합니다.

추가 정보:

공용 키 저장소를 사용하는 여러 정책 저장소 (페이지 121)

트러스트된 호스트의 공유 암호

트러스트된 호스트를 등록하면 설치 프로세스는 다음 작업을 수행합니다.

- 자동으로 웹 에이전트에 대한 공유 암호 만들기
- 호스트 구성 파일(SmHost.conf)에 공유 암호 저장

트러스트된 호스트를 등록할 때 공유 암호 롤오버가 사용되도록 설정한 경우 트러스트된 호스트의 공유 암호를 수동으로 또는 주기적으로 롤오버할 수 있습니다.

수동 또는 주기적 공유 암호 롤오버 중에는 설치 시 롤오버를 허용하도록 구성된 에이전트에 대해서만 공유 암호가 롤오버됩니다.

참고: 웹 에이전트 설치 및 트러스트된 호스트 등록에 대한 자세한 내용은 *SiteMinder 웹 에이전트 설치 안내서*를 참조하십시오.

공유 암호 롤오버는 에이전트 키 생성을 사용하도록 구성된 서버에서만 자동으로 발생합니다. 에이전트 키 생성이 사용되도록 설정하려면 정책 서버 관리 콘솔의 "키" 탭에서 "에이전트 키 생성 사용" 확인란을 선택하십시오. 이 설정은 기본적으로 사용되도록 설정되어 있습니다.

중요! 정책 서버 하나만 키를 생성하도록 설정하는 것이 좋습니다. 환경에 정책 저장소가 여러 개 있지만 공유 키 저장소는 하나뿐인 경우 모든 공유 암호가 자동으로 롤오버되지는 않습니다. 공유 암호는 정책 저장소가 구성된 정책 서버에서 키를 생성하도록 설정된 경우에만 자동으로 롤오버됩니다. 다른 모든 정책 저장소의 경우 수동으로 롤오버를 실행해야 합니다.

공유 암호를 수동으로 롤오버하려면 다음 중 하나를 사용하십시오.

- 관리 UI
- 대상 정책 저장소가 구성된 정책 서버에서 실행 중인 C 정책 관리 API

참고: 공유 암호 정책 개체는 키 저장소에 보관됩니다. 동일한 키 저장소를 공유하는 모든 정책 저장소는 동일한 암호를 공유합니다. 공유 암호 자체는 정책 저장소의 일부인 트러스트된 호스트 개체에 보관됩니다.

트러스트된 호스트의 공유 암호 롤오버 구성

정책 서버는 트러스트된 호스트의 공유 암호에 대한 수동 롤오버와 정기적 롤오버를 지원합니다.

정기적 롤오버는 시간, 일, 주 또는 월 단위로 구성할 수 있습니다. 1 시간이 허용되는 최소 롤오버 간격입니다. 정책 서버는 일, 주 또는 월의 특정 시간이 아니라 각 트러스트된 호스트의 공유 암호 사용 기간을 기반으로 정기적 롤오버를 시작합니다. 각 공유 암호가 만료될 때 롤오버하면 롤오버와 관련된 처리가 시간적으로 분산되므로 정책 서버의 처리 부하가 높아지지 않도록 할 수 있습니다.

수동 롤오버는 공유 암호 롤오버를 허용하는 모든 트러스트된 호스트에 대해 새 공유 암호를 설정하므로 수동 롤오버 기능을 사용할 경우 일반적으로 모든 트러스트된 호스트에 대해 이후의 정기적 롤오버가 함께 클러스터됩니다.

중요! 단일 정책 저장소와 연결된 여러 정책 서버에서 키 생성이 사용되도록 설정할 경우 개체 저장소 전파 지연으로 인해 짧은 기간에 동일한 공유 암호가 두 번 이상 롤오버될 수 있습니다. 이로 인해 새 공유 암호가 삭제된 고아 호스트가 발생할 수 있습니다. 이 잠재적인 문제를 방지하려면 각 정책 저장소마다 단일 정책 서버에 대한 공유 암호 롤오버가 사용되도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔의 "키" 탭에서 "에이전트 키 생성 사용" 확인란이 선택되어 있는지 확인합니다.
2. 관리 UI 에 로그인합니다.
3. "관리", "정책 서버", "공유 암호 롤오버"를 차례로 클릭합니다.
4. "공유 암호 롤오버" 그룹 상자에서 다음 중 하나를 수행합니다.
   - 즉시 롤오버하려면 "지금 롤오버"를 클릭합니다.
   - 공유 암호가 롤오버되지 않도록 하려면 "공유 암호 롤오버 안 함"을 선택합니다.
   - 정기적 롤오버를 지정하려면 "다음마다 공유 암호 롤오버"를 선택하고 다음 필드에 값을 입력합니다.

     롤오버 빈도

     롤오버 기간의 수를 정수로 입력합니다. 이 숫자는 롤오버 기간 값과 함께 적용됩니다.

     롤오버 기간

     풀다운 목록에서 롤오버 수행 간격의 단위를 "시간", "일", "주" 또는 "월"로 선택합니다.

   공유 암호 롤오버를 허용하도록 구성된 모든 트러스트된 호스트에 대해 공유 암호 롤오버 프로세스가 시작됩니다. 배포 환경에 포함된 트러스트된 호스트의 수에 따라 롤오버에 약간의 시간이 소요될 수 있습니다.
5. "제출"을 클릭하여 변경 내용을 저장합니다.

제 9 장: 정책 서버 프로파일러 구성

이 섹션은 다음 항목을 포함하고 있습니다.

정책 서버 프로파일러 구성

정책 서버 프로파일러를 사용하여 내부 정책 서버 진단 및 처리 기능을 추적할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 시작합니다.

   중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "프로파일러" 탭을 클릭합니다.
3. 프로파일링을 사용하도록 "프로파일링 사용" 옵션을 설정합니다.
4. 프로파일러의 구성 설정을 선택하려면 다음 중 하나를 수행합니다.
   - "구성 파일" 드롭다운 목록에 있는 기본 smtracedefault.txt 파일에 지정된 프로파일러 설정을 그대로 사용합니다.
   - "구성 파일" 드롭다운 목록에서 이 관리 세션 중에 이미 선택된 다른 구성 파일을 선택합니다.
   - "찾아보기" 단추를 클릭하여 다른 구성 파일을 선택합니다.
5. 프로파일러 구성 파일에 저장된 프로파일러 설정을 변경한 후 동일한 파일이나 새 파일에 저장하려면 "설정 구성" 단추를 클릭하여 "정책 서버 프로파일러" 대화 상자를 엽니다.
6. "출력" 그룹 상자에 있는 설정을 조정하여 정책 서버 프로파일러에서 생성되는 정보의 출력 형식을 지정합니다.
7. "적용"을 클릭하여 변경 내용을 저장합니다.

참고:

프로파일러 설정에 대한 변경 내용은 자동으로 적용됩니다. 그러나 정책 서버를 다시 시작하면 새 출력 파일이 생성됩니다(프로파일러의 출력 형식이 파일로 구성된 경우). 기존 프로파일러 출력 파일은 버전 번호를 포함하여 자동으로 저장됩니다. 예를 들면 다음과 같습니다.

```
smtracedefault.log.1
```

Windows 에서 콘솔 로깅을 사용하거나 사용하지 않도록 설정할 때처럼 로깅 또는 추적 기능 설정에 대해 변경한 내용이 프로파일 출력 파일과 관련이 없는 경우 하나의 파일 버전이 저장되지 않고 기존 파일에 새 출력이 추가됩니다.

기본적으로 정책 서버는 최대 10 개의 출력 파일(현재 파일과 백업 파일 9 개)을 보존합니다. 파일 제한 10 개에 도달하면 오래된 파일부터 자동으로 최신 파일로 대체됩니다. TraceFilesToKeep DWORD 레지스트리 설정을 필요한 10 진수 값으로 구성하여 보존할 파일 수를 변경할 수 있습니다. TraceFilesToKeep 레지스트리 설정은 다음 레지스트리 위치에 생성해야 합니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\
LogConfig\TraceFilesToKeep
```

"프로파일러" 탭에 있는 "추적 버퍼링" 옵션은 정책 서버 성능을 높이기 위해 기본적으로 설정되어 있습니다. 이 옵션은 Solaris 시스템에만 해당됩니다.

프로파일러 설정 변경

정책 서버 추적에 포함해야 할 구성 요소 및 데이터 필드를 지정할 수 있습니다. 그런 다음 프로파일러에서 지정된 구성 요소 또는 데이터 필드의 특정 값만 캡처하도록 추적 출력에 필터를 적용할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 시작합니다.

   중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "프로파일러" 탭을 클릭합니다.

   참고: 이 탭의 설정과 컨트롤에 대한 자세한 내용을 보려면 "도움말", "관리 콘솔 도움말"을 차례로 클릭하십시오.

3. "설정 구성" 단추를 클릭합니다.

   참고: 이 단추는 "프로파일링 사용" 확인란을 선택한 경우에만 활성화됩니다.

   "정책 서버 프로파일러" 대화 상자가 열립니다.

4. 필요한 경우 "템플릿" 드롭다운 목록에서 특정 추적 태스크에 대해 미리 정의된 구성 요소 및 데이터 필드 집합이 포함되어 있는 프로파일러 템플릿 파일을 선택합니다.

   general_trace.template

   일반적이고 광범위한 추적 옵션을 제공합니다.

   authentication_trace.template

   사용자 인증 추적을 위한 옵션을 제공합니다.

   authorization_trace.template

   사용자 권한 부여 추적을 위한 옵션을 제공합니다.

   samlidp_trace.template

   SAML 아이덴티티 공급자 어설션 추적을 위한 옵션을 제공합니다.

   samlsp_trace.template

   SAML 서비스 공급자 인증 추적을 위한 옵션을 제공합니다.

   프로파일러 구성을 시작할 때 프로파일러 템플릿을 사용할 수 있습니다. 템플릿이 로드되면 템플릿에 지정된 구성 요소 및 데이터 필드를 수동으로 수정하고 데이터 필터를 적용할 수 있습니다.

5. 다음 중 하나 이상을 수행하여 추적 옵션을 검토하고 구성합니다.

   - 구성 요소 선택--추적할 구성 요소, 즉 정책 서버가 실행하는 작업을 "구성 요소" 탭에 지정합니다.
   - 데이터 필드 선택--추적할 데이터 필드, 즉 정책 서버가 태스크를 완료하기 위해 사용하는 실제 데이터 부분을 "데이터" 탭에 지정합니다.
   - 필터 추가--특정 정보를 추적 프로세스에 포함하거나 추적 프로세스에서 제외하는 데이터 필터를 "필터" 탭에 지정합니다.

6. 새 설정을 저장하려면 다음 중 하나를 수행합니다.
   - 현재 선택된 구성 파일에 설정을 저장하려면 "확인"을 클릭합니다.
   - 새 구성 파일에 설정을 저장하려면 "파일", "다른 이름으로 저장"을 차례로 선택하고 새 텍스트 파일을 지정합니다.
7. "파일", "닫기"를 차례로 선택하여 프로파일러를 닫고 정책 서버 관리 콘솔로 돌아갑니다.
8. "구성 파일" 필드 오른쪽의 "찾아보기" 단추를 선택합니다.

Windows 에서 프로파일러 콘솔 출력 문제 방지

Windows 정책 서버에서는 "빠른 편집 모드"와 "삽입 모드"가 사용되지 않도록 설정하여 콘솔 디버깅을 사용할 때 문제가 발생하지 않도록 해야 합니다. "빠른 편집 모드" 및 "삽입 모드" 기능은 Windows 명령 프롬프트 창에서 사용할 수 있습니다.

"빠른 편집 모드" 및 "삽입 모드"가 사용되지 않도록 설정하려면

1. 명령 프롬프트 창에 액세스합니다.
2. 창의 제목 표시줄을 마우스 오른쪽 단추로 클릭하여 풀다운 메뉴를 표시합니다.
3. "속성"을 선택합니다.
4. "빠른 편집 모드" 및 "삽입 모드"가 선택되어 있으면 선택 취소합니다.
5. "확인"을 클릭합니다.

프로파일러 추적 파일 보존 정책 구성

기본적으로 정책 서버는 최대 10 개의 출력 파일(현재 파일과 백업 파일 9 개)을 보존합니다. 파일 제한 10 개에 도달하면 오래된 파일부터 자동으로 최신 파일로 대체됩니다. TraceFilesToKeep DWORD 레지스트리 설정을 필요한 10 진수 값으로 구성하여 보존할 파일 수를 변경할 수 있습니다. TraceFilesToKeep 레지스트리 설정은 다음 레지스트리 위치에 생성해야 합니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\LogConfig\
TraceFilesToKeep
```

수동으로 프로파일러 추적 로그 파일 롤오버

정책 서버에서 smpolicysrv 명령을 사용하여 정책 서버 프로파일러 추적 로그 파일을 수동으로 롤오버할 수 있습니다.

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

파일에 대한 추적 로깅을 시작하려면 다음 명령을 실행하십시오.

```
smpolicysrv -starttrace
```

이 명령은 추적 파일에 대한 로깅을 시작하며 콘솔에 대한 추적 로깅에는 영향을 주지 않습니다. 정책 서버가 실행 중이 아니면 오류가 발생합니다.

정책 서버가 이미 추적 데이터를 로깅 중인 경우 -starttrace 명령을 실행하면 정책 서버는 현재 추적 파일의 이름을 타임스탬프가 추가된 *file_name*.YYYYMMDD_HHmmss.*extension* 형식의 이름으로 변경하고 원래 이름으로 새 추적 파일을 생성합니다. 예를 들어 정책 서버 관리 콘솔의 "프로파일러" 탭에 있는 추적 파일 이름이 C:\temp\smtrace.log 인 경우 새 파일이 생성되고 이전 파일은 c:\temp\smtrace.20051007_121807.log 로 저장됩니다. 타임스탬프는 정책 서버가 이 파일을 2005 년 10 월 7 일 오후 12:18 에 생성했음을 나타냅니다.

정책 서버 관리 콘솔의 "프로파일러" 탭을 사용하여 파일 추적 기능이 사용되도록 설정하지 않은 경우에는 이 명령을 실행해도 아무런 효과가 없습니다.

파일에 대한 추적 로깅을 중지하려면 다음 명령을 실행하십시오.

```
smpolicysrv -stoptrace
```

이 명령은 파일에 대한 로깅을 중지하며 콘솔에 대한 추적 로깅에는 영향을 주지 않습니다. 정책 서버가 실행 중이 아니면 오류가 발생합니다.

참고: Windows 시스템의 경우 원격 데스크톱 또는 터미널 서비스 창에서 smpolicysrv 명령을 실행하지 *마십시오*. smpolicysrv 명령을 실행하려면 프로세스 간 통신이 필요하며 smpolicysrv 프로세스를 원격 데스크톱 또는 터미널 서비스 창에서 실행할 경우에는 프로세스 간 통신이 작동하지 않습니다.

지정된 간격으로 동적 추적 파일 롤오버

추적 파일이 지정된 간격으로 롤오버되도록 스크립트를 작성할 수도 있습니다. 예를 들어 새 추적 파일을 매시간 생성하려면 스크립트를 다음과 같이 작성하십시오.

```
smpolicysrv -starttrace
repeat forever
wait 1 hour
smpolicysrv -starttrace
end repeat
```

이 스크립트는 정책 서버 관리 콘솔의 "로그" 탭에 있는 시간 기반 롤오버 옵션과 유사합니다.

제 10 장: 관리 저널 및 이벤트 처리기 구성

관리 저널 및 이벤트 처리기 개요

정책 서버 관리 저널을 구성하여 관리 변경 내용이 정책 서버에 적용되는 빈도와 정책 서버에서 적용된 변경 내용의 목록이 유지되는 기간을 지정할 수 있습니다.

이벤트 처리기는 특정 이벤트를 처리하기 위해 정책 서버에 추가할 수 있는 공유 라이브러리입니다.

정책 서버에 대한 고급 설정 구성

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 시작합니다.

   중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "고급" 탭을 클릭합니다.

   참고: 이 탭의 설정과 컨트롤에 대한 자세한 내용을 보려면 "도움말", "관리 콘솔 도움말"을 차례로 클릭하십시오.

3. "관리 저널" 그룹 상자에 있는 설정을 조정하여 관리 변경 내용이 정책 서버에 적용되는 빈도와 정책 서버에서 적용된 변경 내용의 목록이 유지되는 기간을 구성합니다.

4. "적용"을 클릭하여 변경 내용을 저장합니다.

이벤트 처리기 라이브러리 추가

SiteMinder 정책 서버에 이벤트 처리기 라이브러리를 추가할 수 있습니다.

참고: 사용자에게 SiteMinder 바이너리 파일(XPS.dll, libXPS.so, libXPS.sl)에 대한 쓰기 액세스 권한이 *없다면* 관리자가 관리 UI 또는 XPSSecurity 도구를 사용하여 관련 XPS 명령줄 도구를 사용할 수 있는 권한을 사용자에게 부여해야 합니다.

다음 단계를 수행하십시오.

1. 정책 서버에서 명령줄을 열고 다음 명령을 입력합니다.

   ```
   xpsconfig
   ```

   이 도구가 시작되어 이 세션에 대한 로그 파일 이름이 표시되고 선택 메뉴가 열립니다.

2. 다음을 입력합니다.

   ```
   xps
   ```

   옵션 목록이 나타납니다.

3. 다음을 입력합니다.

   ```
   5 (AuditSMHandlers)
   ```

   이벤트 처리기 라이브러리에 대한 설정이 표시됩니다.

4. C 를 입력하고 추가할 이벤트 처리기 라이브러리의 경로 및 파일 이름을 입력합니다. 라이브러리 위치가 여러 개인 경우 쉼표로 구분합니다.

   이벤트 처리기 라이브러리에 대한 설정이 표시됩니다. 추가한 값은 설정 맨 아래에 "보류 중인 값"으로 표시됩니다.

5. 다음 작업을 수행하십시오.

   a. Q 를 두 번 입력합니다.

   b. L 을 입력합니다.

   c. Q 를 입력하여 XPS 세션을 종료합니다.

   변경 내용이 저장되고 명령 프롬프트가 표시됩니다.

추가 정보:

정책 서버 관리 콘솔을 열 때 이벤트 처리기 목록 설정에 대한 경고가 발생함 (페이지 331)

제 11 장: 전역 설정 조정

이 섹션은 다음 항목을 포함하고 있습니다.

사용자 추적 사용

정책 서버 "전역 도구" 태스크를 통해 사용자 추적을 사용하거나 사용하지 않도록 설정할 수 있습니다. 사용자 추적이 사용되도록 설정할 경우 SiteMinder 웹 에이전트는 쿠키에 GUID(전역 고유 식별자)를 저장합니다. 사용자가 익명 인증 체계로 보호된 리소스에 처음 액세스할 때 웹 에이전트는 사용자의 GUID 가 포함된 쿠키를 생성합니다. 각 GUID 는 고유한 값이므로 익명 사용자를 추적하고 웹 콘텐츠를 사용자 지정하는 데 사용될 수 있습니다.

가맹 에이전트에는 사용자 추적이 필요합니다. 가맹 에이전트가 포함된 네트워크에서 SiteMinder 를 사용하려면 다음 절차에 설명된 대로 사용자 추적이 사용되도록 설정해야 합니다.

사용자 추적이 사용되도록 설정하려면

1. 관리 UI 에 로그인합니다.
2. "관리", "정책 서버", "전역 도구"를 차례로 클릭합니다.

   "전역 도구" 창이 열립니다.
3. "전역 설정" 그룹 상자에서 "사용자 추적 사용"을 선택합니다.
4. 제출을 클릭합니다.

   사용자 추적이 사용되도록 설정됩니다.

중첩된 보안 사용

이전 버전 SiteMinder 와의 호환성을 제공하는 중첩된 보안이 사용되거나 사용되지 않도록 설정할 수 있습니다.

중첩된 보안 옵션이 사용되도록 설정하려면

1. 관리 UI 에 로그인합니다.
2. "관리", "정책 서버", "전역 도구"를 차례로 클릭합니다.

   "전역 도구" 창이 열립니다.
3. "중첩된 보안 사용" 확인란을 선택합니다.
4. 제출을 클릭합니다.

   중첩된 보안이 사용되도록 설정됩니다.

개선된 Active Directory 통합 기능이 사용되도록 설정하는 방법

개선된 Active Directory 통합 기능이 사용되도록 설정하려면 다음 세 단계를 수행해야 합니다.

1. IgnoreADpwdLastSet 레지스트리 키 만들기
2. 개선된 Active Directory 통합 기능이 사용되도록 설정
3. 사용자 디렉터리 연결 구성

IgnoreADpwdLastSet 레지스트리 키 만들기

사용 중인 Active Directory 버전에 pwdLastSet 특성이 포함되어 있지 않은 경우 정책 서버 레지스트리 키 IgnoreADpwdLastSet 을 생성하십시오.

중요! pwdLastSet 특성이 정의되지 않은 설치 환경에 대해서만 IgnoreADpwdLastSet 레지스트리 키를 생성하고 값을 1 로 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 액세스하여 다음 단계 중 하나를 완료합니다.
   - (Windows) 레지스트리 편집기를 열고 다음 위치로 이동합니다.

     `SiteMinder\CurrentVersion\Ds\LDAPProvider`
   - (UNIX) sm.registry 파일을 엽니다. 이 파일의 기본 위치는 siteminder_home/registry 입니다.

     siteminder_home

     정책 서버 설치 경로를 지정합니다.
2. 레지스트리 값 종류를 REG_DWORD 로 지정하여 IgnoreADpwdLastSet 을 생성합니다.

   값: 1
3. 다음 단계 중 하나를 수행합니다.
   - (Windows) 레지스트리 편집기를 종료합니다.
   - (UNIX) sm.registry 파일을 저장합니다.
4. 정책 서버를 다시 시작합니다.

개선된 Active Directory 통합 기능이 사용되도록 설정

Active Directory 2008 에는 Windows NOS(네트워크 운영 체제)와 관련되고 LDAP 표준에는 필요하지 않은 사용자 및 도메인 특성이 여러 개 있습니다. 이러한 특성은 다음과 같습니다.

- accountExpires
- userAccountControl
- pwdLastSet

- unicodePwd
- lastLogon
- lastLogonTimestamp
- badPasswordTime
- badPwdCount
- lockoutTime
- lockoutDuration
- pwdMaxAge

Active Directory 를 사용자 저장소로 사용하도록 정책 서버를 구성할 경우 관리 UI 의 정책 서버 "전역 도구" 태스크에서 개선된 Active Directory 통합 기능이 사용되도록 설정하십시오. 이 옵션을 사용하면 Active Directory 사용자 특성을 SiteMinder 의 매핑된 사용자 특성과 동기화하여 정책 서버의 사용자 관리 기능 및 암호 서비스와 Active Directory 간의 통합이 개선됩니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "관리", "정책 서버", "전역 도구"를 차례로 클릭합니다.

   "전역 도구" 창이 열립니다.
3. "Active Directory 통합 개선"을 선택합니다. 기본적으로 이 기능은 사용되지 않도록 설정되어 있습니다.

   참고: 이 기능이 사용되도록 설정한 후 AD 사용자 저장소를 수정하려면 관리자 자격 증명이 있어야 하고 AD 특성을 업데이트할 수 있는 권한이 있어야 합니다. 이러한 자격 증명과 권한이 없는 경우 오류 메시지가 반환됩니다.
4. "제출"을 클릭합니다.

   개선된 Active Directory 통합 기능이 사용되도록 설정됩니다.
5. "인프라" 탭의 "사용자 디렉터리" 대화 상자로 이동합니다.
6. 편집할 Active Directory 개체를 엽니다.

7. "루트" 필드에 사용자 디렉터리 루트로 기본 Windows 도메인의 DN 을 입력합니다. 예를 들면 다음과 같습니다.

   ```
   dc=WindowsDomain,dc=com
   ```

   참고: "루트" 필드를 다른 값으로 설정할 경우 AD 관련 기능이 작동하지 않을 수 있습니다.

8. "제출"을 클릭합니다.

사용자 디렉터리 연결 구성

개선된 Active Directory 통합 기능이 사용되도록 설정한 후에는 사용자 디렉터리 연결을 구성하십시오.

다음 단계를 수행하십시오.

1. "인프라", "디렉터리"를 차례로 클릭합니다.
2. "사용자 디렉터리"를 클릭합니다.
3. "사용자 디렉터리 만들기"를 클릭합니다.

   "사용자 디렉터리 만들기" 페이지가 나타나고 LDAP 연결을 구성하는 데 필요한 설정이 표시됩니다.

4. "일반" 및 "디렉터리 설정" 섹션에서 필요한 연결 정보를 지정합니다.

   참고: 정책 서버가 FIPS 모드에서 작동 중이며 정책 서버와 통신할 때 디렉터리 연결이 보안 SSL 연결을 사용할 경우 정책 서버와 디렉터리 저장소가 사용하는 인증서는 FIPS 를 준수해야 합니다.

5. (선택 사항) "관리자 자격 증명" 섹션에서 다음 작업을 수행합니다.

   1. "자격 증명 필요"를 선택합니다.
   2. 관리자 계정의 자격 증명을 입력합니다.

6. "LDAP 설정" 섹션에서 "LDAP 검색" 및 "LDAP 사용자 DN 조회" 설정을 구성합니다.

LDAP 사용자 DN 조회

LDAP 사용자 저장소에서 사용자를 찾기 위한 매개 변수를 지정합니다.

시작

LDAP 검색 식 또는 사용자 DN의 시작을 나타내는 텍스트 문자열을 지정합니다. 사용자가 로그인을 시도할 때 정책 서버는 이 문자열을 사용자 이름의 맨 앞에 추가합니다.

값: (sAMAccountName=

7. "사용자 특성" 섹션에서 다음 특성에 대해 지정된 값을 설정합니다.

유니버설 ID

SiteMinder 가 유니버설 ID 로 사용하는 특성의 이름을 지정합니다.

값: sAMAccountName

비활성화된 플래그

사용자의 비활성화된 상태를 유지하는 사용자 디렉터리 특성의 이름을 지정합니다.

값: carLicense(또는 임의의 정수 특성)

암호

SiteMinder 가 사용자의 암호를 인증하는 데 사용해야 하는 사용자 디렉터리 특성의 이름을 지정합니다.

값: unicodePwd

암호 데이터

SiteMinder 가 암호 서비스 데이터에 사용할 수 있는 사용자 디렉터리 특성의 이름을 지정합니다.

값: audio

"암호 데이터"의 값은 큰 바이너리 특성일 수 있습니다. 이 값은 기본 암호 서비스를 사용하는 경우에만 필요합니다.

참고: 다른 필드에 대한 자세한 내용은 *관리 UI 도움말*을 참조하십시오.

8. (선택 사항) "특성 매핑 목록" 섹션의 "만들기"를 클릭하여 사용자 특성 매핑을 구성합니다.
9. 제출을 클릭합니다.

   사용자 디렉터리 연결이 생성됩니다.

제 12 장: 캐시 관리

이 섹션은 다음 항목을 포함하고 있습니다.

캐시 관리 개요

SiteMinder 에서는 여러 캐시를 제공하며 이러한 캐시에 사용자 권한 부여 같이 최근에 액세스한 데이터의 복사본을 보관하도록 구성하여 시스템 성능을 향상시킬 수 있습니다. 이러한 캐시는 사용 환경의 데이터 특성에 맞게 구성해야 하지만 정기적인 수동 플러시가 필요할 수도 있습니다.

정책 서버에 다음 캐시를 보관하도록 SiteMinder 배포 환경을 구성할 수 있습니다.

- *사용자 권한 부여 캐시* - 정책의 사용자 부분을 기반으로 사용자 DN(고유 이름)을 저장하며 사용자의 그룹 구성원 자격을 포함합니다.

또한 SiteMinder 에서는 각 SiteMinder 에이전트 컴퓨터에 *에이전트 캐시*도 보관합니다. 에이전트 캐시에는 다음 두 개의 구성 요소가 있습니다.

- *에이전트 리소스 캐시* - 다양한 영역으로 보호되는 액세스한 리소스의 레코드를 저장합니다. 에이전트는 이미 요청을 처리한 리소스를 인식하므로 이 캐시는 에이전트와 정책 서버 간의 통신을 빠르게 해 줍니다.
- *에이전트 사용자 캐시* - 사용자의 암호화된 세션 티켓을 보관합니다. 이 캐시는 사용자, 영역 및 리소스 정보를 저장하는 세션 캐시의 역할을 합니다. 이 캐시의 항목은 사용자가 액세스하는 영역에서 설정된 만료 시간에 따라 무효화됩니다.

캐시 업데이트 관리

캐시 플러시 업데이트를 일시 중단했다가 다시 시작하여 정책 평가 문제를 해결할 수 있습니다. 관리 UI 또는 smpolicysrv 명령을 사용하여 캐시 업데이트를 관리할 수 있습니다.

캐시 업데이트 상태를 변경하면 중앙 관리 정책 서버는 모든 보조 정책 서버에 대해 해당 명령을 실행합니다.

참고: 정책 서버 명령은 스레드 관리 모델에 따라 처리됩니다. 따라서 캐시 상태에 대한 변경 내용은 smps.log 파일에 즉시 표시되지 않습니다.

관리 UI 를 사용하여 캐시 업데이트 관리

관리 UI 를 사용하여 정책 서버 캐시 플러시 업데이트의 상태를 확인하고 업데이트를 사용하거나 사용하지 않도록 설정할 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "관리", "정책 서버", "캐시 관리"를 차례로 클릭합니다.
3. "캐시 업데이트" 섹션에서 캐시 상태를 확인합니다.

   캐시 업데이트 사용 안 함: 캐시 플러시를 사용하지 않습니다.

   캐시 업데이트 사용: 캐시 플러시를 사용합니다.
4. (선택 사항) "사용"/"사용 안 함" 단추를 클릭하여 캐시 업데이트의 사용 여부를 전환합니다.

smpolicysrv 명령을 사용하여 캐시 업데이트 관리

smpolicysrv 명령을 사용하여 정책 서버 캐시 플러시 업데이트의 상태를 확인하고 업데이트를 사용하거나 사용하지 않도록 설정할 수 있습니다.

다음 단계를 수행하십시오.

1. 명령 프롬프트를 엽니다.

   Windows 시스템에서는 다음 사항을 고려하십시오.

   - 원격 데스크톱 또는 터미널 서비스 창에서 smpolicysrv 명령을 실행하지 마십시오. 이 명령은 프로세스 간 통신에 의존합니다. smpolicysrv 프로세스를 원격 데스크톱 또는 터미널 서비스 창에서 실행할 경우 이러한 통신이 작동하지 않습니다.
   - 명령줄 창은 관리자 권한으로 열어야 합니다. 관리자로 시스템에 로그인한 경우에도 이 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. 다음 명령 중 하나를 입력합니다.

smpolicysrv -disablecacheupdates

캐시 플러시가 사용되지 않도록 설정합니다.

smpolicysrv -enablecacheupdates

캐시 플러시가 사용되도록 설정합니다.

smpolicysrv -statuscacheupdates

정책 서버 캐시의 새로 고침 상태를 smps.log 로그 파일에 보고합니다.

Disabled: 캐시 플러시를 사용하지 않습니다.

Enabled: 캐시 플러시를 사용합니다.

캐시 플러시

SiteMinder 개체를 변경할 경우 SiteMinder 는 해당 캐시 항목을 자동으로 플러시합니다. 캐시 설정은 정기적으로 관리 변경 내용을 적용할 간격도 지정합니다. 매우 중요한 정보에 대한 액세스 권한을 변경하는 등 중요한 변경 작업을 수행할 경우 SiteMinder 캐시를 수동으로 플러시할 수 있습니다. 이 수동 단계는 권한이 없는 사용자가 캐시에 저장된 정보를 기반으로 보호된 리소스에 액세스할 수 없도록 하는 데 유용합니다.

캐시 관리 기능은 관리 UI 의 정책 서버 "전역 도구" 창에서 액세스할 수 있습니다. 캐시 관리 기능으로 다음 캐시를 수동으로 플러시하여 SiteMinder 데이터를 강제로 업데이트할 수 있습니다.

모든 캐시

사용자 세션, 리소스 정보 및 사용자 디렉터리용 캐시(인증서 CRL 포함)를 비롯한 모든 캐시를 플러시할 수 있습니다.

사용자 세션 캐시

사용자가 보호된 리소스에 액세스하려고 할 때 사용자가 다시 인증되도록 할 수 있습니다.

리소스 캐시

리소스에 대한 캐시된 정보를 플러시할 수 있습니다.

모든 캐시 플러시

관리자는 "캐시 관리" 옵션을 사용하여 모든 캐시의 내용을 플러시할 수 있습니다. 모든 캐시를 플러시할 경우 캐시 플러시 직후의 모든 요청에서는 사용자 디렉터리와 정책 저장소에서 정보를 가져와야 하므로 웹 사이트의 성능이 저하될 수 있습니다. 그러나 중요한 사용자 권한 및 정책 변경 내용을 즉시 적용해야 할 경우에는 이 작업이 필요할 수 있습니다.

"캐시 관리" 기능은 사용자 관리 권한이나 시스템 및 도메인 개체 관리 권한이 있는 관리자만 사용할 수 있습니다. "모두 플러시" 단추는 시스템 및 도메인 개체 관리 권한이 있는 관리자만 사용할 수 있습니다. 이 메뉴 선택 항목은 로그인하는 데 사용한 계정에 캐시 기능에 액세스할 수 있는 충분한 권한이 있는 경우에만 표시됩니다.

모든 캐시를 플러시하려면

1. 관리 UI 에 로그인합니다.
2. "관리", "정책 서버", "캐시 관리"를 차례로 클릭합니다.
3. "모든 캐시" 그룹 상자에서 "모두 플러시"를 클릭합니다.

   참고: "모두 플러시" 단추는 사용자 관리 권한과 SiteMinder 개체 관리 권한이 모두 있는 관리자만 사용할 수 있습니다.

   정책 서버와 관련 SiteMinder 에이전트가 모든 캐시를 플러시합니다. 이 프로세스에는 정책 서버가 캐시를 동기화하는 동안 정책 서버 폴링 간격 시간의 두 배까지 소요될 수 있습니다.
4. "제출"을 클릭합니다.

   모든 캐시가 삭제됩니다.

사용자 세션 캐시 플러시

사용자가 성공적으로 인증되면 정책 서버는 인증된 사용자에 대한 세션을 시작합니다. 세션 도중 웹 에이전트는 권한 부여 정보를 사용자 캐시에 저장됩니다.

다음 사항을 고려하십시오.

- 사용자 액세스 권한을 변경하는 경우 정책 서버가 웹 에이전트 캐시에서 사용자 세션 정보를 플러시하도록 설정해야 할 수 있습니다.
- 사용자 캐시를 플러시하는 옵션은 사용자 관리 권한이 있는 관리자만 사용할 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "관리", "정책 서버", "캐시 관리"를 차례로 클릭합니다.
3. "사용자 세션 캐시" 섹션에서 다음 옵션 중 하나를 선택합니다.

   모두

   사용자 캐시에서 모든 사용자 세션을 플러시합니다.

   특정 사용자 DN

   사용자 캐시에서 특정 DN 을 플러시합니다.

   이 옵션을 선택하는 경우:

   a. 제거할 DN 이 포함된 사용자 디렉터리를 디렉터리 목록에서 선택합니다.

   b. DN 필드에 고유 이름을 입력합니다. 그룹의 DN 이 아니라 사용자 DN 을 지정합니다. DN 을 모르는 경우 "조회"를 클릭하고 DN 을 검색합니다.

4. "플러시"를 클릭합니다.

   SiteMinder 가 사용자 캐시에서 해당 사용자를 플러시합니다. 이 프로세스의 경우 정책 서버가 캐시를 동기화하는 동안 정책 서버 폴링 간격으로 지정된 시간보다 두 배까지 소요될 수 있습니다.

5. "제출"을 클릭합니다.

   사용자 세션 캐시가 지워집니다.

리소스 캐시 플러시

SiteMinder 웹 에이전트는 사용자가 액세스하는 특정 리소스에 대한 정보를 리소스 캐시에 저장합니다. 리소스 캐시에는 다음 내용이 기록됩니다.

- 사용자가 액세스한 리소스에 대한 레코드
- 리소스가 SiteMinder 에서 보호되는지 여부
- 리소스가 보호되는 경우 리소스의 보호 방식

규칙 또는 영역을 변경한 후 변경 내용을 즉시 적용하려는 경우가 있을 수 있습니다. 이 경우 리소스 캐시를 플러시해야 합니다.

참고: 영역 또는 특정 정책의 리소스 캐시 플러시에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

리소스 캐시를 플러시하려면

1. 관리 UI 에 로그인합니다.
2. "관리", "정책 서버", "캐시 관리"를 차례로 클릭합니다.
3. "리소스 캐시" 그룹 상자에서 "플러시"를 클릭합니다.

   그러면 모든 리소스 캐시가 플러시되고 웹 에이전트가 정책 서버에 대한 요청에 권한을 부여하게 됩니다. 이 프로세스에는 정책 서버가 캐시를 동기화하는 동안 정책 서버 폴링 간격 시간에 지정된 시간의 두 배까지 소요됩니다.

   참고: 특정 정책 도메인에 대한 도메인 개체 관리 권한을 가진 관리자의 경우 모든 리소스 캐시를 플러시해도 관리자의 정책 도메인 내에 있는 영역의 캐시만 플러시됩니다.
4. "제출"을 클릭합니다.

   리소스 캐시가 지워집니다.

정책 서버의 요청 큐 플러시

SiteMinder 에이전트의 요청은 일정 간격 이후 시간 만료되도록 설정되어 있습니다. 그러나 정책 서버는 시간 만료된 요청을 포함하여 큐에 있는 모든 에이전트 요청을 받은 순서대로 계속 처리합니다. 다음과 같은 경우 정책 서버가 처리할 수 있는 것보다 빠른 속도로 큐에 에이전트 요청이 채워질 수 있습니다.

- 정책 서버와 정책 저장소 또는 사용자 저장소 데이터베이스 간에 네트워크 지연이 있는 경우
- 정책 저장소 또는 사용자 저장소 데이터베이스의 부하가 높은 경우
- 정책 서버에 성능 문제가 있는 경우

정책 서버가 에이전트 요청으로 채워진 큐를 요청할 경우 현재 에이전트 요청만 유지되도록 시간 만료된 에이전트 요청을 캐시에서 플러시할 수 있습니다. 이 절차는 다음과 같은 경우에만 수행하십시오.

1. 정책 서버 큐에서 대기 중인 에이전트 요청이 시간 만료된 경우
2. 하나 이상의 에이전트가 시간 만료된 요청을 다시 보내 큐가 넘치는 경우

중요! 정상 작동 상태에서는 -flushrequests 를 사용하지 마십시오.

정책 서버의 요청 큐를 플러시하려면

1. 정책 서버에서 명령 프롬프트를 엽니다.
2. 다음 명령을 실행합니다.

   ```
   smpolicysrv -flushrequests
   ```

   요청 큐가 플러시됩니다.

참고: Windows 시스템의 경우 원격 데스크톱 또는 터미널 서비스 창에서 smpolicysrv 명령을 실행하지 *마십시오*. smpolicysrv 명령을 실행하려면 프로세스 간 통신이 필요하며 smpolicysrv 프로세스를 원격 데스크톱 또는 터미널 서비스 창에서 실행할 경우에는 프로세스 간 통신이 작동하지 않습니다.

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

제 13 장: 사용자 세션 및 계정 관리

이 섹션은 다음 항목을 포함하고 있습니다.

사용자 세션 및 계정 관리 사전 요구 사항

정책 서버는 세션 캐시를 플러시하고 사용자를 활성화 또는 비활성화하고 개별 사용자의 암호를 관리할 수 있는 사용자 세션 및 계정 관리 기능을 제공합니다.

사용자 세션 및 계정을 관리하려면 다음 사전 요구 사항을 충족해야 합니다.

- 사용자 관리 권한이 있는 관리자 계정이 있어야 합니다.
- 사용자 계정을 활성화하거나 비활성화하려면 사용자 정보가 포함된 사용자 디렉터리가 "사용자 비활성화" 특성으로 구성되어 있어야 합니다.
- 암호를 변경하거나 강제로 암호를 변경하게 하려면 정책 서버에 암호 정책이 구성되어 있고 사용자 정보가 포함된 사용자 디렉터리가 "암호 데이터" 특성으로 구성되어 있어야 합니다.

참고: 관리자 권한, 사용자 디렉터리 및 암호 정책 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

사용자 활성화 및 비활성화

사용자가 로그인하고 인증되고 나면 SiteMinder 가 사용자 세션을 시작합니다. SiteMinder 는 사용자 특성을 사용자 세션 캐시에 저장합니다. 사용자를 비활성화하면 에이전트가 세션 캐시를 플러시하여 사용자 ID 및 세션 정보를 제거합니다.

해당 사용자가 현재 세션에서 추가 리소스에 액세스하려고 할 때 웹 에이전트는 캐시에 더 이상 사용자의 데이터가 없으므로 정책 서버에 연결하여 사용자를 다시 인증하려고 시도합니다. 정책 서버는 이 사용자가 사용자 디렉터리에서 비활성화되어 있는지 확인하고 에이전트의 인증 요청을 거부하여 세션을 종료합니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "관리", "사용자", "사용자 계정 관리"를 차례로 클릭합니다.

   "사용자 계정 관리" 창이 열립니다.
3. 활성화 또는 비활성화할 사용자가 포함된 디렉터리의 사용자 디렉터리 연결을 선택합니다.
4. "검색" 아이콘을 클릭합니다.

   "디렉터리 사용자" 창이 표시됩니다.
5. "사용자/그룹" 그룹 상자에 검색 조건을 입력하고 "실행"을 클릭하여 활성화 또는 비활성화할 사용자에 대한 검색을 실행합니다. 검색 조건은 선택한 사용자 디렉터리의 유형에 따라 결정됩니다. 검색 조건은 특성과 값으로 입력하거나 식으로 입력할 수 있습니다. "재설정"을 클릭하면 검색 조건을 지울 수 있습니다.

   검색 결과가 "사용자/그룹" 그룹 상자에 표시됩니다.
6. 결과 목록에서 단일 사용자를 선택합니다.

   "사용자 상태 변경" 그룹 상자에는 단추가 있습니다. 이 단추의 레이블은 비활성화된 사용자의 경우 "사용"으로 표시되고, 활성화된 사용자의 경우 "사용 안 함"으로 표시됩니다.
7. "사용/사용 안 함"을 클릭합니다.

   정책 서버가 선택한 사용자의 프로필에 있는 값을 변경하여 해당 사용자를 비활성화하거나 활성화합니다.

사용자 암호 관리

관리 UI 의 "사용자 계정 관리" 창을 사용하여 사용자의 암호를 변경하도록 하거나 사용자 암호를 새 값으로 변경할 수 있습니다.

사용자가 암호를 변경하도록 하기 전에 암호 정책이 있는지 확인하십시오. 암호 정책이 없는 경우에는 사용자가 암호를 변경할 수 없으므로 보호된 리소스에 액세스할 수 없습니다.

사용자가 암호를 변경하도록 할 경우 사용자가 SSL 연결을 사용하지 않는 에이전트를 통해 리소스에 액세스하려고 하면 비보안 연결을 통해 사용자의 새 암호 정보가 수신됩니다. 암호를 안전하게 변경할 수 있도록 하려면 암호를 변경할 때 SSL 연결을 통해 사용자를 리디렉션하는 암호 정책을 설정하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "관리", "사용자", "사용자 계정 관리"를 차례로 클릭합니다. "사용자 계정 관리" 창이 열립니다.
3. 암호를 관리할 사용자가 포함된 디렉터리의 사용자 디렉터리 연결을 선택합니다.
4. "검색" 아이콘을 클릭합니다.

   "디렉터리" 드롭다운 목록에서 선택한 디렉터리 유형과 관련된 사용자 디렉터리 검색 대화 상자가 표시됩니다.
5. "사용자/그룹" 그룹 상자에 검색 조건을 입력하고 "실행"을 클릭하여 활성화 또는 비활성화할 사용자에 대한 검색을 실행합니다. 검색 조건은 선택한 사용자 디렉터리의 유형에 따라 결정됩니다. 특성과 값을 입력하거나 식을 입력할 수 있습니다. "재설정"을 클릭하면 검색 조건을 지울 수 있습니다.

   검색 결과가 "사용자/그룹" 그룹 상자에 표시됩니다.
6. 결과 목록에서 단일 사용자를 선택합니다.
7. 선택한 사용자가 다음에 로그인할 때 암호를 변경하도록 하려면 "사용자 암호 재설정" 그룹 상자의 "암호 변경 강제"를 클릭합니다.

8. 사용자의 암호를 새 값으로 변경하려면 "사용자 암호 변경" 그룹 상자에 새 암호를 입력합니다. 암호를 확인하기 위해 다시 입력합니다.

   참고: 지정하는 암호는 암호 정책에 의해 제한되지 않지만 사용자의 암호 기록에는 기록됩니다.

사용자 권한 부여 감사

사용자 세션 캐시에 저장된 성공한 권한 부여를 추적하고 로깅하려면 웹 에이전트의 감사 기능을 사용하십시오. 이 기능을 통해 사용자 작업을 추적하고 웹 사이트에서 응용 프로그램이 사용되는 빈도를 측정할 수 있습니다.

이 옵션을 선택할 경우 웹 에이전트는 캐시에서 리소스에 액세스할 수 있는 권한이 사용자에게 부여될 때마다 정책 서버에 메시지를 보냅니다. 그러면 각 SiteMinder 세션에서의 사용자 작업을 보여 주는 로그 보고서를 실행할 수 있습니다.

감사가 사용되도록 설정하지 않을 경우 웹 에이전트는 인증과 첫 번째 권한 부여만 감사합니다.

참고: 감사가 사용되도록 설정하는 방법에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

웹 에이전트는 사용자가 리소스에 액세스할 때 자동으로 사용자 이름 및 액세스 정보를 네이티브 웹 서버 로그 파일에 로깅합니다. 감사 로그에는 웹 에이전트가 성공한 각 사용자 권한 부여 요청에 대해 자동으로 생성하는 고유한 트랜잭션 ID 가 포함됩니다. 또한 에이전트는 SiteMinder 가 리소스에 액세스하는 사용자에게 권한을 부여할 때 이 ID 를 HTTP 헤더에 추가합니다. 그러면 웹 서버의 모든 응용 프로그램에서 이 트랜잭션 ID 를 사용할 수 있습니다. 트랜잭션 ID 는 웹 서버 감사 로그에도 기록됩니다. 이 ID 를 사용하여 로그를 비교하고 특정 응용 프로그램에 대한 사용자 작업을 추적할 수 있습니다.

감사 기능의 출력을 보려면 관리 UI 에서 SiteMinder 보고서를 실행하면 됩니다.

제 14 장: 하드웨어 부하 분산 장치를 사용하여 SiteMinder 에이전트와 정책 서버 간 통신 구성

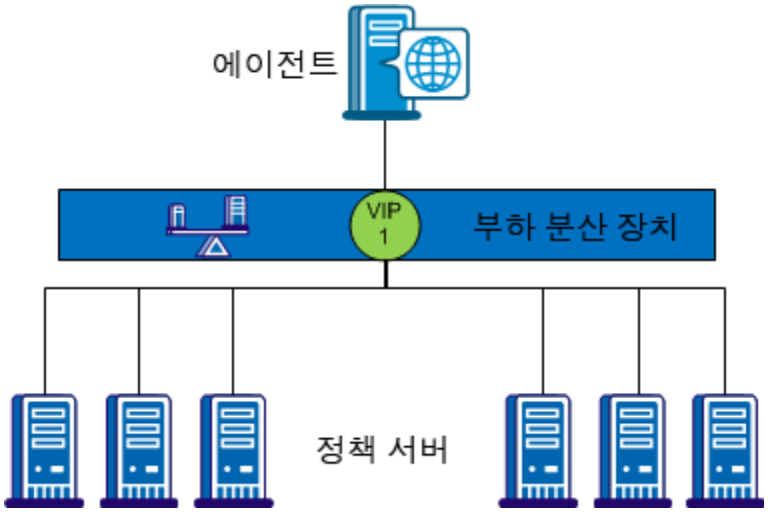
이 섹션은 다음 항목을 포함하고 있습니다.

하드웨어 부하 분산

SiteMinder 에서는 하나 이상의 VIP(가상 IP 주소)를 통해 다중 정책 서버를 노출하도록 구성된 하드웨어 부하 분산 장치를 사용할 수 있도록 지원합니다. 이 경우 하드웨어 부하 분산 장치가 해당 VIP 에 연결된 모든 정책 서버 간에 동적으로 요청 부하를 분산시킵니다. 다음과 같은 하드웨어 부하 분산 구성이 지원됩니다.

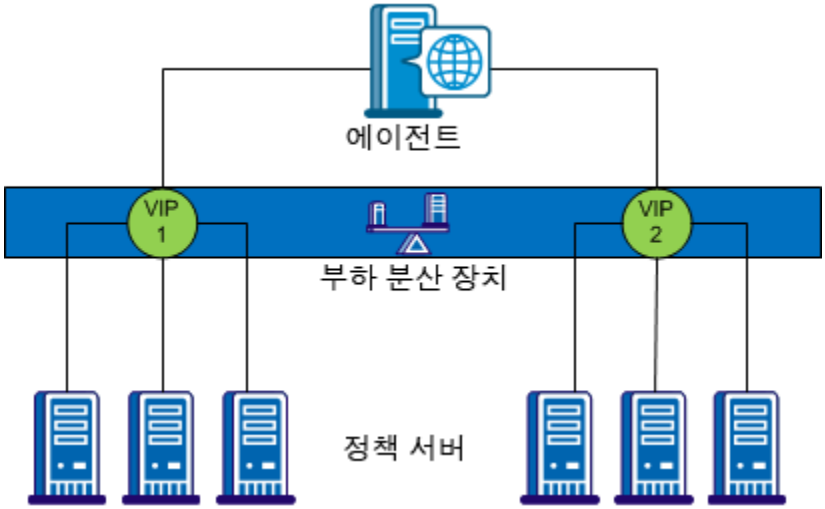
- 단일 VIP 와 VIP 별로 노출되는 다중 정책 서버
- 다중 VIP 와 VIP 별로 노출되는 다중 정책 서버

단일 VIP, VIP 별 다중 정책 서버



이전 다이어그램에 나와 있는 구성에서는 부하 분산 장치가 단일 VIP 를 사용하여 다중 정책 서버를 노출합니다. 이 시나리오에서는 VIP 를 처리하는 부하 분산 장치가 실패하는 경우 단일 실패 지점이 발생합니다.

다중 VIP, VIP 별 다중 정책 서버



이전 다이어그램에 나와 있는 구성에서는 하나 이상의 부하 분산 장치가 정책 서버 그룹을 별도의 VIP 로 노출합니다. 다중 부하 분산 장치를 사용하는 경우 부하 분산 장치 간에 장애 조치가 이루어지므로 단일 실패 지점이 제거됩니다. 하지만 모든 주요 하드웨어 부하 분산 장치 공급업체가 내부적으로 여러 유사한 부하 분산 장치 간의 장애 조치를 처리하기 때문에 단일 VIP 만으로도 충분합니다. 따라서 동일한 공급업체의 중복 부하 분산 장치를 사용하는 경우 에이전트와 정책 서버 간의 통신을 단일 VIP 로 구성해도 계속 강력한 부하 분산 및 장애 조치가 가능합니다.

참고: 하드웨어 부하 분산 장치를 사용하여 정책 서버를 다중 VIP(가상 IP 주소)로 노출하는 경우 장애 조치 구성에서 해당 VIP 를 구성하는 것이 좋습니다. 하드웨어 부하 분산 장치가 동일한 기능을 더욱 효율적으로 수행하기 때문에 라운드 로빈 부하 분산이 필요하지 않습니다.

SiteMinder 에이전트와 정책 서버 간 연결 수명 구성

에이전트와 정책 서버 간 설정된 연결은 세션 기간 동안 유지됩니다. 따라서 하드웨어 부하 분산 장치에서는 초기 연결 요청만 처리하면 됩니다. 동일한 연결의 모든 후속 트래픽은 연결이 종료되고 새 에이전트 연결이 설정되기 전까지 동일한 정책 서버로 전송됩니다.

기본적으로 정책 서버 연결 수명은 360 분이기 때문에 하드웨어 부하 분산 장치를 효율적으로 사용하기에는 너무 깁니다. 효율적인 부하 분산을 위해 모든 에이전트 연결이 자주 갱신되게 하려면 정책 서버에 대해 최대 에이전트 연결 수명을 구성하십시오.

정책 서버에 대해 최대 연결 수명을 구성하려면 다음 매개 변수를 설정하십시오.

AgentConnectionMaxLifetime

에이전트 연결의 최대 수명(분)을 지정합니다.

기본값: 0 특정 값을 설정하지 않습니다. SiteMinder 기본 연결 수명(360 분) 제한만 적용됩니다.

제한: 0~360

예: 15

참고: 사용자에게 SiteMinder 바이너리 파일(XPS.dll, libXPS.so, libXPS.sl)에 대한 쓰기 액세스 권한이 없다면 관리자가 관리 UI 또는 XPSSecurity 도구를 사용하여 관련 XPS 명령줄 도구를 사용할 수 있는 권한을 사용자에게 부여해야 합니다.

AgentConnectionMaxLifetime 매개 변수는 동적이므로, 정책 서버를 다시 시작하지 않고 해당 값을 변경할 수 있습니다.

하드웨어 부하 분산 장치에 대해 최대 에이전트 연결 수명을 구성하려면

1. 정책 서버에서 명령줄을 열고 다음 명령을 입력합니다.

   ```
   xpsconfig
   ```

   이 도구가 시작되어 이 세션에 대한 로그 파일 이름이 표시되고 선택 메뉴가 열립니다.

2. 다음을 입력합니다.

   ```
   sm
   ```

   옵션 목록이 나타납니다.

3. AgentConnectionMaxLifetime 매개 변수에 해당하는 숫자 값(예: 4)을 입력합니다.

   AgentConnectionMaxLifetime 매개 변수 메뉴가 나타납니다.

4. 매개 변수 값을 변경하려면 c 를 입력합니다.

   변경 내용을 로컬에 적용할지, 아니면 전역적으로 적용할지 묻는 메시지가 표시됩니다.

5. 다음 중 하나를 입력합니다.

   - l - 매개 변수 값이 전역 값을 덮어써 로컬 정책 서버에 대해서만 변경됩니다.
   - g - 매개 변수 값이 동일한 정책 저장소를 사용하며 로컬 값 재정의가 설정되어 있지 않은 모든 정책 서버에 대해 전역적으로 변경됩니다.

6. 예를 들어 새 최대 에이전트 연결 수명을 분 단위로 입력합니다.

   ```
   30
   ```

   새 값을 표시하는 AgentConnectionMaxLifetime 매개 변수 메뉴가 다시 나타납니다. 로컬 재정의 값이 설정되어 있는 경우 전역 값과 로컬 값이 모두 표시됩니다.

7. Q 를 세 번 입력하여 XPSConfig 세션을 끝냅니다.

   변경 내용이 저장되고 명령 프롬프트가 표시됩니다.

추가 정보

XPSConfig (페이지 272)

하드웨어 부하 분산 구성의 건전성 모니터링

다양한 하드웨어 부하 분산 장치가 서비스를 제공하는 하드웨어 및 응용 프로그램의 건전성을 확인하는 다양한 방법을 제공합니다. 이 단원에서는 특정 공급업체에 한정된 사례가 아닌 일반적인 권장 사항에 대해 설명합니다.

서버 건전성 확인 문제를 복잡하게 만드는 것은 부하 분산 장치에서 고려할 사항이 SiteMinder 건전성 및 부하만이 아니라는 것입니다. 예를 들어 상대적으로 부하가 적은 정책 서버가 다른 프로세스에 의해 부하가 발생하는 시스템에서 실행되고 있을 수 있습니다. 따라서 부하 분산 장치에서는 서버 자체의 상태(CPU, 메모리 사용량 및 디스크 활동)도 고려해야 합니다.

활성 모니터

하드웨어 부하 분산 장치에서 활성 모니터를 사용하여 하드웨어 또는 응용 프로그램의 상태 정보를 폴링할 수 있습니다. 각 주요 공급업체는 다양한 활성 모니터를 지원합니다. 이 항목에서는 가장 일반적인 모니터 몇 개와 해당 모니터가 정책 서버 모니터링에 적합한지에 대해 설명합니다.

TCP 하프 오픈

TCP 하프 오픈 모니터는 정책 서버와 부분 TCP/IP 핸드셰이크를 수행합니다. 이 모니터는 정책 서버로 SYN 패킷을 전송합니다. 정책 서버가 작동하는 경우 정상 작동 상태를 나타내기 위해 모니터로 SYN-ACK 를 다시 전송합니다.

SNMP(Simple Network Management Protocol)

SNMP 모니터는 SiteMinder MIB 를 쿼리하여 정책 서버의 건전성을 확인할 수 있습니다. 정교하게 구현한 경우 MIB 의 값을 쿼리하여 큐 깊이, 소켓 수, 사용 중인 스레드 수, 사용 가능한 스레드 수 등을 확인할 수 있습니다. 정책 서버 건전성에 대한 심층적인 정보를 얻으려면 SNMP 모니터링이 가장 적합한 방법입니다.

SNMP 모니터링을 사용하려면 각 정책 서버에서 SiteMinder OneView 모니터 및 SNMP 에이전트를 구성하십시오. 자세한 내용은 "OneView 모니터 사용" 및 "SNMP 를 사용한 SiteMinder 모니터링"을 참조하십시오.

참고: 일부 하드웨어 부하 분산 장치는 SNMP 모니터링을 기본으로 제공하지 않습니다.

ICMP(Internet Control Message Protocol)

ICMP 건전성 모니터는 거의 모든 네트워크 기반 하드웨어의 ICMP 포트를 ping 하여 온라인 상태인지 여부를 확인합니다. ICMP 모니터는 정책 서버가 건전한 상태인지 확인할 수 있는 작업을 거의 수행하지 않으므로 정책 서버 건전성 모니터링에는 권장되지 않습니다.

TCP 오픈

TCP 오픈 모니터는 네트워크 기반 응용 프로그램과 완전한 TCP/IP 핸드셰이크를 수행합니다. 이 모니터는 네트워크 기반 응용 프로그램에 잘 알려진 텍스트를 전송하고, 응용 프로그램에서는 작동 중임을 나타내기 위해 이 텍스트에 응답해야 합니다. 정책 서버는 TCP/IP 연결의 종단 간 암호화와 고유한 메시징 프로토콜을 사용하기 때문에 정책 서버 건전성 모니터링에는 TCP 오픈 모니터링이 적합하지 않습니다.

추가 정보:

SNMP 모니터링 (페이지 201)
OneView 모니터 개요 (페이지 179)

수동 모니터

인밴드 건전성 모니터는 하드웨어 부하 분산 장치에서 실행되어 해당 기능을 통해 이동하는 트래픽을 분석합니다. 이 모니터는 활성 모니터보다 훨씬 적은 영향을 미치며 부하 분산 장치에 매우 적은 오버헤드를 발생시킵니다.

특정 실패율이 감지되면 장애 조치하도록 인밴드 모니터를 구성할 수 있습니다. 일부 부하 분산 장치의 인밴드 모니터는 응용 프로그램과 관련된 문제를 감지할 수 있으며, 문제가 해결되어 서버를 다시 사용할 수 있게 되는 때를 확인할 활성 모니터를 지정할 수 있습니다.

제 15 장: 정책 서버 클러스터링

이 섹션은 다음 항목을 포함하고 있습니다.

클러스터된 정책 서버 소개

SiteMinder 배포에서 부하 분산 및 장애 조치는 SiteMinder 에이전트의 요청을 정책 서버에 분산시켜 시스템 가용성을 높은 수준으로 유지하고 응답 시간을 향상시킵니다. 부하 분산 및 장애 조치를 사용하도록 클러스터를 정의하면 시스템 가용성 수준과 시스템 응답 시간을 더욱 향상시킬 수 있습니다.

클러스터를 사용하지 않는 기존의 라운드 로빈 부하 분산에서는 서버 집합에 균등하게 요청을 분산시킵니다. 하지만 각 서버가 컴퓨팅 성능과 관계없이 같은 수의 요청을 받게 되므로 서버마다 컴퓨팅 성능이 다른 이기종 환경에서는 이 방법이 가장 효율적인 방법이 아닙니다.

데이터 센터가 지리적으로 다른 지역에 있는 경우 효율성과 관련된 또 다른 문제가 발생할 수 있습니다. 특정 지역 외부에 있는 서버에 요청을 전송하면 네트워크 통신 오버헤드가 증가할 수 있으며 경우에 따라 네트워크 정체가 발생할 수 있습니다.

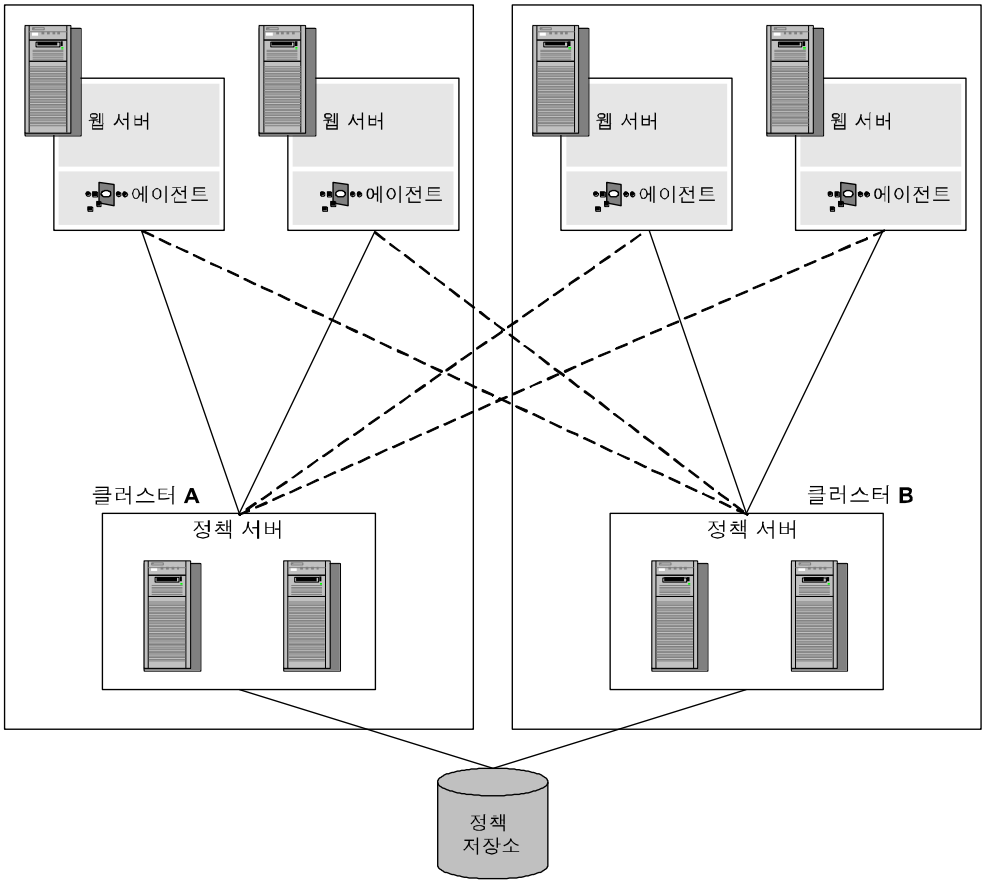
이러한 문제를 해결하고 시스템 가용성과 응답 시간을 향상시키기 위해 정책 서버 및 관련 SiteMinder 에이전트의 클러스터를 정의하고 (소프트웨어 기반) 부하 분산 및 장애 조치를 수행하도록 구성할 수 있습니다.

기존 부하 분산/장애 조치 구성과 비교할 때 정책 서버 클러스터에는 다음과 같은 장점이 있습니다.

- 서버 응답 시간을 기준으로 클러스터의 정책 서버 간에 동적으로 부하가 분산됩니다.
- 클러스터에서 사용할 수 있는 서버 수가 구성 가능한 임계값 아래로 떨어지면 또 다른 클러스터로 장애 조치되도록 클러스터를 구성할 수 있습니다.

참고: 정책 서버와 에이전트가 하드웨어 부하 분산 장치를 통해 통신하는 환경에서는 정책 서버 클러스터가 필요하지 않거나 적절하지 않습니다.

다음 그림에서는 클러스터 두 개를 사용하는 단순한 SiteMinder 배포를 보여 줍니다.



클러스터 A 와 클러스터 B 가 표준 시간대가 몇 시간 차이 나는 지리적으로 서로 다른 두 위치에 분산되어 있다고 가정합니다. 웹 에이전트 및 정책 서버를 뚜렷이 구별되는 클러스터로 나누면 클러스터 중 하나의 정책 서버에 장애가 발생하여 다른 클러스터로 장애 조치를 해야 하는 경우에만 지리적으로 떨어진 지역 간의 부하 분산과 관련된 네트워크 오버헤드가 발생합니다.

추가 정보:

장애 조치 임계값 (페이지 173)
클러스터 환경 모니터링 (페이지 194)

장애 조치 임계값

클러스터된 SiteMinder 환경에서는 장애 조치 임계값을 구성해야 합니다. 사용 가능한 정책 서버 수가 지정된 임계값 미만일 경우 장애가 발생한 정책 서버 클러스터에서 처리해야 할 모든 요청이 다른 클러스터로 전달됩니다.

장애 조치 임계값은 클러스터에 있는 정책 서버의 백분율로 표시됩니다. 예를 들어 클러스터가 네 개의 정책 서버로 구성되어 있고 클러스터의 장애 조치 임계값이 50%로 설정된 경우 클러스터에 있는 네 개의 정책 서버 중 세 개에서 장애가 발생하면 해당 클러스터는 장애 클러스터로 처리되어 모든 요청이 다음 클러스터로 장애 조치됩니다.

기본 장애 조치 임계값은 0 으로, 클러스터의 모든 서버에 장애가 발생해야만 장애 조치가 수행됨 의미합니다.

하드웨어 부하 분산 고려 사항

SiteMinder 정책 서버와 웹 에이전트 사이에 하드웨어 부하 분산 기능을 배포하려는 경우 다음 사항을 고려하십시오.

- 정책 서버 TCP 포트에 대해 직접 TCP 하트비트나 건전성 검사를 구성하지 마십시오. 정책 서버의 TCP 포트에 대해 직접 적용되는 하트비트나 건전성 검사는 해당 작업에 부정적인 영향을 줄 수 있습니다.
- 정책 서버의 작동 건전성을 테스트할 수 있도록 부하 분산 기능에 포괄적인 기능을 설계하십시오.

- 정책 서버를 하나만 구성할 경우 웹 에이전트 장애 조치 알고리즘에 미치는 영향을 여러 정책 서버를 구성할 경우와 비교하여 고려하십시오.
- 웹 에이전트와 정책 서버를 조정 및 모니터링할 때의 성능 및 장애 시나리오를 고려하십시오.
- 부하 분산 기능이 에이전트와 정책 서버의 연결을 프록시하도록 구성된 경우 부하 분산 기능의 시간 만료 및 소켓 상태를 고려하십시오.

  참고: 웹 에이전트와 정책 서버 간에 하드웨어 부하 분산 기능을 배포하는 방법에 대한 자세한 내용은 CA Support 사이트의 관련 기술 자료 문서(TEC511443)를 참조하십시오.

추가 정보:

CA 에 문의 (페이지 4)

정책 서버 클러스터 구성

정책 서버 클러스터는 호스트 구성 개체의 일부로 정의됩니다. SiteMinder 에이전트가 초기화될 때 호스트 구성 개체의 설정을 사용하여 정책 서버와의 통신이 설정됩니다.

참고: 호스트 구성 개체에 대한 자세한 내용은 *웹 에이전트 구성 안내서* 및 *정책 서버 구성 안내서*를 참조하십시오.

다음 단계를 수행하십시오.

1. "인프라", "호스트"를 차례로 클릭합니다. "호스트 구성 개체"를 차례로 선택합니다.
2. "호스트 구성 만들기"를 클릭합니다.
3. "클러스터" 섹션에서 "추가"를 클릭합니다.

   "클러스터 설정" 섹션이 열립니다.

   참고: "도움말"을 클릭하면 필드, 컨트롤 및 해당되는 요구 사항에 대한 설명을 볼 수 있습니다.
4. "호스트" 및 "포트" 필드에 각각 정책 서버의 IP 주소와 포트 번호를 입력합니다.
5. "클러스터에 추가"를 클릭합니다.

   "현재 설정" 섹션의 서버 목록에 정책 서버가 표시됩니다.

6. 다른 정책 서버를 클러스터에 추가하려면 이 단계를 반복합니다.
7. "확인"을 클릭하여 변경 내용을 저장합니다.

   "호스트 구성" 대화 상자가 나타나고 테이블에 정책 서버 클러스터가 표시됩니다.
8. "장애 조치 임계값 백분율" 필드에 활성 상태여야 하는 정책 서버의 수를 백분율로 입력하고 "적용"을 클릭합니다.

   클러스터의 활성 서버 비율이 지정한 비율 아래로 떨어지면 클러스터는 클러스터 목록에 있는 사용 가능한 다음 클러스터로 장애 조치됩니다. 이 설정은 호스트 구성 개체를 사용하는 모든 클러스터에 적용됩니다.

   중요! "구성 값" 섹션에 지정된 정책 서버는 클러스터에 지정된 정책 서버로 덮어쓰여집니다. 클러스터가 구성되었으므로 이 정책 서버는 더 이상 사용되지 않습니다. "구성 값" 섹션의 "정책 서버" 매개 변수 값이 적용되도록 하려면 클러스터에 정책 서버를 지정하지 마십시오. 클러스터를 구성했지만 클러스터를 제거하고 단순 장애 조치 구성을 사용하려는 경우에는 클러스터에서 모든 정책 서버 정보를 삭제하십시오.
9. "제출"을 클릭하여 변경 내용을 저장합니다.

정책 서버를 클러스터의 중앙 집중화된 모니터로 구성

정책 서버 클러스터를 모니터링하도록 OneView 모니터를 구성할 수 있습니다. 이 구성이 사용되도록 설정하려면 정책 서버 하나가 중앙 모니터로 설정되어 있고 클러스터된 다른 정책 서버가 이 모니터에 연결되어야 합니다.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 시작합니다.

   중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.
2. "설정" 탭에서 "수신 원격 연결 허용"을 선택합니다.

   참고: 이 탭의 설정과 컨트롤에 대한 자세한 내용을 보려면 "도움말", "관리 콘솔 도움말"을 차례로 클릭하십시오.

3. "확인"을 클릭하여 변경 내용을 저장하고 정책 서버 관리 콘솔을 닫습니다.
4. OneView 모니터를 다시 시작합니다.

이 설정을 사용하면 중앙 정책 서버 모니터가 클러스터된 다른 정책 서버에서의 원격 연결을 허용할 수 있습니다.

참고: 정책 서버와 모니터 프로세스 간의 네트워크 채널에는 보안이 적용되지 않습니다.

정책 서버를 중앙 모니터로 구성한 후에는 정책 서버 관리 콘솔에서 클러스터된 다른 정책 서버가 이 모니터에 연결하도록 구성하십시오.

추가 정보:

OneView 모니터 포트 번호 구성 (페이지 193)

클러스터된 정책 서버를 중앙 모니터에 연결

다음 단계를 수행하십시오.

1. 모니터링 서비스에 연결할 각 정책 서버에 대해 정책 서버 관리 콘솔을 엽니다.

   중요! Windows Server 2008 에서 이 그래픽 사용자 인터페이스에 액세스하는 경우에는 관리자 권한을 사용하여 바로 가기를 여십시오. 관리자로 시스템에 로그인한 경우에도 관리자 권한을 사용하십시오. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

2. "설정" 탭의 "OneView 모니터"에서 "원격 모니터에 연결"을 선택합니다.

   참고: 이 탭의 설정과 컨트롤에 대한 자세한 내용을 보려면 "도움말", "관리 콘솔 도움말"을 차례로 클릭하십시오.

3. 아래 필드에 모니터링 서비스가 구성된 시스템의 호스트 이름과 TCP 포트 번호를 입력합니다. 예를 들면 다음과 같습니다.

   server.company.com:44449

4. "확인"을 클릭하여 변경 내용을 저장하고 정책 서버 관리 콘솔을 닫습니다.
5. 정책 서버를 다시 시작합니다.

제 16 장: OneView 모니터 사용

이 섹션은 다음 항목을 포함하고 있습니다.

제 17 장: OneView 모니터 개요

SiteMinder OneView 모니터는 성능 병목 문제를 확인하고 SiteMinder 배포 환경의 리소스 사용량에 대한 정보를 제공합니다. 또한 구성 요소 오류와 같은 특정 이벤트가 발생할 때 경고를 표시합니다. 이를 위해 OneView 모니터는 다음 SiteMinder 구성 요소에서 작업 데이터를 수집합니다.

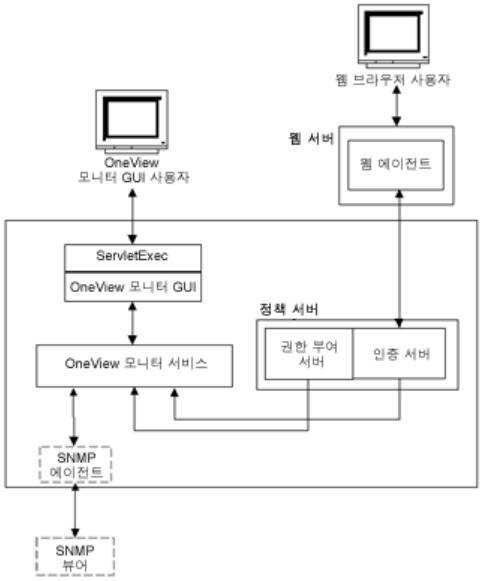
- 정책 서버
- SiteMinder 웹 에이전트

이러한 구성 요소는 SiteMinder 배포 환경에 추가될 때 OneView 모니터에 자동으로 등록됩니다. 따라서 이러한 구성 요소를 모니터링하도록 OneView 를 구성할 필요가 없습니다.

모니터링 대상 구성 요소를 호스트하는 각 컴퓨터에는 OneView 에이전트가 포함됩니다. 에이전트는 정책 서버가 설치된 컴퓨터에 있는 OneView 모니터로 작업 데이터를 보냅니다. OneView 모니터는 웹 브라우저나 필요한 경우 SNMP 에이전트로 작업 데이터를 보냅니다. SNMP 에이전트는 이 데이터를 SNMP 관리자에게 보냅니다.

웹 브라우저나 타사 SNMP 모니터링 응용 프로그램에서 OneView 모니터 데이터에 액세스할 수 있습니다.

다음 그림에서는 SiteMinder 배포 환경에 OneView 모니터가 통합되는 방식을 보여 줍니다.



OneView 모니터는 구성 요소 호스트 컴퓨터의 IP 주소 같은 속성과 사용자가 사이트에 로그인한 횟수 같이 구성 요소의 작업을 반영하는 카운터를 수집합니다. 카운터는 구성 요소가 다시 시작될 때 재설정됩니다.

관리자는 웹 기반 OneView 뷰어를 사용하여 특정 구성 요소에 대한 일부 데이터 또는 모든 데이터를 보기 위한 테이블을 정의할 수 있습니다. 데이터는 구성 가능한 간격으로 새로 고쳐집니다.

SNMP 지원은 모니터링 응용 프로그램이 OneView 모니터에서 작업 데이터를 검색할 수 있도록 합니다. SNMP 지원에는 MIB(관리 정보 베이스)와 SNMP 에이전트가 포함됩니다.

참고: 클러스터된 정책 서버가 포함된 환경에서는 클러스터에 있는 모든 정책 서버의 작업을 모니터링할 단일 OneView 모니터를 지정할 수 있습니다. 중앙 모니터를 구성하려면 클러스터의 각 정책 서버에 대한 정책 서버 관리 콘솔에서 OneView 모니터 설정을 조정해야 합니다.

추가 정보:

SNMP 모니터링 (페이지 201)
OneView 데이터 새로 고침 빈도 및 하트비트 설정 (페이지 192)

정책 서버 데이터

다음은 정책 서버 데이터에 대한 설명입니다.

AgentTable

이 서버에 연결된 에이전트의 테이블입니다.

참고: AgentTable 은 SNMP 를 통해 사용할 수 없습니다.

AuthAcceptCount

성공한 인증 횟수입니다.

AuthRejectCount

실패한 인증 시도 횟수입니다. 인증 시도는 자격 증명이 잘못된 경우에 실패합니다.

AzAcceptCount

성공한 권한 부여 시도 횟수입니다.

AzRejectCount

거부된 권한 부여 시도 횟수입니다. 권한 부여 시도는 액세스 권한이 충분하지 않은 경우에 거부됩니다.

CacheFindCount

권한 부여 캐시에서의 찾기 작업 횟수입니다. 권한 부여 프로세스에서 사용자가 정책에 속하는지 여부가 확인될 때마다 업데이트됩니다.

CacheFindCount/sec

권한 부여 캐시 찾기 작업의 초당 발생 횟수입니다.

CacheHitCount

권한 부여 캐시에서의 적중 횟수입니다. 사용자가 정책에 속하는지 여부에 대한 권한 부여 프로세스의 확인 요청에 캐시가 true 로 응답할 때마다 업데이트됩니다.

CacheHitCount/sec

권한 부여 캐시에서의 초당 적중 횟수입니다.

CacheTTLMissCount

요소가 캐시에 있지만 너무 오래된 것으로 간주되어 발생한 권한 부여 캐시 누락 횟수입니다.

Component Path

서버를 고유하게 식별하는 정책 서버 경로입니다. Component Path 에는 다음 정보가 포함됩니다.

- 호스트 IP 주소
- 구성 요소 유형
- 구성 요소 인스턴스 ID

참고: Component Path 는 SNMP 를 통해 사용할 수 없습니다.

Crypto bits

웹 에이전트와 정책 서버 간에 전송되는 데이터를 암호화하고 암호 해독하는 데 사용되는 암호화 키의 길이입니다.

HitRate

권한 부여 찾기 작업에 대한 권한 부여 캐시 적중 비율로, 권한 부여 캐시 유효성을 나타내는 지표입니다.

호스트

인증 서버가 설치된 컴퓨터의 IP 주소입니다.

참고: 호스트 IP 주소는 Component Path 에 포함됩니다.

IsProtectedCount

에이전트에서 받은 IsProtected 호출의 횟수입니다.

Label

정책 서버 빌드 번호입니다.

LastActivity

정책 서버가 모니터와 마지막으로 상호 작용한 날짜 및 시간입니다.

MaxSockets

정책 서버에 동시 요청을 제출하는 데 사용할 수 있는 최대 웹 에이전트 소켓 수입니다.

MaxThreads

스레드 풀의 최대 작업자 스레드 수입니다.

MaximumThreadsEverUser

스레드 풀에서 지금까지 사용된 최대 작업자 스레드 수입니다.

PriorityQueueLength

우선 순위 큐의 항목 수입니다. 우선 순위 큐에는 우선 순위가 높은 항목이 보관됩니다. ServerQueueLength 를 참조하십시오.

Platform

정책 서버가 설치된 컴퓨터의 운영 체제입니다.

PolicyCacheEnabled

정책 캐시가 사용되는지 여부를 나타냅니다.

Port

정책 서버 포트 번호입니다.

Product

정책 서버 제품 이름입니다.

ServerQueueLength

일반 큐의 항목 수입니다. 일반 큐에는 우선 순위가 보통인 항목이 보관됩니다. PriorityQueueLength 를 참조하십시오.

SocketCount

열려 있는 소켓 수로, 정책 서버와 웹 에이전트 간의 열려 있는 연결 수에 해당합니다.

Status

정책 서버의 상태입니다. 상태는 Active 또는 Inactive 일 수 있습니다.

Inactive 상태는 지정된 기간 동안 정책 서버와 모니터 간에 상호 작용이 없었음을 나타냅니다. 기간은 하트비트 간격에 따라 결정됩니다.

ThreadsAvailable

스레드 풀 내에서 사용할 수 있는 작업자 스레드 수입니다. 요청을 처리하는 모든 작업자 스레드는 스레드 풀에 구성됩니다. 모든 스레드가 즉시 사용되는 것은 아니고 부하가 높을 때만 모든 스레드가 사용됩니다. 이 값은 현재 사용 중이 아닌 스레드 수를 보여 줍니다.

ThreadsInUse

스레드 풀의 사용 중인 작업자 스레드 수입니다.

Time Zone

정책 서버가 설치된 지리적 위치의 표준 시간대입니다.

유형

정책 서버의 유형입니다.

Universal Coordinated Time

정책 서버의 시작 시간입니다.

UserAzCacheEnabled

사용자 권한 부여 캐시가 사용되는지 여부를 나타냅니다.

Update

가장 최근에 적용된 업데이트의 버전 번호입니다.

Version

정책 서버의 버전 번호입니다.

웹 에이전트 데이터

다음은 웹 에이전트 데이터에 대한 설명입니다.

AuthorizeAvgTime

사용자에게 권한을 부여하는 데 소요되는 평균 시간(밀리초)을 나타냅니다.

AuthorizeCount

해당 에이전트에서의 권한 부여 시도 횟수입니다. 사용자가 보호된 리소스에 액세스하기 위해 정책 서버에 자격 증명을 제공하면 권한 부여 시도가 발생합니다.

AuthorizeErrors

해당 웹 에이전트가 권한 부여를 시도하는 동안 발생한 오류 수입니다. 이 오류는 권한 부여 호출 중 웹 에이전트와 정책 서버 간에 발생한 통신 오류를 나타냅니다.

AuthorizeFailures

실패한 권한 부여 시도 횟수입니다. 사용자에게 리소스에 액세스할 수 있는 충분한 권한이 없으면 권한 부여 시도가 실패합니다.

BadCookieHitsCount

웹 에이전트가 암호 해독하지 못한 쿠키 수입니다.

BadURLcharsHits

잘못된 URL 문자 때문에 에이전트가 거부한 요청 수입니다. 잘못된 URL 문자는 특히 웹 클라이언트가 SiteMinder 규칙을 위반하지 못하도록 하기 위해 차단됩니다. 이러한 문자는 웹 에이전트 구성에서 지정합니다.

Component Path

웹 에이전트의 경로입니다. Component Path 에는 다음 정보가 포함됩니다.

- 호스트 IP 주소
- 구성 요소 유형
- 구성 요소 인스턴스 ID

참고: Component Path 는 SNMP 를 통해 사용할 수 없습니다.

CrosssiteScriptHits

교차 사이트 스크립팅 적중 횟수입니다. 교차 사이트 스크립팅 적중은 사이트의 페이지에 포함된 악의적 코드로 구성됩니다.

참고: 교차 사이트 스크립팅에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

Crypto bits

웹 에이전트와 정책 서버 간에 전송되는 데이터를 암호화하고 암호 해독하는 데 사용되는 암호화 키의 길이입니다.

ExpiredCookieHitsCount

만료된 쿠키가 포함된 요청 수입니다.

호스트

웹 에이전트가 설치된 컴퓨터의 IP 주소입니다.

참고: 호스트 IP 주소는 Component Path 에 포함됩니다.

IsProtectedAvgTime

웹 에이전트가 정책 서버에서 리소스 보호 여부를 확인하는 데 소요되는 평균 시간(밀리초)입니다.

IsProtectedCount

웹 에이전트가 정책 서버에서 리소스 보호 여부를 확인한 횟수입니다.

참고: 리소스 캐시가 0 으로 설정된 경우 OneView 모니터는 각 로그인 시도에 대해 둘 이상의 IsProtected 호출을 기록할 수 있습니다. 정보를 캐시하지 않는 경우 웹 에이전트는 웹 서버에 대한 요청이 있을 때마다 정책 서버에서 리소스 보호 여부를 확인해야 합니다.

리소스 캐시가 0 으로 설정되어 있지 않으면 OneView 모니터는 IsProtected 호출을 하나만 기록합니다. 이 경우 웹 에이전트는 정책 서버에 대해 IsProtected 를 한 번만 호출하며, 이후 캐시의 리소스가 만료되거나 리소스 캐시가 플러시될 때까지는 웹 서버에 동일한 리소스가 요청될 때마다 웹 에이전트의 리소스 캐시에서 요청이 처리됩니다.

IsProtectedErrors

웹 에이전트가 정책 서버에 리소스 보호 여부를 확인할 때 발생한 오류 수입니다. 이 오류는 웹 에이전트와 정책 서버 간의 통신 오류를 나타냅니다.

Label

웹 에이전트 빌드 번호입니다.

Last Activity

웹 에이전트의 마지막 작업 날짜 및 시간입니다.

LoginAvgTime

사용자 로그인에 소요되는 평균 시간입니다.

LoginCount

해당 웹 에이전트가 시도한 로그인 횟수입니다.

LoginErrors

로그인 시도 중 발생한 오류 수입니다. 이 오류는 웹 에이전트와 정책 서버 간의 통신 오류를 나타냅니다.

LoginFailures

실패한 로그인 시도 횟수입니다. 사용자가 잘못된 자격 증명을 제공하면 로그인이 실패합니다.

이름

웹 에이전트의 이름입니다.

Platform

웹 에이전트가 설치된 컴퓨터의 운영 체제입니다.

Product

웹 에이전트 제품 이름입니다.

ResourceCacheCount

리소스 캐시의 항목 수입니다. 리소스 캐시에는 최근에 액세스한 리소스에 대한 정보가 저장되므로 동일한 리소스에 대한 이후 요청을 빠르게 처리할 수 있습니다.

리소스 캐시의 항목 수는 0 에서 *n* 사이일 수 있습니다. 여기서 *n* 은 웹 에이전트 구성에 지정된 최대 캐시 크기입니다.

ResourceCacheHits

웹 에이전트가 리소스 캐시에서 리소스를 찾은 횟수입니다. 이 숫자는 SiteMinder 가 캐시된 리소스를 사용하는 빈도를 나타냅니다.

ResourceCacheMax

리소스 캐시에 포함될 수 있는 최대 항목 수입니다. 이 숫자는 웹 에이전트 구성에서 지정합니다.

참고: 리소스 캐시 크기 설정에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

ResourceCacheMisses

- 웹 에이전트가 리소스 캐시에서 리소스를 찾지 못한 횟수입니다. 이는 다음과 같은 경우에 발생합니다.
- 이전에 리소스에 액세스한 적이 없는 경우
- 캐시된 정보가 만료된 경우

SocketCount

열려 있는 소켓 수로, 정책 서버와 웹 에이전트 간의 열려 있는 연결 수에 해당합니다.

참고: 웹 에이전트 아키텍처가 변경되었기 때문에 SocketCount 에는 값이 없습니다.

Status

웹 에이전트의 상태입니다. 상태는 Active 또는 Inactive 일 수 있습니다.

Inactive 상태는 지정된 기간 동안 웹 에이전트와 모니터 간에 상호 작용이 없었음을 나타냅니다. 기간은 하트비트 간격에 따라 결정됩니다.

Time Zone

웹 에이전트가 설치된 지리적 위치의 표준 시간대입니다.

유형

모니터링되는 구성 요소의 유형입니다. 이 경우에는 웹 에이전트입니다.

Universal Coordinated Time

웹 에이전트가 설치된 웹 서버의 시작 시간입니다.

Update

최신 소프트웨어 업데이트의 버전 번호입니다.

UserSessionCacheCount

사용자 세션 캐시의 항목 수입니다. 사용자 세션 캐시에는 최근에 리소스에 액세스한 사용자에 대한 정보가 저장됩니다. 사용자 정보를 저장하면 리소스 요청이 빠르게 처리됩니다.

사용자 세션 캐시의 항목 수는 0 에서 *n* 사이일 수 있습니다. 여기서 *n* 은 웹 에이전트 구성에 지정된 최대 캐시 크기입니다. 사용자 세션 캐시 크기 설정에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

참고: 사용자 세션 캐시 수는 세션 캐시가 있는 웹 서버에 따라 달라질 수 있습니다.

IIS 웹 에이전트, iPlanet 4.*x* 및 6.0 웹 에이전트(Windows 운영 체제), Domino 웹 에이전트(Windows 및 UNIX 운영 체제)와 같이 다중 스레드 캐시를 사용하는 웹 에이전트의 경우, OneView 모니터는 사용자가 성공적으로 인증될 때 사용자 세션 캐시 수를 늘리고 웹 에이전트에서 세션 쿠키를 받습니다.

다중 프로세스 캐시를 사용하는 UNIX 운영 체제에서 실행되는 Apache 웹 에이전트와 iPlanet 4.*x* 및 6.0 웹 에이전트는 세션 수를 다르게 계산합니다. 웹 에이전트에 세션 쿠키가 제공될 때까지 사용자의 세션은 세션 캐시에 추가되지 않습니다. 웹 에이전트는 사용자가 성공적으로 인증된 *후*사용자에 대한 세션 쿠키를 생성합니다. 해당 사용자로부터 추가 리소스 요청이 있으면 SiteMinder 는 이 쿠키를 사용하여 사용자를 인증합니다. 따라서 사용자의 첫 번째 로그인은 사용자 세션 캐시 수에 기록되지 않습니다. 사용자가 다른 요청을 하면 SiteMinder 는 세션 쿠키를 사용하여 해당 사용자를 인증하며 이때 사용자 세션 캐시 수는 늘어납니다.

모든 웹 에이전트에서 사용자 세션은 한 영역의 리소스에 대해서만 유효합니다. 사용자가 세션 쿠키를 사용하여 다른 영역의 리소스에 액세스할 경우에는 다른 사용자 세션이 제공되므로 사용자 세션 캐시 수가 늘어납니다.

UserSessionCacheHits

웹 에이전트가 사용자 세션 캐시에 액세스한 횟수입니다.

UserSessionCacheMax

사용자 세션 캐시에 포함될 수 있는 최대 항목 수입니다. 이 숫자는 웹 에이전트 구성에서 지정합니다.

참고: 사용자 세션 캐시 크기 설정에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

UserSessionCacheMisses

웹 에이전트가 사용자 세션 캐시에서 사용자 세션 정보를 찾지 못한 횟수입니다. 이는 다음과 같은 경우에 발생합니다.

- 사용자가 이전에 리소스에 액세스한 적이 없는 경우
- 캐시된 정보가 만료된 경우

ValidationAvgTime

사용자 인증 시 사용되는 쿠키의 유효성을 검사하는 데 소요되는 평균 시간(밀리초)입니다. 쿠키는 싱글 사인온 환경에서 사용자를 인증하는 데 사용될 수 있습니다.

ValidationCount

특정 웹 에이전트가 사용자 인증을 위해 사용자의 자격 증명을 사용자 디렉터리 항목과 비교하는 대신 정책 서버에 대해 세션 쿠키의 유효성을 검사하려고 시도한 횟수입니다. 웹 에이전트는 사용자가 성공적으로 인증되면 사용자의 브라우저에 세션 쿠키를 생성하며, 이후에 해당 사용자가 새 리소스를 요청할 때 이 쿠키를 사용하여 사용자를 인증합니다.

ValidationCount 에 영향을 주는 요소는 다음과 같습니다.

사용자 세션 캐시 크기

웹 에이전트의 사용자 세션 캐시가 0 보다 큰 값으로 설정되어 있으면 사용자의 세션 정보가 캐시에 저장됩니다. 웹 에이전트는 정책 서버가 아니라 세션 캐시에 대해 세션의 유효성을 검사하므로 ValidationCount 가 늘어나지 않습니다. 사용자 세션 캐시가 0 으로 설정되어 있으면 웹 에이전트는 정책 서버에 대해 세션의 유효성을 검사해야 하므로 사용자가 보호된 리소스를 요청할 때마다 ValidationCount 가 늘어납니다.

다중 스레드와 다중 프로세스 비교

IIS 웹 에이전트, iPlanet 4.x 및 6.0 웹 에이전트(Windows 운영 체제), Domino 웹 에이전트(Windows 및 UNIX 운영 체제)와 같이 다중 스레드 캐시를 사용하는 웹 에이전트는 세션 캐시 크기가 0 보다 크고 사용자가 성공적으로 인증된 경우 세션 캐시에 세션을 추가합니다. 해당 사용자가 동일한 영역에서 추가 리소스를 요청할 경우 웹 에이전트는 세션 캐시에 대해 사용자의 유효성을 검사하므로 ValidationCount 가 늘어나지 않습니다.

다중 프로세스 캐시를 사용하는 UNIX 운영 체제에서 실행되는 Apache 웹 에이전트와 iPlanet 4.x 및 6.0 웹 에이전트는 사용자가 웹 에이전트에 쿠키를 제공할 때까지는 해당 사용자가 인증된 영역의 다른 리소스를 요청할 때 세션 캐시에 세션 쿠키를 추가하지 않습니다. 웹 에이전트는 정책 서버에 대해 세션 쿠키를 사용하여 이루어진 첫 번째 요청의 유효성을 검사하므로 ValidationCount 가 늘어납니다. 이후 요청은 캐시에 대해 유효성이 검사됩니다.

ValidationErrors

웹 에이전트가 사용자 세션의 유효성 검사를 시도할 때 발생한 오류 수입니다. 이 오류는 웹 에이전트와 정책 서버 간의 통신 오류를 나타냅니다.

ValidationFailures

웹 에이전트가 유효하지 않은 세션 쿠키로 인해 사용자 세션의 유효성을 검사하는 데 실패한 횟수입니다.

Version

웹 에이전트의 버전 번호입니다.

OneView 모니터 구성

OneView 모니터를 구성하려면 다음 작업을 수행합니다.

- 데이터 새로 고침 빈도 및 하트비트 설정
- 포트 번호 구성

OneView 데이터 새로 고침 빈도 및 하트비트 설정

다음 설정을 수정하여 OneView 모니터와 모니터링되는 구성 요소 간의 데이터 전송 빈도를 변경할 수 있습니다.

- 새로 고침 빈도는 OneView 모니터가 인증 및 권한 부여 서버에 데이터를 요청하는 빈도를 결정합니다. 기본 새로 고침 빈도는 5 초입니다.
- 하트비트는 모니터링되는 구성 요소가 모니터로 하트비트를 보내는 빈도를 지정합니다. 인증 및 권한 부여 서버의 경우 하트비트는 구성 요소가 활성 상태인지 여부를 나타냅니다. 웹 에이전트의 경우 하트비트는 모니터가 웹 에이전트의 작업 데이터를 받는 빈도를 결정합니다. 기본값은 30 초입니다.

기본값을 수정하려면

1. *Policy_Server_installation*/monitor/mon.conf 를 엽니다.
2. 다음 속성의 값을 필요한 대로 변경합니다.
   - 새로 고침 빈도: nete.mon.refreshPeriod
   - 하트비트: nete.mon.hbPeriod

   참고: 이러한 속성 값은 초 단위로 지정됩니다.
3. mon.conf 를 저장한 후 닫습니다.
4. OneView 모니터를 다시 시작합니다.

추가 정보:

Windows 시스템에서 정책 서버 서비스 시작 및 중지 (페이지 28)
UNIX 시스템에서 정책 서버 프로세스 시작 및 중지 (페이지 28)

OneView 모니터 포트 번호 구성

OneView 모니터는 다음과 같은 기본 포트 번호를 사용합니다.

- OneView 에이전트 - 44449

  참고: 기본 포트를 사용할 경우 OneView 에이전트는 이 포트에서만 수신합니다. 기본 포트를 변경하면 OneView 에이전트는 지정된 포트에서 수신하고 지정된 원격 호스트의 동일한 포트에 연결합니다. 예를 들어 포트를 55555 로 변경하면 OneView 에이전트는 55555 포트에서 수신하고 원격 호스트의 55555 포트에 연결합니다.

- OneView 모니터 - 44450

기본 포트 번호를 변경하려면

1. 텍스트 편집기에서 *Policy_Server_installation_directory*/config/conapi.conf 파일을 엽니다.
2. 다음 OneView 에이전트 속성의 값을 필요한 대로 변경합니다.

   `nete.conapi.service.monagn.port=`*`port_number`*

   `nete.conapi.service.monagn.host=`*`fully_qualified_domain_name_of_remote_host`*
3. 다음 OneView 모니터 속성의 값을 필요한 대로 변경합니다.

   `nete.conapi.service.mon.port=`*`port_number`*
4. conapi.conf 파일을 저장한 후 닫습니다.

   참고: conapi.conf 의 속성에 대한 자세한 내용은 conapi.conf 파일 내의 설명을 참조하십시오.
5. OneView 모니터를 다시 시작합니다.

추가 정보:

Windows 시스템에서 정책 서버 서비스 시작 및 중지 (페이지 28)
UNIX 시스템에서 정책 서버 프로세스 시작 및 중지 (페이지 28)
정책 서버를 클러스터의 중앙 집중화된 모니터로 구성 (페이지 175)

클러스터 환경 모니터링

클러스터되지 않은 SiteMinder 배포 환경에서는 모니터 프로세스가 정책 서버와 동일한 시스템에 있습니다. 모니터 사용자 인터페이스와 SNMP 는 단일 정책 서버에 정보를 제공합니다. 클러스터를 모니터링하려면 클러스터의 정책 서버가 단일 모니터 프로세스에 연결하도록 구성해야 합니다. 정책 서버 관리 콘솔을 사용하여 모니터 프로세스 호스트를 지정할 수 있습니다.

클러스터 환경에서 모니터링 기능을 구현하는 경우 다음 사항을 고려하십시오.

- 정책 서버와 모니터 프로세스 간의 네트워크 채널에는 보안이 적용되지 않습니다.
- 모니터 프로세스에 오류가 발생하면 모든 모니터링이 중지됩니다. 모니터 호스트의 연결이 해제되면 모니터링이 중지됩니다.
- 클러스터에는 SNMP 를 통한 모니터링이 지원됩니다.

참고: 클러스터링이 사용되도록 설정하지 않은 경우 모든 서버는 기본 클러스터에 있습니다. 클러스터되지 않은 환경에서는 중앙 모니터링이 사용되도록 설정할 수 있습니다.

추가 정보:

클러스터된 정책 서버를 중앙 모니터에 연결 (페이지 176)

OneView 뷰어 액세스

OneView 뷰어에 액세스하기 전에 OneView 모니터 서비스가 실행 중인지 확인하십시오.

OneView 뷰어에 액세스하려면 브라우저에 다음 URL 을 입력하십시오.

http://*your_server.your_company.org:port*/sitemindermonitor

여기서 *your_server.your_company.org:port* 는 OneView 모니터용으로 구성된 웹 서버의 호스트 이름 또는 IP 주소와 포트 번호입니다.

참고: OneView 모니터용 웹 서버 구성에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

OneView 뷰어 보호

OneView 뷰어를 보호하려면 siteminderмonitor 의 리소스를 보호하는 SiteMinder 정책을 생성하십시오.

모니터링되는 구성 요소 보기

OneView 모니터는 다음과 같은 기본 테이블을 제공합니다.

- 모든 구성 요소(표시됨)
- 정책 서버
- 에이전트

"모든 구성 요소" 테이블은 OneView 를 열 때 표시됩니다.

참고: Apache 또는 iPlanet 6.0 웹 서버에 설치된 웹 에이전트는 해당 웹 에이전트가 정책 서버에 리소스 보호 여부를 확인하기 전까지는 OneView 뷰어에 표시되지 않습니다. 이러한 웹 에이전트는 정책 서버에 정보를 요청할 때 OneView 모니터에 등록됩니다.

OneView 뷰어는 구성 가능한 테이블에 작업 데이터를 표시합니다. 테이블에는 "상세 정보" 열이 포함될 수 있습니다. "상세 정보" 열의 아이콘을 클릭하면 특정 구성 요소에 대해 모니터링되는 모든 데이터가 표시된 창이 열립니다.

OneView 표시 내용을 사용자 지정하는 방법

OneView 표시 내용을 사용자 지정하는 작업에는 다음이 포함됩니다.

- 테이블 설정 (페이지 196)
- 경고 구성 (페이지 196)
- 테이블 표시 (페이지 197)
- 테이블 정렬 (페이지 197)
- 데이터 업데이트 구성 (페이지 197)
- 설정 저장 (페이지 198)
- 기본 표시 내용 변경 (페이지 198)
- 설정 로드 (페이지 199)

테이블 설정

테이블을 설정하려면

1. "구성"을 클릭합니다.

   "Table Configuration"(테이블 구성) 대화 상자가 열립니다.

2. 다음 옵션 중 하나를 완료합니다.

   - "Existing Table"(기존 테이블)을 선택합니다. 목록 상자에서 테이블을 선택합니다.
   - "New Custom Table"(새 사용자 지정 테이블)을 선택합니다. "Table Name"(테이블 이름) 필드에 이름을 입력합니다.

3. 테이블에 표시할 구성 요소를 선택합니다.

4. 테이블에 표시할 필드를 선택합니다. 필드를 선택하고 위쪽 또는 아래쪽 화살표로 필드를 배치하여 필드가 표시되는 순서를 지정합니다. 사용 가능한 필드는 테이블에 표시하도록 선택한 구성 요소의 유형에 따라 달라집니다.

   참고: 일부 필드 값은 계속해서 늘어나는 숫자로 표시되거나(구성 요소를 다시 시작할 때 재설정됨) 마지막 업데이트 기간 이후의 평균 값으로 표시될 수 있습니다. 평균 값을 보려면 /sec 가 추가된 필드 이름을 선택합니다.

5. "확인"을 클릭합니다.

   참고: 테이블을 구성한 후 테이블을 저장해야 합니다.

추가 정보:

설정 저장 (페이지 198)

경고 구성

경고를 구성하려면

1. "구성"을 클릭합니다.
2. "경고" 탭을 클릭합니다.
3. 왼쪽 목록 상자에서 필드를 선택합니다. 이 목록 상자에는 현재 로드된 테이블의 모든 필드가 포함되어 있습니다.
4. 가운데 목록 상자에서 연산자를 선택합니다.

5. 3 단계에서 선택한 필드의 값을 지정합니다.
6. 필요한 경우 "Highlight the table cell"(테이블 셀 강조 표시)을 선택하여 지정된 조건을 충족하면 OneView 에 지정된 테이블 셀이 강조 표시되도록 지정합니다.
7. 필요한 경우 "Pop up a warning message"(경고 메시지 팝업)를 선택하여 지정된 조건을 충족하면 OneView 에 팝업 창이 표시되도록 지정합니다.

테이블 표시

테이블을 표시하려면 기본 뷰어 페이지의 "View Table"(테이블 보기) 목록 상자에서 테이블을 선택하십시오. 이 목록에서 테이블을 선택하면 선택한 테이블이 OneView 의 기존 테이블 아래에 표시됩니다.

테이블을 숨기려면 "Hide"(숨기기) 단추를 클릭하십시오.

테이블 정렬

테이블에 있는 각 열의 데이터를 오름차순이나 내림차순으로 정렬할 수 있습니다. 열을 정렬하면 테이블을 손쉽게 구성할 수 있습니다. 예를 들어 "상태"를 기준으로 테이블을 정렬하여 함께 그룹화된 모든 비활성 구성 요소를 볼 수 있습니다.

참고: 열 머리글의 화살표는 정렬된 열을 나타냅니다.

데이터 업데이트 구성

기본적으로 OneView 는 30 초마다 데이터를 업데이트합니다. 다음을 수행할 수 있습니다.

- 자동 업데이트 사이의 경과 시간 수정
- 브라우저를 새로 고칠 때만 데이터를 업데이트하도록 OneView 구성

데이터 업데이트를 구성하려면

1. "업데이트"를 클릭합니다.

   "업데이트" 대화 상자가 열립니다.

2. 다음 중 하나를 선택하십시오.
   - Live Updates(라이브 업데이트) - 지정된 기간 후 데이터를 업데이트합니다. 시간 간격(초)을 지정합니다.
   - Manual Updates(수동 업데이트) - 사용자가 페이지를 새로 고칠 때 데이터를 업데이트합니다.
3. "확인"을 클릭합니다.

설정 저장

설정을 저장하면 다음 사항이 저장됩니다.

- 테이블 정의
- 기본 페이지 표시 내용
- 테이블 정렬
- 업데이트 비율

설정을 저장하려면

1. "설정 저장"을 클릭합니다.

   설정의 이름을 지정할 수 있는 대화 상자가 표시됩니다.

2. 텍스트 상자에 이름을 입력합니다.
3. "확인"을 클릭합니다.

기본 표시 내용 변경

기본 표시 내용을 변경하려면

1. *siteminder_installation*\monitor\settings 에 있는 기본 파일의 이름을 변경합니다.
2. OneView 모니터 콘솔에서 설정을 구성합니다.
3. 설정을 기본값으로 저장합니다.

설정 로드

설정을 로드하려면

1. "설정 로드"를 클릭합니다.

   로드할 설정을 선택할 수 있는 대화 상자가 표시됩니다.
2. 목록 상자에서 설정을 선택합니다.
3. "확인"을 클릭합니다.

제 18 장: SNMP 를 사용한 SiteMinder 모니터링

이 섹션은 다음 항목을 포함하고 있습니다.

SNMP 모니터링

SiteMinder SNMP 모듈을 사용하면 SNMP 호환 네트워크 관리 응용 프로그램으로 SiteMinder 환경의 여러 작업 요소를 모니터링할 수 있습니다.

SNMP 개요

네트워크 관리는 두 유형의 시스템, 즉 관리 시스템이라고 하는 제어 시스템과 관리되는 시스템이라고 하는 관찰 및 제어 대상 시스템 사이에서 이루어집니다. 관리되는 시스템에는 호스트 및 서버와 함께 해당 시스템에서 실행되는 소프트웨어 구성 요소나 라우터 또는 지능형 리피터 등의 네트워크 구성 요소가 포함될 수 있습니다.

상호 운용성을 높이기 위해 상호 운용 시스템은 네트워크 장치 간의 관리 정보 교환을 쉽게 하기 위한 응용 프로그램 계층 프로토콜인 업계 표준 SNMP(Simple Network Management Protocol)를 따릅니다.

전체 SNMP 솔루션은 다음 세 가지 구성 요소로 구성됩니다.

- SNMP MIB(관리 정보 베이스) - 관리되는 개체의 데이터베이스입니다. 관리 시스템은 관리되는 개체, 즉 변수를 읽고 관리되는 시스템에 대한 정보를 제공할 수 있습니다.
- SNMP 에이전트 - 관리되는 시스템에 대한 정보에 액세스하고 관리 시스템에서 해당 정보를 사용할 수 있도록 해 주는 저영향 소프트웨어 모듈입니다. 소프트웨어 시스템의 경우 호스트 운영 체제가 제공하는 마스터 에이전트와 관리되는 응용 프로그램이 제공하는 하위 에이전트 간에 에이전트 기능이 분할될 수도 있습니다.

  참고: 모든 SNMP 구현의 표준 구성 요소인 SNMP 에이전트와 SiteMinder 에이전트를 혼동하지 마십시오.
- SNMP 관리자 - 일반적으로 HP OpenView 와 같은 NMS(네트워크 관리 시스템) 응용 프로그램입니다.

SiteMinder SNMP 모듈은 SiteMinder 환경에 SNMP 요청 처리 및 구성 가능한 이벤트 트래핑 기능을 제공합니다. 이를 위해 SiteMinder OneView 모니터에서 작업 데이터를 수집하고 MIB 에서 SNMP 프로토콜을 지원하는 타사 NMS 응용 프로그램(예: HP OpenView)이 해당 작업 데이터를 사용할 수 있도록 합니다.

참고: 6.0 SNMP 에이전트는 이전 버전의 모든 SiteMinder 5.x 기반 에이전트 응용 프로그램과 호환됩니다.

SiteMinder SNMP 모듈 구성 항목

SiteMinder SNMP 모듈은 다음 항목으로 구성되어 있습니다.

- SiteMinder SNMP MIB - SNMP 호환 네트워크 관리 시스템이 모니터링할 수 있는 SiteMinder 개체의 데이터베이스입니다.
- SiteMinder SNMP 하위 에이전트 - SNMP 마스터 에이전트에서 전달되는 SNMP 요청(GET 및 GETNEXT 만 해당)에 응답합니다.
- SiteMinder 이벤트 관리자 - 정책 서버 이벤트를 캡처하고 SNMP 트랩을 생성합니다(트랩 생성 기능이 구성된 경우). SNMP 트랩은 이벤트가 발생했음을 알리기 위해 SNMP 에이전트가 SNMP NMS 에 임의로 보내는 메시지입니다.

추가 정보:

SiteMinder MIB (페이지 205)
SiteMinder SNMP 지원 시작 및 중지 (페이지 216)

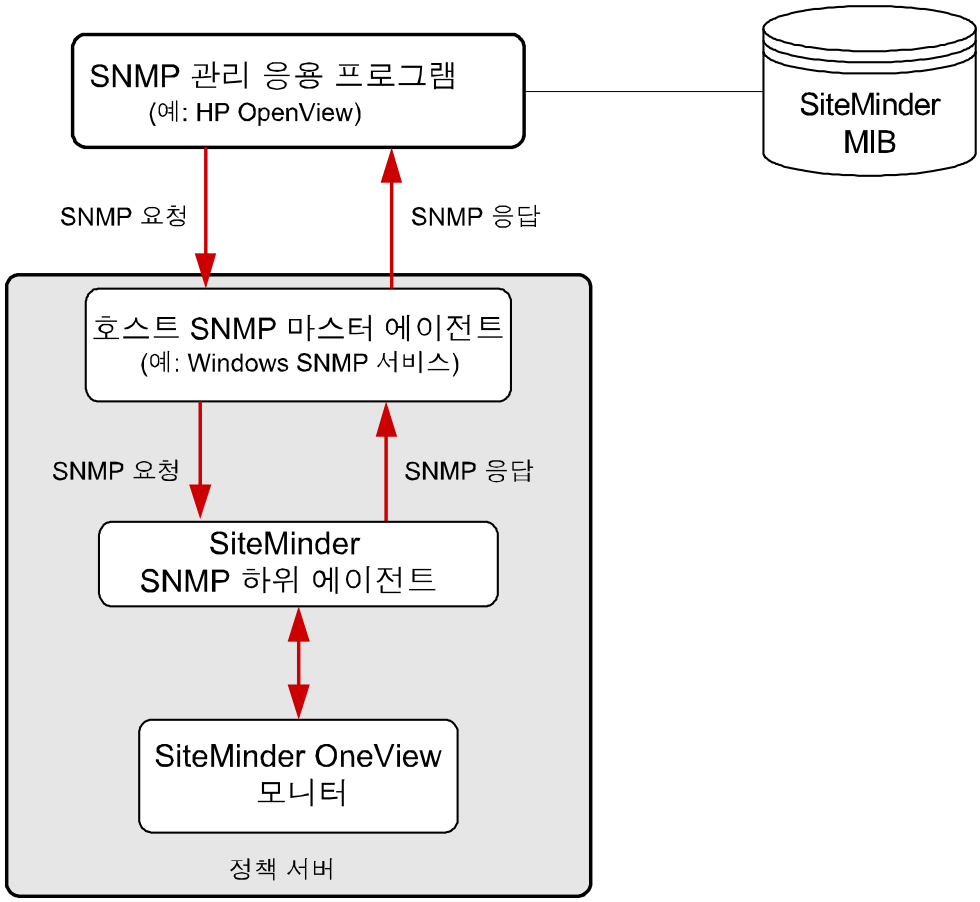
종속성

SiteMinder SNMP 모듈에는 다음과 같은 종속성이 있습니다.

- **SiteMinder OneView 모니터** - SiteMinder SNMP 모듈은 OneView 모니터에서 작업 정보를 가져옵니다. 또한 SiteMinder SNMP 모듈을 실행할 정책 서버에 OneView 모니터가 *반드시* 구성되어 있고 실행 중이어야 합니다.
- **SNMP 마스터 에이전트** - SiteMinder SNMP 모듈은 SNMP 마스터 에이전트를 제공하지 *않습니다*. 또한 SiteMinder SNMP 모듈을 실행 중인 정책 서버의 운영 체제에 적절한 SNMP 마스터 에이전트(Windows SNMP 서비스 또는 Solstice Enterprise Master Agent)가 설치되어 있고 사용되도록 설정되어 있는지 확인해야 합니다.

SNMP 구성 요소 아키텍처 및 데이터 흐름

다음 그림에서는 SNMP 모듈의 데이터 흐름을 보여 줍니다.



SiteMinder SNMP 데이터 흐름

1. SNMP 마스터 에이전트가 관리 응용 프로그램에서 SNMP 요청을 받습니다.
2. SNMP 마스터 에이전트가 SNMP 요청을 SNMP 하위 에이전트에 전달합니다.
3. SiteMinder SNMP 하위 에이전트가 OneView 모니터에서 요청된 정보를 검색합니다.
4. SiteMinder SNMP 하위 에이전트가 검색된 정보를 다시 SNMP 마스터 에이전트에 전달합니다.
5. SNMP 마스터 에이전트가 SNMP 응답을 생성하여 요청하는 관리 응용 프로그램에 보냅니다.

SiteMinder MIB

SiteMinder MIB 는 SiteMinder 환경에서 모니터링되는 모든 구성 요소를 SNMPv2 호환 데이터로 나타냅니다.

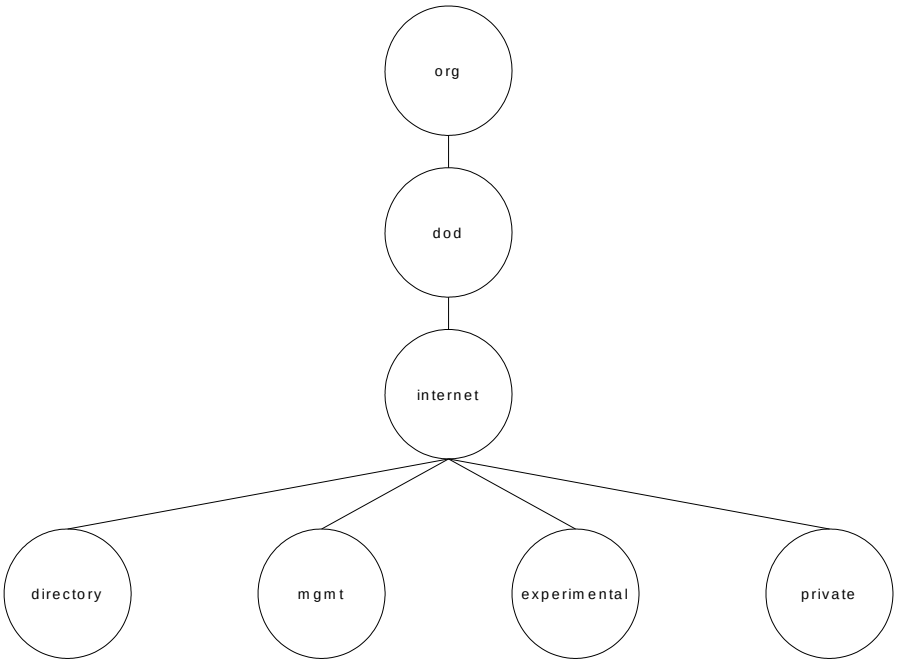
SiteMinder MIB 는 다음 위치에 ASCII 텍스트 파일로 제공됩니다.

SiteMinder_Install_Directory\mibs\NetegritySNMP.mib

MIB 개요

SNMP MIB 구조는 논리적으로 역 트리 계층 구조로 표현됩니다. SiteMinder 와 같은 인터넷 관련 제품의 MIB 는 MIB 계층 구조의 ISO 기본 분기 아래에 있습니다.

다음 그림에서는 ISO 분기의 위쪽 부분을 보여 줍니다.

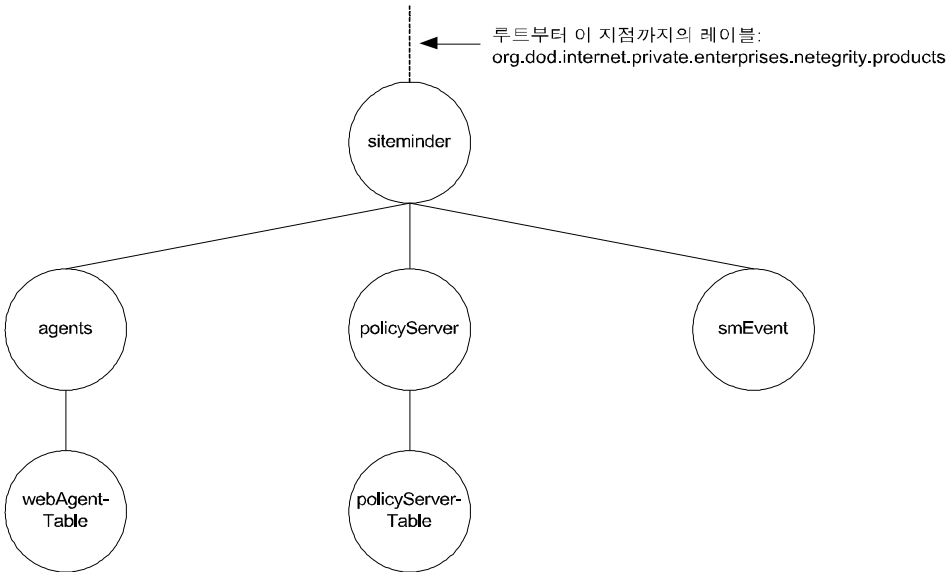


MIB 분기, MIB 및 MIB 내의 관리되는 개체는 모두 짧은 텍스트 문자열로 식별됩니다. 전체 MIB 계층 구조는 분기와 개체 식별자를 연결하고 각 항목을 마침표로 구분하는 표기 방식으로 나타낼 수 있습니다. 예를 들어 위에 표시된 internet 항목의 private 하위 분기는 *iso.org.dod.internet.private* 로 나타낼 수 있습니다.

SiteMinder MIB 계층 구조

SiteMinder MIB 는 *iso.org.dod.internet.private.enterprises.netegrity.products.siteminder* 로 나타낼 수 있습니다.

MIB 개체가 나타내는 지원되는 관리 대상 구성 요소는 정책 서버와 웹 에이전트입니다. 이러한 각 구성 요소의 인스턴스가 여러 개 있을 수 있으므로 이러한 각 구성 요소의 관리되는 속성은 열 형식 개체입니다.



SiteMinder MIB 에는 다음 세 개의 하위 분기가 있습니다.

Policy Server

정책 서버(policyServerTable) 개체를 포함합니다.

agents

웹 에이전트(webAgent) 개체를 포함합니다.

smEvent

시스템 이벤트에 대한 SNMP 트랩 유형을 포함합니다.

MIB 개체 참조

다음 단원에는 정책 서버, 웹 에이전트 및 이벤트 MIB 개체에 대한 상세 목록이 포함되어 있습니다.

인증 서버 데이터

다음 표에서는 SiteMinder MIB 에서 iso.org…siteminder.policyServer.policyServerTable 아래의 개체로 제공되는 인증 서버 속성 중 일부를 보여 줍니다.

개체 이름	SNMP 유형	개체 설명
policyServerIndex	Integer32	현재 정책 서버 인스턴스의 고유 식별자입니다.
policyServerHostID	IP 주소	정책 서버가 설치된 컴퓨터의 IP 주소입니다.
policyServerType	표시 문자열	구성 요소의 유형입니다.
policyServerStatus	Integer32	정책 서버의 상태입니다. 상태는 Active 또는 Inactive 일 수 있습니다.
policyServerPort	Integer32	정책 서버 포트 번호입니다.
policyServerProduct	표시 문자열	정책 서버 제품 이름입니다.
policyServerPlatform	표시 문자열	정책 서버가 설치된 컴퓨터의 운영 체제입니다.
policyServerVersion	표시 문자열	정책 서버의 버전 번호입니다.
policyServerUpdate	표시 문자열	가장 최근에 적용된 업데이트의 버전 번호입니다.
policyServerLabel	표시 문자열	정책 서버 빌드 번호입니다.
policyServerCrypto	Integer32	웹 에이전트와 정책 서버 간에 전송되는 데이터를 암호화하고 암호 해독하는 데 사용되는 암호화 키의 길이입니다.
policyServerUTC	표시 문자열	정책 서버가 설치된 웹 서버의 시작 시간입니다. 이 시간은 UTC(협정 세계 표준시) 형식으로 지정됩니다.
policyServerTime Zone	Integer32	정책 서버가 설치된 지리적 위치의 표준 시간대입니다.
policyServerMaxSockets	Integer32	정책 서버가 지원할 수 있는 열려 있는 소켓의 최대 개수입니다. 이 수는 정책 서버와 웹 에이전트 간의 열려 있는 연결 수에 해당합니다.
policyServerSocketCount	Gauge32	열려 있는 소켓 수로, 정책 서버와 웹 에이전트 간의 열려 있는 연결 수에 해당합니다.

개체 이름	SNMP 유형	개체 설명
policyServerAuth AcceptCount	Counter32	성공한 인증 횟수입니다.
policyServerAuthReject-Count	Counter32	실패한 인증 시도 횟수입니다. 인증 시도는 자격 증명이 잘못된 경우에 실패합니다.
policyServerAzAccept-Count	Counter32	성공한 권한 부여 횟수입니다.
policyServerAzReject-Count	Counter32	실패한 권한 부여 시도 횟수입니다. 인증 시도는 자격 증명이 잘못된 경우에 실패합니다.
policyServerPolicy-Cache Enabled	진리값	정책 캐시가 사용되는지 여부를 나타냅니다.
policyServerL2Cache-Enabled	진리값	L2 캐시가 사용되는지 여부를 나타냅니다.

SiteMinder MIB 의 웹 에이전트 개체

다음 표에서는 SiteMinder MIB 에서 iso.org…siteminder.webAgentTable.webAgentEntry 아래의 개체로 제공되는 웹 에이전트 속성을 보여 줍니다.

개체 이름	SNMP 유형	개체 설명
webAgentIndex	Integer32	현재 웹 에이전트 인스턴스의 고유 식별자입니다.
webAgentHostID	IP 주소	웹 에이전트 서버가 설치된 컴퓨터의 IP 주소입니다.
webAgentType	표시 문자열	구성 요소의 유형입니다.
webAgentStatus	Integer32	웹 에이전트의 상태입니다. 상태는 Active 또는 Inactive 일 수 있습니다.
webAgentPort	Integer32	웹 에이전트 포트 번호입니다.
webAgentProduct	표시 문자열	웹 에이전트 제품 이름입니다.
webAgentPlatform	표시 문자열	웹 에이전트가 설치된 컴퓨터의 운영 체제입니다.
webAgentVersion	표시 문자열	웹 에이전트의 버전 번호입니다.
webAgentUpdate	표시 문자열	가장 최근에 적용된 업데이트의 버전 번호입니다.

개체 이름	SNMP 유형	개체 설명
webAgentLabel	표시 문자열	웹 에이전트 빌드 번호입니다.
webAgentCrypto	Integer32	웹 에이전트와 정책 서버 간에 전송되는 데이터를 암호화하고 암호 해독하는 데 사용되는 암호화 키의 길이입니다.
webAgentUTC	표시 문자열	웹 에이전트가 설치된 웹 서버의 시작 시간입니다. 이 시간은 UTC(협정 세계 표준시) 형식으로 지정됩니다.
webAgentTime Zone	Integer32	웹 에이전트가 설치된 지리적 위치의 표준 시간대입니다.
webAgentSocketCount	Gauge32	열려 있는 소켓 수로, 정책 서버와 웹 에이전트 간의 열려 있는 연결 수에 해당합니다. **참고:** 웹 에이전트 아키텍처가 변경되었기 때문에 SocketCount 에는 값이 없습니다.
webAgentResource-CacheCount	Integer32	리소스 캐시의 항목 수입니다. 리소스 캐시에는 최근에 액세스한 리소스에 대한 정보가 저장되므로 동일한 리소스에 대한 이후 요청을 빠르게 처리할 수 있습니다. 리소스 캐시의 항목 수는 0 에서 *n* 사이일 수 있습니다. 여기서 n 은 웹 에이전트 구성에 지정된 최대 캐시 크기입니다.
webAgentResource-CacheHits	Integer32	리소스 캐시에 액세스한 횟수입니다. 이 숫자는 SiteMinder 가 캐시된 리소스를 사용하는 빈도를 나타냅니다.
webAgentResource-CacheMisses	Integer32	웹 에이전트가 리소스 캐시에서 리소스를 찾지 못한 횟수입니다. 이는 다음과 같은 경우에 발생합니다. ■ 이전에 리소스에 액세스한 적이 없는 경우 ■ 캐시된 정보가 만료된 경우

개체 이름	SNMP 유형	개체 설명
webAgentUserSession-CacheCount	Integer32	사용자 세션 캐시의 항목 수입니다. 사용자 세션 캐시에는 최근에 리소스에 액세스한 사용자에 대한 정보가 저장됩니다. 사용자 정보를 저장하면 리소스 요청이 빠르게 처리됩니다. 사용자 세션 캐시의 항목 수는 0 에서 *n* 사이일 수 있습니다. 여기서 *n* 은 웹 에이전트 구성에 지정된 최대 캐시 크기입니다. **참고:** 사용자 세션 캐시 수는 세션 캐시가 있는 웹 서버에 따라 달라질 수 있습니다.
webAgentUserSession-CacheHits	Integer32	웹 에이전트가 사용자 세션 캐시에 액세스한 횟수입니다.
webAgentUserSession-CacheMisses	Integer32	웹 에이전트가 사용자 세션 캐시에서 사용자 세션 정보를 찾지 못한 횟수입니다. 이는 다음과 같은 경우에 발생합니다. ■ 사용자가 이전에 리소스에 액세스한 적이 없는 경우 ■ 캐시된 정보가 만료된 경우
webAgentIsProtected-Count	Integer32	웹 에이전트가 정책 서버에서 리소스 보호 여부를 확인한 횟수입니다. **참고:** 리소스 캐시가 0 으로 설정된 경우 각 로그인 시도에 대해 둘 이상의 IsProtected 호출이 기록될 수 있습니다. 정보를 캐시하지 않는 경우 웹 에이전트는 웹 서버에 대한 요청이 있을 때마다 정책 서버에서 리소스 보호 여부를 확인해야 합니다. 리소스 캐시가 0 으로 설정되어 있지 않으면 IsProtected 호출이 하나만 기록됩니다. 이 경우 웹 에이전트는 정책 서버에 대해 IsProtected 를 한 번만 호출하며, 이후 캐시의 리소스가 만료되거나 리소스 캐시가 플러시될 때까지는 웹 서버에 동일한 리소스가 요청될 때마다 웹 에이전트의 리소스 캐시에서 요청이 처리됩니다.
webAgentIsProtected-Errors	Integer32	웹 에이전트가 정책 서버에 리소스 보호 여부를 확인할 때 발생한 오류 수입니다. 이 오류는 웹 에이전트와 정책 서버 간의 통신 오류를 나타냅니다.

개체 이름	SNMP 유형	개체 설명
webAgentIsProtected-AvgTime	Unsigned32	웹 에이전트가 정책 서버에서 리소스 보호 여부를 확인하는 데 소요되는 평균 시간입니다.
webAgentLoginCount	Counter32	해당 웹 에이전트가 시도한 로그인 횟수입니다.
webAgentLoginErrors	Counter32	로그인 시도 중 발생한 오류 수입니다. 이 오류는 웹 에이전트와 정책 서버 간의 통신 오류를 나타냅니다.
webAgentLoginFailures	Counter32	사용자가 정책 서버에서 인증되지 않았거나 권한이 부여되지 않아 실패한 로그인 시도 횟수입니다.
webAgentLoginAvgTime	Unsigned32	사용자가 리소스에 로그인하는 데 소요되는 평균 시간입니다.
webAgentValidation-Count	Counter32	특정 웹 에이전트가 사용자 인증을 위해 사용자의 자격 증명을 사용자 디렉터리 항목과 비교하는 대신 정책 서버에 대해 세션 쿠키의 유효성을 검사하려고 시도한 횟수입니다. 웹 에이전트는 사용자가 성공적으로 인증되면 사용자의 브라우저에 세션 쿠키를 생성하며, 이후에 해당 사용자가 새 리소스를 요청할 때 이 쿠키를 사용하여 사용자를 인증합니다.
webAgentValidation-Errors	Counter32	웹 에이전트가 사용자 세션의 유효성 검사를 시도할 때 발생한 오류 수입니다. 이 오류는 웹 에이전트와 정책 서버 간의 통신 오류를 나타냅니다.
webAgentValidation-Failures	Counter32	웹 에이전트가 유효하지 않은 세션 쿠키로 인해 사용자 세션의 유효성을 검사하는 데 실패한 횟수입니다.
webAgentValidation-AvgTime	Unsigned32	사용자 인증 시 사용되는 쿠키의 유효성을 검사하는 데 소요되는 평균 시간(밀리초)입니다. 쿠키는 싱글 사인온 환경에서 사용자를 인증하는 데 사용될 수 있습니다.
webAgentAuthorize-Count	Counter32	해당 에이전트에서의 권한 부여 시도 횟수입니다. 사용자가 보호된 리소스에 액세스하기 위해 정책 서버에 자격 증명을 제공하면 권한 부여 시도가 발생합니다.

개체 이름	SNMP 유형	개체 설명
webAgentAuthorize-Errors	Counter32	해당 웹 에이전트가 권한 부여를 시도하는 동안 발생한 오류 수입니다. 이 오류는 권한 부여 호출 중 웹 에이전트와 정책 서버 간에 발생한 통신 오류를 나타냅니다.
webAgentAuthorize-Failures	Counter32	실패한 권한 부여 시도 횟수입니다. 사용자가 잘못된 자격 증명을 입력하면 권한 부여 시도가 실패합니다.
webAgentAuthorize-AvgTime	Integer32	사용자에게 권한을 부여하는 데 소요되는 평균 시간(밀리초)을 나타냅니다.
webAgentCrosssite-ScriptHits	Integer32	교차 사이트 스크립팅 적중 횟수입니다. 교차 사이트 스크립팅 적중은 사이트의 페이지에 포함된 악의적 코드로 구성됩니다. 교차 사이트 스크립팅에 대한 자세한 내용은 *SiteMinder 웹 에이전트 구성 안내서*를 참조하십시오.
webAgentBadURL-charsHits	Integer32	잘못된 URL 문자 때문에 에이전트가 거부한 요청 수입니다. 잘못된 URL 문자는 특히 웹 클라이언트가 SiteMinder 규칙을 위반하지 못하도록 하기 위해 차단됩니다. 이러한 문자는 웹 에이전트 구성에서 지정합니다.
webAgentBadCookie-HitsCount	Gauge32	웹 에이전트가 암호 해독하지 못한 쿠키 수입니다.
webAgentExpired-CookieHitsCount	Gauge32	만료된 쿠키가 포함된 요청 수입니다.

이벤트 데이터

다음 표에서는 SiteMinder MIB 에서 iso.org…siteminder.smEvents 아래에 표시되는 개체, 즉 SiteMinder 이벤트 관리자를 사용하여 SNMP 트랩에 매핑할 수 있는 시스템 이벤트 개체를 보여 줍니다.

이벤트 이름	이벤트 ID	이벤트 범주	이벤트 범주 유형
serverInit	SmLogSystemEvent_ServerInit	서버 작업	시스템
serverUp	SmLogSystemEvent_ServerUP		
serverDown	SmLogSystemEvent_ServerDown		
serverInitFail	SmLogSystemEvent_ServerInitFail		
dbConnectionFailed	SmLogSystemEvent_DbConnectFail		
ldapConnection-Failed	SmLogSystemEvent_LDAP-ConnectFail		
logFileOpenFail	SmLogSystemEvent_LogFile-OpenFail	시스템 작업	
agentConnection-Failed	SmLogSystemEvent_Agent-ConnectionFail		
authReject	SmLogAccessEvent_AuthReject	인증	액세스
validateReject	SmLogAccessEvent_ValidateReject		
azReject	SmLogAccessEvent_AzReject	권한 부여	
adminReject	SmLogAccessEvent_AdminReject	관리	
objectLoginReject	SmLogObjEvent_LoginReject	인증	개체
objectFailedLoginAttemptsCount	SmLogObjEvent_FailedLogin-AttemptsCount		

이벤트 이름	이벤트 ID	이벤트 범주	이벤트 범주 유형
emsLoginFailed	SmLogEmsEvent_LoginFail	디렉터리 세션	EMS
emsAuthFailed	SmLogEmsAuthFail		

SiteMinder 이벤트 관리자 구성

정책 서버 이벤트를 캡처하는 이벤트 관리자 응용 프로그램(라이브러리 파일 EventSNMP.dll 로 제공됨)은 정책 서버 이벤트에 대한 SNMP 트랩을 생성해야 하는지 여부(구성 파일에 지정됨)를 확인하고, 필요한 경우 지정된 NMS 에 SNMP 트랩을 생성합니다.

이벤트 라이브러리(EventSNMP.dll)를 구성하려면 이벤트 처리기 라이브러리 추가 (페이지 144)를 참조하십시오.

처리할 이벤트와 트랩을 보내야 하는 대상 NMS 의 주소를 정의하는 이벤트 구성 파일(*SM_Install_Directory*\config\snmptrap.conf)을 정의하여 SiteMinder 이벤트 관리자를 구성할 수 있습니다.

이벤트 구성 파일 구문

snmptrap.conf 는 다음과 같이 이벤트 구문당 간단한 행 하나가 있는 편집 가능한 ASCII 파일입니다.

Event_Name Destination_Address

Event_Name

MIB 이벤트 개체의 이름(또는 쉼표로 구분된 이벤트 개체 이름 그룹)입니다.

예:

serverUP

serverUp,serverDown

serverUp,serverDown,serverInitFail

Destination_Address

생성된 트랩을 보낼 대상 NMS 의 주소(또는 쉼표로 구분된 NMS 주소 그룹)입니다. 각 주소는 *HostID*:*port*:*community* 형식이어야 합니다.

HostID

(필수) 호스트 이름이나 IP 주소입니다.

Port

(선택 사항) IP 포트 번호입니다.

기본값: 162

community

(선택 사항) SNMP 커뮤니티입니다. community 를 지정한 경우 port 도 지정해야 합니다.

기본값: "public"

예: 100.132.5.166

예: 100.132.5.166:162

예: victoria:162:public

참고: 이벤트가 중복되지 않도록 주의하십시오. 즉, 여러 항목에 동일한 이벤트를 배치하지 않아야 합니다. 또한 "#" 문자를 접두사로 사용하여 주석 행을 추가할 수 있습니다.

이벤트 구성 파일 예

```
ServerDown,serverUp     111.123.0.234:567:public
```

이 항목은 이벤트 관리자가 serverDown 및 serverUp SNMP 트랩을 IP 주소 111.123.0.234, 포트 567 의 공용 커뮤니티에 있는 NMS 로 보내도록 구성합니다.

```
agentConnectionFailed    111.123.0.234,victoria
```

이 항목은 이벤트 관리자가 agentConnectionFailed 유형의 SNMP 트랩을 IP 주소 111.123.0.234, 포트 567 의 공용 커뮤니티와 포트 567 의 공용 커뮤니티에 있는 호스트 "victoria"로 보내도록 구성합니다.

```
azReject
```

이 항목은 이벤트 관리자가 azReject 유형의 모든 이벤트를 삭제하여 트랩을 보내지 않도록 구성합니다.

SiteMinder SNMP 지원 시작 및 중지

정책 서버를 설치할 때 SiteMinder SNMP 지원을 설치하도록 선택한 경우 정책 서버가 초기화될 때마다 SiteMinder SNMP 에이전트 서비스가 자동으로 시작됩니다.

이 단원에서는 Windows 및 UNIX 정책 서버에서 SiteMinder SNMP 하위 에이전트를 수동으로 시작 및 중지하는 방법에 대해 설명합니다.

Windows Netegrity SNMP 에이전트 서비스 시작 및 중지

Windows 정책 서버에서 SiteMinder SNMP 하위 에이전트를 시작하려면

1. "서비스" 제어판을 엽니다.
   - (Windows Server) "시작", "설정", "제어판", "관리 도구", "서비스"를 차례로 클릭합니다.
   - (Windows NT) "시작", "설정", "제어판", "서비스"를 차례로 클릭합니다.
2. "Netegrity SNMP Agent"(Netegrity SNMP 에이전트) 서비스를 선택합니다.
3. "시작"을 클릭합니다.

   참고: Windows SNMP 서비스를 다시 시작할 경우 Netegrity SNMP 에이전트 서비스도 수동으로 다시 시작하십시오.

Windows 정책 서버에서 SiteMinder SNMP 하위 에이전트를 중지하려면

1. "서비스" 제어판을 엽니다.
   - (Windows Server) "시작", "설정", "제어판", "관리 도구", "서비스"를 차례로 클릭합니다.
   - (Windows NT) "시작", "설정", "제어판", "서비스"를 차례로 클릭합니다.
2. "Netegrity SNMP Agent"(Netegrity SNMP 에이전트) 서비스를 선택합니다.
3. "중지"를 클릭합니다.

   참고: Windows SNMP 서비스를 중지할 경우 Netegrity SNMP 에이전트 서비스는 일반적으로 사용할 수 없게 되지만 포트 801 을 통해 액세스할 수 있습니다.

UNIX 정책 서버에서 SNMP 지원 시작 및 중지

UNIX 정책 서버에서는 Solstice Enterprise Master Agent(snmpdx) 데몬을 시작 또는 중지하는 방법으로만 SiteMinder 서비스를 시작하거나 중지할 수 있습니다.

UNIX 정책 서버에서 Netegrity SNMP 에이전트 서비스를 시작하려면

1. 슈퍼 사용자(루트)로 로그인합니다.
2. cd /etc/rc3.d 를 입력합니다.
3. sh SXXsnmpdx (S76snmpdx) start 를 입력합니다.

UNIX 정책 서버에서 Netegrity SNMP 에이전트 서비스를 중지하려면

1. 슈퍼 사용자(루트)로 로그인합니다.
2. cd /etc/rc3.d 를 입력합니다.
3. sh SXXsnmpdx (S76snmpdx) stop 을 입력합니다.

   참고: Sun Solstice Enterprise Master Agent 작업을 중지하면 UNIX 호스트의 모든 SNMP 서비스가 사용되지 않도록 설정됩니다.

SiteMinder SNMP 모듈 문제 해결

이 단원에서는 SiteMinder 에 대한 관리 연결을 설정하거나 SiteMinder 에서 SNMP 트랩을 받는 데 문제가 있을 경우 문제 부분을 정확히 파악할 수 있도록 SiteMinder 에서 제공하는 몇 가지 도구와 권고 사항에 대해 설명합니다.

이벤트 후 SNMP 트랩을 받지 못함

증상:

SNMP 트랩을 생성해야 하는 이벤트가 발생해도 SNMP 트랩이 수신되지 않습니다.

해결책:

1. NMS 와 모니터링되는 정책 서버 간의 네트워크 연결을 확인합니다.
2. SiteMinder SNMP 하위 에이전트와 SNMP 마스터 에이전트가 정책 서버에서 실행 중인지 확인합니다.
3. NETE_SNMPLOG_ENABLED 시스템 환경 변수를 설정하여 트랩 로깅이 사용되도록 설정합니다.

   SiteMinder 는 sminstalldir/log 에 다음과 같은 로그 파일을 생성합니다.

   Windows:

   ```
   SmServAuth_snmptrap.log
   SmServAz_snmptrap.log
   SmServAcct_snmptrap.log
   SmServAdm_snmptrap.log
   ```

   UNIX:

   ```
   smservauth_snmptrap.log
   smservaz_snmptrap.log
   smservacct_snmptrap.log
   smservadm_snmptrap.log
   ```

중요! 생성되는 로그 파일이 매우 급속히 증가할 수 있습니다. 트랩 수신 문제를 해결한 후에는 즉시 트랩 로깅이 사용되지 않도록 설정하고 이러한 파일을 삭제해야 합니다.

제 19 장: SiteMinder 보고서

이 섹션은 다음 항목을 포함하고 있습니다.

보고서 설명

SiteMinder 보고서는 다음 두 그룹으로 구성됩니다.

- 감사 보고서
- 분석 보고서

감사 보고서는 정책 서버의 기존 감사 기능을 통해 생성됩니다. 따라서 정책 서버가 데이터베이스에 쓰도록 구성되어 있어야 합니다.

분석 보고서는 어떤 사용자가 어떤 태스크를 수행할 수 있는지 평가하는 등의 런타임 정책 평가를 기반으로 합니다.

SiteMinder 관리 UI 를 사용하여 다음 보고서를 생성할 수 있습니다.

사용자별 작업

지정된 기간 동안 모든 사용자의 작업을 나열합니다.

관리자별 관리 작업

관리자별 정책 저장소의 모든 관리 작업을 나열합니다.

응용 프로그램

사용자에게 사용 권한이 부여된 모든 구성된 응용 프로그램을 나열합니다.

사용자별 응용 프로그램

지정된 응용 프로그램 집합의 모든 사용자를 나열합니다.

거부된 권한

거부된 모든 권한을 나열합니다.

거부된 리소스

요청된 리소스 중 거부된 모든 리소스를 나열합니다.

역할별 정책

응용 프로그램의 지정된 역할 집합에 대한 모든 정책을 나열합니다.

보호된 리소스

모든 보호된 리소스(영역 + 규칙 필터)를 나열합니다.

리소스 작업

리소스별 인증 및 권한 부여 작업을 모두 나열합니다.

사용자별 리소스

지정된 사용자 집합의 모든 리소스를 나열합니다.

응용 프로그램별 역할

지정된 각 응용 프로그램에 대해 정의된 모든 역할을 나열합니다.

리소스별 역할

지정된 리소스에 대해 정의된 모든 역할을 나열합니다.

리소스별 사용자

지정된 각 리소스와 연결된 모든 사용자를 나열합니다. 이 보고서를 실행할 경우 사용자 디렉터리에서 유효한 유니버설 ID 를 설정해야 합니다.

역할별 사용자

지정된 역할에 속하는 모든 사용자를 나열합니다.

SiteMinder 보고서 예약

관리 UI 의 "보고서" 탭에서 SiteMinder 감사 또는 분석 보고서를 예약할 수 있습니다.

다음 단계를 수행하십시오.

1. "보고서", "감사" 또는 "분석"을 클릭합니다.
2. 원하는 보고서를 선택합니다.
3. 필요한 매개 변수를 모두 채웁니다. 이러한 매개 변수는 보고서 유형에 따라 달라집니다.
4. "다음"을 클릭합니다.
5. 드롭다운 목록에서 옵션 하나를 선택합니다.
6. 설명을 입력합니다.
7. 제출을 클릭합니다.

SiteMinder 보고서 보기

관리 UI 의 "보고서" 탭에서 "완료" 상태의 SiteMinder 보고서를 볼 수 있습니다. 상태가 "Failed"(실패)인 경우 상태 상세 정보를 볼 수 있습니다.

SiteMinder 보고서를 보려면

1. "보고서", "일반", "SiteMinder 보고서 보기"를 차례로 클릭합니다.

   "SiteMinder Report Search"(SiteMinder 보고서 검색) 창이 나타납니다.
2. 보려는 보고서의 라디오 단추를 클릭합니다. "상태" 필드에 해당 보고서가 완료된 것으로 표시되어야 합니다.
3. "선택"을 클릭합니다.

   화면에 보고서가 표시됩니다.
4. (선택 사항) 보고서를 파일로 저장하려는 경우 파일 아이콘을 클릭합니다. 드롭다운 목록에서 출력 파일 형식을 선택합니다.
5. (선택 사항) 프린터 아이콘을 클릭하여 보고서를 인쇄합니다.
6. (선택 사항) 보고서 페이지를 탐색하거나 검색 문자열을 입력할 수 있습니다.
7. 보고서 보기를 마쳤으면 "닫기"를 클릭합니다.

SiteMinder 보고서 삭제

관리 UI 의 "보고서" 탭에서 SiteMinder 보고서를 하나 이상 삭제할 수 있습니다.

SiteMinder 보고서를 삭제하려면

1. "보고서", "일반", "SiteMinder 보고서 삭제"를 차례로 클릭합니다.

   "SiteMinder 보고서 삭제" 창이 열립니다.

2. 보고서 이름이나 설명을 기준으로 삭제할 SiteMinder 보고서를 검색하거나 모든 SiteMinder 보고서를 검색합니다.
3. 삭제할 SiteMinder 보고서를 하나 이상 또는 모두 선택하고 "제출"을 클릭합니다.

처리를 위해 "SiteMinder 보고서 삭제" 태스크가 제출됩니다.

제 20 장: 정책 서버 도구

이 섹션은 다음 항목을 포함하고 있습니다.

정책 서버 도구 소개

SiteMinder 에는 환경을 관리하는 데 도움이 되는 다양한 관리 도구가 있습니다. 다음 목록에서는 각 도구의 기능에 대해 설명합니다.

smobjimport

SiteMinder 정책 저장소로 정책 데이터를 가져옵니다.

참고: 기존 백업 smdif 파일을 정책 저장소로 가져오는 경우에만 이 유틸리티를 사용할 수 있습니다. 수동으로 정책 저장소를 마이그레이션하려면 XPSExport 및 XPSImport 유틸리티를 사용하십시오.

smkeyexport

키 저장소에서 키를 내보냅니다.

smkeyimport

키 저장소로 키를 가져옵니다.

smkeytool

인증서 데이터 저장소를 관리할 수 있습니다.

12.52 SP1 버전으로 마이그레이션하는 동안 기존 smkeydatabase 를 관리하기 위해 이 유틸리티와 레거시 키 저장소 액세스 플래그(-accessLegacyKS)를 사용할 수도 있습니다.

참고: smkeydatabase 의 콘텐츠를 인증서 데이터 저장소로 마이그레이션하는 것에 대한 자세한 내용은 *SiteMinder 업그레이드 안내서*를 참조하십시오.

smldapsetup

LDAP 디렉터리에서 SiteMinder 정책 저장소를 관리합니다.

ODBC 데이터베이스 SQL 스크립트

ODBC 데이터베이스에서 SiteMinder 정책 저장소, 토큰 데이터 및 로그 스키마를 제거합니다.

smpatchcheck

Solaris 시스템에 모든 필수/권장 패치가 설치되어 있는지 확인합니다.

smreadclog

정책 서버가 생성하는 RADIUS 로그 파일을 읽습니다.

smreg

SiteMinder 슈퍼 사용자 암호를 변경할 수 있습니다.

SiteMinder 에서는 정책 데이터 작업에 사용하는 도구도 제공합니다. 다음 목록에서는 XPS 도구 모음을 간략하게 보여 줍니다. XPS 도구는 플랫폼 독립적인 명령줄 유틸리티로, XPS 관리자가 정책 저장소 데이터를 관리하는 데 사용할 수 있습니다. 특정 도구의 다양한 옵션에 대해 알아보려면 명령줄에서 도구 이름을 입력한 다음 물음표를 입력하십시오. 예를 들면 다음과 같습니다.

```
XPSConfig ?
```

XPSConfig

공급업체, 제품 및 제품 매개 변수를 포함하는 구성 데이터를 관리합니다.

참고: XPSConfig 를 사용하려면 관리자 계정에 XPSConfig 권한이 있어야 합니다.

XPSEvaluate

식을 평가하고 성능을 테스트할 수 있습니다.

참고: XPSEvaluate 를 사용하려면 관리자 계정에 XPSEvaluate 권한이 있어야 합니다.

XPSExplorer

공급업체, 제품 및 응용 프로그램을 비롯한 정책 데이터를 관리합니다.

참고: XPSExplorer 를 사용하려면 관리자 계정에 XPSExplorer 권한이 있어야 합니다.

XPSExport

정책 저장소에서 데이터를 내보냅니다.

XPSImport

정책 저장소로 데이터를 가져옵니다.

XPSSecurity

XPS 관리자 및 관련 권한을 대화형으로 작성하고 편집할 수 있습니다. 이 도구를 사용하려면 Support 사이트에서 다운로드한 SiteMinder 설치 파일의 \win32\tools 또는 /solaris/tools 에 있는 도구를 *siteminder_home*\bin 으로 복사합니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

중요! XPSSecurity 를 사용한 후에는 권한 없는 사용자가 사용하지 못하도록 *siteminder_home*\bin 에서 삭제하십시오.

참고: XPSSecurity 를 사용하려면 관리자 계정에 XPSSecurity 권한이 있어야 합니다.

XPSSweeper

XPS 및 SiteMinder 정책 저장소를 동기화합니다.

참고: XPSSweeper 를 사용하려면 관리자 권한이 필요합니다. 다른 추가 권한은 필요하지 않습니다.

Windows 2008 정책 서버 도구 요구 사항

Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하려면 시스템에 관리자로 로그인했더라도 관리자 권한으로 명령줄 창을 열어야 합니다. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

Linux Red Hat 에서 정책 서버 도구 사용 시 요구 사항

Linux Red Hat 운영 체제에서 정책 서버 도구가 제대로 작동할 수 있도록 /etc/hosts 에서 정책 서버 호스트 이름을 정의하십시오. 이 위치에 호스트 이름을 정의하는 이유는 이러한 유틸리티가 adminoid 및 OID 를 생성하기 때문입니다. 운영 체제에서는 이러한 OID 를 생성할 때 gethostid() 및 gettimeofday() Linux 함수를 사용합니다.

smobjimport 를 사용하여 정책 데이터 가져오기

smobjimport 도구를 사용하여 전체 정책 저장소 또는 단일 정책 도메인을 가져올 수 있습니다.

참고: 기존 백업 smdif 파일을 정책 저장소로 가져오는 경우에만 이 유틸리티를 사용할 수 있습니다. 수동으로 정책 저장소를 마이그레이션하려면 XPSExport 및 XPSImport 유틸리티를 사용하십시오.

다음 단계를 수행하십시오.

1. 다음 위치 중 하나로 이동합니다.
   - (Windows) *siteminder_home*\bin

     siteminder_home

     정책 서버 설치 경로를 지정합니다.
   - (Unix) *siteminder_home*/bin
2. 다음 명령을 실행합니다.

   ```
   smobjimport -ifile_name -dadmin-name -wadmin-pw -v -t [-cf | -cb]
   ```

   예 1: smobjimport -ipstore.smdif -dSiteMinder -wpassword -v -t -cf

   예 2: smobjimport -ipstore.smdif -dSiteMinder -wpassword -v -t -cb

   -cf

   (선택 사항) FIPS 호환(AES) 암호화 알고리즘을 사용하여 중요한 데이터를 가져옵니다.

   참고: 이 인수는 정책 서버가 FIPS 전용 모드에서 실행 중인 경우에만 필요합니다.

   -cb

   (선택 사항) RC2 암호화 알고리즘을 사용하여 중요한 데이터를 가져옵니다.

   중요!

   - 가져오려는 파일에 중요한 데이터가 일반 텍스트로 포함되어 있는 경우 데이터를 가져오려면 다음 옵션을 사용해야 합니다.

     -c

     이 옵션을 사용하지 않으면 정책 저장소가 손상될 수 있습니다.

- smobjimport 명령에는 smdif 파일만 입력하십시오. smdif 파일과 cfg 파일이 한 디렉터리에 있으면 유틸리티가 자동으로 두 파일을 모두 가져옵니다. cfg 파일에 저장된 환경 속성이 smdif 파일에 저장된 환경 속성보다 우선합니다. 다른 cfg 파일을 smdif 파일과 조합하여 환경 데이터를 덮어쓸 수 있습니다.

XML 기반 데이터 형식 개요

엔터프라이즈 환경에서는 정책 저장소 데이터를 한 환경에서 다른 환경으로(예: 개발 환경에서 스테이징 환경으로) 이동해야 하는 경우가 있습니다. r12 이전 릴리스에서는 정책 개체가 데이터 마이그레이션을 위한 smobjimport 및 smobjexport 를 사용하여 고유한 SMDIF(SiteMinder 데이터 교환 형식)로 표현되었습니다. 이 내보내기 형식과 이러한 도구는 이제 XPSExport 와 XPSImport 를 사용하여 데이터를 마이그레이션하는 XML 기반 내보내기 형식으로 대체되었습니다.

XML 기반 내보내기 형식에는 다음과 같은 기본 스키마가 사용됩니다.

XPSDeployment.xsd

다른 스키마를 포함하는 최상위 스키마를 설명합니다. 이 스키마는 루트 요소와 하위 요소를 정의합니다. 이 스키마를 준수하는 XML 파일에는 데이터 사전, 정책 및 보안 데이터의 인스턴스가 포함될 수 있습니다.

XPSDataDictionary.xsd

개체 유형 및 해당 속성에 대한 메타 데이터 정보를 설명합니다.

XPSPolicyData.xsd

도메인, 정책, 규칙, 응용 프로그램 및 이러한 개체 간의 관계 등 정책 저장소에 저장된 개체에 대한 메타 데이터 정보를 설명합니다.

XPSSecurityData.xsd

정책 저장소 관리자와 관리자의 액세스 권한을 나타내는 데 사용되는 메타 데이터를 설명합니다.

XPSGeneric.xsd

다른 스키마 파일에 사용되는 일반 데이터 형식의 정의가 포함되어 있습니다.

이 형식을 사용하면 정책 데이터 전체를 내보내고 가져올 수 있을 뿐 아니라 정책 데이터를 일부만 내보내고 가져올 수도 있습니다. 세부적 내보내기를 수행할 경우 데이터를 가져오는 방법을 알고 있어야 합니다. 내보낼 때 개체 식별자와 다음 내보내기 유형 중 하나를 선택적으로 사용하여 정책 데이터 전체나 일부를 지정할 수 있습니다.

- 추가 - 가져오기 중 추가만 수행할 수 있도록 지정합니다.
- 대체 - 가져오기 중 기존 정책 데이터를 덮어쓰도록 지정합니다.
- 오버레이 - 가져오기 중 정책 데이터에 대한 업데이트를 수행하도록 지정합니다.

참고: XPSExport 및 XPSImport 도구는 정책 서버가 작동하는 FIPS 모드에 따라 중요한 데이터를 암호화합니다. 이러한 도구에는 데이터 암호화를 위해 설정할 추가 매개 변수가 없습니다.

XPSExport

XPSExport 도구는 정책 저장소 데이터 마이그레이션을 위한 다음 태스크를 지원합니다.

- 모든 보안 데이터 내보내기
- 모든 정책 데이터 내보내기
- 모든 구성 데이터 내보내기
- 일부 정책 데이터 내보내기

루트 개체의 식별자를 지정하여 일부 정책 데이터를 내보낼 수 있습니다. -xf 매개 변수를 사용하여 명령줄 또는 파일에 이 식별자를 지정하십시오. 부모 클래스가 없는 개체만 내보낼 수 있습니다. 예를 들어 영역 개체를 내보내려면 해당 영역에 대한 부모 도메인의 식별자(XID)를 지정해야 합니다.

XPSExplorer(XPSExplorer -xf)의 "쇼핑 카트" 기능, 즉 XCart 를 사용하여 사용자 지정 내보내기 파일을 생성하고 편집할 수도 있습니다. 가져오기 모드(ADD, OVERLAY, REPLACE 또는 DEFAULT)를 XCart 파일의 개체 단위로 설정할 수 있습니다. 그런 다음 -xf 매개 변수를 사용하여 XCart 파일을 XSPExport 에 전달할 수 있습니다.

다음 사항을 고려하십시오.

- XPSExport 는 키 저장소에서 키를 내보내지 *않습니다*. 키를 내보내려면 smkeyexport 명령을 사용하십시오.
- 특정 환경의 정책을 다른 환경으로 이동하는 경우 해당 환경에만 사용되는 일부 개체가 내보내기 파일에 포함됩니다. 예를 들면 다음과 같은 개체입니다.
  - 트러스트된 호스트
  - HCO 정책 서버 설정
  - 인증 체계 URL
  - 암호 서비스 리디렉션
  - 리디렉션 응답

XPSExport 를 사용할 때 선택하는 모드에 따라 이러한 개체가 새 환경에 추가되거나 기존 설정을 덮어쓸 수 있습니다. 이러한 개체를 가져올 때는 환경 설정에 부정적인 영향이 없는지 확인하십시오.

구문

XPSExport 구문은 다음과 같습니다.

```
XPSExport output_file [-xo object_XID] [-xo-add object_XID] [-xo-replace object_XID]
[-xo-overlay object_XID] [-xf file_name] [-xb] [-xe] [-xp] [-xs] [-xc] [-xi] [-xm]
[-f] [-fm] [-q] [-m <number>[%]] [-pass <passphrase>][-npass] [-comment comment]
[-cf commentpath] [-?] [-vT] [-vI] [-vW] [-vE] [-vF] [-l log_file] [-e err_file]
```

매개 변수

output_file

출력 XML 파일입니다.

-xo *object_XID*

세부적으로 내보낼 개체를 하나 이상 지정합니다. 필요에 따라 다음 내보내기 유형 중 하나를 지정할 수 있습니다.

-xo-add *object_XID*

가져오는 동안 추가 작업만 수행되도록 지정합니다.

-xo-replace *object_XID*

가져오는 동안 정책 데이터를 덮어씁니다.

-xo-overlay *object_XID*

가져오는 동안 정책 데이터를 업데이트합니다.

-xf *file_name*

(선택 사항) 내보낼 개체의 XID 목록을 포함하는 파일의 절대 이름을 지정합니다.

이 파일에 입력되는 내용은 다음 형식을 따릅니다.

CA.SM::UserDirectory@0e-255e2456-556d-40fb-93cd-f2fed81f656e

ADD = CA.SM::AuthScheme@0d-4afc0e41-ae25-11d1-9cdd-006008aac24b

REPLACE = CA.SM::Agent@01-cb8b3401-a6aa-4794-964e-c569712269c0

OVERLAY = CA.SM::Domain@03-7bdf31f2-44d7-4d7b-a8f5-5de2eaa0b634

이러한 항목은 다음 명령줄 매개 변수에 해당합니다.

```
-xo CA.SM::UserDirectory@0e-255e2456-556d-40fb-93cd-f2fed81f656e
-xo-add CA.SM::AuthScheme@0d-4afc0e41-ae25-11d1-9cdd-006008aac24b
-xo-replace CA.SM::Agent@01-cb8b3401-a6aa-4794-964e-c569712269c0
-xo-overlay CA.SM::Domain@03-7bdf31f2-44d7-4d7b-a8f5-5de2eaa0b634
```

-xb

(선택 사항) 정책 저장소 위치를 포함하여 정책 저장소의 모든 개체를 내보냅니다. 정책 저장소 위치는 정책 서버 관리 콘솔의 "데이터" 탭에 설정되어 있습니다.

중요! 이 데이터를 가져오는 정책 서버는 내보내기 중에 지정된 정책 저장소를 사용합니다. 예를 들어 ODBC 데이터베이스를 정책 저장소로 사용하는 정책 서버 A 에서 데이터를 내보냅니다. 그런 다음, Active Directory 를 정책 저장소로 사용하는 정책 서버 B 에 이 데이터를 가져옵니다. 정책 서버 B 에 대한 Active Directory 정책 저장소의 위치는 정책 서버 A 에 대한 ODBC 데이터베이스로 대체됩니다.

-xe

(선택 사항) 실행 환경과 관련된 개체 유형을 내보냅니다.

-xp

(선택 사항) 정책과 관련된 개체 유형을 내보냅니다.

-xe 및 -xp 옵션은 -xo, -xo-add, -xo-replace, -xo-overlay 또는 -xf 와 함께 사용할 수 없습니다.

중요! -xe 및 -xp 옵션은 -xa 옵션을 대체하여 페더레이션 관련 개체를 제외한 모든 정책 데이터를 추출합니다. 또한 정책 서버 위치 관련 데이터(예: 정책 저장소 위치)를 포함하여, 전체 정책 저장소의 백업을 만들 수 있는 -xb 옵션을 사용할 수도 있습니다.

-xs

(선택 사항) 전체 보안 데이터를 내보냅니다.

-xc

(선택 사항) 전체 구성 데이터를 내보냅니다.

-xi

(선택 사항) 처음에 설치된 개체 유형을 내보냅니다.

예: AgentType

-xm

(선택 사항) ExtractManifest 개체에 지정된 개체를 내보냅니다.

-f

(선택 사항) 출력 파일을 덮어씁니다.

-fm

(선택 사항) 메모리를 적게 사용하지만 성능에 영향을 줍니다.

-q

(선택 사항) 진행률 메시지를 표시하지 않습니다.

-m <number>[%]

(선택 사항) <number>개의 개체를 내보낼 때마다 진행률 메시지가 출력됨을 나타냅니다.

선택적 백분율 기호("%")가 포함된 경우 <number>는 개체 수가 아니라 총 개체 수에 대한 백분율입니다.

기본값: 10%

-pass <passphrase>

(선택 사항) 중요한 데이터를 암호화하는 데 필요한 암호를 지정합니다. 이 암호는 8 자 이상이고 숫자, 대문자, 소문자를 각각 하나 이상 포함해야 합니다. 따옴표로 묶을 경우 암호에 공백을 포함할 수 있습니다. 명령줄 옵션으로 지정되지 않으면 중요한 데이터를 내보낼 때 암호를 묻는 프롬프트가 표시됩니다.

-npass

(선택 사항) 암호를 사용하지 않도록 지정합니다.

중요! 중요한 데이터가 ClearText 로 내보내집니다.

-comment

(선택 사항) 출력 파일에 주석을 추가합니다.

-cf commentpath

(선택 사항) <commentpath>에서 주석을 가져와 출력 파일에 추가합니다.

-?

명령줄 도움말을 표시합니다.

-nb

(선택 사항) 오류 발생 시 경고음을 울리지 않습니다.

-vT

(선택 사항) 세부 정보 표시 수준을 "추적"으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "정보"로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "경고"(기본값)로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "오류"로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "치명적 오류"로 설정합니다.

-l log_file

(선택 사항) 지정된 파일에 로그를 출력합니다.

-e err_file

(선택 사항) 오류 및 예외가 로깅되는 파일을 지정합니다. 생략할 경우 stderr 가 사용됩니다.

예

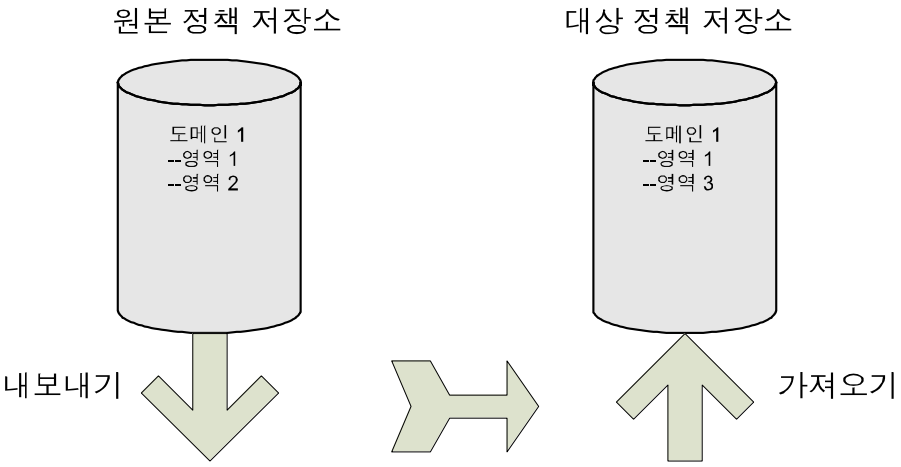
```
XPSExport PolicyData.xml -xo
CA.SM::UserDirectory@0e-255e2456-556d-40fb-93cd-f2fed81f656e
-xo-overlay CA.SM::Domain@03-7bdf31f2-44d7-4d7b-a8f5-5de2eaa0b634
```

참고: 세부적인 내보내기의 경우 내보내기 유형이 명령줄에 명시적으로 지정되거나 데이터 사전에서 검색됩니다. 덤프 내보내기의 경우에는 모든 개체의 내보내기 유형 특성이 Replace 입니다. 정책 데이터의 로드 가져오기는 정책 저장소의 모든 정책 데이터를 덮어씁니다.

XPSExport 도구를 사용하는 동안 명령줄 옵션에서 오류가 발생하면 도구가 중단되고 예외 파일 또는 stderr 에 오류가 로깅됩니다. 또한 개체를 *하나라도* 내보내는 데 실패할 경우 내보내기 프로세스가 중단됩니다. 이 경우 해당 오류가 예외 파일 또는 stderr 에 로깅되고 XML 출력 파일이 생성되었으면 삭제됩니다.

정책 데이터 추가

다음 다이어그램에서는 내보낸 후 대상 정책 저장소로 내보내고 가져와야 하는 원본 정책 저장소의 도메인 1 이라는 SiteMinder 정책 도메인을 보여 줍니다.



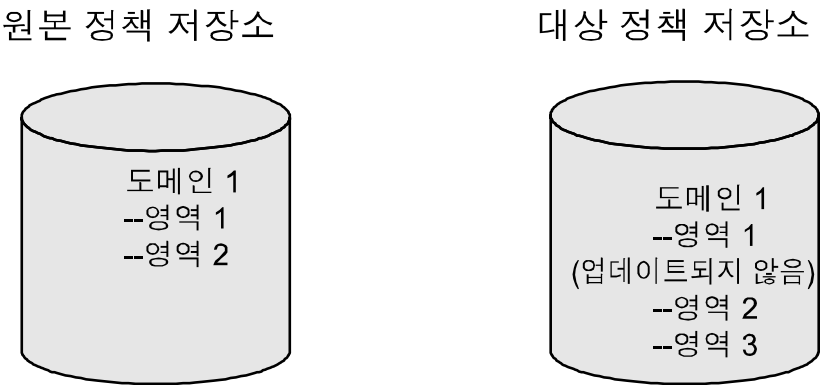
대상 정책 저장소에는 이미 동일한 이름의 도메인이 있지만 두 도메인에는 다음과 같은 차이점이 있습니다.

- 영역 1 의 속성이 원본 정책 저장소에서는 업데이트되었으므로 대상 정책 저장소의 해당 속성은 다른 값을 가집니다.
- 도메인 1 의 영역 2 는 대상 정책 저장소에 없습니다.

개체 하나(영역 2)만 대상 정책 저장소로 세부적으로 가져오도록 지정하려는 경우 내보내기 명령줄은 다음과 같습니다.

```
XPSExport gran-add.xml -xo-add
CA.SM: :Domain@03-0fb7bd02-6986-4bb9-b240-c232358958b1
```

가져오기에 성공한 후 대상 정책 저장소의 도메인 1 에는 세 개의 영역이 포함됩니다. 다음 그림과 같이 영역 1 의 속성은 업데이트되지 않습니다.



add 메서드를 사용하여 명시적으로 지정된 개체(도메인)를 대상 정책 저장소로 세부적으로 가져오도록 지정하려면 다음 명령을 사용하십시오.

```
XPSExport -ma -xo <object_XID>
```

-ma

명령줄에서 이 매개 변수 뒤에 있는 개체를 모두 추가합니다.

add 메서드를 사용하여 명시적으로 지정된 개체(도메인)의 모든 관련 개체를 대상 정책 저장소로 세부적으로 가져오도록 지정하려면 다음 명령을 사용하십시오.

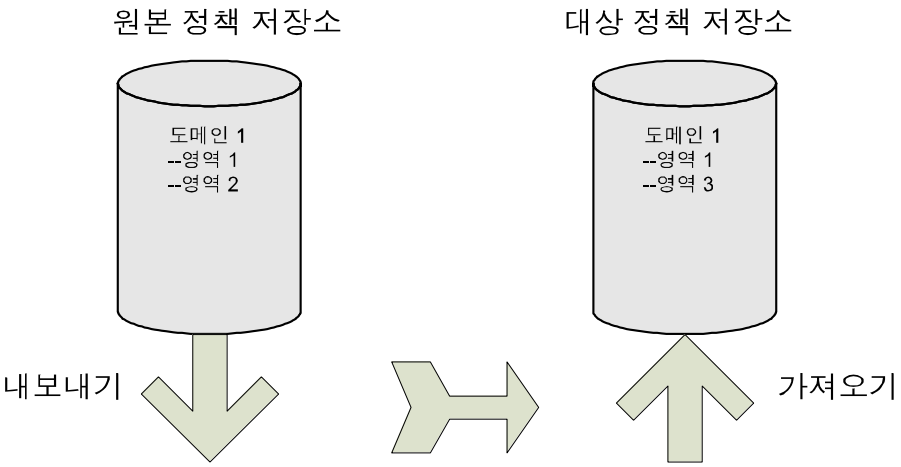
```
XPSExport -ra -xo <object_XID>
```

-ra

명령줄에서 이 매개 변수 뒤에 있는 개체의 관련 시스템 개체를 추가합니다.

정책 데이터 오버레이

다음 다이어그램에서는 내보낸 후 대상 정책 저장소로 내보내고 가져와야 하는 원본 정책 저장소의 도메인 1 이라는 SiteMinder 정책 도메인을 보여 줍니다.



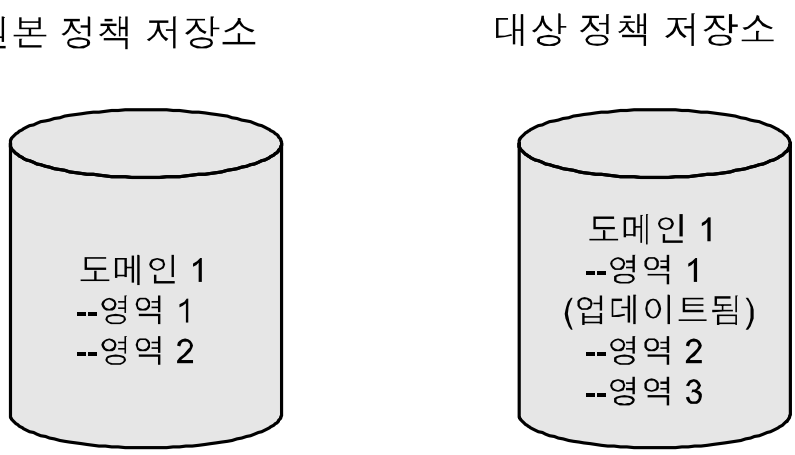
대상 정책 저장소에는 이미 동일한 이름의 도메인이 있지만 두 도메인에는 다음과 같은 차이점이 있습니다.

- 영역 1 의 속성이 원본 정책 저장소에서는 업데이트되었으므로 대상 정책 저장소의 해당 속성은 다른 값을 가집니다.
- 도메인 1 의 영역 2 는 대상 정책 저장소에 없습니다.

대상 정책 저장소를 원본 정책 저장소의 최신 변경 내용으로 업데이트하도록 세부적인 가져오기를 지정하려는 경우 내보내기 명령줄은 다음과 같습니다.

```
XPSExport gran-add.xml -xo-overlay
CA.SM: :Domain@03-0fb7bd02-6986-4bb9-b240-c232358958b1
```

가져오기에 성공한 후 대상 정책 저장소의 영역 1 에 대한 속성은 다음 그림과 같이 업데이트됩니다.



overlay 메서드를 사용하여 명시적으로 지정된 개체(도메인)를 대상 정책 저장소로 세부적으로 가져오도록 지정하려면 다음 명령을 사용하십시오.

```
XPSExport -mo -xo <object_XID>
```

-mo

명령줄에서 이 매개 변수 뒤에 있는 개체를 모두 오버레이합니다.

overlay 메서드를 사용하여 명시적으로 지정된 개체(도메인)의 모든 관련 개체를 대상 정책 저장소로 세부적으로 가져오도록 지정하려면 다음 명령을 사용하십시오.

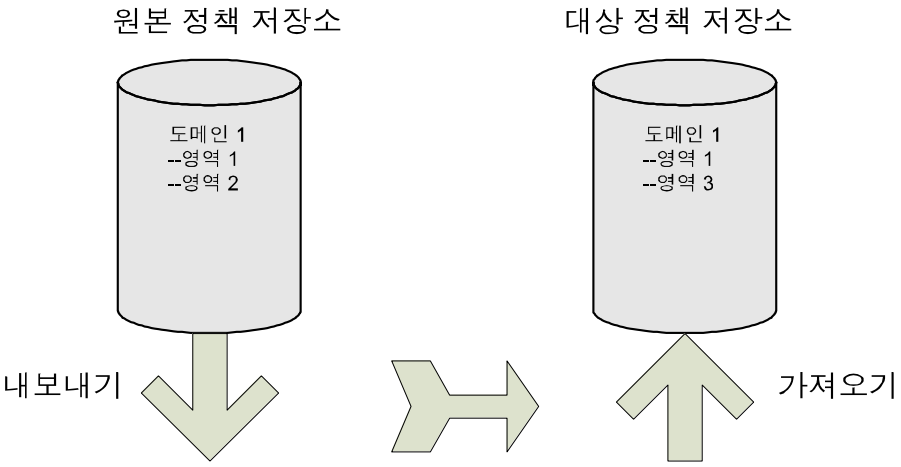
```
XPSExport -ro -xo <object_XID>
```

-ro

명령줄에서 이 매개 변수 뒤에 있는 개체의 관련 시스템 개체를 오버레이합니다.

정책 데이터 교체

다음 다이어그램에서는 내보낸 후 대상 정책 저장소로 내보내고 가져와야 하는 원본 정책 저장소의 도메인 1 이라는 SiteMinder 정책 도메인을 보여 줍니다.



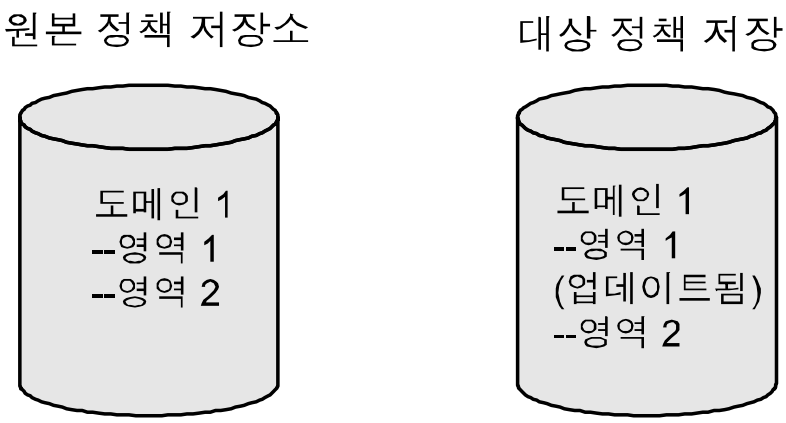
대상 정책 저장소에는 이미 동일한 이름의 도메인이 있지만 두 도메인에는 다음과 같은 차이점이 있습니다.

- 영역 1 의 속성이 원본 정책 저장소에서는 업데이트되었으므로 대상 정책 저장소의 해당 속성은 다른 값을 가집니다.
- 도메인 1 의 영역 2 는 대상 정책 저장소에 없습니다.

원본 정책 저장소의 내용을 대상 정책 저장소에 복제하려는 경우 내보내기 명령줄은 다음과 같습니다.

```
XPSExport gran-add.xml -xo-replace
CA.SM: :Domain@03-0fb7bd02-6986-4bb9-b240-c232358958b1
```

가져오기에 성공한 후 대상 정책 저장소의 도메인 1 은 다음 그림과 같이 원본 정책 저장소의 도메인 1 과 정확히 동일하게 됩니다.



replace 메서드를 사용하여 명시적으로 지정된 개체(도메인)를 대상 정책 저장소로 세부적으로 가져오도록 지정하려면 다음 명령을 사용하십시오.

```
XPSExport -mr -xo <object_XID>
```

-mr

명령줄에서 이 매개 변수 뒤에 있는 개체를 모두 교체합니다.

replace 메서드를 사용하여 명시적으로 지정된 개체(도메인)의 모든 관련 개체를 대상 정책 저장소로 세부적으로 가져오도록 지정하려면 다음 명령을 사용하십시오.

```
XPSExport -rr -xo <object_XID>
```

-rr

명령줄에서 이 매개 변수 뒤에 있는 개체의 관련 시스템 개체를 교체합니다.

정책 데이터 병합

한 정책 저장소의 도메인 개체를 다른 정책 저장소로 마이그레이션할 경우 명시적으로 지정된 개체(도메인)만 마이그레이션됩니다. 도메인의 모든 관련 개체(예: 사용자 디렉터리, 에이전트, 에이전트 유형)는 대상 정책 저장소로 마이그레이션되지 않습니다. 관련 시스템 개체 없이는 도메인을 정책 저장소로 가져올 수 없습니다.

merge 메서드를 사용하여 명시적으로 지정된 개체(도메인)를 대상 정책 저장소로 세부적으로 가져오도록 지정하려면 다음 명령을 사용하십시오.

```
XPSExport -mm -xo <object_XID>>
```

-mm

명령줄에서 이 매개 변수 뒤에 있는 개체를 모두 병합합니다.

merge 메서드를 사용하여 명시적으로 지정된 개체(도메인)의 모든 관련 개체를 대상 정책 저장소로 세부적으로 가져오도록 지정하려면 다음 명령을 사용하십시오.

```
XPSExport -rm -xo <object_XID>
```

-rm

명령줄에서 이 매개 변수 뒤에 있는 개체의 관련 시스템 개체를 병합합니다.

참고: Merge 옵션은 Add, Replace 또는 Overlay 옵션 대신 사용할 수 있습니다. Merge 옵션은 누락된 개체뿐만 아니라 기존 개체의 누락된 특성도 추가한다는 차이점을 제외하고는 Add 옵션과 유사합니다.

XPSImport

XPSImport 도구는 정책 저장소 데이터를 마이그레이션하기 위한 다음 태스크를 지원합니다.

- 전체 정책 데이터 가져오기
- 일부 정책 데이터 가져오기
- 구성 데이터 가져오기

참고: XPSImport 는 키를 키 저장소로 가져오지 않습니다. 키를 가져오려면 smkeyimport 를 사용해야 합니다.

구문

XPSImport 의 구문은 다음과 같습니다.

```
XPSImport input_file [-pass <passphrase>] [-npass] [-validate] [-fo] [-vT] [-vI] [-vW] [-vE] [-vF]
[-e file_name] [-l log_path] [-?]
```

매개 변수

input_file

입력 XML 파일을 지정합니다.

-q

(선택 사항) 진행률 메시지를 표시하지 않습니다.

-m <number>[%]

(선택 사항) <number>개의 개체를 내보낼 때마다 진행률 메시지가 출력됨을 나타냅니다.

선택적 백분율 기호("%")가 포함된 경우 <number>는 개체 수가 아니라 총 개체 수에 대한 백분율입니다.

기본값: 10%

-pass <passphrase>

(선택 사항) 중요한 데이터를 암호 해독하는 데 필요한 암호를 지정합니다. 이 암호는 내보내기 중에 지정한 암호와 동일해야 합니다. 그렇지 않으면 암호 해독에 실패합니다.

-npass

(선택 사항) 암호를 사용하지 않도록 지정합니다.

중요! 중요한 데이터는 일반 텍스트로 가져옵니다.

-validateOnly

(선택 사항) 데이터베이스를 업데이트하지 않고 입력 XML 파일의 유효성을 검사합니다.

-schemaFile

입력 파일의 유효성을 검사할 스키마 파일을 지정합니다. 이 옵션을 지정하지 않으면 입력 파일의 유효성이 검사되지 않습니다.

-fo

덤프 로드를 위해 기존 정책 저장소 날짜를 강제로 덮어쓸 수 있습니다.

-?

명령줄 도움말을 표시합니다.

-nb

(선택 사항) 오류 발생 시 경고음을 울리지 않습니다.

-vT

(선택 사항) 세부 정보 표시 수준을 "추적"으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "정보"로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "경고"(기본값)로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "오류"로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "치명적 오류"로 설정합니다.

-l log_file

(선택 사항) 지정된 파일에 로그를 출력합니다.

-e err_file

(선택 사항) 오류 및 예외가 로깅되는 파일을 지정합니다. 생략할 경우 stderr 가 사용됩니다.

예

```
XPSImport PolicyData.xml -e C:\\tmp\\ExceptionLog.txt
```

이 예에서는 PolicyData.xml 파일에 지정된 대로 정책 데이터 개체를 가져옵니다. 가져오기가 덤프 로드 또는 세부적인 가져오기일 경우 결과가 명령줄에서 즉시 확인되지 않습니다. 그러나 입력 XML 파일에 있는 <PolicyData> 요소의 IsDumpExport 특성을 확인하여 해당 정보를 검색할 수 있습니다. 이 특성이 true 로 설정되어 있으면 덤프 로드에 입력 XML 파일을 사용해야 함을 나타냅니다.

정책 데이터 전송 문제 해결

정책 저장소 데이터를 전송할 때 다음 사항과 관련된 문제가 발생할 수 있습니다.

- 오류가 콘솔(stdout/stderr)에 로깅되거나 파일에 직접 출력됩니다.
- 다음과 같은 로깅 수준이 사용됩니다.
  - Trace
  - Information
  - Warning
  - Error
  - Fatal
- 파일이 이미 있는 경우 내보내기가 실패합니다.
- XML 파일의 개체에 대한 유효성 검사가 실패할 경우 가져오기가 롤백됩니다.
- "추가" 유형으로 내보낸 개체가 대상 정책 저장소에 이미 있는 경우 세부적 가져오기가 실패합니다.

smkeyexport

smexportkey 도구는 키 저장소에서 키를 내보냅니다. smkeyexport 의 구문은 다음과 같습니다.

`smkeyexport -d`*`adminname`* `-w`*`adminpw`* `[-o`*`output_filename`*`] [-f] [-c] [-cb] [-cf] [-l] [-v] [-t] [-?]`

-d

SiteMinder 관리자의 이름을 지정합니다.

-w

SiteMinder 관리자의 암호를 지정합니다.

-o

(선택 사항) 출력 파일을 지정합니다. 기본적으로 stdout.smdif 로 설정됩니다.

-f

(선택 사항) 기존 출력 파일을 덮어씁니다.

-c

(선택 사항) 중요한 데이터를 암호화하지 않고 내보냅니다.

-cb

(선택 사항) 중요한 데이터를 이전 버전과 호환되는 암호화 기능으로 암호화하여 내보냅니다.

-cf

(선택 사항) 중요한 데이터를 FIPS 호환 암호화 기능으로 암호화하여 내보냅니다.

-l

(선택 사항) 항목을 생성하고 지정된 파일(filename.log)에 로깅합니다.

-v

(선택 사항) 메시지에 세부 정보를 표시하도록 지정합니다.

-t

(선택 사항) 추적이 사용되도록 설정합니다.

-?

(선택 사항) 명령 옵션을 표시합니다.

SiteMinder 키 도구

SiteMinder 키 도구 유틸리티(smkeytool)는 다음과 같은 기능을 지원합니다.

- 12.52 SP1 인증서 데이터 저장소를 관리할 수 있게 합니다.
- 12.52 SP1 로 업그레이드하는 동안 레거시 smkeydatabase 에 대한 액세스를 지원합니다. 레거시 키 저장소 액세스 플래그(-accessLegacyKS)를 사용하여 인증서 데이터 저장소로의 마이그레이션 실패를 초래할 수 있는 모든 데이터 충돌을 해결할 수 있습니다.
- 다음 위치에 설치됩니다.

  siteminder_home\bin

  siteminder_home

  정책 서버 설치 경로를 지정합니다.

다음 단계를 수행하십시오.

1. 명령줄 또는 셸을 엽니다.
2. 다음 명령 중 하나를 실행합니다.
   - (Windows) smkeytool.bat *-option* [*-arguments*]
   - (UNIX) smkeytool.sh *-option* [*-arguments*]

smkeytool 을 사용하여 다음을 수행하십시오.

- 클라이언트 인증서 키 추가

  smkeydatabase 에 나열되지 않은 소비 기관에서 체인 인증 기관 또는 루트를 사용하는 경우에는 이를 smkeydatabase 에 추가하십시오.

  예를 들어 서명된 VeriSign CA 서버 측 인증서는 웹 에이전트 옵션 팩을 통해 설치된 생산자측 웹 서버에서 SSL 을 사용하도록 지정하는 데 사용됩니다. 이 인증서를 SSL 을 통한 기본 인증에 사용하려면 소비자에서 smkeydatabase 에 VeriSign 인증서를 추가하십시오. 인증서를 추가하면 소비자가 서버 측 인증서가 있는 생산자와 통신할 수 있습니다. 또한 인증서가 있으면 트러스트된 CA 가 인증서를 확인했음을 확인하는 데도 도움이 됩니다.

개인 키 및 인증서 쌍 추가

개인 키/인증서 쌍만 인증서 데이터 저장소로 가져오려면 addPrivKey 옵션을 사용하십시오. 다음 사항을 고려하십시오.

- 저장소에 여러 개의 개인 키/인증서 쌍이 있을 수 있지만 SiteMinder 는 저장소의 RSA 키만 지원합니다.
- 개인 키/인증서 쌍만 암호화된 형식으로 저장됩니다.
- 생산 기관의 정책 서버는 다음을 수행합니다.
  - 단일 개인 키/인증서 쌍을 사용하여 SAML 어설션에 서명합니다.
  - 인증서를 사용하여 소비 기관에서 받은 암호화된 SAML 어설션을 암호 해독합니다.

  일반적으로 키는 인증서 데이터 저장소에서 발견된 첫 번째 개인 키/인증서 쌍입니다.

- 인증서 파일을 가져오기 전에 인증서 파일에서 인증서 메타데이터를 삭제하십시오. --BEGIN CERTIFICATE-- 표시로 시작하고 --END CERTIFICATE-- 표시로 끝나는 데이터만 가져오십시오. 표시를 포함하십시오.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-alias *alias*

필수입니다. 데이터베이스의 개인 키/인증서 쌍에 별칭을 할당합니다. 별칭은 고유한 문자열이어야 하며 영숫자 문자만 포함할 수 있습니다.

-certfile *cert_file*

개인 키/인증서 쌍과 연결된 인증서 위치의 전체 경로를 지정합니다. PKCS1, PKCS5 및 PKCS8 형식의 키에 필요합니다.

-keyfile *private_key_file*

개인 키 파일 위치의 전체 경로를 지정합니다. PKCS1, PKCS5 및 PKCS8 형식의 키에 필요합니다.

-keycertfile *key_cert_file*

개인 키/인증서 쌍 데이터가 포함된 PKCS12 파일 위치의 전체 경로를 지정합니다. PKCS12 형식의 키에 필요합니다.

-password *password*

(선택 사항) 쌍이 생성될 때 개인 키/인증서 쌍을 암호화하는 데 사용된 암호를 지정합니다. 인증서 데이터 저장소에 쓰기 전에 개인 키/인증서 쌍을 암호 해독하려면 이 암호를 제공하십시오.

참고: 이 암호는 인증서 데이터 저장소에 저장되지 않습니다.

키/인증서 쌍이 암호 해독되어 인증서 데이터 저장소에 저장된 후에는 SiteMinder 에서 자체 암호를 사용하여 쌍을 다시 암호화합니다.

인증서 추가

공개 인증서 또는 트러스트된 CA 인증서를 인증서 데이터 저장소에 추가하려면 addCert 옵션을 사용하십시오.

다음 사항을 고려하십시오.

- 인증서는 개인 키/인증서 쌍과 연결된 인증서일 수 있습니다. 하지만 인증서만 인증서 데이터 저장소에 추가됩니다.
- 인증서를 인증 기관으로 신뢰하는 경우 이 인증서는 항상 CA 인증서로 취급됩니다.
- X.509 인증서 형식의 경우 SiteMinder 는 V1, V2 및 V3 버전을 지원합니다. 인코딩 형식의 경우 SiteMinder 는 DER 및 PEM 형식을 지원합니다.
- 인증 기관 인증서를 추가할 때 웹 에이전트를 다시 시작하십시오.
- 인증서 파일을 가져오기 전에 인증서 파일에서 인증서 메타데이터를 삭제하십시오. --BEGIN CERTIFICATE-- 표시로 시작하고 --END CERTIFICATE-- 표시로 끝나는 데이터만 가져오십시오. 표시를 포함하십시오.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-alias *alias*

필수입니다. 인증서 데이터 저장소의 개인 키와 연결된 인증서에 별칭을 지정합니다.

제한: 영숫자 문자만 포함하는 고유한 문자열이어야 합니다.

-infile *cert_file*

필수입니다. 새로 추가된 인증서 위치의 전체 경로를 지정합니다.

-trustcacert

선택 사항입니다. 인증서를 추가할 사용자 공급자 인증서가 CA 인증서인지 확인합니다. 유틸리티가 인증서에 디지털 서명 확장이 있고 인증서에 동일한 IssuerDN 및 SubjectDN 값이 있는지를 확인합니다.

-noprompt

(선택 사항) 사용자에게 인증서 추가를 확인하라는 메시지가 표시되지 않습니다.

해지 정보 추가

CRL 의 위치를 지정하려면 addRevocationInfo 옵션을 사용하십시오. 인증서 데이터 저장소는 CRL 의 위치를 참조합니다.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-issueralias *issuer_alias*

필수입니다. CRL 을 발급하는 인증 기관의 별칭을 지정합니다.

예: -issueralias verisignCA

-type (*ldapcrl* | *filecrl*)

필수입니다. CRL 이 LDAP 기반인지 아니면 파일 기반인지를 지정합니다.

-location *location*

필수입니다. CRL 의 위치를 지정합니다.

- (파일 기반) 파일의 전체 경로입니다.

  예: -location c:\crls\siteminder_root_ca.crl

- (LDAP 디렉터리 서비스) LDAP 서버 노드의 전체 경로입니다.

  예: -location "http://localhost:880/sn=siteminderroot, dc=crls,dc=com"

해지 정보 삭제

인증서 데이터 저장소에서 CRL 을 삭제하려면 deleteRevocationInfo 옵션을 사용하십시오.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-issueralias *issuer_alias*

(필수) CRL 을 발급하는 인증 기관의 이름을 지정합니다.

-noprompt

(선택 사항) 사용자에게 CRL 이 삭제될 수 있음을 확인하라는 메시지가 표시되지 않습니다.

인증서 데이터 제거

인증서 데이터 저장소에서 모든 인증서 데이터를 제거하려면 removeAllCertificateData 옵션을 사용하십시오.

이 옵션의 인수는 다음과 같습니다.

-noprompt

(선택 사항) 사용자에게 인증서 데이터가 제거될 수 있음을 확인하라는 메시지가 표시되지 않습니다.

인증서 삭제

인증서를 인증서 데이터 저장소에서 제거하려면 delete 옵션을 사용하십시오. 인증서에 개인 키가 연결되어 있는 경우에는 개인 키도 삭제됩니다.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-alias *<alias>*

(필수) 옵션으로 제거할 인증서의 별칭을 지정합니다.

-noprompt

(선택 사항) 사용자에게 인증서가 제거될 수 있음을 확인하라는 메시지가 표시되지 않습니다.

인증서 또는 개인 키 내보내기

인증서 또는 개인 키를 파일로 내보내려면 export 옵션을 사용하십시오.

다음 사항을 고려하십시오.

- 인증서 데이터는 PEM 인코딩을 사용하여 내보냅니다.
- 개인 키 데이터는 DER 인코딩 PKCS8 형식을 사용하여 내보냅니다.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-alias *alias*

(필수) 내보낼 인증서 또는 키를 식별합니다.

-outfile *out_file*

(필수) 데이터를 내보낼 파일의 전체 경로를 지정합니다.

-type (key|cert)

(선택 사항) 인증서 또는 키 중에서 어느 것을 내보낼지 지정합니다.

기본값: certificate.

-password *password*

개인 키를 내보낼 때만 필요합니다. 내보낼 때 개인 키를 암호화하는 데 사용할 암호를 지정합니다. 공개 키가 있는 인증서를 내보낼 때는 인증서를 일반 텍스트로 내보내므로 암호가 필요하지 않습니다.

이 개인 키를 다시 인증서 데이터 저장소에 추가하려면 이 암호와 함께 addPrivKey 옵션을 함께 사용하십시오.

별칭 찾기

인증서 데이터 저장소의 인증서와 연결된 별칭을 찾으려면 findAlias 옵션을 사용하십시오.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-infile *cert_file*

(필수) 원하는 별칭과 연결된 인증서 파일의 전체 경로를 지정합니다.

-password *password*

password–protected P12 파일이 인증서 파일로 지정된 경우에만 필요합니다.

기본 CA 인증서 가져오기

SiteMinder 에 포함된 모든 기본 트러스트된 인증 기관 인증서를 인증서 데이터 저장소로 가져오려면 importDefaultCACerts 옵션을 사용하십시오.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 12.52 SP1 인증서 데이터 저장소에 적용됩니다.

모든 인증서의 메타데이터 나열

인증서 데이터 저장소에 저장된 모든 인증서의 일부 메타데이터를 나열하려면 listCerts 옵션을 사용하십시오.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-alias *alias*

(선택 사항) 지정된 별칭과 연결된 인증서 및 키의 메타데이터 상세 정보를 나열합니다.

이 옵션은 별표(*)를 와일드카드 문자로 지원합니다. 와일드카드는 다음 위치에 사용할 수 있습니다.

- 별칭 값의 시작 또는 끝
- 별칭 값의 시작 및 끝

명령 셸이 와일드카드 문자를 해석하지 않도록 하려면 와일드카드를 따옴표로 묶으십시오.

해지 정보 나열

인증서 데이터 저장소에 있는 인증서 해지 목록의 목록을 표시하려면 listRevocationInfo 옵션을 사용하십시오. 다음 항목이 나열됩니다.

- CRL 이름
- CRL 이 파일 기반인지 LDAP 기반인지 여부
- CRL 위치

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-issueralias *issuer_alias*

(선택 사항) CRL 을 발급하는 인증 기관의 이름입니다.

이 옵션은 별표(*)를 와일드카드 문자로 지원합니다. 와일드카드는 다음 위치에 사용할 수 있습니다.

- 별칭 값의 시작 또는 끝
- 별칭 값의 시작 및 끝

명령 셸이 와일드카드 문자를 해석하지 않도록 하려면 와일드카드를 따옴표로 묶으십시오.

인증서 메타데이터 표시

지정된 인증서에 대한 일부 메타데이터를 표시하려면 printCert 옵션을 사용하십시오. 이 명령은 인증서 속성을 보기 어려운 시스템에서 유용합니다.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-infile *cert_file*

필수입니다. 인증서 파일의 위치입니다.

-password *password*

암호는 암호로 보호된 P12 파일이 인증서 파일로 지정된 경우에만 필요합니다.

별칭 이름 변경

인증서와 연결된 별칭의 이름을 바꾸려면 renameAlias 옵션을 사용하십시오.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-alias *current_alias*

(필수) 인증서와 연결된 별칭을 지정합니다.

-newalias *new_alias*

(필수) 새 별칭 이름을 지정합니다.

제한: 영숫자 문자만 포함하는 고유한 문자열이어야 합니다.

인증서 유효성 검사

인증서가 해지되었는지 확인하려면 validateCert 옵션을 사용하십시오.

이 옵션의 인수는 다음과 같습니다.

-accessLegacyKS

옵션이 레거시 smkeydatabase 에 적용되도록 지정합니다. 이 인수를 제공하지 않으면 옵션이 12.52 SP1 인증서 데이터 저장소에 적용됩니다.

-alias *alias*

(필수) 인증서 데이터 저장소의 개인 키와 연결된 인증서에 별칭을 지정합니다.

제한: 영숫자 문자만 포함하는 고유한 문자열이어야 합니다.

-infile *crl_file*

(선택 사항) 유틸리티에서 유효성을 확인하기 위해 인증서를 찾을 CRL 을 지정합니다.

OCSP 구성 파일 로드

정책 서버를 다시 시작할 필요 없이 OCSP 구성 파일을 인증서 데이터 저장소로 다시 로드하려면 loadOCSPConfigFile 옵션을 사용하십시오. 파일이 로드되면 모든 기존 OCSP 구성이 데이터 저장소에서 제거되고 구성이 파일 내용으로 바뀝니다. OCSPUpdater 는 다음에 실행될 때 구성 변경 내용을 가져옵니다.

OCSP 구성 파일의 이름은 SMocsp.conf 입니다.

Windows 의 명령 구문은 다음과 같습니다.

```
smkeytool.bat -loadOCSPConfigFile
```

UNIX 의 명령 구문은 다음과 같습니다.

```
smkeytool.sh -loadOCSPConfigFile
```

smldapsetup

smldapsetup 유틸리티를 사용하여 명령줄에서 LDAP 정책 저장소를 관리할 수 있습니다. smldapsetup 을 사용하면 LDAP 정책 저장소를 구성하고, LDIF 파일을 생성하고, 정책 저장소 데이터 및 스키마를 제거할 수 있습니다.

smldapsetup 을 사용하려면 smldapsetup 이 수행할 작업을 결정하는 모드와 LDAP 서버를 구성하는 데 사용되는 값을 포함하는 인수를 지정하십시오.

다음 표에는 smldapsetup 과 함께 사용할 수 있는 모드와 각 모드에서 사용하는 인수가 나와 있습니다.

모드	인수
reg	-h*host*, -p*portnumber*, -d*userdn*, -w*userpw*, -r*root*, -ssl*1|0*, -c*certdb*, -k1
ldgen	-h*host*, -p*portnumber*, -d*userdn*, -w*userpw*, -r*root*, -m*n*, -ssl*1|0*, -c*certdb* -f*ldif*, -t*tool*, -s*suffix*, -e, -k
ldmod	-h*host*, -p*portnumber*, -d*userdn*, -w*userpw*, -r*root*, -ssl*1|0*, -c*certdb*, -f*ldif*, -s*suffix*, -e, -k, -i
remove	-h*host*, -p*portnumber*, -d*userdn*, -w*userpw*, -r*root*, -ssl*1|0*, -c*certdb*, -k
switch	없음
revert	-v
status	-v

smldapsetup 을 사용하려면

1. 다음 위치 중 하나로 이동합니다.
   - (Windows) *siteminder_home*\bin
   - (UNIX) *siteminder_home*/bin

   siteminder_home

   SiteMinder 가 설치된 위치를 지정합니다.
2. 다음 명령을 입력합니다.

   `smldapsetup mode arguments`

   중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

   예: smldapsetup reg -hldapserver.mycompany.com -d"LDAP User" -wMyPassword123 -ro=security.com

   참고: smldapsetup 을 실행하려면 지정한 LDAP 사용자에게 LDAP 디렉터리 서버의 스키마를 수정할 수 있는 적절한 관리자 권한이 있어야 합니다. 이 사용자에게 적절한 권한이 없으면 LDAP 서버에서 정책 저장소 스키마를 생성할 수 없으며 정책 저장소 데이터를 업데이트 또는 제거할 수 없습니다. smldapsetup 명령을 실행하면 정책 서버 관리 콘솔의 "데이터" 탭에 있는 "관리자 사용자 이름" 필드에 이 사용자가 표시됩니다.

추가 정보:

smldapsetup 모드 (페이지 258)

smldapsetup 모드

smldapsetup 모드는 smldapsetup 이 수행하는 작업을 나타냅니다. LDAP 서버에 연결할 모드를 지정하고, LDIF 파일을 생성하고, LDAP 정책 저장소를 구성하고, 정책 데이터를 제거할 수 있습니다.

smldapsetup 모드에는 다음이 포함됩니다.

reg

LDAP 서버에 대한 연결을 테스트합니다. 연결에 성공하면 smldapsetup 은 -h*host*, -p*portnumber*, -*duserdn*, -w*userpw*, -r*root*, -ssl*1/0* 및 -c*certdb* 인수를 사용하여 SiteMinder LDAP 서버를 정책 저장소로 구성합니다.

ldgen

지원되는 LDAP 서버를 자동으로 검색하고, SiteMinder 스키마를 사용하여 LDIF 파일을 생성합니다. 생성된 파일은 smldapsetup ldmod 에서 SiteMinder 스키마를 생성하는 데 사용됩니다. -e 인수가 지정된 경우 smldapsetup ldgen 은 ldmod 에서 SiteMinder 스키마를 삭제하는 데 사용할 수 있는 LDIF 파일을 생성합니다. LDAP 서버 자동 검색을 건너뛰려면 -m 스위치를 사용하십시오. 이전에 reg 모드에서 구성하지 않은 경우 ldgen 모드에서 -f 스위치를 사용해야 합니다.

ldmod

정책 저장소에 데이터를 채우지 않고 LDAP 서버와 SiteMinder 스키마에 연결합니다. 이 작업에는 -*fldif* 인수로 지정된 LDAP 수정 프로그램 및 LDAP 파일이 필요합니다. -h*host*, -p*port_number*, -d*userdn*, -w*userpw*, -r*root*, -ssl*1/0* 및 -c*certdb* 인수를 지정할 경우 smldapsetup ldmod 는 이러한 인수로 지정된 LDAP 디렉터리를 수정합니다. -h*host*, -p*portnumber*, -d*userdn*, -*wuserpw*, -r*root*, -ssl*1/0* 및 -c*certdb* 를 지정하지 않을 경우 smldapsetup ldmod 는 이전에 smldapsetup reg 또는 정책 서버 관리 콘솔을 사용하여 정의된 LDAP 디렉터리를 사용합니다.

remove

LDAP 서버에 연결한 다음 현재 smldapsetup 버전에 해당하는 SiteMinder LDAP 노드 아래에 저장된 모든 정책 데이터를 제거합니다. -*hhost*, -p*port_number*, -d*userdn*, -w*userpw*, -r*root*, -ssl*1/0* 및 -c*certdb* 인수를 지정할 경우 smldapsetup remove 는 이러한 인수로 지정된 LDAP 디렉터리에서 정책 데이터를 제거합니다. -h*host*, -p*port*, -d*userdn*, -w*userpw*, -r*root*, -*ssl1/0* 및 -c*certdb* 를 지정하지 않을 경우 smldapsetup remove 는 이전에 smldapsetup reg 또는 정책 서버 관리 콘솔을 사용하여 정의된 LDAP 디렉터리에서 정책 데이터를 제거합니다.

switch

ODBC 대신 LDAP 를 사용하도록 정책 서버를 다시 구성합니다. 변경 작업을 수행하기 전에 LDAP 저장소 또는 LDAP 연결 매개 변수를 준비하지 않습니다.

revert

LDAP 에서 ODBC 정책 저장소로 되돌립니다. 이 모드에서는 -v 인수만 사용됩니다.

status

LDAP 정책 저장소 연결 매개 변수가 올바르게 구성되어 있는지 확인합니다. -v 인수가 필요합니다. 인수로 -h*host*, -p*port_number*, -d*userdn*, -w*userpw*, -r*root*, -ssl*1/0* 및 -c*certdb* 를 지정할 경우 smldapsetup status 는 이러한 인수를 사용하여 지정된 LDAP 디렉터리에 대한 연결을 테스트합니다. -h*host*, -p*port_number*, -*duserdn*, -w*userpw*, -r*root*, -ssl*1/0* 및 -c*certdb* 를 지정하지 않을 경우 smldapsetup status 는 이전에 smldapsetup reg 또는 정책 서버 관리 콘솔을 사용하여 정의된 LDAP 디렉터리에 대한 연결을 확인합니다.

정책 서버 관리 콘솔의 "데이터" 탭에서 GUI 인터페이스를 사용하여 reg, switch 및 revert 함수와 함께 구성한 설정을 보거나 변경할 수 있습니다. ldgen, ldmod, remove 및 status 함수를 수행하려면 smldapsetup 을 사용해야 합니다.

smldapsetup 인수

인수로 모드에서 사용되는 정보를 지정하여 LDAP 정책 저장소를 관리할 수 있습니다. 인수를 지정하지 않으면 정책 서버 관리 콘솔에 구성된 값이 사용됩니다.

참고: 인수와 값 사이에는 공백을 사용할 수 없습니다. 예를 들어 -h 인수는 다음과 같이 지정해야 합니다.
smldapsetup ldmod -hldapserver.mycompany.com

smldapsetup 호출에 지정할 수 있는 인수는 다음과 같습니다.

-h*host*

LDAP 서버의 정규화된 이름, 상대 이름(컴퓨터가 동일한 도메인, 즉 -hldapserver 에 있는 경우), 또는 IP 주소(-h123.12.12.12)를 지정합니다. 호스트를 지정하지 않으면 이전에 구성된 값이 기본값으로 사용됩니다.

예: -hldapserver.mycompany.com

-p*port_number*

비표준 LDAP 포트를 지정합니다. LDAP 서버가 비표준 포트를 사용하는 경우나 서버를 다른 포트를 사용하는 새 서버로 이동(예: SSL 을 사용하는 서버를 그렇지 않은 서버로 이동)할 경우에는 LDAP 포트를 지정해야 합니다. 포트를 지정하지 않으면 이전 구성 값이 사용됩니다. 이전 포트 구성이 지정되지 않은 경우에는 SSL 이 사용되고 있지 않으면 기본 포트 389 가 사용되고 SSL 이 사용되고 있으면 636 이 사용됩니다.

-d*userdn*

새 LDAP 디렉터리 스키마 및 항목을 생성할 수 있는 사용자의 LDAP 사용자 이름을 지정합니다. 반드시 LDAP 서버 관리자의 사용자 이름일 필요는 없습니다. 사용자 이름을 지정하지 않으면 이전에 구성된 이름이 기본값으로 사용됩니다.

-w*userpw*

-d 인수에서 식별된 사용자의 암호를 지정합니다. 암호를 지정하지 않으면 이전에 구성된 값이 사용됩니다.

예: -wMyPassword123

-r*root*

LDAP 트리에서 SiteMinder 가 정책 저장소 스키마를 검색할 노드의 고유 이름을 지정합니다. 루트를 지정하지 않으면 이전에 구성된 루트가 사용됩니다.

예: -ro=security.com

-e

smldapsetup ldgen 과 함께 지정된 경우 SiteMinder 스키마를 삭제할 수 있는 LDIF 파일을 생성합니다. 스키마를 제거하려면 생성된 파일을 smldapsetup ldmod 와 함께 사용해야 합니다.

-m*n*

LDAP 서버 자동 검색을 건너뛰고 LDAP 정책 저장소의 유형을 지정합니다. 여기서 *n* 은 다음 중 하나입니다.

2

iPlanet v4 LDAP 서버

3

Active Directory LDAP 서버

4

Oracle Internet Directory

5

iPlanet v5

6

Sun Directory Server

9

ADAM(Active 디렉터리 Application Mode)

-fldif

smldapsetup 이 실행 중인 디렉터리에서 LDIF 파일까지의 절대 또는 상대 경로를 지정합니다.

예: -f../siteminder/db/smldap.ldif

기본값: 경로를 지정하지 않으면 현재 디렉터리가 기본값으로 사용됩니다.

-ttool

파일 이름 및 확장명을 포함하여 ldapmodify 명령줄 유틸리티의 절대 또는 상대 경로를 지정합니다. ldapmodify 는 LDIF 형식 명령을 사용하여 서버 스키마를 구성하는 데 사용됩니다. LDAP 서버와 SiteMinder 는 ldapmodify 의 복사본을 제공합니다. 이 유틸리티가 기본 위치에 없는 경우 이 인수를 사용하여 해당 위치를 지정합니다.

-ssl1_or_0

LDAP 서버에 대해 SSL 로 암호화된 연결을 사용하려면 -ssl1 을 지정하고, 비 SSL 연결을 사용하려면 -ssl0 을 지정합니다. -ssl 값을 지정하지 않으면 이전에 구성된 값이 사용됩니다. 이전에 LDAP 연결을 구성한 적이 없는 경우 초기 기본값은 0 입니다.

-c*cert*

이 인수는 SSL 로 암호화된(-ssl1) LDAP 연결을 사용할 경우에 지정해야 합니다. 일반적으로 cert8.db 라는 SSL 클라이언트 Netscape 인증서 데이터베이스 파일이 있는 디렉터리의 경로를 지정합니다.

예: cert8.db 가 /app/siteminder/ssl 에 있는 경우 -c/app /siteminder/ssl 을 지정합니다. 즉, smldapsetup ldmod -f/app/siteminder/pstore.ldif -p81 -ssl1 -c/app/siteminder/ssl 을 실행합니다.

참고: Sun Java System LDAP 에 대해 SSL 로 암호화된 연결을 사용하는 정책 저장소의 경우 key3.db 파일은 cert8.db 와 동일한 디렉터리에 있어야 합니다.

-k-k1

키 정보를 다른 LDAP 디렉터리에 저장할 경우 smldapsetup 을 사용하여 키 저장소를 설정하거나 수정할 수 있습니다. -k 를 지정하면 smldapsetup 은 함수를 수행하기 전에 정책 서버가 키 저장소에 연결되어 있는지 여부를 확인합니다. 정책 서버가 키 저장소에 연결되어 있지 않은 경우에는 경고가 발생합니다. 새 정책 저장소를 사용할 경우 smldapsetup ldgen 및 다른 인수와 함께 -k1 을 지정하면 지정한 위치에 별도의 키 저장소가 생성됩니다. -k 또는 -k1 을 지정하지 않으면 정책 저장소가 수정됩니다.

-v

문제 해결을 위한 세부 정보 표시 모드가 사용되도록 설정합니다. -v 를 사용하면 smldapsetup 은 LDAP 마이그레이션의 각 단계를 수행할 때 명령줄 인수 및 구성 항목을 로깅합니다.

-i*userDN*

SiteMinder 가 정책 저장소를 수정하는 데 사용해야 하는 계정의 고유 이름을 지정합니다. 이 인수를 사용하면 관리자 계정이 계속해서 SiteMinder 스키마를 제어하면서 SiteMinder 데이터의 일상적인 수정에는 다른 계정을 사용할 수 있습니다. 관리 UI 를 사용하여 변경 작업을 수행할 경우 이 인수로 지정된 계정이 사용됩니다. 이 인수를 사용할 경우 계정의 전체 DN 을 입력해야 합니다.

-q

확인할 사항이 없는 경우 자동 모드가 사용되도록 설정합니다.

-u

6.x 업그레이드 스키마 파일(LDIF)을 생성합니다.

-x

다른 5.x Sun Java System Directory Server Enterprise Edition(이전의 Sun ONE/iPlanet) LDAP 디렉터리 서버에 대한 복제 인덱스를 생성하려면 ldmod 와 함께 -x 인수를 사용하십시오.

-ssuffix

이 옵션을 사용하면 Sun Java System Directory Server Enterprise Edition(이전의 Sun ONE/iPlanet) LDAP 디렉터리 서버에서 6.x 정책 서버의 스키마를 구성할 때 기본 부모 접미사 이외의 접미사를 지정할 수 있습니다.

예: 다음과 같이 가정합니다.

ou=Apps,o=test.com 은 정책 저장소 루트입니다.

o=test.com 은 루트 접미사입니다.

ou=netegrity,ou=Apps,o=test.com 은 하위 접미사입니다.

smldapsetup 과 함께 -s 매개 변수를 사용하지 않으면 정책 서버는 ou=netegrity,ou=Apps,o=test.com 의 부모 접미사로 ou=Apps,o=test.com 을 할당합니다. 이를 변경하고 적절한 부모 접미사를 설정하려면 o=test.com 을 지정하고 -s 매개 변수를 사용하여 smldapsetup 을 실행하십시오.

-?

도움말 메시지를 표시합니다.

참고: 인수에 공백이 있는 경우에는 전체 인수를 큰따옴표로 묶어야 합니다. 예를 들어 SiteMinder 관리자의 이름이 LDAP user 인 경우 smldapsetup 의 인수는 -d"LDAP user"가 됩니다.

smldapsetup 및 Sun Java System Directory Server Enterprise Edition

Sun Java System Directory Server Enterprise Edition(이전의 Sun ONE/iPlanet) 디렉터리 서버에서 smldapsetup 은 ou=Netegrity, *root* 하위 접미사 및 PolicySvr4 데이터베이스를 생성합니다.

root

정책 서버 관리 콘솔의 "데이터" 탭에서 "루트 DN" 필드에 지정한 디렉터리 루트입니다. 이 변수는 기존의 루트 접미사 또는 하위 접미사여야 합니다.

예: 루트 접미사가 dc=netegrity,dc=com 일 경우 smldapsetup 을 실행하면 디렉터리 서버에 다음 항목이 생성됩니다.

- 루트 접미사, dc=netegrity,dc=com 과 해당 userRoot 데이터베이스
- 하위 접미사, ou=Netegrity,dc=netegrity,dc=com 과 해당 PolicySvr4 데이터베이스

예: 정책 저장소를 ou=apps,dc=netegrity,dc=com 아래에 배치하려는 경우 ou=apps,dc=netegrity,dc=com 은 루트 접미사이거나 루트 접미사 c=netegrity,dc=com 의 하위 접미사여야 합니다.

하위 접미사일 경우 smldapsetup 을 실행하면 다음 항목이 생성됩니다.

- 루트 접미사, dc=netegrity,dc=com 과 해당 userRoot 데이터베이스
- 하위 접미사, ou=apps,dc=netegrity,dc=com 과 해당 Apps 데이터베이스
- 하위 접미사, ou=Netegrity,ou=apps,dc=netegrity,dc=com 과 해당 PolicySvr4 데이터베이스

참고: 루트 및 하위 접미사에 대한 자세한 내용은 Sun Microsystems 설명서를 참조하십시오.

smldapsetup 을 사용하여 SiteMinder 정책 저장소 제거

LDAP 디렉터리에서 SiteMinder 정책 저장소 데이터 및 스키마를 제거하려면 데이터를 먼저 삭제한 다음 스키마를 제거해야 합니다.

중요!

- SiteMinder 정책 저장소 데이터를 제거하기 전에 삭제하려는 데이터가 포함된 정책 저장소에 정책 서버가 연결되어 있는지 확인하십시오. smldapsetup 은 정책 서버가 연결된 정책 저장소의 데이터를 제거합니다. 또한 데이터를 제거하기 전에 정책 저장소 데이터를 출력 파일로 내보내고 해당 파일의 백업을 생성하십시오.
- Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하려면 시스템에 관리자로 로그인했더라도 관리자 권한으로 명령줄 창을 열어야 합니다. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

smldapsetup 을 사용하여 정책 저장소를 제거하려면

1. 다음 위치로 이동합니다.
   - (Windows) *siteminder_home*\bin
   - (UNIX) *siteminder_home*/bin

   siteminder_home

   SiteMinder가 설치된 위치를 지정합니다.
2. 다음 명령을 입력하여 정책 저장소 데이터를 제거합니다.

   ```
   smldapsetup remove -hLDAP_IP_Address -pLDAP_Port
   -d LDAP_Admin -wLDAP_Admin_Password -rLDAP_Base_DN
   -v
   ```

   예: smldapsetup remove -h192.169.125.32 -p552 -d"cn=directory manager" -wfirewall -rdc=ad,dc=test,dc=com -v

   참고: 정책 저장소 데이터를 제거하는 데는 약간의 시간이 걸릴 수 있습니다.
3. 다음을 입력하여 스키마를 삭제하는 데 사용할 LDIF 파일을 생성합니다.

   ```
   smldapsetup ldgen -e -fldif
   ```

   ldif

   생성할 LDIF 파일의 이름을 지정합니다.

   예: smldapsetup ldgen -e -fdelete.ldif
4. 다음 명령을 실행하여 SiteMinder 스키마를 제거합니다.

   ```
   smldapsetup ldmod -fldif
   ```

   ldif

   smldapsetup ldgen -e 를 사용하여 생성된 LDIF 파일의 이름을 지정합니다.

   예: smldapsetup ldmod -fdelete.ldif

ODBC 데이터베이스의 SiteMinder 데이터 삭제

SiteMinder 는 ODBC 데이터베이스에서 SiteMinder 스키마를 삭제하는 SQL 스크립트를 제공합니다. 다음 목록에서는 각 SQL 스크립트에 대해 설명합니다.

sm_oracle_ps_delete.sql

Oracle 데이터베이스에서 SiteMinder 정책 저장소 및 데이터를 제거합니다.

sm_oracle_logs_delete.sql

데이터베이스가 sm_oracle_logs.sql 을 사용하여 생성된 경우 Oracle 데이터베이스에 저장된 SiteMinder 로그를 제거합니다.

sm_oracle_ss_delete.sql

Oracle 데이터베이스에서 SiteMinder 세션 저장소 테이블 및 데이터를 제거합니다.

sm_mssql_ps_delete.sql

SQL 데이터베이스에서 SiteMinder 정책 저장소 및 데이터를 제거합니다.

sm_mssql_logs_delete.sql

데이터베이스가 sm_mssql_logs.sql 을 사용하여 생성된 경우 SQL 데이터베이스에 저장된 SiteMinder 로그를 제거합니다.

sm_mssql_ss_delete.sql

SQL 데이터베이스에서 SiteMinder 세션 저장소 테이블 및 데이터를 제거합니다.

sm_db2_ps_delete.sql

DB2 데이터베이스에서 SiteMinder 정책 저장소 및 데이터를 제거합니다.

sm_db2_logs_delete.sql

데이터베이스가 sm_db2_logs.sql 을 사용하여 생성된 경우 DB2 데이터베이스에 저장된 SiteMinder 로그를 제거합니다.

sm_db2_ss_delete.sql

DB2 데이터베이스에서 SiteMinder 세션 저장소 테이블 및 데이터를 제거합니다.

ODBC 데이터베이스 SQL 스크립트는 다음 위치에 있습니다.

- (Windows) *siteminder_home*\db

  siteminder_home

  정책 서버 설치 경로를 지정합니다.

- (UNIX) *siteminder_home*/db

  siteminder_home

  정책 서버 설치 경로를 지정합니다.

DB2, SQL Plus for Oracle 또는 SQL Server 쿼리 분석기를 통해 적절한 SQL 스크립트를 실행하여 데이터베이스 개체를 삭제하십시오.

참고: SQL 스크립트 실행에 대한 자세한 내용은 데이터베이스 설명서를 참조하십시오.

smpatchcheck

smpatchcheck 도구를 사용하여 정책 서버 및 웹 에이전트에 필요한 Solaris 패치가 시스템에 설치되어 있는지 여부를 확인할 수 있습니다. Smpatchcheck 는 "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)에 나열된 Solaris 버전에서 실행할 수 있습니다. 이 지원표에 액세스하려면 기술 지원 사이트로 이동하여 "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)를 검색하십시오.

smpatchcheck 를 사용하려면

1. *siteminder_home*/bin 으로 이동합니다.

   siteminder_home

   정책 서버 설치 경로를 지정합니다.

2. smpatchcheck 를 입력합니다.

   smpatchcheck 가 각 필수/권장 패치를 찾아 해당 상태를 표시합니다.

   예를 들면 다음과 같습니다.

```
Testing for Required Patches:
  Testing for Patch: 106327-09 ... NOT Installed
Testing for Recommended Patches:
  Testing for Patch: 106541-08 ... Installed
  Testing for Patch: 106980-00 ... Installed
SiteMinder Patch Check: Failed
```

Smpatchcheck 는 다음 메시지 중 하나를 반환합니다.

실패

필수 패치 하나 이상이 설치되어 있지 않습니다.

Partially Failed

권장 패치 하나 이상이 설치되어 있지 않습니다.

Success

필수 및 권장 패치가 모두 설치되어 있습니다.

SiteMinder 테스트 도구

SiteMinder 테스트 도구는 에이전트와 정책 서버 간의 상호 작용을 시뮬레이트하는 유틸리티로, 정책 서버의 기능을 테스트합니다. 테스트 중 테스트 도구는 에이전트의 역할을 하여 실제 에이전트와 동일하게 정책 서버에 요청합니다. 따라서 SiteMinder 구성을 배포하기 전에 테스트할 수 있습니다.

참고: 이 도구에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

smreg

슈퍼 사용자 암호를 변경하려면

1. 정책 서버가 실행 중이고 구성된 정책 저장소에 연결되어 있는지 확인합니다.
2. smreg 유틸리티가 *policy_server_home*\bin 에 있는지 확인합니다.

   policy_server_home

   정책 서버 설치 경로를 지정합니다.

   참고: 이 유틸리티가 없는 경우 CA Support 사이트에서 제공되는 정책 서버 설치 미디어에서 찾을 수 있습니다.

3. 다음 명령을 실행합니다.

   `smreg -su password`

   password

   SiteMinder 슈퍼 사용자 계정의 암호를 지정합니다.

   참고: -su 와 암호 사이에 공백이 있어야 합니다.

   이 유틸리티는 슈퍼 사용자 계정 암호를 변경합니다.

4. smreg 유틸리티를 삭제합니다.

   이 유틸리티를 삭제하면 다른 사용자가 슈퍼 사용자의 암호를 변경하는 것을 방지할 수 있습니다.

XPSCounter

SiteMinder 사용권 계약을 준수하려면 SiteMinder 환경의 사용자 수를 계산하십시오. 다음 과정에서는 디렉터리를 구성하고 해당 디렉터리 내에 저장된 SiteMinder 사용자 수를 계산하는 방법에 대해 설명합니다.

1. 사용자 수를 계산할 각 사용자 디렉터리를 다음과 같이 변경합니다.

   참고: 자세한 내용은 *SiteMinder 정책 서버 구성 안내서*를 참조하십시오.

   - 관리 UI 에서 디렉터리 관리자의 사용자 이름과 암호를 입력하여 관리자 자격 증명을 사용하도록 합니다.
   - 관리 UI 를 사용하여 유니버설 ID 및 기타 사용자 특성 매핑을 정의합니다.

2. Microsoft Active Directory 사용자 저장소의 경우 관리 UI 를 사용하여 inetOrgPerson 특성을 매핑합니다.
3. SiteMinder 정책과 연결된 사용자 수를 확인합니다.

Active Directory inetOrgPerson 특성 매핑

SiteMinder 사용자 저장소가 Microsoft Active Directory 서버에 있는 경우 SiteMinder 사용자를 계산하기 전에 각 서버에서 inetOrgPerson 을 매핑합니다.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. "인프라", "디렉터리"를 차례로 클릭합니다.

3. "사용자 디렉터리"를 클릭합니다.
4. 원하는 사용자 디렉터리를 검색하고 디렉터리 이름을 클릭합니다.
5. "수정"을 클릭합니다.
6. "특성 매핑 목록" 섹션에서 "만들기"를 클릭합니다.
7. 개체를 만드는 옵션을 선택하고 "확인"을 클릭합니다.
8. 다음 이름을 입력합니다.

   inetOrgPerson
9. 다음 설명을 입력합니다.

   Active Directory 사용자를 계산하기 위한 사용자 지정 매핑(XPSCounter 사용)
10. "속성" 섹션에서 다음 작업을 수행하십시오.
    a. "별칭" 옵션이 선택되어 있는지 확인합니다.
    b. 다음 정의를 입력합니다.

       사용자
11. "확인"을 클릭합니다.
12. "제출"을 클릭합니다.

    inetOrgPerson 특성이 매핑됩니다.

SiteMinder 정책과 연결된 사용자 수 확인

SiteMinder 사용권 계약을 준수하려면 조직에서 SiteMinder 정책과 연결된 사용자 수를 확인하면 됩니다.

참고: 사용자에게 SiteMinder 바이너리 파일(XPS.dll, libXPS.so, libXPS.sl)에 대한 쓰기 액세스 권한이 *없다면* 관리자가 관리 UI 또는 XPSSecurity 도구를 사용하여 관련 XPS 명령줄 도구를 사용할 수 있는 권한을 사용자에게 부여해야 합니다.

사용자 수를 확인하려면

1. 정책 서버에서 명령 창을 열고 다음 명령을 입력합니다.

   XPSCounter

   이 도구가 시작되어 이 세션에 대한 로그 파일 이름이 표시되고 "License Parameters"(라이선스 매개 변수) 메뉴가 열립니다.

2. 1 을 입력합니다.

   "Parameter"(매개 변수) 메뉴가 나타납니다.

3. C 를 입력합니다.

   "Counter"(카운터) 메뉴가 나타납니다.

4. I 를 입력합니다.

5. ?를 입력하여 사용자 디렉터리 XID 를 검색합니다. 정책 저장소에 정의된 사용자 디렉터리만 목록에 표시됩니다.

6. 사용자 수를 확인할 디렉터리의 번호를 입력합니다.

   참고: 이 도구는 지정된 각 디렉터리에 있는 사용자 개체의 수를 계산합니다. 하지만 여러 디렉터리에 나열된 동일한 사용자 개체 또는 한 디렉터리에 있는 동일한 사용자에 대한 여러 사용자 개체는 계산하지 않습니다. 이 도구에서 제공된 결과를 해석할 때는 이 점을 고려해야 합니다.

7. (선택 사항) 결과를 설명하기 위한 주석을 입력합니다.

   사용자 수가 계산되고 확인 메시지가 표시됩니다.

8. (선택 사항) 5~8 단계를 반복하여 다른 디렉터리의 사용자 수를 계산합니다.

9. V 를 입력합니다.

   계산된 *각* 디렉터리에 대해 다음 정보가 표시됩니다.

   XID

   지정한 사용자 디렉터리에 대한 고유 식별자를 표시합니다.

   예: CA.SM::UserDirectory@0e-50ea30f0-b5c0-450c-a135-1e317dd25f11

   이름

   관리 UI 에 정의되어 있는 지정한 사용자 디렉터리의 이름을 표시합니다.

   : *count*

   지정한 사용자 디렉터리의 최신 사용자 수를 표시합니다. 이 값은 카운터가 실행될 때마다 자동으로 업데이트되므로 카운터에 저장된 이전 값을 삭제할 필요가 *없습니다*.

   예: 23

   합계

   계산한 모든 사용자 디렉터리의 사용자 수 합계를 표시합니다. 예를 들어 두 개의 서로 다른 디렉터리에서 사용자 수를 계산하고 각 디렉터리의 사용자 수가 23 일 경우 표시되는 합계는 46 입니다.

XPSConfig

XPSConfig 는 관리자 및 작업 구성원이 제품 매개 변수를 보고, 허용된 경우 해당 설정을 편집하는 데 사용할 수 있는 대화형 명령줄 유틸리티입니다. XPS 프로그래밍 인터페이스를 사용하는 제품 관련 구성 도구를 사용할 수도 있고 XPSConfig 를 사용할 수도 있으므로 XPSConfig 는 필수 도구는 아닙니다.

각 공급업체와 설치된 제품에 대해 XPSConfig 는 제품의 데이터 사전에 정의된 매개 변수 또는 명명된 설정을 관리합니다. 각 제품은 해당 제품의 매개 변수 설정을 읽고, 쓰고, 유효성을 검사할 수 있습니다.

XPSConfig 는 XPSConfig 권한이 있는 관리자만 사용할 수 있습니다.

매개 변수에는 다음과 같은 특성이 있습니다.

이름

매개 변수의 이름을 지정합니다.

제한:

- 이름은 문자나 밑줄로 시작해야 하며 문자, 숫자 및 밑줄만 포함해야 합니다.
- 이름에는 최대 32 자를 사용할 수 있습니다.
- 이름은 대/소문자를 구분하지 않습니다.

유형

매개 변수 값의 데이터 형식을 지정합니다.

`Logical | Numeric | String`

Logical

부울 값(TRUE 또는 FALSE)을 지정합니다.

Numeric

정수를 지정합니다.

문자열

문자열을 지정합니다.

범위

매개 변수의 값 또는 범위를 지정합니다.

`Ask | Global | Local | Managed | Overrideable | Read Only`

Ask

값이 XPS 가 아니라 제품에 의해 관리되며 읽기 전용임을 지정합니다.

Global

값을 정책 저장소에 저장하며 해당 정책 저장소를 공유하는 모든 정책 서버에서 액세스할 수 있도록 지정합니다.

로컬

각 정책 서버가 고유한 값을 저장하도록 지정합니다.

Managed

값이 XPS 가 아니라 제품에 의해 관리되며 읽기/쓰기가 가능함을 지정합니다.

Overrideable

정책 서버에 로컬로 저장된 값이 공유 정책 저장소에 전역적으로 저장된 값을 재정의하도록 지정합니다.

Read Only

값이 기본값이고 읽기 전용임을 지정합니다.

Export

정책 저장소를 내보낼 때 매개 변수를 포함할지 여부를 지정합니다.

형식: 부울

보고서

매개 변수를 정책 서버에 대한 보고 기능에 포함할지 여부를 지정합니다.

형식: 부울

RemoteAccess

매개 변수에 대한 원격 API 의 액세스 유형을 지정합니다.

`None | Read | ReadWrite`

설명

매개 변수의 용도를 설명합니다.

LicenseType

라이선스 제한의 유형을 지정합니다.

`None | SoftLimit | HardLimit | ExpDate`

없음

매개 변수가 라이선스 제한이 아님을 지정합니다.

SoftLimit

매개 변수가 유연하거나 권장되는 라이선스 제한임을 지정합니다.

HardLimit

매개 변수가 엄격하거나 절대적인 라이선스 제한임을 지정합니다.

ExpDate

매개 변수가 라이선스 만료 날짜임을 지정합니다.

Default Value

현재 값이 정의되어 있지 않은 경우 사용할 기본값을 지정합니다.

참고: 기본값이 정의되지 않은 경우 해당 데이터 형식에 따라 기본값이 지정됩니다.

문자열

공백

숫자

zero

부울

FALSE

Visible

매개 변수가 XPSConfig 에 표시되도록 지정합니다.

형식: 부울

구문

XPSConfig 구문 형식은 다음과 같습니다.

```
XPSConfig [-vendor vendor] [-product product]
[-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path] [-r rec_path]
```

매개 변수

XPSConfig 에는 다음 옵션이 포함되어 있습니다.

-vendor

(선택 사항) 보려는 데이터의 관련 공급업체 이름을 지정합니다.

-product

(선택 사항) 보려는 데이터의 관련 제품 이름을 지정합니다.

-?

(선택 사항) 이 유틸리티에 대한 도움말 정보를 표시합니다.

-vT | -vI | -vW | -vE | -vF

(선택 사항) 오류 파일에 오류 정보를 로깅할 시기와 로깅할 정보의 양을 지정합니다.

-vT

오류를 추적(TRACE)할 수 있도록 상세 정보를 로깅합니다.

-vI

오류가 발생할 경우 정보를 로깅합니다.

-vW

"WARNING"(경고), "ERROR"(오류) 또는 "FATAL"(치명적 오류) 수준의 오류가 발생할 경우 오류 정보를 로깅합니다.

-vE

"ERROR"(오류) 또는 "FATAL"(치명적 오류) 수준의 오류가 발생할 경우 오류 정보를 로깅합니다.

-vF

"FATAL"(치명적 오류) 수준의 오류가 발생할 경우 오류 정보를 로깅합니다.

-l

(선택 사항) 지정된 위치에 로깅 정보를 출력합니다.

기본값: stdout

-e

(선택 사항) 지정된 위치에 오류 정보를 출력합니다.

기본값: stderr

-r

(선택 사항) 세션의 레코드를 지정된 위치로 출력합니다.

XPSEvaluate

XPSEvaluate 는 관리자 및 응용 프로그램 개발자가 식을 평가하고 성능을 테스트하는 데 사용할 수 있는 대화형 명령줄 유틸리티입니다.
XPSEvaluate 는 XPSEvaluate 권한이 있는 관리자만 사용할 수 있습니다.

구문

XPSEvaluate 구문 형식은 다음과 같습니다.

```
XPSEvaluate [-np] [-trace] [-dbg debuglist]
[-f DB | formulapath] [-c contextpath] [-u userpath] [-step]
[-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path] [-r rec_path]
```

매개 변수

XPSEvaluate 에는 다음 옵션이 포함되어 있습니다.

-np

(선택 사항) 프롬프트를 표시하지 않도록 지정합니다.

-trace

(선택 사항) 추적 기능을 설정합니다.

-dbg

(선택 사항) 디버그 목록을 지정합니다.

-f

(선택 사항) 명명된 식의 위치를 지정합니다.

참고: DB 는 정책 저장소를 지정합니다.

-c

(선택 사항) 컨텍스트 값의 위치를 지정합니다.

-u

(선택 사항) 사용자 특성의 위치를 지정합니다.

-step

(선택 사항) 평가 단계를 표시합니다.

-?

(선택 사항) 이 유틸리티에 대한 도움말 정보를 표시합니다.

-vT | -vI | -vW | -vE | -vF

(선택 사항) 오류 파일에 오류 정보를 로깅할 시기와 로깅할 정보의 양을 지정합니다.

-vT

오류를 추적(TRACE)할 수 있도록 상세 정보를 로깅합니다.

-vI

오류가 발생할 경우 정보를 로깅합니다.

-vW

"WARNING"(경고), "ERROR"(오류) 또는 "FATAL"(치명적 오류) 수준의 오류가 발생할 경우 오류 정보를 로깅합니다.

-vE

"ERROR"(오류) 또는 "FATAL"(치명적 오류) 수준의 오류가 발생할 경우 오류 정보를 로깅합니다.

-vF

"FATAL"(치명적 오류) 수준의 오류가 발생할 경우 오류 정보를 로깅합니다.

-l

(선택 사항) 지정된 위치에 로깅 정보를 출력합니다.

기본값: stdout

-e

(선택 사항) 지정된 위치에 오류 정보를 출력합니다.

기본값: stderr

-r

(선택 사항) 세션의 레코드를 지정된 위치로 출력합니다.

XPSExplorer

XPSExplorer 는 관리자 또는 응용 프로그램 개발자가 정책 저장소의 데이터를 보는 데 사용할 수 있는 대화형 명령줄 유틸리티입니다. XPSExplorer 는 다음 두 가지 용도로 사용됩니다.

- 도메인 또는 영역 목록을 탐색하여 세부적으로 내보내거나 가져올 개체의 식별자를 결정하려는 경우
- 개체 저장소가 손상되어 수동으로 복원해야 할 경우. 이 작업은 CA 지원 담당자의 안내에 따라서만 수행해야 합니다.

XPSExplorer 는 XPSExplorer 권한이 있는 관리자만 사용할 수 있습니다.

구문

XPSExplorer 구문 형식은 다음과 같습니다.

```
XPSExplorer [-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path] [-r rec_path]
```

매개 변수

XPSExplorer 에는 다음 옵션이 포함되어 있습니다.

-?

(선택 사항) 이 유틸리티에 대한 도움말 정보를 표시합니다.

-vT | -vI | -vW | -vE | -vF

(선택 사항) 오류 파일에 오류 정보를 로깅할 시기와 로깅할 정보의 양을 지정합니다.

-vT

오류를 추적(TRACE)할 수 있도록 상세 정보를 로깅합니다.

-vI

오류가 발생할 경우 정보를 로깅합니다.

-vW

"WARNING"(경고), "ERROR"(오류) 또는 "FATAL"(치명적 오류) 수준의 오류가 발생할 경우 오류 정보를 로깅합니다.

-vE

"ERROR"(오류) 또는 "FATAL"(치명적 오류) 수준의 오류가 발생할 경우 오류 정보를 로깅합니다.

-vF

"FATAL"(치명적 오류) 수준의 오류가 발생할 경우 오류 정보를 로깅합니다.

-l

(선택 사항) 지정된 위치에 로깅 정보를 출력합니다.

기본값: stdout

-e

(선택 사항) 지정된 위치에 오류 정보를 출력합니다.

기본값: stderr

-r

(선택 사항) 세션의 레코드를 지정된 위치로 출력합니다.

일부 정책 저장소 데이터 내보내기

일부 정책 저장소 데이터를 내보내려면 내보낼 개체의 식별자(XID)가 필요합니다. XPSExplorer 를 사용하여 개체 식별자를 찾을 수 있습니다. XPSExplorer 는 XPSExplorer 권한이 있는 관리자만 사용할 수 있습니다.

이 사용 사례에서는 다음과 같은 회계 응용 프로그램을 내보냅니다.

- Accounts Payable
- Accounts Receivable
- General Ledger
- Payroll

일부 정책 저장소 데이터 내보내기

1. 정책 서버를 호스트하는 컴퓨터에서 명령 프롬프트를 엽니다.
2. 다음 명령을 입력합니다.

   ```
   XPSExplorer
   ```

   "Main Menu"(기본 메뉴)가 열리고 공급업체, 제품 및 클래스 목록이 표시됩니다.

   참고: 최상위 클래스의 개체만 내보낼 수 있습니다. 최상위 클래스는 별표로 표시됩니다.
3. 내보낼 개체의 클래스에 해당하는 번호를 입력합니다.

   "Class Menu"(클래스 메뉴)가 열립니다.

   예: accounting 에 해당하는 번호가 15 인 경우 15 를 입력합니다.
4. S 를 입력하여 해당 클래스의 개체를 표시합니다.

   "Search Menu"(검색 메뉴)가 열리고 해당 클래스의 개체가 표시됩니다.

   검색 결과 예:

   1-CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8

   (I) Name : "Accounts Payable"

   (C) Desc : "accounts payable"

   2-CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244

   (I) Name : "Accounts Receivable"

   (C) Desc : "accounts receivable"

   3-CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92

   (I) Name : "General Ledger"

   (C) Desc : "general ledger"

   4-CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b

   (I) Name : "Payroll"

   (C) Desc : "payroll"

   5-CA.SM::Accounting@@12-88f119a0-3fd1-46d0-b8ac-c1e83f00f97d

   (I) Name : "Job Costing"

   (C) Desc : "job costing"

개체 식별자(XID) 예:

CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8

CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244

CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92

CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b

CA.SM::Accounting@@12-88f119a0-3fd1-46d0-b8ac-c1e83f00f97d

5. Q 를 세 번 입력하여 "Search Menu"(검색 메뉴), "Class Menu"(Class 메뉴) 및 "Main Menu"(기본 메뉴)를 종료하고 명령 프롬프트로 돌아갑니다.
6. 명령 프롬프트에 다음 명령을 입력합니다.

```
XPSExport output_file -xo object_XID_1 -xo object_XID_2
-xo object_XID_3 -xo object_XID_4
```

output_file

정책 저장소 데이터를 내보낼 XML 파일을 지정합니다.

-xo *object_XID*

내보낼 각 개체의 식별자를 지정합니다.

참고: 검색 결과에서 개체 식별자(XID)를 복사하여 명령줄에 붙여 넣을 수 있습니다.

예:

```
XPSExport accounting.xml
-xo CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8
-xo CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244
-xo CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92
-xo CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b
```

지정한 회계 응용 프로그램의 정책 저장소 데이터가 accounting.xml 로 내보내집니다.

XCart 관리

XPSExplorer 에는 XCart 기능이 포함되어 있습니다. 내보낼 개체의 식별자(XID)를 수동으로 복사하여 붙여 넣을 필요 없이 XCart 를 사용하여 해당 식별자를 수집하고 나중에 사용할 수 있도록 파일에 저장할 수 있습니다. XPSExplorer 는 XPSExplorer 권한이 있는 관리자만 사용할 수 있습니다.

XCart 에 액세스하려면 XPSExplorer 의 "Main Menu"(기본 메뉴)에서 "XCart Management"(XCart 관리)에 해당하는 X 를 입력하십시오. "XCart Menu"(XCart 메뉴)가 열리고 XCart 에 있는 개체가 표시됩니다. 다음 옵션은 상황에 맞는 옵션이므로 경우에 따라 표시되지 않을 수 있습니다.

C - Clear cart(카트 지우기)

XCart 를 비웁니다.

L - Load cart from file(파일에서 카트 로드)

- 초기 로드 - 지정된 파일의 내용과 함께 XCart 를 로드하고 지정된 파일 이름을 XCart 파일로 기억합니다.
- 이후 로드 - 지정된 파일의 내용을 XCart 에 추가합니다.

  참고: XCart 파일의 이름은 변경되지 않습니다.

S - Save cart to file: xcart_file(xcart_file 파일에 카트 저장)

XCart 의 내용을 XCart 파일에 저장합니다.

중요! S 명령은 덮어쓰기 여부를 묻지 않고 XCart 파일의 내용을 덮어씁니다.

N - Save cart to new file(새 파일에 카트 저장)

지정된 파일에 XCart 의 내용을 저장하고 지정된 파일 이름을 XCart 파일로 기억합니다.

참고: N 명령을 사용할 경우 지정된 파일을 덮어쓰기 전에 메시지가 표시됩니다.

각 개체는 XPS 파일에서 정책 저장소로 개체를 가져오는 방법을 결정하는 가져오기 모드로 태그가 지정됩니다.

A - Set import mode to ADD(가져오기 모드를 ADD 로 설정)

기존 개체를 대체하지 않고 새 개체를 추가합니다.

O - Set import mode to OVERLAY(가져오기 모드를 OVERLAY 로 설정)

기존 개체를 대체하고 새 개체를 추가하지 않습니다.

R - Set import mode to REPLACE(가져오기 모드를 REPLACE 로 설정)

기존 개체를 대체하고 새 개체를 추가합니다.

D - Set import mode to default(가져오기 모드를 기본값으로 설정)

기본 가져오기 모드를 지정합니다.

참고: 제품의 데이터 사전에 각 제품 클래스에 대한 기본 가져오기 모드가 정의되어 있습니다.

Q - Quit(종료)

"XCart Menu"(XCart 메뉴)를 종료하고 "Main Menu"(기본 메뉴)로 돌아갑니다.

XCart 를 사용하여 일부 정책 저장소 데이터 내보내기

일부 정책 저장소 데이터를 내보내려면 내보낼 개체의 식별자(XID)가 필요합니다. XPSExplorer 의 XCart 기능을 사용하여 개체를 찾고 나중에 내보낼 때 사용할 수 있도록 해당 개체를 XCart 파일에 저장할 수 있습니다. 예를 들어 관리자는 작업 구성원의 XCart 파일을 설정하여 필요할 때 사용할 수 있습니다. XPSExplorer 는 XPSExplorer 권한이 있는 관리자만 사용할 수 있습니다.

이 사용 사례에서는 다음과 같은 네 개의 회계 응용 프로그램을 나중에 사용할 수 있도록 파일에 저장합니다.

- Accounts Payable
- Accounts Receivable
- General Ledger
- Payroll

XCart 를 사용하여 일부 정책 저장소 데이터 내보내기

1. 정책 서버를 호스트하는 컴퓨터에서 명령 프롬프트를 엽니다.
2. 다음 명령을 입력합니다.

   ```
   XPSExplorer
   ```

   "Main Menu"(기본 메뉴)가 열리고 공급업체, 제품 및 클래스 목록이 표시됩니다.

   참고: 최상위 클래스의 개체만 내보낼 수 있습니다. 최상위 클래스는 별표로 표시됩니다.

3. "XCart Management"(XCart 관리)에 해당하는 X 를 입력합니다.

   "XCart Menu"(XCart 메뉴)가 열립니다.

4. 텍스트 파일을 생성합니다.

   예: C:\xcart\accounting.txt

   참고: 이 파일에 XCart 의 내용이 저장됩니다.

5. Load cart from file(파일에서 카트 로드)에 해당하는 L 을 입력합니다.

6. 생성한 텍스트 파일의 경로와 이름을 입력합니다.

   지정한 파일 이름은 XCart 파일로 기억됩니다.

   예: C:\xcart\accounting.txt

   참고: 파일이 이미 있어야 합니다. 그렇지 않으면 L 을 입력해도 소용이 없습니다.

7. Q 를 입력하여 "Main Menu"(기본 메뉴)로 돌아갑니다.

8. 내보낼 클래스에 해당하는 번호를 입력합니다.

   "Class Menu"(클래스 메뉴)가 열립니다.

   예: Accounting 에 해당하는 번호가 15 인 경우 15 를 입력합니다.

9. S 를 입력하여 해당 클래스의 개체를 표시합니다.

   "Search Menu"(검색 메뉴)가 열리고 해당 클래스의 개체가 표시됩니다.

   검색 결과 예:

   1-CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8

   (I) Name : "Accounts Payable"

   (C) Desc : "accounts payable"

   2-CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244

   (I) Name : "Accounts Receivable"

   (C) Desc : "accounts receivable"

   3-CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92

   (I) Name : "General Ledger"

   (C) Desc : "general ledger"

4-CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b

(I) Name : "Payroll"

(C) Desc : "payroll"

5-CA.SM::Accounting@@12-88f119a0-3fd1-46d0-b8ac-c1e83f00f97d

(I) Name : "Job Costing"

(C) Desc : "job costing"

10. Accounting 응용 프로그램 1~4 에 대해 다음을 수행합니다.
    a. 응용 프로그램에 해당하는 번호를 입력합니다.
    b. "Add to XCart"(XCart 에 추가)에 해당하는 X 를 입력합니다.
    c. Q 를 입력하여 "XCart Menu"(XCart 메뉴)를 종료하고 "Search Menu"(검색 메뉴)로 돌아갑니다.

    참고: 응용 프로그램 앞의 별표는 해당 응용 프로그램이 XCart 에 있음을 나타냅니다.
11. Q 를 두 번 입력하여 "Search Menu"(검색 메뉴)와 "Class Menu"(Class 메뉴)를 종료하고 "Main Menu"(기본 메뉴)로 돌아갑니다.
12. "XCart Management"(XCart 관리)에 해당하는 X 를 입력합니다.
13. S 를 입력하여 XCart 파일(C:\xcart\accounting.txt)에 카트를 저장합니다.
14. Q 를 두 번 입력하여 "XCart Menu"(XCart 메뉴)와 "Main Menu"(기본 메뉴)를 종료하고 명령 프롬프트로 돌아갑니다.
15. 명령 프롬프트에 다음 명령을 입력합니다.

    `XPSExport output_file -xf xcart_file`

    output_file

    정책 저장소 데이터를 내보낼 XML 파일을 지정합니다.

    -xf *xcart_file*

    내보낼 개체의 식별자(XID)가 포함된 XCart 파일의 경로와 이름을 지정합니다.

    예:

    ```
    XPSExport accounting.xml C:\xcart\accounting.txt
    ```

    XCart 파일에 저장된 회계 응용 프로그램의 정책 저장소 데이터가 accounting.xml 로 내보내집니다.

XCart 파일에 응용 프로그램 추가

이 사용 사례에서는 XPSExplorer 의 XCart 기능을 사용하여 XCart 파일 accounting.txt 에 이미 있는 다음 네 개의 회계 응용 프로그램에 다섯 번째 회계 응용 프로그램 Job Costing 을 추가합니다.

- Accounts Payable
- Accounts Receivable
- General Ledger
- Payroll

참고: XPSExplorer 는 XPSExplorer 권한이 있는 관리자만 사용할 수 있습니다.

XCart 파일에 응용 프로그램 추가

1. 정책 서버를 호스트하는 컴퓨터에서 명령 프롬프트를 엽니다.
2. 다음 명령을 입력합니다.

   ```
   XPSExplorer
   ```

   "Main Menu"(기본 메뉴)가 열리고 공급업체, 제품 및 클래스 목록이 표시됩니다.

   참고: 최상위 클래스의 개체만 내보낼 수 있습니다. 최상위 클래스는 별표로 표시됩니다.
3. "XCart Management"(XCart 관리)에 해당하는 X 를 입력합니다.

   "XCart Menu"(XCart 메뉴)가 열립니다.
4. Load cart from file(파일에서 카트 로드)에 해당하는 L 을 입력합니다.
5. 네 개의 회계 응용 프로그램이 포함된 기존 텍스트 파일의 경로와 이름을 입력합니다.

   지정한 파일 이름은 XCart 파일로 기억됩니다.

   예: C:\xcart\accounting.txt
6. Q 를 입력하여 "Main Menu"(기본 메뉴)로 돌아갑니다.
7. XCart 파일에 추가할 클래스에 해당하는 번호를 입력합니다.

   "Class Menu"(클래스 메뉴)가 열립니다.

   예: accounting 에 해당하는 번호가 15 인 경우 15 를 입력합니다.

8. S 를 입력하여 해당 클래스의 개체를 표시합니다.

   "Search Menu"(검색 메뉴)가 열리고 해당 클래스의 개체가 표시됩니다.

   검색 결과 예:

   1-CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8

   (I) Name : "Accounts Payable"

   (C) Desc : "accounts payable"

   2-CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244

   (I) Name : "Accounts Receivable"

   (C) Desc : "accounts receivable"

   3-CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92

   (I) Name : "General Ledger"

   (C) Desc : "general ledger"

   4-CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b

   (I) Name : "Payroll"

   (C) Desc : "payroll"

   5-CA.SM::Accounting@@12-88f119a0-3fd1-46d0-b8ac-c1e83f00f97d

   (I) Name : "Job Costing"

   (C) Desc : "job costing"

   참고: 응용 프로그램 앞의 별표는 해당 응용 프로그램이 XCart 에 있음을 나타냅니다.

9. XCart 파일에 Job Costing 을 추가하려면

   a. Job Costing 응용 프로그램에 해당하는 5 를 입력합니다.

   b. "Add to XCart"(XCart 에 추가)에 해당하는 X 를 입력합니다.

   c. Q 를 입력하여 "XCart Menu"(XCart 메뉴)를 종료하고 "Search Menu"(검색 메뉴)로 돌아갑니다.

      응용 프로그램 앞의 별표는 해당 응용 프로그램이 XCart 에 있음을 나타냅니다.

   d. Q 를 두 번 입력하여 "Search Menu"(검색 메뉴)와 "Class Menu"(Class 메뉴)를 종료하고 "Main Menu"(기본 메뉴)로 돌아갑니다.

e. "XCart Management"(XCart 관리)에 해당하는 X 를 입력합니다.

f. S 를 입력하여 XCart 파일(C:\xcart\accounting.txt)에 XCart 를 저장합니다.

Job Costing 이 accounting.txt 에 추가됩니다.

10. Q 를 두 번 입력하여 "XCart Menu"(XCart 메뉴)와 "Main Menu"(기본 메뉴)를 종료하고 명령 프롬프트로 돌아갑니다.

XPSSecurity

XPSSecurity 는 관리자 및 작업 구성원이 관리자를 생성 및 삭제하고 해당 권한을 편집하는 데 사용할 수 있는 대화형 명령줄 유틸리티입니다. XPSSecurity 는 XPSSecurity 권한이 있는 관리자만 사용할 수 있습니다.

구문

XPSSecurity 구문 형식은 다음과 같습니다.

```
XPSSecurity [-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path] [-r rec_path]
```

매개 변수

XPSSecurity 에는 다음 옵션이 포함되어 있습니다.

-?

(선택 사항) 이 유틸리티에 대한 도움말 정보를 표시합니다.

-vT | -vI | -vW | -vE | -vF

(선택 사항) 오류 파일에 오류 정보를 로깅할 시기와 로깅할 정보의 양을 지정합니다.

-vT

오류를 추적(TRACE)할 수 있도록 상세 정보를 로깅합니다.

-vI

오류가 발생할 경우 정보를 로깅합니다.

-vW

"WARNING"(경고), "ERROR"(오류) 또는 "FATAL"(치명적 오류) 수준의 오류가 발생할 경우 오류 정보를 로깅합니다.

-vE

"ERROR"(오류) 또는 "FATAL"(치명적 오류) 수준의 오류가 발생할 경우 오류 정보를 로깅합니다.

-vF

"FATAL"(치명적 오류) 수준의 오류가 발생할 경우 오류 정보를 로깅합니다.

-l

(선택 사항) 지정된 위치에 로깅 정보를 출력합니다.

기본값: stdout

-e

(선택 사항) 지정된 위치에 오류 정보를 출력합니다.

기본값: stderr

-r

(선택 사항) 세션의 레코드를 지정된 위치로 출력합니다.

관리자를 슈퍼 사용자로 설정

슈퍼 사용자는 외부 관리자 저장소에 대한 연결을 구성할 때 정의합니다. 슈퍼 사용자는 다른 모든 관리자 계정을 생성하고 관리하는 데 사용됩니다. 슈퍼 사용자를 사용할 수 없는 경우 XPSSecurity 를 사용하여 외부 저장소의 사용자를 슈퍼 사용자로 설정하십시오.

관리자를 슈퍼 사용자로 설정하려면

1. XPSSecurity 권한이 있는 SiteMinder 관리자 계정을 사용하여 정책 서버 호스트 시스템에 로그인합니다.

   참고: XPSSecurity 권한이 있는 관리자를 사용할 수 없는 경우 다음 중 하나로 로그인하십시오.

   - (Windows) 시스템 관리자
   - (UNIX) 루트
   - 정책 서버를 설치한 사용자

2. XPSSecurity 유틸리티가 *policy_server_home*\bin 에 있는지 확인합니다.

   policy_server_home

   정책 서버 설치 경로를 지정합니다.

   참고: 이 유틸리티가 없는 경우 CA Support 사이트에서 제공되는 정책 서버 설치 미디어에서 찾을 수 있습니다.

3. 명령 창을 열고 다음 명령을 실행합니다.

   ```
   XPSSecurity
   ```

   기본 메뉴가 나타납니다.

4. A 를 입력하고 Enter 키를 누릅니다.

   관리자 메뉴에 외부 저장소의 SiteMinder 관리자 목록이 표시됩니다. 각 관리자 앞에는 번호가 있습니다.

5. 관리자의 번호를 입력하고 Enter 키를 누릅니다.

   관리자 메뉴에 선택한 관리자와 관련된 특성이 표시됩니다. 각 특성 앞에는 번호가 있습니다.

6. 2 를 입력하고 Enter 키를 누릅니다.

   관리자 메뉴가 플래그 설정으로 업데이트됩니다.

7. 물음표(?)를 입력하고 Enter 키를 누릅니다.

   "사용 안 함" 및 "슈퍼 사용자" 플래그가 나타납니다. 각 플래그 앞에는 번호가 있습니다.

8. 2 를 입력하고 Enter 키를 누릅니다.

   "슈퍼 사용자" 플래그가 선택됩니다.

9. Q 를 입력하고 Enter 키를 누릅니다.

   관리자 메뉴에 해당 관리자와 관련된 특성이 표시됩니다. "플래그" 특성이 "슈퍼 사용자"로 설정됩니다.

10. U 를 입력하고 Enter 키를 누릅니다.

    관리자 레코드가 업데이트됩니다.

11. Q 를 입력하고 Enter 키를 누릅니다.

    관리자 메뉴에 외부 저장소의 SiteMinder 관리자 목록이 표시됩니다. 선택한 관리자가 슈퍼 사용자로 표시됩니다.

12. 다음에 나오는 두 메시지에서 Q 를 입력하고 Enter 키를 눌러 유틸리티를 종료합니다.

    선택한 관리자는 이제 슈퍼 사용자입니다. 수정하거나 삭제한 권한을 복원하려면 이 관리자를 사용하십시오.

-XPSSweeper

XPSSweeper 는 명령줄 유틸리티로, 일괄 작업으로도 실행할 수 있습니다. XPSSweeper 를 사용하여 XPS 와 SiteMinder 정책 저장소를 동기화할 수 있습니다. 일반적으로 XPS 는 서로 다른 여러 정책 저장소를 동기화합니다. 그러나 레거시 도구가 사용되는 경우 XPSSweeper 를 사용하여 정책 저장소를 다시 동기화해야 할 수 있습니다. 어떠한 경우에도 XPSSweeper 는 정책 저장소에 손상을 주지 않으며 예방 차원에서 이 도구를 실행할 수 있습니다.

구문

XPSSweeper 구문 형식은 다음과 같습니다.

```
XPSSweeper [-f] [-s seconds] [-m entries]
[-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path]
```

매개 변수

XPSSweeper 에는 다음 옵션이 포함되어 있습니다.

-f

(선택 사항) XPSSweeper 를 영구적 루프로 실행합니다.

참고: 종료하려면 Ctrl+C 를 사용하십시오.

-s

(선택 사항) 각 XPSSweeper 반복 사이에 지정된 시간(초) 동안 대기합니다.

-m

(선택 사항) 항목이 지정된 수만큼 로깅될 때마다 중요 시점 메시지를 출력합니다.

-?

(선택 사항) 이 유틸리티에 대한 도움말 정보를 표시합니다.

-vT | -vI | -vW | -vE | -vF

(선택 사항) 오류 파일에 오류 정보를 로깅할 시기와 로깅할 정보의 양을 지정합니다.

-vT

오류를 추적(TRACE)할 수 있도록 상세 정보를 로깅합니다.

-vI

오류가 발생할 경우 정보(INFOrmation)를 로깅합니다.

-vW

"WARNING"(경고), "ERROR"(오류) 또는 "FATAL"(치명적 오류) 수준의 오류가 발생할 경우 오류 정보를 로깅합니다.

-vE

"ERROR"(오류) 또는 "FATAL"(치명적 오류) 수준의 오류가 발생할 경우 오류 정보를 로깅합니다.

-vF

"FATAL"(치명적 오류) 수준의 오류가 발생할 경우 오류 정보를 로깅합니다.

-l

(선택 사항) 지정된 위치에 로깅 정보를 출력합니다.

기본값: stdout

-e

(선택 사항) 지정된 위치에 오류 정보를 출력합니다.

기본값: stderr

일괄 작업으로 XPSSweeper 실행

XPSConfig 로 다음 두 개의 XPS 구성 매개 변수를 설정하여 XPSSweeper 를 일괄 작업으로 실행할 수 있습니다.

CA.XPS::$Autosweep

XPSweeper 를 Autosweep(자동 정리) 일정에 따라 실행할지, 아니면 XPSSweeper 를 전혀 실행하지 않을지를 지정합니다.

형식: 부울

CA.XPS::$AutosweepSchedule

다음 형식을 사용하여 자동 정리 일정을 GMT 로 지정합니다.

```
DDD@{HH:MM}[,DDD@{HH:MM}] ... [,DDD@{HH:MM}]
```

DDD

(선택 사항) 요일을 지정합니다.

```
Sun | Mon | Tue | Wed | Thu | Fri | Sat
```

HH

시간을 지정합니다.

범위: 00~23

MM

분을 지정합니다.

범위: 00-59

예:

Sun@08:30

일요일 오전 8:30(GMT)마다

Tue@14:00

화요일 오후 2:00(GMT)마다

15:15

매일 오후 3:15(GMT)마다

Sun@08:30,Tue@14:00,15:15

일요일 오전 8:30 분마다, 화요일 오후 2:00 마다, 화요일을 제외한 매일 오후 3:15

참고: 여러 개의 자동 정리 시간을 쉼표, 공백 또는 세미콜론으로 구분하여 입력할 수 있습니다.

정책 서버는 XPSSweeper 자동 정리 시간을 다음과 같이 관리합니다.

- 캐시 검사가 몇 분마다 수행되므로 XPSSweeper 는 일정보다 몇 분 늦게 실행될 수 있습니다.
- 실행 예약된 시간에 XPSSweeper 가 이미 실행 중일 경우 XPSSweeper 가 중지되었다가 다시 시작되지는 않지만 정리 프로세스를 종료할 수 있습니다.
- 예약된 시간이 되어도 이전 실행 시간과의 간격이 2 시간 미만이면 XPSSweeper 가 실행되지 않습니다.

  예: XPSSweeper 가 화요일 오후 2:00 와 매일 오후 3:15 에 실행되도록 예약된 경우 화요일에는 오후 3:15 의 정리가 실행되지 않습니다.

XPSConfig 를 사용하여 24 시간마다 자동 정리가 실행되도록 구성

XPSSweeper 유틸리티가 24 시간마다 한 번씩 실행되도록 구성하는 것이 좋습니다. XPSSweeper 유틸리티가 자주 실행되지 *않으면* 정책 서버를 시작하는 데 문제가 생길 수 있습니다. 정책 저장소에 삭제 표시 개체가 너무 많으면 다음과 같은 오류가 발생합니다.

```
LDAP_SIZELIMIT_EXCEEDED
```

XPSSweeper 유틸리티를 자동으로 실행하도록 설정하는 경우 다음과 같은 XPS 구성 매개 변수가 사용됩니다.

- CA.XPS::$Autosweep
- CA.XPS::$AutosweepSchedule

다음 단계를 수행하십시오.

1. 정책 서버를 호스트하는 컴퓨터에서 명령줄 창을 엽니다.
2. 다음 명령을 입력합니다.

   ```
   XPSConfig
   ```

   "Products Menu"(제품 메뉴)가 열리고 제품 목록이 표시됩니다.
3. "Extensible Policy Store"(확장 가능한 정책 저장소)에 해당하는 XPS 를 입력합니다.

   "Parameters Menu"(매개 변수 메뉴)가 열리고 XPS 매개 변수 목록이 표시됩니다.
4. "Autosweep"(자동 정리)에 해당하는 7 을 입력합니다.

   "Autosweep Parameter Menu"(자동 정리 매개 변수 메뉴)가 열립니다.
5. "Autosweep"(자동 정리) 값이 TRUE 로 설정되어 있는지 확인하고, 그렇지 않으면 C 를 입력하여 값을 TRUE 로 변경합니다.

   참고: 이 단계에서는 자동 정리 일정에 따라 XPSSweeper 를 실행하도록 지정합니다.
6. Q 를 입력하여 "Autosweep Menu"(자동 정리 메뉴)를 종료하고 "Parameters Menu"(매개 변수 메뉴)로 돌아갑니다.
7. "AutosweepSchedule"(자동 정리 일정)에 해당하는 8 을 입력합니다.

   "AutosweepSchedule Parameter Menu"(자동 정리 일정 매개 변수 메뉴)가 열립니다.
8. C 를 입력하여 "AutosweepSchedule"(자동 정리 일정) 매개 변수의 값을 변경합니다.
9. "New Value"(새 값)에 원하는 시간을 입력합니다.
10. Q 를 세 번 입력합니다.

    명령 프롬프트가 나타납니다.

제 21 장: 정책 서버 구성 파일

이 섹션은 다음 항목을 포함하고 있습니다.

CA Compliance Security Manager 구성 파일

SiteMinder 에는 CA Security Compliance Manager 로 수동으로 가져올 수 있는 규정 준수 보고서를 생성하는 명령줄 도구 smcompliance 가 있습니다. CA Compliance Security Manager 구성 파일(compliance.conf)을 사용하면 규정 준수 보고서의 내용을 수정할 수 있습니다.

위치: *siteminder_home*\compliance\config

siteminder_home

정책 서버 설치 경로를 지정합니다.

추가 정보:

기존 규정 준수 보고서의 내용 변경 (페이지 308)
새 규정 준수 보고서 추가 (페이지 307)

연결 API 구성 파일

연결 API 파일(conapi.conf)은 연결 API 를 통해 서비스를 구성하는 데 사용됩니다. 이러한 서비스에는 OneView 모니터가 포함됩니다.

위치: *siteminder_home*\config

siteminder_home

정책 서버 설치 경로를 지정합니다.

추가 정보:

OneView 모니터 포트 번호 구성 (페이지 193)

OneView 모니터 구성 파일

SiteMinder OneView 모니터는 다음을 수행합니다.

- 성능 병목 문제를 확인하고 SiteMinder 배포 환경의 리소스 사용량에 대한 정보를 제공합니다.
- 구성 요소 오류와 같은 특정 이벤트가 발생할 때 경고를 표시합니다.

OneView 모니터 구성 파일(mon.conf)을 사용하여 다음을 지정할 수 있습니다.

- OneView 모니터가 등록된 구성 요소에 데이터를 요청하는 빈도
- 등록된 구성 요소가 OneView 모니터에 하트비트 이벤트를 보내는 빈도
- 정책 서버 구성 요소 인덱스가 상수인지 여부

위치: *siteminder_home*\monitor

siteminder_home

정책 서버 설치 경로를 지정합니다.

추가 정보:

OneView 데이터 새로 고침 빈도 및 하트비트 설정 (페이지 192)

SiteMinder 구성 파일

SiteMinder 구성 파일(siteminder.conf)은 다음을 수행하는 데 사용됩니다.

- 정책 서버 프로세스 시작 및 중지
- 실행 요소 구성 및 사용 여부 설정

하나 이상의 감독 응용 프로그램이 정책 서버 프로세스의 상태를 모니터링하고 실패한 프로세스를 자동으로 다시 시작합니다.

위치: *siteminder_home*\config

siteminder_home

정책 서버 설치 경로를 지정합니다.

추가 정보:

UNIX 감독 기능 구성 (페이지 31)
Windows 감독 기능 구성 (페이지 31)

SNMP 구성 파일

SNMP 호환 네트워크 관리 응용 프로그램은 SiteMinder 환경의 여러 작업 요소를 모니터링할 수 있습니다. SiteMinder SNMP 모듈을 사용하면 이러한 응용 프로그램과 정보를 교환할 수 있습니다.

SNMP 구성 파일(snmp.conf)은 SiteMinder SNMP 모듈에 대한 설정을 제공합니다.

위치: *siteminder_home*\config

siteminder_home

정책 서버 설치 경로를 지정합니다.

참고: 이 파일의 사용에 대한 자세한 내용은 *정책 서버 설치 안내서*의 "Windows 에 SNMP 에이전트 구성"을 참조하십시오.

SNMP 이벤트 트래핑 구성 파일

SNMP 이벤트 트래핑 구성 파일(snmptrap.conf)은 다음 항목에 대한 설정을 제공합니다.

- SNMP 트랩에 매핑할 시스템 이벤트
- 트랩을 보낼 네트워크 관리 시스템의 주소

위치: *siteminder_home*\config

siteminder_home

정책 서버 설치 경로를 지정합니다.

참고: 이 파일과 관련된 태스크는 *정책 서버 설치 안내서*의 "Windows 에서 SNMP 이벤트 트래핑을 구성하는 방법" 및 "UNIX 시스템에서 SNMP 이벤트 트래핑을 구성하는 방법"을 참조하십시오.

추가 정보:

이벤트 데이터 (페이지 213)
SiteMinder MIB (페이지 205)

정책 서버 레지스트리 키

정책 서버 레지스트리 키는 다음 위치 중 하나에 있습니다.

- (Windows) HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\PolicyServer.
- (UNIX) sm.registry 파일

  이 파일의 기본 위치는 *siteminder_home*/registry 입니다.

  siteminder_home

  정책 서버 설치 경로를 지정합니다.

다음 사항을 고려하십시오.

- 일부 경우 다음 중 하나를 수행해야 할 수 있습니다.
  - 기존 레지스트리 키 수정
  - 레지스트리 키 생성 및 값 할당

  이러한 경우 필요한 단계는 SiteMinder 설명서에 자세히 설명되어 있습니다.
- 다른 모든 경우에는 SiteMinder 설명서에 설명된 대로 관리 UI 또는 정책 서버 관리 콘솔을 사용하여 정책 서버 설정을 수정하는 것이 좋습니다. SiteMinder 지원 담당자로부터 또는 설명서에서 안내를 받은 경우가 아니면 레지스트리 키를 사용하여 정책 서버 설정을 수정하지 마십시오.

부록 A: SiteMinder 및 CA Security Compliance Manager

이 섹션은 다음 항목을 포함하고 있습니다.

SiteMinder 와 CA Security Compliance Manager 의 통합 작동 방식

CA SiteMinder 는 수동으로 CA Security Compliance Manager 에 가져올 수 있는 규정 준수 보고서를 생성하는 명령줄 도구인 smcompliance 를 제공합니다. smcompliance 도구는 기본적으로 다음과 같은 유형의 보고서를 생성합니다.

정책

명령이 실행된 SiteMinder 정책 서버에 저장된 모든 정책을 나열합니다.

사용자 디렉터리

정책 서버와 연결된 정책 저장소의 모든 사용자 디렉터리를 나열합니다.

User Resources(사용자 리소스)

사용자, 해당 사용자 디렉터리 및 모든 관련 정책을 나열합니다.

SiteMinder 규정 준수 데이터를 CA Security Compliance Manager 로 내보내려면 다음 절차를 따르십시오.

1. (선택 사항) 다음을 수행하려는 경우 규정 준수 도구에 대한 구성 파일을 업데이트합니다.
   - 기존 보고서의 보고서 이름 또는 필드 이름 변경
   - 새 보고서 추가
   - 보고서 삭제

2. 정책 서버에서 규정 준수 도구를 실행하여 보고서를 생성합니다.
3. 생성된 보고서를 조직의 CA Security Compliance Manager 관리자에게 보냅니다.

규정 준수 보고서 생성

CA Security Compliance Manager 용 SiteMinder 규정 준수 보고서는 명령줄 도구를 사용하여 생성합니다. 보고서가 생성된 후에는 이를 CA Security Compliance Manager 로 가져올 수 있도록 조직의 CA Security Compliance Manager 관리자에게 보내야 합니다.

규정 준수 보고서를 생성하려면

1. 정책 서버를 호스트하는 컴퓨터에서 명령줄 창을 엽니다.
2. smcompliance 명령을 다음 옵션과 함께 실행합니다.

-dir *directory_name*

생성된 보고서가 저장되는 출력 디렉터리의 전체 경로를 지정합니다. 이 디렉터리가 이미 있을 경우 기존 디렉터리는 백업으로 이름이 바뀝니다.

기본값: *siteminder_home*/compliance/output

-conf *configuration_file*

보고서의 내용과 형식을 결정하는 구성 파일의 전체 경로를 지정합니다. 기본 구성 파일은 CA Security Compliance Manager 에 대한 내용을 포함하지만 자신의 요구에 맞게 구성 파일을 사용자 지정할 수 있습니다.

기본값: *siteminder_home*/compliance/config

-log *log_file*

로그 파일의 전체 경로를 지정합니다.

기본값: *siteminder_home*/compliance/output

-format *format_type*

보고서에 대해 다음 파일 형식 중 하나를 지정합니다.

- CSV(쉼표로 구분된 값) 파일
- XML 파일

기본값: csv

보고서 및 로그 파일이 생성됩니다. 이제 파일을 CA Security Compliance Manager 관리자에게 보낼 수 있습니다.

사용 가능한 규정 준수 보고서 또는 해당 필드 목록 표시

SiteMinder 규정 준수 보고서 도구인 smcompliance 는 기본적으로 생성되는 보고서 외에도 다른 유형의 보고서를 생성할 수 있습니다.

사용 가능한 규정 준수 보고서의 목록을 표시하려면

1. 정책 서버에서 명령 프롬프트를 엽니다.
2. 다음 명령을 입력합니다.

   ```
   smcompliance -help reports
   ```

   보고서 이름 목록이 표시됩니다.
3. (선택 사항) 보고서에 포함된 필드를 보려면 다음 명령을 입력합니다.

   ```
   smcompliance -generate report_name
   ```

   report_name 은 2 단계에서 목록에 표시된 이름과 일치해야 합니다. 예를 들어 agents 보고서에 포함된 필드를 보려면 다음을 입력합니다.

   smcompliance -generate agents

   보고서의 필드 목록이 XML 형식으로 표시됩니다. 구성 파일에 XML 을 추가하여 새 보고서를 생성할 수 있습니다.

새 규정 준수 보고서 추가

smcompliance 도구에서 사용되는 구성 파일에 새 보고서를 추가하여 다른 유형의 규정 준수 보고서를 생성할 수 있습니다.

새 규정 준수 보고서를 추가하려면

1. smcompliance 도구를 사용하여 추가할 보고서의 이름이 사용 가능한 규정 준수 보고서 목록에 표시되는지 확인합니다.
2. 추가할 보고서의 필드를 표시하고 화면의 xml 형식 텍스트를 복사합니다.
3. 정책 서버의 다음 디렉터리로 이동합니다.

   siteminder_home\compliance\config
4. 텍스트 편집기에서 기본 구성 파일인 compliance.conf 를 엽니다.
5. 기본 파일의 복사본을 다른 이름으로 저장합니다.
6. 기존 <report> 섹션을 복사하여 구성 파일 맨 아래의 </reports> 태그 위에 붙여 넣습니다.
7. <columns> 태그 사이의 기존 텍스트를 제거합니다.
8. <columns> 태그 사이에 2 단계에서 복사한 텍스트를 추가합니다.
9. <report> 태그의 name 특성 값을 1 단계에서 확인한 보고서 이름으로 바꿉니다.
10. <table> 태그의 name 특성을 새 보고서를 설명하는 값으로 변경합니다. 이 이름은 생성되는 보고서 파일에 사용됩니다.
11. 변경 내용을 저장하고 새 구성 파일을 닫습니다.

    새 보고서가 추가됩니다.
12. smcompliance 명령을 실행하고 새 구성 파일을 지정합니다.

기존 규정 준수 보고서의 내용 변경

기본 구성 파일에 의해 생성되는 보고서는 CA Security Compliance Manager 에 필요한 일반적인 규정 준수 정보를 제공합니다. 조직에 다른 정보가 필요한 경우 고유한 사용자 지정 구성 파일을 생성하여 원하는 정보가 포함된 보고서를 생성할 수 있습니다.

1. 정책 서버의 다음 디렉터리로 이동합니다.

   siteminder_home\compliance\config

2. 텍스트 편집기에서 기본 구성 파일인 compliance.conf 를 엽니다.
3. 기본 파일의 복사본을 다른 이름으로 저장합니다.
4. 구성 파일의 새 복사본을 다음과 같이 변경합니다.
   - 보고서를 제거하려면 제거할 보고서에 해당하는 <report> 태그와 </report> 태그 사이의 내용을 확인하고 해당 섹션과 태그를 삭제합니다.
   - 보고서의 이름을 변경하려면 <table> 태그의 name 특성 값을 수정합니다.
   - 보고서의 필드에 포함된 정보가 *아니라* 필드 이름을 변경하려면 <column> 태그의 name 특성 값을 수정합니다.
   - 추가할 열을 구성 파일의 <comment> 섹션에서 <columns> 섹션으로 이동합니다.

부록 B: 일반적인 SiteMinder 문제 해결

LDAP 검색 시간 만료 문제 해결

증상:

smps.log 에 LDAP 서버가 검색 결과를 반환하기 전에 시간이 만료되었다고 표시됩니다. 시간 만료 간격을 늘리려면 어떻게 해야 합니까?

해결책:

다음 레지스트리 설정 (페이지 42)의 값을 변경하십시오.

SearchTimeout

관리 UI 가 응답하지 않음

증상:

독립 실행형 관리 UI 설치(JBoss 응용 프로그램 서버 포함)에서 관리 UI 가 응답하지 않습니다. 즉, 관리 UI 가 시작되지 않거나 일정 기간 동안 정상 작업 후 로그인이 되지 않습니다.

해결책:

1. 관리 UI 응용 프로그램 서버를 중지합니다.
2. 응용 프로그램 서버가 중지되는 경우 다음 위치에 있는 data 디렉터리의 이름을 변경하거나 삭제합니다.

   \adminui\server\default

3. 응용 프로그램 서버를 다시 시작합니다.
4. 정책 서버에서 다음 명령을 실행합니다.

   XPSRegClient *client_name*[:*passphrase*] -adminui -t *timeout* -r *retries* -c *comment*
   -cp -l *log_path* -e *error_path*
   -vT -vI -vW -vE -vF

   참고: *client_name* 과 [:*passphrase*] 사이에 공백을 삽입하면 오류가 발생합니다.

client_name

등록할 관리 UI 를 식별합니다.

제한: 이 값은 고유해야 합니다. 예를 들어 이전에 smui1 을 사용하여 관리 UI 를 등록했으면 smui2 를 입력합니다.

참고: 이 값을 기록해 두십시오. 이 값은 관리 UI 에서 등록 프로세스를 완료하는 데 필요합니다.

passphrase

관리 UI 등록을 완료하는 데 필요한 암호를 지정합니다.

제한:

- 암호에 6 자 이상을 포함해야 합니다.
- 암호에 앰퍼샌드(&)나 별표(*)는 포함할 수 없습니다.
- 암호에 공백이 포함되어 있는 경우 암호를 따옴표로 묶어야 합니다.
- 업그레이드의 일부로 관리 UI 를 등록하는 경우 이전 암호를 다시 사용할 수 있습니다.

참고: 이 단계에서 암호를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고 확인하라는 메시지가 표시됩니다.

중요! 나중에 참조할 수 있도록 암호를 기록해 두십시오.

-adminui

관리 UI 를 등록하도록 지정합니다.

-t *timeout*

(선택 사항) 관리 UI 에서 등록 프로세스를 완료해야 하는 시간을 지정합니다. 이 시간 만료 값에 도달할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 1

최대 제한: 1440(1 일)

-r *retries*

(선택 사항) 관리 UI 에서 등록 프로세스를 완료할 때 허용되는 시도 실패 횟수를 지정합니다. 등록 프로세스 중 정책 서버에 제출한 클라이언트 이름이나 암호가 올바르지 않으면 등록 시도가 실패할 수 있습니다.

기본값: 1

최대 제한: 5

-c *comment*

(선택 사항) 정보 제공을 위해 등록 로그 파일에 지정된 설명을 삽입합니다.

참고: 설명을 따옴표로 묶으십시오.

-cp

(선택 사항) 등록 로그 파일에 여러 줄로 된 설명을 포함할 수 있도록 지정합니다. 그러면 등록 도구에서 여러 줄로 된 설명에 대한 메시지가 표시되고 정보 제공을 위해 등록 로그 파일에 지정된 설명이 삽입됩니다.

참고: 설명을 따옴표로 묶으십시오.

-l *log_path*

(선택 사항) 등록 로그 파일을 내보낼 위치를 지정합니다.

기본값: *siteminder_home*\log

siteminder_home

정책 서버 설치 경로를 지정합니다.

-e *error_path*

(선택 사항) 예외를 지정된 경로로 보냅니다.

기본값: stderr

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(경고)으로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(경고)으로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(경고)으로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(경고)으로 설정합니다.

등록 로그 파일의 이름이 표시되고 암호를 묻는 메시지가 표시됩니다.

5. Enter 키를 누릅니다.

   클라이언트 이름 및 암호 쌍이 생성됩니다.

6. 정책 서버에 관리 UI 를 등록하려면 관리 UI 호스트에서 다음 단계 중 하나를 완료합니다.

   - Windows:
     - (권장) 관리 UI 바로 가기를 사용하여 관리 UI 를 엽니다. 바로 가기를 사용하면 관리 UI 가 SSL 을 통해 등록됩니다. 바로 가기에 대한 액세스 권한이 없을 경우 웹 브라우저를 열고 다음 위치로 이동하십시오.

       https://*host*:8443/iam/siteminder/adminui

       참고: 10 년 동안 유효한 자체 서명 인증서가 생성되고 연결에 사용됩니다. 인증서는 RSA 2048 키 강도를 사용하여 생성됩니다.
     - 웹 브라우저를 열고 다음 위치로 이동합니다.

       http://host:8080/iam/siteminder/adminui
   - UNIX:
     - (권장) 웹 브라우저를 열고 다음 위치로 이동하여 SSL 을 통해 관리 UI 를 등록합니다.

       https://host:8443/iam/siteminder/adminui
     - 브라우저를 열고 다음 위치로 이동합니다.

       http://*host*:8080/iam/siteminder/adminui

       참고: 호스트 시스템에 웹 브라우저가 없을 경우 원격으로 로그인 화면에 액세스할 수 있습니다.

   host

   정규화된 관리 UI 호스트 시스템 이름을 지정합니다.

   SiteMinder 관리 UI 로그인 화면이 표시됩니다.

7. "사용자 이름" 필드에 다음 값을 입력합니다.

   `siteminder`

8. "암호" 필드에 SiteMinder 슈퍼 사용자 계정 암호를 입력합니다.

MySQL 세션 저장소 시간 만료 오류 해결

증상:

MySQL 데이터베이스를 세션 저장소로 구성하는 경우 다음과 같은 시간 만료 메시지가 정책 서버 로그에 주기적으로 나타납니다.

```
[ERROR][sm-Server-07011] failed.Exception : State = HYT00 Internal
Code = 0 - [DataDirect][ODBC MySQL Wire Protocol driver]Timeout
expired.. Error code -4007
```

해결책:

다음 레지스트리 위치에서 MaintenanceQueryTimeout 레지스트리 키 값을 수정하여 세션 서버 유지 관리 쿼리 시간 만료를 늘리십시오.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Se
ssionServer
```

다음 값을 사용하는 것이 좋습니다.

```
MaintenanceQueryTimeout=0x12c
```

LDAP 관리 제한 초과 오류와 함께 정책 서버가 종료됨

증상:

정책 저장소/키 저장소에 대한 LDAP 검색이 다음 오류와 함께 실패할 경우 정책 서버가 정상 종료됩니다.

```
LDAP_ADMINLIMIT_EXCEEDED(오류 코드 11)
```

해결책:

다음의 선택적 레지스트리 키가 사용되도록 설정하십시오.

```
EnableRetryOnAdminLimitExceededFailure
```

그러면 정책 서버가 포기하기 전에 검색을 한 번 더 시도할 수 있습니다.

값: 0(사용 안 함) 또는 1(사용)

기본값: 0

Windows

다음 단계를 수행하십시오.

1. Windows "시작" 메뉴에서 "실행"을 선택합니다.
2. "실행" 대화 상자에 regedit 를 입력하고 "확인"을 클릭합니다.
3. 레지스트리 편집기에서 다음 위치로 이동합니다.

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netegrity\SiteMinder\CurrentVersion\ObjectStore
   ```

4. 다음 레지스트리 키의 값을 수정합니다.

   ```
   EnableRetryOnAdminLimitExceededFailure
   ```

5. 정책 서버를 다시 시작합니다.

UNIX

다음 단계를 수행하십시오.

1. 다음 위치로 이동합니다.

   install_directory/siteminder/registry

2. 텍스트 편집기에서 sm.registry 를 엽니다.
3. 파일에서 다음 텍스트를 찾습니다.

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\ObjectStore
   ```

4. 다음 레지스트리 키의 값을 수정합니다.

   ```
   EnableRetryOnAdminLimitExceededFailure
   ```

5. 정책 서버를 다시 시작합니다.

명령줄에서 정책 서버 문제 해결

별도의 창에서 디버깅 옵션을 설정한 상태로 정책 서버 프로세스를 대화형으로 실행하여 문제를 해결할 수 있습니다. 다음의 서버 감독 기능을 명령줄에서 실행할 수 있습니다.

install_dir/siteminder/bin/smpolicysrv

참고: Windows 시스템의 경우 원격 데스크톱 또는 터미널 서비스 창에서 smpolicysrv 명령을 실행하지 *마십시오*. smpolicysrv 명령을 실행하려면 프로세스 간 통신이 필요하며 smpolicysrv 프로세스를 원격 데스크톱 또는 터미널 서비스 창에서 실행할 경우에는 프로세스 간 통신이 작동하지 않습니다.

smpolicysrv 명령에는 다음 옵션을 사용합니다.

-t*port_number*

이 옵션은 서버가 에이전트 연결에 대해 바인딩하는 TCP 포트를 수정하는 데 사용됩니다. 이 스위치를 사용하지 않으면 서버는 기본적으로 정책 서버 관리 콘솔을 통해 지정된 TCP 포트를 사용합니다.

-u*port_number*

이 옵션은 서버가 RADIUS 연결에 대해 바인딩하는 UDP 포트를 수정하는 데 사용됩니다. 이 스위치를 사용하지 않으면 서버는 기본적으로 정책 서버 관리 콘솔을 통해 지정된 UDP 포트를 사용합니다. 이 스위치는 인증 및 계정 서버에만 적용됩니다.

-stop

이 스위치는 가능한 한 가장 정상적인 방법으로 서버를 중지합니다. 이 방법을 사용하면 모든 데이터베이스 및 네트워크 연결이 제대로 닫힙니다.

-abort

이 스위치는 데이터베이스 및 네트워크 연결을 먼저 닫는 과정 없이 서버를 즉시 중지합니다.

-stats

이 스위치는 스레드 풀 제한, 스레드 풀 메시지 및 연결 수와 같은 현재 서버 런타임 통계를 생성합니다.

-resetstats

이 스위치는 정책 서버를 다시 시작하지 않고 현재 서버 런타임 통계를 재설정합니다. 이 스위치는 다음 카운터를 재설정합니다.

- "Max Threads"(최대 스레드 수)가 "Current Threads"(현재 스레드 수) 값으로 재설정됩니다.
- "Max Depth of the message queue"(메시지 큐의 최대 깊이)가 "Current Depth of the message queue"(메시지 큐의 현재 깊이)로 재설정됩니다.
- "최대 연결 수"가 "현재 연결 수"로 재설정됩니다.
- "Msgs"(메시지), "Waits"(대기), "Misses"(누락) 및 "Exceeded"(초과) 제한이 0 으로 재설정됩니다.

이 스위치는 다음 카운터는 재설정하지 않습니다.

- Thread pool limit(스레드 풀 제한)
- Current Threads(현재 스레드 수)
- Current Depth of the message queue(메시지 큐의 현재 깊이)
- Current Connections(현재 연결 수)
- 연결 수 제한

-publish

정책 서버에 대한 정보를 게시합니다.

-tadm*port_number*

관리 서비스용 TCP 포트를 설정합니다.

-uac*port_number*

Radius 계정용 UDP 포트를 설정합니다.

-uadm*port_number*

관리 서비스용 UDP 포트를 설정합니다.

-uauth*port_number*

Radius 인증용 UDP 포트를 설정합니다.

-ac

에이전트 API 요청을 처리하도록 설정합니다.

-noac

에이전트 API 요청을 처리하지 않도록 설정합니다.

-adm

관리 요청을 처리하도록 설정합니다.

-noadm

관리 요청을 처리하지 않도록 설정합니다.

-radius

RADIUS 요청을 처리하도록 설정합니다.

-noradius

RADIUS 요청을 처리하지 않도록 설정합니다.

-onlyadm

다음 옵션을 단일 옵션으로 결합합니다.

- -adm
- -noac
- -noradius

-starttrace

이 명령은 다음을 수행합니다.

- 추적 파일에 대한 로깅을 시작하며 콘솔에 대한 추적 로깅에는 영향을 주지 않습니다.
- 정책 서버가 실행 중이 아니면 오류를 발생시킵니다.

정책 서버가 이미 추적 데이터를 로깅 중인 경우 -starttrace 명령을 실행하면 정책 서버에 다음과 같은 영향이 있습니다.

- 현재 추적 파일의 이름이 타임스탬프가 추가된 *file_name*.YYYYMMDD_HHmmss.*extension* 형식의 이름으로 변경됩니다.
- 원래 이름으로 새 추적 파일이 생성됩니다.

  예를 들어 정책 서버 관리 콘솔의 "프로파일러" 탭에 있는 추적 파일 이름이 C:\temp\smtrace.log 인 경우 새 파일이 생성되고 이전 파일은 c:\temp\smtrace.20051007_121807.log 로 저장됩니다. 타임스탬프는 정책 서버가 이 파일을 2005 년 10 월 7 일 오후 12:18 에 생성했음을 나타냅니다. 정책 서버 관리 콘솔의 "프로파일러" 탭을 사용하여 파일 추적 기능이 사용되도록 설정하지 않은 경우에는 이 명령을 실행해도 아무런 효과가 없습니다.

-stoptrace

이 명령은 다음을 수행합니다.

- 파일에 대한 로깅을 중지하며 콘솔에 대한 추적 로깅에는 영향을 주지 않습니다.
- 정책 서버가 실행 중이 아니면 오류를 발생시킵니다.

정책 서버 메시지 큐가 가득 찬 경우 두 개의 smpolicysrv 명령줄 옵션 -dumprequests 및 -flushrequests 를 사용하여 신속하게 문제를 해결하고 복구할 수 있습니다. 이러한 옵션은 다음과 같은 경우에만 사용하십시오.

1. 정책 서버 메시지 큐에서 대기 중인 에이전트 요청이 시간 만료된 경우
2. 하나 이상의 에이전트가 시간 만료된 요청을 다시 보내 메시지 큐가 넘치는 경우

중요: 정상적으로 작동하는 경우에는 -dumprequests 와 -flushrequests 를 사용하지 마십시오.

-dumprequests

정책 서버 메시지 큐의 각 요청에 대한 요약을 감사 로그에 출력합니다.

-flushrequests

전체 정책 서버 메시지 큐를 플러시하므로 요청이 유지되지 않습니다.

동적으로 디버깅 시작 또는 중지

정책 서버를 다시 시작하지 *않고도* 언제든지 특정 구성 요소의 디버깅 기능을 시작하거나 중지할 수 있습니다.

참고: 이 기능은 CA Technologies 기술 지원 담당자가 안내한 경우에만 사용하는 것이 좋습니다.

다음 단계를 수행하십시오.

1. 정책 서버를 호스트하는 컴퓨터에서 명령 창을 엽니다.
2. 다음 명령을 입력합니다.

   ```
   SmCommand -i SiteMinder
   ```

   옵션 목록이 나타납니다.
3. CA 지원 담당자가 제공하는 지침에 따라 다음 디버깅 옵션 중 하나를 선택합니다.

   CA.EPM::EPMObjects_Debug

   SiteMinder EPM 구성 요소의 디버깅 상태를 전환합니다.

   CA.XPS::Debug

   SiteMinder XPS 구성 요소의 디버깅 상태를 전환합니다.

   CA.XPS::XPSEval_Debug

   SiteMinder XPSEvaluate 구성 요소의 디버깅 상태를 전환합니다.

동적으로 추적 시작 또는 중지

정책 서버를 다시 시작하지 *않고도* 언제든지 특정 구성 요소의 추적 기능을 시작하거나 중지할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버를 호스트하는 컴퓨터에서 명령 창을 엽니다.
2. 다음 명령을 입력합니다.

   ```
   SmCommand -i SiteMinder
   ```

3. 옵션 목록이 나타납니다. 추적 옵션은 현재 상태의 *반대 상태*를 표시합니다. 예를 들어 CA XPS 에 대한 추적이 현재 사용되지 않도록 설정되어 있는 경우 다음과 같이 사용되도록 설정하기 위한 옵션이 표시됩니다.

   ```
   item_number - CA.XPS::TraceOn
   ```

4. 다음 옵션 중 원하는 옵션 번호를 입력하여 선택합니다.

   CA.EPM::EPMObjects_Trace*State*

   EPM 개체 구성 요소에 대한 추적을 설정/해제합니다.

   CA.XPS::Trace*State*

   XPS 구성 요소에 대한 추적을 설정/해제합니다.

   CA.XPS::XPSEval_Trace*State*

   XPS 식 계산기 구성 요소에 대한 추적을 설정/해제합니다.

   확인 메시지가 표시됩니다. 옵션 목록이 변경 내용과 함께 다시 표시됩니다.

5. (선택 사항) 4 단계를 반복하여 다른 구성 요소의 추적을 시작하거나 중지합니다.
6. Q 를 입력하여 종료합니다.

   추적이 동적으로 변경되었습니다.

웹 에이전트 통신 오류 후 정책 서버가 중단됨

증상:

정책 서버 요청 중에 네트워크 중단 등의 이유로 웹 에이전트가 오프라인 상태가 되고 정책 서버에 통신 장애를 알리지 않을 경우 정책 서버는 웹 에이전트 데이터를 받기 위해 계속 대기합니다. 정책 서버는 웹 에이전트에서 네트워크가 다시 작동하고 정책 서버와의 연결을 종료한 후에도 계속 대기합니다.

하나 이상의 웹 에이전트에서 많은 요청이 이러한 방식으로 손실되는 경우 요청을 처리하는 작업자 스레드가 해제되지 않기 때문에 정책 서버가 응답을 중지하게 될 수 있습니다.

해결책:

SiteMinder 의 TCP 연결 유지 사용(SM_ENABLE_TCP_KEEPALIVE) 환경 변수를 생성하고 활성화하여 정책 서버가 KeepAlive 패킷을 유휴 웹 에이전트 연결에 보내도록 구성합니다. 정책 서버가 패킷을 보내는 간격은 OS 별 TCP/IP 매개 변수에 의해 결정됩니다.

이 변수는 웹 에이전트, 응용 프로그램 서버 에이전트(ASA), 관리 UI, SDK 로 만든 사용자 지정 에이전트에 대한 위치에서 설정할 수도 있습니다.

매개 변수를 구성할 때는 다음 사항을 고려하십시오.

- 정책 서버가 패킷을 보내기 시작해야 할 시기
- 정책 서버가 패킷을 보내는 간격
- 웹 에이전트 연결이 끊어졌다고 결정하기 전까지 정책 서버가 패킷을 보내는 횟수

  참고: TCP/IP 매개 변수 구성에 대한 자세한 내용은 OS 별 설명서를 참조하십시오.

정책 서버가 KeepAlive 패킷을 유휴 웹 에이전트 연결에 보내도록 구성하려면

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 작업 중 하나를 수행하십시오.
   - (Windows) 다음 시스템 환경 변수 값을 1 로 지정하여 생성합니다.

     SM_ENABLE_TCP_KEEPALIVE

- (UNIX)
  a. 다음 시스템 환경 변수를 생성합니다.

     SM_ENABLE_TCP_KEEPALIVE=1

  b. 환경 변수를 내보냅니다.

참고: 값은 0(해제) 또는 1(설정)이어야 합니다. 0 또는 1 이 아닌 값을 구성하면 환경 변수가 비활성화됩니다. 환경 변수가 비활성화되면 정책 서버가 KeepAlive 패킷을 유휴 웹 에이전트 연결에 보내지 않습니다.

설치된 JDK 버전 확인

정책 서버가 시작되지 않는 경우 올바른 버전의 JDK 가 설치되어 있는지 확인하십시오.

정책 서버 로그의 로컬 시간 설정 재정의

정책 서버 로그 파일 *install_dir*/siteminder/log/smps.log 에는 정책 서버가 설치된 컴퓨터의 운영 체제에 지정된 현지 표준 시간대의 시간이 표시됩니다.

이 로그 파일의 시간을 GMT 시간으로 표시하려면

1. 다음 레지스트리 설정을 찾습니다.

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\LogConfig\LogLocalTime

2. 값을 1(기본값)에서 0 으로 변경합니다.

시스템 응용 프로그램 로그 검토

정책 서버가 시작되지 않을 경우 이벤트 로그(Windows) 또는 syslog(UNIX)에서 정책 서버에 대한 정보를 검토하십시오.

- Windows 의 경우 이벤트 뷰어를 사용하여 이벤트 로그를 확인합니다. 이벤트 뷰어의 "로그" 메뉴에서 "응용 프로그램"을 선택합니다.
- UNIX 의 경우 텍스트 편집기를 사용하여 syslog 를 확인합니다.

LDAP SDK 계층에서 처리되는 LDAP 조회

SiteMinder 의 LDAP 조회 처리 기능이 개선되어 성능 및 중복성이 향상되었습니다. 이전 버전의 SiteMinder 에서는 LDAP SDK 계층을 통해 자동 LDAP 조회 처리 기능이 지원되었습니다. LDAP 조회가 발생하면 LDAP SDK 계층에서 정책 서버와의 상호 작용 없이 조회 대상 서버에 대한 요청 실행이 처리되었습니다.

이제 SiteMinder 에는 향상된 비자동 LDAP 조회 처리에 대한 지원이 포함되어 있습니다. 비자동 조회 처리 기능을 사용하면 LDAP 조회가 LDAP SDK 계층 대신 정책 서버로 반환됩니다. 조회에는 해당 조회를 처리하는 데 필요한 모든 정보가 포함됩니다. 정책 서버는 조회에 지정된 LDAP 디렉터리가 작동하는지 여부를 확인하며, 적절한 LDAP 디렉터리가 작동하지 않는 경우 요청을 종료할 수 있습니다. 이 기능은 오프라인 시스템에 대한 LDAP 조회로 인해 요청 대기 시간이 계속해서 증가할 경우 발생하는 성능 문제를 해결합니다. 이와 같이 대기 시간이 증가하면 SiteMinder 가 요청으로 포화 상태가 됩니다.

LDAP 조회가 사용되지 않도록 설정

LDAP 조회로 인해 오류가 발생할 경우 모든 LDAP 조회가 사용되지 않도록 설정할 수 있습니다. LDAP 조회가 사용되지 않도록 설정하면 디렉터리 조회 시 오류가 반환됩니다.

Windows 에서 정책 서버에 대한 LDAP 조회 처리가 사용되지 않도록 설정하려면

1. Windows "시작" 메뉴에서 "실행"을 선택합니다.
2. "실행" 대화 상자에 regedit 를 입력하고 "확인"을 클릭합니다.
3. 레지스트리 편집기에서 다음 위치로 이동합니다.

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\
   CurrentVersion\Ds\LDAPProvider
   ```

4. 다음 레지스트리 값을 수정합니다.

   참고: 이 값은 16 진수 표기법으로 표시됩니다.

   ```
   "EnableReferrals"=dword:00000001
   ```

   이 레지스트리 값은 정책 서버에서 LDAP 조회를 처리할지 여부를 결정합니다. 0 으로 설정된 경우 정책 서버에서 LDAP 조회가 허용되지 않습니다. 1 로 설정된 경우 정책 서버에서 LDAP 조회가 허용됩니다.

   LDAP 조회는 기본적으로 사용되도록 설정되어 있습니다. 이 설정은 레지스트리를 편집해야만 수정할 수 있습니다.

5. 정책 서버를 다시 시작합니다.

Solaris 에서 정책 서버의 LDAP 조회 처리가 사용되지 않도록 설정하려면

1. 다음 위치로 이동합니다.

   install_dir/siteminder/registry

2. 텍스트 편집기에서 sm.registry 를 엽니다.
3. 파일에서 다음 텍스트를 찾습니다.

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\
   CurrentVersion\Ds\LDAPProvider
   ```

4. 3 단계에서 찾은 행 뒤에서 다음으로 시작하는 행을 찾습니다.

   ```
   EnableReferrals
   ```

5. 세미콜론 바로 앞의 값을 다음과 같이 수정합니다.

   참고: 이 값은 16 진수 표기법으로 변환해야 합니다.

   이 레지스트리 값은 정책 서버에서 LDAP 조회를 처리할지 여부를 결정합니다. 0 으로 설정된 경우 정책 서버에서 LDAP 조회가 허용되지 않습니다. 1 로 설정된 경우 정책 서버에서 LDAP 조회가 허용됩니다.

6. 정책 서버를 다시 시작합니다.

바인딩 작업 시 LDAP 조회 처리

Windows 에서 정책 서버에 대한 바인딩 작업 시 LDAP 조회를 구성하려면

1. Windows "시작" 메뉴에서 "실행"을 선택합니다.
2. "실행" 대화 상자에 regedit 를 입력하고 "확인"을 클릭합니다.

3. 레지스트리 편집기에서 다음 위치로 이동합니다.

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider

4. 다음 레지스트리 값을 수정합니다.

   참고: 이 값은 16 진수 표기법으로 표시됩니다.

   "ChaseReferralsOnBind"=dword:00000001

   이 레지스트리 값은 바인딩 작업 시 LDAP 조회를 추적해야 하는지 여부를 결정합니다. 대부분의 LDAP 디렉터리 서버는 바인딩 시 LDAP 조회를 처리합니다. 디렉터리 서버가 바인딩 시 조회를 처리하는 경우 ChaseReferralsOnBind 는 아무런 효과가 없습니다. 그러나 디렉터리가 바인딩 시 조회를 처리하지 않는 경우 이 설정을 사용하면 정책 서버가 바인딩 조회를 처리할 수 있게 됩니다.

   서버가 바인딩 작업 시 조회를 처리하는 경우 이 설정을 0 으로 변경하여 정책 서버의 바인딩 조회 처리 기능이 사용되지 않도록 설정할 수 있습니다.

   바인딩 시 조회 추적은 기본적으로 사용되도록 설정되어 있습니다. 이 설정은 레지스트리를 편집해야만 수정할 수 있습니다.

5. 정책 서버를 다시 시작합니다.

Solaris 에서 정책 서버에 대한 바인딩 작업 시 LDAP 조회를 구성하려면

1. 다음 위치로 이동합니다.

   install_dir/siteminder/registry

2. 텍스트 편집기에서 sm.registry 를 엽니다.

3. 파일에서 다음 텍스트를 찾습니다.

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider

4. 3 단계에서 찾은 행 뒤에서 다음으로 시작하는 행을 찾습니다.

   ChaseReferralsOnBind

5. 세미콜론 바로 앞의 값을 다음과 같이 수정합니다.

   참고: 이 값은 16 진수 표기법으로 변환해야 합니다.

   이 레지스트리 값은 바인딩 작업 시 LDAP 조회를 추적해야 하는지 여부를 결정합니다. 대부분의 LDAP 디렉터리 서버는 바인딩 시 LDAP 조회를 처리합니다. 디렉터리 서버가 바인딩 시 조회를 처리하는 경우 ChaseReferralsOnBind 는 아무런 효과가 없습니다. 그러나 디렉터리가 바인딩 시 조회를 처리하지 않는 경우 이 설정을 사용하면 정책 서버가 바인딩 조회를 처리할 수 있게 됩니다.

   서버가 바인딩 작업 시 조회를 처리하는 경우 이 설정을 0 으로 변경하여 정책 서버의 바인딩 조회 처리 기능이 사용되지 않도록 설정할 수 있습니다.

6. 정책 서버를 다시 시작합니다.

유휴 시간 만료 및 상태 저장 검사 장치

방화벽과 같은 상태 저장 검사 장치에는 대개 유휴 시간 만료 설정이 있습니다. SiteMinder 에서 정책 서버가 에이전트에 연결할 때도 유휴 시간 만료 설정이 적용됩니다.

정책 서버는 서비스를 정기적으로 폴링합니다. 폴링 간격은 최대 5 분입니다. 즉, 유휴 연결은 구성된 값으로부터 5 분 이내에 시간 만료됩니다. 예를 들어 만료 시간 값으로 55 분이 지정된 경우 연결은 55 분에서 60 분 사이에 연결이 시간 만료됩니다.

기본적으로 정책 서버와 웹 에이전트 간에 생성된 연결은 비활성 상태가 된 지 10 분 후에 만료됩니다. 정책 서버와 웹 에이전트 사이에 방화벽이나 다른 상태 저장 네트워크 장치가 있는 경우 연결이 장치의 유휴 만료 시간보다 오래 유휴 상태이면 해당 장치는 정책 서버나 웹 에이전트에 알리지 않고 연결을 종료합니다.

웹 에이전트가 네트워크 장치에 의해 종료된 연결을 사용하려고 하면 네트워크 오류가 발생하고 연결이 재설정되며 브라우저에 500 오류(20-0003)가 보고됩니다. 또한 에이전트는 연결 풀에서 오류가 발생한 연결과 사용 기간이 동일하거나 보다 오래된 다른 모든 연결을 닫습니다. 그러나 정책 서버 측에는 이러한 연결에 대한 소켓이 설정된 상태로 유지됩니다. 사이트의 부하 패턴에 따라서는 정책 서버의 정상적인 작동에 방해가 될 정도로 연결이 증가할 수도 있습니다.

방화벽이나 다른 상태 저장 네트워크 장치가 정책 서버와 웹 에이전트 간의 연결을 종료하지 못하도록 하려면 정책 서버에 대한 유휴 만료 시간을 구성해야 합니다. 정책 서버는 TCP/IP 연결을 닫을 때 지정된 비활성 기간 동안 기다린 다음 RESET 을 보내 연결의 서버 측과 클라이언트 측을 완전히 닫습니다. 비활성 기간은 정책 서버 관리 콘솔의 "설정" 탭에 있는 "유휴 시간 만료(분)" 필드에서 지정합니다.

참고: "유휴 시간 만료(분)" 필드를 사용하여 관리자가 연결할 수 있는 시간을 제한할 수도 있습니다.

설치 시 "유휴 시간 만료" 값은 10 분으로 설정됩니다. 상태 저장 네트워크 장치에 적용하려면 이 값을 웹 에이전트와 정책 서버 사이에 있는 장치의 TCP/IP 유휴 만료 시간보다 짧은 시간으로 설정하십시오. 정책 서버의 시간 만료가 먼저 발생하도록 하려면 TCP 유휴 세션 만료 시간을 상태 저장 장치에 대한 유휴 만료 시간의 60%로 설정하는 것이 좋습니다.

오류 - 선택적 기능이 구현되지 않음

정책 서버가 ODBC 데이터 원본을 사용하려고 할 때 데이터베이스에 연결할 수 없으면 다음과 같은 오류 메시지가 나타날 수 있습니다.

`Optional feature not implemented. Error code -1 (선택적 기능이 구현되지 않았습니다. 오류 코드 -1)`

이 메시지는 구성 요소가 일치하지 않거나, 구성이 잘못되었거나, 자격 증명이 잘못되었음을 나타내기도 합니다.

참고: CA 의 Intersolv 또는 Merant 드라이버 구성은 기본 구성과 다릅니다.

위의 메시지를 나타나는 경우 ODBC 데이터 원본을 정책 저장소로 사용하거나 로깅용으로 사용하려면 *정책 서버 설치 안내서*에서 ODBC 데이터 원본 구성에 대해 설명하는 단원을 참조하십시오.

관리자 작업을 로깅할 때의 오류 또는 성능 문제

정책 서버 관리 콘솔의 "감사" 탭에서 "관리자가 다음으로 변경: 정책 저장소 개체"를 "모든 이벤트 로깅"으로 설정하고 ODBC 데이터 원본에 로깅할 경우 다음과 같은 문제 중 하나가 발생할 수 있습니다.

- 관리 UI 에서 개체를 저장할 때 오래 지연됨
- 다음 오류 메시지가 나타남

  `Exception occurred while executing audit log insert.` (감사 로그 삽입을 실행하는 중 예외가 발생했습니다.)

이러한 경우 중 하나가 발생할 경우 대신 텍스트 파일에 로깅하십시오.

정책 서버 공유 정책 저장소가 일관되게 업데이트되지 않음

증상:

여러 정책 서버에서 단일 정책 저장소를 공유할 경우 정책 저장소 내의 데이터가 동기화되지 않을 수 있습니다. 동기화 문제는 다음과 같은 경우에 발생할 수 있습니다.

- 정책 서버의 시스템 시간이 서로 다른 경우
- 네트워크 지연이 발생한 경우

예를 들어 정책 서버 A 의 시스템 시간은 10:00 이고 정책 서버 B 의 시스템 시간은 10:05 라고 가정합니다. 정책 서버 A 는 10:00 에 해당 데이터를 정책 저장소에 보냅니다. 정책 서버 B 는 타임스탬프가 10:05 *이전*으로 지정된 데이터의 모든 변경 내용을 기록하지 *않습니다*. 이는 해당 이벤트가 그 전에 발생한 것으로 나타나기 때문입니다.

해결책:

시스템 시간이 다른 문제나 네트워크 지연 문제를 해결하려면

1. 다음 DWORD 레지스트리 설정을 생성합니다.

   `SiteMinder\CurrentVersion\ObjectStore`
   `키: ServerCommandTimeDelay`

2. 이 키 값을 시간차에 해당하는 초 수로 설정합니다. 예를 들어 시간차가 5 분인 경우 키 값을 300 으로 설정합니다.

캐시 실패 시간 만료

다음 개체를 삭제한 후 정책 서버가 이벤트를 처리하지 못하는 경우가 있습니다.

- 정책
- 규칙
- 영역
- 정책 도메인

캐시 실패 시간 만료 기능이 이 문제를 처리합니다.

보조 캐시를 생성하지 못한 경우 시간 만료 기간이 지나면 정책 서버가 중단됩니다. 다음 레지스트리 키를 사용하여 시간 만료 기간을 지정하십시오.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\ObjectStore\CacheFailureTimeout
```

이 키의 값은 초 단위입니다. 기본값은 시간 만료가 없음을 나타내는 0 입니다.

정책 서버가 종료된 후 smexec 는 다음 프로세스 이벤트 요청을 즉시 가져옵니다.

키 롤오버 로그 메시지

정책 서버가 웹 에이전트에 대해 키 롤오버 명령을 실행할 때 웹 에이전트가 명령을 성공적으로 처리하는 경우도 있고 명령이 실패하는 경우도 있습니다. 명령이 실패할 경우 문제를 쉽게 해결하기 위해 정책 서버는 SMPS.log 에 다음 세 가지 유형의 메시지를 로깅합니다.

[INFO] ([정보] 키 롤오버 요청이 수 Key Rollover Request has been initiated manually 동으로 시작됨)

이 메시지는 관리자가 수동으로 키 롤오버를 시작할 때 로깅됩니다.

[INFO] Key Rollover Request has been initiated automatically by Policy Server([정보] 키 롤오버 요청이 정책 서버에 의해 자동으로 시작됨)

이 메시지는 정책 서버가 자동으로 키 롤오버를 시작할 때 로깅됩니다.

[INFO] Key distribution has been initiated by Policy Server([정보] 키 배포가 정책 서버에 의해 시작됨)

이 메시지는 키 롤오버 요청이 자동 또는 수동으로 시작된 경우에 로깅됩니다.

캐시 업데이트 로그 메시지

관리 UI 나 명령줄 인터페이스를 통해 캐시 플러시 또는 업데이트가 사용되거나 사용되지 않도록 설정할 수 있습니다. 문제를 쉽게 해결하기 위해 정책 서버는 SMPS.log 에 다음 두 가지 유형의 메시지를 로깅합니다.

[INFO] Server 'enablecacheupdates' command received([정보] 서버 'enablecacheupdates' 명령이 수신됨)

이 메시지는 관리 UI 또는 명령줄 인터페이스를 통해 캐시 플러시가 사용되도록 설정된 경우에 로깅됩니다.

[INFO] Server 'disablecacheupdates' command received([정보] 서버 'disablecacheupdates' 명령이 수신됨)

이 메시지는 관리 UI 또는 명령줄 인터페이스를 통해 캐시 플러시가 사용되지 않도록 설정된 경우에 로깅됩니다.

정책 서버 관리 콘솔을 열 때 이벤트 처리기 목록 설정에 대한 경고가 발생함

증상:

SiteMinder 12.52 SP1 로 업그레이드한 후 처음으로 정책 서버 관리 콘솔에 로그인할 때 이벤트 처리기 목록을 XPSAudit 로 설정해야 한다는 경고 메시지가 표시됩니다.

해결책:

SiteMinder 12.52 SP1 에서는 더 이상 정책 서버 관리 콘솔을 사용하여 사용자 지정 이벤트 처리기 라이브러리를 추가할 수 없습니다. 사용자 지정 이벤트 처리기 라이브러리를 추가하려면 XPSConfig 명령줄 도구를 사용하십시오.

추가 정보:

이벤트 처리기 라이브러리 추가 (페이지 144)

SiteMinder 정책 서버 시작 이벤트 로그

증상:

정책 서버가 시작 도중 작동 중단됩니다. 정책 서버가 작동 중단되기 전에는 SiteMinder 시작 이벤트가 발생합니다.

해결책:

시작 시 정책 서버가 작동 중단될 경우 시작 이벤트 로그가 다음 파일에 저장됩니다.

policy_server_home/audit/SmStartupEvents.audit

일부 LDAP 사용자 디렉터리에서 VLV 인덱싱으로 인해 SiteMinder 에이전트 그룹 조회가 실패함(174279)

증상:

일부 LDAP 사용자 디렉터리에서 VLV(Virtual List View) 구현의 결함으로 인해 SiteMinder 에이전트 그룹 조회가 실패하고, 그 결과로 항목이 반환되지 않고 “directory unwilling to perform"(디렉터리가 수행되지 않음) 오류가 발생합니다.

해결책:

위에서 설명한 대로 SiteMinder 에이전트 그룹 조회가 실패하는 경우 정책 서버에서 VLV 조회를 비활성화하십시오.

다음 위치에 종류가 DWORD 인 EnableVLV 레지스트리 키를 생성하십시오.

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\Siteminder\CurrentVersion\DS\LDAPProvider

EnableVLV

VLV 에서 LDAP 디렉터리 조회를 비활성화 또는 활성화합니다. VLV 를 비활성화하려면 EnableVLV 를 0 으로 설정하십시오. VLV 를 활성화하려면 EnableVLV 를 1 로 설정하십시오.

값: 0(사용 안 함) 또는 1(사용)

기본값: 1(사용됨)

STAR 이슈: 20397633-1

부록 C: 로그 파일 설명

smaccesslog4

다음 표에서는 인증 및 권한 부여 작업을 로깅하는 smaccesslog4 에 표시되는 로깅에 대해 설명합니다.

필드 이름	설명	Null 여부	필드 형식
sm_timestamp	데이터베이스에 항목이 만들어진 시간을 표시합니다.	NOT NULL	DATE
sm_categoryid	로깅 유형에 대한 식별자입니다. 다음 중 하나일 수 있습니다. ■ 1 = Auth ■ 2 = Az ■ 3 = Admin ■ 4 = Affiliate	NOT NULL	NUMBER(38)

필드 이름	설명	Null 여부	필드 형식
sm_eventid	로깅 발생의 원인이 된 특정 이벤트를 표시합니다. 다음 중 하나일 수 있습니다. ■ 1 = AuthAccept ■ 2 = AuthReject ■ 3 = AuthAttempt ■ 4 = AuthChallenge ■ 5 = AzAccept ■ 6 = AzReject ■ 7 = AdminLogin ■ 8 = AdminLogout ■ 9 = AdminReject ■ 10 = AuthLogout ■ 11 = ValidateAccept ■ 12 = ValidateReject ■ 13 = Visit	NOT NULL	NUMBER(38)
sm_hostname	서버가 실행되는 컴퓨터입니다.		VARCHAR2(255)
sm_sessionid	해당 사용자의 작업에 대한 세션 식별자입니다.		VARCHAR2(255)
sm_username	이 세션에서 현재 로그인한 사용자의 사용자 이름입니다.		VARCHAR2(512)
sm_agentname	정책 서버와 함께 사용되는 에이전트에 연관된 이름입니다.		VARCHAR2(255)
sm_realmname	사용자가 원하는 리소스가 현재 있는 영역입니다.		VARCHAR2(255)
sm_realmoid	영역의 고유 식별자입니다.		VARCHAR2(64)
sm_clientip	보호된 리소스를 사용하려고 하는 클라이언트 컴퓨터의 IP 주소입니다.		VARCHAR2(255)
sm_domainoid	사용자가 액세스하려는 영역 및 리소스가 있는 도메인의 고유 식별자입니다.		VARCHAR2(64)

필드 이름	설명	Null 여부	필드 형식
sm_authdirname	이 필드는 보고서 생성기에서 사용되지 않습니다.		VARCHAR2(255)
sm_authdirserver	이 필드는 보고서 생성기에서 사용되지 않습니다.		VARCHAR2(512)
sm_authdir-namespace	이 필드는 보고서 생성기에서 사용되지 않습니다.		VARCHAR2(255)
sm_resource	사용자가 요청하는 웹 페이지 등의 리소스입니다.		VARCHAR2(512)
sm_action	HTTP 작업입니다. Get, Post 및 Put		VARCHAR2(255)
sm_status	작업에 대한 설명 텍스트입니다.		VARCHAR2(1024)

필드 이름	설명	Null 여부	필드 형식
sm_reason	로깅 이유입니다. 32000 이상은 사용자가 정의합니다. 다음 값이 사용됩니다. ■ 0 = None ■ 1 = PwMustChange ■ 2 = InvalidSession ■ 3 = RevokedSession ■ 4 = ExpiredSession ■ 5 = AuthLevelTooLow ■ 6 = UnknownUser ■ 7 = UserDisabled ■ 8 = InvalidSessionId ■ 9 = InvalidSessionIp ■ 10 = CertificateRevoked ■ 11 = CRLOutOfDate ■ 12 = CertRevokedKeyCompromised ■ 13 = CertRevokedAffiliationChange ■ 14 = CertOnHold ■ 15 = TokenCardChallenge ■ 16 = ImpersonatedUserNotInDi ■ 17 = Anonymous ■ 18 = PwWillExpire ■ 19 = PwExpired ■ 20 = ImmedPWChangeRequired ■ 21 = PWChangeFailed ■ 22 = BadPWChange ■ 23 = PWChangeAccepted ■ 24 = ExcessiveFailedLoginAttempts ■ 25 = AccountInactivity ■ 26 = NoRedirectConfigured ■ 27 = ErrorMessageIsRedirect	NOT NULL	NUMBER(38)

필드 이름	설명	Null 여부	필드 형식
sm_reason (계속)	■ 28 = Tokencode ■ 29 = New_PIN_Select ■ 30 = New_PIN_Sys_Tokencode ■ 31 = New_User_PIN_Tokencode ■ 32 = New_PIN_Accepted ■ 33 = Guest ■ 34 = PWSelfChange ■ 35 = ServerException ■ 36 = UnknownScheme ■ 37 = UnsupportedScheme ■ 38 = Misconfigured ■ 39 = BufferOverflow		
sm_transactionid	이 필드는 보고서 생성기에서 사용되지 않습니다.		VARCHAR2(255)
sm_domainname	사용자가 액세스하려는 영역 및 리소스가 있는 도메인의 이름입니다.	NULL	VARCHAR2(255)
sm_impersonator-name	가장된 세션에서 가장 주체 역할을 하는 관리자의 로그인 이름입니다.	NULL	VARCHAR2(512)
sm_impersonator-dirname	가장 주체가 포함된 디렉터리 개체의 이름입니다.	NULL	VARCHAR2(255)

smobjlog4

다음 표에서는 관리 이벤트를 로깅하는 smobjlog4 에 표시되는 로깅에 대해 설명합니다.

필드 이름	설명	Null 여부	유형
sm_timestamp	데이터베이스에 항목이 만들어진 시간을 표시합니다.	NOT NULL	DATE

필드 이름	설명	Null 여부	유형
sm_categoryid	로깅 유형에 대한 식별자입니다. 다음 중 하나일 수 있습니다. ■ 1 = Auth ■ 2 = Agent ■ 3 = AgentGroup ■ 4 = Domain ■ 5 = Policy ■ 6 = PolicyLink ■ 7 = Realm ■ 8 = Response ■ 9 = ResponseAttr ■ 10 = ResponseGroup ■ 11 = Root ■ 12 = Rule ■ 13 = RuleGroup ■ 14 = Scheme ■ 15 = UserDirectory ■ 16 = UserPolicy ■ 17 = Vendor ■ 18 = VendorAttr ■ 19 = Admin ■ 20 = AuthAzMap ■ 21 = CertMap ■ 22 = ODBCQuery ■ 23 = SelfReg ■ 24 = PasswordPolicy ■ 25 = KeyManagement ■ 26 = AgentKey ■ 27 = ManagementCommand ■ 28 = RootConfig	NOT NULL	NUMBER(38)

필드 이름	설명	Null 여부	유형
sm_categoryid (계속)	■ 29 = Variable ■ 30 = VariableType ■ 31 = ActiveExpr ■ 32 = PropertyCollection ■ 33 = PropertySection ■ 34 = Property ■ 35 = TaggedString ■ 36 = TrustedHost ■ 37 = SharedSecretPolicy	NOT NULL	NUMBER(38)
sm_eventid	로깅 발생의 원인이 된 특정 이벤트를 표시합니다. 다음 중 하나일 수 있습니다. ■ 1 = Create ■ 2 = Update ■ 3 = UpdateField ■ 4 = Delete ■ 5 = Login ■ 6 = Logout ■ 7 = LoginReject ■ 8 = FlushAll ■ 9 = FlushUser ■ 10 = FlushUsers ■ 11 = FlushRealms ■ 12 = ChangeDynamicKeys ■ 13 = ChangePersistentKey ■ 14 = ChangeDisabledUserState ■ 15 = ChangeUserPassword ■ 16 = FailedLoginAttemptsCount ■ 17 = ChangeSessionKey	NOT NULL	NUMBER(38)

필드 이름	설명	Null 여부	유형
sm_hostname	이 필드는 보고서 생성기에서 관리 로깅에 사용되지 않습니다.		VARCHAR2(255)
sm_sessionid	해당 사용자의 작업에 대한 세션 식별자입니다.		VARCHAR2(255)
sm_username	해당 관리자의 사용자 이름입니다.		VARCHAR2(512)
sm_objname	액세스 중인 관리자의 개체입니다.		VARCHAR2(512)
sm_objoid	관리자에서 액세스 중인 개체의 고유 식별자입니다. 이 필드는 보고서 생성기에서 사용되지 않습니다.		VARCHAR2(64)
sm_fielddesc	관리자가 수행하는 작업에 대한 설명 텍스트입니다.		VARCHAR2(1024)
sm_domainoid	관리자에서 액세스 중인 개체가 있는 도메인의 고유 식별자입니다. 이 필드는 보고서 생성기에서 사용되지 않습니다.		VARCHAR2(64)
sm_status	작업에 대한 설명 텍스트입니다. 이 필드는 보고서 생성기에서 사용되지 않습니다.		VARCHAR2(1024)

부록 D: 진단 정보 게시

진단 정보 개요

정책 서버에는 SiteMinder 배포 환경에 대한 진단 정보를 게시할 수 있는 명령줄 도구가 포함되어 있습니다. 이 도구를 사용하여 정책 서버, 정책 저장소, 사용자 디렉터리, 에이전트 및 사용자 지정 모듈에 대한 정보를 게시할 수 있습니다.

명령줄 인터페이스 사용

정책 서버에는 정보 게시를 위해 명령줄에서 실행할 수 있는 명령이 포함되어 있습니다. 이 명령은 *installation_dir*/siteminder/bin 디렉터리에 있습니다.

정보를 게시하려면 smpolicysrv 명령을 사용하고 그 뒤에 -publish 스위치를 사용하십시오. 예를 들면 다음과 같습니다.

```
smpolicysrv -publish <optional file_name>
```

참고: Windows 시스템의 경우 원격 데스크톱 또는 터미널 서비스 창에서 smpolicysrv 명령을 실행하지 *마십시오*. smpolicysrv 명령을 실행하려면 프로세스 간 통신이 필요하며 smpolicysrv 프로세스를 원격 데스크톱 또는 터미널 서비스 창에서 실행할 경우에는 프로세스 간 통신이 작동하지 않습니다.

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

게시되는 정보의 위치 지정

게시되는 정보는 지정된 파일에 XML 형식으로 기록됩니다. 지정된 파일 이름은 다음 레지스트리 키에 저장됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\
Publish
```

이 키는 시스템 레지스트리(Windows 시스템) 및 *install_dir*/registry/sm.registry 파일(UNIX)에 있습니다. 레지스트리 설정의 기본값은 다음과 같습니다.

<*policy_server_install_dir*>\log\smpublish.xml

명령줄에서 **smpolicysrv -publish** 를 실행할 때 경로와 파일 이름을 지정하지 않으면 이 레지스트리 설정의 값에 따라 게시되는 XML 파일의 위치가 결정됩니다.

참고: Windows 시스템의 경우 원격 데스크톱 또는 터미널 서비스 창에서 smpolicysrv 명령을 실행하지 *마십시오*. smpolicysrv 명령을 실행하려면 프로세스 간 통신이 필요하며 smpolicysrv 프로세스를 원격 데스크톱 또는 터미널 서비스 창에서 실행할 경우에는 프로세스 간 통신이 작동하지 않습니다.

중요! Windows Server 2008 에서 SiteMinder 유틸리티 또는 실행 파일을 실행하기 전에 관리자 권한을 사용하여 명령줄 창을 여십시오. 사용하는 계정에 관리자 권한이 있는 경우에도 이 방식으로 명령줄 창을 여십시오.

위치를 지정하고 XML 파일에 출력을 생성하려면

1. 명령줄에서 다음 위치로 이동합니다.

   installation_dir/siteminder/bin

2. 다음 명령을 입력합니다.

   smpolicysrv -publish *path_and_file_name*

   예를 들어 Windows 의 경우 다음 명령을 입력합니다.

   smpolicysrv -publish c:\netegrity\siteminder\published-data.txt

   예를 들어 UNIX 의 경우 다음 명령을 입력합니다.

   smpolicysrv -publish /netegrity/siteminder/published-data.txt

   그러면 정책 서버가 지정된 위치에 XML 출력을 생성하고 지정된 위치와 일치하도록 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Publish 레지스트리 키의 값을 업데이트합니다.

게시되는 데이터

이 단원에서는 다음 항목에 대해 게시될 수 있는 정보를 간략히 설명합니다.

- 정책 서버
- 정책/키 저장소
- 사용자 디렉터리
- 에이전트
- 사용자 지정 모듈

게시되는 정책 서버 정보

정책 서버 정보에는 서버 이름, 플랫폼, 구성 및 서버 버전 정보가 포함됩니다. 또한 정책 서버를 구성하는 데 사용되는 레지스트리 설정도 게시될 수 있습니다.

게시되는 정책 서버 정보에는 다음이 포함됩니다.

- 기본 정보
  - 이름
  - 버전
  - Platform
  - 스레드 풀 통계
- 서버 구성(정책 서버 관리 콘솔에 설정된 값)
  - 키 관리
  - 저널링
  - 캐싱
  - 이벤트 처리기
  - 추적 로깅
  - 감사 로깅

게시되는 정책 서버 XML 출력 형식

다음 예에서는 정책 서버 정보의 형식을 지정하는 방법을 보여 줍니다.

```
<SERVER>
     < SHORT_NAME>   smpolicysrv </SHORT_NAME>
     <FULL_NAME>    SiteMinder Policy Server </FULL_NAME>
     <PRODUCT_NAME> SiteMinder(tm) </PRODUCT_NAME>
     <VERSION>  6.0 </VERSION>
     <UPDATE>   01 </UPDATE>
     <LABEL>    283 </LABEL>
     <PLATFORM> Windows (Build 3790)
    </PLATFORM>
     <SERVER_PORT>     44442 </SERVER_PORT>
     <RADIUS_PORT> 0 </RADIUS_PORT>
     <THREADPOOL>
         <MSG_TOTALS>    15011 </MSG_TOTALS>
         <MSG_DEPTH>     2 </MSG_DEPTH>
         <THREADS_LIMIT> 8 </THREADS_LIMIT>
         <THREADS_MAX>   3 </THREADS_MAX>
         <THREADS_CURRENT> 3 </THREADS_CURRENT>
     </THREADPOOL>
     <CRYPTO> 128 </CRYPTO>
     <KEYMGT>
         <GENERATION> enabled </GENERATION>
         <UPDATE>     disabled </UPDATE>
     </KEYMGT>
     <JOURNAL>
         <REFRESH> 60 </REFRESH>
         <FLUSH>   60 </FLUSH>
     </JOURNAL>
     <PSCACHE>
         <STATE>          enabled </STATE>
         <PRELOAD>        enabled </PRELOAD>
     </PSCACHE>
     <USERAZCACHE>
         <STATE>    enabled </STATE>
         <MAX>      10 </MAX>
         <LIFETIME> 3600 </LIFETIME>
     </USERAZCACHE>
</SERVER>
```

다음 표에서는 게시되는 정책 서버 정보를 정의합니다.

태그	포함 내용	설명	부모 태그	필수
SERVER	요소	서버 정보를 나타냄	SMPUBLSIH	필수
SHORT_NAME	텍스트	서버의 약식 이름	SERVER	필수
FULL_NAME	텍스트	실행 중인 서버의 server	SERVER	필수
PRODUCT_NAME	텍스트	제품 이름	SERVER	필수
VERSION	텍스트	서버 버전	SERVER	필수
UPDATE	텍스트	서비스 팩 버전	SERVER	필수
LABEL	텍스트	빌드 또는 CR 번호	SERVER	필수
PLATFORM	텍스트	OS 플랫폼 식별 데이터	SERVER	필수
THREAD_POOL	요소	스레드 풀에 대한 정보	SERVER	필수
MSG_TOTAL	정수	처리된 스레드 풀 메시지 수	THREAD_POOL	필수
MSG_DEPTH	정수	스레드 풀의 최대 메시지 수	THREAD_POOL	필수
THREADS_LIMIT	정수	최대 스레드 수	THREAD_POOL	필수
THREADS_MAX	정수	사용된 최대 스레드 수	THREAD_POOL	필수
THREADS_CURRENT	정수	사용된 현재 스레드 수	THREAD_POOL	필수
PSCACHE	요소	정책 서버 캐시 설정에 대한 정보를 나타냄	SERVER	필수
PRELOAD	텍스트	사용/사용 안 함을 나타냄	PSCACHE	필수
JOURNAL	비어 있음	저널링 설정, 새로 고침 빈도 및 플러시할 시점 값을 나타냄	SERVER	필수
FLUSH	정수	플러시할 시점의 값	JOURNAL	필수

태그	포함 내용	설명	부모 태그	필수
REFRESH	정수	새로 고침 빈도	JOURNAL	필수
KEYMGT	비어 있음	키 관리 설정을 나타냄 GENERATION: 자동 키 생성이 사용되도록 설정된 경우 UPDATE: 에이전트 키의 자동 업데이트가 수행되는 경우	SERVER	필수
GENERATION	enabled 또는 disabled	enabled 또는 disabled 는 자동 키 생성이 사용되는지를 나타냄	KEYMGT	필수
UPDATE	enabled 또는 disabled	에이전트 키의 자동 업데이트가 사용되는지를 enabled	KEYMGT	필수
USERAZCACHE	요소	사용자 AZ 캐시 설정에 대한 정보	SERVER	필수
MAX	정수	최대 캐시 항목 수	USERAZCACHE	필수
LIFETIME	정수	캐시된 개체의 수명	USERAZCACHE	필수
PORT	정수	포트 번호	SERVER	필수
RADIUS_PORT	정수	Radius 포트 번호 (사용되도록 설정된 경우)	SERVER	필수
STATE	텍스트, enabled 또는 disabled	항목이 사용되는지 여부를 나타냄	여러 태그	경우에 따라 다름

게시된 개체 저장소 정보

정책 서버는 다음과 같은 유형의 개체 저장소에 정보를 저장할 수 있습니다.

- 정책 저장소
- 키 저장소

- 감사 로그 저장소
- 세션 저장소

게시된 개체 저장소 정보에는 사용되는 개체 저장소의 유형, 백엔드 데이터베이스 정보, 구성 및 연결 정보가 포함됩니다.

게시되는 정책/키 저장소 XML 출력 형식

다음 예에서는 정책/키 저장소 정보의 형식을 지정하는 방법을 보여 줍니다.

```
<POLICY_STORE>

   <DATASTORE>
      <NAME> Policy Store   </NAME>
      <USE_DEFAULT_STORE>  false </USE_DEFAULT_STORE>
      <LOADED> true </LOADED>
      <SERVER_LIST>
         <CONNECTION_INFO>
            <TYPE> ODBC</TYPE>
            <SERVICE_NAME> sm </SERVICE_NAME>
            <USER_NAME> sa </USER_NAME>
            <DBMS_NAME> Microsoft SQL Server </DBMS_NAME>
            <DRIVER_NAME> Microsoft SQL Server </DRIVER_NAME>
            <DBMS_VERSION> 08.00.0760 </DBMS_VERSION>
         </CONNECTION_INFO>
     </SERVER_LIST>
   </DATASTORE>

   <DATASTORE>
      <NAME>  Key Store </NAME>
      <USE_DEFAULT_STORE> true </USE_DEFAULT_STORE>
      <LOADED> true </LOADED>
   </DATASTORE>

   <DATASTORE>
      <NAME> Audit Log Store </NAME>
      <USE_DEFAULT_STORE> true </USE_DEFAULT_STORE>
      <LOADED> true </LOADED>
   </DATASTORE>

   <DATASTORE>
      <NAME> Session Server Store </NAME>
      <USE_DEFAULT_STORE>  false </USE_DEFAULT_STORE>
      <LOADED> false </LOADED>
   </DATASTORE>

</POLICY_STORE>
```

다음 표에서는 게시되는 정책/키 저장소 정보를 정의합니다.

태그	포함 내용	설명	부모 태그	필수
POLICY_STORE	요소	모든 데이터 저장소 정보를 나타냄	SMPUBLISH	필수
DATASTORE	요소	특정 개체 저장소에 대한 정보를 나타냄 ■ TYPE 은 데이터 저장소의 유형입니다. ■ USE_DEFAULT_STORE 는 해당 유형에 기본 개체 저장소가 사용됨을 나타냅니다. ■ LOADED 는 해당 유형이 로드되는지 여부를 나타냅니다.	POLICY_STORE	필수
NAME	텍스트	데이터 저장소의 이름/유형	DATASTORE	필수
USE_DEFAULT_STORE	텍스트	저장소가 기본 '정책 저장소' 내에 있는지 여부(True/false)를 나타냄	DATASTORE	필수
LOADED	텍스트	데이터 저장소가 로드되고 초기화되었는지 여부(true/false)를 나타냄	DATASTORE	필수
TYPE	텍스트	정책 저장소의 유형, 즉 ODBC/LDAP	DATASTORE	필수
SERVER_ LIST	요소	데이터 저장소(ODBC)에 사용되는 장애 조치 서버의 목록	DATASTORE	선택 사항
CONNECTION_INFO	요소	서버 연결의 유형	SERVER_LIST	선택 사항
DRIVER_NAME	텍스트	ODBC 드라이버 이름	CONNECTION	선택 사항
IP	텍스트	IP 주소	DATASTORE	선택 사항
LDAP_VERSION	텍스트	LDAP 버전	DATASTORE	선택 사항

태그	포함 내용	설명	부모 태그	필수
API_VERSION	텍스트	LDAP API 버전	DATASTORE	선택 사항
PROTOCOL_VERSION	텍스트	LDAP 프로토콜 버전	DATASTORE	선택 사항
API_VENDOR	텍스트	API 공급업체	DATASTORE	선택 사항
VENDOR_VERSION	텍스트	공급업체 버전	DATASTORE	선택 사항

게시되는 사용자 디렉터리 정보

정책 서버가 로드하고 액세스한 각 사용자 디렉터리에 대해 다음 정보가 게시될 수 있습니다.

- 구성
- 연결
- 버전

게시되는 사용자 디렉터리 XML 출력 형식

사용자 디렉터리 정보의 형식은 다음 예와 같이 지정됩니다.

참고: 게시되는 정보는 사용자 디렉터리의 유형에 따라 달라집니다.

```
< USER_DIRECTORIES>

   <DIRECTORY_STORE >
      <TYPE> ODBC </TYPE>
      <NAME> sql5.5sample </NAME>
      <MAX_CONNECTIONS> 15 </MAX_CONNECTIONS>
         <SERVER_LIST>
            <CONNECTION_INFO>
               <TYPE> ODBC</TYPE>
               <SERVICE_NAME> sql5.5sample </SERVICE_NAME>
               <USER_NAME> sa </USER_NAME>
               <DBMS_NAME> Microsoft SQL Server </DBMS_NAME>
               <DRIVER_NAME> Microsoft SQL Server </DRIVER_NAME>
               <DBMS_VERSION> 08.00.0760 </DBMS_VERSION>
            </CONNECTION_INFO>
         </SERVER_LIST>
   </DIRECTORY_STORE >
   <DIRECTORY_STORE>
      <TYPE> LDAP:  </TYPE>
      <NAME> LDAPsample </NAME>
      <FAILOVER_LIST> 172.26.14.101:12002 </FAILOVER_LIST>
      <VENDOR_NAME> Netscape-Directory/4.12 B00.193.0237
      </VENDOR_NAME>
      <SECURE_CONNECTION> disabled </SECURE_CONNECTION>
      <CREDENTIALS>       required </CREDENTIALS>
      <CONNECTION_INFO>
         <PORT_NUMBER> 12002 </PORT_NUMBER>
         <DIR_CONNECTION> 172.26.14.101:12002 </DIR_CONNECTION>
         <USER_CONNECTION> 172.26.14.101:12002 </USER_CONNECTION>
      </CONNECTION_INFO>
      <LDAP_VERSION>     1 </LDAP_VERSION>
      <API_VERSION>      2005 </API_VERSION>
      <PROTOCOL_VERSION> 3 </PROTOCOL_VERSION>
      <API_VENDOR>       mozilla.org </API_VENDOR>
      <VENDOR_VERSION>   500 </VENDOR_VERSION>
   </DIRECTORY_STORE>
</USER_DIRECTORIES>
```

다음 표에서는 게시되는 사용자 디렉터리 정보를 정의합니다.

태그	포함 내용	설명	부모 태그	필수
USER_DIRECTORIES	요소	로드된 디렉터리 저장소의 컬렉션을 나타냄	SMPUBLISH	필수
DIRECTORY_STORE	요소	특정 디렉터리 저장소를 나타냄	USER_DIRECTORIES	선택 사항
TYPE	텍스트	디렉터리 저장소의 유형	DIRECTORY_STORE	필수
NAME	텍스트	디렉터리 저장소의 정의된 이름	DIRECTORY_STORE	필수
MAX_CONNECTIONS	정수	정의된 최대 연결 수	DIRECTORY_STORE	선택 사항
SERVER_LIST	요소	서버 컬렉션 (ODBC)	DIRECTORY_STORE	선택 사항
FAILOVER_LIST	텍스트			

게시되는 에이전트 정보

게시되는 에이전트 정보에는 IP 주소 및 이름을 포함하여 정책 서버에 현재 연결된 에이전트가 나열됩니다.

게시되는 에이전트 XML 출력 형식

에이전트 정보의 형식은 다음 예와 같이 지정됩니다.

```
< AGENT_CONNECTION_MANAGER>
   <CURRENT>      4 </CURRENT>
   <MAX>          4 </MAX>
   <DROPPED>      0 </DROPPED>
   <IDLE_TIMEOUT> 0 </IDLE_TIMEOUT>
   <ACCEPT_TIMEOUT> 10 </ACCEPT_TIMEOUT>

   <AGENT_CONNECTION>
      <NAME> agent1 </NAME>
      <IP>   172.26.6.43 </IP>
      <API_VERSION> 1024 </API_VERSION>
      <LAST_MESSAGE_TIME> 0x05705E0C </LAST_MESSAGE_TIME>
   </AGENT_CONNECTION>
   <AGENT_CONNECTION>
      <NAME> agent1 </NAME>
      <IP>   172.26.6.43 </IP>
      <API_VERSION> 1024 </API_VERSION>
      <LAST_MESSAGE_TIME> 0x05705E0C </LAST_MESSAGE_TIME>
   </AGENT_CONNECTION>
   <AGENT_CONNECTION>
      <NAME> agent1 </NAME>
      <IP>   172.26.6.43 </IP>
      <API_VERSION> 1024 </API_VERSION>
      <LAST_MESSAGE_TIME> 0x05705E0C </LAST_MESSAGE_TIME>
   </AGENT_CONNECTION>
   <AGENT_CONNECTION>
      <NAME> 940c0728-d405-489c-9a0e-b2f831f78c56 </NAME>
      <IP>   172.26.6.43 </IP>
      <API_VERSION> 1482282902 </API_VERSION>
      <LAST_MESSAGE_TIME> 0x05705E0C </LAST_MESSAGE_TIME>
   </AGENT_CONNECTION>
</AGENT_CONNECTION_MANAGER>
```

참고: 에이전트 연결 정보는 <AGENT_CONNECTION_MANAGER> 태그 내에 포함됩니다.

다음 표에서는 게시되는 에이전트 정보를 정의합니다.

태그	포함 내용	설명	부모 태그	필수
AGENT_CONNECTION-_MANAGER	요소	에이전트 연결에 대한 데이터 정의	SM_PUBLISH	필수
CURRENT	정수	현재 연결 수	AGENT_CONNECTION-_MANAGER	필수
MAX	정수	최대 연결 수	AGENT_CONNECTION-_MANAGER	필수
DROPPED	정수	최대 연결 수	AGENT_CONNECTION-_MANAGER	필수
IDLE_TIMEOUT	정수	유휴 연결이 시간 만료되기까지의 시간	AGENT_CONNECTION-_MANAGER	필수
ACCEPT_TIMEOUT	정수	시도된 연결이 시간 만료되기까지의 시간	AGENT_CONNECTION-_MANAGER	필수
AGENT_CONNECTION	요소	활성 에이전트 연결에 대한 데이터를 나타냄	AGENT_CONNECTION-_MANAGER	선택 사항
IP	텍스트	에이전트의 IP 주소	AGENT_CONNECTION	필수
API_VERSION	정수	연결된 에이전트에서 사용되는 API 버전	AGENT_CONNECTION	필수
NAME	텍스트	에이전트 이름	AGENT_CONNECTION	필수
LAST_MESSAGE_TIME	정수	에이전트의 마지막 메시지 이후 경과 시간	AGENT_CONNECTION	필수
AGENT_CONNECTION-_MANAGER	요소	에이전트 연결에 대한 데이터 정의	SM_PUBLISH	필수

게시되는 사용자 지정 모듈 정보

사용자 지정 모듈은 기존 정책 서버의 기능을 확장하기 위해 생성할 수 있는 DLL 또는 라이브러리입니다. 사용자 지정 모듈은 이벤트 처리기, 인증 모듈, 권한 부여 모듈, 디렉터리 모듈 및 터널링 모듈 같은 여러 유형으로 제공됩니다. 인증 모듈은 일반적으로 사용자 지정 인증 스키마라고 하며 권한 부여 모듈은 활성 정책이라고 합니다. 터널 모듈은 에이전트와의 보안 통신을 정의하는 데 사용됩니다. 이벤트 모듈은 이벤트 알림을 받기 위한 메커니즘을 제공합니다. 정책 서버가 어떤 사용자 지정 모듈을 로드했는지에 대한 정보가 게시될 수 있습니다. 각 사용자 지정 모듈 유형은 고유한 XML 태그로 정의됩니다.

게시되는 사용자 지정 모듈 XML 출력 형식

다음 표에서는 게시되는 사용자 지정 모듈 정보를 정의합니다.

태그	포함 내용	설명	부모 태그	필수
EVENT_LIB	요소	이벤트 API 사용자 지정 모듈에 대한 데이터를 나타냄	SMPUBLISH	선택 사항
AUTH_LIB	요소	인증 API 사용자 지정 모듈에 대한 데이터를 나타냄	SMPUBLISH	선택 사항
DS_LIB	요소	디렉터리 API 사용자 지정 모듈에 대한 데이터를 나타냄	SMPUBLISH	선택 사항
TUNNEL_LIB	요소	터널 API 사용자 지정 모듈에 대한 데이터를 나타냄	SMPUBLISH	선택 사항
AZ_LIB	요소	권한 부여 API 사용자 지정 모듈에 대한 데이터를 나타냄	SMPUBLISH	선택 사항

다음은 모든 유형의 사용자 지정 모듈에 공통적으로 사용됩니다.

태그	포함 내용	설명	부모 태그	필수
FULL_NAME	텍스트	경로를 포함한 라이브러리 또는 DLL 의 전체 이름		필수
CUSTOM_INFO	텍스트	사용자 지정 라이브러리가 제공하는 정보		선택 사항

LIB_NAME	텍스트	라이브러리 또는 DLL 이름	선택 사항
VERSION	정수	지원되는 API 버전	선택 사항

다음은 특정 유형의 모듈에만 사용됩니다.

태그	포함 내용	설명	API 유형	필수
ACTIVE_FUNCTION	텍스트	활성 식으로 호출할 수 있도록 로드된 함수 이름	권한 부여 API	선택 사항

부록 E: 오류 메시지

인증

메시지	Function	설명
1) Sending a new PIN to ACE/Server for validation.	SmLoginLogoutMessage::Send-NewPinForValidation1	정보 제공 목적으로만 사용됩니다. ACE/SecurID 인증 체계와 관련하여 문제가 발생할 경우 기술 지원부에 이 메시지를 제공하십시오.
2) Sending a new PIN to ACE/Server for validation %1s	SmLoginLogoutMessage::Send-NewPinForValidation2	정보 제공 목적으로만 사용됩니다. ACE/SecurID 인증 체계와 관련하여 문제가 발생할 경우 기술 지원부에 이 메시지를 제공하십시오.
Ace Server --- couldn't get PIN policies	SmLoginLogoutMessage::Sm-AuthAceGetPinPoliciesFail	이 메시지는 SecurID 인증 체계에서 SecurID/ACE API 호출을 사용하여 ACE 서버 백엔드 PIN 정책을 검색할 수 없는 경우에 발생합니다.
Ace Server --- couldn't get PIN params	SmLoginLogoutMessage::Sm-AceHtmlPinParamFail	이 메시지는 SecurID 인증 체계에서 SecurID/ACE API 호출을 사용하여 ACE PIN 매개 변수를 검색할 수 없는 경우에 발생합니다.
ACE State not ACM_NEXT_CODE_ REQUIRED. State = %1i	SmLoginLogoutMessage::Ace-NextTokenCodeState	이 메시지는 HTML SecurID 인증 체계에서 토큰 코드 값이 만료되어 사용자가 새 인증을 시도하기 전에 다음 코드를 기다려야 하는 경우에 발생합니다.

메시지	Function	설명
Ace/Server - new PIN is required, AceAPI returned ambiguous value for isselectable PIN attribute. Cannot complete Ace authentication.	SmLoginLogoutMessage::Sm-AceHtmlPinRequired	정보 제공 목적으로만 사용됩니다. ACE/SecurID 인증 체계와 관련하여 문제가 발생할 경우 기술 지원부에 이 메시지를 제공하십시오.
Ace/Server - new PIN is required, can choose or accept system PIN , returning Sm_AuthApi_Reject, Sm_Api_Reason_New_PIN_Select.	SmLoginLogoutMessage::Sm-AceHtmlChooseNewOrSysPin	이 메시지는 SecurID 인증 체계에서 ACE 사용자가 직접 선택한 PIN 이나 시스템에서 생성된 PIN 을 사용하도록 구성된 경우에 발생합니다.
Ace/Server - new PIN is required, Must accept system PIN, returned Sm_Api_Reason_New_PIN_Sys_Tokencode	SmLoginLogoutMessage::Sm-AceHtmlCannotChoosePin	이 메시지는 SecurID 인증 체계에서 ACE 사용자가 항상 시스템에서 생성된 PIN 을 사용하도록 구성된 경우에 발생합니다.
Ace/Server - new PIN is required, must choose PIN, returning Sm_AuthApi_Reject, Sm_Api_Reason_New_User_-PIN_Tokencode.	SmLoginLogoutMessage::Sm-AceHtmlChooseNewPin	이 메시지는 SecurID 인증 체계에서 ACE 사용자가 항상 직접 선택한 PIN 을 사용하도록 구성된 경우에 발생합니다.
ACE/Server: ACM_NEW_PIN_ACCEPTED failed with aceRetVal %1i	SmLoginLogoutMessage::Ace-ServerNewPinAcceptedFailed	HTML SecurID 인증 체계에 사용됩니다. ACE 서버가 새 사용자 PIN 을 허용하지 않은 경우에 발생합니다.
ACE/Server: ACM_NEW_PIN_ACCEPTED failed with aceRetVal %1i, ACE status %2i	SmLoginLogoutMessage::Not-WinAceServerNewPinAccepted-Failed	HTML SecurID 인증 체계에 사용됩니다. ACE 서버가 새 사용자 PIN 을 허용하지 않은 경우에 발생합니다.
ACE/Server: ACM_NEW_PIN_ACCEPTED failed.	SmLoginLogoutMes-sage::NewPinAcceptedFailed	HTML SecurID 인증 체계에 사용됩니다. ACE 서버가 새 사용자 PIN 을 허용하지 않은 경우에 발생합니다.
AceCheck Access denied by ACE/Server.	SmLoginLogoutMessage::Ace-CheckAccessDenied	이 메시지는 SecurID 인증 체계에서 ACE 서버가 인증 요청을 거부한 경우에 발생합니다.

메시지	Function	설명
AceCheck not processed aceRetVal = %1i	SmLoginLogoutMessage::Ace-CheckNotProcessed	이 오류 메시지는 SecurID 인증 체계에서 ACE/SecurID API 를 통한 ACE 인증 프로세스를 완료할 수 없는 경우에 발생합니다.
AceCheck returned not ACM_NEW_PIN_REQUIRED but %1i	SmLoginLogoutMessage::Acm-NewPinRequiredFail	정보 제공 목적으로만 사용됩니다. ACE/SecurID 인증 체계와 관련하여 문제가 발생할 경우 기술 지원부에 이 메시지를 제공하십시오.
AceCheck returned not ACM_NEW_PIN_REQUIRED but %1i	SmLoginLogoutMessage::Invalid-ReturnAceCheckNewPin	정보 제공 목적으로만 사용됩니다. ACE/SecurID 인증 체계와 관련하여 문제가 발생할 경우 기술 지원부에 이 메시지를 제공하십시오.
AceCheck:Denied---aceRetVal = %1i	SmLoginLogoutMessage::Sm-AuthAceCheck-Denial	이 메시지는 SecurID 인증 체계에서 ACE 서버가 인증 요청을 거부한 경우에 발생합니다.
AceGetMaxPinLen failed	#REF!	HTML SecurID 인증 체계에 사용됩니다. 인증 체계가 ACE 서버에서 허용되는 최대 사용자 PIN 길이를 검색하지 못한 경우에 발생합니다.
AceSendPin failed	SmLoginLogoutMessage::Ace-SendPinFailed	이 오류 메시지는 HTML SecurID 인증 체계에서 사용 중인 사용자 PIN 을 RSA ACE 서버 ACE/SecurID API 로 보내지 못한 경우에 발생합니다. 인증 체계는 해당 요청을 거부합니다.
AceServer - CANNOT_CHOOSE_PIN	SmLoginLogoutMessage::Ace-ServerCannotChoosePin	정보 제공 목적으로만 사용됩니다. ACE/SecurID 인증 체계와 관련하여 문제가 발생할 경우 기술 지원부에 이 메시지를 제공하십시오.

메시지	Function	설명
AceServer - MUST_CHOOSE_PIN	SmLoginLogoutMessage::Ace-ServerMustChoosePin	정보 제공 목적으로만 사용됩니다. ACE/SecurID 인증 체계와 관련하여 문제가 발생할 경우 기술 지원부에 이 메시지를 제공하십시오.
AceServer :: Sm_Api_Reason_New_PIN_ 선택	SmLoginLogoutMessage::Sm-ApiNewPinSelectReason	정보 제공 목적으로만 사용됩니다. ACE/SecurID 인증 체계와 관련하여 문제가 발생할 경우 기술 지원부에 이 메시지를 제공하십시오.
AceServer returning Sm_Api_Reason_New_PIN_ Accepted	SmLoginLogoutMessage::Sm-ApiSuccessReason	HTML SecurID 인증 체계에 사용됩니다. 사용자가 사용자 PIN 을 성공적으로 변경한 경우에 발생합니다.
AceServer:: returning Sm_AuthApi_Reject Sm_Api_Reason_New_PIN_ Accepted, but not success message can be given, don't know the target.	SmLoginLogoutMessage::Sm-ApiRejectReasonMessage	정보 제공 목적으로만 사용됩니다. ACE/SecurID 인증 체계와 관련하여 문제가 발생할 경우 기술 지원부에 이 메시지를 제공하십시오.
AceSetPasscode = %1s	SmLoginLogoutMessage::Sm-AuthAceSetPassCode	이 메시지는 SecurID 인증 체계에서 ACE/SecurID API 를 통해 ACE 인증을 위한 암호 코드를 등록하려고 할 경우에 발생합니다.
AceSetPasscode failed with aceRetVal = %1i	SmLoginLogoutMessage::Ace-SetPasscodeFailed	이 오류 메시지는 SecurID 인증 체계에서 ACE/SecurID API 를 통해 ACE 인증을 위한 암호 코드를 등록하는 데 실패할 경우에 발생합니다. 인증 체계는 해당 요청을 거부합니다.
AceSetPin failed	SmLoginLogoutMessage::Ace-SetPinFailed	이 오류 메시지는 HTML SecurID 인증 체계에서 ACE/SecurID API 를 사용하여 사용자 PIN 을 설정하는 데 실패할 경우에 발생합니다. 인증 체계는 해당 요청을 거부합니다.

메시지	Function	설명
AceSetSelectionCode DECRYPT = %1s	SmLoginLogoutMessage::-SelectioncodeDecrypt	정보 제공 목적으로만 사용됩니다. ACE/SecurID 인증 체계와 관련하여 문제가 발생할 경우 기술 지원부에 이 메시지를 제공하십시오.
AceSetUsername failed with aceRetVal = %1i	SmLoginLogoutMessage::Ace-SetUserNameFailed	이 메시지는 SecurID 인증 체계에서 ACE/SecurID API 를 통해 ACE 인증을 위한 사용자 이름을 등록하는 데 실패할 경우에 발생합니다. 인증 체계는 해당 요청을 거부합니다.
AddCurrentPWToHistory - Can't set password history info.	SmLoginLogoutMes-sage::ErrorSettingPassword-History	현재 암호를 최근 암호 목록에 추가하지 못했습니다.
AuthenticateUserDir - Can't update user blob data	SmLoginLogoutMessage::Blob-UpdateFailed	인증 프로세스 중 암호 Blob 데이터를 업데이트하지 못했습니다.
Cannot get AceAlphanumeric	SmLoginLogoutMessage::Get-AceAlphanumericFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceCancelPin	SmLoginLogoutMessage::Get-AceCancelPinFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceCheck	SmLoginLogoutMessage::Get-AceCheckFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceClientCheck	SmLoginLogoutMessage::Get-AceClientCheckFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceClose	SmLoginLogoutMessage::Get-AceCloseFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceGetAuthenticationStatus	SmLoginLogoutMessage::Ace-GetAuthenticationStatusFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceGetMaxPinLen	SmLoginLogoutMessage::Null-AceGetMaxPinLen	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceGetMinPinLen	SmLoginLogoutMessage::Null-AceGetMinPinLen	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.

메시지	Function	설명
Cannot get AceGetPinParams	SmLoginLogoutMessage::Get-AcePinParamFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceGetShell	SmLoginLogoutMessage::Ace-GetShellFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceGetSystemPin	SmLoginLogoutMessage::Ace-GetSystemPinFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceGetTime	SmLoginLogoutMessage::Ace-GetTimeFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceGetUserData	SmLoginLogoutMessage::Ace-GetUserDataFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceGetUserSelectable	SmLoginLogoutMessage::Ace-GetUserSelectable-Fail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceInit	SmLoginLogoutMessage::Get-AceInitFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceInitialize	SmLoginLogoutMessage::Ace-InitializeFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceLock	SmLoginLogoutMessage::Ace-LockFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceSendNextPasscode	SmLoginLogoutMessage::Ace-SendNextPasscodeFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceSendPin	SmLoginLogoutMessage::Null-AceSendPin	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceSetNextPasscode	SmLoginLogoutMessage::Ace-SetNextPasscodeFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceSetPasscode	SmLoginLogoutMessage::Ace-SetPasscodeFail	정보 제공 목적으로만 사용됩니다. ACE/SecurID 인증 체계와 관련하여 문제가 발생할 경우 기술 지원부에 이 메시지를 제공하십시오.
Cannot get AceSetPin	SmLoginLogoutMessage::Null-AceSetPin	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.

메시지	Function	설명
Cannot get AceSetUserClientAddress	SmLoginLogoutMessage::Ace-SetUserClientAddressFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot get AceSetUsername	SmLoginLogoutMessage::Ace-SetUsernameFail	ACE Client 라이브러리에서 메서드를 찾지 못했습니다.
Cannot load aceclnt.dll	SmLoginLogoutMessage::Ace-lntDllLoadFail	ACE Client 라이브러리를 로드하지 못했습니다.
Cannot retrieve new password from password message	SmLoginLogoutMessage::New-PasswordRetrieveFail	로그인 요청을 처리하고 새 암호와 이전 암호를 분석할 때 새 암호를 가져오지 못했습니다.
Cannot retrieve old password from password message	SmLoginLogoutMessage::Old-PaswordRetrieveFail	로그인 요청을 처리하고 새 암호와 이전 암호를 분석할 때 이전 암호를 가져오지 못했습니다.
Cannot retrieve token from password message	SmLoginLogoutMessage::Token-RetrieveFail	로그인 요청을 처리하고 새 암호와 이전 암호를 분석할 때 암호 토큰을 가져오지 못했습니다.
ChangePassword - Can't change password via the provider	SmLoginLogoutMessage::Pwd-ChangeFailViaProvider	암호 변경 요청 중 사용자 디렉터리에서 암호를 변경하지 못했습니다.
ChangePassword - Can't validate the new password	SmLoginLogout-Message::ChangePwdValidation-Fail	암호 변경 요청 중 사용자 디렉터리에서 암호의 유효성을 검사하지 못했습니다.
CheckPasswordPolicies - authentication status changed to failure due to password policy misconfiguration.	SmLoginLogout-Message::CheckPwdFailCause-Misconfig	암호 정책을 확인할 때 로그인 시도의 유효성을 검사하지 못했습니다. 암호 정책이 잘못 구성되었기 때문일 수 있습니다.
Could not find the Variable to delete %1s	SmLoginLogout-Message::VariableFindErrorTo-Delete	요청의 일부로 "세션 변수" 이름 앞에 "세션 변수" 플래그가 전달되었습니다.
CSmAuthUser - ChangePassword - Can't update user blob data	SmLoginLogoutMes-sage::ChangePwdBlobUpdateFail	암호 변경 요청 중 암호 Blob 데이터를 업데이트하지 못했습니다.

메시지	Function	설명
DelVariable :Internal Error : Could not find the Variable	SmLoginLogoutMessage::Del-VariableFindError	세션 저장소에서 변수 이름을 삭제하려고 할 때 변수 이름이 비어 있는 것으로 확인되었습니다.
DelVariable Returned Error %1i for Variable %2s	SmLoginLogoutMessage::Del-VariableReturnError	세션 저장소에서 이 변수를 삭제하지 못했습니다.
Did not set AceSetUsername = %1s	SmLoginLogoutMessage::Sm-AuthNotSetUserId	이 메시지는 SecurID 인증 체계에서 ACE/SecurID API 를 통해 ACE 인증을 위한 사용자 이름을 등록하는 데 실패할 경우에 발생합니다. 인증 체계는 해당 요청을 거부합니다.
Error finding the name of variable to be deleted %1s:Invalid Index %2i	SmLoginLogout-Message::VariableNameFind-InvalidIndexError	요청의 일부로 이름이 비어 있는 "세션 변수"에 대해 "세션 변수" 플래그가 전달되었습니다.
Error in scheme configuration parameter lpszServerParam corrupted.	SmLoginLogoutMessage::Error-SchemeConfigServerParam	SecurID 인증 체계에 사용됩니다. 위의 설명과 동일합니다.
Error in scheme configuration parameter: Empty String	SmLoginLogoutMessage::Error-SchemeConfigParam	기본 인증 체계와 양식 기반 SecurID 인증 체계 모두에 "디렉터리의 Ace 사용자 ID 특성 이름" 매개 변수가 필요합니다. 이 매개 변수가 누락되거나 잘못 구성된 경우에 이 오류가 표시됩니다.
Failed to authenticate user '%1s' using scheme '%2s'. Unsupported API version.	SmLoginLogoutMessage::User-AuthFail	인증 공급자 라이브러리가 이전 버전이어서 인증하지 못했습니다.
Failed to find authentication realm '%1s	SmLoginLogoutMessage::Auth-RealmFindFail	Radius 인증 요청을 처리할 때 에이전트/에이전트 그룹에 의해 보호되는 영역을 찾지 못했습니다.
FindApplicablePassword Policies - error fetching Root	SmLoginLogoutMessage::Error-FetchingApplicablePolicyRoot	로깅 시도의 유효성을 검사하는 중 루트 개체를 가져오지 못했습니다.

메시지	Function	설명
FindApplicablePassword Policies - error finding Matching Password Policies	SmLoginLogoutMessage::Error-FindingMatchingPolicies	로깅 시도의 유효성을 검사하는 중 PasswordPolicy 개체를 가져오지 못했습니다.
FindApplicablePassword Policies - No Password Data attribute defined for user dir %1s	SmLoginLogout-Message::PasswordDataAttrib-NotDefined	사용 중인 사용자 디렉터리에 Blob 에 대한 적절한 특성이 정의되어 있지 않습니다.
FindApplicablePassword Policies - user or directory is NULL	SmLoginLogoutMessage::Null-ApplicablePwdPolicyDir	로깅 시도의 유효성을 검사하는 중 적용 가능한 암호 정책을 찾을 때 사용자 및 디렉터리 개체가 모두 NULL 로 확인되었습니다.
GetRandomPassword - Shortest Length greater than Longest Length	SmLoginLogoutMessage::Long-PwdLength	생성된 임의 암호가 허용되는 최대 길이를 초과합니다.
GetRedirect - Can't find applicable password policies.	SmLoginLogoutMessage::Error-FindingPasswordPolicy	리디렉션 정보가 포함된 첫 번째 적용 가능한 암호 정책을 찾는 중 적용 가능한 정책을 찾지 못했습니다.
GetRedirect - Can't retrieve password policy.	SmLoginLogoutMessage::Error-RetrievePasswordPolicy	새 암호의 유효성을 검사하는 중 PasswordPolicy 개체를 가져오지 못했습니다.
GetVariable : Internal Error:DelVar %1s does not match Var: %2s	SmLoginLogoutMessage::Get-VariableMatchError	가져올 때 삭제할 변수의 이름이 가져오기 및 삭제 작업에 대해 서로 다르게 지정되었습니다.
GetVariable(Del) Returned Error %1i for Variable %2s	SmLoginLogoutMessage::Get-VariableDelReturnError	세션 저장소에서 이 변수를 삭제하지 못했습니다.
GetVariable(Fetch) Returned Error %1i for Variable %2s	SmLoginLogoutMessage::Get-VariableFetchReturnError	세션 저장소에서 이 변수를 찾지 못했습니다.
GetVariable: Internal Error :Could not find variable	SmLoginLogoutMessage::Get-VariableFindError	세션 변수를 가져오려고 할 때 변수 이름이 비어 있는 것으로 확인되었습니다.
Invalid format for SiteMinder generated user attribute %1s	SmLoginLogoutMessage::Invalid-SmUserAttribFormat	"Applcation Role User"(응용 프로그램 역할 사용자) 속성의 형식이 잘못되었습니다.

메시지	Function	설명
New PIN was accepted = %1s	SmLoginLogoutMessage::New-PinAccepted	HTML SecurID 인증 체계에 사용됩니다. 사용자가 사용자 PIN 을 성공적으로 변경한 경우에 발생합니다.
Nonstandard SelectionCode = %1s	SmLoginLogoutMessage::Ace-ServerNonStandard-Selectioncode	정보 제공 목적으로만 사용됩니다. ACE/SecurID 인증 체계와 관련하여 문제가 발생할 경우 기술 지원부에 이 메시지를 제공하십시오.
Passcode not allocated.	SmLoginLogout-Message::PasscodeNot-Allocated	SecurID 인증 체계에 사용됩니다. 사용자 암호 코드에 대한 버퍼를 할당하지 못했습니다.
PassCode1 not Allocated	SmLoginLogoutMessage::Mem-AllocPasscode1Fail	SecurID 인증 체계에 사용됩니다. 사용자 암호 코드에 대한 버퍼를 할당하지 못했습니다.
PassCode1 not Allocated	SmLoginLogout-Message::Passcode1Not-Allocated	SecurID 인증 체계에 사용됩니다. 다음 사용자 암호 코드에 대한 버퍼를 할당하지 못했습니다.
PassCode1 not checked, Error = %1i	SmLoginLogoutMes-sage::PassCode1NotChecked	이 오류 메시지는 SecurID 인증 체계에서 ACE/SecurID API 를 통한 ACE 인증 프로세스를 완료할 수 없는 경우에 발생합니다.
PassCode1 not set, Error = %1i	SmLoginLogoutMessage::Pass-Code1NotSet	이 메시지는 SecurID 인증 체계에서 ACE/SecurID API 를 통해 ACE 인증을 위한 암호 코드를 등록하려고 할 경우에 발생합니다.
PassCode1 not set, Error = %1i	SmLoginLogoutMessage::Pass-Code2NotSet	이 오류 메시지는 HTML SecurID 인증 체계에서 ACE/SecurID API 를 통해 ACE 인증을 위한 다음 암호 코드를 등록하는 데 실패할 경우에 발생합니다. 인증 체계는 해당 요청을 거부합니다.

메시지	Function	설명
PassCode2 not Allocated	SmLoginLogoutMessage::Mem-AllocPasscode2Fail	SecurID 인증 체계에 사용됩니다. 사용자 암호 코드에 대한 버퍼를 할당하지 못했습니다.
PassCode2 not Sent as NextPasscode, Error = %1i	SmLoginLogoutMessage::Pass-Code2NotSentAsNextPasscode	이 오류 메시지는 HTML SecurID 인증 체계에서 ACE/SecurID API 를 통해 ACE 서버로 다음 암호 코드를 보내는 데 실패할 경우에 발생합니다. 인증 체계는 해당 요청을 거부합니다.
Password Message could not be parsed	SmLoginLogout-Message::PasswordMessage-ParseFail	로그인 요청을 처리하고 새 암호와 이전 암호를 분석할 때 암호 문자열을 구문 분석하지 못했습니다.
PIN allocation failed	SmLoginLogoutMessage::Pin-AllocationFailed	HTML SecurID 인증 체계에 사용됩니다. 사용자 PIN 에 대한 버퍼를 할당하지 못했습니다.
pszBuf allocation failed	SmLoginLogoutMessage:pszBuf-AllocFail	SecurID 인증 체계에 사용됩니다. SiteMinder 사용자 디렉터리에 RSA SecurID 사용자 ID 특성 이름에 대한 버퍼를 할당하지 못했습니다.
Returning encrypted System PIN in Cookie via UserMsg %1s	SmLoginLogoutMes-sage::ReturningEncrypted-SystemPin	정보 제공 목적으로만 사용됩니다. ACE/SecurID 인증 체계와 관련하여 문제가 발생할 경우 기술 지원부에 이 메시지를 제공하십시오.
SelectionCode not allocated.	SmLoginLogout-Message::SelectionCodeNot-Allocated	정보 제공 목적으로만 사용됩니다. ACE/SecurID 인증 체계와 관련하여 문제가 발생할 경우 기술 지원부에 이 메시지를 제공하십시오.
Server exception occurred while authenticating user '%1s' using scheme '%2s	'SmLoginLogoutMessage::User-AuthException	인증 프로세스 중 알 수 없는 오류가 발생했습니다. 인증 공급자 라이브러리 문제일 수 있습니다.

메시지	Function	설명
Server exception occurred while validating authentication for user '%1s	'SmLoginLogoutMessage::Valid-AuthException	인증 프로세스 중 고급 암호 서비스 공유 라이브러리가 호출될 때 오류가 발생했습니다.
Set Username Error = %1i	SmLoginLogoutMessage::Set-UserNameError	이 메시지는 SecurID 인증 체계에서 ACE/SecurID API 를 통해 ACE 인증을 위한 사용자 이름을 등록하는 데 실패할 경우에 발생합니다. 인증 체계는 해당 요청을 거부합니다.
SetVariable :Internal Error: Could not find Variable	SmLoginLogoutMessage::Set-VariableFindError	세션 저장소에 변수 이름을 설정하려고 할 때 변수 이름이 비어 있는 것으로 확인되었습니다.
SetVariable :Internal Error: NULL Value found for Variable %1s	SmLoginLogoutMessage::Set-VariableNullValueFound	세션 저장소에 변수 값을 설정하려고 시도할 때 변수 값이 비어 있는 것으로 확인되었습니다.
SetVariable Returned Error %1i for Variable %2s	SmLoginLogoutMessage::Set-VariableReturnError	세션 저장소에 이 변수를 추가/업데이트하지 못했습니다.
SmAuthenticate: AceInitialization failed	SmLoginLogoutMessage::Sm-AuthAceInitFail	ACE Client 라이브러리를 초기화하지 못했습니다.
SmAuthenticate: Cannot create Event.	SmLoginLogoutMessage::Create-EventFail	SecurID 인증 체계에 사용됩니다. SecurID 인증 체계에 이벤트 개체를 생성하지 못했습니다.
SmAuthenticate: Couldn't get allocate memory for PIN	SmLoginLogoutMessage::Sm-AceHtmlPinMemAllocFail	SecurID 인증 체계에 사용됩니다. ACE 시스템에서 생성된 PIN 에 대한 버퍼를 할당하지 못했습니다.
SmAuthenticate: Did not set AceSetPasscode = %1s	SmLoginLogoutMessage::Sm-AuthAceDidNotSetPassCode	이 오류 메시지는 SecurID 인증 체계에서 ACE/SecurID API 를 통해 ACE 인증을 위한 암호 코드를 등록하는 데 실패할 경우에 발생합니다. 인증 체계는 해당 요청을 거부합니다.

메시지	Function	설명
SmAuthenticate: No numeric value found for SM_ACE_FAILOVER_ATTEMPTS environment variable, proceeding with default value.	SmLoginLogoutMessage::Zero-SmAuthAceFailover	RSA ACE/SecurID 장애 조치를 지원하기 위해 SiteMinder 정책 서버에는 환경 변수 SM_ACE_FAILOVER_ATTEMPTS 가 있습니다. 이 환경 변수는 기본적으로 3 으로 설정됩니다. 이 오류 메시지는 SM_ACE_FAILOVER_ATTEMPTS 값이 0 인 경우에 발생합니다. 이 경우 SiteMinder 에서 RSA ACE/SecurID 장애 조치가 제대로 작동하지 않을 수 있습니다.
SmAuthenticate:Cannot allocate storage for EventData	SmLoginLogoutMessage::Event-DataMemAllocFail	SecurID 인증 체계에 사용됩니다. RSA SecurID API 구조에 대한 메모리를 할당하지 못했습니다.
SmAuthenticate:Cannot proceed to AceInit--NOT ACE_PROCESSING. aceRetVal= %1i	SmLoginLogoutMessage::Sm-AuthAceInitProcessingFail	이 메시지는 SecurID 인증 체계에서 ACE/SecurID API 를 초기화하지 못할 경우에 발생합니다. 인증 체계는 요청을 거부하고 인증이 실패합니다.
SmAuthenticate:Did not continue to AceCheck. aceRetVal= %1i	SmLoginLogoutMessage::Sm-AuthAceCheckDidNotContinue	이 오류 메시지는 SecurID 인증 체계에서 ACE/SecurID API 를 통한 ACE 인증 프로세스를 완료할 수 없는 경우에 발생합니다.
SmAuthenticate:Did not continue to AceInit completion. pEventData->asynchAceRet= %1i	SmLoginLogoutMessage::Sm-AuthAceInitCompletionFail	이 메시지는 SecurID 인증 체계에서 ACE/SecurID API 를 초기화하지 못할 경우에 발생합니다. 인증 체계는 요청을 거부하고 인증이 실패합니다.
SmAuthenticate:Name Lock Request has been denied by ACE/Server communication failure.	SmLoginLogoutMessage::Sm-AuthNameLockReqDenied	이 메시지는 SecurID 인증 체계에서 ACE/SecurID API 를 초기화하지 못할 경우에 발생합니다. 인증 체계는 요청을 거부하고 인증이 실패합니다.

메시지	Function	설명
SmAuthenticate:Thread Sync failed. wRet= %1ul	SmLoginLogoutMessage::Sm-AuthThreadSyncFail	이 메시지는 Windows 플랫폼의 SecurID 인증 체계에서 비동기 ACE API 에 대한 호출이 실패할 경우에 발생합니다.
SmAuthenticate:Unable to Lock the UserName. aceRetVal= %1i	SmLoginLogoutMessage::Sm-AuthUserNameLockFail	이 메시지는 SecurID 인증 체계에서 ACE 서버의 사용자 이름을 잠그지 못할 경우에 발생합니다. 이 경우 SiteMinder 인증 체계가 인증 요청을 거부합니다. 이름 잠금 기능은 RSA ACE 제품 버전 5.0 이상에서 사용할 수 있습니다. 이름 잠금 기능에 대한 자세한 내용은 RSA ACE 제품 설명서를 참조하십시오.
SmAuthUser - Failed to fetch Az Realm.	SmLoginLogoutMessage::Fetch-AzRealmFailed	"Application Role User"(응용 프로그램 역할 사용자) 속성을 가져올 때 사용자 영역을 찾지 못했습니다.
SmAuthUser - Failed to fetch Domain object.	SmLoginLogoutMessage::Fetch-DomainObjFailed	"Application Role User"(응용 프로그램 역할 사용자) 속성을 가져올 때 사용자 도메인을 찾지 못했습니다.
The new PIN can contain alpha-numeric characters only.	SmLoginLogoutMessage::Alpha-NumericOnlyNewPin	이 메시지는 HTML SecurID 인증 체계에서 사용자가 PIN 을 변경해야 하는데 영숫자가 아닌 문자가 포함된 PIN 을 입력할 경우에 사용됩니다.
The new PIN can contain digits only.	SmLoginLogoutMessage::Digit-OnlyNewPin	이 메시지는 HTML SecurID 인증 체계에서 사용자가 PIN 을 변경해야 하는데 숫자가 아닌 문자가 포함된 PIN 을 입력할 경우에 사용됩니다.
The new PIN is too long	SmLoginLogoutMessage::Long-NewPin	이 메시지는 HTML SecurID 인증 체계에서 사용자가 PIN 을 변경해야 하는데 새 PIN 이 너무 길 경우에 사용됩니다.

메시지	Function	설명
The new PIN is too short	SmLoginLogoutMessage::Short-NewPin	이 메시지는 HTML SecurID 인증 체계에서 사용자가 PIN 을 변경해야 하는데 새 PIN 이 너무 짧을 경우에 사용됩니다.
Unable to proceed PIN change, unknown PIN type.	SmLoginLogoutMessage::Ace-ServerUnableToProceedPin-Change	정보 제공 목적으로만 사용됩니다. ACE/SecurID 인증 체계와 관련하여 문제가 발생할 경우 기술 지원부에 이 메시지를 제공하십시오.
Unexpected Message ID found while looking for SmPasswordMsg_Change Password: %1ul	SmLoginLogout-Message::UnexpectedMessage-ID	로그인 요청을 처리하고 새 암호와 이전 암호를 분석할 때 암호 필드에 저장된 메시지 ID 를 알 수 없습니다.
Usage: %1s[:AppName]	SmLoginLogoutMessage::Usage-SmUserAttribFormat	"Application Role User"(응용 프로그램 역할 사용자) 속성의 형식을 올바르게 지정하기 위한 도움말 문자열입니다.
UserPIN not allocated.	SmLoginLogoutMessage::User-PinNotAllocated	SecurID 인증 체계에 사용됩니다. 사용자 PIN 에 대한 버퍼를 할당하지 못했습니다.
ValidateLoginAttempt - Error Applying Password Policy	SmLoginLogoutMessage::Error-ApplyingPasswordPolicy	로깅 시도의 유효성을 검사하는 중 암호 정책을 적용하지 못했습니다.
ValidateLoginAttempt - Error Fetching Password Policy	SmLoginLogoutMessage::Error-FetchingPasswordPolicy	로깅 시도의 유효성을 검사하는 중 PasswordPolicy 개체를 가져오지 못했습니다.
ValidateLoginAttempt - Error Finding Applicable Policies	SmLoginLogoutMessage::Error-FindingApplicablePolicy	로깅 시도의 유효성을 검사하는 중 적용 가능한 정책을 찾지 못했습니다.
ValidateNewPassword - Can't set password change info.	SmLoginLogoutMessage::Error-PasswordChange	암호 Blob 데이터를 업데이트하는 중 암호 정보를 설정하지 못했습니다.
ValidateNewPassword - Error fetching Match regular expressions	SmLoginLogoutMessage::Match-ExprFetchError	암호 정책에 대해 원하는 정규식을 가져오지 못했습니다.

메시지	Function	설명
ValidateNewPassword - Error fetching NoMatch regular expressions	SmLoginLogoutMessage::No-MatchExprFetchError	암호 정책에 대해 원하는 정규식을 가져오지 못했습니다.
ValidateNewPassword - Error fetching password policy	SmLoginLogoutMessage::Err-FetchingValidPwdPolicy	새 암호의 유효성을 검사하는 중 PasswordPolicy 개체를 가져오지 못했습니다.
ValidateNewPassword - Error finding applicable password policies.	SmLoginLogoutMessage::Err-FindingValidPwdPolicy	새 암호의 유효성을 검사하는 중 적용 가능한 정책을 찾지 못했습니다.
ValidateNewPassword could not load callout '%1s	'SmLoginLogoutMessage::Load-CalloutFail	암호 확인을 위해 외부 라이브러리를 로드하는 데 실패했습니다.
ValidateNewPassword failed to resolve function '%1s' in '%2s'. Error: %3s	SmLoginLogoutMessage::Err-ResolveFuncValidPwd	암호 확인을 위해 외부 라이브러리에서 메서드를 찾는 데 실패했습니다.

권한 부여

오류 메시지	Function	설명
Bad %1s request detected	SmIsAuthorizedMessage::Bad-RequestDetected	권한 부여 요청 메시지가 올바른 형식을 따르지 않습니다.
Cannot process active expression with variables without licensed eTelligent Options	SmIsAuthorizedMessage::CanNot-ProcessActiveExpr	eTelligent 규칙 기능에 대한 라이선스를 찾을 수 없습니다. 활성 식이 처리되지 않습니다.
Caught exception while adding variable	SmIsAuthorizedMessage::Exc-AddingVar	eTelligent 규칙 변수를 확인하는 중 소프트웨어 예외가 발생했습니다.
Exception in IsOk.	SmIsAuthorizedMessage::Unk-ExclnIsOK	권한 부여를 수행하는 중 알 수 없는 예외가 발생했습니다.

오류 메시지	Function	설명
Exception in IsOk. %1s	SmIsAuthorizedMessage::ExcIn-IsOK	권한 부여를 수행하는 중 예외가 발생했습니다.
Failed to Fetch Active Expression %1s	SmIsAuthorizedMessage::Failed-FetchActiveExpr	개체 저장소에서 활성 식 개체를 가져올 수 없습니다.
Failed to Load Active Expression %1s	SmIsAuthorizedMessage::Failed-LoadActiveExpr	활성 식을 로드할 수 없습니다.
Failed to Load Domain %1s	SmIsAuthorizedMessage::Failed-LoadDomain	eTelligent 규칙 변수를 처리하는 중 도메인 개체를 가져오지 못했습니다.
Failed to Load Variable %1s	SmIsAuthorizedMessage::Failed-LoadVar	지정된 eTelligent 규칙 변수를 가져오지 못했습니다.
Failed to Load Variable Type %1s	SmIsAuthorizedMessage::Failed-LoadVarType	지정된 변수의 유형을 가져오지 못했습니다.
Failed to Load Variables for Active Expression %1s	SmIsAuthorizedMessage::Failed-LoadVarActiveExpr	변수를 확인하는 중 문제가 발생하여 활성 식이 호출되지 않습니다.
Failed to Load Variables for active expression %1s	SmIsAuthorizedMessage::Failed-LoadVarsForActiveExpr	활성 식에 대한 eTelligent 규칙 변수를 로드하지 못했습니다.
Failed to resolve attribute %1s	SmIsAuthorizedMes-sage::FailedToResolveAttr	개체 저장소에서 응답 특성 개체를 가져올 수 없습니다.
Failed to resolve dictionary vendor attribute %1s	SmIsAuthorizedMes-sage::FailedToResolveDictVendAttr	공급업체 특성 사전에서 지정된 공급업체 특성을 찾을 수 없습니다.
Failed to resolve response %1s	SmIsAuthorizedMes-sage::FailedToResolveResponse	개체 저장소에서 응답 개체를 가져올 수 없습니다.
Failed to resolve response group %1s	SmIsAuthorizedMes-sage::FailedToResolveResponseGp	개체 저장소에서 응답 그룹 개체를 가져올 수 없습니다.
Failed to resolve user policy %1u	SmIsAuthorizedMes-sage::FailedToResolveUserPolicy	개체 저장소에서 사용자 정책 개체를 가져올 수 없습니다.

오류 메시지	Function	설명
Ignoring variable response - no license for eTelligent Options	SmIsAuthorizedMessage::No-eTelligentLicense	eTelligent 규칙 기능에 대한 라이선스를 찾지 못했습니다. 변수가 처리되지 않습니다.
Invalid response attribute %1s. Dictionary conflict - attribute may not be in the response	SmIsAuthorizedMessage::Invalid-ResponseAttr	잘못된 응답 특성이 권한 부여 응답에 포함되지 않았습니다.
IsOk failed. %1s	SmIsAuthorizedMessage::IsOK-Failed	권한 부여 검사에 실패했습니다.

서버

메시지	Function	설명
Failed to initialize TCP server socket: Socket error:%1i	SmServerMessage::TCP-ServerSocketInitFail	소켓 오류에 대한 자세한 내용은 운영 체제 설명서를 참조하십시오. 가장 일반적인 오류는 시스템에서 이미 사용 중인 소켓을 열려고 하거나 소켓에 대한 충분한 권한이 없는 경우에 발생합니다.
Failed to initialize UDP server socket on port: %1ul. Socket error:%2i	SmServerMessage::UDP-ServerSocketInitFailOnPort	소켓 오류에 대한 자세한 내용은 운영 체제 설명서를 참조하십시오. 가장 일반적인 오류는 시스템에서 이미 사용 중인 소켓을 열려고 하거나 소켓에 대한 충분한 권한이 없는 경우에 발생합니다.
Failed to initialize WinSock library	SmServerMessage::WinSock-LibInitFail	(Windows 시스템) Windows 소켓 라이브러리를 초기화할 수 없습니다. 해당 라이브러리가 설치되어 있고 지원되는 버전인지 확인하십시오.

메시지	Function	설명
Failed to listen on TCP server socket. Socket error %1i	SmServerMessage::TCP-ServerSocketListenFail	소켓 오류에 대한 자세한 내용은 운영 체제 설명서를 참조하십시오. 가장 일반적인 오류는 시스템에서 이미 사용 중인 소켓을 열려고 하거나 소켓에 대한 충분한 권한이 없는 경우에 발생합니다.
Failed to load event handler	SmServerMessage::Event-HandlerLoadFail	이벤트 처리기 라이브러리를 로드할 수 없습니다. 구성된 이벤트 처리기의 경로 이름과 액세스 권한을 확인하십시오.
Failed to load library '%1s'. Error: %2s	SmServerMessage::FailedTo-LoadLib	보고된 인증 체계 라이브러리를 로드할 수 없습니다. 제공되는 오류 텍스트에 문제에 대한 설명이 없으면 명명된 라이브러리가 있으며 파일 시스템 보호 기능에서 액세스를 허용하는지 확인하십시오.
Failed to locate required entry point(s) in event provider '%1s'	SmServerMessage::Req-EntryPointInEventProvider-LocateFail	명명된 라이브러리가 올바른 이벤트/감사 로그 공급자가 아닙니다.
Failed to write audit log record. Record dropped.	CSmReports::LogAccess	정책 서버가 감사 로그에 기록할 수 없습니다. 감사 로그 저장소의 상태를 확인하십시오.
Failed to obtain host name. Socket error %1i	SmServerMessage::Host-NameObtainError	감사 로거 공급자가 로컬 시스템의 네트워크 호스트 이름을 가져올 수 없습니다. 네트워크 오류 때문일 수 있습니다. 제공되는 오류 코드(UNIX 시스템의 경우 errno, Windows 시스템의 경우 SOCKET_ERROR)에서 상세 정보를 얻을 수 있습니다.

메시지	Function	설명
Failed to obtain host name. Socket error %1i	SmServerMessage::Host-NameObtainFail	로컬 시스템의 네트워크 호스트 이름을 가져올 수 없습니다. 네트워크 오류 때문일 수 있습니다. 제공되는 오류 코드(UNIX 시스템의 경우 errno, Windows 시스템의 경우 SOCKET_ERROR)에서 상세 정보를 얻을 수 있습니다.
Failed to open Audit log file for append '%1s'	SmServerMessage::Audit-LogFileAppendFail	감사 로거 공급자가 항목을 추가하기 위해 명명된 파일을 열 수 없습니다. 제공된 경로 이름이 유효하고 파일 액세스 권한이 올바른지 확인하십시오.
Failed to open RADIUS log file (no file defined)	SmServerMessage::Radius-LogFileNotDefined	레지스트리에 RADIUS 로그 파일의 이름에 대한 항목이 없거나 이름이 빈 문자열입니다.
Failed to open RADIUS log file: %1s	SmServerMessage::Radius-LogFileOpenFail	지정된 이름의 RADIUS 로그 파일을 덮어쓰거나(이미 있는 경우) 생성(아직 없는 경우)하기 위해 열 수 없습니다. 디렉터리 및 파일(있는 경우)에 대한 액세스 권한을 확인하십시오.
Failed to query authentication scheme '%1s'	SmServerMessage::Fail-QueryAuthScheme	정책 서버에서 지정된 인증 체계를 쿼리하지 못해 인증 체계를 초기화할 수 없습니다.

메시지	Function	설명
Failed to read on UDP socket. Socket error %1i	SmServerMessage::UDP-SocketReadFail	관리 서비스 연결 요청이나 RADIUS 메시지를 전달하는 UDP 패킷을 읽는 중 정책 서버가 예기지 않은 네트워크 오류를 감지했습니다. 제공되는 오류 코드(UNIX 시스템의 경우 errno, Windows 시스템의 경우 SOCKET_ERROR)에서 상세 정보를 얻을 수 있습니다.
Failed to receive request on session # %1i : %2s/%3s:%4i. Socket error %5s	SmServerMessage::Request-ReceiveOnSessionFail	지정된 세션에서 에이전트 요청을 읽는 중 정책 서버가 예기치 않은 네트워크 오류를 감지하여 연결을 닫았습니다. 제공되는 오류 코드(UNIX 시스템의 경우 errno, Windows 시스템의 경우 SOCKET_ERROR)에서 상세 정보를 얻을 수 있습니다.
Failed to resolve agent key '%1s'	SmServerMessage::Unresolved-AgentKey	에이전트 키가 업데이트될 때 정책 저장소에서 보고된 에이전트 키를 찾을 수 없습니다.
Failed to resolve agent keys	SmServerMessage::FailTo-ResolveAgentKeys	에이전트 키 업데이트를 위해 정책 저장소의 에이전트 키에 액세스할 수 없습니다.
Failed to resolve agent keys	SmServerMessage::Agent-KeysResolveFail	에이전트 키 업데이트를 위해 정책 저장소의 에이전트 키에 액세스할 수 없습니다.
Failed to resolve agent keys '%1s'	SmServerMessage::Fail-ToResolveAgentKey	에이전트 키가 업데이트될 때 정책 저장소에서 보고된 에이전트 키를 찾을 수 없습니다.
Failed to resolve Agent or AgentGroup %1s	SmServerMessage::Agent-OrAgentGroupResolveFail	지정된 에이전트 또는 에이전트 그룹이 없거나 해당 정책 저장소 레코드가 손상되었습니다.

메시지	Function	설명
Failed to resolve all domains	SmServerMessage::Domain-ResolutionFailed	정책 저장소의 도메인 루트 개체 레코드가 누락되었거나 손상되었습니다.
Failed to resolve all vendors. No vendor dictionary will be created.	SmServerMessage::Failed-ToResolveVendors	정책 저장소의 공급업체 루트 개체 레코드가 누락되었거나 손상되었습니다.
Failed to resolve auth-az mapping %1s	SmServerMessage::Fail-ToResolveAuthAzMap	지정된 Auth-Az 맵이 없거나 해당 정책 저장소 레코드가 손상되었습니다.
Failed to resolve function '%1s' in '%2s' . Error: %3s	SmServerMessage::Failed-ToResolveFunc	지정된 인증 체계 라이브러리에서 보고된 진입점을 확인할 수 없어(제공되는 오류 텍스트 참조) 라이브러리가 로드되지 않았습니다.
Failed to resolve function '%1s' in '%2s'. Error: %3s	SmServerMessage::Function-ResolveFail	지정된 TransactEMS 라이브러리에서 보고된 진입점을 확인할 수 없어(제공되는 오류 텍스트 참조) 라이브러리가 로드되지 않았습니다.
Failed to resolve function '%1s' in '%2s'. Error: %3s	SmServerMessage::Fail-ToResolveFunction	시스템 구성 정보를 보고하는 지정된 라이브러리에서 보고된 진입점을 확인할 수 없어(제공되는 오류 텍스트 참조) 라이브러리가 로드되지 않았습니다.
management object	SmServerMessage::Key-ManagementObjResolveFail	정책 서버가 정책 저장소에서 키 관리 개체를 읽으려고 할 때 오류가 감지되었습니다.
Failed to resolve key management object	SmServerMessage::Resolve-KeyMgmtObjFail	정책 저장소에서 에이전트 키 관리 개체를 읽을 수 없습니다.

메시지	Function	설명
Failed to resolve key management object '%1s'	SmServerMessage::Key-ManagementObjResolve-FailwithVal	에이전트 키 관리 스레드가 정책 저장소에서 지정된 에이전트 키 관리 개체를 읽으려고 할 때 오류가 감지되었습니다.
Failed to resolve list of auth-az mappings	SmServerMessage::Fail-ToResolveAuthAzMapList	정책 저장소의 Auth-Az 맵 루트 개체 레코드가 누락되었거나 손상되었습니다.
Failed to resolve log file name	SmServerMessage::Log-FileNameRosolveFail	감사 로거 공급자가 레지스트리에서 로그 파일의 이름을 가져올 수 없습니다. 파일 이름이 구성되었는지 확인하십시오.
Failed to resolve shared secret policy object	SmServerMessage::Shared-SecretResolveFail	정책 저장소의 공유 암호 롤오버 정책 개체 레코드가 누락되었거나 손상되었습니다.
Failed to resolve user directory %1s	SmServerMessage::Fail-ToResolveUserDir	지정된 사용자 디렉터리 개체가 없거나 해당 정책 저장소 레코드가 손상되었습니다.
Failed to resolve user identity. Denying access.	SmServerMessage::User-IdentityFail	적용 가능한 영역의 정책을 검색하는 중 오류가 발생하여 사용자 아이덴티티를 확인하지 못했으며 액세스가 거부되었습니다.
Failed to resolve Version 6 function '%1s' in '%2s' . Error: %3s	SmServerMessage::Failed-ToResolveVer6Func	지정된 버전 6 인증 체계 라이브러리에서 보고된 진입점을 확인할 수 없어(제공되는 오류 텍스트 참조) 라이브러리가 사용되지 않습니다. 인증 체계가 이전 버전이 아닌지 확인하십시오.

메시지	Function	설명
Failed to retrieve audit log flush interval. Setting to infinite	SmServerMessage::Audit-LogFlushIntervalRetrieveFail	감사 로거 ODBC 공급자가 레지스트리에서 플러시 간격을 가져올 수 없습니다. 간격이 구성되었는지 확인하십시오.
Failed to retrieve audit log provider library for namespace '%1s'	SmServerMessage::AuditLog-ProviderLibRetrieveFail	레지스트리에 지정된 감사 로그 공급자 네임스페이스에 대한 라이브러리 이름 항목이 없습니다.
Failed to retrieve audit log row flush count. Setting to 1000	SmServerMessage::Audit-LogRowFlushCountRetrieveFail	레지스트리에 비동기 로깅을 위한 ODBC 감사 로그 공급자의 행 플러시 횟수에 대한 항목이 없어 기본값 1000 이 사용됩니다.
Failed to retrieve message from the message queue	SmServerMessage::Retrieve-FromMessageQueueFail	(Windows) 정책 서버 프로세스가 Windows 응용 프로그램 큐에서 메시지를 가져오려고 할 때 오류가 발생했습니다.
Failed to rollover trusted host shared secrets	SmServerMessage::Trusted-HostSharedSecretsRolloverFail	트러스트된 호스트 공유 암호를 롤오버하는 중 오류가 발생했습니다. 롤오버 정책이 유효한지 확인하십시오.
Failed to save key management object	SmServerMessage::Save-NewMgmtKeyObjFail	새 영구 키를 저장할 때 정책 저장소에서 에이전트 키 관리 개체를 읽지 못했습니다.
Failed to save key management object after key update	SmServerMessage::Save-NewMgmtKeyObjAfter-KeyUpdateFail	정책 서버가 롤오버를 위한 새 에이전트 키를 생성했지만 해당 에이전트 키를 사용할 수 있는 것으로 기록하지 못했습니다.
Failed to save key management object after persistent key update	SmServerMessage::Save-NewMgmtKeyObjAfter-PersistentKeyUpdateFail	새 영구 키를 정책 저장소의 에이전트 키 관리 개체에 저장할 수 없습니다.

메시지	Function	설명
Failed to save key management object after session key update	SmServerMessage::Save-NewMgmtKeyObjAfterSession-KeyUpdateFail	새 에이전트 세션 키를 정책 저장소에 저장할 수 없습니다.
Failed to save new 'current' agent key '%1s'	SmServerMessage::Save-NewCurrentAgentKeyFail	지정된 에이전트 세션 키를 에이전트의 "현재" 키로 저장할 수 없습니다.
Failed to save new key management object	SmServerMessage::Agent-KeyManagementObjSaveFail	에이전트 키 관리 스레드가 롤오버를 위한 새 에이전트 키를 생성했지만 해당 에이전트 키를 사용할 수 있는 것으로 기록하지 못했습니다.
Failed to save new 'last' agent key '%1s'	SmServerMessage::Save-NewLastAgentKeyFail	지정된 에이전트 세션 키를 정책 저장소에 에이전트의 "마지막" 키로 저장할 수 없습니다.
Failed to save new 'next' agent key '%1s'	SmServerMessage::Save-NewNextAgentKeyFail	지정된 에이전트 세션 키를 정책 저장소에 에이전트의 "다음" 키로 저장할 수 없습니다.
Failed to save new persistent agent key '%1s'	SmServerMessage::Failed-ToSaveNewPersistentAgentKey	지정된 영구 에이전트 키를 정책 저장소에 저장할 수 없습니다.
Failed to send response on session # %1i : %2s/%3s:%4i. Socket error %5i	SmServerMessage::Response-SendOnSessionFail	네트워크 오류(또는 에이전트 오류)로 인해 지정된 세션의 에이전트 요청에 대한 응답을 보낼 수 없습니다. 제공되는 오류 코드(UNIX 시스템의 경우 errno, Windows 시스템의 경우 SOCKET_ERROR)에서 상세 정보를 얻을 수 있습니다.

메시지	Function	설명
Failed to start agent command management watchdog thread	SmServerMessage::Agent-CommandManagementThread-CreationFail	에이전트 명령 관리 스레드가 실행 중인지 확인하는 "watchdog" 스레드를 시작하지 못했습니다. 운영 체제에서 최대 스레드 수와 열려 있는 파일 설명자의 최대 수에 대해 구성된 프로세스별 제한을 확인하십시오.
Failed to start journal management thread	SmServerMessage::Journal-ThreadCreateFail	"watchdog" 스레드가 정책 저장소 저널 정리 관리 스레드를 시작(다시 시작)할 수 없습니다. 운영 체제에서 최대 스레드 수와 열려 있는 파일 설명자의 최대 수에 대해 구성된 프로세스별 제한을 확인하십시오.
Failed to start journal management watchdog thread	SmServerMessage::Journal-ManagementThreadFail	정책 저장소 저널 관리 정리 스레드가 실행 중인지 확인하는 "watchdog" 스레드를 시작하지 못했습니다. 운영 체제에서 최대 스레드 수와 열려 있는 파일 설명자의 최대 수에 대해 구성된 프로세스별 제한을 확인하십시오.
Failed to start key management thread	SmServerMessage::AgentKey-ThreadCreateFail	"watchdog" 스레드가 에이전트 키 관리 스레드를 시작(다시 시작)할 수 없습니다. 운영 체제에서 최대 스레드 수와 열려 있는 파일 설명자의 최대 수에 대해 구성된 프로세스별 제한을 확인하십시오.

메시지	Function	설명
Failed to start key management watchdog thread	SmServerMessage::Key-ManagementThreadCreateFail	에이전트 키 관리 스레드가 실행 중인지 확인하는 "watchdog" 스레드를 시작하지 못했습니다. 운영 체제에서 최대 스레드 수와 열려 있는 파일 설명자의 최대 수에 대해 구성된 프로세스별 제한을 확인하십시오.
Failed to start main reactor thread	SmServerMessage::Main-ReactorThreadStartFail	네트워크 IO 디스패처 스레드를 시작하지 못했습니다. 운영 체제에서 최대 스레드 수와 열려 있는 파일 설명자의 최대 수에 대해 구성된 프로세스별 제한을 확인하십시오.
Failed to start object store journal thread	SmServerMessage::Journal-StartFailed	"watchdog" 스레드가 정책 저장소 저널 관리 스레드를 시작(다시 시작)할 수 없습니다. 운영 체제에서 최대 스레드 수와 열려 있는 파일 설명자의 최대 수에 대해 구성된 프로세스별 제한을 확인하십시오.
Failed to start object store watchdog thread	SmServerMessage::Watchdog-Failed	정책 저장소 저널 관리 스레드가 실행 중인지 확인하는 "watchdog" 스레드를 시작하지 못했습니다. 운영 체제에서 최대 스레드 수와 열려 있는 파일 설명자의 최대 수에 대해 구성된 프로세스별 제한을 확인하십시오.

메시지	Function	설명
Failed to stat management command channel	SmServerMessage::Stat-MangmCmdChannelFail	(Unix/Linux) 기존 서버 명령 관리 파이프/파일의 stat()이 예기치 않게 실패했습니다. 서버 명령 관리 스레드도 시작하지 못한 경우 실행 중인 다른 정책 서버 프로세스가 없는지 확인하고 파이프/파일을 수동으로 삭제하십시오.
Failed to update agent keys	SmServerMessage::FailTo-UpdateAgentKeys	에이전트가 에이전트 키를 업데이트하는 관리자 명령을 정책 저장소에 저장할 수 없습니다.
Failed to update agent keys from server command	SmServerMessage::Failed-ToUpdateAgentKeys	에이전트의 새로운 "현재" 또는 "다음" 세션 키를 정책 저장소에 저장할 수 없습니다.
Failed to update changes agent keys	SmServerMessage::Fail-ToUpdateChangesToAgentKeys	에이전트가 에이전트 키를 업데이트하는 명령을 정책 저장소에 저장할 수 없습니다.
Failed to update persistent key	SmServerMessage::Failed-ToUpdatePersistentKey	에이전트의 영구 키를 정책 저장소에 저장할 수 없습니다.
Failed to write on UDP socket. Socket error %1i	SmServerMessage::UDP-SocketWriteFail	네트워크 오류(또는 에이전트 오류)로 인해 관리 GUI 초기화 패킷 또는 RADIUS 응답 패킷을 보낼 수 없습니다. 제공되는 오류 코드(UNIX 시스템의 경우 errno, Windows 시스템의 경우 SOCKET_ERROR)에서 상세 정보를 얻을 수 있습니다.
file not found	SmServerMessage::File-NotFound	(Windows 시스템) OneView 모니터를 시작하는 서비스가 bin\smmon.bat 파일을 읽을 수 없습니다.

메시지	Function	설명
Getting processor affinity failed	SmServerMessage::Get-ProcessorAffinityFail	(Windows) 프로세서 선호도에 대한 성능 조정 매개 변수를 처리할 수 없으므로 기존 선호도 설정이 변경되지 않습니다.
Handshake error: Unknown client name '%1s' in hello message	SmServerMessage::Handshake-ErrorUnknownClient	연결을 시도할 때 클라이언트가 보고된 이름을 제공했지만 해당 이름의 에이전트를 정책 저장소에서 찾을 수 없습니다. 이 메시지는 에이전트가 잘못된 공유 암호를 사용하는 경우에도 발생합니다.
Inconsistent agent key marker (%1i)	SmServerMes-sage::InconsistentAgent-KeyMarker	정책 저장소의 에이전트 키 레코드에 지정된 것과 같은 인식할 수 없는 키 유형이 있습니다.
Inconsistent number of agent keys (%1i)	SmServerMes-sage::InconsistentNumberOf-AgentKeys	정책 저장소에 포함된 에이전트 키 수가 지정된 것과 같이 올바르지 않습니다.
Internal error computing realm list. Denying access.	SmServerMessage::Realm-Corrupt	액세스 권한 부여를 수행하기 위해 영역 목록을 가져오는 중 예기치 않은 정책 저장소 오류가 발생하여 액세스가 거부되었습니다.
Invalid agent key marker (%1i)	SmServerMessage::Invalid-AgentKeyMarker	정책 저장소의 에이전트 키 레코드에 지정된 것과 같은 인식할 수 없는 키 유형이 있습니다.
IP address resource filter not yet suppported by IsOk	SmServerMessage::IPAddr-ResourceFilterNotSupported	영역에서 일치하는 작업 규칙이 일치하는 IP 주소 또는 범위를 지원하지 않습니다.

메시지	Function	설명
IsInDictionary - Could not add Password Dictionary to holder %1s	SmServerMessage::Add-PasswordDictToHolderFailed	명명된 암호 사전을 캐시할 수 없습니다. 사전은 100 개까지만 캐시할 수 있기 때문일 수 있습니다. 사전의 항목과 일치하는지 확인하려는 암호는 일치하는 것으로 간주됩니다.
IsInDictionary - Could not create Password Dictionary %1s	SmServerMessage::Create-PasswordDictFailed	명명된 암호 사전을 캐시하기 위해 준비하는 중 예기치 않은 오류가 발생했습니다. 메모리가 부족하기 때문일 수 있습니다. 사전의 항목과 일치하는지 확인하려는 암호는 일치하는 것으로 간주됩니다.
IsInDictionary - Could not set the Password Dictionary %1s	SmServerMessage::Set-PasswordDictFailed	명명된 암호 사전을 캐시하는 중 오류가 발생했습니다. 사전의 항목과 일치하는지 확인하려는 암호는 일치하는 것으로 간주됩니다.
IsInDictionary - Password Dictionary not open %1s	SmServerMessage::Open-PasswordDictFailed	지정된 암호 사전이 로드되었지만 예기치 않게 열리지 않습니다. 사전의 항목과 일치하는지 확인하려는 암호는 일치하지 않는 것으로 간주됩니다.
IsInProfileAttributes - Error fetching property names	SmServerMessage::Fetching-PropertyNameFail	암호와 사용자 프로필 특성 값을 비교하는 중 사용자 특성 이름을 가져올 수 없어 암호가 일치하는 것으로 간주됩니다.
IsInProfileAttributes - Error fetching property values	SmServerMessage::Fetching-PropertyValueFail	암호와 사용자 프로필 특성 값을 비교하는 중 특성 값을 가져올 수 없어 암호가 일치하는 것으로 간주됩니다.

메시지	Function	설명
Monitor request for unrecorded data, Null values returned	SmServerMessage::MonReq-UnrecordedDataNullValue	정책 서버가 모니터링되는 데이터에 대한 요청에서 전달된 이름을 인식하지 못했습니다.
No agent encryption keys found	SmServerMessage::Agent-EncryptionKeyNotFound	정책 저장소에서 에이전트의 키 집합을 가져올 때 전체 집합을 찾지 못했습니다.
No agent keys in key store	SmServerMessage::AgentKey-NotFoundInKeyStore	정책 저장소의 에이전트 키를 업데이트하는 중 에이전트 키를 전혀 찾지 못했습니다.
No initial agent keys	SmServerMessage::Empty-AgentKeys	정책 저장소에 에이전트 키가 없고 키 생성이 사용되도록 설정되어 있지 않습니다.
No initial key management object found. This policy server is configured in read-only key management mode. Unable to proceed	SmServerMessage::Key-ManagementObjNotFound	정책 저장소에 초기 에이전트 키 관리 개체가 없고 키 생성이 사용되도록 설정되어 있지 않습니다.
No namespace available for the audit log provider	SmServerMessage::No-NamespaceAvailForAudit-LogProvider	레지스트리에 감사 로그 공급자 네임스페이스에 대한 항목이 없습니다.
No Root Config object found, Please run smobjimport to import smpolicy.smdif!	SmServerMessage::Root-ConfigObjNotFound	정책 저장소가 초기화되지 않았습니다.
No session pointer while processing request %1s	SmServerMessage::Null-SessionPointer	지정된 에이전트 요청을 받았지만 해당하는 에이전트 세션 개체가 찾을 수 없거나 유효하지 않아 요청 패킷이 처리되지 않고 반환되었습니다.

메시지	Function	설명
Please check file permissions or path for validity	SmServerMessage::File-PermissionOrPathCheck	파일을 열 수 없습니다. 이 메시지보다 먼저 나타난 파일 경로 이름을 제공하는 오류 메시지에서 제공된 경로 이름이 유효하고 파일 액세스 권한이 올바른지 확인하십시오.
Policy Server caught exception in ProcessMessage. (no message text)	SmServerMessage::Unknown-PolSrvExcpCaught	에이전트 요청을 처리하는 중 정책 서버에서 예기치 않은 예외가 발생하여 빈 응답이 반환되었습니다.
Policy Server caught exception in ProcessMessage. Text: %1s	SmServerMessage::PolSrv-ExcpCaught	에이전트 요청을 처리하는 중 정책 서버에서 예기치 않은 예외가 발생하여 빈 응답이 반환되었습니다. 제공되는 텍스트에 권장되는 수정 방법이 있을 수 있습니다.
Policy store failed operation '%1s' for object type '%2s' . %3s	SmServerMessage::Policy-StoreOperFail	정책 저장소 개체 계층에서 설명된 예외가 발생했습니다.
Processor affinity left at default setting, cannot set affinity to zero	SmServerMessage::Processor-AffinitySetZeroFail	(Windows) 0 은 프로세서 선호도에 대한 성능 조정 매개 변수 값으로 유효하지 않으므로 기존 선호도 설정이 변경되지 않습니다.
Reject %1s : Failed to write access log	SmServerMessage::Write-FailInAccessLog	거부된 특정 인증 또는 권한 부여 요청에 대한 감사 로깅이 실패했습니다.
Saw agent name in DoManagement() command %1s, request %2s	SmServerMessage::Agent-NameInDoManagement	"Do Management" 에이전트 명령이 거부되었습니다.
Saw agent name in Logout() command %1s , request %2s	SmServerMessage::Agent-NameInLogout	로그아웃 요청이 거부되었습니다.

메시지	Function	설명
Setting processor affinity failed	SmServerMessage::Set-ProcessorAffinityFail	(Windows) 프로세서 선호도에 대한 성능 조정 매개 변수를 처리할 수 없으므로 기존 선호도 설정이 변경되지 않습니다.
SM exception caught during initialization (%1s)	SmServerMessage::SMExcp-DuringInit	정책 서버가 "GlobalInit" 단계를 시작하는 중 예외가 발생하여 시작 작업이 실패했습니다. 제공되는 텍스트에 상세 정보가 있을 수 있습니다.
SM exception caught during server shutdown (%1s)	SmServerMessage::SMExcp-DuringServerShutdown	정책 서버가 "GlobalRelease" 단계를 종료하는 중 예외가 발생했습니다. 제공되는 텍스트에 상세 정보가 있을 수 있습니다.
TCP port initialization failure	SmServerMessage::TCP-PortInitFail	정책 서버를 시작하는 중 액세스 제어 또는 관리 요청에 사용되도록 설정된 TCP 포트를 초기화할 수 없어 시작 작업이 종료되었습니다.
The service loader failed to start %1s. Error %2i %3s	SmServerMes-sage::SZSERVER_StartFail	(Windows) 서비스 로더를 시작할 수 없어(오류 텍스트 참조) 정책 서버 또는 OneView 모니터를 시작할 수 없습니다.
This policy server does not have a session encryption 키	SmServerMessage::Session-EncryptKeyNotFound	정책 서버에 초기 세션 키가 없고 키 생성이 사용되도록 설정되어 있지 않습니다. 액세스 제어 요청이나 관리 요청이 처리되도록 구성된 경우 시작 작업이 종료됩니다.
Thread Pool thread caught exception	SmServerMessage::ExcpIn-ThreadPool	예기치 않은 상황으로 인해 정책 서버 작업자 스레드가 종료되었습니다. 대체 스레드가 스레드 풀에 추가됩니다.

메시지	Function	설명
UDP port initialization failure	SmServerMessage::UDPPort-InitFail	정책 서버를 시작하는 중 관리 또는 RADIUS 요청에 사용되도록 설정된 UDP 포트를 초기화할 수 없어 시작 작업이 종료되었습니다.
UDP processing exception.	SmServerMessage::UDP-ProcessingExcp	관리 GUI 초기화 패킷 또는 RADIUS 응답 패킷을 처리하는 중 예기치 않은 오류가 발생했습니다. No response is sent.
Unable to create console output collector. Tracing will not be enabled	SmServerMessage::Trace-NotEnableConsoleOutput-CollecCreateFail	정책 서버 프로세스가 프로파일러(추적) 로그 출력에 대한 출력 대상인 콘솔(또는 터미널 창)에 액세스할 수 없습니다. 콘솔을 열 수 있는 적절한 액세스 권한이 있는지 확인하십시오.
Unable to create file output collector. Tracing will not be enabled	SmServerMessage::Trace-NotEnableFileOutput-CollecCreateFail	프로파일러(추적) 로그 파일을 덮어쓰거나(이미 있는 경우) 생성(아직 없는 경우)하기 위해 열 수 없습니다. 디렉터리 및 파일(있는 경우)에 대한 액세스 권한을 확인하십시오.
Unable to create shared secret rollover policy object	SmServerMessage::Shared-SecretCreateFail	정책 서버를 시작하는 중 정책 저장소에서 공유 암호 정책 개체를 찾을 수 없어 초기 정책 개체를 생성하는 데 실패했으므로 시작 작업이 종료되었습니다.
Unable to enable tracing	SmServerMessage::Trace-NotEnable	프로파일러(추적) 로깅의 초기 설정에 성공했지만 나머지 설정에는 성공하지 못했습니다.

메시지	Function	설명
Unable to reset logger options dynamically	SmServerMessage::Dynamic-LoggerResetFail	정책 서버가 실행 중일 때 로거 구성 옵션이 변경되었음을 감지하는 스레드를 시작할 수 없으므로 정책 서버가 다시 시작될 때까지 해당 변경 내용이 적용되지 않습니다.
Unable to resolve agent for request %1s	SmServerMessage::Unresolved-AgentIdentity	에이전트 요청에 에이전트 아이덴티티를 포함해야 하지만 에이전트 아이덴티티를 확인할 수 없습니다. 요청이 거부되었습니다.
Unable to resolve agent name %1s , request %2s	SmServerMessage::AgentName-UnResolved	에이전트 요청에 에이전트 아이덴티티를 포함해야 하지만 명명된 에이전트에 대해 에이전트 아이덴티티를 확인할 수 없습니다. 요청이 거부되었습니다.
Unable to update password blob data	SmServerMessage::Blob-UpdateFailed	암호 서비스에 대한 사용자의 "암호 Blob" 데이터를 사용자 저장소에서 업데이트할 수 없습니다. 이렇게 구성된 경우 정책 서버는 사용자의 인증 시도를 거부합니다.
Unexpected exception while publishing AZ Libs	SmServerMes-sage::UnexpectedException-PublishingAzLibs	로드된 사용자 지정 권한 부여 모듈에 대한 정보에서 진단 "게시" 정보를 쿼리하는 중 예기치 않은 예외가 발생하여 사용자 지정 권한 부여 라이브러리에 대한 정보가 게시되지 않습니다.
Unknown agent key type %1i	SmServerMessage::Agent-KeyTypeUnknown	"Do Management" 요청을 처리하는 중 정책 저장소에서 인식할 수 없는 특정 키 유형의 에이전트 키 레코드가 발견되어 요청이 거부되었습니다.

메시지	Function	설명
Unknown Exception caught while publishing Auth Libs	SmServerMessage::Unknown-ExcpPublishAuthLibs	사용자 지정 인증 체계에서 진단 "게시" 정보를 쿼리하는 중 예기치 않은 예외가 발생하여 로드된 사용자 지정 인증 체계에 대한 정보가 게시되지 않습니다.
Unknown exception caught while publishing Event Lib info	SmServerMessage::Unknown-ExcpWhilePublishEventLibInfo	사용자 지정 이벤트 처리기 라이브러리에서 진단 "게시" 정보를 쿼리하는 중 예기치 않은 예외가 발생하여 SiteMinder 가 로드한 사용자 지정 이벤트 라이브러리에 대한 정보가 게시되지 않습니다.
Socket Error 104	104 - A call to bind() function failed.	TLI 계층을 통해 메시지를 보낼 때 오류가 발생하면 이 메시지가 반환됩니다.

Java API

오류 메시지	Function	설명
%1s could not fetch administrator directory	SmJavaApiMes-sage::AdministratorDirectory-FetchFail	등록 관리자 사용자 디렉터리를 가져올 수 없습니다. 정책 저장소를 확인하십시오.
%1s could not fetch registration directory	SmJavaApiMes-sage::RegistrationDirectory-FetchFail	등록 사용자 디렉터리를 가져올 수 없습니다. 정책 저장소를 확인하십시오.
%1s could not fetch registration domain	SmJavaApiMes-sage::RegistrationDomain-FetchFail	등록 도메인을 가져올 수 없습니다. 정책 저장소를 확인하십시오.
%1s could not fetch registration realm	SmJavaApiMes-sage::RegistrationRealm-FetchFail	등록 영역을 가져올 수 없습니다. 정책 저장소를 확인하십시오.

오류 메시지	Function	설명
%1s could not fetch registration scheme	SmJavaApiMes-sage::RegistrationScheme-FetchFail	등록 체계를 가져올 수 없습니다. 정책 저장소를 확인하십시오.
%1s invalid realm oid (null)	SmJavaApiMessage::Invalid-RealmOid	영역 OID 를 가져올 수 없습니다. 사용자 로그인이 성공했고 유효한 세션 ID 를 사용할 수 있는지 확인하십시오.
(CSmEmsCommand::Set-ObjectClasses) Could not rollback properties of directory user %1s after setting properties failed	SmJavaApiMessage::Csm-EmsSetObjectClasses-RollBackPropertiesFail	새 값이 거부된 후 사용자의 속성을 재설정할 수 없습니다. 사용자 저장소가 올바르게 작동 중이고 정책 서버가 연결을 설정할 수 있는지 확인하십시오.
(CSmEmsCommand::Set-Properties) Could not rollback properties of directory user %1s after setting properties failed.	SmJavaApiMessage::CSm-EmsSetPropertiesRollback-PropertiesFail	새 값이 거부된 후 사용자의 속성을 재설정할 수 없습니다. 사용자 저장소가 올바르게 작동 중이고 정책 서버가 연결을 설정할 수 있는지 확인하십시오.
(CSmEmsCommandV2::Set-ObjectClasses) Could not rollback properties of directory user %1s after setting properties failed.	SmJavaApiMessage::Set-ObjectClassesDir-UserRollbackFail	새 값이 거부된 후 사용자의 속성을 재설정할 수 없습니다. 정책 저장소에 정의된 디렉터리 연결을 확인하십시오.
(CSmEmsCommandV2::Set-Properties) Could not rollback properties of directory object %1s after setting properties failed.	SmJavaApiMessage::Set-PropertiesDirObjRollbackFail	새 값이 거부된 후 개체의 속성을 재설정할 수 없습니다. 정책 저장소에 정의된 디렉터리 연결을 확인하십시오.
Exception in Transact SessionTimeoutThread.	SmJavaApiMessage::Unknown-ExcpTransactSessionTimeout-Thread	만료된 세션을 처리하는 중 알 수 없는 오류가 발생했습니다.
Exception in Transact SessionTimeoutThread. Msg: %1s	SmJavaApiMessage::Excp-TransactSessionTimeoutThread	만료된 세션을 처리하는 중 오류가 발생했습니다.
Failed to create EmsSession Timeout Thread	SmJavaApiMessage::Ems-SessionTimeoutThread-CreateFail	새 스레드를 생성하기에 충분한 시스템 리소스가 없습니다.

오류 메시지	Function	설명
Failed to resolve all domains	SmJavaApiMessage::Domain-ResolveFail	현재 관리자와 관련된 모든 도메인을 가져오는 중 문제가 발생했습니다. Check for Policy Store corruption.
getUsersDelegatedRoles failed, error = %1s	SmJavaApiMessage::IMSget-UsersDelegatedRolesFail	이 사용자에 대한 역할을 가져올 수 없습니다. smobjims.dll(libsmobjims.so) 라이브러리가 설치되어 있는지 확인하십시오.
getUsersDelegatedRolesInApp failed, error = %1s	SmJavaApiMessage::IMSget-UsersDelegatedRolesInAppFail	응용 프로그램에 대한 사용자 역할을 가져올 수 없습니다. smobjims.dll(libsmobjims.so) 라이브러리가 설치되어 있는지 확인하십시오.
getUsersDelegatedTasks failed, error = %1s	SmJavaApiMessage::IMSget-UsersDelegatedTasksFail	이 사용자에 대한 태스크를 가져올 수 없습니다. smobjims.dll(libsmobjims.so) 라이브러리가 설치되어 있는지 확인하십시오.
getUsersDelegatedTasksInApp failed, error = %1s	SmJavaApiMessage::IMS-getUsersDelegatedTasksIn-AppFail	응용 프로그램에 대한 사용자 태스크를 가져올 수 없습니다. smobjims.dll(libsmobjims.so) 라이브러리가 설치되어 있는지 확인하십시오.
getUsersRoles failed, error = %1s	SmJavaApiMessage::IMS-getUsersRolesFail	이 사용자에 대한 역할을 가져올 수 없습니다. smobjims.dll(libsmobjims.so) 라이브러리가 설치되어 있는지 확인하십시오.
getUsersRolesInApp failed, error = %1s	SmJavaApiMessage::IMS-getUsersRolesInAppFail	응용 프로그램에 대한 사용자 역할을 가져올 수 없습니다. smobjims.dll(libsmobjims.so) 라이브러리가 설치되어 있는지 확인하십시오.

오류 메시지	Function	설명
getUsersTasks failed, error = %1s	SmJavaApiMessage::IMS-getUsersTasksFail	이 사용자에 대한 태스크를 가져올 수 없습니다. smobjims.dll(libsmobjims.so) 라이브러리가 설치되어 있는지 확인하십시오.
getUsersTasksInApp failed, error = %1s	SmJavaApiMessage::IMS-getUsersTasksInAppFail	응용 프로그램에 대한 사용자 태스크를 가져올 수 없습니다. smobjims.dll(libsmobjims.so) 라이브러리가 설치되어 있는지 확인하십시오.
IMSObjectProviderFactory: getIMSBaseObjectProvider() - getProcAddress('%1s') failed	SmJavaApiMessage::getIMSB-aseObjectProvider_getProc-AddressFail	smobjims.dll(libsmobjims.so) 라이브러리가 설치되어 있는지 확인하십시오.
IMSObjectProviderFactory:get-Provider() - error loading provider library	SmJavaApiMes-sage::IMS_getProviderLib-LoadError	이 메시지는 IdentityMinder 가 설치되지 않았거나 올바르지 않게 설치된 경우에 시작 시 생성됩니다.
IMSObjectProviderFactory:get-Provider() - getProcAddress of %1s failed	SmJavaApiMes-sage::IMS_getProvider_get-ProcAddressFail	라이브러리가 손상되었거나, 리소스가 부족하여 정책 서버가 라이브러리를 로드할 수 없습니다.
ImsRBACProviderFactory:get-Provider() - getProcAddress of %1s failed	SmJavaApiMessage::Ims-RBACProvider-Factory_getProviderFail	이 메시지는 IdentityMinder 가 설치되지 않았거나 올바르지 않게 설치된 경우에 시작 시 생성됩니다.
IsAssociatedWithDirectory failed, error = %1s	SmJavaApiMessage::IMSIs-AssociatedWithDirectoryFail	사용자 디렉터리가 연결된 IMS 환경에 유효한지 확인하는 중 오류가 발생했습니다.
IsUserAssignedRole failed, error = %1s	SmJavaApiMessage::IMSIs-UserAssignedRoleFail	사용자가 역할에 속하는지 확인하는 중 오류가 발생했습니다.
IsUserDelegatedRole failed, error = %1s	SmJavaApiMessage::IMSIs-UserDelegatedRoleFail	사용자가 역할에 속하는지 확인하는 중 오류가 발생했습니다.

오류 메시지	Function	설명
SmJavaAPI: Error finding class ActiveExpressionContext %1p	SmJavaApiMessage::MSG_E_-FINDING_CAEClog	단위화 중 JVM 이 활성 식 클래스를 찾지 못했습니다. 정책 서버에 옵션 팩이 설치되어 있는지 확인하십시오. smjavaapi.jar 의 클래스 경로를 확인하십시오.
SmJavaAPI: Error finding class NativeCallbackError %1p	SmJavaApiMessage::MSG_E_-FINDING_CNCElog	유효한 smjavaapi.jar 가 있고 클래스 경로에 포함되었는지 확인하십시오. 이 릴리스에 대해 해당 JVM 버전이 지원되는지 확인하십시오.
SmJavaAPI: Error finding class SmAuthenticationContext %1p	SmJavaApiMessage::MSG_E_-FINDING_CAUTHClog	유효한 smjavaapi.jar 가 있고 클래스 경로에 포함되었는지 확인하십시오.
SmJavaAPI: Error finding class Throwable %1p	SmJavaApiMessage::MSG_E_-FINDING_CTHROWlog	JVM/JRE 가 올바르게 설치되지 않은 것 같습니다. 유효한 rt.jar 가 있는지 확인하십시오. SiteMinder 가 지원되는 버전의 JVM 을 사용하도록 구성되어 있는지 확인하십시오.
SmJavaAPI: Error finding class TunnelServiceContext %1p	SmJavaApiMessage::MSG_E_-FINDING_CTSClog	정책 서버에 옵션 팩이 설치되어 있고, 유효한 smjavaapi.jar 가 있으며 클래스 경로에 포함되었는지 확인하십시오.
SmJavaAPI: Error finding class UserAuthenticationException %1p	SmJavaApiMessage::MSG_E_-FINDING_CUAElog	유효한 smjavaapi.jar 가 있고 클래스 경로에 포함되었는지 확인하십시오. 이 릴리스에 대해 해당 JVM 버전이 지원되는지 확인하십시오.
SmJavaAPI: Error finding method ActiveExpressionContext. invoke %1p	SmJavaApiMessage::MSG_E_-FIND_MINVOKElog	정책 서버에 옵션 팩이 설치되어 있고, 유효한 smjavaapi.jar 가 있으며 클래스 경로에 포함되었는지 확인하십시오.

오류 메시지	Function	설명
SmJavaAPI: Error finding method ActiveExpressionContext. release %1p	SmJavaApiMessage::MSG_E_-FIND_MRELEASElog	정책 서버에 옵션 팩이 설치되어 있고, 유효한 smjavaapi.jar 가 있으며 클래스 경로에 포함되었는지 확인하십시오.
SmJavaAPI: Error finding method SmAuthenticationContext. authenticate %1p	SmJavaApiMessage::MSG_E_-FIND_MAUTHENTICATElog	유효한 smjavaapi.jar 가 있고 클래스 경로에 포함되었는지 확인하십시오. 이 릴리스에 대해 해당 JVM 버전이 지원되는지 확인하십시오.
SmJavaAPI: Error finding method SmAuthenticationContext. init %1p	SmJavaApiMessage::MSG_E_-FIND_MAUTHINITlog	유효한 smjavaapi.jar 가 있고 클래스 경로에 포함되었는지 확인하십시오. 이 릴리스에 대해 해당 JVM 버전이 지원되는지 확인하십시오.
SmJavaAPI: Error finding method SmAuthenticationContext. query %1p	SmJavaApiMessage::MSG_E_-FIND_MAUTHQUERYlog	유효한 smjavaapi.jar 가 있고 클래스 경로에 포함되었는지 확인하십시오. 이 릴리스에 대해 해당 JVM 버전이 지원되는지 확인하십시오.
SmJavaAPI: Error finding method SmAuthenticationContext. release %1p	SmJavaApiMessage::MSG_E_-FIND_MAUTHRELEASElog	유효한 smjavaapi.jar 가 있고 클래스 경로에 포함되었는지 확인하십시오. 이 릴리스에 대해 해당 JVM 버전이 지원되는지 확인하십시오.
SmJavaAPI: Error finding method Throwable.getLocalized-Message %1p	SmJavaApiMessage::MSG_E_-FIND_GLMlog	JVM/JRE 가 올바르게 설치되지 않은 것 같습니다. 유효한 rt.jar 가 있는지 확인하십시오. SiteMinder 가 지원되는 버전의 JVM 을 사용하도록 구성되어 있는지 확인하십시오.
SmJavaAPI: Error finding method TunnelServiceContext.tunnel %1p	SmJavaApiMessage::MSG_E_-FIND_MTUNNELlog	유효한 smjavaapi.jar 가 있고 클래스 경로에 포함되었는지 확인하십시오.

오류 메시지	Function	설명
SmJavaAPI: Error initializing Java active expressions %1p	SmJavaApiMessage::MSG_E_-ACTEXPR_INITlog	활성 식 라이브러리를 로드할 수 없습니다. smactiveexpr.jar 가 클래스 경로에 있는지 확인하십시오.
SmJavaAPI: Error initilizing JNI references for SMJavaAPI %1p	SmJavaApiMessage::MSG_E_-INIT_JNI_REFSlog	JVM 에서 내부 오류가 발생했습니다. JVM 설치를 확인하십시오.
SmJavaAPI: Error making global reference to class ActiveExpressionContext %1p	SmJavaApiMessage::MSG_E_-GLOBAL_CAEClog	활성 식 컨텍스트를 설정하는 중 JVM 에서 내부 오류가 발생했습니다.
SmJavaAPI: Error making global reference to class NativeCallbackError %1p	SmJavaApiMessage::MSG_E_-GLOBAL_CNCElog	유효한 smjavaapi.jar 가 있고 클래스 경로에 포함되었는지 확인하십시오. 이 릴리스에 대해 해당 JVM 버전이 지원되는지 확인하십시오.
SmJavaAPI: Error making global reference to class SmAuthenticationContext %1p	SmJavaApiMessage::MSG_E_-GLOBAL_CAUTHClog	인증 컨텍스트를 설정하는 중 JVM 에서 내부 오류가 발생했습니다.
SmJavaAPI: Error making global reference to class Throwable %1p	SmJavaApiMessage::MSG_E_-GLOBAL_CTHROWlog	JVM/JRE 가 올바르게 설치되지 않은 것 같습니다. 유효한 rt.jar 가 있는지 확인하십시오. SiteMinder 가 지원되는 버전의 JVM 을 사용하도록 구성되어 있는지 확인하십시오.
SmJavaAPI: Error making global reference to class TunnelServiceContext %1p	SmJavaApiMessage::MSG_E_-GLOBAL_CTSClog	터널 연결을 설정하는 중 JVM 에서 내부 오류가 발생했습니다.
SmJavaAPI: Error making global reference to class UserAuthenticationException %1p	SmJavaApiMessage::MSG_E_-GLOBAL_CUAElog	유효한 smjavaapi.jar 가 있고 클래스 경로에 포함되었는지 확인하십시오. 이 릴리스에 대해 해당 JVM 버전이 지원되는지 확인하십시오.

오류 메시지	Function	설명
SmJavaAPI: Error releasing Java active expressions %1p	SmJavaApiMessage::MSG_E_-ACTEXPR_RELEASElog	JVM 에서 내부 오류가 발생했습니다. JVM 설치를 확인하십시오.
SmJavaAPI: Error releasing JNI references for SMJavaAPI %1p	SmJavaApiMessage::MSG_E_-REL_JNI_REFSlog	JVM 에서 내부 오류가 발생했습니다. JVM 설치를 확인하십시오.
SmJavaAPI: Unable to get a JVM environment %1p	SmJavaApiMessage::MSG_-ERR_GETTING_JVMlog	JVM 에서 내부 오류가 발생했습니다. JVM 설치를 확인하십시오.
SmJavaAPI: Unable to initialize JNI references %1p	SmJavaApiMessage::MSG_-ERR_INIT_JNI_REFlog	JVM 에서 내부 오류가 발생했습니다. JVM 설치를 확인하십시오.
SmJavaAPI: Unable to release JNI references %1p	SmJavaApiMessage::MSG_-ERR_REL_JNI_REFlog	정책 서버가 권한 부여 후 또는 종료 중에 리소스를 완전히 해제할 수 없습니다.
SmJVMSupport: Error attaching JVM to thread %1p	SmJavaApiMessage::MSG_E_-ATTACH_TO_THREADlog	JVM 이 올바르게 초기화되지 않았을 수 있습니다. 불필요한 java 프로세스가 실행되고 있지 않은지 확인하십시오.
SmJVMSupport: Error creating JVM %1p	SmJavaApiMessage::MSG_E_-CREATE_JVMlog	JVM 이 올바르게 설치되어 있고 jvm.dll(libjvm.so) 라이브러리가 유효한지 확인하십시오.
SmJVMSupport: Error destroying JVM %1p	SmJavaApiMessage::MSG_E_-DESTROYING_JAVA_VMlog	정책 서버가 완전한 종료를 실행하지 못했습니다. JVM 리소스가 해제되지 않았습니다.
SmJVMSupport: Error detaching JVM from thread %1p	SmJavaApiMessage::MSG_E_-DETACH_THREADlog	정책 서버가 완전한 종료를 실행하지 못했습니다. JVM 리소스가 해제되지 않았습니다.
SmJVMSupport: Error finding class System to release resources from JVM %1p	SmJavaApiMessage::MSG_E_-JVM_RR_FSYSlog	정책 서버가 완전한 종료를 실행하지 못했습니다. JVM 리소스가 해제되지 않았습니다.

오류 메시지	Function	설명
SmJVMSupport: Error getting CLASSPATH environment variable when creating JVM %1p	SmJavaApiMessage::MSG_E_-GETENV_CPlog	CLASSPATH 변수가 올바르게 정의되었는지 확인하십시오.
SmJVMSupport: Error getting JVM environment to release resources from JVM %1p	SmJavaApiMessage::MSG_E_-JVM_RR_ENVlog	정책 서버가 완전한 종료를 실행하지 못했습니다. JVM 리소스가 해제되지 않았습니다.
SmJVMSupport: Error getting method GC on class System to release resources from JVM %1p	SmJavaApiMessage::MSG_E_-JVM_RR_GGClog	JVM 이 가비지 수집을 실행하지 못했습니다. rt.jar 의 유효성을 확인하십시오.
SmJVMSupport: Error opening NETE_JVM_OPTION_FILE %1p	SmJavaApiMessage::MSG_E_-OPEN_JVM_OPTION_FILElog	환경 변수 NETE_JVM_OPTION_FILE 이 설정되어 있고 파일이 유효한지 확인하십시오.
SmJVMSupport: Error trying to get a created JVM %1p	SmJavaApiMessage::MSG_E_-GET_CREATED_JVM_LOG	JVM 이 올바르게 초기화되지 않았을 수 있습니다. 불필요한 java 프로세스가 실행되고 있지 않은지 확인하십시오.
SmJVMSupport: Unknown error caught when creating JVM %1p	SmJavaApiMessage::MSG_E_-CAUGHT_CREATE_JVMlog	JVM 이 올바르게 설치되어 있고 jvm.dll(libjvm.so) 라이브러리가 유효한지 확인하십시오.

LDAP

오류 메시지	Function	설명
(AddMember) Group DN: '%1s', User DN: '%2s'. Status: Error %3i . %4s	SmLdapMessage::ErrorLdap-AddMemberGroupDN	지정된 사용자를 LDAP 사용자 디렉터리의 지정된 그룹에 추가하지 못했습니다. 자세한 내용은 포함된 LDAP 오류 메시지를 참조하십시오.
(AuthenticateUser) DN: '%1s' . Status: Error %2i . %3s	SmLdapMes-sage::AuthenticateUserDNLd-Error	정책 서버가 LDAP 사용자 디렉터리에 대한 사용자를 인증하지 못했습니다. 이 오류는 사용자가 잘못된 암호를 제공하는 등의 다양한 원인으로 발생할 수 있습니다. 자세한 내용은 포함된 LDAP 오류 메시지를 참조하십시오.
(Bind - init) Server: '%1s', Port: %2ul. Status: Error	SmLdapMessage::ErrorBindInit	사용자 디렉터리에 대해 구성된 LDAP 서버를 초기화할 수 없습니다. 오류 메시지에 지정된 LDAP 서버의 문제를 해결하십시오.
(Bind - init) Server: failed to load Security Integration file	SmLdapMessage::BindInit-LoadSecurityIntegrationFileFail	(더 이상 사용되지 않음)
(Bind - init) Server: failed to load Security Integration secret	SmLdapMessage::BindInit-LoadSecurityIntegrationSecret-Fail	(더 이상 사용되지 않음)
(Bind - ldap_set_option CONNECT_TIMEOUT). Status: Error %1i . %2s	SmLdapMessage::ErrorBind-LdapOptionConnectTimeout	LDAP 옵션을 설정할 수 없습니다. 자세한 내용은 오류 문자열을 확인하십시오.
(Bind - ldap_set_option LDAP_OPT_PROTOCOL_-VERSION). Status: Error %1i . %2s	SmLdapMessage::ErrorBind-LdapOptionProtocolVersion	LDAP 옵션을 설정할 수 없습니다. 자세한 내용은 오류 문자열을 확인하십시오.

오류 메시지	Function	설명
(Bind - ldap_set_option LDAP_OPT_REFERRALS). Status: Error %1i. %2s	SmLdapMessage::ErrorBind-LdapOptionReferrals	자동 조회 처리가 사용되도록 설정할 수 없습니다. 자세한 내용은 오류 문자열을 확인하십시오.
(Bind - ldap_set_option LDAPL_VERSION2). Status: Error %1i . %2s	SmLdapMessage::ErrorBind-LdapOptionVersion2	LDAP 옵션을 설정할 수 없습니다. 자세한 내용은 오류 문자열을 확인하십시오. LDAP 서버가 지원되는 버전 중 하나인지 확인하십시오.
(Bind - ldap_set_option SIZELIMIT). Status: Error %1i. %2s	SmLdapMessage::ErrorBind-LdapOptionSizeLimit	LDAP 옵션을 설정할 수 없습니다. 자세한 내용은 오류 문자열을 확인하십시오.
(Bind - ldap_set_option THREAD_FN_PTRS). Status: Error %1i . %2s	SmLdapMessage::ErrorBind-LdapOptionThreadFnPirs	LDAP 옵션을 설정할 수 없습니다. 자세한 내용은 오류 문자열을 확인하십시오.
(Bind - ldap_set_option TIMELIMIT). Status: Error %1i. %2s	SmLdapMessage::ErrorBind-LdapOptionTimeLimit	LDAP 옵션을 설정할 수 없습니다. 자세한 내용은 오류 문자열을 확인하십시오.
(Bind - SSL client init failed during LDAP Initialization) Server: '%1s', Port: %2ul, Cert DB: '%3s' . Status: Error	SmLdapMessage::BindSSL-LdapClientInitFailed	LDAP 서버에 연결할 수 없습니다. LDAP 서버가 실행 중이고 LDAP 서버와 포트가 올바른지 확인하십시오. 정책 서버 컴퓨터에서 ping 해 보십시오.
(Bind - SSL client init) Cert DB: '%1s' . Status: Error	SmLdapMessage::BindSSL-ClientCertDBFailed	클라이언트 측에서 사용자 디렉터리에 대해 구성된 LDAP 서버와의 SSL 연결을 초기화하지 못했습니다. 인증서 데이터베이스가 올바르게 지정되었는지 확인하십시오.
(Bind - SSL init) Server: '%1s', Port: %2ul. Status: Error. Check LDAP server and port.	SmLdapMessage::BindSSL-InitFailed	SSL 을 사용하여 LDAP 서버를 초기화할 수 없습니다. LDAP 서버 및 포트를 확인하십시오. LDAP 서버에 SSL 이 구성되어 있는지 확인하십시오.

오류 메시지	Function	설명
(Bind) DN: '%1s'. Status: Error %2i . %3s	SmLdapMessage::BindDN-RequireCredentialsError	LDAP 서버에 바인딩할 수 없습니다. 자격 증명이 올바른지 확인하십시오. SiteMinder 관리 콘솔을 참조하십시오.
(Bind) Status: Error %1i. %2s	SmLdapMessage::Bind-StatusError	LDAP 옵션을 설정할 수 없습니다. 자세한 내용은 오류 문자열을 확인하십시오.
(ChangeUserPassword) DN: '%1s'. Status: Error %2i. %3s	SmLdapMessage::Change-UserPasswordLdError	지정된 사용자의 이전 암호를 사용하여 LDAP 서버에 바인딩할 수 없으므로 해당 암호를 변경하지 못했습니다. 자세한 내용은 오류 메시지를 참조하십시오.
(ChangeUserPassword) DN: '%1s'. Status: Error %2s	SmLdapMessage::Change-UserPasswordDNFail	지정된 사용자의 암호를 변경하지 못했습니다. 자세한 내용은 오류 메시지를 참조하십시오.
(CSmDsLdapProvider::Add-Entry) DN: '%1s'. Status: Error %2i . %3s	SmLdapMessage::ErrorLdap-AddEntryDN	지정된 DN 항목을 LDAP 사용자 디렉터리에 추가하지 못했습니다. 자세한 내용은 포함된 LDAP 오류 메시지를 참조하십시오.
(GetObjProperties) DN: '%1s' . Status: Error %2i . %3s	SmLdapMessage::GetObj-PropertiesDNLdError	정책 서버가 LDAP 사용자 디렉터리에서 요청된 DN 의 요청된 속성을 가져오지 못했습니다. 자세한 내용은 포함된 LDAP 오류 메시지를 참조하십시오.
(GetUserProp) DN: '%1s', Filter: '%2s' . Status: Error %3i . %4s	SmLdapMessage::GetUser-PropDNLd-Error	지정된 DN 을 검색하고 가져올 특성을 지정하는 중 오류가 발생했습니다. 자세한 내용은 포함된 LDAP 오류 메시지를 참조하십시오.
(GetUserProp) DN: '%1s', Filter: '%2s' . Status: Error %3i . %4s	SmLdapMessage::GetUser-PropsDNLdError	지정된 DN 을 검색하고 가져올 특성을 지정하는 중 오류가 발생했습니다. 자세한 내용은 포함된 LDAP 오류 메시지를 참조하십시오.

오류 메시지	Function	설명
(RemoveEntry) DN: '%1s'. Status: Error %2i . %3s	SmLdapMessage::ErrorLdap-RemoveEntryDN	제거할 DN 항목을 LDAP 사용자 디렉터리에서 찾지 못했습니다. 자세한 내용은 포함된 LDAP 오류 메시지를 참조하십시오.
(RemoveMember) Group DN: '%1s', User DN: '%2s'. Status: Error %3i . %4s	SmLdapMessage::ErrorLdap-RemoveMemberGroupDN	지정된 사용자를 LDAP 사용자 디렉터리의 지정된 그룹에서 제거하지 못했습니다. 자세한 내용은 포함된 LDAP 오류 메시지를 참조하십시오.
(SetUserProp) DN: '%1s', PropName: '%2s', PropValue: '%3s' . Status: Error %4i . %5s	SmLdapMessage::SetUser-PropDNError	LDAP 사용자 디렉터리의 지정된 DN 항목을 수정하지 못했습니다. 자세한 내용은 포함된 LDAP 오류 메시지를 참조하십시오.
(SetUserProp) DN: '%1s'. Status: Error %2i . %3s	SmLdapMessage::SetUser-PropsDNLdError	LDAP 사용자 디렉터리의 지정된 DN 항목을 수정하지 못했습니다. 자세한 내용은 포함된 LDAP 오류 메시지를 참조하십시오.
(SI Bind - init) Server: '%1s', Port: %2ul. Status: Error	SmLdapMessage::ErrorSI-BindInit	사용자 디렉터리에 대해 구성된 LDAP 서버를 초기화할 수 없습니다. 오류 메시지에 지정된 LDAP 서버의 문제를 해결하십시오.
(SmDsLdap) Failed to get servers.	SmLdapMessage::SmDs-LdapFailToGetServers	조회 대상 LDAP 서버에 리바인딩하는 중 내부 오류가 발생했습니다. 데이터를 사용할 수 없습니다.
(SmDsLdapConnMgr(Bind): SSL client init failed in LDAP Initialization). Server %1s : %2ul, Cert DB: %3s	SmLdapMessage::Ldap-ConnMgrBindSSLCertDBInit-Fail	SSL 을 사용하여 LDAP 서버를 초기화할 수 없습니다. LDAP 서버 및 포트를 확인하십시오. LDAP 서버에 SSL 이 구성되어 있는지 확인하십시오.
"ldap_url_parse returns error '1%i' when parsing '%2s'"	SmLdapMessage::Error_ldap_url_parse	내부 LDAP URL 을 구문 분석할 수 없습니다. 내부 LDAP URL 은 RFC 2255 형식을 준수해야 합니다.

오류 메시지	Function	설명
(SmDsLdap-LdapAdd) DN: '%1s'. Status: Received referral but no handling is implemented.	SmLdapMessage::SmDsLdap-AddHandlingImplError	Add 호출이 조회 요청을 반환하는 동안 오류가 발생했습니다.
(SmDsLdap-LdapDelete) DN: '%1s'. Status: Received referral but no handling is implemented.	SmLdapMessage::SmDs-LdapDeleteHandlingImplError	Delete 호출이 조회 요청을 반환하는 동안 오류가 발생했습니다.
(SmDsLdap-LdapModify) DN: '%1s'. Status: Received referral but no handling is implemented.	SmLdapMessage::SmDs-LdapModifyHandlingImplError	Modify 호출이 조회 요청을 반환하는 동안 오류가 발생했습니다.
(SmDsLdap-Referral) Error while parsing %1s LDAP URL.	SmLdapMessage::Ldap-URLParsingError	정책 서버가 지정된 LDAP URL 을 구문 분석하지 못했습니다. 이 오류는 일반적으로 조회로 전달된 LDAP URL 이 올바르지 않기 때문에 발생합니다. 이 경우 LDAP 토폴로지가 올바르게 정의되었는지 확인하고 정책 서버 관리 콘솔에서 향상된 LDAP 조회 처리가 사용되지 않도록 설정하십시오.
CSmDsLdapConnMgr (ldap_unbind_s). Server %1s : %2ul	SmLdapMessage::Error-LdapConnMgrUnbind	LDAP 서버에서 바인딩을 해제하는 중 오류가 발생했습니다.
CSmDsLdapConnMgr (ldap_unbind_s). Server %1s : %2ul	SmLdapMessage::Unknown-ExceptionLdapConnMgrUnbind	LDAP 서버에서 바인딩을 해제하는 중 내부 오류가 발생했습니다.
CSmDsLdapProvider::Search(): Wrong syntax of LDAP search filter: %1s	SmLdapMessage::Wrong-SyntaxLdapSearchFilter	LDAP 검색 필터의 구문이 올바른지 확인하십시오.
CSmDsLdapProvider::Search-Binary(): Wrong syntax of LDAP search filter: %1s	SmLdapMessage::Wrong-SyntaxLdapSearchBinFilter	LDAP 검색 필터의 구문이 올바른지 확인하십시오.
CSmDsLdapProvider::Search-Count(): Wrong syntax of LDAP search filter: %1s	SmLdapMessage::Wrong-SyntaxLdapSearchCountFilter	LDAP 검색 필터의 구문이 올바른지 확인하십시오.

오류 메시지	Function	설명
CSmObjLdapConnMgr Exception (ldap_unbind_s). Server %1s:%2ul	SmLdapMessage::Excp-CSmObj LdapConn-Mgrldap_unbind_s	SiteMinder 정책 서버가 정책 저장소에 대해 구성된 LDAP 서버에서 바인딩 해제하지 못했습니다. 오류 메시지에 지정된 LDAP 서버의 문제를 해결하십시오.
Directory's Disabled Flag attribute not proper for password services functionality in CSmDsLdapProvider::Set-DisabledUserState	SmLdapMessage::DirDisabled-FlagNotProper	디렉터리에 비활성화된 플래그를 나타내는 사용자 특성이 있습니다. 암호 서비스를 사용할 경우 이 특성이 작동하지 않습니다. 특성을 변경하십시오.
Exception (ldap_controls_free) in CSmDsLDAPConn::Create-LDAPControls	SmLdapMessage::Unknown-ExceptionFreeLDAPControls	내부 개체를 해제하여 LDAP 라이브러리로 되돌리는 중 예기치 않은 오류가 발생했습니다. 정책 서버 시스템의 메모리 또는 구성 오류일 수 있습니다.
Exception (ldap_count_entries) in CSmDsLdapProvider::Search-Count	SmLdapMessage::Unknown-ExceptionLdapCountEntries	사용자 디렉터리 공급자 계층에서 LDAP 검색 결과를 처리하는 중 알 수 없는 예외가 발생했습니다.
Exception (ldap_explode_dn) in CSmDsLdapProvider::Get-GroupMembers	SmLdapMessage::Ldap-ExplodeExceptionGet-GroupMembers	DN 을 해당 구성 요소 부분으로 변환하는 중 알 수 없는 예외가 발생했습니다.
Exception (ldap_init) in CSmDsLdapProvider::Bind	SmLdapMessage::Unknown-ExceptionLdapInitBind	사용자 디렉터리에 대해 구성된 LDAP 서버를 초기화하는 중 알 수 없는 예외가 발생했습니다.
Exception (ldap_init) in SecurityIntegrationCheck	SmLdapMessage::Unknown-ExceptionLdapInit	사용자 디렉터리에 대해 구성된 LDAP 서버를 초기화하는 중 알 수 없는 예외가 발생했습니다.
Exception (ldap_modify_s) in CSmDsLdapProvider::Add-Entry	SmLdapMessage::Unknown-ExceptionLdapModifyAdd-Entries	LDAP 사용자 디렉터리에 항목을 추가하는 중 알 수 없는 예외가 발생했습니다.

오류 메시지	Function	설명
Exception (ldap_modify_s) in CSmDsLdapProvider::Set-UserProps	SmLdapMessage::Unknown-ExceptionLdapModify-SetUserProps	LDAP 사용자 디렉터리의 항목을 수정하는 중 알 수 없는 예외가 발생했습니다.
Exception (ldap_search_ext_s) in CSmDsLdapProvider::Ping-Server	SmLdapMessage::Unknown-ExceptionPingServer	LDAP 서버에 연결할 수 없습니다. LDAP 서버가 실행 중이고 LDAP 서버와 포트가 올바른지 확인하십시오. 정책 서버 컴퓨터에서 ping 해 보십시오.
Exception (ldap_search_ext_s) in CSmDsLdap-Provider::Search	SmLdapMessage::Unknown-ExceptionLdapSearchExt	사용자 디렉터리 공급자 계층에서 LDAP 검색을 수행하는 중 알 수 없는 예외가 발생했습니다.
Exception (ldap_search_ext_s) in CSmDsLdapProvider::-SearchBinary	SmLdapMessage::Unknown-ExceptionLdapSearchBinExt	사용자 디렉터리 공급자 계층에서 LDAP 검색을 수행하는 중 알 수 없는 예외가 발생했습니다.
Exception (ldap_search_ext_s) in CSmDsLdapProvider::-SearchCount	SmLdapMessage::Unknown-ExceptionSearchCount	사용자 디렉터리 공급자 계층에서 LDAP 검색을 수행하는 중 알 수 없는 예외가 발생했습니다.
Exception (ldap_search_s) in CSmDsLdapProvider::Get-ObjProperties	SmLdapMessage::Unknown-ExceptionLdapSearchGet-ObjProperties	사용자 디렉터리 공급자 계층에서 LDAP 검색을 수행하는 중 알 수 없는 예외가 발생했습니다.
Exception (ldap_search_s) in CSmDsLdapProvider::Get-UserProp	SmLdapMessage::Unknown-ExceptionLdapSearchGet-UserProp	사용자 디렉터리 공급자 계층에서 LDAP 검색을 수행하는 중 알 수 없는 예외가 발생했습니다.
Exception (ldap_search_s) in CSmDsLdapProvider::Get-UserProps	SmLdapMessage::Unknown-ExceptionLdapSearchGet-UserProps	사용자 디렉터리 공급자 계층에서 LDAP 검색을 수행하는 중 알 수 없는 예외가 발생했습니다.
Exception (ldap_search_s) in CSmObjLdapProvider::Ping-Server	SmLdapMessage::Excp-Ldap_Search_S	정책 저장소에 대해 구성된 LDAP 서버를 ping 할 수 없습니다. LDAP 서버가 시작되어 실행 중인지 확인하십시오.

오류 메시지	Function	설명
Exception (ldap_search_st) in CSmObjLdapProvider::Ping-Server	SmLdapMessage::Excpldap_-search_st	정책 저장소에 대해 구성된 LDAP 서버를 지정된 시간 만료 값 내에 ping 할 수 없습니다. LDAP 서버가 시작되어 실행 중인지 확인하십시오.
Exception (ldap_simple_bind_s) in CSmDsLdapProvider::Bind	SmLdapMessage::Unknown-Exception-LdapSimpleBind	LDAP 서버에 연결할 수 없습니다. LDAP 서버가 실행 중이고 LDAP 서버와 포트가 올바른지 확인하십시오. 정책 서버 컴퓨터에서 ping 해 보십시오.
Exception (LdapModify) in CSmDsLdapProvider::Add-Entry	SmLdapMessage::Unknown-ExceptionLdapModifyAddEntry	LDAP 사용자 디렉터리에 항목을 추가하는 중 알 수 없는 예외가 발생했습니다. 고급 조회 처리가 사용되지 않도록 설정해 보고 문제가 해결되는지 확인하십시오.
Exception (LdapModify) in CSmDsLdapProvider::Add-Member	SmLdapMessage::Unknown-ExceptionLdapModifyAdd-Member	LDAP 사용자 디렉터리의 그룹에 구성원을 추가하는 중 알 수 없는 예외가 발생했습니다. 고급 조회 처리가 사용되지 않도록 설정해 보고 문제가 해결되는지 확인하십시오.
Exception (LdapModify) in CSmDsLdapProvider::Remove-Member	SmLdapMessage::Unknown-ExceptionLdapModify-RemoveMember	LDAP 사용자 디렉터리의 그룹에서 구성원을 제거하는 중 알 수 없는 예외가 발생했습니다. 고급 조회 처리가 사용되지 않도록 설정해 보고 문제가 해결되는지 확인하십시오.
Exception (LdapModify) in CSmDsLdapProvider::Set-UserProp	SmLdapMessage::Unknown-ExceptionLdapModifySet-UserProp	LDAP 사용자 디렉터리의 항목을 수정하는 중 알 수 없는 예외가 발생했습니다. 고급 조회 처리가 사용되지 않도록 설정해 보고 문제가 해결되는지 확인하십시오.

오류 메시지	Function	설명
Exception (ldapssl_client_init) in CSmDsLdapProvider::Init-Instance	SmLdapMessage::Unknown-ExceptionLdapSSLClinetInit	클라이언트 측에서 사용자 디렉터리에 대해 구성된 LDAP 서버와의 SSL 연결을 초기화하지 못했습니다. 인증서 데이터베이스가 올바르게 지정되었는지 확인하십시오.
Exception (ldapssl_init) in CSmDsLdapProvider::Bind	SmLdapMessage::Unknown-ExceptionLdapSSLInitBind	SSL 을 사용하여 LDAP 서버를 초기화할 수 없습니다. LDAP 서버 및 포트를 확인하십시오. LDAP 서버에 SSL 이 구성되어 있는지 확인하십시오.
Exception in CSmDsLDAPConn::Create-LDAPControls	SmLdapMessage::Unknown-ExceptionCreateLDAPControls	LDAP 라이브러리의 내부 개체를 요청하는 중 예기치 않은 오류가 발생했습니다. 정책 서버 시스템의 메모리 또는 구성 오류일 수 있습니다.
Exception in CSmDsLDAPConn::Free-LDAPControls	SmLdapMessage::Unknown-exceptionCSmDsLDAP-Conn_FreeLDAPControls	LDAP 컨트롤을 해제하는 중 내부 오류가 발생했습니다.
Exception in CSmDsLDAPConn::Parse-LDAPControls	SmLdapMessage::Unknown-ExceptionParseLDAPControls	LDAP 서버의 응답을 구문 분석할 수 없습니다. LDAP 서버가 올바르게 실행되고 있는지 확인하십시오.
Exception in CSmDsLdapProvider::Get-ObjProperties	SmLdapMessage::Unknown-ExceptionGetObjProperties	사용자 디렉터리 공급자 계층에서 LDAP 검색 결과를 처리하는 중 알 수 없는 예외가 발생했습니다.
Exception in CSmDsLdapProvider::Get-UserProp	SmLdapMessage::Unknown-ExceptionGetUserProp	사용자 디렉터리 공급자 계층에서 LDAP 검색 결과를 처리하는 중 알 수 없는 예외가 발생했습니다.
Exception in CSmDsLdapProvider::Get-UserProps	SmLdapMessage::Unknown-ExceptionGetUserProps	사용자 디렉터리 공급자 계층에서 LDAP 검색 결과를 처리하는 중 알 수 없는 예외가 발생했습니다.
Exception in CSmDsLdapProvider::Search	SmLdapMessage::Unknown-ExceptionCSmDsLdap-ProviderSearch	사용자 디렉터리 공급자 계층에서 LDAP 검색 결과를 처리하는 중 알 수 없는 예외가 발생했습니다.

오류 메시지	Function	설명
Exception in CSmDsLdapProvider::Search-Binary	SmLdapMessage::Unknown-ExceptionSearchBinary	사용자 디렉터리 공급자 계층에서 LDAP 검색 결과를 처리하는 중 알 수 없는 예외가 발생했습니다.
Exception in SecurityIntegrationCheck	SmLdapMessage::Unknown-ExceptionSecurityIntegration-Check	사용자 디렉터리에 대해 구성된 LDAP 서버가 보안 통합 LDAP 의 인스턴스인지 여부를 확인하는 중 알 수 없는 예외가 발생했습니다.
Failed to create a paging control	SmLdapMessage::Create-PagingControlFail	LDAP 라이브러리의 내부 개체를 요청하는 중 내부 오류가 발생했습니다. 정책 서버 시스템의 메모리 또는 구성 오류일 수 있습니다.
Failed to create a sorting LDAP control	SmLdapMessage::Create-SortLdapControlFail	LDAP 라이브러리의 내부 개체를 요청하는 중 내부 오류가 발생했습니다. 정책 서버 시스템의 메모리 또는 구성 오류일 수 있습니다.
Failed to fetch user property '%1s' for DN '%2s'	SmLdapMessage::FailedTo-FetchUserPropertyForDN	지정된 DN 이 사용자 디렉터리에 대해 구성된 LDAP 서버에 없거나 지정된 속성이 없습니다. 이 오류는 예를 들어 SiteMinder SDK 응용 프로그램이 사용자를 존재하지 않는 그룹에 추가하려고 할 경우에 발생할 수 있습니다.
Failed to parse LDAP message	SmLdapMessage::Ldap-ParseMsgFail	LDAP 서버에서 잘못된 응답을 받았습니다. LDAP 서버가 올바르게 실행되고 있는지 확인하십시오.
Failed to parse the server-side sorting response control	SmLdapMessage::Parsing-ServerSideResponse-ControlFail	LDAP 서버의 응답을 구문 분석할 수 없습니다. LDAP 서버가 올바르게 실행되고 있는지 확인하십시오.
Failed to parse the virtual list view response control	SmLdapMessage::Virtual-ListViewResponseControlFail	LDAP 서버의 응답을 구문 분석할 수 없습니다. LDAP 서버가 올바르게 실행되고 있는지 확인하십시오.

오류 메시지	Function	설명
Failed to retrieve cert db location from registry	SmLdapMessage::Retrieve-CertDBRegFailed	HKLM\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\LdapPolicyStore\CertDbPath 레지스트리 항목을 찾을 수 없습니다. 해당 항목을 생성하십시오. 이때 적절한 SSL 인증서 데이터베이스 경로를 입력하거나, 정책 저장소에 대한 SSL 연결을 사용하지 않을 경우 경로를 비워 두십시오. UNIX 시스템의 경우 <install-dir>/registry 의 sm.registry 파일을 사용하십시오.
Failure executing the server-side sorting LDAP control	SmLdapMessage::Server-SideSortingLdapExecFail	LDAP 서버의 응답을 구문 분석할 수 없습니다. LDAP 서버가 올바르게 실행되고 있는지 확인하십시오.
LDAP admin limit exceeded searching for ActiveExpr entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-ActiveExpr	정책 저장소에서 활성 식을 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.
LDAP admin limit exceeded searching for Agent entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_Device	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP admin limit exceeded searching for AgentCommand entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_AgentCommand	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.

오류 메시지	Function	설명
LDAP admin limit exceeded searching for AgentGroup entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_DeviceGroup	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP admin limit exceeded searching for AgentKey entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_AgentKey	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP admin limit exceeded searching for AgentType entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-AgentType	정책 저장소에서 에이전트 유형을 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.
LDAP admin limit exceeded searching for AgentTypeAttr entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-AgentTypeAttr	정책 저장소에서 에이전트 유형 특성을 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.
LDAP admin limit exceeded searching for AuthAzMap entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_AuthAzMap	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.

오류 메시지	Function	설명
LDAP admin limit exceeded searching for CertMap entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_CertMap	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP admin limit exceeded searching for Domain entries in policy store	SmLdapMessage::LdapAdmin-SizeLimitExceeded_Domain	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP admin limit exceeded searching for KeyManagement entries in policy store	SmLdapMessage::LdapAdmin-SizeLimit-Exceeded_KeyManagement	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP admin limit exceeded searching for ODBCQuery entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_ODBCQuery	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.

오류 메시지	Function	설명
LDAP admin limit exceeded searching for PasswordPolicy entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_PasswordPolicy	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP admin limit exceeded searching for Policy entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_Policy	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP admin limit exceeded searching for PolicyLink entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_PolicyLink	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP admin limit exceeded searching for Property entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-Property	정책 저장소에서 속성 개체를 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.
LDAP admin limit exceeded searching for PropertyCollection entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-PropertyCollection	정책 저장소에서 속성 컬렉션을 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.

오류 메시지	Function	설명
LDAP admin limit exceeded searching for PropertySection entries in policy store	SmLdapMessage::AdminLimit-ExceedSearchForProperty-Section	정책 저장소에서 속성 섹션을 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.
LDAP admin limit exceeded searching for Realm entries in policy store	SmLdapMessage::LdapAdmin-SizeLimitExceeded_Realm	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP admin limit exceeded searching for Response entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_Response	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP admin limit exceeded searching for ResponseAttr entries in policy store	SmLdapMessage::AdminLimit-ExceedSearchForRespAttr	정책 저장소에서 응답 특성을 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.
LDAP admin limit exceeded searching for ResponseGroup entries in policy store	SmLdapMessage::AdminLimit-ExceedSearchForRespGroup	정책 저장소에서 응답 그룹을 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.
LDAP admin limit exceeded searching for RootConfig entries in policy store	SmLdapMessage::AdminLimit-ExceedSearchForRootConfig	정책 저장소에는 RootConfig 개체가 하나만 있을 수 있으므로 이 문제가 발생하지 않아야 합니다. 정책 저장소가 손상되었을 수 있습니다.

오류 메시지	Function	설명
LDAP admin limit exceeded searching for Rule entries in policy store	SmLdapMessage::AdminLimit-ExceedSearchForRule	정책 저장소에서 규칙을 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.
LDAP admin limit exceeded searching for RuleGroup entries in policy store	SmLdapMessage::AdminLimit-ExceedSearchForRuleGroup	정책 저장소에서 규칙 그룹을 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.
LDAP admin limit exceeded searching for Scheme entries in policy store	SmLdapMessage::AdminLimit-ExceedSearchForScheme	정책 저장소에서 인증 체계를 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.
LDAP admin limit exceeded searching for SelfReg entries in policy store	SmLdapMessage::AdminLimit-ExceedSearchForSelfReg	정책 저장소에서 등록 체계를 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.
LDAP admin limit exceeded searching for ServerCommand entries in policy store	SmLdapMessage::Admin-LimitExceedSearchForServer-Command	정책 저장소에서 서버 명령을 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.
LDAP admin limit exceeded searching for SharedSecretPolicy entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-SharedSecretPolicy	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.

오류 메시지	Function	설명
LDAP admin limit exceeded searching for TaggedString entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-TaggedString	정책 저장소에서 태그가 지정된 문자열을 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.
LDAP admin limit exceeded searching for TrustedHost entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-TrustedHost	정책 저장소에서 트러스트된 호스트를 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.
LDAP admin limit exceeded searching for UserDirectory entries in policy store	SmLdapMessage::Admin-LimitExceedSearchForUser-Directory	정책 저장소에서 사용자 디렉터리를 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.
LDAP admin limit exceeded searching for UserPolicy entries in policy store	SmLdapMessage::Admin-LimitExceedSearchForUser-Policy	정책 저장소에서 사용자 정책을 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.
LDAP admin limit exceeded searching for Variable entries in policy store	SmLdapMessage::Admin-LimitExceedSearchForVariable	정책 저장소에서 변수를 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.
LDAP admin limit exceeded searching for VariableType entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-VariableType	정책 저장소에서 변수 유형을 검색할 때 LDAP 인스턴스에 구성된 조회 제한을 초과했습니다. LDAP 서버 측의 조회 제한을 늘리십시오.

오류 메시지	Function	설명
LDAP admin size limit exceeded searching for Admin entries in policy store	SmLdapMessage::LdapAdmin-SizeLimitExceeded_Admin	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP Error in Domain_FetchProperty for IMSEnvironments - unsupported policy store version for IMS objects	SmLdapMessage::Error-DomainFetchIMSEnv	정책 서버 버전이 5.1 이상이어야 합니다.
LDAP Error in Domain_SaveProperty for IMSEnvironments - unsupported policy store version for IMS objects	SmLdapMessage::Error-DomainSaveIMSEnv	정책 서버 버전이 5.1 이상이어야 합니다.
LDAP size limit exceeded searching for ActiveExpr entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForActiveExpr	정책 저장소에서 활성 식을 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.
LDAP size limit exceeded searching for Admin entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_Admin	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.

오류 메시지	Function	설명
LDAP size limit exceeded searching for Agent entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_Device	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP size limit exceeded searching for AgentCommand entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_Agent-Command	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP size limit exceeded searching for AgentGroup entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_DeviceGroup	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP size limit exceeded searching for AgentKey entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_AgentKey	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP size limit exceeded searching for AgentType entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForAgentType	정책 저장소에서 에이전트 유형을 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.

오류 메시지	Function	설명
LDAP size limit exceeded searching for AgentTypeAttr entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForAgent-TypeAttr	정책 저장소에서 에이전트 유형 특성을 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.
LDAP size limit exceeded searching for AuthAzMap entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_AuthAzMap	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP size limit exceeded searching for CertMap entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_CertMap	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP size limit exceeded searching for Domain entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_Domain	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP size limit exceeded searching for KeyManagement entries in policy store	SmLdapMessage::LdapSize-Limit-Exceeded_KeyManagement	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.

오류 메시지	Function	설명
LDAP size limit exceeded searching for ODBCQuery entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_ODBCQuery	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP size limit exceeded searching for PasswordPolicy entries in policy store	SmLdapMessage::LdapSize-Limit-Exceeded_PasswordPolicy	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP size limit exceeded searching for Policy entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_Policy	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP size limit exceeded searching for PolicyLink entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_PolicyLink	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP size limit exceeded searching for Property entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForProperty	정책 저장소에서 속성 개체를 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.

오류 메시지	Function	설명
LDAP size limit exceeded searching for PropertyCollection entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForProperty-Collection	정책 저장소에서 속성 컬렉션을 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.
LDAP size limit exceeded searching for PropertySection entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForProperty-Section	정책 저장소에서 속성 섹션을 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.
LDAP size limit exceeded searching for Realm entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_Realm	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP size limit exceeded searching for Response entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_Response	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP size limit exceeded searching for ResponseAttr entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForResponse-Attr	정책 저장소에서 응답 특성을 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.
LDAP size limit exceeded searching for ResponseGroup entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForRespGroup	정책 저장소에서 응답 그룹을 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.

오류 메시지	Function	설명
LDAP size limit exceeded searching for RootConfig entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForRootConfig	정책 저장소에는 RootConfig 개체가 하나만 있을 수 있으므로 이 문제가 발생하지 않아야 합니다. 정책 저장소가 손상되었을 수 있습니다.
LDAP size limit exceeded searching for Rule entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForRule	정책 저장소에서 규칙을 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.
LDAP size limit exceeded searching for RuleGroup entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForRuleGroup	정책 저장소에서 규칙 그룹을 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.
LDAP size limit exceeded searching for Scheme entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForScheme	정책 저장소에서 인증 체계를 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.
LDAP size limit exceeded searching for SelfReg entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForSelfReg	정책 저장소에서 등록 체계를 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.
LDAP size limit exceeded searching for ServerCommand entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForServer-Command	정책 저장소에서 서버 명령을 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.

오류 메시지	Function	설명
LDAP size limit exceeded searching for SharedSecretPolicy entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForShared-SecretPolicy	특정 LDAP 서버에 대한 크기 제한을 확인하십시오. LDAP 서버 매뉴얼을 참조하십시오. 또한 SiteMinder 관리 UI 를 실행하여 SiteMinder 가 이 LDAP 서버에 사용할 크기 제한을 확인한 후 이를 서버 구성과 일치하도록 설정하십시오.
LDAP size limit exceeded searching for TaggedString entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForTaggedString	정책 저장소에서 태그가 지정된 문자열을 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.
LDAP size limit exceeded searching for TrustedHost entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForTrustedHost	정책 저장소에서 트러스트된 호스트를 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.
LDAP size limit exceeded searching for UserDirectory entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForUser-Directory	정책 저장소에서 사용자 디렉터리를 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.
LDAP size limit exceeded searching for UserPolicy entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForUserPolicy	정책 저장소에서 사용자 정책을 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.
LDAP size limit exceeded searching for Variable entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForVariable	정책 저장소에서 변수를 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.

오류 메시지	Function	설명
LDAP size limit exceeded searching for VariableType entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForVariableType	정책 저장소에서 변수 유형을 검색할 때 LDAP 인스턴스에 구성된 크기 제한을 초과했습니다. LDAP 서버 측의 크기 제한을 늘리십시오.
Length of the string supplied is more than the allowed limit.Please see LDAP store documentation for more details .	SmLdapMessage::Ldap-LengthConstrain-Violation_CertMap	검색에 사용된 값이 너무 깁니다.
SmDsLdapConnMgr (ldap_search_ext_s) in PingServer : %1s	SmLdapMessage::ErrorLdap-ConnMgrPingServer	LDAP 서버에 연결할 수 없습니다. LDAP 서버가 실행 중이고 LDAP 서버와 포트가 올바른지 확인하십시오. 정책 서버 컴퓨터에서 ping 해 보십시오.
SmDsLdapConnMgr Bind - init. Server %1s : %2ul	SmLdapMessage::LdapConn-MgrBindInitFail	LDAP 서버에 연결할 수 없습니다. LDAP 서버가 실행 중이고 LDAP 서버와 포트가 올바른지 확인하십시오. 정책 서버 컴퓨터에서 ping 해 보십시오.
SmDsLdapConnMgr Bind - SetOption CONNECT_TIMEOUT %1i . Server %2s : %3ul	SmLdapMessage::LdapConn-MgrBindSetOptionConnect-Timeout	LDAP 옵션을 설정할 수 없습니다. 자세한 내용은 오류 문자열을 확인하십시오.
SmDsLdapConnMgr Bind - SSL init. Server %1s : %2ul	SmLdapMessage::LdapConn-MgrBindSSLInitFail	SSL 을 사용하여 LDAP 서버를 초기화할 수 없습니다. LDAP 서버 및 포트를 확인하십시오. LDAP 서버에 SSL 이 구성되어 있는지 확인하십시오.
SmDsLdapConnMgr Bind. Server %1s : %2ul. Error %3i-%4s	SmLdapMessage::ErrorLdap-ConnMgrBind	LDAP 서버에 연결할 수 없습니다. LDAP 서버가 실행 중이고 LDAP 서버와 포트가 올바른지 확인하십시오. 정책 서버 컴퓨터에서 ping 해 보십시오.

오류 메시지	Function	설명
SmDsLdapConnMgr Exception (ldap_init). Server %1s : %2ul	SmLdapMessage::Unknow-ExceptionLdapConnMgrInit	LDAP 서버에 연결하는 중 예기치 않은 오류가 발생했습니다. LDAP 서버 및 포트 구성 설정을 확인하십시오.
SmDsLdapConnMgr Exception (ldap_simple_bind_s). Server %1s : %2ul	SmLdapMessage::Unknown-ExceptionLdapConnMgrSimpleBind	LDAP 서버에 연결하는 중 예기치 않은 오류가 발생했습니다. LDAP 서버 및 포트 구성 설정을 확인하십시오.
SmDsLdapConnMgr Exception (ldapssl_init). Server %1s : %2ul	SmLdapMessage::Unknow-ExceptionLdapConnMgrSSLInit	SSL 을 사용하여 LDAP 서버에 연결하는 중 예기치 않은 오류가 발생했습니다. LDAP 서버 및 포트 구성 설정을 확인하십시오. Is the server configured for SSL?
SmObjLdap failed to bind to LDAP server %1s:%2i as %3s . LDAP error %4i-%5s	SmLdapMessage::SmObj-LdapFailToBindToLdapServer	LDAP 서버에 연결할 수 없습니다. LDAP 서버가 실행 중이고 LDAP 서버와 포트가 올바른지 확인하십시오. 정책 서버 컴퓨터에서 ping 해 보십시오.
SmObjLdap failed to init LDAP connection to %1s : %2i	SmLdapMessage::SmObj-LdapInitLdapConnFail	LDAP 서버에 연결할 수 없습니다. LDAP 서버가 실행 중이고 LDAP 서버와 포트가 올바른지 확인하십시오. 정책 서버 컴퓨터에서 ping 해 보십시오.
SmObjLdap failed to init SSL LDAP connection to %1s : %2i	SmLdapMessage::SmObj-LdapInitSSLLdapFail	LDAP 옵션을 설정할 수 없습니다. 정책 서버 시스템의 구성 오류일 수 있습니다. 사용 중인 LDAP 라이브러리가 올바른지 확인하십시오.
SmObjLdap failed to init SSL using %1s	SmLdapMessage::SmObj-LdapInitSSLFail	SSL 을 사용하여 LDAP 서버를 초기화할 수 없습니다. LDAP 서버 및 포트를 확인하십시오. LDAP 서버에 SSL 이 구성되어 있는지 확인하십시오.

오류 메시지	Function	설명
SmObjLdap failed to set LDAP CONNECT_TIMEOUT option	SmLdapMessage::SmObj-LdapConnectTimeoutOptFail	LDAP 옵션을 설정할 수 없습니다. 정책 서버 시스템의 구성 오류일 수 있습니다. 사용 중인 LDAP 라이브러리가 올바른지 확인하십시오.
SmObjLdap failed to set LDAP PROTOCOL V3 option	SmLdapMessage::SmObj-LdapProtocolV3OptFail	LDAP 옵션을 설정할 수 없습니다. 정책 서버 시스템의 구성 오류일 수 있습니다. 사용 중인 LDAP 라이브러리가 올바른지 확인하십시오.
SmObjLdap failed to set LDAP RECONNECT option	SmLdapMessage::SmObj-LdapReconnectOptFail	LDAP 옵션을 설정할 수 없습니다. 정책 서버 시스템의 구성 오류일 수 있습니다. 사용 중인 LDAP 라이브러리가 올바른지 확인하십시오.
SmObjLdap failed to set LDAP THREAD_FN option	SmLdapMessage::SmObjLdap-ThreadFnOptFail	LDAP 옵션을 설정할 수 없습니다. 정책 서버 시스템의 구성 오류일 수 있습니다. 사용 중인 LDAP 라이브러리가 올바른지 확인하십시오.
SmObjLdap failed to set LDAP TIMELIMIT option	SmLdapMessage::SmObjLdap-TimeoutOptFail	LDAP 옵션을 설정할 수 없습니다. 정책 서버 시스템의 구성 오류일 수 있습니다. 사용 중인 LDAP 라이브러리가 올바른지 확인하십시오.
SmObjLdap failed to set LDAP_OPT_REFERRALS option	SmLdapMessage::SmObj-LdapOptReferralsFail	LDAP 옵션을 설정할 수 없습니다. 정책 서버 시스템의 구성 오류일 수 있습니다. 사용 중인 LDAP 라이브러리가 올바른지 확인하십시오.
SmObjLdapConnMgr Bind - init. Server: %1s:%2ul	SmLdapMessage::SmObj-LdapConnMgrBindinitServer	정책 저장소에 대해 구성된 LDAP 서버를 초기화할 수 없습니다. 오류 메시지에 지정된 LDAP 서버의 문제를 해결하십시오.

오류 메시지	Function	설명
SmObjLdapConnMgr Bind - SetOption CONNECT_TIMEOUT %1i. Server %2s:%3ul	SmLdapMessage::SmObj-LdapConnMgrBindSetOption-CONNECT_TIMEOUT	정책 저장소에 대해 구성된 LDAP 서버에서 LDAP_X_OPT_CONNECT_TIMEOUT 옵션(Microsoft Active Directory SDK 를 사용하는 경우 LDAP_OPT_SEND_TIMEOUT)을 설정할 수 없습니다. 오류 메시지에 지정된 LDAP 서버의 문제를 해결하십시오.
SmObjLdapConnMgr Bind - SSL client init. Server: %1s:%2ul, Cert DB: %3s	SmLdapMessage::SmObj-LdapConnMgrBindSSLclientinit	클라이언트 측에서 정책 저장소에 대해 구성된 LDAP 서버와의 SSL 연결을 초기화하지 못했습니다. 인증서 데이터베이스가 올바르게 지정되었는지 확인하십시오.
SmObjLdapConnMgr Bind - SSL init. Server: %1s:%2ul	SmLdapMessage::SmObj-LdapConnMgrBindSSLinit	SSL 연결에서 정책 저장소에 대해 구성된 LDAP 서버를 초기화할 수 없습니다. 오류 메시지에 지정된 LDAP 서버의 문제를 해결하십시오.
SmObjLdapConnMgr Bind. Server %1s:%2ul. Error %3i - %4s	SmLdapMessage::SmObj-LdapConnMgrBindServerError	SiteMinder 정책 서버가 정책 저장소에 대해 구성된 LDAP 서버에 바인딩하지 못했습니다. 자세한 내용은 포함된 LDAP 오류 메시지를 참조하십시오. 또한 정책 서버가 올바른 LDAP 관리자 자격 증명을 사용하는지 확인하십시오. LDAP 관리자 자격 증명은 정책 서버 관리 콘솔의 "데이터" 탭에서 다시 설정할 수 있습니다.
SmObjLdapConnMgr Exception (ldap_init). Server %1s:%2ul	SmLdapMessage::ExcpSm-ObjLdapConnMgrldap_init	정책 저장소에 대해 구성된 LDAP 서버를 초기화할 수 없습니다. 오류 메시지에 지정된 LDAP 서버의 문제를 해결하십시오.

오류 메시지	Function	설명
SmObjLdapConnMgr Exception (ldap_simple_bind_s). Server %1s:%2ul	SmLdapMessage::ExcpSm-ObjLdapConnMgrldap_simple_-bind_s	SiteMinder 정책 서버가 정책 저장소에 대해 구성된 LDAP 서버에 바인딩하지 못했습니다. 정책 서버가 올바른 LDAP 관리자 자격 증명을 사용하는지 확인하십시오. LDAP 관리자 자격 증명은 정책 서버 관리 콘솔의 "데이터" 탭에서 다시 설정할 수 있습니다.
SmObjLdapConnMgr Exception (ldapssl_client_init). Server %1s:%2ul	SmLdapMessage::ExcpSm-ObjLdapConnMgrldap-ssl_client_init	클라이언트 측에서 정책 저장소에 대해 구성된 LDAP 서버와의 SSL 연결을 초기화하지 못했습니다. 인증서 데이터베이스가 올바르게 지정되었는지 확인하십시오.
SmObjLdapConnMgr Exception (ldapssl_init). Server %1s:%2ul	SmLdapMessage::ExcpSm-ObjLdapConnMgrldapssl_init	SSL 연결에서 정책 저장소에 대해 구성된 LDAP 서버를 초기화할 수 없습니다. 오류 메시지에 지정된 LDAP 서버의 문제를 해결하십시오.
Terminating the server/process.....	SmLdapMes-sage::Terminating Server-Processes	서버 프로세스를 종료하며 중요한 재구성이 발생할 수 있습니다. 로그의 이전 오류를 참조하십시오.

오류 메시지	Function	설명
Unable to fetch more than %1i data entries from the Data Store. \n %2s LDAP_SIZELIMIT_EXCEEDED, Error has been detected. \n %3s Please re-configure the sizelimit parameter of your Directory Server, \n %4s as suggested in your \""Directory Server Manual\"" \n %5s or bind the Directory Server with root dn to overcome this problem. \n %6s Ex : For Iplanet / Netscape, bind the Directory Server as \""cn=Directory Manager\""	SmLdapMessage::Unable-ToFetchMoreEntriesFromData-Source	LDAP 서버의 sizelimit 매개 변수를 늘리십시오.
Unable to retrieve LDAP directory type	SmLdapMessage::Unable-ToRetrieveLdapDir	LDAP 공급업체 및 유형을 확인할 수 없습니다. 대상 서버가 지원되는 LDAP 서버 중 하나인지 확인하십시오. 처리가 계속되지만 예기치 않은 오류가 추가로 발생할 수 있습니다.
Unable to search and fetch more data entries from the Data Store. \n %1s LDAP_SIZELIMIT_EXCEEDED, Error has been detected. \n %2s Please re-configure the sizelimit parameter of your Directory Server, \n %3s as suggested in your \""Directory Server Manual\"" \n %4s or bind the Directory Server with root dn to overcome this problem. \n %5s Ex : For Iplanet / Netscape, bind the Directory Server as \""cn=Directory Manager\""	SmLdapMessage::Unable-ToSearchFetchMore-EntriesFromDataSource	정책 서버가 디렉터리 서버에서 추가 데이터를 검색할 수 없습니다. 가능한 구성 변경은 오류 메시지 텍스트를 참조하십시오.

오류 메시지	Function	설명
Unexpected value of 'arg' argument in rebindproc %1i	SmLdapMes-sage::Unexpected ValueArg-Argument	rebindproc 호출에 'arg' 인수로 잘못된 값이 전달되고 있습니다. rebindproc 함수가 자동 조회 처리를 위한 리바인딩 콜백으로 설정되어 있습니다. 대신 향상된 조회 처리가 사용되도록 설정해 보십시오.
Unexpected value of 'arg' argument in rebindproc_sm %1i	SmLdapMes-sage::Unexpected ValueArg-Argument2	rebindproc_sm 호출에 'arg' 인수로 잘못된 값이 전달되고 있습니다. rebindproc_sm 함수가 자동 조회 처리를 위한 리바인딩 콜백으로 설정되어 있습니다. 대신 향상된 조회 처리가 사용되도록 설정해 보십시오.
Unknown value of 'freeit' argument in rebindproc_sm %1i	SmLdapMes-sage::Unexpected ValueFreeit-Argument	rebindproc 호출에 freeit 인수로 잘못된 값이 전달되고 있습니다. 0 과 1 만 허용됩니다. rebindproc 함수가 자동 조회 처리를 위한 리바인딩 콜백으로 설정되어 있습니다. 대신 향상된 조회 처리가 사용되도록 설정해 보십시오.
Unknown value of 'freeit' argument in rebindproc_sm %1i	SmLdapMes-sage::Unexpected Value-FreeitArgument2	rebindproc_sm call 호출에 freeit 인수로 잘못된 값이 전달되고 있습니다. 0 과 1 만 허용됩니다. rebindproc_sm 함수가 자동 조회 처리를 위한 리바인딩 콜백으로 설정되어 있습니다(Microsoft Active Directory SDK 를 사용하는 경우에는 적용되지 않음). 대신 향상된 조회 처리가 사용되도록 설정해 보십시오.

ODBC

오류 메시지	Function	설명
Could not save IMS Environments. Possibly missing schema support	SmOdbcMessage::IMSSave-ErrorMissingSchema	정책 서버 데이터베이스에 IMS 를 지원하는 스키마가 없습니다.
Database Error executing query (%1s) . Unknown failure.	SmOdbcMessage::Unknown-FailureDBExecQuery	지정된 SQL 문을 실행하는 중 알 수 없는 오류 또는 예외가 발생했습니다.
Database Error executing query (%1s) . Unknown failure.	SmOdbcMessage::Unknown-FailureExecODBCQuery	지정된 SQL 문을 실행하는 중 알 수 없는 오류 또는 예외가 발생했습니다.
Database Error executing query ('%1s'). Error: %2s .	SmOdbcMessage::DBError-ExecQuery	지정된 SQL 문을 실행하는 중 특정 오류가 발생했습니다.
Database Error executing query ('%1s'). Unknown failure.	SmOdbcMessage::Unknown-ExceptionDBExecQuery	지정된 SQL 문을 실행하는 중 알 수 없는 오류 또는 예외가 발생했습니다.
Database Error executing query. Error: %1s .	SmOdbcMessage::ErrorDB-ExecQuery	SQL 쿼리를 실행하는 중 특정 오류가 발생했습니다.
Database error getting escape chars. Error: %1s.	SmOdbcMessage::DBError-GetEscapeChar	데이터베이스에 사용할 이스케이프 문자를 설정하는 중 오류가 발생했습니다.
Database error getting escape chars: unknown failure.	SmOdbcMessage::Unknown-ExceptionDBGetEscapeChar	데이터베이스에 사용할 이스케이프 문자를 설정하는 중 알 수 없는 예외가 발생했습니다.
DB Warning: Data truncation will occur with data value: '%1s' Actual length: '%2u' Maximum allowed length: '%3u	'SmOdbcMessage::Data-TruncationInfo	지정된 입력에 대한 데이터 값이 최대 허용 길이를 초과했습니다. 값이 지정된 최대 길이로 잘립니다.
Error Code is %1i message is '%2s'.	SmOdbcMessage::ErrorCode-AndMessage	지정된 데이터 원본에 연결하는 중 오류가 발생했습니다. 문제를 나타내는 오류 코드와 오류 메시지가 제공됩니다.

오류 메시지	Function	설명
Error Code is %1i.	SmOdbcMessage::ErrorCode	지정된 데이터 원본에 연결하는 중 오류가 발생했습니다. 문제를 나타내는 오류 코드가 제공됩니다.
Failed to allocate query for user directory with oid: '%1s'.	SmOdbcMessage::FailedTo-AllocMemForUserDir	지정된 OID 가 나타내는 사용자 디렉터리에 사용되는 쿼리를 할당하지 못했습니다.
Failed to connect to any of the following data sources: '%1s'.	SmOdbcMessage::FailedTo-ConnectToAnyOfDataSources	지정된 사용자 디렉터리에 연결하지 못했습니다.
Failed to connect to data-source '%1s'.	SmOdbcMessage::FailedTo-ConnectToDataSource	지정된 데이터 원본에 연결하는 중 오류가 발생했습니다.
Failed to fetch query for user directory with oid: '%1s'.	SmOdbcMessage::FailedTo-FetchQueryForUserDir	지정된 OID 로 사용자 디렉터리 쿼리를 검색하지 못했습니다.
Failed to fetch user directory with oid: '%1s'.	SmOdbcMessage::FailedTo-FetchUserDir	지정된 OID 로 사용자 디렉터리를 검색하지 못했습니다.
Failed to find data source name for database '%1s'.	SmOdbcMessage::FailedTo-FindDataSource	지정된 SiteMinder 데이터베이스에 대한 "ProviderNameSpace" 레지스트리 키를 찾을 수 없습니다.
Failed to find query definition for %1s	SmOdbcMessage::FailTo-FindQueryDefinition	지정된 쿼리에 대한 쿼리 정의를 찾지 못했습니다.
Failed to init DataDirect ODBC driver. Unable to load function '%1s' in library '%2s'.	DataDirectODBCDriverFunc-LoadFail	DataDirect ODBC 라이브러리를 초기화하지 못했습니다. 제공된 라이브러리에서 지정된 초기화 함수를 찾을 수 없습니다.
Failed to init DataDirect ODBC driver. Unable to load library '%1s	SmOdbcMessage::DataDirect-ODBCDriverLibLoadFail	지정된 ODBC 라이브러리를 로드할 수 없습니다. 라이브러리 경로에 SiteMinder ODBC 라이브러리 디렉터리가 포함되어 있는지 확인하십시오.

오류 메시지	Function	설명
Failed to load ODBC branding library '%1s' .	SmOdbcMessage::ODBC-BrandingLibraryLoadFail	SiteMinder 에서 사용하도록 브랜드된 ODBC 라이브러리를 로드하지 못했습니다.
Failed to resolve name of the ODBC branding library.	SmOdbcMessage::ODBC-BrandingLibraryNameResolve-Fail	브랜딩 라이브러리의 이름을 확인하지 못했습니다. 라이브러리 이름은 Netegrity/Siteminder/Database 아래의 레지스트리에 있는 레지스트리 키 OdbcBrandingLib 에서 지정됩니다.
Failed to retrieve database registry keys for database '%1s'.	SmOdbcMessage::FailedTo-RetrieveDBRegKeys	지정된 SiteMinder 데이터베이스에 대한 레지스트리 키(Data Source, User Name 또는 Password) 중 하나를 찾을 수 없습니다.
Invalid credentials or server not found attempting to connect to '%1s' server '%2s'.	SmOdbcMessage::Unable-ToConnect	SiteMinder ODBC 데이터베이스에 액세스하기 위해 제공한 자격 증명이 잘못되었습니다.
ODBC Error executing query ('%1s') . Error: %2s.	SmOdbcMessage::ErrorExec-ODBCQuery	지정된 SQL 문을 실행하는 중 특정 ODBC 오류가 발생했습니다.
ODBC Error executing query. Error: %1s.	SmOdbcMessage::Error-ODBCQueryExec	SQL 쿼리를 실행하는 중 특정 ODBC 오류가 발생했습니다.
ODBC Error executing query. Unknown failure	SmOdbcMessage::Unknown-ExceptionExecODBCQuery	ODBC 데이터베이스에 대해 SQL 쿼리를 실행하는 중 알 수 없는 예외가 발생했습니다.

디렉터리 액세스

메시지	메시지 ID	설명
%1s failed for path '%2s	'FuncFailForPath	정책 서버가 사용자 지정 공급자를 사용하여 디렉터리 정보를 가져오지 못했습니다.
ADs EnumContainer failed; Error %1xl. %2s	ADsEnumContainerFailed	정책 서버가 ADSI 인터페이스를 통해 컨테이너 구성원을 열거하지 못했습니다.
ADs Get failed for property '%1s' ; Error %2xl. %3s	ADsGetFailForProperty	정책 서버가 ADSI 인터페이스를 통해 사용자 속성을 가져오지 못했습니다.
ADs GetGroups failed; Error %1xl. %2s	ADsGetGroupsFail	정책 서버가 사용자 그룹을 가져오지 못했습니다.
ADs Put failed for property '%1s' ; Error %2xl. %3s	ADsPutFailForProperty	정책 서버가 ADSI 인터페이스를 통해 사용자 속성을 설정하지 못했습니다.
ADs put_Filter failed; Error %1xl. %2s	ADsPutFilterFailed	정책 서버가 ADSI 인터페이스를 통해 열거 필터를 생성하지 못했습니다.
ADs Search failed; Error %1xl. %2s	ADsSearchFail	정책 서버가 ADSI 인터페이스를 통해 검색하지 못했습니다.
ADsBuildEnumerator failed; Error %1xl. %2s	ADsBuildEnumeratorFailed	정책 서버가 ADSI 인터페이스를 통해 컨테이너 구성원을 열거하지 못했습니다.
ADsBuildVarArrayStr failed; Error %1xl. %2s	ADsBuildVarArrayStrFailed	정책 서버가 ADSI 인터페이스를 통해 변수 배열을 만들지 못했습니다.
ADsEnumerateNext failed; Error %xl. %2s	ADsEnumerateNextFailed	정책 서버가 ADSI 인터페이스를 통해 컨테이너 구성원을 열거하지 못했습니다.
ADsGetObject failed; Error %1xl. %2s	ADsGetObjectFail	정책 서버가 ADSI 인터페이스를 통해 개체 속성을 가져오지 못했습니다.

메시지	메시지 ID	설명
ADsOpenObject failed on '%1s' . ADSI Error %2xl. %3s	ADsOpenObjectFailed	정책 서버가 ADSI 인터페이스에 대한 핸들을 생성하지 못했습니다.
Affiliate PropertyCollection does not match group name	AffiliatePropertyCollection-GroupNameMismatch	정책 서버가 정책에 대한 가맹 관계의 유효성을 검사하지 못했습니다. 가맹 속성 컬렉션 이름이 지정된 정책 이름과 일치하지 않습니다.
Could not fetch properties using '%1s' function	PropertiesFetchFail	정책 서버가 사용자 지정 공급자를 통해 개체 속성을 가져오지 못했습니다.
Exception in SmDsObj	SmDsObjUnknownException	정책 서버가 DS 공급자를 조회하지 못했습니다. 정책 서버 프로세스에서 공급자 공유 라이브러리를 로드할 수 있는지 확인하십시오.
Exception in SmDsObj: %1s	SmDsObjException	정책 서버가 DS 공급자를 조회하지 못했습니다. 정책 서버 프로세스에서 공급자 공유 라이브러리에 액세스할 수 있는지 확인하십시오.
Failed to find an Affiliate PropertyCollections	AffiliatePropertyCollectionsFail	정책 서버가 가맹 도메인을 가져오지 못했습니다. 정책 저장소의 일관성을 확인하십시오.
Failed to find attribute	AttributeFindFail	정책 서버가 지정된 사용자 특성을 찾지 못했습니다.
Failed to find password property	PasswordPropertyFindFail	정책 서버가 지정된 가맹에 대한 암호를 찾지 못했습니다.
Failed to find Property in PropertySection acting as Affiliate user	AffilateUserPropertyIn-PropertySectionFindFail	정책 서버가 지정된 가맹 속성을 가져오지 못했습니다.
Failed to find Property-Collection acting as Affiliate user directory	ActingAffiliateUserDirProps-FindFail	정책 서버가 가맹 도메인을 가져오지 못했습니다. 정책 저장소의 일관성을 확인하십시오.

메시지	메시지 ID	설명
Failed to find PropertySection as Affiliate 사용자	AffilateUserPropertySection-FindFail	정책 서버가 지정된 가맹을 조회하지 못했습니다.
Failed to find PropertySection in Affiliate user directory	InAffiliateUserDirPropsFindFail	정책 서버가 가맹 도메인에서 가맹을 가져오지 못했습니다. 정책 저장소의 일관성을 확인하십시오.
Failed to find root object!	RootObjFindFail	정책 서버가 가맹 도메인을 찾지 못했습니다. SiteMinder 관리 UI 를 통해 가맹 개체를 볼 수 있는지 확인하십시오.
Failed to find user in Affiliate PropertyCollection	AffiliatePropertyCollection-UserFindFail	정책 서버가 지정된 가맹을 조회하지 못했습니다.
Failed to initialize custom directory API module '%1s	'CustomDirAPIModInitFail	정책 서버가 사용자 지정 공급자 라이브러리를 초기화하지 못했습니다.
Failed to load custom directory API library '%1s'. System error: %2s	CustormDirAPILibLoadFail	정책 서버가 사용자 지정 공급자 라이브러리를 로드하지 못했습니다. 정책 서버 프로세스에서 해당 사용자 지정 공급자 라이브러리에 액세스할 수 있는지 확인하십시오.
Failed to resolve function '%1s' in custom directory API library '%2s'. 시스템 error: %3s	CustormDirAPILibFuncResovl-Fail	정책 서버가 사용자 지정 공급자 라이브러리를 초기화하지 못했습니다. 정책 서버 프로세스에서 해당 사용자 지정 공급자 라이브러리에 액세스할 수 있는지 확인하십시오.
Get Disabled State not supported for namespace ADSI	ADSIGetDisabledState-Supported	정책 서버가 ADSI 인터페이스를 통해 사용자 비활성 상태를 가져오는 기능을 지원하지 않습니다.

메시지	메시지 ID	설명
No function '%1s' is available in custom directory API library '%2s'	CustomDirAPILibFunctNot-Found	정책 서버가 사용자 지정 공급자 라이브러리에서 필요한 메서드 중 하나를 찾지 못했습니다. 정책 서버 프로세스에서 해당 사용자 지정 공급자 라이브러리에 액세스할 수 있는지 확인하십시오.
Password change not supported for namespace ADSI	ADSINoPasswordChange	정책 서버가 ADSI 인터페이스를 통해 사용자 암호를 변경하는 기능을 지원하지 않습니다.
Password change not supported for namespace LanMan:	LanManPasswordChangeNot-Supported	정책 서버 LanMan 공급자가 사용자 암호 변경을 지원하지 않습니다.
QueryInterface (IID_IADsContainer) failed; Error %1s %2s %3i . %4s	IID_IADsContainerFail	정책 서버가 ADSI 인터페이스를 통해 컨테이너 구성원을 열거하지 못했습니다.
QueryInterface (IID_IADsContainer) failed; Error %1xl. %2s	QueryInterfaceIID_IADs-ContainerFail	정책 서버가 ADSI 인터페이스를 통해 컨테이너 구성원을 열거하지 못했습니다.
QueryInterface (IID_IADsUser) failed; Error %1xl. %2s	IID_IADsUserFail	정책 서버가 사용자 그룹을 가져오지 못했습니다.
QueryInterface (IID_IDirectorySearch) failed; Error %1xl. %2s	IID_IDirectorySearchFail	정책 서버가 ADSI 인터페이스를 통해 검색하지 못했습니다.
Set Disabled State not supported for namespace ADSI	ADSISetDisabledState-Supported	정책 서버가 ADSI 인터페이스를 통해 사용자 비활성 상태를 설정하는 기능을 지원하지 않습니다.
Unsupported function called: SmDirAddEntry	UnsupportedFuncCallSmDir-AddEntry	SmDirAddEntry 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.
Unsupported function called: SmDirAddMemberToGroup	UnsupportedFuncCallSmDir-AddMemberToGroup	SmDirAddMemberToGroup 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.

메시지	메시지 ID	설명
Unsupported function called: SmDirAddMemberToRole	UnsupportedFuncCallSmDir-AddMemberToRole	SmDirAddMemberToRole 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.
Unsupported function called: SmDirChangeUserPassword	UnsupportedFuncCallSmDir-ChangeUserPassword	SmDirChangeUserPassword 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.
Unsupported function called: SmDirGetGroupMembers	UnsupportedFuncCallSmDir-GetGroupMembers	SmDirGetGroupMembers 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.
Unsupported function called: SmDirGetRoleMembers	UnsupportedFuncCallSmDir-GetRoleMembers	SmDirGetRoleMembers 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.
Unsupported function called: SmDirGetUserAttrMulti	UnsupportedFuncCallSmDir-GetUserAttrMulti	SmDirGetUserAttrMulti 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.
Unsupported function called: SmDirGetUserClasses	UnsupportedFuncCallSmDir-GetUserClasses	SmDirGetUserClasses 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.
Unsupported function called: SmDirGetUserGroups	UnsupportedFuncCallSmDir-GetUserGroups	SmDirGetUserGroups 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.
Unsupported function called: SmDirGetUserProperties	UnsupportedFuncCallSmDir-GetUserProperties	SmDirGetUserProperties 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.
Unsupported function called: SmDirGetUserRoles	UnsupportedFuncCallSmDir-GetUserRoles	SmDirGetUserRoles 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.
Unsupported function called: SmDirLookup	UnsupportedFuncCallSmDir-Lookup	SmDirLookup 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.
Unsupported function called: SmDirRemoveEntry	UnsupportedFuncCallSmDir-RemoveEntry	SmDirRemoveEntry 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.

메시지	메시지 ID	설명
Unsupported function called: SmDirRemoveMemberFrom-Group	UnsupportedFuncCallSmDir-RemoveMemberFromGroup	SmDirRemoveMemberFromGroup 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.
Unsupported function called: SmDirRemoveMemberFrom-Role	UnsupportedFuncCallSmDir-RemoveMemberFromRole	SmDirRemoveMemberFromRole 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.
Unsupported function called: SmDirSearch	UnsupportedFuncCallSmDir-Search	SmDirSearch 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.
Unsupported function called: SmDirSearchCount	UnsupportedFuncCallSmDir-SearchCount	SmDirSearchCount 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.
Unsupported function called: SmDirSetUserAttr	UnsupportedFuncCallSmDir-SetUserAttr	SmDirSetUserAttr 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.
Unsupported function called: SmDirSetUserAttrMulti	UnsupportedFuncCallSmDir-SetUserAttrMulti	SmDirSetUserAttrMulti 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.
Unsupported function called: SmDirSetUserDisabledState	UnsupportedFuncCallSmDir-SetUserDisabledState	SmDirSetUserDisabledState 함수는 가맹 공급자 라이브러리에서 지원되지 않습니다.

터널

오류 메시지	Function	설명
Bad security handshake attempt. Handshake error: %1i	SmTunnelMessage::Hand-shake AttemptError	특정 시스템 오류로 인해 클라이언트/서버 보안 핸드셰이크가 실패했습니다.
Client cannot encrypt data successfully during handshake	SmTunnelMessage::Client-Encr yptFail	클라이언트/서버 보안 핸드셰이크가 실패했습니다. 클라이언트가 핸드셰이크 메시지를 올바르게 암호화할 수 없습니다.
Exception caught during handshake attempt	SmTunnelMessage::ExcpIn-Han dshakeAttempt	클라이언트/서버 보안 핸드셰이크 도중 지정되지 않은 오류가 발생했습니다.
Failed to initialize tunnel service library '%1s'. %2s	SmTunnelMessage::Tunnel-Ser viceLibInitFail	요청된 터널 서비스 라이브러리를 초기화하지 못했습니다.
Failed to load tunnel service library '%1s'. System error: %2s	SmTunnelMessage::Tunnel-Ser viceLibLoadFail	요청된 터널 서비스 라이브러리를 로드할 수 없습니다.
Failed to resolve function '%1s' in tunnel service library '%2s'. System error: %3s	SmTunnelMessage::Tunnel-Ser viceLibFuncResolveFail	시스템 오류로 인해 요청된 터널 서비스 라이브러리에서 요청된 함수를 찾을 수 없습니다.
Handshake error: Bad host-name in hello message	SmTunnelMessage::Hand-shake ErrorBadHostname	클라이언트/서버 보안 핸드셰이크가 실패했습니다. 클라이언트에서 서버로 보내는 초기 메시지에 잘못된 호스트 이름이 포함되었습니다.
Handshake error: Bad version number in hello message	SmTunnelMessage::Hand-shake ErrorBadVersionNo	클라이언트/서버 보안 핸드셰이크가 실패했습니다. 클라이언트에서 서버로 보내는 초기 메시지에 잘못된 버전 번호가 포함되었습니다.

오류 메시지	Function	설명
Handshake error: Failed to receive client ack. Socket error %1i	SmTunnelMessage::Hand-shakeErrorToReceiveClientACK	클라이언트/서버 보안 핸드셰이크가 실패했습니다. 서버에서 클라이언트로 보내는 초기 메시지를 클라이언트가 승인하지 않았습니다.
Handshake error: Failed to receive client hello. Client disconnected	SmTunnelMessage::Hand-shakeErrorClientHelloNot-Receive	클라이언트/서버 보안 핸드셰이크가 실패했습니다. 초기 메시지를 보내기 전에 클라이언트의 연결이 끊어졌습니다.
Handshake error: Failed to receive client hello. Socket error %1i	SmTunnelMessage::Hand-shakeErrorSocketError	클라이언트/서버 보안 핸드셰이크가 실패했습니다. 클라이언트가 초기 메시지를 보내지 않았습니다.
Handshake error: Failed to send server hello. Socket error %1i	SmTunnelMessage::Hand-ShakeErrorInSendSocketError	클라이언트/서버 보안 핸드셰이크가 실패했습니다. 통신 오류로 인해 서버에서 클라이언트로 초기 메시지를 보낼 수 없습니다.
Handshake error: Shared secret incorrect for this client	SmTunnelMessage::Hand-shakeErrorSharedSecret-Incorrect	클라이언트/서버 보안 핸드셰이크가 실패했습니다. 클라이언트에서 서버로 보내는 초기 메시지에 잘못된 공유 암호가 포함되었습니다.
This Policy Server version does not support 3.6 agents	SmTunnelMessage::Agent-VersionNotSupported	클라이언트/서버 보안 핸드셰이크가 실패했습니다. 해당 클라이언트 버전에서는 더 이상 터널 연결을 설정할 수 없습니다.
Tunnel callers are not allowed to execute request %1ul	SmTunnelMessage::Tunnel-CallerExecDenied	터널 호출 시 허용되지 않는 요청을 시도했습니다.
Unexpected handshake 오류	SmTunnelMessage::Hand-shakeErrorUnexpected	예상치 못한 이유로 클라이언트/서버 보안 핸드셰이크에 실패했습니다.

오류 메시지	Function	설명
Unknown Exception caught while publishing Tunnel Libs	SmTunnelMessage::Unknown-ExcpPublishTunnelLibs	터널 서비스 라이브러리가 게시 인터페이스를 통해 해당 라이브러리를 설명하는 도중 알 수 없는 예외가 발생했습니다.