SiteMinder

업그레이드 안내서

12.52 SP1

ca technologies

CA Technologies 제품 참조

이 문서는 다음 CA Technologies 제품을 참조합니다 :

- SiteMinder
- eTrust SOA Security Manager(CA SOA Security Manager)
- CA Security Command Center
- CA Audit iRecorder for SiteMinder

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

SiteMinder 의 이전 릴리스에서 발견된 문제점으로 인해 다음과 같은 내용이 12.52 설명서에서 업데이트되었습니다.

- 어설션 특성 로깅을 적용하기 위해 감사 저장소 업그레이드 - DB2 지침이 수정되었습니다. 업그레이드 스크립트는 NULL 값을 올바로 추가하며, 업그레이드 스크립트는 더 이상 수동으로 편집할 필요가 없습니다.
- 병렬 환경을 구성 하는 방법 (페이지 118) - 단계 및 XPSImport 명령 스위치에 대한 설명이 수정되었습니다.
- 이 안내서의 구성 요소 버전 - r12.5 에서의 업그레이드가 지원됨을 나타내기 위해 r12.5 에 대한 참조가 추가되었습니다.
- Linux 에서 Korn 셸(ksh) 패키지가 필요함 (페이지 54) - 정책 서버를 업그레이드하는 데 필요한 라이브러리를 설명하는 내용이 추가되었습니다.

- 백 채널 사용자 이름이 각 SAML 파트너 관계에 대해 고유한지 확인 (페이지 100) - 기존 파트너 관계가 (동일 프로토콜 내에서) 동일한 수신 백 채널 사용자 이름을 사용할 수 없는 조건에 대한 설명이 추가되었습니다. CQ 177179 를 해결합니다.
- 12.x 마이그레이션 작동 방식 (페이지 91) - 정책 저장소를 업그레이드해야만 12.52 SP1 웹 에이전트를 12.52 SP1 정책 서버와 함께 설치 및 구성할 수 있음을 알려 주는 참고가 제거되었습니다. 정책 저장소를 업그레이드하기 전에 12.52 SP1 웹 에이전트를 설치하는 지침을 수정하는 참고가 추가되었습니다.

이 안내서의 두 번째 에디션에는 다음과 같은 변경된 사항이 포함되어 있습니다.

설명서에서만 변경된 내용

- r6.x 정책 마이그레이션 (페이지 85) - Oracle Directory Server 에 대한 마이그레이션 절차가 수정되었습니다. 설명서는 12.52 SP1 에서 업데이트되었습니다. 이 변경 사항은 CQ 182636 및 STAR 21697346-1 을 해결합니다.
- CA Arcot WebFort 및 CA Arcot RiskFort 와 SiteMinder 통합 (페이지 91) - CA Arcot WebFort 및 CA RiskFort 와 <stmdnr> 통합을 위해 SiteMinder 를 업그레이드하는 방법을 설명하는 단원이 추가되었습니다.

목차

제 1 장: SiteMinder 업그레이드 계획

이 섹션은 다음 항목을 포함하고 있습니다.

구성 요소 버전 및 업그레이드 지원

다음과 같은 버전에서 12.52 SP1 로 업그레이드할 수 있습니다.

- r6.0 SP5 CR32
- r6.0 SP5 J
- r12.0 SP2
- r12.0 SP3
- r12.0 SP3 J
- r12.5
- r12.51
- r12.52

이 안내서의 구성 요소 버전에는 다음이 포함됩니다.

- SiteMinder 관리 UI r12.x 업그레이드. 이 안내서에서 버전은 다음과 같이 표시됩니다.
  - r12.x 는 r12.0 SP2, r12.0 SP3, 12.5, r12.51 및 r12.52 입니다.
- 정책 서버 및 정책 저장소 r6.x 및 r12.x 업그레이드. 이 안내서에서 버전은 다음과 같이 표시됩니다.
  - r6.x 는 r6.0 SP5 입니다.
  - r12.x 는 r12.0 SP2, r12.0 SP3, 12.5, r12.51 및 r12.52 입니다.

- CA Business Intelligence 공용 보고 구성 요소(보고서 서버) r12.x 업그레이드. 이 안내서에서 버전은 다음과 같이 표시됩니다.
  - r12.x 는 r12 SP2 및 r12.0 SP3 까지이며 cr3 이 포함됩니다.

    참고: r12.0 SP3 cr4 이상의 보고서 서버를 설치하고 구성한 경우에는 업그레이드할 필요가 없습니다.
- 웹 에이전트 r6.x 및 r12.x 업그레이드. 이 안내서에서 버전은 다음과 같이 표시됩니다.
  - r6.x 는 r6.x QMR 5 입니다.
  - r12.x 는 r12.0 SP2, r12.0 SP3, r12.5, r12.51 및 r12.52 입니다.

업그레이드 경로

업그레이드는 12.52 SP1 구성 요소를 기존 SiteMinder 환경에 배포하는 과정으로 구성됩니다. 12.52 SP1 업그레이드는 두 가지 방법으로 완료할 수 있습니다.

- 마이그레이션 완료
- 기존 환경과 함께 병렬로 12.52 SP1 환경 구성. 두 환경 모두 하나 이상의 키 저장소를 사용하여 싱글 사인온을 유지합니다.

마이그레이션

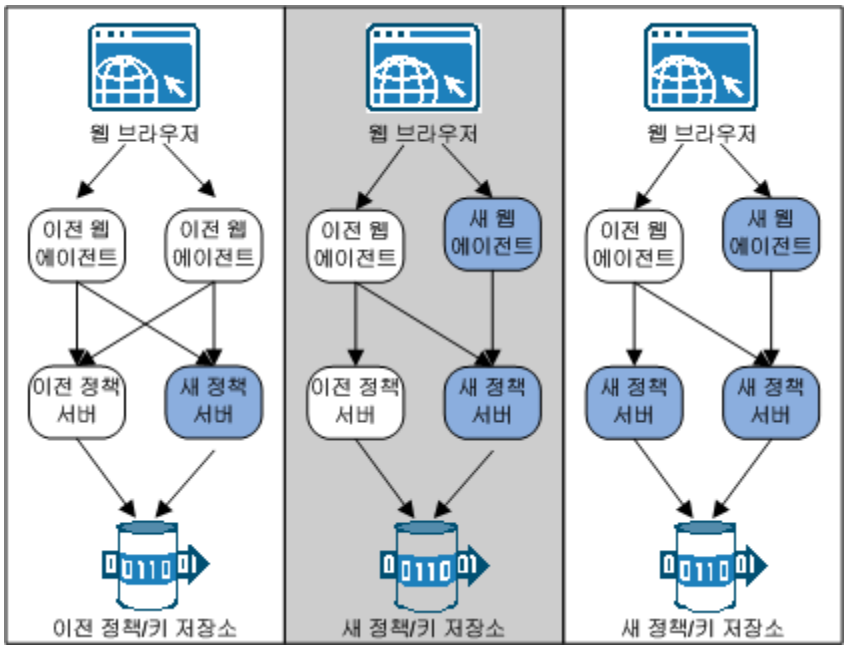
마이그레이션은 12.52 SP1 에서 작동하는 환경이 될 때까지 개별 SiteMinder 구성 요소를 업그레이드하는 프로세스입니다. 개별 구성 요소 업그레이드는 다음과 같은 작업을 수행하는 하나 이상의 단계로 구성됩니다.

- 구성 요소를 오프라인 상태로 만듭니다.
- 구성 요소를 업그레이드합니다.
- 구성 요소를 온라인 상태로 만듭니다.

시스템 가용성을 유지하기 위해서 개별 구성 요소를 장기간에 걸쳐 업그레이드하게 됩니다. 시스템 가용성 유지의 핵심은 구성 요소를 업그레이드하는 순서입니다. 마이그레이션 기간 동안 업그레이드된 특정 구성 요소가 이전 버전과 계속해서 통신할 수 있습니다. 이러한 유형의 통신을 혼합 모드 지원이라고 합니다.

다음 다이어그램은 마이그레이션의 개념을 보여 줍니다. r6.x 또는 r12.x 에서 마이그레이션하는 방법에 대한 자세한 내용은 관련 장을 참조하십시오.

그림 1: 간단한 마이그레이션 개요



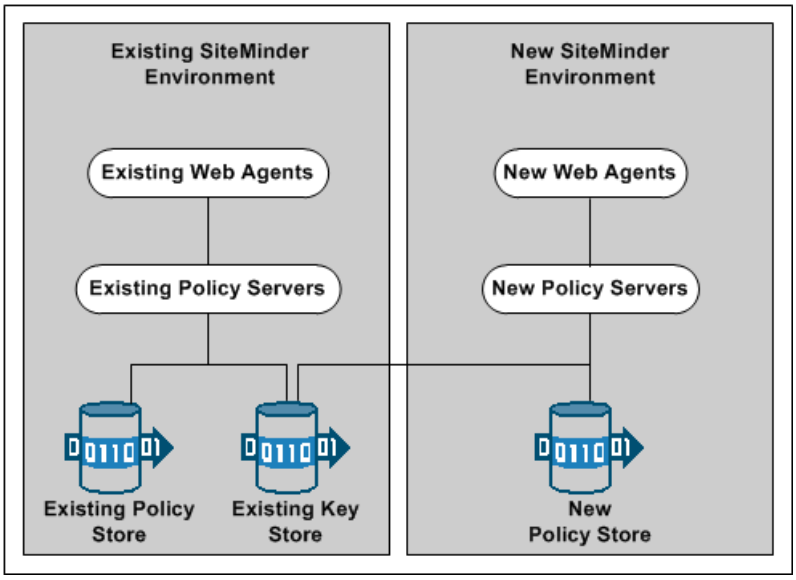
병렬 업그레이드

병렬 업그레이드는 기존 환경과 함께 12.52 SP1 환경을 구성하는 프로세스입니다. 병렬 업그레이드 구성은 다음과 같은 작업을 수행하는 여러 단계로 구성됩니다.

- 기존 환경을 변경되지 않은 상태로 유지합니다.
- 12.52 SP1 환경을 구성합니다.
- 공용 키 저장소나 다중 키 저장소를 사용하여 두 환경 간에 싱글 사인온이 사용되도록 설정합니다.

다음 다이어그램은 병렬 업그레이드의 개념을 설명합니다. r6.x 또는 r12.x 에서 병렬 업그레이드를 완료하는 것에 대한 자세한 내용은 관련 장을 참조하십시오.

그림 2: 병렬 업그레이드 개요



마이그레이션 계획 방법

복잡한 SiteMinder 환경을 마이그레이션하려면 환경을 업그레이드하기 전에 여러 구성 요소를 업그레이드해야 합니다. 중요한 리소스에 보안 위험이나 다운타임이 발생하지 않도록 하면서 마이그레이션이 효율적으로 완료될 수 있도록 마이그레이션 전략을 세워야 합니다.

마이그레이션 전략은 다음 항목으로 구성될 수 있습니다.

- 테스트 환경

  프로세스에 익숙해질 수 있도록 테스트 마이그레이션을 수행합니다. 테스트 마이그레이션을 수행하면 프로덕션 환경을 마이그레이션할 때 업무에 핵심적인 리소스에 악영향을 줄 수 있는 문제를 미리 파악하고 이를 해결 및 방지할 수 있습니다.

- 현재 타사 제품 및 하드웨어

  12.52 SP1 에서 현재 타사 제품 및 하드웨어가 지원되는지 여부를 확인합니다.

  참고: 지원되는 CA 및 타사 구성 요소의 목록에 대해서는 기술 지원 사이트의 SiteMinder 12.52 SP1 Platform Support Matrix(플랫폼 지원표)를 참조하십시오.

- 사이트 분석

  SiteMinder 환경의 현재 상태와 각 구성 요소를 업그레이드하기에 가장 적합한 시기를 확인합니다.

- SiteMinder 구성 요소

  업그레이드하려는 개별 SiteMinder 구성 요소를 나열하고 각 구성 요소가 호스트되는 위치를 파악합니다.

- 복구 계획

  마이그레이션 중에 문제가 발생할 경우에 대비하여 기존 구성 요소를 백업합니다.

- 업그레이드 경로

  마이그레이션 시 지원되는 개별 구성 요소 업그레이드 경로를 확인합니다.

- 혼합 모드 지원

  혼합 모드 지원을 이해합니다.

- 성능 테스트

  마이그레이션이 완료될 때 환경의 성능을 테스트하기 위한 전략을 개발합니다.

정책 서버 릴리스 정보 검토

정책 서버 릴리스 정보에는 설치 및 업그레이드 주의 사항이 포함되어 있습니다. 마이그레이션을 시작하기 전에 이 자료를 검토하는 것이 좋습니다.

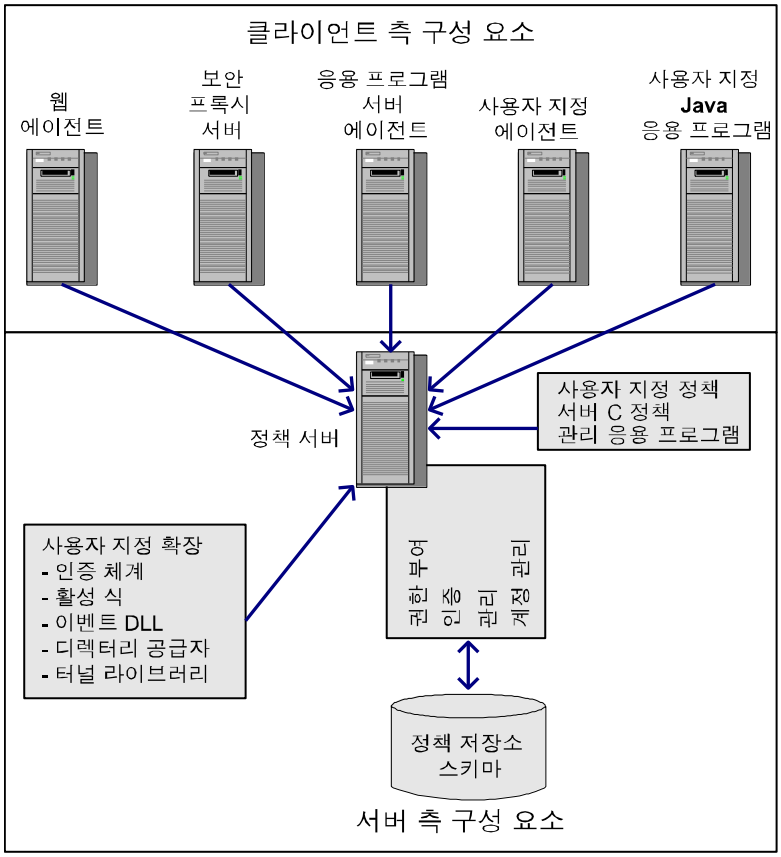
SiteMinder 환경 분석

SiteMinder 환경을 분석하여 마이그레이션의 복잡성을 확인할 수 있습니다. 다음 질문을 고려하십시오.

질문	권장 사항
사용 환경에서 실행 중인 정책 서버 및 에이전트는 몇 개입니까?	정책 서버 감사 로그를 사용하여 수를 확인하십시오.
정책 서버 및 에이전트의 버전은 어떻게 됩니까?	정책 서버 감사 로그를 사용하여 버전을 확인하십시오.
어떤 정책 서버가 어떤 웹 에이전트와 통신합니까?	정책 서버 감사 로그를 사용하여 이 정보를 확인하십시오.
각 사이트에서 하루 중 트래픽이 가장 적은 시간은 언제입니까?	웹 서버 로그와 정책 서버 감사 로그를 검토하십시오.
웹 에이전트가 장애 조치 또는 라운드 로빈 모드에서 작동 중입니까?	장애 조치 및 라운드 로빈을 유지하려면 "혼합 SiteMinder 환경"을 참조하십시오.
SiteMinder 환경에서 싱글 사인온을 사용 중입니까?	싱글 사인온을 유지하는 방법에 대한 자세한 내용은 이 안내서를 참조하십시오.
인증 체계에 자격 증명 수집기를 사용 중입니까?	혼합 환경에서 자격 증명 수집기를 사용하는 방법에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.
12.52 SP1 에서 타사 하드웨어 및 소프트웨어를 지원합니까?	기술 지원 사이트의 "SiteMinder 12.52 SP1 Platform Support Matrix"(SiteMinder 12.52 SP1 플랫폼 지원표)를 참조하십시오.
Professional Services 에서 사용자 지정한 SiteMinder 소프트웨어가 있습니까?	지침은 고객 지원부에 문의하십시오.

질문	권장 사항
이전 버전의 SiteMinder 설명서에 액세스할 수 있습니까? 이 안내서에서는 이전 SiteMinder 설명서를 참조합니다.	기술 지원 사이트에서 SiteMinder 설명서를 찾으십시오.
업그레이드 시 덮어쓰여질 수 있는 사용자 지정 파일이 있습니까?	마이그레이션을 시작하기 전에 사용자 지정 파일을 백업하십시오.

다음 그림에서는 업그레이드 전에 고려해야 할 SiteMinder 구성 요소를 보여 줍니다.



복구 전략 계획

원래 구성을 복구할 수 있는 복구 계획을 구현합니다. 구성 요소를 업그레이드하거나 마이그레이션한 후에는 되돌릴 수 없습니다.

중요! 가장 완벽한 복구 계획은 각 정책 서버 및 웹 에이전트 호스트의 전체 이미지를 백업하는 것이며, 이 방법을 권장합니다.

각 시스템의 전체 이미지를 백업하지 않으려면 다음 단계를 수행하십시오.

- 모든 웹 에이전트 및 정책 서버 바이너리를 백업합니다. 이러한 파일은 대부분 정책 서버 및 웹 에이전트를 설치한 위치의 bin 하위 디렉터리에 있습니다.
- 웹 에이전트 구성 파일(WebAgent.conf)을 백업합니다.

  중앙의 12.52 SP1 정책 서버에서 에이전트를 관리하려면 에이전트 구성 파일을 정책 서버 관리자에게 제공하십시오. 관리자가 에이전트 구성 개체를 만들려면 이 파일이 필요합니다.

  참고: 중앙에서 웹 에이전트를 관리하는 것에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.
- r6.x 에서 마이그레이션할 경우, smobjexport 유틸리티를 사용하여 정책 저장소를 일반 텍스트 형식으로 파일로 내보내십시오.

  정책 저장소를 일반 텍스트로 내보내면 공유 암호와 같은 암호화된 정보가 기록됩니다. 이러한 정보를 사용하여 문제를 해결할 수 있습니다. 키 저장소가 정책 저장소에 위치하는 경우 smobjexport 유틸리티에서 -k 옵션을 사용하십시오. 이 옵션을 사용하면 내보낸 정보에 키가 포함됩니다.
- r12.x 에서 마이그레이션할 경우, XPSExport 유틸리티를 사용하여 정책 저장소를 파일로 내보내십시오.
- 필요한 경우 다시 설치할 수 있도록 r6.x 또는 r12.x 설치 스크립트, 핫픽스 및 서비스 팩을 복사합니다. 기술 지원 사이트에서 복사본을 다운로드할 수 있습니다.

혼합 SiteMinder 환경

12.52 SP1 로 마이그레이션하면 환경에 서로 다른 버전의 SiteMinder 구성 요소가 포함되어 있을 수 있습니다. 또한 모든 구성 요소를 12.52 SP1 로 업그레이드할 필요는 없으므로 일부 구성 요소를 현재 버전으로 유지할 수 있습니다. 다음 사항을 고려하십시오.

- 환경에 r6.x 구성 요소의 조합이 포함된 경우 12.52 SP1 정책 서버는 r6.x 정책 저장소와 계속해서 통신할 수 있습니다.
- 환경에 r12.x 구성 요소의 조합이 포함된 경우 12.52 SP1 정책 서버는 r12.x 정책 저장소와 계속해서 통신할 수 있습니다.

- 환경에 혼합된 정책 서버 버전이 포함된 경우 사용자는 리소스에 계속 액세스할 수 있으며 동일한 사용 환경에서 r6.x QMR6, r12.0 SP2 또는 r12.0 SP3 에이전트를 사용할 수 있습니다.
- 혼합 환경은 싱글 사인온을 지원할 수 있습니다.

혼합 모드 지원 사용

혼합 모드 지원을 사용하면 마이그레이션하는 동안 12.52 SP1 정책 서버가 r6.x 또는 r12.x 정책 저장소와 통신할 수 있습니다. 정책 서버를 업그레이드하는 경우 정책 서버 설치 관리자가 해당 정책 저장소 버전을 감지합니다.

정책 저장소가 이전 버전에서 작동하는 경우 설치 관리자는 정책 서버를 업그레이드하고 혼합(호환성) 모드가 사용되도록 설정합니다. 혼합 모드 지원을 비활성화할 수 없습니다.

정책 서버 관리 콘솔을 사용하면 12.52 SP1 정책 서버가 사용하는 정책 저장소 버전을 확인할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 시작합니다.
2. "데이터" 탭을 클릭합니다.
3. "도움말", "정보"를 선택하여 정책 서버 버전을 표시합니다.

   참고: 정책 저장소 버전도 표시됩니다. 정책 저장소 버전은 정책 서버 버전과 일치하지 않습니다.

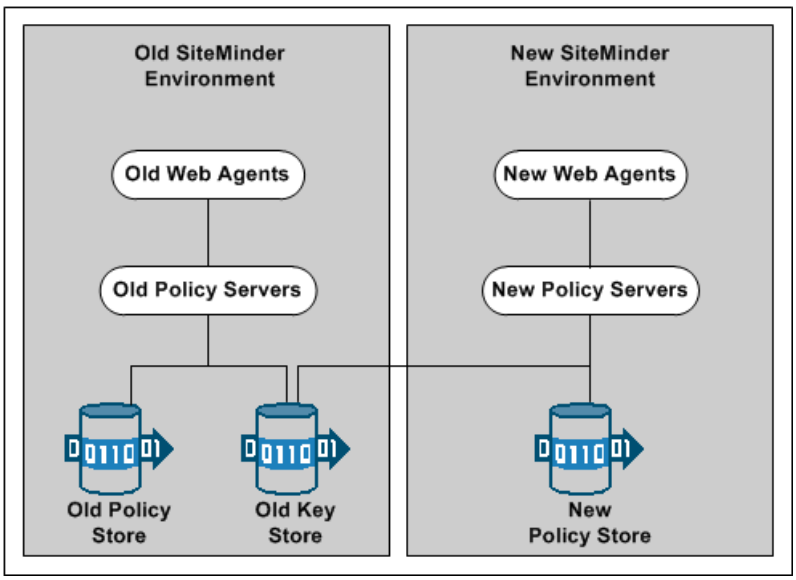
6.x 혼합 모드 지원

r6.x 에서 12.52 SP1 로 마이그레이션할 때 다음 사항을 고려하십시오.

- r6.x 정책 서버는 12.52 SP1 정책 저장소와 통신할 수 없습니다.
- 12.52 SP1 정책 서버는 r6.x 정책 저장소와 통신할 수 있습니다.
- r6.x 및 12.52 SP1 정책 서버는 키 저장소를 공유할 수 있습니다.
- r6.x 및 12.52 SP1 정책 서버는 세션 저장소를 공유할 수 있습니다.
- r6.x 웹 에이전트는 12.52 SP1 정책 서버와 통신할 수 있습니다.

다음 그림은 r6.x 혼합 모드 지원에 대해 설명합니다.

그림 3: r6.x 공용 키 저장소 배포



6.x 혼합 환경의 제한 사항

12.52 SP1 정책 서버는 r6.x 정책 저장소와 통신할 수 있지만 r6.x 정책 서버는 12.52 SP1 정책 저장소에 연결할 수 없습니다. 결과적으로 혼합 환경에서 모든 기존 r6.x 기능은 사용할 수 있지만 r12.x 및 12.52 SP1 에 한정된 기능은 사용할 수 없습니다.

참고: r12.x 및 12.52 SP1 의 기능에 대한 자세한 내용은 릴리스 정보를 참조하십시오.

r12.x 혼합 모드 지원

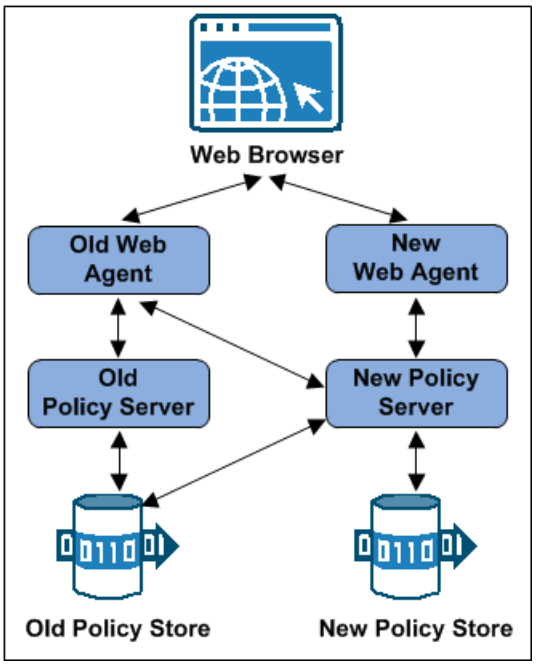
r12.0 SP1 또는 r12.0 SP2 에서 12.52 SP1 로 마이그레이션할 때 다음 사항을 고려하십시오.

- r12.x 정책 서버는 12.52 SP1 정책 저장소와 통신할 수 없습니다.
- 12.52 SP1 정책 서버는 12.52 SP1 정책 저장소와 통신할 수 있습니다.
- r12.x 정책 서버는 12.52 SP1 정책 서버와 키 저장소를 공유할 수 있습니다.

- r12.x 정책 서버는 12.52 SP1 정책 서버와 세션 저장소를 공유할 수 있습니다.
- r12.x 웹 에이전트는 12.52 SP1 정책 서버와 통신할 수 있습니다.

다음 그림은 혼합 모드 지원에 대해 설명합니다.

그림 4: r12.x 혼합 모드 지원



r12.x 혼합 환경의 제한 사항

12.52 SP1 정책 서버는 r12.x 정책 저장소와 통신할 수 있지만 r12.x 정책 서버는 12.52 SP1 정책 저장소에 연결할 수 없습니다. 결과적으로 혼합 환경에서 모든 기존 r12.x 기능은 사용할 수 있지만 12.52 SP1 에 한정된 기능은 사용할 수 없습니다.

참고: 12.52 SP1 의 기능에 대한 자세한 내용은 릴리스 정보를 참조하십시오.

병렬 업그레이드 계획 방법

기존 환경에 추가로 병렬 SiteMinder 환경을 구성하려면 다음 항목을 설치해야 합니다.

- 정책 서버 하나 이상
- 정책 저장소
- 관리 UI
- 웹 에이전트 하나 이상
- CA Business Intelligence(보고서 서버)

참고: 이 안내서에는 두 환경 간의 싱글 사인온을 설정하기 위한 요구 사항이 나와 있습니다.

간단한 테스트 환경 업그레이드 방법

싱글 사인온 또는 장애 조치를 유지해야 하는 경우에만 이 안내서에 설명된 업그레이드 경로를 따르십시오.

테스트 환경에 후자가 필요하지 않은 경우 가장 효율적인 업그레이드 방법은 다음과 같습니다.

1. 12.52 SP1 정책 서버를 설치합니다.

   참고: 새 정책 서버를 설치해야 합니다. 기존 정책 서버를 업그레이드하면 안 됩니다. 정책 서버 설치에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

2. 다음 작업 중 하나를 수행하십시오.

   - r6.x 에서 업그레이드하려면 smobjexport 를 사용하여 r6.x 정책 저장소에서 데이터를 내보냅니다.
   - r12.x 에서 업그레이드하려면 XPSExport 를 사용하여 r12.x 정책 저장소에서 데이터를 내보냅니다.

   참고: 이러한 유틸리티의 사용에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

3. 다음 작업 중 하나를 수행하십시오.
   - r6.x 에서 업그레이드하려면 smobjimport 를 사용하여 r6.x 정책 저장소 데이터를 12.52 SP1 정책 저장소로 가져옵니다.
   - r12.x 에서 업그레이드하려면 XPSImport 를 사용하여 r12.x 정책 저장소 데이터를 12.52 SP1 정책 저장소로 가져옵니다.

   참고: 이러한 유틸리티의 사용에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.
4. SiteMinder r6.x 또는 r12.x 를 제거합니다.

업그레이드나 정책 마이그레이션의 일부로 한 환경의 SiteMinder 정책을 다른 환경으로 이동할 경우 환경과 관련된 일부 개체가 내보내기 파일에 포함됩니다. 이러한 개체에는 다음이 포함됩니다.

- 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.

일반 SiteMinder 환경

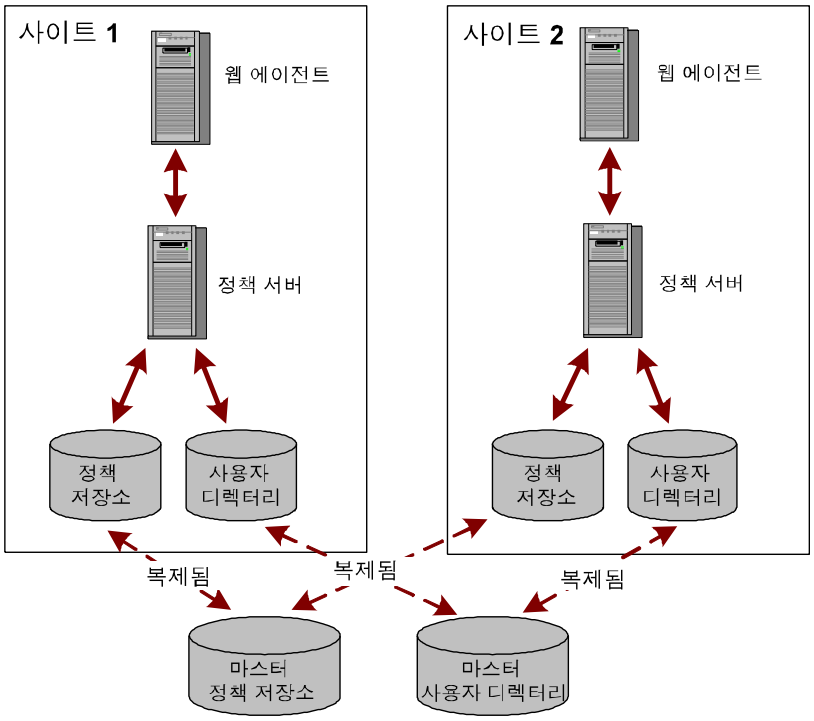
12.52 SP1 로 업그레이드하기 전에 고려해야 할 몇 가지 일반적인 SiteMinder 환경이 있습니다. 사이트가 다음 중 하나와 일치하는지 확인하십시오.

- 단일 정책 저장소, 여러 정책 서버 및 웹 에이전트 (페이지 24)
- 클러스터 환경 (페이지 25)
- 공유 사용자 디렉터리 환경 (페이지 26)

단일 정책 저장소, 여러 정책 서버 및 웹 에이전트

이 SiteMinder 환경에는 전 세계에 위치한 20~100 개의 정책 서버에서 사용되는 단일 정책 저장소가 포함됩니다. 성능상의 이유로 정책 저장소 및 사용자 디렉터리는 자동으로 복제되어 각 정책 서버가 가장 가까운 복제 버전과 통신할 수 있습니다. 각 정책 서버는 50~300 개의 웹 에이전트와 통신합니다.

다음 그림에서는 소규모 배포에서의 이러한 환경을 보여 줍니다.



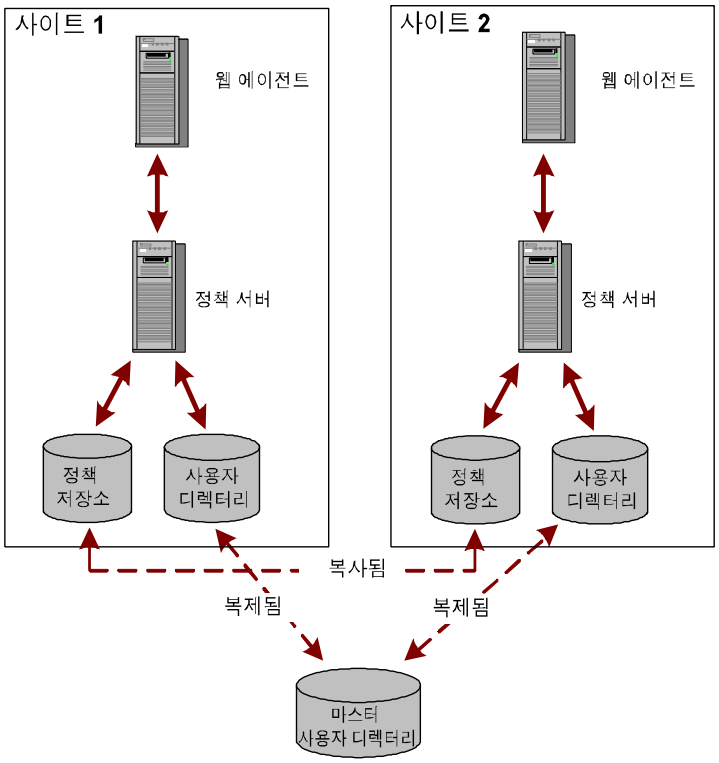
이 환경을 업그레이드하려면 이 안내서에 간략하게 설명된 절차를 따르십시오.

클러스터 환경

클러스터 환경은 단일 정책 저장소와 여러 웹 에이전트 및 정책 서버가 있는 SiteMinder 환경과 유사합니다. 그러나 클러스터에서는 정책 저장소가 복제되지 않고 복사되며, 복사된 저장소는 특정 시점의 정책 저장소 스냅숏이므로 동적으로 업데이트되지 않는다는 차이점이 있습니다. 복제된 저장소는 자동으로 업데이트됩니다. 일반적으로 변경 작업은 기본 데이터베이스에 대해 수행되며, 그런 다음 변경 내용이 보조 데이터베이스로 전파됩니다.

또한 클러스터 사이트를 다른 클러스터 사이트와는 독립적으로 업그레이드하고, 클러스터 사이트 간의 싱글 사인온을 유지할 수 있습니다.

다음 그림에서는 소규모 배포에서의 클러스터 환경을 보여 줍니다.

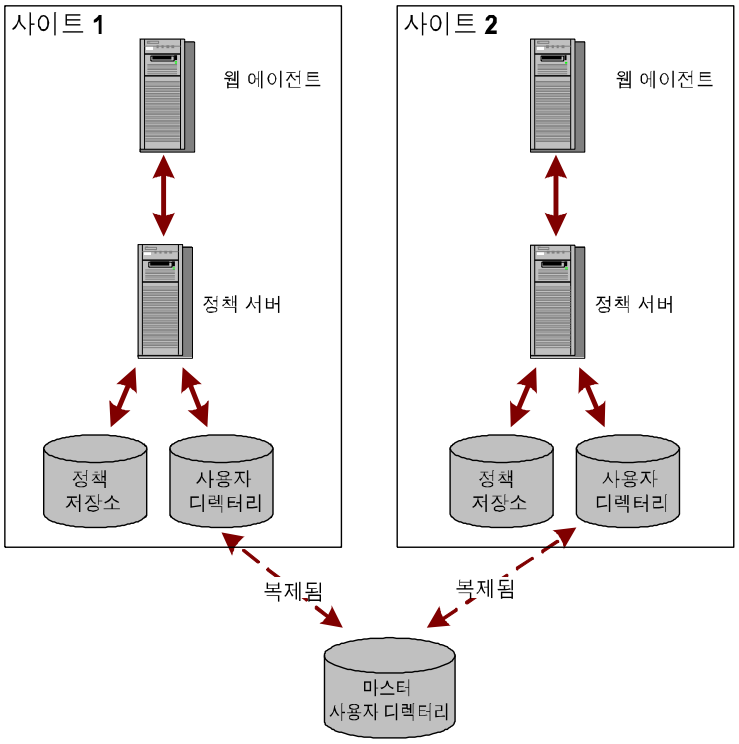


이 환경을 업그레이드하려면 이 안내서에 간략하게 설명된 절차를 따르십시오.

공유 사용자 디렉터리 환경

이 환경에서는 두 사이트에 여러 웹 에이전트와 여러 정책 서버가 있지만 각각이 두 개의 개별 정책 저장소에 저장된 고유한 정책 집합을 유지합니다. 이러한 사이트에서는 동일한 마스터 사용자 디렉터리를 복제하여 싱글 사인온을 유지합니다.

다음 그림에서는 소규모 배포에서의 공유 사용자 디렉터리 환경을 보여 줍니다.



이 환경을 업그레이드하려면 이 안내서에 간략하게 설명된 절차를 따르십시오.

제 2 장: SiteMinder r6.x 에서 업그레이드

이 섹션은 다음 항목을 포함하고 있습니다.

마이그레이션 고려 사항

r6.x 에서 마이그레이션하는 경우 마이그레이션을 시작하기 전에 다음 사항을 고려하십시오.

정책 서버 옵션 팩 지원

PSOP(정책 서버 옵션 팩) 기능은 핵심적인 정책 서버 기능의 일부입니다. PSOP 기능을 사용하는 r6.x 환경을 마이그레이션할 경우 다음 사항을 고려하십시오.

- PSOP 에는 더 이상 별도의 업그레이드가 필요하지 않습니다.
- 정책 서버 설치 관리자는 정책 서버 업그레이드 시 PSOP 구성 파일을 백업하고 PSOP 를 제거합니다.
- 정책 서버 설치 관리자는 정책 서버 업그레이드 시 최신 버전의 PSOP 를 설치합니다.

참고: PSOP 기능을 사용하는 r6.x 환경의 마이그레이션에 대한 자세한 내용은 "r6.x 에서 마이그레이션하는 방법"을 참조하십시오.

12.x 의 Crystal Reports

12.52 SP1 정책 서버 설치 관리자에는 Crystal Reports 9.0 과 호환되는 보고서 파일(.rpt)이 더 이상 포함되어 있지 않습니다. SiteMinder 보고서는 이제 12.52 SP1 관리 UI 와 통합되어 있습니다. 보고서 서버를 설치하는 데는 별도의 설치 관리자를 사용할 수 있습니다. 보고서 서버는 보고서(r6.x 에서 사용 가능한 보고서 포함)를 예약하고 보는 데 필요합니다.

다음 사항을 고려하십시오.

- 마이그레이션 중에 Crystal Reports 서버와 함께 보고서 파일을 계속 사용하여 보고서를 예약하고 볼 수 있습니다. 12.52 SP1 정책 서버는 r6.x 감사 로그 데이터베이스와 통신할 수 있습니다.
- 정책 서버 업그레이드 시 r6.x 보고서 데이터 원본은 제거됩니다. 따라서 r6.x 보고서 데이터 원본을 백업해 두십시오.
- 마이그레이션의 마지막 단계에서는 관리 UI 를 설치하고 r6.x 정책 서버 인터페이스의 사용을 중단합니다. 마이그레이션을 완료한 후에는 보고서 파일에 액세스할 수 없습니다. 또한 r6.x 정책 서버 사용자 인터페이스에서 보고서 파일을 사용하여 생성된 보고서에 액세스할 수 없습니다. 이러한 보고서에 액세스해야 하는 경우 r6.x 정책 서버 사용자 인터페이스의 사용을 중단하기 전에 해당 보고서를 백업하는 것이 좋습니다.
- 12.52 SP1 관리 UI 를 사용하여 r6.x 에서 사용할 수 있었던 보고서를 예약하고 볼 수 있습니다.

참고: 보고서 서버 설치에 대한 자세한 내용은 "정책 서버 설치 안내서"를 참조하십시오. 보고서 예약 및 보기에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

관리자 인증

이 릴리스에서는 정책 서버 사용자 인터페이스가 SiteMinder 관리 UI 로 대체됩니다.

기본적으로 관리 UI 는 다음과 같습니다.

- 정책 저장소를 관리자 아이덴티티의 원본으로 사용합니다.

  기본 구성을 사용하면 관리 UI 설치 후 즉시 환경을 관리할 수 있습니다. 외부 사용자 저장소에 저장된 기존 r6.x 관리자는 관리 UI 에서 사용할 수 없습니다.
- 사용자 이름과 암호를 묻는 메시지만 표시됩니다. SiteMinder 가 관리 UI 를 보호하지 않습니다.

다음과 같이 외부 관리자 저장소 연결을 구성합니다.

- 관리 UI 에서 r6.x 관리자를 사용할 수 있게 설정합니다.
- SiteMinder 를 사용하여 관리 UI 를 보호합니다.

  참고: 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

인증서 데이터 관리

인증서 데이터 저장소는 SiteMinder 키 데이터베이스(smkeydatabase)를 대체합니다. 환경에 하나 이상의 smkeydatabase 를 배포한 경우에는 다음 사항을 고려하십시오.

- 인증서 데이터 저장소는 12.52 SP1 정책 저장소와 같은 곳에 배치됩니다. 인증서 데이터 저장소 하나가 있으면 각 정책 서버 호스트 시스템마다 개별적인 smkeydatabase 인스턴스가 있을 필요가 없습니다.
- 정책 서버 업그레이드의 일환으로 모든 smkeydatabase 콘텐츠가 자동으로 백업되고 인증서 데이터 저장소로 마이그레이션됩니다.
- 12.52 SP1 정책 서버는 인증서 데이터 저장소와만 통신할 수 있습니다. 12.52 SP1 정책 서버와 해당 로컬 smkeydatabase 는 호환성 모드에서 작동하지 않습니다. 하지만 업그레이드되지 않은 모든 정책 서버는 계속해서 로컬 버전의 smkeydatabase 와 통신합니다.

  중요! smkeydatabase 의 마이그레이션이 실패한 경우 정책 서버를 환경으로 되돌리지 마십시오. 마이그레이션 실패 후 정책 서버를 되돌리면 인증서 데이터가 필요한 모든 트랜잭션이 실패합니다.
- 마이그레이션을 시작하기 전에 모든 smkeydatabase 인스턴스를 동기화하십시오. 모든 인스턴스를 동기화하면 데이터 충돌을 방지할 수 있습니다. 데이터 충돌이 있으면 마이그레이션에 성공할 수 없습니다.
- 동일한 정책 저장소에 대한 공통의 뷰를 공유하는 모든 정책 서버는 동일한 키, 인증서 및 CRL(인증서 해지 목록)에 액세스할 수 있습니다.
- 인증서 데이터 저장소의 용도는 smkeydatabase 의 용도에서 변경되지 않고 유지됩니다. 이 저장소는 SiteMinder 환경에서 다음을 사용할 수 있게 합니다.
  - CA(인증 기관) 인증서
  - 공개 키 및 개인 키
  - 인증서 해지 목록

- SiteMinder 키 도구를 사용하여 인증서 데이터 저장소를 계속 관리할 수 있습니다. 하지만 몇 가지 옵션은 더 이상 사용할 수 없습니다.

  참고: 자세한 내용은 *정책 서버 릴리스 정보*를 참조하십시오.

- CRL 이 LDAP 디렉터리 서비스에 저장된 경우 다음 사항을 고려하십시오.
  - SiteMinder 에서는 더 이상 CRL 의 발급자가 해당 루트 인증서를 발급한 CA 와 동일하지 않아도 됩니다.
  - SiteMinder 에서는 더 이상 인증서 해지 목록의 발급자를 확인하지 않습니다. 이 동작은 텍스트 기반 CRL 에 대한 요구 사항과 일치합니다.

페더레이션 통합

이 릴리스에서는 정책 서버 사용자 인터페이스가 관리 UI 로 대체됩니다. 이전에 Federation Security Services 를 관리했던 경우 이제는 이 기능을 레거시 페더레이션이라고 합니다.

관리 UI 에는 파트너 관계 페더레이션도 포함됩니다. 이 기능은 CA SiteMinder?Federation 를 통해 사용할 수 있는 파트너 관계 기반 페더레이션에 한정됩니다.

싱글 사인온

12.52 SP1 로 마이그레이션하는 동안 싱글 사인온을 유지할 수 있습니다. 다음 사항을 고려하십시오.

- 12.52 SP1 정책 서버는 r6.x 정책 저장소 및 r6.x 키 저장소와 통신할 수 있습니다.
- 12.52 SP1 정책 서버는 r6.x 세션 저장소와 통신할 수 있습니다.

정책 저장소 손상 방지

가능한 정책 저장소 손상을 방지하려면 정책 저장소를 호스트하는 서버가 개체를 UTF-8 형식으로 저장하도록 구성되어 있는지 확인하십시오.

참고: 개체를 UTF-8 형식으로 저장하도록 서버를 구성하는 방법에 대한 자세한 내용은 해당 공급업체의 설명서를 참조하십시오.

Advanced Password Services

고급 암호 서비스를 배포한 경우 정책 서버 업그레이드 시 모든 LANG(번역), CFG(구성) 및 메일 파일이 유지됩니다. 12.52 SP1 버전의 기본 파일은 *siteminder_home*\samples 에 설치됩니다

siteminder_home

정책 서버 설치 경로를 지정합니다.

r6.x 마이그레이션 작동 방식

여러 정책 서버 및 웹 에이전트가 포함된 SiteMinder 배포를 업그레이드하려면 SiteMinder 환경에서 정책 서버 및 웹 에이전트 중 하나를 제거하십시오. 이러한 구성 요소가 업그레이드되는 동안 나머지 정책 서버 및 웹 에이전트에서 리소스를 계속 보호합니다.

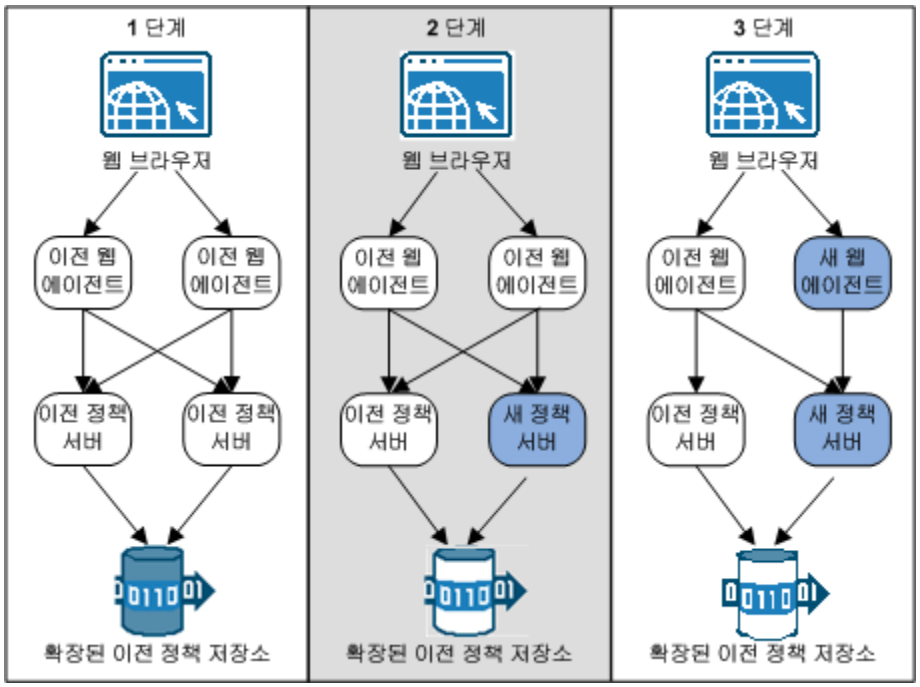
모든 구성 요소가 업그레이드되거나 혼합 모드 호환성 상태로 작동할 때까지 SiteMinder 구성 요소 제거 및 업그레이드를 계속하십시오.

다음 그림에서는 간단한 r6.x 환경과 상세 정보를 보여 줍니다.

- 기존 구성 요소 업그레이드 순서
- 새 구성 요소 설치 순서

참고: 각 그림에는 단일 정책 저장소가 있습니다. 이 정책 저장소에는 키 저장소가 포함되어 있습니다. 실제 사용 환경에서는 별개의 정책 저장소와 키 저장소를 사용할 수 있습니다.

그림 5: r6 SP5 마이그레이션. 1~3 단계



1. 1 단계에서는 r6.x 정책 저장소 스키마가 확장됩니다.

   기존 r6.x 정책 저장소 스키마는 아직 변경되지 않았습니다. 12.52 SP1 마이그레이션을 수행하려면 12.52 SP1 에 필요한 개체의 정책 저장소에 맞게 정책 저장소 스키마를 확장해야 합니다.

   smkeydatabase 를 배포한 경우 첫 번째 정책 서버를 업그레이드하기 전에 정책 저장소 스키마를 확장하십시오. 스키마를 확장하면 정책 서버 업그레이드 시 smkeydatabase 를 인증서 데이터 저장소로 마이그레이션할 수 있도록 정책 저장소가 준비됩니다. 스키마를 확장해도 호환성 모드에는 영향이 없습니다. 정책 저장소는 r6.x 에서와 같이 계속해서 작동합니다.

   smkeydatabase 를 배포하지 않은 경우에는 정책 저장소 업그레이드 프로세스의 일부로 스키마를 확장하십시오.

2. 2 단계에서는 r6.x 정책 서버가 12.52 SP1 로 업그레이드됩니다. 12.52 SP1 정책 서버는 호환성 모드에서 작동합니다. 다음 사항을 고려하십시오.
   - r6.x 웹 에이전트는 12.52 SP1 정책 서버와 계속해서 통신합니다.
   - 12.52 SP1 정책 서버는 r6.x 정책 및 키 저장소와 계속해서 통신합니다.
   - r6.x 정책 서버는 r6.x 정책 및 키 저장소와 계속해서 통신합니다. r6.x 정책 서버 사용자 인터페이스를 계속해서 사용하여 r6.x 정책 서버를 통해 r6.x 정책 저장소를 관리할 수 있습니다.
   - 정책 서버 설치 관리자는 업그레이드 시 정책 서버 사용자 인터페이스를 제거합니다. 12.52 SP1 정책 서버는 액세스 제어를 계속해서 제공하고 감사 정보가 포함된 로그 파일을 생성합니다. 그러나 관리 UI 를 설치할 때까지는 12.52 SP1 정책 서버를 통해 r6.x 정책 저장소를 관리할 수 없습니다.
   - 12.52 SP1 정책 서버는 12.52 SP1 인증서 데이터 저장소와만 통신할 수 있습니다. 레거시 페더레이션 환경을 업그레이드할 경우 정책 서버 설치 관리자는 기존의 모든 smkeydatabase 콘텐츠를 인증서 데이터 저장소로 마이그레이션하려고 시도합니다.

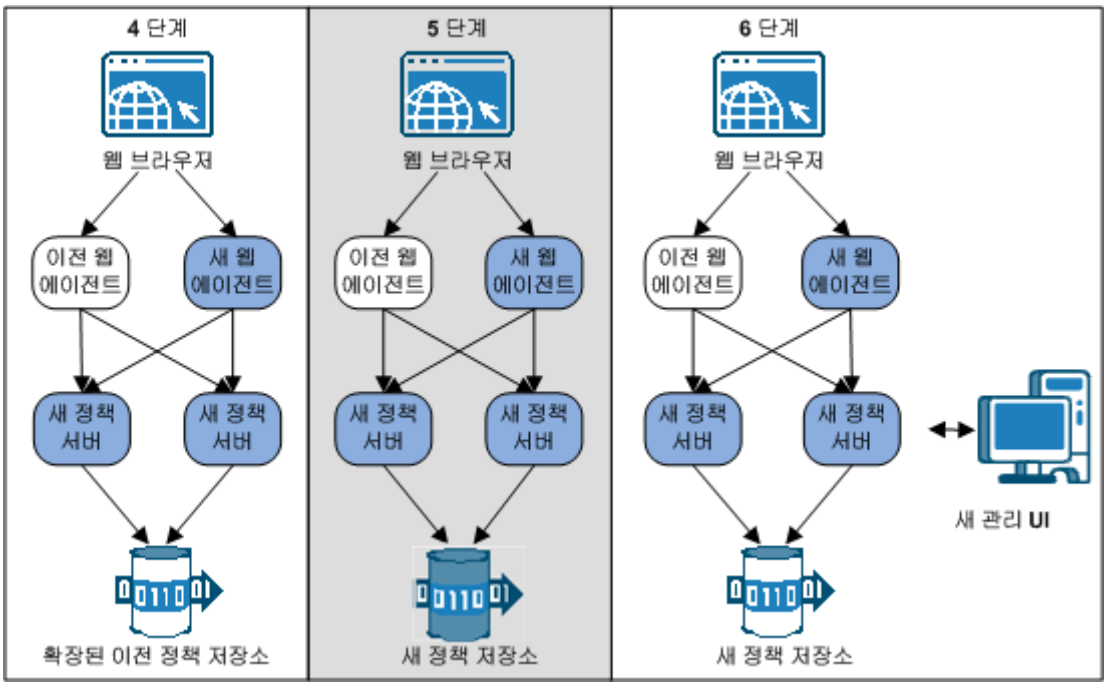
     중요! smkeydatabase 의 마이그레이션이 실패한 경우 정책 서버를 환경으로 되돌리지 마십시오. 마이그레이션 실패 후 정책 서버를 되돌리면 인증서 데이터가 필요한 모든 트랜잭션이 실패합니다.
3. 3 단계에서는 r6.x 웹 에이전트가 12.52 SP1 로 업그레이드됩니다. 다음 사항을 고려하십시오.
   - r6.x 웹 에이전트는 r6.x 및 12.52 SP1 정책 서버와 계속해서 통신합니다.
   - 12.52 SP1 웹 에이전트는 12.52 SP1 정책 서버와만 통신합니다.

     참고: 정책 저장소가 12.52 SP1 로 업그레이드될 때까지는 12.52 SP1 정책 서버로 새 12.52 SP1 에이전트를 구성할 수 없습니다.

4. 4 단계에서는 나머지 정책 서버가 12.52 SP1 로 업그레이드됩니다. 12.52 SP1 정책 서버는 r6.x 정책 및 키 저장소와의 호환성 모드에서 작동합니다.

   중요! 모든 정책 서버가 리소스를 계속 보호하고 정책 서버 관리 콘솔에 액세스할 수 있더라도 정책 서버를 관리할 수 없습니다. 정책 서버 설치 프로그램이 업그레이드 도중 정책 서버 사용자 인터페이스를 제거했기 때문입니다. 12.52 SP1 관리 UI 를 설치하기 전까지는 정책 저장소의 정책 정보를 관리할 수 없습니다. 마이그레이션을 계획할 때 이 시기를 고려하십시오.

그림 6: r6 SP^ 마이그레이션. 4~6 단계



5. 5 단계에서는 r6.x 정책 및 키 저장소가 12.52 SP1 로 업그레이드됩니다.
6. 6 단계에서는 관리 UI 가 설치되고 정책 서버에 등록됩니다. 다음 사항을 고려하십시오.
   - 정책 저장소를 업그레이드하기 전에 관리 UI 를 설치할 수 있습니다. 하지만 정책 서버가 업그레이드되기 전에는 관리 UI 를 등록할 수 없습니다. 정책 서버 업그레이드 전에 관리 UI 를 설치하면 정책 저장소가 관리 UI 를 사용하지 못하는 시간이 최소화됩니다.
   - 그림에는 혼합 모드 호환성의 예로 r6.x 웹 에이전트가 나와 있습니다.

7. (선택 사항) 그림에는 나와 있지 않지만 마지막 단계에서는 보고서 서버가 설치 및 등록됩니다.

r6.x 에서 마이그레이션하는 방법

r6.x 에서 12.52 SP1 로의 마이그레이션을 완료하려면 다음 단계를 수행하십시오.

1. *정책 서버 릴리스 정보*에서 설치 및 업그레이드 고려 사항을 검토합니다.
2. 정책 저장소 스키마 파일을 다운로드합니다.
3. r6.x 정책 저장소 스키마를 확장합니다.
4. 환경에 smkeydatabase 인스턴스가 여러 개인 경우 이를 동기화합니다. 정책 서버를 업그레이드하는 중에 설치 관리자는 smkeydatabase 의 모든 콘텐츠를 인증서 데이터 저장소로 마이그레이션하려고 시도합니다.
5. "정책 서버를 업그레이드하기 전에"의 단원을 검토합니다.
6. r6.x 정책 서버를 12.52 SP1 로 업그레이드합니다.
7. "정책 서버를 업그레이드한 후에"를 검토합니다.
8. r6.x 웹 에이전트를 12.52 SP1 로 업그레이드합니다.
9. 나머지 r6.x 정책 서버 및 r6.x 웹 에이전트를 각각 12.52 SP1 로 업그레이드합니다.
10. r6.x 정책 및 키 저장소를 12.52 SP1 로 업그레이드합니다.
11. 12.52 SP1 관리 UI 를 설치합니다.
12. (선택 사항) 보고서 서버를 설치합니다.

    참고: 보고서 서버 설치에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

정책 저장소 스키마 파일 다운로드

정책 서버 저장소 스키마를 확장하는 데 필요한 파일은 정책 서버 설치 zip 의 루트에 있습니다.

12.52 SP1 의 기본 릴리스로 업그레이드하는 경우 다음 단계를 수행하십시오.

1. CA Support 사이트에 로그인합니다.
2. "Support"(지원) 아래에서 "Support by Product"(제품별 지원)를 클릭합니다.
3. "Select a Product Page"(제품 페이지 선택) 필드에 "SiteMinder"를 입력하고 Enter 키를 누릅니다.
4. "Select a Product Page"(제품 페이지 선택) 목록에서 "Downloads"(다운로드)를 클릭합니다.
5. 제품 선택 목록에서 특정 SiteMinder 제품을 찾아서 해당 SiteMinder 제품을 찾습니다. 이름을 클릭합니다.
6. 릴리스와 gen 레벨을 선택한 다음 "Go"(이동)를 클릭합니다.
7. 정책 서버 설치 zip 을 로컬에 저장하고 임시 위치에 압축을 풉니다.

   정책 저장소 스키마 파일은 policy_store_schema_ext.zip 에 있습니다.

12.52 SP1 의 누적 릴리스(cr)로 업그레이드하는 경우 다음 단계를 수행하십시오.

1. CA Support 사이트에 로그인합니다.
2. "Support"(지원) 아래에서 "Support by Product"(제품별 지원)를 클릭합니다.
3. "Select a Product Page"(제품 페이지 선택) 필드에 "SiteMinder"를 입력하고 Enter 키를 누릅니다.
4. "Select a Product Page"(제품 페이지 선택) 목록에서 "Recommended Reading"(권장 참고 자료)을 클릭합니다.
5. "Recommended Reading"(권장 참고 자료) 목록에서 "SiteMinder Hotfix/Cumulative Release Hot Index"(SiteMinder 핫픽스/누적 릴리스 핫 인덱스)를 클릭합니다.
6. SiteMinder Web Access Manager 를 클릭합니다.
7. 원하는 누적 릴리스를 클릭합니다.

8. 누적 릴리스를 다운로드합니다.
9. 정책 서버 설치 zip 을 로컬에 저장하고 임시 위치에 압축을 풉니다.

   정책 저장소 스키마 파일은 policy_store_schema_ext.zip 에 있습니다.

정책 저장소 스키마 확장

기존 r6.x 정책 저장소 스키마는 아직 변경되지 않았습니다. 12.52 SP1 마이그레이션을 수행하려면 12.52 SP1 에 필요한 개체의 정책 저장소에 맞게 정책 저장소 스키마를 확장해야 합니다.

smkeydatabase 를 배포한 경우 첫 번째 정책 서버를 업그레이드하기 전에 정책 저장소 스키마를 확장하십시오. 스키마를 확장하면 정책 서버 업그레이드 시 smkeydatabase 를 인증서 데이터 저장소로 마이그레이션할 수 있도록 정책 저장소가 준비됩니다. 스키마를 확장해도 호환성 모드에는 영향이 없습니다. 정책 저장소는 r6.x 에서와 같이 계속해서 작동합니다.

smkeydatabase 를 배포하지 않은 경우에는 정책 저장소 업그레이드 프로세스의 일부로 스키마를 확장하십시오.

Active Directory Server 를 위한 정책 저장소 스키마 확장

다음 단계를 수행하십시오.

1. 다음 ZIP 파일을 정책 서버 호스트 시스템에 복사하고 임시 위치에 압축을 풉니다.

   `policy_store_schema_ext.zip`
2. 다음 디렉터리로 이동합니다.

   `schema_extension\db\Active Directory`
3. ActiveDirectory.ldif 파일을 열고 <RootDN>의 각 인스턴스를 정책 저장소 스키마 위치를 나타내는 DN(도메인 이름)으로 수동으로 바꿉니다. 정책 저장소 개체 위치를 사용하지 마십시오.

   예: 다음 루트 DN 은 정책 저장소 개체를 나타냅니다.

   `ou=policystore,dc=domain,dc=com`

   <RootDN>의 각 인스턴스를 다음 DN 으로 바꾸십시오.

   `dc=domain,dc=com`
4. 파일을 저장합니다.

5. 명령 창에서 *siteminder_home*/bin 으로 이동합니다.

   siteminder_home

   정책 서버 설치 경로를 지정합니다.

6. 다음 명령을 실행합니다.

   ```
   smldapsetup ldmod -fpath/ActiveDirectory.ldif
   ```

   path

   스키마 파일의 경로를 지정합니다.

   정책 저장소 스키마가 확장됩니다.

정책 저장소 스키마를 Active Directory LDS Server 에 대해 확장

다음 단계를 수행하십시오.

1. 다음 ZIP 파일을 정책 서버 호스트 시스템에 복사하고 임시 위치에 압축을 풉니다.

   ```
   policy_store_schema_ext.zip
   ```

2. 다음 디렉터리로 이동합니다.

   ```
   schema_extension\db\Active Directory LDS
   ```

3. ADLDS.ldif 파일을 열고 {guid}의 각 인스턴스를 중괄호로 묶은 GUID 의 실제 값으로 바꿉니다.

   예: {CF151EA3-53A0-44A4-B4AC-DA0EBB1FF200}

4. 파일을 저장합니다.

5. 명령 창에서 *siteminder_home*/bin 으로 이동합니다.

   siteminder_home

   정책 서버 설치 경로를 지정합니다.

6. 다음 명령을 실행합니다.

   ```
   smldapsetup ldmod -fpath/ADLDS.ldif
   ```

   path

   스키마 파일의 경로를 지정합니다.

   정책 저장소 스키마가 확장됩니다.

정책 저장소 스키마를 CA Directory Server 에 대해 확장

다음 단계를 수행하십시오.

1. 다음 ZIP 파일을 CA Directory 호스트 시스템에 복사하고 임시 위치에 압축을 풉니다.

   `policy_store_schema_ext.zip`

2. 다음 디렉터리로 이동합니다.

   `schema_extension\db\CA Directory`

3. 다음 파일을 CA Directory DXHOME\config\schema 디렉터리에 복사합니다.

   `etrust.dxc`

4. SiteMinder 스키마 파일(.dxg)을 열고 파일의 맨 끝에 다음 행을 추가합니다.

   ```
   #CA Schema
   source "netegrity.dxc"
   source "etrust.dxc"
   ```

5. 파일 끝에 다음 행을 추가하여 DSA 용 DXI 파일을 편집합니다.

   - **r12**

     ```
     # cache configuration
     set max-cache-size = 100;
     set cache-attrs = all-attributes;
     set cache-load-all = true;
     set ignore-name-bindings = true;
     ```

     참고: DXI 파일은 DXHOME\config\servers 에 있습니다. max-cache-size 항목은 총 캐시 크기(MB 단위)입니다. CA Directory Server 에서 사용할 수 있는 총 메모리와 정책 저장소의 전체 크기에 따라 이 값을 조정하십시오.

   - **r12 SP1 이상**

     ```
     # cache configuration
     #set max-cache-size = 100;
     #set cache-attrs = all-attributes;
     #set cache-load-all = true;
     set ignore-name-bindings = true;
     ```

6. DSA 에 대한 기본 DXC 파일(default.dxc)을 열고 다음 섹션을 찾습니다.

```
# size limits
set max-users = 255;
set credits = 5;
set max-local-ops = 100;
set max-dsp-ops = 100;
set max-op-size = 200;
set multi-write-queue = 20000;
```

참고: 기본 DXC 파일은 DXHOME\dxserver\config\limits 에 있습니다.

7. 다음 설정과 일치하도록 설정을 편집하고 DXC 파일을 저장합니다.

```
# size limits
set max-users = 1000;
set credits = 5;
set max-local-ops = 1000;
set max-dsp-ops = 1000;
set max-op-size = 4000;
set multi-write-queue = 20000;
```

참고: 크기 제한 설정을 편집하면 캐시 크기 오류가 CA Directory 로그 파일에 표시되지 않습니다.

중요! multi-write-queue 설정은 텍스트 기반 구성 전용입니다. DXmanager 를 사용하여 DSA 를 설치한 경우에는 이 설정을 생략하십시오.

8. JXplorer 를 사용하여 정책 저장소 DSA 에 액세스합니다.
9. 루트 요소를 찾은 후에 다음과 같은 기본 트리 구조를 찾습니다.

   Netegrity, SiteMinder, PolicySvr4

10. PolicySvr4 아래에서 다음과 같은 이름의 조직 단위(루트 요소)를 생성합니다.

    XPS

11. 다음 명령을 사용하여 DSA 를 중지했다가 다시 시작합니다(DSA 사용자로).

    `dxserver stop *DSA_Name*`

    `dxserver start *DSA_Name*`

    DSA_Name

    정책 저장소 DSA 의 이름을 지정합니다.

    정책 저장소 스키마가 확장됩니다.

IBM DB2 Server 를 위한 정책 저장소 스키마 확장

다음 단계를 수행하십시오.

1. 다음 ZIP 파일을 IBM DB2 호스트 시스템에 복사하고 임시 위치에 압축을 풉니다.

   `policy_store_schema_ext.zip`

2. 다음 디렉터리로 이동합니다.

   `schema_extension\db\IBM DB2`

3. 다음 파일을 찾습니다.
   `DB2.sql`

4. 명령 프롬프트를 열고 다음 명령을 실행합니다.
   `db2 -td@ [-v] -f path\DB2.sql`

   path

   DB2 스키마 파일의 경로를 지정합니다.

   정책 저장소 스키마가 확장됩니다.

IBM Tivoli Directory Server 를 위한 정책 저장소 스키마 확장

다음 단계를 수행하십시오.

1. IBM Tivoli Directory Server 관리 도구를 사용하여 정책 저장소 기본 트리 구조를 업데이트합니다. ou=Netegrity,ou=SiteMinder,ou=PolicySvr4 아래에 다음과 같은 루트 노드를 생성합니다.

   `ou=XPS`

2. 다음 ZIP 파일을 IBM Directory Server 호스트 시스템에 복사하고 임시 위치에 압축을 풉니다.

   `policy_store_schema_ext.zip`

3. 다음 디렉터리로 이동합니다.

   `schema_extension\db\IBM Tivoli Directory Server`

4. 다음 파일을 찾습니다.

   `IBMDirectoryServer.ldif`

5. IBM Directory Server Configuration Tool 을 사용하여 다음 파일을 스키마 구성의 "Manage Schema Files"(스키마 파일 관리) 섹션에 추가합니다.

   `IBMDirectoryServer.ldif`

6. 디렉터리 서버를 다시 시작합니다.

   정책 저장소 스키마가 확장됩니다.

Novell eDirectory Server 를 위한 정책 저장소 스키마 확장

다음 단계를 수행하십시오.

1. 다음 ZIP 파일을 정책 서버 호스트 시스템에 복사하고 임시 위치에 압축을 풉니다.

   `policy_store_schema_ext.zip`

2. 다음 디렉터리로 이동합니다.

   `schema_extension\db\Novell eDirectory`

3. 다음 파일을 찾아서 엽니다.

   `Novell.ldif`

4. 명령 창에서 *siteminder_home*\bin 으로 이동합니다.

   siteminder_home

   정책 서버 설치 경로를 지정합니다.

5. 다음 명령을 실행합니다.

   `ldapsearch -h`*`host`* `-p`*`port`* `-b`*`container`* `-s`*`sub`* `-D`*`AdminDN`* `-w`*`AdminPW`* `objectclass=ncpServer dn`

   예:

   `ldapsearch -h`*`192.168.1.47`* `-p`*`389`* `-b`*`o=nwqa47container`* `-s`*`sub`* `-d`*`cn=admin,o=nwqa47container`* `-w`*`password`* `objectclass=ncpServer dn`

   Novell 서버 DN 이 열립니다.

6. 열린 스키마 파일을 편집합니다. 모든 <ncpserver> 변수를 Novell 서버 DN(도메인 이름)의 값으로 바꿉니다.

   예: Novell 서버 DN 값이 cn=servername,o=servercontainer 인 경우 <ncpserver>의 모든 인스턴스를 다음 값으로 바꿉니다.

   `cn=servername,o=servercontainer`

7. 스키마 파일을 저장한 후 닫습니다.
8. 다음 명령을 실행합니다.

   ```
   smldapsetup ldmod -fpath\Novell.ldif
   ```

   -f*path*

   스키마 파일의 경로를 지정합니다.

   정책 저장소 스키마가 확장됩니다.

OpenLDAP Server 를 위한 정책 저장소 스키마 확장

다음 단계를 수행하십시오.

참고: 이 절차에서는 OpenLDAP 서버가 /usr/local/etc/openldap 에 있고 스키마 파일이 스키마 하위 디렉터리에 있다고 가정합니다.

1. 정책 저장소 기본 트리 구조를 업데이트합니다.
   ou=Netegrity,ou=SiteMinder,ou=PolicySvr4 아래에 다음과 같은 루트 노드를 생성합니다.

   ```
   ou=XPS
   ```

2. 다음 ZIP 파일을 OpenLDAP 호스트 시스템에 복사하고 임시 위치에 압축을 풉니다.

   ```
   policy_store_schema_ext.zip
   ```

3. 다음 디렉터리로 이동합니다.

   ```
   schema_extension\db\OpenLDAP
   ```

4. 다음 스키마 파일을 찾습니다.

   ```
   openldap_attribute_XPS.schema
   openldap_object_XPS.schema
   ```

5. 4 단계에서 찾은 스키마 파일을 OpenLDAP 설치 디렉터리의 스키마 폴더에 복사합니다.
6. slapd 구성 파일의 include 섹션에 다음 항목을 입력합니다.

   ```
   ....
   .....
   include /usr/local/etc/openldap/schema/openldap_attribute_XPS.schema
   include /usr/local/etc/openldap/schema/openldap_object_XPS.schema
   ```

   정책 저장소 스키마가 확장됩니다.

Oracle Internet Directory Server 를 위한 정책 저장소 스키마 확장

다음 단계를 수행하십시오.

1. Oracle Internet Directory 호스트 시스템에 로그인합니다.
2. Oracle 카탈로그 명령줄 도구를 사용하여 다음 특성을 인덱싱합니다. 특성을 인덱싱하면 기본 정책 저장소 개체를 가져올 때 오류가 발생하지 않습니다.

   `modifyTimestamp`

   다음 명령을 실행합니다.

   oracle_home`/ldap/bin/catalog connect=`*conn_str* `add=TRUE attribute=modifyTimestamp`

   oracle_home

   Oracle Internet Directory 설치 경로를 지정합니다.

   conn_str

   디렉터리 데이터베이스 연결 문자열을 지정합니다. tnsnames.ora 파일을 구성한 경우 이 파일에 지정된 net 서비스 이름을 입력합니다.

   참고: 카탈로그 명령줄 도구에 대한 자세한 내용은 Oracle 설명서를 참조하십시오.
3. 다음 ZIP 파일을 정책 서버 호스트 시스템에 복사하고 임시 위치에 압축을 풉니다.

   `policy_store_schema_ext.zip`
4. 다음 디렉터리로 이동합니다.

   `schema_extension\db\Oracle Internet Directory`
5. 다음 파일을 찾습니다.

   `OID_10g.ldif`
6. 명령 창에서 *siteminder_home*\bin 으로 이동합니다.

   siteminder_home

   정책 서버 설치 경로를 지정합니다.
7. 다음 명령을 실행합니다.

   `ldapmodify -h`*host* `-p`*port* `-d`*AdminDN* `-w`*AdminPW*
   `-c -f`*path*`\OID_10g.ldif`
   `-Z -P`*cert*

-h*host*

LDAP 디렉터리 서버의 IP 주소를 지정합니다.

예: 123.123.12.12

-p*port*

LDAP 디렉터리 서버의 포트 번호를 지정합니다.

예: 3500

-d*AdminDN*

LDAP 스키마를 생성할 수 있는 권한이 있는 LDAP 사용자의 이름을 지정합니다.

-w*AdminPW*

–d 옵션으로 지정된 관리자의 암호를 지정합니다.

-c

연속 모드(오류 시 중지되지 않음)를 지정합니다.

-f*path*

추출된 스키마 파일의 경로를 지정합니다.

-Z

SSL 로 암호화되는 연결을 지정합니다.

-P*cert*

SSL 클라이언트 인증서 데이터베이스 파일(cert7.db)이 있는 디렉터리의 경로를 지정합니다.

예:

cert7.db 가 app/siteminder/ssl 에 있는 경우 다음을 지정합니다.

```
-Papp/siteminder/ssl
```

정책 저장소 스키마가 확장됩니다.

Red Hat Directory Server 를 위한 정책 저장소 스키마 확장

다음 단계를 수행하십시오.

1. 다음 ZIP 파일을 정책 서버 호스트 시스템에 복사하고 임시 위치에 압축을 풉니다.

   `policy_store_schema_ext.zip`

2. 다음 디렉터리로 이동합니다.

   `schema_extension\db\Red Hat Directory Server`

3. 다음 파일을 찾습니다.

   `RedHat_7_1.ldif`

4. 명령 창에서 *siteminder_home*/bin 으로 이동합니다.

   siteminder_home

   정책 서버 설치 경로를 지정합니다.

5. 다음 명령을 실행합니다.

   `smldapsetup ldmod -f`*`path`*`/RedHat_7_1.ldif`

   path

   추출된 스키마 파일의 경로를 지정합니다.

   정책 저장소 스키마가 확장됩니다.

Siemens DirX Server 를 위한 정책 저장소 스키마 확장

다음 단계를 수행하십시오.

1. DirXmanage 도구를 사용하여 정책 저장소 기본 트리 구조를 업데이트합니다. 다음과 같은 기존 루트 경로 아래로 이동합니다.

   `ou=Netegrity,ou=SiteMinder,ou=PolicySvr4`

   여기에 다음과 같은 루트 노드를 생성합니다.

   `ou=XPS`

2. ZIP 파일 policy_store_schema_ext.zip 을 Siemens DirX 호스트 시스템에 복사하고 임시 위치에 압축을 풉니다.

3. 다음 디렉터리로 이동합니다.

   `schema_extension\db\Siemens DirX`

4. 압축이 풀린 다음의 파일을 찾아서 *DirX_install_path*\scripts\security\Netegrity\SiteMinder 에 복사합니다.
   - bind.tcl
   - GlobalVar.tcl
   - l-bind.cp
   - schema_ext_for_XPS.adm

   DirX_install_path

   DirX 설치 경로를 지정합니다.

   예: C:\program files\siemens\dirx

5. 압축 해제된 파일 dirxabbr-ext.XPS 를 찾아서 *DirX_install_path*\client\conf 에 복사합니다.
6. DirX 서비스를 중지했다가 다시 시작합니다.
7. GlobalVar.tcl 파일을 편집하여 DirX 스크립트가 참조하는 전역 변수를 업데이트합니다.

   기본값:
   - LDAP 포트: 389
   - 루트 DN: o=pqr
   - 관리자 사용자 이름: cn=admin,o=pqr
   - 관리자 암호: dirx

   참고: 값을 수정하여 기존 설정에 적용되도록 합니다.
8. *DirX_install_path*\scripts\security\CA\SiteMinder 로 이동합니다.
9. 다음 명령을 실행합니다.

   ```
   dirxadm schema_ext_for_XPS.adm
   ```
10. DirXmanage 유틸리티를 사용하여 DSA 로 리바인딩합니다.

    참고: 오류가 있는지 확인하십시오.

    정책 저장소 스키마가 확장됩니다.

Sun Java System Directory Server 를 위한 정책 저장소 스키마 확장

다음 단계를 수행하십시오.

1. 다음 ZIP 파일을 정책 서버 호스트 시스템에 복사하고 임시 위치에 압축을 풉니다.

   `policy_store_schema_ext.zip`

2. 다음 디렉터리로 이동합니다.

   `schema_extension\db\Sun Java System Directory Server`

3. 다음 파일을 찾습니다.

   `OracleDirectoryServer.ldif`

4. 명령 창에서 *siteminder_home*\bin 으로 이동합니다.

   siteminder_home

   정책 서버 설치 경로를 지정합니다.

5. 다음 명령을 실행합니다.

   `smldapsetup ldmod -f`*`path`*`\OracleDirectoryServer.ldif`

   -fpath

   추출된 스키마 파일의 경로를 지정합니다.

   정책 저장소 스키마가 확장됩니다.

Microsoft SQL Server 를 위한 정책 저장소 스키마 확장

다음 단계를 수행하십시오.

1. 다음 ZIP 파일을 SQL Server 호스트 시스템에 복사하고 임시 위치에 압축을 풉니다.

   `policy_store_schema_ext.zip`

2. 다음 디렉터리로 이동합니다.

   `schema_extension\db\Microsoft SQL Server`

3. 다음 파일을 찾습니다.

   `SQLServer.sql`

4. 정책 저장소 데이터베이스를 관리하는 사용자로 SQL Server 에 로그인합니다.

5. 쿼리 분석기를 시작합니다.

6. 데이터베이스 목록에서 정책 저장소 데이터베이스 인스턴스를 선택합니다.
7. 파일을 텍스트 편집기에서 열고 전체 파일의 내용을 복사합니다.
8. 스키마를 쿼리에 붙여 넣고 쿼리를 실행합니다.

   정책 저장소 스키마가 확장됩니다.

MySQL Server 를 위한 정책 저장소 스키마 확장

다음 단계를 수행하십시오.

1. 다음 ZIP 파일을 MySQL 호스트 시스템에 복사하고 임시 위치에 압축을 풉니다.

   `policy_store_schema_ext.zip`
2. 다음 디렉터리로 이동합니다.

   `schema_extension\db\MySQL`
3. 다음 파일을 찾습니다.

   `MySQL.sql`
4. 파일을 텍스트 편집기에서 열고 전체 파일의 내용을 복사합니다.
5. 파일 내용을 쿼리에 붙여 넣습니다.
6. MySQL 명령줄 도구를 사용하여 쿼리를 실행합니다.

   정책 저장소 스키마가 확장됩니다.

Oracle Server 를 위한 정책 저장소 스키마 확장

다음 단계를 수행하십시오.

1. 다음 ZIP 파일을 Oracle 호스트 시스템에 복사하고 임시 위치에 압축을 풉니다.

   `policy_store_schema_ext.zip`
2. 다음 디렉터리로 이동합니다.

   `schema_extension\db\Oracle`
3. 다음 파일을 찾습니다.

   `Oracle.sql`
4. sqlplus 또는 다른 Oracle 유틸리티를 사용하여 정책 저장소 데이터베이스를 관리하는 사용자로 Oracle 서버에 로그인합니다.

참고: SYS 또는 SYSTEM 사용자로 SiteMinder 스키마를 생성하지 않는 것이 좋습니다. 필요한 경우 SMOWNER 와 같은 Oracle 사용자를 생성하고 그 사용자로 스키마를 생성하십시오.

5. 파일을 r6.x 데이터베이스 인스턴스로 가져옵니다.

   참고: sqlplus 를 사용하는 경우에는 @ 기호를 사용하여 스키마를 실행합니다.

   정책 저장소 스키마가 확장됩니다.

키 데이터베이스 인스턴스 동기화

새 버전으로 마이그레이션을 시작하기 전에 모든 smkeydatabase 인스턴스를 동기화하십시오.

참고: smkeydatabase 를 동기화하고 smkeydatabase 인스턴스 간의 모든 데이터 불일치를 해결하려면 smkeytool 유틸리티를 사용하십시오. smkeytool 유틸리티에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

이전 버전의 SiteMinder 에서는 인증서 데이터를 저장하는 데 로컬 smkeydatabase 가 사용되었습니다. 각 정책 서버에는 고유한 smkeydatabase 가 필요했습니다. 12.52 SP1 버전의 경우 중앙 집중화된 인증서 데이터 저장소가 로컬 smkeydatabase 를 대체합니다.

설치 관리자는 정책 서버 업그레이드의 일부로 로컬 smkeydatabase 를 자동으로 백업하고 모든 콘텐츠를 인증서 데이터 저장소로 마이그레이션하려고 시도합니다. 이 과정에는 마이그레이션 시작 전 두 저장소 모두를 비교하는 작업이 포함됩니다.

중요! smkeydatabase 의 마이그레이션이 실패한 경우 정책 서버를 환경으로 되돌리지 마십시오. 마이그레이션 실패 후 정책 서버를 되돌리면 인증서 데이터가 필요한 모든 트랜잭션이 실패합니다.

다음 지침을 따라 smkeydatabase 간의 데이터 일관성을 확인하고 해결하십시오.

- 각 인증 기관 인증서가 인스턴스 간에 일관되게 인증서 해지 목록을 참조하는지 확인하십시오.

  예: 인증 기관 인증서는 LDAP 디렉터리 서비스의 인증서 해지 목록을 일관되게 참조합니다.

- defaultentpriseprivatekey 별칭이 모든 인스턴스에서 동일한 개인 키/인증서 쌍을 나타내는지 확인하십시오.
- 동일한 별칭이 동일한 인증서 또는 키/인증서 쌍에 매핑되는지 확인하십시오.
- 동일한 인증 기관 인증서가 동일한 인증서 해지 목록에 매핑되는지 확인하십시오.
- 해지되거나 만료된 인증서가 없는지 확인하십시오.
- 모든 CRL 정보가 유효한지 확인하십시오.

중요! 모든 데이터 불일치를 해결한 후에는 마이그레이션이 모두 완료될 때까지 smkeydatabase 를 수정하지 않는 것이 좋습니다.

r6.x 정책 서버 업그레이드

다음 단원에서는 Windows 및 UNIX 에서 r6.x 정책 서버를 업그레이드하는 방법에 대해 자세히 설명합니다.

업그레이드하기 전에

정책 서버를 업그레이드하기 전에 다음 사항을 고려하십시오.

- 환경에 smkeydatabase 인스턴스가 여러 개 있는 경우에는 모든 콘텐츠를 동기화해야 합니다. 동기화하면 정책 서버 설치 관리자가 콘텐츠를 인증서 데이터 저장소로 마이그레이션하는 데 방해가 되는 데이터 불일치 문제가 해결됩니다.
- (Linux) 필요한 Linux 라이브러리가 정책 서버 호스트 시스템에 설치되었는지 확인하십시오. 자세한 내용은 "필요한 Linux 라이브러리"를 참조하십시오.

- 업그레이드 중인 정책 서버를 환경에서 제거하십시오. 정책 서버를 제거하면 업그레이드 중에 웹 에이전트가 정책 서버에 연결하는 것을 방지할 수 있습니다.
- 모든 정책 서버 관리 콘솔 인스턴스를 종료하십시오.
- 업그레이드 중에 구성 마법사에서 정책 저장소 확인란을 선택 취소한 상태로 두고 기존 정책 저장소를 유지합니다. 하지만 구성 마법사에서 고급 인증 서버에 대한 암호화 키를 요구하는 메시지가 표시됩니다. 이 키는 각 정책 서버에 저장되지만 모든 정책 서버에 동일한 키가 필요합니다.
- (UNIX) 정책 서버를 업그레이드하는 사용자 계정에는 설치 미디어가 포함된 디렉터리에 대한 실행 권한이 있어야 합니다. 사용자 계정에 이러한 권한이 없는 경우 다음 명령을 실행하십시오.

  `chmod +x installation_media`

  installation_media

  정책 서버 설치 실행 파일을 지정합니다.
- (UNIX) 여러 서브넷에서 정책 서버 설치 관리자를 실행하면 설치 관리자가 충돌할 수 있습니다. 설치 관리자를 정책 서버 호스트 시스템에서 직접 실행하십시오.

필요한 Linux 라이브러리

Linux 운영 환경에서 작동하는 구성 요소의 경우 특정 라이브러리 파일이 필요합니다. 올바른 라이브러리를 설치하지 못하면 다음과 같은 오류가 발생할 수 있습니다.

```
java.lang.UnsatisfiedLinkError
```

이 구성 요소의 Linux 버전을 설치, 구성 또는 업그레이드하는 경우 호스트 시스템에 다음 패키지가 필요합니다.

Red Hat 5.x:

- compat–gcc-34-c++-3.4.6-*patch_version*.I386
- libstdc++-4.x.x-x.el5.i686.rpm
- libidn.so.11.rpm
- ncurses

Red Hat 6.x:

- libstdc++-4.x.x-x.el6.i686.rpm
- libidn-1.18-2.el6.i686
- libXext.i686.rpm
- libXrender.i686.rpm
- linXtst.i686.rpm
- libidn.so.11.rpm
- ncurses

또한 Red Hat 6.x(64 비트)의 경우:

64 비트 Red Hat 6.x 에 필요한 모든 RPM 패키지는 *32 비트* 패키지입니다.

- libXau-1.0.5-1.el6.i686.rpm
- libxcb-1.5-1.el6.i686.rpm
- compat-db42-4.2.52-15.el6.i686.rpm
- compat-db43-4.3.29-15.el6.i686.rpm
- libX11-1.3-2.el6.i686.rpm
- libXrender-0.9.5-1.el6.i686.rpm
- libexpat.so.1(expat-2.0.1-11.el6_2.i686.rpm 에서 제공)
- libfreetype.so.6(freetype-2.3.11-6.el6_2.9.i686.rpm 에서 제공)
- libfontconfig.so.1(fontconfig-2.8.0-3.el6.i686.rpm 에서 제공)
- libICE-1.0.6-1.el6.i686.rpm
- libuuid-2.17.2-12.7.el6.i686.rpm
- libSM-1.1.0-7.1.el6.i686.rpm
- libXext-1.1-3.el6.i686.rpm
- compat-libstdc++-33-3.2.3-69.el6.i686.rpm
- compat-db-4.6.21-15.el6.i686.rpm
- libXi-1.3-3.el6.i686.rpm
- libXtst-1.0.99.2-3.el6.i686.rpm
- libXft-2.1.13-4.1.el6.i686.rpm
- libXt-1.0.7-1.el6.i686.rpm
- libXp-1.0.0-15.1.el6.i686.rpm

- libstdc++.i686.rpm
- compat-libtermcap.rpm
- libidn.i686.rpm
- ncurses

Linux 에서 Korn 셸(ksh) 패키지가 필요함

Linux 플랫폼에서 정책 서버를 설치 및 업그레이드하는 중에 ksh Korn 셸이 필요합니다. 사용하는 Linux 환경에 대한 적절한 버전이 설치되어 있는지 확인하십시오.

Red Hat 5.x 32 비트

ksh-20100621-12.el5.i386.rpm

Red Hat 5.x 64 비트

ksh-20100621-12.el5.x86_64.rpm

Red Hat 6.x 32 비트

ksh-20100621-16.el6.i686.rpm

Red Hat 6.x 64 비트

ksh-20100621-16.el6.x86_64.rpm

Windows

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. 업그레이드할 정책 서버를 중지합니다.
3. *installation_media* 를 두 번 클릭합니다.

   installation_media

   정책 서버 설치 실행 파일을 지정합니다.
4. 설치 관리자를 실행할 때는 다음 사항을 고려하십시오.
   - SiteMinder 구성 요소를 선택하라는 메시지가 표시됩니다. 구성 요소를 선택하는 경우:
     - 환경에 대해 이전에 구성된 모든 구성 요소를 재구성하십시오. 각 구성 요소를 선택하십시오.

- 업그레이드 중에 구성 마법사에서 정책 저장소 확인란을 선택 취소한 상태로 두고 기존 정책 저장소를 유지합니다. 기존 정책 저장소를 수동으로 업그레이드하십시오. 하지만 구성 마법사에서 고급 인증 서버에 대한 암호화 키를 요구하는 메시지가 표시됩니다. 이 키는 각 정책 서버에 저장되지만 모든 정책 서버에 동일한 키가 필요합니다.
- 다른(n 번째) 정책 서버를 업그레이드하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

- 설치 관리자는 smkeydatabase 를 발견하면 다음을 수행합니다.
  - smkeydatabase 를 백업합니다.
  - 콘텐츠를 인증서 데이터 저장소로 마이그레이션하려고 시도합니다.

  중요! smkeydatabase 의 마이그레이션이 실패한 경우 정책 서버를 환경으로 되돌리지 마십시오. 마이그레이션 실패 후 정책 서버를 되돌리면 인증서 데이터가 필요한 모든 트랜잭션이 실패합니다.
- 경로 정보를 잘라내서 마법사에 붙여 넣은 경우 문자를 입력하여 "다음" 단추가 사용되도록 설정합니다.

5. 설치 설정을 검토하고 "설치"를 클릭합니다.

   정책 서버가 업그레이드됩니다. 선택한 구성 요소가 정책 서버와 함께 사용할 수 있도록 구성됩니다.
6. 업그레이드하는 정책 서버에 대해 고급 인증 서버를 사용하도록 설정합니다.

UNIX GUI

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. 업그레이드할 정책 서버를 중지합니다.
3. SiteMinder 설치 디렉터리의 ksh 셸에서 다음 스크립트를 실행합니다.

   ```
   . ./ca_ps_env.ksh
   ```

   참고: 마침표 사이에 공백이 있어야 합니다.
4. 셸을 열고 설치 실행 파일이 있는 위치로 이동합니다.

5. 다음 명령을 입력합니다.

   ./installation_media

   installation_media

   정책 서버 설치 실행 파일을 지정합니다.

6. 설치 관리자를 실행할 때는 다음 사항을 고려하십시오.

   - SiteMinder 구성 요소를 선택하라는 메시지가 표시됩니다. 구성 요소를 선택하는 경우:
     - 환경에 대해 이전에 구성된 구성 요소를 재구성하십시오. 각 구성 요소를 선택하십시오.
     - 업그레이드 중에 구성 마법사에서 정책 저장소 확인란을 선택 취소한 상태로 두고 기존 정책 저장소를 유지합니다. 기존 정책 저장소를 수동으로 업그레이드하십시오. 하지만 구성 마법사에서 고급 인증 서버에 대한 암호화 키를 요구하는 메시지가 표시됩니다. 이 키는 각 정책 서버에 저장되지만 모든 정책 서버에 동일한 키가 필요합니다.
     - 다른(n 번째) 정책 서버를 업그레이드하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.
   - 설치 관리자는 smkeydatabase 를 발견하면 다음을 수행합니다.
     - smkeydatabase 를 백업합니다.
     - 콘텐츠를 인증서 데이터 저장소로 마이그레이션하려고 시도합니다.

     중요! smkeydatabase 의 마이그레이션이 실패한 경우 정책 서버를 환경으로 되돌리지 마십시오. 마이그레이션 실패 후 정책 서버를 되돌리면 인증서 데이터가 필요한 모든 트랜잭션이 실패합니다.
   - 경로 정보를 잘라내서 마법사에 붙여 넣은 경우 문자를 입력하여 "다음" 단추가 사용되도록 설정합니다.

7. 설치 설정을 검토하고 "설치"를 클릭합니다.

   정책 서버가 업그레이드됩니다. 선택한 구성 요소가 정책 서버와 함께 사용할 수 있도록 구성됩니다.

   참고: 업그레이드는 몇 분 정도 걸릴 수 있습니다.

8. "Done"(완료)을 클릭합니다.
9. SiteMinder 설치 디렉터리의 ksh 셸에서 다음 스크립트를 실행합니다.

   ```
   . ./ca_ps_env.ksh
   ```

   참고: 마침표 사이에 공백이 있어야 합니다.
10. 업그레이드하는 정책 서버에 대해 고급 인증 서버를 사용하도록 설정합니다.

UNIX 콘솔

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. 업그레이드할 정책 서버를 중지합니다.
3. SiteMinder 설치 디렉터리의 ksh 셸에서 다음 스크립트를 실행합니다.

   ```
   ../ca_ps_env.ksh
   ```

   참고: 마침표 사이에 공백이 있어야 합니다.
4. 셸을 열고 설치 실행 파일이 있는 위치로 이동합니다.
5. 다음 명령을 입력합니다.

   ```
   ./installation_media -i console
   ```

   installation_media

   정책 서버 설치 실행 파일을 지정합니다.
6. 설치 관리자를 실행할 때는 다음 사항을 고려하십시오.
   - SiteMinder 구성 요소를 선택하라는 메시지가 표시됩니다. 각 구성 요소 앞에 숫자가 붙어 있습니다. 하나 이상의 구성 요소를 선택하려면 쉼표(,)로 분리된 숫자를 입력하십시오. 기능을 선택하지 않으려면 쉼표만 입력하십시오. 구성 요소를 선택하는 경우:
     - 환경에 대해 이전에 구성된 구성 요소를 재구성하십시오. 각 구성 요소를 선택하십시오.

- 업그레이드 중에 구성 마법사에서 정책 저장소 확인란을 선택 취소한 상태로 두고 기존 정책 저장소를 유지합니다. 기존 정책 저장소를 수동으로 업그레이드하십시오. 하지만 구성 마법사에서 고급 인증 서버에 대한 암호화 키를 요구하는 메시지가 표시됩니다. 이 키는 각 정책 서버에 저장되지만 모든 정책 서버에 동일한 키가 필요합니다.
- 다른(n 번째) 정책 서버를 업그레이드하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

- 설치 관리자는 smkeydatabase 를 발견하면 다음을 수행합니다.
  - smkeydatabase 를 백업합니다.
  - 콘텐츠를 인증서 데이터 저장소로 마이그레이션하려고 시도합니다.

  중요! smkeydatabase 의 마이그레이션이 실패한 경우 정책 서버를 환경으로 되돌리지 마십시오. 마이그레이션 실패 후 정책 서버를 되돌리면 인증서 데이터가 필요한 모든 트랜잭션이 실패합니다.

7. 설치 설정을 검토하고 Enter 키를 누릅니다.

   정책 서버가 업그레이드됩니다. 선택한 구성 요소가 정책 서버와 함께 사용할 수 있도록 구성됩니다.

   참고: 업그레이드는 몇 분 정도 걸릴 수 있습니다.

8. Enter 키를 누릅니다.
9. "Done"(완료)을 클릭합니다.
10. SiteMinder 설치 디렉터리의 ksh 셸에서 다음 스크립트를 실행합니다.

    ```
    ../ca_ps_env.ksh
    ```

    참고: 마침표 사이에 공백이 있어야 합니다.

11. 업그레이드하는 정책 서버에 대해 고급 인증 서버를 사용하도록 설정합니다.

고급 인증 서버를 사용하도록 설정

정책 서버를 구성하는 과정에서 고급 인증 서버를 사용하도록 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 구성 마법사를 시작합니다.
2. 마법사의 첫 번째 화면에서 모든 확인란을 *선택 취소한* 상태로 둡니다.
3. "다음"을 클릭합니다.
4. 고급 인증 서버에 대한 마스터 암호화 키를 생성합니다.

   참고: 다른(n 번째) 정책 서버를 설치하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.
5. 정책 서버 구성 마법사의 나머지 과정을 완료합니다.

   고급 인증 서버가 사용되도록 설정되었습니다.

사용자 지정된 파일 수정

정책 서버 업그레이드 중 설치 관리자는 특정 파일의 새 버전을 만듭니다. 설치 관리자는 *policy_server_home*/config 디렉터리에 다음과 같은 파일을 만듭니다.

- conapi.conf
- JVMOptions.txt
- profiler_templates
- siteminder.conf
- SMocsp.sample.conf
- SmSWEC.cfg
- smtracedefault.txt
- snmp.conf
- snmptrap.conf
- trace.conf

설치 관리자는 *policy_server_home*/properties 디렉터리에 다음과 같은 파일을 만듭니다.

- AMAssertionGenerator.properties
- AssertionGeneratorFramework.properties
- cdslog4j.properties
- EntitlementGenerator.properties
- FederationAttributeConfig.properties
- InfoCard.properties
- JSAMLAssertionStrings.properties
- JSAMLProtocolStrings.properties
- log4j.properties
- LoggerConfig.properties
- logging.properties
- openformatexpression.conf
- scriptActiveExpConfig.properties
- smkeydatabase.properties
- WebServiceConfig.properties
- xsw.properties

이러한 12.52 SP1 파일은 .new 확장명을 사용합니다. 예를 들어, 이전 버전의 JVMOptions.txt 파일은 그대로 유지됩니다. 설치 관리자는 이름이 JVMOPtions.new 인 JVMOptions.txt 파일의 12.52 SP1 버전을 만듭니다.

원래 파일이 사용자 지정된 설정을 포함한 경우 사용자 지정된 설정으로 .new 파일을 수정하십시오. 원래 파일의 확장명을 사용하여 .new 파일의 이름을 변경하십시오.

예를 들어, JVMOptions.txt 파일에 사용자 지정된 설정이 있는 경우 이러한 변경 내용을 JVMOptions.txt.new 에 복사하십시오. JVMOptions.txt.new 를 JVMOptions.txt 로 이름을 변경하십시오.

사용자 지정 서버 측 코드 요구 사항

정책 서버 운영 체제는 사용자 지정 서버 측 코드를 다시 컴파일해야 하는지 여부를 확인합니다. 다음 표를 사용하여 요구 사항을 확인하십시오.

운영 체제	필수
Microsoft Windows 및 UNIX	아니요. 필요한 경우에만 사용자 지정 코드를 다시 컴파일합니다.
Red Hat Linux	예. SDK 를 업그레이드하고 GCC 3.4 를 사용하여 사용자 지정 코드를 다시 컴파일합니다.

정책 서버 업그레이드 문제 해결

업그레이드 중 문제가 발생하는 경우:

- *siteminder_home*\siteminder\install_config_info 에서 정책 서버 설치 로그 파일을 찾아 보십시오.

  siteminder_home

  정책 서버 설치 경로를 지정합니다.

- *siteminder_home*\log 에서 smkeydatabase 마이그레이션 로그(smkeydatabaseMigration.log)를 찾아 보십시오.

  참고: 정책 서버 업그레이드와 smkeydatabase 마이그레이션은 별개의 프로세스입니다. 따라서 smkeydatabase 마이그레이션이 실패하더라도 정책 서버 업그레이드는 실패하지 않습니다.

정책 서버 업그레이드 후 작업

관리자가 정책 저장소 개체에 대해 변경한 내용을 포함하도록 정책 서버 감사 로그를 구성한 경우 다음 사항을 고려하십시오.

- 정책 서버 관리 콘솔을 처음 열 때 이 유형의 관리자 감사는 사용되지 않도록 설정하라는 메시지가 표시됩니다.
- 이 유형의 관리자 이벤트가 정책 서버 감사 로그에 포함되는 방식을 변경한 경우 이 메시지가 표시됩니다. 이 유형의 관리자 이벤트를 감사 로그에 포함하려면 정책 서버 관리 콘솔이 아니라 XPSConfig 유틸리티를 사용합니다. 기본적으로 XPSConfig 유틸리티에서는 정책 저장소 개체에 대한 관리자 변경 내용을 로깅하도록 설정됩니다.

이 메시지는 "로그" 탭에 있는 "관리자가 다음으로 변경: 정책 저장소 개체" 설정을 "이벤트 로깅 안 함"으로 변경할 때까지 계속 표시됩니다. 이와 같이 변경한 후 해당 설정은 사용되지 않는 것으로 표시되지만 정책 저장소 개체에 대한 관리자 변경 내용은 계속 로깅됩니다.

정책 서버 감사 로그에서 이 유형의 관리자 이벤트를 제외하려면 XPSConfig 유틸리티를 사용하여 이 기능이 사용되지 않도록 설정합니다.

참고: XPSConfig 유틸리티 사용에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

r6.x 웹 에이전트 업그레이드

마이그레이션 프로세스의 두 번째 단계에서는 웹 에이전트를 업그레이드합니다.

SiteMinder r6.x 웹 에이전트는 12.52 SP1 정책 서버와 통신할 수 있습니다. 따라서 웹 에이전트를 12.52 SP1 로 업그레이드하기 전에 정책 서버를 12.52 SP1 로 업그레이드합니다.

r6.x 웹 에이전트 업그레이드 전 작업

웹 에이전트를 업그레이드하기 전에 다음 사항을 고려하십시오.

- (UNIX) 웹 에이전트를 설치하는 데 사용된 것과 동일한 계정으로 웹 에이전트를 업그레이드해야 합니다. 다른 계정을 사용할 경우 업그레이드에 실패할 수 있습니다.
- WAOP(웹 에이전트 옵션 팩) 구성 파일을 백업하고 WAOP 를 제거하십시오.

  참고: WAOP 제거에 대한 자세한 내용은 *웹 에이전트 옵션 팩 안내서*를 참조하십시오.
- 정책 서버가 구성되어 있는지 확인하십시오.
- 필요한 관리자 및 정책 서버 개체 이름을 확인하십시오.
- 웹 에이전트 요구 사항을 확인하십시오.

정책 서버가 구성되어 있는지 확인

웹 에이전트를 업그레이드하기 전에 다음 사항을 고려하십시오.

- 정책 서버가 웹 에이전트 호스트 시스템에 연결할 수 있는지 확인하십시오.
- 트러스트된 호스트를 등록하기 전에 정책 서버가 실행 중인지 확인하십시오. 정책 서버 관리 콘솔의 "상태" 탭에서 정책 서버를 시작합니다.

필요한 관리자 및 정책 서버 개체 이름 확인

웹 에이전트를 업그레이드하기 전에 정책 서버 관리자의 다음 정보가 필요합니다.

- 호스트를 등록할 수 있는 SiteMinder 관리자의 이름
- 호스트 구성 개체의 이름
- 에이전트 구성 개체의 이름

웹 에이전트 요구 사항 확인

패치 및 기타 웹 에이전트 요구 사항에 대한 자세한 내용은 *웹 에이전트 설치 안내서*를 참조하십시오.

r6.x 웹 에이전트 업그레이드

12.52 SP1 웹 에이전트 설치 관리자를 사용하여 r6.x 웹 에이전트를 업그레이드하십시오. 다음 사항을 고려하십시오.

- 12.52 SP1 웹 에이전트 옵션 팩을 설치하려면 먼저 옵션 팩 기능이 필요한 에이전트를 12.52 SP1 로 업그레이드해야 합니다.

  참고: 웹 에이전트 업그레이드에 대한 자세한 내용은 *웹 에이전트 설치 안내서*를 참조하십시오. 12.52 SP1 웹 에이전트 옵션 팩 설치에 대한 자세한 내용은 *웹 에이전트 옵션 팩 안내서*를 참조하십시오.

- 고급 암호 서비스를 배포한 경우 웹 에이전트 업그레이드에서 모든 LANG(변환) 및 CFG(구성) 파일을 유지합니다. 파일의 기본 12.52 SP1 버전은 *agent_home*\samples 에 설치됩니다.

  agent_home

  웹 에이전트 설치 경로를 지정합니다.

- r6 용 시작 스크립트를 사용한 경우 "nete_wa..."의 모든 인스턴스를 "ca_wa..."로 대체하십시오.

사용자 지정 에이전트 요구 사항

사용자 지정 에이전트를 다시 컴파일해야 하는지 여부를 확인하려면 다음 표를 사용하십시오.

에이전트 유형	필수
SiteMinder 에이전트	운영 체제에 따라 다릅니다. 에이전트 운영 체제가 만료된 경우에는 사용자 지정 에이전트를 다시 컴파일해야 합니다. SiteMinder SDK 를 업그레이드하고 지원되는 운영 체제에서 에이전트를 다시 컴파일합니다.
타사 에이전트	공급업체에 따라 다릅니다. 타사 공급업체에 문의하여 에이전트가 지원되는지 여부를 확인합니다.

r6.x 정책 저장소 업그레이드

마이그레이션 프로세스의 세 번째 단계에서는 정책 및 키 저장소를 업그레이드합니다. 다음 단원에서는 r6.x 정책 및 키 저장소를 12.52 SP1 로 업그레이드하는 방법에 대해 자세히 설명합니다.

정책 저장소 업그레이드에 대한 옵션

r6.x 정책 저장소를 12.52 SP1 버전으로 업그레이드할 수 있는 두 가지 방법이 있으며, 다음을 수행할 수 있습니다.

- 기존 정책 및 키 저장소를 12.52 SP1 버전으로 업그레이드할 수 있습니다.
- 12.52 SP1 정책 및 키 저장소를 생성하고 기존 정책 및 키 저장소 데이터를 새 인스턴스로 가져올 수 있습니다.

이 안내서에는 기존 정책 및 키 저장소를 업그레이드하는 자세한 단계가 나와 있습니다.

기존 정책 저장소를 12.52 SP1 정책 및 키 저장소로 마이그레이션하려면 다음 단계를 완료하십시오.

1. smobjexport 의 r6.x 버전을 사용하여 정책 및 키 저장소 데이터를 내보냅니다.

   참고: 자세한 내용은 r6.x 버전의 *정책 서버 설치 안내서*를 참조하십시오.

2. 12.52 SP1 버전의 정책 및 키 저장소를 생성합니다.

   참고: 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

3. smobjimport 의 12.52 SP1 버전을 사용하여 정책 및 키 저장소 데이터를 12.52 SP1 버전의 정책 및 키 저장소로 가져옵니다.

   참고: 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

키 저장소 업그레이드에 대한 옵션

r6.x 키 저장소를 12.52 SP1 로 업그레이드하는 두 가지 경로가 존재합니다. 다음을 수행할 수 있습니다.

- 기존 정책 및 키 저장소를 12.52 SP1 버전으로 업그레이드할 수 있습니다.
- 독립 실행형 12.52 SP1 키 저장소를 만들고 기존 에이전트 키를 새 인스턴스로 가져올 수 있습니다.

이 안내서에는 기존 정책 및 키 저장소를 업그레이드하는 자세한 단계가 나와 있습니다.

독립 실행형 12.52 SP1 키 저장소를 만들려는 경우:

1. r6.x 버전의 smobjexport 를 사용하여 정책 저장소에 저장되어 있는 에이전트 키만 내보냅니다.

   참고: 자세한 내용은 r6.x *정책 서버 설치 안내서*를 참조하십시오.

2. 기본 정책 저장소 스키마를 사용하여 12.52 SP1 키 저장소를 만듭니다.

   참고: 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

3. 12.52 SP1 버전의 smobjimport 를 사용하여 12.52 SP1 키 저장소로 에이전트 키를 가져옵니다.

   참고: 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

4. 정책 서버 관리 콘솔을 사용하여 정책 서버에 독립 실행형 키 저장소를 연결합니다.

   참고: 자세한 내용은 *정책 서버 관리 콘솔 도움말*을 참조하십시오.

r6.x 정책 저장소를 업그레이드하는 방법

r6.x 정책 저장소를 12.52 SP1 로 업그레이드하려면 다음 절차를 완료하십시오.

1. 정책 저장소와 통신 중인 모든 정책 서버를 중지합니다.
2. 정책 서버 업그레이드 시 smkeydatabase 마이그레이션을 쉽게 하기 위해 정책 저장소 스키마를 확장하지 않은 경우 해당 스키마를 확장합니다.
3. 정책 저장소 데이터 정의를 가져옵니다.
4. 기본 정책 저장소 개체를 가져옵니다.

   참고: 레거시 페더레이션 환경을 업그레이드할 경우에는 PSOP(정책 서버 옵션 팩) 스키마를 변경할 필요가 없습니다.

5. FSS 관리 UI 를 사용하여 r6.x 레거시 페더레이션 환경을 관리했던 경우 XPS 스위퍼 유틸리티를 실행하여 레거시 페더레이션 개체의 마이그레이션을 완료합니다.
6. 정책 저장소와 통신 중인 모든 정책 서버를 시작합니다.

모든 정책 서버 중지

정책 저장소와 통신하는 모든 정책 서버를 중지하면 업그레이드 중 정책 저장소의 손상을 방지할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 단계 중 하나를 완료하십시오.
   - (Windows)
     a. 정책 서버 관리 콘솔을 열고 "중지"를 클릭합니다.
     b. "확인"을 클릭하여 콘솔을 닫습니다.
   - (UNIX) 제공된 다음 스크립트를 사용합니다.
     install_path/siteminder/stop-all

     install_path

     정책 서버 설치 경로를 지정합니다.
3. 정책 저장소와 통신하는 각 정책 서버에 대해 이 절차를 반복합니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home*\xps\dd 로 이동합니다.

   siteminder_home

   정책 서버 설치 경로를 지정합니다.
2. 다음 명령을 실행합니다.

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

기본 정책 저장소 개체는 다음 XML 파일에 존재합니다.

- smpolicy.xml
- smpolicy-secure.xml

smpolicy-secure.xml 파일은 smpolicy.xml 파일보다 제한적인 보안 설정을 제공합니다. 이 두 파일 중 *하나*만 선택하여 기본 정책 저장소 개체를 가져옵니다.

두 파일 중 어느 것을 사용해도 새 정책 저장소가 구성되고 기존 저장소가 업그레이드됩니다. 업그레이드 과정에서 개체를 가져오는 경우 해당 파일은 이미 수정된 기존의 기본 개체를 *덮어쓰지 않습니다*. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다.

두 파일 중 하나를 가져오면 레거시 페더레이션 및 웹 서비스 변수 기능을 사용할 수 있게 됩니다. 이러한 기능에는 별도의 라이선스가 필요합니다. 웹 서비스 변수 기능을 사용하려면 CA 고객 담당자에게 라이선스 정보에 대해 문의하십시오.

다음 단계를 수행하십시오.

1. 명령줄 창을 열고 *siteminder_home*\db 로 이동합니다.
2. 다음 파일 중 *하나*를 가져옵니다.
   - smpolicy.xml 을 가져오려면 다음 명령을 실행합니다.

     ```
     XPSImport smpolicy.xml -npass
     ```

   - smpolicy-secure.xml 을 가져오려면 다음 명령을 실행합니다.

     ```
     XPSImport smpolicy-secure.xml -npass
     ```

   -npass

   암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다. 기본 정책 저장소 개체를 가져오는 데에는 암호가 필요하지 않습니다.

   정책 저장소 개체를 가져왔습니다.

관리 UI 에서 레거시 페더레이션 개체를 사용할 수 있도록 설정하기

정책 서버 UI 를 사용하여 Federation Security Services(레거시 페더레이션) 개체를 관리하는 경우, XPS 스위퍼 유틸리티를 실행하여 해당 개체를 관리 UI 로 마이그레이션하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 레거시 페더레이션 개체를 관리 UI 에서 사용할 수 있도록 설정합니다.

   ```
   XPSSweeper
   ```

   이제 정책 서버 UI 를 사용하여 생성한 모든 레거시 페더레이션을 관리 UI 에서 사용할 수 있습니다.

   업그레이드 프로세스의 다음 단계인 관리 UI 업그레이드 단계를 계속할 준비가 되었습니다.

모든 정책 서버 시작

모든 정책 서버를 시작하면 정책 서버와 업그레이드된 정책 저장소 간의 통신이 다시 시작됩니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 단계 중 하나를 완료하십시오.
   - (Windows)
     a. 정책 서버 관리 콘솔을 열고 "시작"을 클릭합니다.
     b. "확인"을 클릭하여 콘솔을 닫습니다.
   - (UNIX) 제공된 다음 스크립트를 사용합니다.
     install_path/siteminder/start-all

     install_path

     정책 서버 설치 경로를 지정합니다.
3. 정책 저장소와 통신하는 각 정책 서버에 대해 이 절차를 반복합니다.

정책 저장소가 업그레이드됩니다.

r6.x 마이그레이션을 위한 관리 사용자 인터페이스 설치

이전 버전의 SiteMinder 와 달리 정책 서버 사용자 인터페이스는 정책 서버와 함께 설치되지 않습니다. 12.52 SP1 관리 UI 는 개별적으로 설치해야 합니다.

참고: 관리 UI 설치에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

r6.x 세션 저장소 업그레이드

세션 저장소 업그레이드는 필요하지 않습니다. 12.52 SP1 세션 저장소 스키마는 r6.0 SP5 에서 변경되지 않았습니다.

r6.x 감사 로그 데이터베이스 업그레이드

Security Command Center(SCC)에서는 iRecorder for SiteMinder 를 사용하여 SiteMinder SQL Server 또는 Oracle 로그 데이터베이스의 보안 관련 로깅 데이터를 읽을 수 있습니다.

참고: iRecorder for SiteMinder 에 대한 자세한 내용은 *eTrust Audit iRecorder Reference Guide*(eTrust Audit iRecorder 참조 안내서)를 참조하십시오. 감사 로그 스키마 가져오기에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

통합하려면 *policy_server_home*\db\SQL 에 있는 sm_mssql_logs_eaudit_upgrade.sql 스크립트나 sm_oracle_logs_eaudit_upgrade.sql 스크립트를 가져와 감사 로그 데이터베이스의 스키마를 업그레이드해야 합니다. SiteMinder 를 SCC 와 통합하는 경우에만 이 스크립트를 가져옵니다.

policy_server_home

정책 서버 설치 경로를 지정합니다.

참고: DB2 로깅 데이터베이스의 경우에는 SiteMinder/SCC 통합이 작동하지 않습니다.

감사 로그 데이터베이스를 업그레이드하려면 다음 스키마 스크립트 중 하나를 기존 SiteMinder 감사 로그 데이터베이스로 가져옵니다.

sm_mssql_logs_eaudit_upgrade.sql

r6.x 의 SQL Server 감사 로그 데이터베이스를 12.52 SP1 로 업그레이드합니다.

sm_oracle_logs_eaudit_upgrade.sql

r6.x 의 Oracle 감사 로그 데이터베이스를 12.52 SP1 로 업그레이드합니다.

참고: SiteMinder Platform Support Matrix(SiteMinder 플랫폼 지원표)에 나열된 SiteMinder 저장소를 구성하거나 업그레이드하려고 하지만 본 안내서에서 절차를 찾을 수 없을 경우 *Directory Configuration Guide*(디렉터리 구성 안내서)를 참조하십시오.

r6.x 병렬 업그레이드 작동 방법

기존 r6.x 환경을 12.52 SP1 환경으로 마이그레이션할 필요는 없습니다. 대신 기존 배포에서 병렬 12.52 SP1 환경을 구성할 수 있습니다.

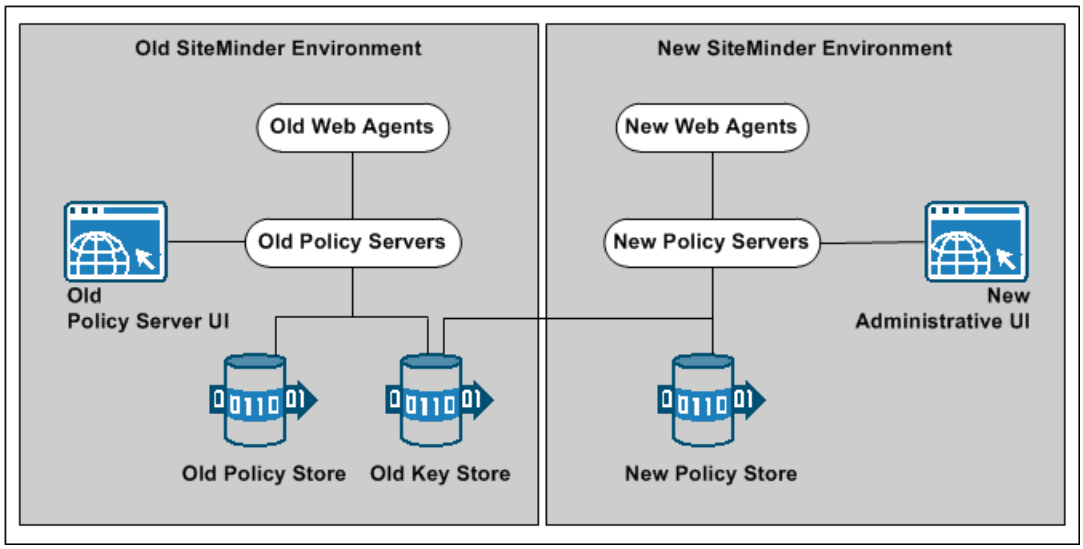
다음 그림에서는 간단한 병렬 업그레이드와 상세 정보를 보여 줍니다.

- r6.x 환경 - 기존 리소스를 계속해서 보호합니다.
- r6.x 정책 서버 사용자 인터페이스 - r6.x 정책 저장소에서 SiteMinder 개체를 관리하는 데 사용됩니다.
- 12.52 SP1 환경 - 새 리소스를 보호합니다.

- 12.52 SP1 관리 UI - 12.52 SP1 정책 저장소에서 SiteMinder 개체를 관리하는 데 사용됩니다.
- 공용 r6.x 키 저장소 - 공용 키 저장소를 사용하여 두 환경 간에서 싱글 사인온을 사용할 수 있습니다.

  참고: 설명에 나와 있지 않지만 다중 키 저장소를 사용하여 두 환경 간에서 싱글 사인온을 사용할 수 있습니다.

그림 7: r6.x 병렬 업그레이드 개요



r6.x 병렬 환경을 구성하는 방법

병렬 환경을 구성하는 절차는 다음과 같습니다.

1. 병렬 환경 키 관리 옵션을 검토하여 싱글 사인온을 구축하는 방법을 결정합니다.
2. 12.52 SP1 환경을 생성합니다.
3. 다음 단계 중 하나를 완료하십시오.
   - 두 환경 모두가 공통 키 저장소 싱글 사인온 요구 사항을 충족하는지 확인합니다.
   - 두 환경 모두가 다중 키 저장소 싱글 사인온 요구 사항을 충족하는지 확인합니다.

4. r6.x 환경에 smkeydatabase 가 포함된 경우:
   a. 모든 인스턴스를 동기화합니다.
   b. smkeydatabase 의 콘텐츠를 12.52 SP1 인증서 데이터 저장소로 마이그레이션합니다.
5. r6.x 환경에서 레거시 페더레이션(Federation Security Services) 개체를 관리하는 경우 어설션 발급자 ID 를 마이그레이션합니다.
6. (선택 사항) r6.x 정책 저장소 데이터를 마이그레이션합니다.
7. 사용자 디렉터리 싱글 사인온 요구 사항을 검토합니다.

병렬 환경 키 관리 옵션

병렬 업그레이드에 성공하려면 SiteMinder 키를 관리하여 기존 환경과 12.52 SP1 환경 간의 싱글 사인온을 유지해야 합니다. 두 가지 SiteMinder 키 관리 옵션을 사용할 수 있습니다. 배포 옵션은 두 환경 모두에서 키 저장소를 하나 이상 구현하는 방법에 따라 달라집니다. 옵션에는 다음이 포함됩니다.

- 공용 키 저장소를 사용하는 여러 정책 저장소
- 개별 키 저장소를 사용하는 여러 정책 저장소

공용 키 저장소 배포

모든 정책 서버가 키 롤오버에 대해 단일 키 저장소를 사용할 수 있습니다. 다음 그림을 참조하십시오.

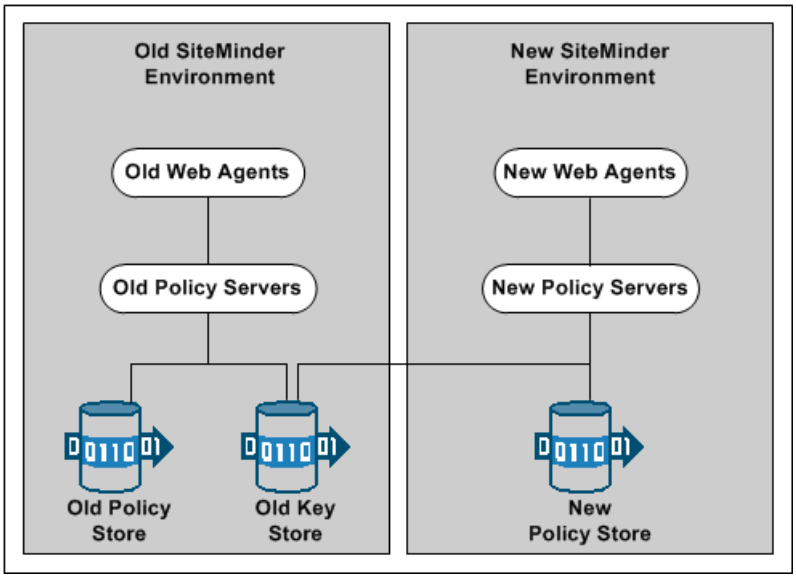
- r6.x 정책 서버는 r6.x 정책 저장소에 연결합니다.
- 12.52 SP1 정책 서버는 12.52 SP1 정책 저장소에 연결합니다.
- 공용 r6.x 키 저장소는 모든 정책 서버에 대한 키 데이터를 유지 관리합니다. 공용 키 저장소를 사용하면 모든 정책 서버에 연결된 에이전트가 키를 공유할 수 있습니다. 키를 공유하면 두 환경 간에서 싱글 사인온을 사용할 수 있습니다.

  중요! r6.x 정책 저장소와 별도로 r6.x 키 저장소를 구성해야 합니다.
- 모든 정책 서버는 공용 키 저장소에 연결하여 새 키를 검색합니다.

  중요! 12.52 SP1 정책 서버에 r6.x 키 저장소가 구성되어 있어야 합니다. r6.x 정책 서버는 12.52 SP1 키 저장소와 통신할 수 없습니다.
- 모든 웹 에이전트는 해당하는 정책 서버를 폴링하여 새 키를 검색합니다.

참고: 설명에 나와 있지 않지만 장애 조치를 위해 정책 저장소 및 키 저장소 데이터를 복제할 수 있습니다. 데이터베이스 또는 디렉터리 서버 유형에 따라 데이터를 복제하는 방법이 결정됩니다. 마스터/슬레이브 환경의 키 관리에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오. 데이터 복제에 대한 자세한 내용은 공급업체별 설명서를 참조하십시오.

그림 8: r6.x 공용 키 저장소 배포



다중 키 저장소 배포

기존 r6.x 정책 서버는 키 롤오버를 위해 r6.x 키 저장소를 사용하고, 12.52 SP1 정책 서버는 키 롤오버를 위해 12.52 SP1 키 저장소를 사용할 수 있습니다. 다음 그림을 참조하십시오.

- r6.x 정책 서버는 r6.x 정책 저장소에 연결합니다.

12.52 SP1 정책 서버는 12.52 SP1 정책 저장소에 연결합니다.

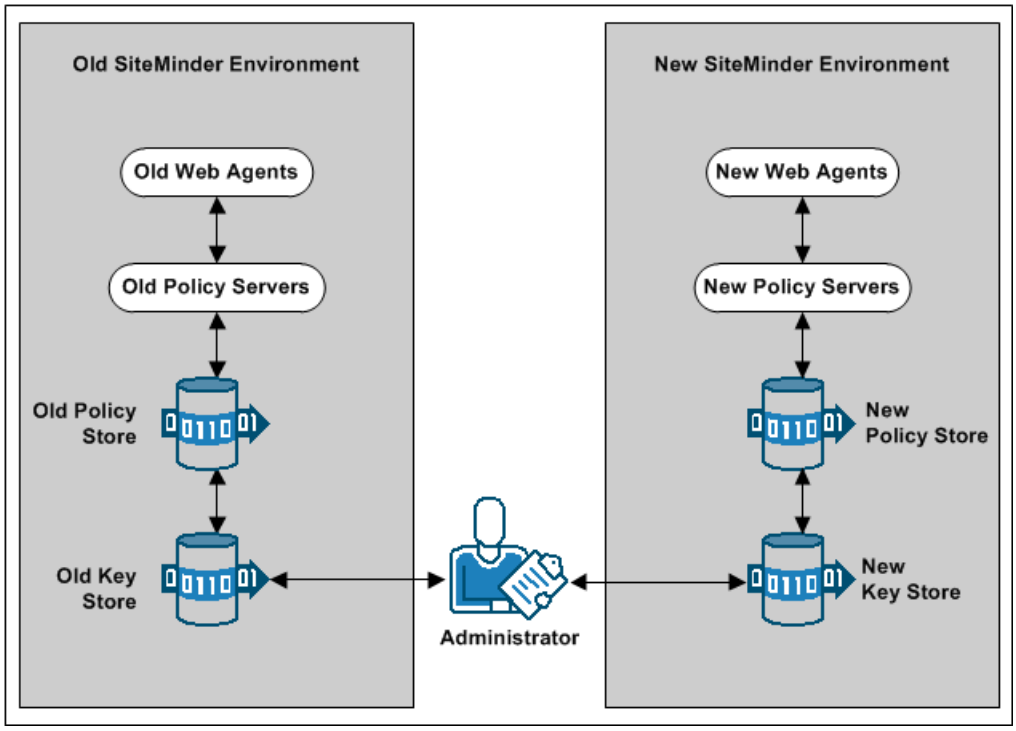
- r6.x 정책 서버는 r6.x 키 저장소에 연결하여 새 키를 검색합니다.
- 12.52 SP1 정책 서버는 12.52 SP1 키 저장소에 연결하여 새 키를 검색합니다.
- SiteMinder 관리자는 관리 UI 를 사용하여 각 키 저장소에 대한 정적 에이전트 및 세션 키를 구성합니다.

  중요! 모든 키 저장소가 동일한 에이전트 및 세션 키를 사용하지 않으면 싱글 사인온에 실패합니다.

- r6.x 웹 에이전트는 해당하는 r6.x 정책 서버를 폴링하여 새 키를 검색합니다.
- 12.52 SP1 웹 에이전트는 해당하는 12.52 SP1 정책 서버를 폴링하여 새 키를 검색합니다.

참고: 설명에 나와 있지 않지만 장애 조치를 위해 정책 저장소 및 키 저장소 데이터를 복제할 수 있습니다. 데이터베이스 또는 디렉터리 서버 유형에 따라 데이터를 복제하는 방법이 결정됩니다. 마스터/슬레이브 환경의 키 관리에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오. 데이터 복제에 대한 자세한 내용은 공급업체별 설명서를 참조하십시오.

그림 9: r6.x 다중 키 저장소 배포



12.52 SP1 환경 만들기

기존 환경과는 독립적으로 12.52 SP1 환경을 구성할 수 있습니다. 다음 순서로 12.52 SP1 구성 요소를 설치하고 구성하십시오.

1. 정책 서버 하나 이상

   중요! 공통 키 저장소로 싱글 사인온을 유지하는 경우 모든 정책 서버에서 동일한 암호화 키를 사용해야 합니다. 암호화 키 값을 알 수 없는 경우에는 정책 저장소의 r6.x 값을 재설정할 수 있습니다. 12.52 SP1 정책 서버를 설치할 때 새 값을 사용하십시오.

   참고: 정책 저장소 암호화 키의 재설정에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

2. 정책 저장소 하나
3. 관리 UI 하나
4. 웹 에이전트 하나 이상
5. 보고서 서버 하나

참고: 정책 서버, 정책 저장소, 관리 UI 및 보고서 서버 설치에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오. 웹 에이전트 설치에 대한 자세한 내용은 *웹 에이전트 설치 안내서*를 참조하십시오.

공용 키 저장소의 싱글 사인온 요구 사항

공용 키 저장소를 배포하는 경우 다음을 수행하지 않으면 싱글 사인온에 실패합니다.

- r6.x 정책 저장소와 키 저장소가 별도로 구성되어 있는지 확인합니다.
  - r6.x 환경에 별도의 키 저장소가 구성되어 있으면 키 저장소 버전을 r6.x 로 유지합니다. 12.52 SP1 정책 서버는 r6.x 키 저장소와 통신할 수 있지만 r6.x 정책 서버는 12.52 SP1 키 저장소와 통신할 수 없습니다.
  - r6.x 환경에 배치된 정책/키 저장소가 구성되어 있는 경우 r6.x 키를 별도의 r6.x 키 저장소로 분리합니다.
- 모든 정책 서버가 공용 r6.x 키 저장소를 사용하도록 구성합니다.
- 모든 정책 서버가 동일한 암호화 키를 사용하는지 확인합니다. 암호화 키 값을 알 수 없는 경우에는 정책 저장소의 r6.x 값을 재설정할 수 있습니다. 12.52 SP1 정책 서버를 설치할 때 이 새 값을 사용합니다.

참고: 정책 저장소 암호화 키의 재설정에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

- 동적 에이전트 키를 생성하는 단일 정책 서버를 지정합니다. 나머지 정책 서버에 대한 에이전트 키 생성이 사용되지 않도록 설정합니다.

  참고: 에이전트 키 동적 생성에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

정책 저장소에서 키 저장소를 분리하는 방법

정책 저장소에서 키 저장소를 분리하려면 다음 단계를 수행하십시오.

1. 설정 정책 서버를 설치하거나 찾습니다. 설정 정책 서버는 배치된 정책/키 저장소가 구성되지 않은 정책 서버입니다.
   - 정책 서버에 배치된 저장소가 구성되어 있다면 해당 정책 서버를 새 키 저장소 인스턴스를 구성하는 데 사용할 수 없습니다. 이 경우 정책 서버 호스트 시스템에서 제공되는 필수 SiteMinder 유틸리티가 배치된 저장소를 관리할 수 있도록 구성됩니다.
   - 설정 정책 서버에서는 별도의 필수 유틸리티 집합을 사용할 수 있습니다. 별도의 집합을 사용하면 배치된 저장소에 영향을 주지 않고 키 저장소를 구성할 수 있습니다.
2. 설정 정책 서버 호스트 시스템을 사용하여 별도의 r6.x 키 저장소 인스턴스를 만듭니다. 다음 사항을 고려하십시오.
   - 키 저장소에는 기본 정책 저장소 스키마만 필요합니다. 기본 정책 저장소 스키마 가져오기에 대한 자세한 내용은 r6.x *정책 서버 설치 안내서*를 참조하십시오.
   - 키 저장소의 경우 다음을 수행할 필요가 없습니다.
     - SiteMinder 슈퍼 사용자 암호를 설정합니다.
     - 기본 정책 저장소 개체를 가져옵니다.
3. r6.x 환경에서 동적 에이전트 키 생성이 사용되지 않도록 설정합니다.

   참고: 환경에서 정적 키를 사용하는 경우 이 단계가 필요하지 않습니다. 그러나 정책 저장소에서 키를 내보낸 후에는 SiteMinder 관리자가 임의 에이전트 키를 생성하지 않도록 확인해야 합니다.
4. r6.x 정책/키 저장소에서 에이전트 키를 내보냅니다.
5. r6.x 키 저장소로 에이전트 키를 가져옵니다.

6. 모든 정책 서버가 별도의 키 저장소를 사용하도록 구성합니다.
7. 동적 에이전트 키 생성이 사용되지 않도록 설정한 경우 다시 사용하도록 설정합니다.

동적 에이전트 키 생성 사용 안 함

키 저장소 분리를 완료하기 전에는 r6.x 환경이 두 개의 키 저장소를 사용하여 작동합니다.

- 일부 정책 서버는 배치된 정책/키 저장소에 있는 에이전트 키를 사용합니다.
- 일부 정책 서버는 별도의 키 저장소에 있는 에이전트 키를 사용합니다.

별도의 저장소로 키를 내보낸 후 동적 에이전트 키 생성이 사용되지 않도록 설정하면 정책 서버가 키를 생성하는 것을 방지할 수 있습니다. 정책 서버가 키를 생성하지 못하도록 설정하면 모든 저장소에서 키가 동기화되지 않을 때 발생할 수 있는 싱글 사인온 문제를 막을 수 있습니다.

다음 단계를 수행하십시오.

1. r6.x 정책 서버 사용자 인터페이스에 로그인합니다.
2. "도구", "키 관리"를 선택합니다.
3. "정적 에이전트 키 사용" 옵션을 선택합니다.
4. "적용"을 클릭합니다.

   정책 서버가 정적 키를 사용하도록 구성됩니다. 정책 서버가 키를 자동으로 생성하지 않습니다.

에이전트 키 내보내기

배치된 정책/키 저장소에서 키를 내보내 별도의 키 저장소에서 키가 사용되도록 설정할 수 있습니다.

다음 단계를 수행하십시오.

1. r6.x 정책 서버 호스트 시스템에 로그인합니다. 이 정책 서버에 배치된 정책/키 저장소가 구성되어 있는지 확인합니다.
2. 다음 명령을 실행하여 정책 저장소에서 키만 내보냅니다.

   ```
   smobjectexport -ffile_name -x
   ```

   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.

   참고: 이 명령의 모드와 인수에 대한 자세한 내용은 r6.x *정책 서버 설치 안내서*를 참조하십시오.

   예:

   ```
   smobjexport -fagentkeys -x
   ```

   배치된 정책/키 저장소에서 에이전트 키를 내보냈습니다.
3. 에이전트 키가 들어 있는 파일을 설정 정책 서버 호스트 시스템에 복사합니다.

에이전트 키 가져오기

배치된 정책/키 저장소에서 키를 가져와 별도의 키 저장소에서 키가 사용되도록 설정할 수 있습니다.

다음 단계를 수행하십시오.

1. r6.x 설정 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 에이전트 키를 별도의 키 저장소로 가져옵니다.

   ```
   smobjimport -ffile_name -k
   ```

   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.

참고: 이 명령의 모드와 인수에 대한 자세한 내용은 r6.x *정책 서버 설치 안내서*를 참조하십시오.

예:

```
smobjimport -fagentkeys -k
```

에이전트 키를 별도의 키 저장소로 가져옵니다.

모든 정책 서버가 키 저장소를 사용하도록 구성

병렬 환경의 모든 정책 서버가 공용 r6.x 키 저장소를 사용하도록 구성하여 두 환경 간에서 싱글 사인온을 유지합니다.

다음 단계를 수행하십시오.

1. 에이전트 키를 동적으로 생성하도록 지정된 정책 서버를 파악합니다. 가장 마지막에 이 정책 서버에서 키 저장소를 구성합니다.
2. 환경의 다른 모든 정책 서버에 대해 다음 단계를 수행하십시오.
   a. 정책 서버 호스트 시스템에 로그인합니다.
   b. 정책 서버 관리 콘솔을 엽니다.
   c. "데이터" 탭을 클릭합니다.
   d. 데이터베이스 목록에서 키 저장소를 선택하고 "정책 저장소 데이터베이스 사용" 옵션을 해제합니다.
   e. 저장소 목록에서 키 저장소 유형을 선택합니다.
   f. 다음 단계 중 하나를 수행합니다.
      a. (LDAP) "LDAP 키 저장소" 섹션에 필수 연결 정보를 입력합니다.
      b. (ODBC) "데이터 원본 정보" 섹션에 데이터 원본 정보를 입력합니다.
   g. 연결을 테스트합니다.
   h. "확인"을 클릭합니다.
   i. 정책 서버를 다시 시작하여 정책 서버가 키 저장소를 사용하도록 구성합니다.
3. 에이전트 키를 생성하도록 지정된 정책 서버가 키 저장소를 사용하도록 구성합니다.

동적 에이전트 키 생성을 사용하도록 다시 설정

동적 에이전트 키 생성이 사용되지 않도록 설정한 경우 에이전트 키를 생성하도록 지정된 정책 서버에서 이 기능을 다시 사용하도록 설정합니다. 환경의 모든 정책 서버가 새 키 저장소를 사용하도록 구성된 후에만 이 절차를 완료하십시오.

다음 단계를 수행하십시오.

1. r6.x 정책 서버 사용자 인터페이스에 로그인합니다.
2. "도구", "키 관리"를 선택합니다.
3. "동적 에이전트 키 사용" 옵션을 선택합니다.
4. "적용"을 클릭합니다.

   지정된 정책 서버가 키를 동적으로 생성하도록 설정됩니다.

정책 저장소에서 키 저장소를 분리하는 데 필요한 태스크를 완료했습니다.

여러 키 저장소의 싱글 사인온 요구 사항

여러 키 저장소를 배포하는 경우 다음을 수행하십시오. 그러지 않으면 싱글 사인온에 실패합니다.

- 모든 정책 서버에 대해 동적 에이전트 키 생성이 사용되지 않도록 설정하십시오.
- r6.x 및 12.52 SP1 키 저장소에 동일한 정적 에이전트 키와 동일한 세션 티켓을 지정하는 데 필요한 정책 서버 사용자 인터페이스 및 관리 UI 권한이 SiteMinder 관리자에게 있는지 확인하십시오.

  참고: 관리자 권한 위임에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.
- **중요!** r6.x 및 12.52 SP1 키 저장소에 동일한 정적 에이전트 키와 동일한 세션 티켓이 구성되어 있는지 확인하십시오.

  참고: 정적 에이전트 키 및 세션 티켓 구성에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

키 및 인증서 마이그레이션

환경에 하나 이상의 smkeydatabase 가 포함된 경우 해당 내용을 12.52 SP1 인증서 데이터 저장소로 마이그레이션합니다.

다음 단계를 수행하십시오.

1. 모든 r6.x smkeydatabase 가 동기화 (페이지 50)되었는지 확인합니다.
2. r6.x 정책 서버 호스트 시스템에 로그인하고 다음 위치로 이동합니다.

   siteminder_home\config\properties

   siteminder_home

   정책 서버 설치 경로를 지정합니다.
3. 다음 파일을 복사합니다.

   smkeydatabase.properties
4. 12.52 SP1 정책 서버 호스트 시스템에 로그인하고 다음 단계를 완료합니다.
   a. 다음 위치로 이동합니다.

      siteminder_home\config\properties

   b. smkeydatabase 속성 파일의 12.52 SP1 버전의 이름을 다음 값으로 변경합니다.

      newsmkeydatabase.properties

   c. 디렉터리에 r6.x 버전의 속성 파일을 추가합니다.

   d. 12.52 SP1 및 r6.x 속성 파일을 텍스트 편집기에서 엽니다.

   e. r6.x 버전의 데이터베이스 위치 경로를 12.52 SP1 버전의 경로와 일치하도록 편집합니다.

      예:

      r6.x 파일이 다음 경로를 참조합니다.

      ```
      DBLocation=C\:/Program
      Files/netegrity/siteminder/smkeydatabase
      ```

      12.52 SP1 파일은 다음 경로를 참조합니다.

      ```
      DBLocation=C:/Program Files/CA/siteminder/smkeydatabase
      ```

      r6.x 파일을 업데이트하여 다음 경로를 참조하도록 합니다.

      ```
      DBLocation=C\:/Program Files/CA/siteminder/smkeydatabase
      ```

f. r6.x 속성 파일을 저장하고 12.52 SP1 속성 파일을 닫습니다.

g. 정책 서버 설치 루트에 다음 디렉터리를 생성합니다.

```
smkeydatabase
```

예:

```
C:\Program Files\CA\SiteMinder\smkeydatabase
```

5. r6.x 정책 서버 호스트 시스템으로 돌아가서 smkeydatabase 디렉터리의 내용을 복사합니다.

   참고: 이 디렉터리의 기본 위치는 *siteminder_home* 입니다.

6. 12.52 SP1 정책 서버 호스트 시스템으로 돌아가서 다음 단계를 완료합니다.

   a. r6.x smkeydatabase 디렉터리의 내용을 앞에서 생성한 12.52 SP1 smkeydatabase 디렉터리에 추가합니다.

   b. 다음 마이그레이션 유틸리티를 사용하여 smkeydatabase 를 인증서 데이터 저장소로 마이그레이션합니다.

   ```
   smmigratecds
   ```

   c. 마이그레이션에 성공하면 smkeydatabase 속성 파일과 smkeydatabase 디렉터리를 제거합니다.

   마이그레이션이 완료되었습니다.

추가 정보:

SiteMinder 키 데이터베이스 수동 마이그레이션 (페이지 177)

어설션 발급자 ID 마이그레이션

r12.x 환경에서 Federation Security Services(레거시 페더레이션) 개체를 관리하는 경우 어설션 발급자 ID 를 r12.x Producer 에서 12.52 SP1 Producer 로 마이그레이션하십시오. ID 를 마이그레이션하면 SAML 1.1 트랜잭션이 서비스 공급자에서 실패하지 않습니다.

다음 단계를 수행하십시오.

1. r6.x 정책 서버 호스트 시스템에 로그인하고 다음 위치로 이동합니다.

   siteminder_home\config\properties

   siteminder_home

   정책 서버 설치 경로를 지정합니다.

2. 다음 파일을 복사합니다.

   AMAssertionGenerator.properties

3. 12.52 SP1 정책 서버 호스트 시스템에 로그인하고 다음 위치로 이동합니다.

   siteminder_home\config\properties

4. 12.52 SP1 버전의 어설션 생성기 속성 파일의 이름을 다음 값으로 변경합니다.

   newAMAssertionGenerator.properties

5. 디렉터리에 r6.x 버전의 속성 파일을 추가합니다.

   마이그레이션이 완료되었습니다.

r6.x 정책 마이그레이션

r6.x 리소스를 보호하기 위해 12.52 SP1 배포를 사용할 계획이라면 정책 저장소 데이터를 12.52 SP1 정책 저장소로 마이그레이션하는 것이 좋습니다.

12.52 SP1 정책 저장소를 관리하기 전에 정책 저장소 데이터를 마이그레이션하면 개체가 중복되어 혼란이 발생하는 문제를 방지할 수 있습니다.

다음 단계를 수행하십시오.

1. r6.x 버전의 smobjexport 유틸리티를 사용하여 r6.x 정책 저장소 데이터를 내보냅니다.

   참고: r6.x 버전의 smobjexport 유틸리티에 대한 자세한 내용은 r6.x 정책 서버 설치 안내서를 참조하십시오.

2. 12.52 SP1 버전의 smobjimport 유틸리티를 사용하여 정책 데이터를 12.52 SP1 정책 저장소로 가져옵니다.

   업그레이드나 정책 마이그레이션의 일부로 한 환경의 SiteMinder 정책을 다른 환경으로 이동할 경우 환경과 관련된 일부 개체가 내보내기 파일에 포함됩니다. 예를 들면 다음과 같은 개체입니다.

   - 트러스트된 호스트
   - HCO 정책 서버 설정
   - 인증 체계 URL
   - 암호 서비스 리디렉션
   - 리디렉션 응답

3. Oracle Directory Server 의 경우 모든 인덱스를 다시 생성합니다.

사용자 디렉터리 싱글 사인온 요구 사항

두 환경 모두에서 생성한 SiteMinder 사용자 디렉터리 개체의 이름이 동일한지 확인하십시오. 다른 이름을 사용하여 r6.x 및 12.52 SP1 정책 서버를 동일한 사용자 저장소에 연결할 경우 싱글 사인온에 실패합니다.

제 3 장: SiteMinder r12.x 에서 업그레이드

이 섹션은 다음 항목을 포함하고 있습니다.

마이그레이션 고려 사항

r12.x 에서 마이그레이션하는 경우 마이그레이션을 시작하기 전에 다음 사항을 고려하십시오.

관리 UI 업그레이드 경로

다음과 같은 업그레이드 고려 사항을 검토하십시오.

- 기존 응용 프로그램 서버에서 12.5 이전 버전의 관리 UI 를 12.52 SP1 버전으로 업그레이드할 수 없습니다. 대신 다음 단계를 완료하십시오.
  a. 관리 UI 의 r12.x 버전을 제거합니다.
  b. SiteMinder 가 지원하는 응용 프로그램 서버를 설치합니다.
  c. 새 12.52 SP1 관리 UI 를 설치합니다.

  참고:관리 UI 설치에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.
- 기존 응용 프로그램 서버 인프라에서는 12.5 버전의 관리 UI 만 12.52 SP1 버전으로 업그레이드할 수 있습니다.
- 포함된 버전의 JBoss 를 사용하는 r12.x 관리 UI 를 12.52 SP1 버전으로 업그레이드할 수 있습니다.

참고: 관리 UI 업그레이드에 대한 자세한 내용은 r12.x 에서 마이그레이션하는 방법 (페이지 94) 및 r12.x 관리 UI 업그레이드 (페이지 111)의 지침을 참조하십시오.

SiteMinder 를 사용한 관리 UI 보호

SiteMinder 를 사용하여 12.52 SP1 관리 UI 를 보호할 수 있습니다. 관리 UI 를 보호하려면 다음 단계를 완료해야 합니다.

1. 에이전트가 리버스 프록시 서버에서 작동하도록 구성합니다.

   참고: 리버스 프록시 서버를 구성하는 방법에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

2. 외부 관리자 저장소를 구성합니다. 저장소를 구성할 때 SiteMinder 인증이 사용되도록 설정합니다.

   참고: 외부 관리자 저장소 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

r12.x 관리 UI 를 외부 관리자 저장소와 함께 구성한 상태에서 SiteMinder 인증이 사용되도록 설정하려면 다음 단계를 완료하십시오.

1. 에이전트가 리버스 프록시 서버에서 작동하도록 구성합니다.
2. 필요한 에이전트 설정을 사용하여 외부 관리자 저장소를 다시 구성합니다.

중요! 저장소를 다시 구성하면 관리 UI 에서 설정이 유지되지 않습니다. 따라서 연결을 다시 구성하기 전에 먼저 연결을 확인하고 설정을 기록해 두는 것이 좋습니다.

싱글 사인온

12.52 SP1 로 마이그레이션하는 동안 싱글 사인온을 유지할 수 있습니다. 다음 사항을 고려하십시오.

- 12.52 SP1 정책 서버는 r12.x 정책 저장소 및 r12.x 키 저장소와 통신할 수 있습니다.
- 12.52 SP1 정책 서버는 r12.x 세션 저장소와 통신할 수 있습니다.

인증서 데이터 관리

인증서 데이터 저장소는 SiteMinder 키 데이터베이스(smkeydatabase)를 대체합니다. 환경에 하나 이상의 smkeydatabase 를 배포한 경우에는 다음 사항을 고려하십시오.

- 인증서 데이터 저장소는 12.52 SP1 정책 저장소와 같은 곳에 배치됩니다. 인증서 데이터 저장소 하나가 있으면 각 정책 서버 호스트 시스템마다 개별적인 smkeydatabase 인스턴스가 있을 필요가 없습니다.
- 정책 서버 업그레이드의 일환으로 모든 smkeydatabase 콘텐츠가 자동으로 백업되고 인증서 데이터 저장소로 마이그레이션됩니다.
- 12.52 SP1 정책 서버는 인증서 데이터 저장소와만 통신할 수 있습니다. 12.52 SP1 정책 서버와 해당 로컬 smkeydatabase 는 호환성 모드에서 작동하지 않습니다. 하지만 업그레이드되지 않은 모든 정책 서버는 계속해서 로컬 버전의 smkeydatabase 와 통신합니다.

  중요! smkeydatabase 의 마이그레이션이 실패한 경우 정책 서버를 환경으로 되돌리지 마십시오. 마이그레이션 실패 후 정책 서버를 되돌리면 인증서 데이터가 필요한 모든 트랜잭션이 실패합니다.
- 마이그레이션을 시작하기 전에 모든 smkeydatabase 인스턴스를 동기화하십시오. 모든 인스턴스를 동기화하면 데이터 충돌을 방지할 수 있습니다. 데이터 충돌이 있으면 마이그레이션에 성공할 수 없습니다.
- 동일한 정책 저장소에 대한 공통의 뷰를 공유하는 모든 정책 서버는 동일한 키, 인증서 및 CRL(인증서 해지 목록)에 액세스할 수 있습니다.
- 인증서 데이터 저장소의 용도는 smkeydatabase 의 용도에서 변경되지 않고 유지됩니다. 이 저장소는 SiteMinder 환경에서 다음을 사용할 수 있게 합니다.
  - CA(인증 기관) 인증서
  - 공개 키 및 개인 키
  - 인증서 해지 목록
- SiteMinder 키 도구를 사용하여 인증서 데이터 저장소를 계속 관리할 수 있습니다. 하지만 몇 가지 옵션은 더 이상 사용할 수 없습니다.

  참고: 자세한 내용은 *정책 서버 릴리스 정보*를 참조하십시오.

- CRL 이 LDAP 디렉터리 서비스에 저장된 경우 다음 사항을 고려하십시오.
  - SiteMinder 에서는 더 이상 CRL 의 발급자가 해당 루트 인증서를 발급한 CA 와 동일하지 않아도 됩니다.
  - SiteMinder 에서는 더 이상 인증서 해지 목록의 발급자를 확인하지 않습니다. 이 동작은 텍스트 기반 CRL 에 대한 요구 사항과 일치합니다.

페더레이션 통합

r12.x FSS 관리 UI 에서 사용할 수 있는 모든 Federation Security Services 기능이 관리 UI 로 이전되었습니다. 이전에 페더레이션 환경을 관리했던 경우 이제는 이 기능을 레거시 페더레이션이라고 합니다.

관리 UI 에는 파트너 관계 페더레이션도 포함됩니다. 이 기능은 CA SiteMinder?Federation 를 통해 사용할 수 있는 파트너 관계 기반 페더레이션에 한정됩니다.

정책 저장소 손상 방지

가능한 정책 저장소 손상을 방지하려면 정책 저장소를 호스트하는 서버가 개체를 UTF-8 형식으로 저장하도록 구성되어 있는지 확인하십시오.

참고: 개체를 UTF-8 형식으로 저장하도록 서버를 구성하는 방법에 대한 자세한 내용은 해당 공급업체의 설명서를 참조하십시오.

Advanced Password Services

고급 암호 서비스를 배포한 경우 정책 서버 업그레이드 시 모든 LANG(번역), CFG(구성) 및 메일 파일이 유지됩니다. 12.52 SP1 버전의 기본 파일은 *siteminder_home*\samples 에 설치됩니다

siteminder_home

정책 서버 설치 경로를 지정합니다.

CA Arcot WebFort 및 CA Arcot RiskFort 와 SiteMinder 통합

SiteMinder 12.5 또는 이전 릴리스를 CA Arcot Adapter 를 사용하여 CA Arcot WebFort 및 CA RiskFort 와 통합한 경우, SiteMinder 를 12.52 이상으로 업그레이드하려면 다음 단계를 수행하십시오.

1. AFM_HOME\conf 디렉터리로 이동합니다.
2. adaptershim.ini 파일을 백업합니다.
3. SiteMinder 를 업그레이드합니다.
4. ARCOT_HOME\conf 디렉터리에서 백업된 adaptershim.ini 파일을 복사합니다.

r12.x 마이그레이션 작동 방법

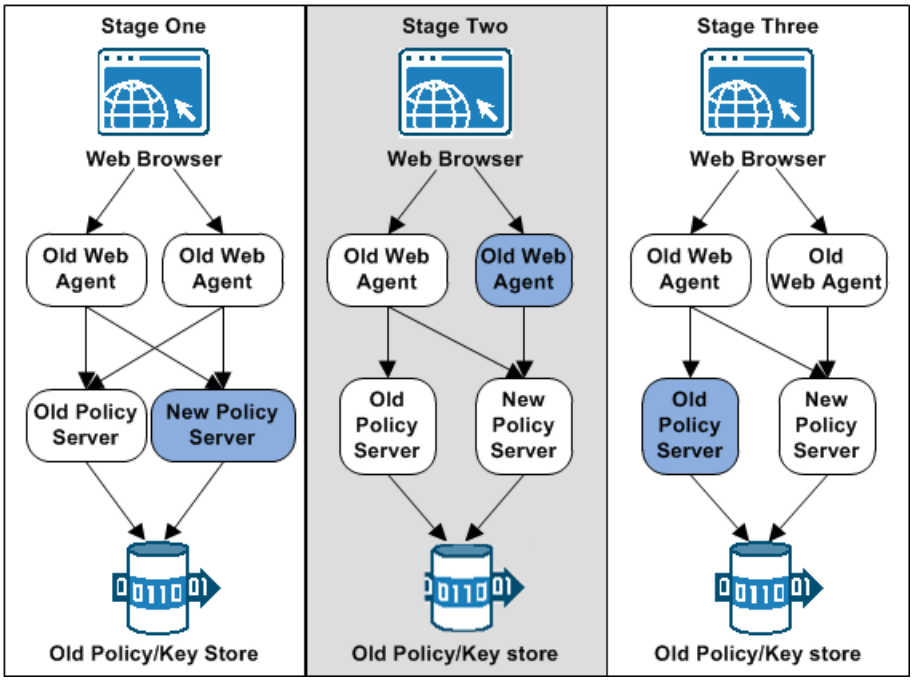
여러 정책 서버 및 웹 에이전트가 포함된 SiteMinder 배포를 마이그레이션하려면 SiteMinder 환경에서 정책 서버 및 웹 에이전트 중 하나를 제거하십시오. 이러한 구성 요소가 업그레이드되는 동안 나머지 정책 서버 및 웹 에이전트에서 리소스를 계속 보호합니다.

모든 구성 요소가 업그레이드되거나 혼합 모드 호환성 상태로 작동할 때까지 SiteMinder 구성 요소 제거 및 업그레이드를 계속하십시오.

다음 그림에는 간단한 r12.x 환경이 나와 있으며 기존 구성 요소를 업그레이드하는 순서가 설명되어 있습니다.

참고: 각 그림에는 단일 정책/키 저장소가 있습니다. 실제 사용 환경에서는 별개의 정책 저장소와 키 저장소를 사용할 수 있습니다.

그림 10: r12.x 마이그레이션 개요.

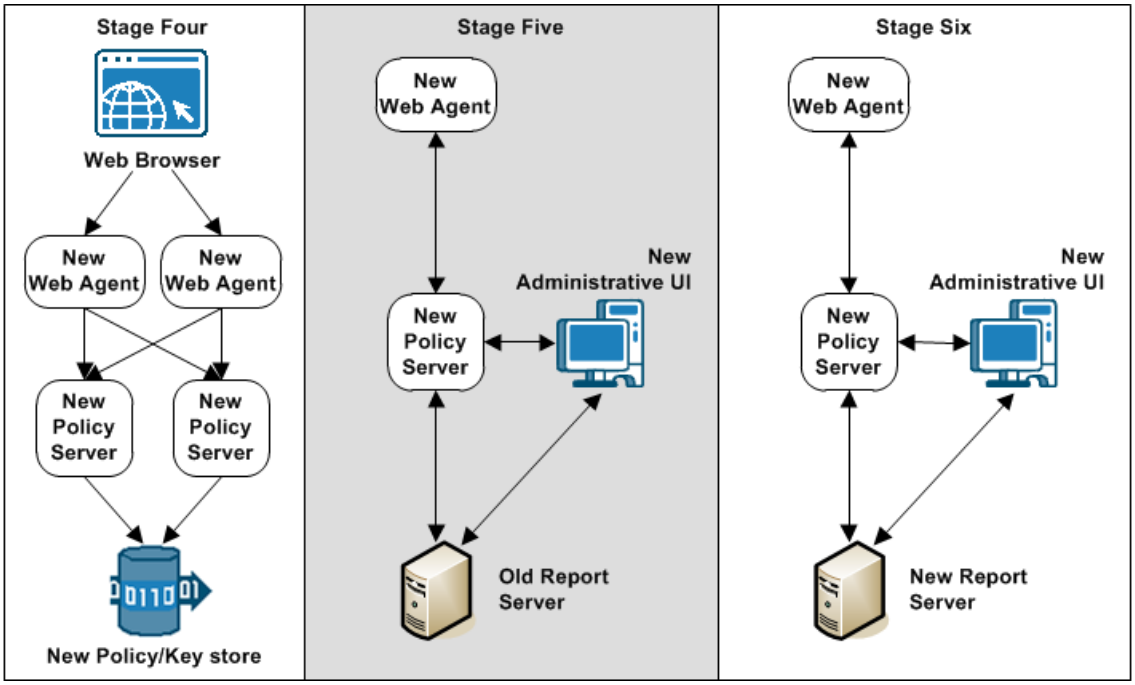


1. 1 단계에서는 r12.x 정책 서버를 업그레이드합니다. 12.52 SP1 정책 서버는 호환성 모드에서 작동합니다. 다음 사항을 고려하십시오.
   - r12.x 웹 에이전트는 12.52 SP1 정책 서버와 계속해서 통신합니다.
   - 12.52 SP1 정책 서버는 r12.x 정책 및 키 저장소와 계속해서 통신합니다.
   - r12.x 정책 서버는 r12.x 정책 및 키 저장소와 계속해서 통신합니다.
   - r12.x 관리 UI 에 12.52 SP1 정책 서버가 구성되어 있으면 관리 UI 는 해당 정책 서버와 계속해서 통신하여 r12.x 정책 저장소의 개체를 관리합니다.
   - r12.x 보고서 서버에 12.52 SP1 정책 서버가 구성되어 있으면 보고서 서버가 보고서를 계속해서 생성합니다.

2. 2 단계에서는 r12.x 웹 에이전트가 12.52 SP1 로 업그레이드됩니다.
   - r12.x 웹 에이전트는 r12.x 및 12.52 SP1 정책 서버와 계속해서 통신합니다.
   - 12.52 SP1 웹 에이전트는 12.52 SP1 정책 서버와만 통신합니다.

     참고: 마이그레이션 중에 12.52 SP1 정책 서버와 함께 새로운 12.52 SP1 웹 에이전트를 구성할 수 있습니다. 하지만 12.52 SP1 구성 요소는 최신 버전의 정책 서버에서 지원되는 기능만 지원합니다.
3. 3 단계에서는 나머지 정책 서버가 12.52 SP1 로 업그레이드됩니다. 12.52 SP1 정책 서버는 r12.x 정책 및 키 저장소와의 호환성 모드에서 작동합니다.

그림 11: rr12.x 마이그레이션 개요.



4. 4 단계에서는 r12.x 정책 및 키 저장소가 12.52 SP1 로 업그레이드됩니다.
5. 5 단계에서는 관리 UI 가 업그레이드됩니다.
6. 6 단계에서는 r12.x 보고서 서버가 제거됩니다. 12.52 SP1 보고서 서버를 설치하고 정책 서버에 등록한 다음 관리 UI 에 연결합니다.

   참고: r12.0 SP3 cr4 이상의 보고서 서버를 설치하고 구성한 경우에는 이 단계가 필요하지 않습니다.

r12.x 에서 마이그레이션하는 방법

r12.x 에서 12.52 SP1 로 마이그레이션하려면 다음 절차를 완료하십시오.

1. *정책 서버 릴리스 정보*에서 설치 및 업그레이드 고려 사항을 검토합니다.
2. (선택 사항) 환경에 여러 개의 smkeydatabase 인스턴스가 포함된 경우 모든 인스턴스를 동기화합니다. 정책 서버 업그레이드에는 smkeydatabase 의 모든 콘텐츠를 인증서 데이터 저장소로 마이그레이션하는 작업이 포함됩니다.
3. "정책 서버를 업그레이드하기 전에"의 단원을 검토합니다.
4. r12.x 정책 서버를 12.52 SP1 로 업그레이드합니다.
5. r12.x 웹 에이전트를 12.52 SP1 로 업그레이드합니다.
6. 나머지 r12.x 정책 서버와 웹 에이전트를 각각 12.52 SP1 로 업그레이드합니다.
7. r12.x 정책 및 키 저장소를 12.52 SP1 로 업그레이드합니다.
8. r12.x 관리 UI 를 업그레이드합니다.
9. 필요한 경우 관리 UI 를 사용하여 기존 보고서를 로컬로 저장하고 r12.x 보고서 서버 및 보고서 데이터베이스를 환경에서 제거합니다. 12.52 SP1 보고 환경을 구축하는 가장 간단한 방법은 새 보고서 서버 및 보고서 데이터베이스를 설치하고 구성하는 것입니다.

키 데이터베이스 인스턴스 동기화

새 버전으로 마이그레이션을 시작하기 전에 모든 smkeydatabase 인스턴스를 동기화하십시오.

참고: smkeydatabase 를 동기화하고 smkeydatabase 인스턴스 간의 모든 데이터 불일치를 해결하려면 smkeytool 유틸리티를 사용하십시오. smkeytool 유틸리티에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

이전 버전의 SiteMinder 에서는 인증서 데이터를 저장하는 데 로컬 smkeydatabase 가 사용되었습니다. 각 정책 서버에는 고유한 smkeydatabase 가 필요했습니다. 12.52 SP1 버전의 경우 중앙 집중화된 인증서 데이터 저장소가 로컬 smkeydatabase 를 대체합니다.

설치 관리자는 정책 서버 업그레이드의 일부로 로컬 smkeydatabase 를 자동으로 백업하고 모든 콘텐츠를 인증서 데이터 저장소로 마이그레이션하려고 시도합니다. 이 과정에는 마이그레이션 시작 전 두 저장소 모두를 비교하는 작업이 포함됩니다.

중요! smkeydatabase 의 마이그레이션이 실패한 경우 정책 서버를 환경으로 되돌리지 마십시오. 마이그레이션 실패 후 정책 서버를 되돌리면 인증서 데이터가 필요한 모든 트랜잭션이 실패합니다.

다음 지침을 따라 smkeydatabase 간의 데이터 일관성을 확인하고 해결하십시오.

- 각 인증 기관 인증서가 인스턴스 간에 일관되게 인증서 해지 목록을 참조하는지 확인하십시오.

  예: 인증 기관 인증서는 LDAP 디렉터리 서비스의 인증서 해지 목록을 일관되게 참조합니다.

- defaultentpriseprivatekey 별칭이 모든 인스턴스에서 동일한 개인 키/인증서 쌍을 나타내는지 확인하십시오.
- 동일한 별칭이 동일한 인증서 또는 키/인증서 쌍에 매핑되는지 확인하십시오.
- 동일한 인증 기관 인증서가 동일한 인증서 해지 목록에 매핑되는지 확인하십시오.
- 해지되거나 만료된 인증서가 없는지 확인하십시오.
- 모든 CRL 정보가 유효한지 확인하십시오.

중요! 모든 데이터 불일치를 해결한 후에는 마이그레이션이 모두 완료될 때까지 smkeydatabase 를 수정하지 않는 것이 좋습니다.

r12.x 정책 서버 업그레이드

다음 단원에서는 Windows 및 UNIX 에서 r12.x 정책 서버를 업그레이드하는 방법에 대해 자세히 설명합니다.

업그레이드하기 전에

정책 서버를 업그레이드하기 전에 다음 사항을 고려하십시오.

- (선택 사항) 환경에 smkeydatabase 인스턴스가 여러 개 있는 경우에는 모든 콘텐츠를 동기화해야 합니다. 동기화하면 정책 서버 설치 관리자가 콘텐츠를 인증서 데이터 저장소로 자동으로 마이그레이션하는 데 방해가 되는 데이터 불일치 문제가 해결됩니다.
- 기술 지원 사이트의 설치 미디어를 사용하여 정책 서버를 업그레이드하십시오.
- (Linux) 필요한 Linux 라이브러리가 정책 서버 호스트 시스템에 설치되었는지 확인하십시오. 자세한 내용은 "필요한 Linux 라이브러리"를 참조하십시오.
- 환경에서 정책 서버를 제거하십시오. 정책 서버를 제거하면 업그레이드 중에 SiteMinder 에이전트가 정책 서버에 연결하는 것을 방지할 수 있습니다.
- 정책 서버 관리 콘솔의 모든 인스턴스를 종료합니다.
- (UNIX) 정책 서버를 업그레이드하는 사용자 계정에는 설치 미디어가 포함된 디렉터리에 대한 실행 권한이 있어야 합니다. 사용자 계정에 이러한 권한이 없는 경우 다음 명령을 실행하십시오.

  `chmod +x installation_media`

  installation_media

  정책 서버 설치 실행 파일을 지정합니다.
- (UNIX) 여러 서브넷에서 정책 서버를 실행하면 정책 서버가 충돌할 수 있습니다. 정책 서버 설치 관리자를 호스트 시스템에서 직접 실행하십시오.
- (UNIX) 최소한 정책 서버를 설치한 사용자와 동일한 권한을 가진 계정을 사용하여 정책 서버를 업그레이드하십시오. 예를 들어 루트 사용자가 정책 서버를 설치한 경우 루트 사용자를 사용하여 정책 서버를 업그레이드하십시오.

필요한 Linux 라이브러리

Linux 운영 환경에서 작동하는 구성 요소의 경우 특정 라이브러리 파일이 필요합니다. 올바른 라이브러리를 설치하지 못하면 다음과 같은 오류가 발생할 수 있습니다.

```
java.lang.UnsatisfiedLinkError
```

이 구성 요소의 Linux 버전을 설치, 구성 또는 업그레이드하는 경우 호스트 시스템에 다음 패키지가 필요합니다.

Red Hat 5.x:

- compat–gcc-34-c++-3.4.6-*patch_version*.I386
- libstdc++-4.x.x-x.el5.i686.rpm
- libidn.so.11.rpm
- ncurses

Red Hat 6.x:

- libstdc++-4.x.x-x.el6.i686.rpm
- libidn-1.18-2.el6.i686
- libXext.i686.rpm
- libXrender.i686.rpm
- linXtst.i686.rpm
- libidn.so.11.rpm
- ncurses

또한 Red Hat 6.x(64 비트)의 경우:

64 비트 Red Hat 6.x 에 필요한 모든 RPM 패키지는 *32 비트* 패키지입니다.

- libXau-1.0.5-1.el6.i686.rpm
- libxcb-1.5-1.el6.i686.rpm
- compat-db42-4.2.52-15.el6.i686.rpm
- compat-db43-4.3.29-15.el6.i686.rpm
- libX11-1.3-2.el6.i686.rpm
- libXrender-0.9.5-1.el6.i686.rpm
- libexpat.so.1(expat-2.0.1-11.el6_2.i686.rpm 에서 제공)
- libfreetype.so.6(freetype-2.3.11-6.el6_2.9.i686.rpm 에서 제공)
- libfontconfig.so.1(fontconfig-2.8.0-3.el6.i686.rpm 에서 제공)
- libICE-1.0.6-1.el6.i686.rpm
- libuuid-2.17.2-12.7.el6.i686.rpm
- libSM-1.1.0-7.1.el6.i686.rpm
- libXext-1.1-3.el6.i686.rpm
- compat-libstdc++-33-3.2.3-69.el6.i686.rpm
- compat-db-4.6.21-15.el6.i686.rpm
- libXi-1.3-3.el6.i686.rpm
- libXtst-1.0.99.2-3.el6.i686.rpm
- libXft-2.1.13-4.1.el6.i686.rpm
- libXt-1.0.7-1.el6.i686.rpm
- libXp-1.0.0-15.1.el6.i686.rpm

- libstdc++.i686.rpm
- compat-libtermcap.rpm
- libidn.i686.rpm
- ncurses

정책 서버 업그레이드 전에 XML 서명 래핑 검사 사용 안 함

서비스 공급자의 정책 서버를 업그레이드한 후 SiteMinder Federation(레거시 또는 파트너 관계) 배포에서 SAML 2.0 아티팩트 트랜잭션이 실패합니다.

다음과 같은 경우에 트랜잭션이 실패합니다.

- SiteMinder Federation 이 서비스 공급자 사이트에 배포된 경우
- SAML 2.0 HTTP-아티팩트 SSO 가 구성된 경우
- 어설션 또는 아티팩트 확인 응답을 위해 서비스 공급자에서 서명 확인이 구성된 경우
- XML 서명 래핑 공격을 방지하는 정책 서버 설정을 사용할 수 있는 경우

정책 서버에서 아티팩트 응답의 서명을 확인하려고 하면 SSO 트랜잭션이 실패합니다.

아티팩트 SSO 가 실패하지 않게 하려면 서명 취약성 검사를 일시적으로 해제하십시오. 서비스 공급자의 정책 서버를 업그레이드한 후 정책 서버를 사용하기 전에 이 검사를 해제해야 합니다.

다음 단계를 수행하십시오.

1. xsw.properties 파일로 이동합니다. 이 파일은 다음 디렉터리에 있습니다.

   siteminder_install_dir\config\properties\xsw.properties

   siteminder_install_dir 는 정책 서버를 설치한 위치입니다.
2. 텍스트 편집기에서 파일을 열고 DisableXSWCheck 를 true 로 설정합니다(DisableXSWCheck=true). 이 값을 true 로 설정하면 취약성 검사가 해제됩니다.
3. 전체 배포가 12.52 SP1 버전으로 업그레이드되고 정책 서버가 실행되면 DisableXSWCheck 설정을 false 로 되돌립니다(DisableXSWCheck=false). 이 값을 false 로 설정하면 서명 취약성 검사가 실행됩니다.

각 SAML 파트너 관계에서 백 채널 사용자 이름이 고유한지 확인

HTTP-아티팩트 싱글 사인온 트랜잭션 중에 어설션 당사자가 보안이 유지되는 백 채널을 통해 어설션을 신뢰 당사자에게 반환합니다. 엔터티가 백 채널에 액세스하려면 인증이 필요하도록 설정할 수 있습니다. 백 채널에 대한 인증 방법으로 "기본"을 선택하는 경우 사용자 이름이 필요합니다.

업그레이드하기 전에 동일한 SAML 프로필 내 각 페더레이션된 파트너 관계가 수신 백 채널에 대해 고유한 사용자 이름을 사용하는지 확인하십시오. 두 개의 SAML 2.0 또는 SAML 1.x 파트너 관계가 수신 백 채널 사용자 이름을 공유할 수 없습니다.

참고: SAML 1.x 및 SAML 2.0 파트너 관계는 수신 백 채널 사용자 이름을 공유할 수 있지만 권장되지는 않습니다.

수신 백 채널 사용자 이름을 공유하는 동일한 프로토콜의 파트너 관계가 있는 경우 업그레이드 전에 다음 단계를 수행하십시오.

1. 파트너 관계 중 하나를 비활성화합니다.
2. 파트너 관계에 정의된 백 채널 사용자 이름을 변경합니다.
3. 원격 파트너에게 이 변경 사항을 알립니다.
4. 파트너 관계를 다시 활성화합니다.

Windows 에서 정책 서버 업그레이드

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. 설치 미디어를 탐색합니다.
3. *installation_media* 를 두 번 클릭합니다.

   installation_media

   정책 서버 설치 실행 파일의 이름을 지정합니다.
4. 설치 관리자를 실행할 때는 다음 사항을 고려하십시오.
   - 구성 요소를 선택하라는 메시지가 표시됩니다. 구성 요소를 선택하는 경우:
     - 환경에 대해 이전에 구성된 구성 요소를 재구성하십시오. 각 구성 요소를 선택하십시오.

- 업그레이드 중에 구성 마법사에서 정책 저장소 확인란을 선택 취소한 상태로 두고 기존 정책 저장소를 유지합니다. 하지만 구성 마법사에서 고급 인증 서버에 대한 암호화 키를 요구하는 메시지가 표시됩니다. 이 키는 각 정책 서버에 저장되지만 모든 정책 서버에 동일한 키가 필요합니다.
- 다른(n 번째) 정책 서버를 업그레이드하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.

- 설치 관리자는 smkeydatabase 를 발견하면 다음을 수행합니다.
  - smkeydatabase 를 백업합니다.
  - 콘텐츠를 인증서 데이터 저장소로 마이그레이션하려고 시도합니다.

  중요! smkeydatabase 의 마이그레이션이 실패한 경우 정책 서버를 환경으로 되돌리지 마십시오. 마이그레이션 실패 후 정책 서버를 되돌리면 인증서 데이터가 필요한 모든 트랜잭션이 실패합니다.

5. 설치 설정을 검토하고 "설치"를 클릭합니다.

   정책 서버가 업그레이드됩니다. 선택한 구성 요소가 정책 서버와 함께 사용할 수 있도록 구성됩니다.

UNIX 에서 GUI 를 사용하여 정책 서버 업그레이드

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. SiteMinder 설치 디렉터리의 ksh 셸에서 다음 스크립트를 실행합니다.

   ```
   ../ca_ps_env.ksh
   ```

   참고: 마침표 사이에 공백이 있어야 합니다.
3. 셸을 열고 설치 실행 파일이 있는 위치로 이동합니다.
4. 다음 명령을 입력합니다.

   ```
   ./installation_media
   ```

   installation_media

   정책 서버 설치 관리자 실행 파일의 이름을 지정합니다.

5. 설치 관리자를 실행할 때는 다음 사항을 고려하십시오.
   - 구성 요소를 선택하라는 메시지가 표시됩니다. 구성 요소를 선택하는 경우:
     - 환경에 대해 이전에 구성된 구성 요소를 재구성하십시오. 각 구성 요소를 선택하십시오.
     - 업그레이드 중에 구성 마법사에서 정책 저장소 확인란을 선택 취소한 상태로 두고 기존 정책 저장소를 유지합니다. 기존 정책 저장소를 수동으로 업그레이드하십시오. 하지만 구성 마법사에서 고급 인증 서버에 대한 암호화 키를 요구하는 메시지가 표시됩니다. 이 키는 각 정책 서버에 저장되지만 모든 정책 서버에 동일한 키가 필요합니다. 기존 정책 저장소를 수동으로 업그레이드하십시오.
     - 다른(n 번째) 정책 서버를 업그레이드하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.
   - 설치 관리자는 smkeydatabase 를 발견하면 다음을 수행합니다.
     - smkeydatabase 를 백업합니다.
     - 콘텐츠를 인증서 데이터 저장소로 마이그레이션하려고 시도합니다.

     중요! smkeydatabase 의 마이그레이션이 실패한 경우 정책 서버를 환경으로 되돌리지 마십시오. 마이그레이션 실패 후 정책 서버를 되돌리면 인증서 데이터가 필요한 모든 트랜잭션이 실패합니다.
6. 설치 설정을 검토하고 "설치"를 클릭합니다.

   정책 서버가 업그레이드됩니다. 선택한 구성 요소가 정책 서버와 함께 사용할 수 있도록 구성됩니다.
7. "Done"(완료)을 클릭합니다.
8. SiteMinder 설치 디렉터리의 ksh 셸에서 다음 스크립트를 실행합니다.

   ```
   ../ca_ps_env.ksh
   ```

   참고: 마침표 사이에 공백이 있어야 합니다.

UNIX 에서 콘솔을 사용하여 정책 서버 업그레이드

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.

2. SiteMinder 설치 디렉터리의 ksh 셸에서 다음 스크립트를 실행합니다.

   ```
   ../ca_ps_env.ksh
   ```

   참고: 마침표 사이에 공백이 있어야 합니다.

3. 셸을 열고 설치 실행 파일이 있는 위치로 이동합니다.

4. 다음 명령을 입력합니다.

   ```
   ./installation_media -i console
   ```

   installation_media

   정책 서버 설치 관리자 실행 파일의 이름을 지정합니다.

5. 설치 관리자를 실행할 때는 다음 사항을 고려하십시오.

   SiteMinder 구성 요소를 선택하라는 메시지가 표시됩니다. 각 구성 요소 앞에 숫자가 붙어 있습니다. 쉼표(,)로 분리된 숫자를 입력하여 하나 이상의 구성 요소를 선택하십시오. 기능을 선택하지 않으려면 쉼표만 입력하십시오.

   - 구성 요소를 선택할 때는 다음 사항을 고려하십시오.
     - 환경에 대해 이전에 구성된 구성 요소를 재구성하십시오. 각 구성 요소를 선택하십시오.
     - 업그레이드 중에 구성 마법사에서 정책 저장소 확인란을 선택 취소한 상태로 두고 기존 정책 저장소를 유지합니다. 기존 정책 저장소를 수동으로 업그레이드하십시오. 하지만 구성 마법사에서 고급 인증 서버에 대한 암호화 키를 요구하는 메시지가 표시됩니다. 이 키는 각 정책 서버에 저장되지만 모든 정책 서버에 동일한 키가 필요합니다.
     - 다른(n 번째) 정책 서버를 업그레이드하는 경우 고급 인증 서버에 대해 이전에 사용한 것과 동일한 암호화 키를 사용하십시오.
   - 설치 관리자는 smkeydatabase 를 발견하면 다음을 수행합니다.
     - smkeydatabase 를 백업합니다.
     - 콘텐츠를 인증서 데이터 저장소로 마이그레이션하려고 시도합니다.

     중요! smkeydatabase 의 마이그레이션이 실패한 경우 정책 서버를 환경으로 되돌리지 마십시오. 마이그레이션 실패 후 정책 서버를 되돌리면 인증서 데이터가 필요한 모든 트랜잭션이 실패합니다.

6. 설치 설정을 검토하고 Enter 키를 누릅니다.

   정책 서버가 업그레이드됩니다. 선택한 구성 요소가 정책 서버와 함께 사용할 수 있도록 구성됩니다.

7. "Done"(완료)을 클릭합니다.
8. SiteMinder 설치 디렉터리의 ksh 셸에서 다음 스크립트를 실행합니다.

   ```
   ../ca_ps_env.ksh
   ```

   참고: 마침표 사이에 공백이 있어야 합니다.

사용자 지정된 JVMOptions 파일 수정

정책 서버 업그레이드 중에 기존 JVMOptions.txt 파일의 이름이 JVMOptions.txt.backup 으로 변경됩니다. 새 JVMOptions.txt 파일이 생성됩니다.

원본 파일에 사용자 지정된 매개 변수가 포함된 경우 이러한 사용자 지정된 매개 변수를 포함하도록 새로 생성된 파일을 수정해야 합니다.

Apache 기반 에이전트의 경우 다음 예제처럼 JVMOptions.txt 파일의 CLASSPATH 에 SiteMinder/resources 디렉터리를 추가하십시오.

```
-Djava.class.path=C:/Program Files (x86)/CA/siteminder/resources;
```

사용자 지정 서버 측 코드 요구 사항

정책 서버 운영 체제는 사용자 지정 서버 측 코드를 다시 컴파일해야 하는지 여부를 확인합니다. 다음 표를 사용하여 요구 사항을 확인하십시오.

운영 체제	필수
Microsoft Windows 및 UNIX	아니요. 필요한 경우에만 사용자 지정 코드를 다시 컴파일합니다.
Red Hat Linux	예. SDK 를 업그레이드하고 GCC 3.4 를 사용하여 사용자 지정 코드를 다시 컴파일합니다.

정책 서버 업그레이드 문제 해결

업그레이드 중 문제가 발생하는 경우:

- *siteminder_home*\siteminder\install_config_info 에서 정책 서버 설치 로그 파일을 찾아 보십시오.

  siteminder_home

  정책 서버 설치 경로를 지정합니다.

- *siteminder_home*\log 에서 smkeydatabase 마이그레이션 로그(smkeydatabaseMigration.log)를 찾아 보십시오.

  참고: 정책 서버 업그레이드와 smkeydatabase 마이그레이션은 별개의 프로세스입니다. 따라서 smkeydatabase 마이그레이션이 실패하더라도 정책 서버 업그레이드는 실패하지 않습니다.

r12.x 웹 에이전트 업그레이드

마이그레이션 프로세스의 두 번째 단계에서는 웹 에이전트를 업그레이드합니다.

SiteMinder r12.x 웹 에이전트는 12.52 SP1 정책 서버와 통신할 수 있습니다. 따라서 웹 에이전트를 12.52 SP1 로 업그레이드하기 전에 정책 서버를 r12.5 로 업그레이드하십시오.

r12.x 웹 에이전트 업그레이드 전 작업

웹 에이전트를 업그레이드하기 전에 다음 사항을 고려하십시오.

- (UNIX) 웹 에이전트를 설치하는 데 사용된 것과 동일한 계정으로 웹 에이전트를 업그레이드해야 합니다. 다른 계정을 사용할 경우 업그레이드에 실패할 수 있습니다.
- 정책 서버가 구성되어 있는지 확인하십시오.
- 필요한 관리자 및 정책 서버 개체 이름을 확인하십시오.
- 웹 에이전트 요구 사항을 확인하십시오.

정책 서버가 구성되어 있는지 확인

웹 에이전트를 업그레이드하기 전에 다음 사항을 고려하십시오.

- 정책 서버가 웹 에이전트 호스트 시스템에 연결할 수 있는지 확인하십시오.
- 트러스트된 호스트를 등록하기 전에 정책 서버가 실행 중인지 확인하십시오. 정책 서버 관리 콘솔의 "상태" 탭에서 정책 서버를 시작합니다.

필요한 관리자 및 정책 서버 개체 이름 확인

웹 에이전트를 업그레이드하기 전에 정책 서버 관리자의 다음 정보가 필요합니다.

- 호스트를 등록할 수 있는 SiteMinder 관리자의 이름
- 호스트 구성 개체의 이름
- 에이전트 구성 개체의 이름

웹 에이전트 요구 사항 확인

패치 및 기타 웹 에이전트 요구 사항에 대한 자세한 내용은 *웹 에이전트 설치 안내서*를 참조하십시오.

r12.x 웹 에이전트 업그레이드

12.52 SP1 웹 에이전트 설치 관리자를 사용하여 웹 에이전트를 업그레이드하십시오.

- 12.52 SP1 웹 에이전트 옵션 팩을 설치하려면 먼저 옵션 팩 기능이 필요한 에이전트를 12.52 SP1 로 업그레이드해야 합니다.

  참고: 웹 에이전트 업그레이드에 대한 자세한 내용은 *웹 에이전트 설치 안내서*를 참조하십시오. 12.52 SP1 웹 에이전트 옵션 팩 설치에 대한 자세한 내용은 *웹 에이전트 옵션 팩 안내서*를 참조하십시오.

- 고급 암호 서비스를 배포한 경우 웹 에이전트 업그레이드에서 모든 LANG(변환) 및 CFG(구성) 파일을 유지합니다. 파일의 기본 12.52 SP1 버전은 agent_home\samples 에 설치됩니다.

  agent_home

  웹 에이전트 설치 경로를 지정합니다.

사용자 지정 에이전트 요구 사항

사용자 지정 에이전트를 다시 컴파일해야 하는지 여부를 확인하려면 다음 표를 사용하십시오.

에이전트 유형	필수
SiteMinder 에이전트	운영 체제에 따라 다릅니다. 에이전트 운영 체제가 만료된 경우에는 사용자 지정 에이전트를 다시 컴파일해야 합니다. SiteMinder SDK 를 업그레이드하고 지원되는 운영 체제에서 에이전트를 다시 컴파일합니다.
타사 에이전트	공급업체에 따라 다릅니다. 타사 공급업체에 문의하여 에이전트가 지원되는지 여부를 확인합니다.

r12.x 정책 저장소를 업그레이드하는 방법

r12.x 정책 저장소를 12.52 SP1 로 업그레이드하려면 다음 절차를 완료하십시오.

1. 정책 저장소와 통신 중인 모든 정책 서버를 중지합니다.
2. 정책 저장소 데이터 정의를 가져옵니다.
3. 기본 정책 저장소 개체를 가져옵니다.
4. FSS 관리 UI 를 사용하여 r12.x 레거시 페더레이션 환경을 관리했던 경우 XPS 스위퍼 유틸리티를 실행하여 레거시 페더레이션 개체의 마이그레이션을 완료합니다.
5. 정책 저장소와 통신 중인 모든 정책 서버를 시작합니다.

모든 정책 서버 중지

정책 저장소와 통신하는 모든 정책 서버를 중지하면 업그레이드 중 정책 저장소의 손상을 방지할 수 있습니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 단계 중 하나를 완료하십시오.
   - (Windows)
     a. 정책 서버 관리 콘솔을 열고 "중지"를 클릭합니다.
     b. "확인"을 클릭하여 콘솔을 닫습니다.
   - (UNIX) 제공된 다음 스크립트를 사용합니다.
     install_path/siteminder/stop-all

     install_path

     정책 서버 설치 경로를 지정합니다.
3. 정책 저장소와 통신하는 각 정책 서버에 대해 이 절차를 반복합니다.

정책 저장소 데이터 정의 가져오기

정책 저장소 데이터 정의 가져오기를 사용하여 정책 저장소에서 생성하고 저장할 수 있는 개체의 유형을 정의합니다.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home*\xps\dd 로 이동합니다.

   siteminder_home

   정책 서버 설치 경로를 지정합니다.
2. 다음 명령을 실행합니다.

   ```
   XPSDDInstall SmMaster.xdd
   ```

   XPSDDInstall

   필수 데이터 정의를 가져옵니다.

기본 정책 저장소 개체 가져오기

기본 정책 저장소 개체 가져오기를 사용하여 관리 UI 및 정책 서버에서 사용할 정책 저장소를 구성합니다.

다음 사항을 고려하십시오.

- *siteminer_home*\bin 에 대한 쓰기 액세스 권한이 있는지 확인하십시오. 가져오기 유틸리티에서 정책 저장소 개체를 가져오려면 이 권한이 필요합니다.

  siteminder_home

  정책 서버 설치 경로를 지정합니다.

- 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. 자세한 내용은 SiteMinder 구성 요소의 릴리스 정보를 참조하십시오.

다음 단계를 수행하십시오.

1. 명령 창을 열고 *siteminder_home*\db 로 이동합니다.
2. 다음 파일 중 하나를 가져옵니다.
   - smpolicy.xml 을 가져오려면 다음 명령을 실행합니다.

     ```
     XPSImport smpolicy.xml -npass
     ```

   - smpolicy-secure.xml 을 가져오려면 다음 명령을 실행합니다.

     ```
     XPSImport smpolicy-secure.xml -npass
     ```

   참고: 두 파일 중 하나를 사용하여 새 정책 저장소를 구성하거나 기존 저장소를 업그레이드합니다. 업그레이드 과정에서 개체를 가져오는 경우 해당 파일은 이미 수정된 기존의 기본 개체를 덮어쓰지 않습니다. 두 파일 모두 기본 정책 저장소 개체를 포함합니다. 이러한 개체는 기본 ACO(에이전트 구성 개체) 템플릿의 기본 보안 설정을 포함합니다. secure 파일은 보다 제한적인 보안 설정을 제공합니다.

   -npass

   암호를 사용할 필요가 없음을 지정합니다. 기본 정책 저장소 개체에 암호화된 데이터가 포함되지 않습니다.

   기본 정책 저장소 개체를 가져왔습니다.

XPS 스위퍼 유틸리티 실행

FSS 관리 UI 를 사용하여 Federation Security Services(레거시 페더레이션) 개체를 관리한 경우 XPS 스위퍼 유틸리티(XPSSweeper)를 실행하여 해당 개체의 마이그레이션을 완료하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 레거시 페더레이션 개체를 관리 UI 에서 사용할 수 있도록 설정합니다.

   `XPSSweeper`

   이제 FSS 관리 UI 를 사용하여 생성한 모든 레거시 페더레이션을 관리 UI 에서 사용할 수 있습니다.

모든 정책 서버 시작

모든 정책 서버를 시작하면 정책 서버와 업그레이드된 정책 저장소 간의 통신이 다시 시작됩니다.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 단계 중 하나를 완료하십시오.
   - (Windows)
     a. 정책 서버 관리 콘솔을 열고 "시작"을 클릭합니다.
     b. "확인"을 클릭하여 콘솔을 닫습니다.
   - (UNIX) 제공된 다음 스크립트를 사용합니다.
     install_path`/siteminder/start-all`

     install_path

     정책 서버 설치 경로를 지정합니다.
3. 정책 저장소와 통신하는 각 정책 서버에 대해 이 절차를 반복합니다.

정책 저장소가 업그레이드됩니다.

r12.x 관리 UI 업그레이드

다음 단원에서는 Windows 및 UNIX 에서 관리 UI 를 업그레이드하는 방법에 대해 자세히 설명합니다.

업그레이드하기 전에

관리 UI 를 업그레이드하기 전에 다음 사항을 고려하십시오.

- **중요!** 관리 UI 업그레이드 경로 (페이지 87)를 검토하십시오.
- 기술 지원 사이트의 설치 미디어를 사용하여 관리 UI 를 업그레이드하십시오.

  참고: 설치 미디어 이름의 목록에 대해서는 *정책 서버 릴리스 정보*를 참조하십시오.
- (포함된 JBoss 설치만 해당) 관리 UI 설치 관리자의 콘텐츠를 추출한 디렉터리에 필수 구성 요소 설치 관리자의 콘텐츠를 추출합니다. 각 설치 관리자 zip 파일의 콘텐츠는 layout.properties 파일과 같은 위치에 있어야 합니다. 관리 UI 설치 zip 에 포함된 layout.properties 파일은 항상 두 실행 파일과 같은 위치에 있어야 하며 그렇지 않을 경우 설치가 실패합니다.
- (Windows) 관리 UI 호스트 시스템에서 설치 관리자를 실행합니다. 설치 관리자를 매핑된 네트워크 공유 또는 UNC 경로에서 실행하지 마십시오.
- (Linux) 필요한 Linux 라이브러리가 관리 UI 호스트 시스템에 설치되었는지 확인합니다. 자세한 내용은 "필요한 Linux 라이브러리"를 참조하십시오.
- **중요!** (UNIX) 권한에 따라 다음 명령을 실행하여 설치 미디어가 있는 디렉터리에 대한 실행 권한을 추가합니다.

  `chmod -R+x directory`

  directory

  설치 미디어가 들어 있는 디렉터리를 지정합니다.
- (UNIX) 여러 서브넷에서 관리 UI 설치 관리자를 실행하면 설치 관리자가 충돌할 수 있습니다. 호스트 시스템에서 직접 관리 UI 설치 관리자를 실행합니다.

필요한 Linux 라이브러리

Linux 운영 환경에서 작동하는 구성 요소의 경우 특정 라이브러리 파일이 필요합니다. 올바른 라이브러리를 설치하지 못하면 다음과 같은 오류가 발생할 수 있습니다.

```
java.lang.UnsatisfiedLinkError
```

이 구성 요소의 Linux 버전을 설치, 구성 또는 업그레이드하는 경우 호스트 시스템에 다음 패키지가 필요합니다.

Red Hat 5.x:

- compat–gcc-34-c++-3.4.6-*patch_version*.I386
- libstdc++-4.x.x-x.el5.i686.rpm
- libidn.so.11.rpm
- ncurses

Red Hat 6.x:

- libstdc++-4.x.x-x.el6.i686.rpm
- libidn-1.18-2.el6.i686
- libXext.i686.rpm
- libXrender.i686.rpm
- linXtst.i686.rpm
- libidn.so.11.rpm
- ncurses

또한 Red Hat 6.x(64 비트)의 경우:

64 비트 Red Hat 6.x 에 필요한 모든 RPM 패키지는 *32 비트* 패키지입니다.

- libXau-1.0.5-1.el6.i686.rpm
- libxcb-1.5-1.el6.i686.rpm
- compat-db42-4.2.52-15.el6.i686.rpm
- compat-db43-4.3.29-15.el6.i686.rpm
- libX11-1.3-2.el6.i686.rpm
- libXrender-0.9.5-1.el6.i686.rpm
- libexpat.so.1(expat-2.0.1-11.el6_2.i686.rpm 에서 제공)
- libfreetype.so.6(freetype-2.3.11-6.el6_2.9.i686.rpm 에서 제공)
- libfontconfig.so.1(fontconfig-2.8.0-3.el6.i686.rpm 에서 제공)
- libICE-1.0.6-1.el6.i686.rpm
- libuuid-2.17.2-12.7.el6.i686.rpm
- libSM-1.1.0-7.1.el6.i686.rpm
- libXext-1.1-3.el6.i686.rpm
- compat-libstdc++-33-3.2.3-69.el6.i686.rpm
- compat-db-4.6.21-15.el6.i686.rpm
- libXi-1.3-3.el6.i686.rpm
- libXtst-1.0.99.2-3.el6.i686.rpm
- libXft-2.1.13-4.1.el6.i686.rpm
- libXt-1.0.7-1.el6.i686.rpm
- libXp-1.0.0-15.1.el6.i686.rpm

- libstdc++.i686.rpm
- compat-libtermcap.rpm
- libidn.i686.rpm
- ncurses

Windows 에서 관리 UI 업그레이드

다음 단계를 수행하십시오.

1. (포함된 JBoss 설치만 해당) 관리 UI 설치 관리자 zip 의 압축을 푼 디렉터리에 필수 구성 요소 설치 관리자 zip 의 압축을 풀었는지 확인합니다. 관리 UI 설치 zip 에 포함된 layout.properties 파일은 두 실행 파일과 같은 디렉터리에 있어야 합니다.

   참고: zip 파일의 압축을 푼 후 필수 구성 요소 또는 관리 UI 설치 실행 파일을 이동하면 layout.properties 파일도 같은 위치로 이동하십시오.

2. 실행 중인 응용 프로그램을 모두 종료합니다.
3. 관리 UI 를 호스팅 중인 응용 프로그램 서버를 중지합니다.

   참고: 포함된 JBoss 응용 프로그램 서버의 시작 및 중지에 대한 자세한 내용은 r12.x *정책 서버 설치 안내서*를 참조하십시오. 기존 응용 프로그램 서버 중지에 대한 자세한 내용은 해당 공급업체의 설명서를 참조하십시오.

4. 포함된 JBoss 설치의 경우 다음 실행 파일을 실행하고 설치 관리자의 프롬프트에 따릅니다. 그렇지 않은 경우 다음 단계로 건너뜁니다.

   `adminui-pre-req-version-cr-win32.exe`

5. 다음 실행 파일을 실행합니다.

   `ca-adminui-version-cr-win32.exe`

6. 설치 관리자의 프롬프트에 따라 관리 UI 업그레이드를 확인합니다.
7. 설치 설정을 검토하고 "설치"를 클릭합니다.
8. 기존 응용 프로그램 서버의 경우 설치가 완료된 후 응용 프로그램 서버를 다시 시작합니다.

   참고: 포함된 JBoss 응용 프로그램 서버는 설치가 완료된 후 자동으로 다시 시작됩니다.

관리 UI 가 업그레이드됩니다.

UNIX 에서 관리 UI 업그레이드

UNIX 플랫폼에서 GUI 또는 콘솔 모드를 사용하여 관리 UI 를 설치할 수 있습니다.

다음 단계를 수행하십시오.

1. (포함된 JBoss 설치만 해당) 관리 UI 설치 관리자 zip 의 압축을 푼 디렉터리에 필수 구성 요소 설치 관리자 zip 의 압축을 풀었는지 확인합니다. 관리 UI 설치 zip 에 포함된 layout.properties 파일은 두 실행 파일과 같은 디렉터리에 있어야 합니다.

   참고: zip 파일의 압축을 푼 후 필수 구성 요소 또는 관리 UI 설치 실행 파일을 이동하면 layout.properties 파일도 같은 위치로 이동하십시오.

2. 실행 중인 응용 프로그램을 모두 종료합니다.

3. 관리 UI 를 호스팅 중인 응용 프로그램 서버를 중지합니다.

   참고: 포함된 JBoss 응용 프로그램 서버의 시작 및 중지에 대한 자세한 내용은 r12.x *정책 서버 설치 안내서*를 참조하십시오. 기존 응용 프로그램 서버 중지에 대한 자세한 내용은 해당 공급업체의 설명서를 참조하십시오.

4. 포함된 JBoss 설치의 경우 필수 구성 요소 설치 관리자를 실행합니다. 그렇지 않은 경우 다음 단계로 건너뜁니다.

   a. 셸을 열고 다음과 같은 필수 구성 요소 설치 실행 파일 중 하나로 이동합니다.
   ```
   adminui-pre-req-version-cr-linux.bin
   adminui-pre-req-version-cr-sol.bin
   ```

   b. 해당 모드에 맞는 명령을 입력합니다.

   GUI 모드
   ```
   ./prerequisite_installation_media
   ```

   콘솔 모드
   ```
   ./prerequisite_installation_media –i console
   ```

   c. 필수 구성 요소 설치 관리자의 지시를 따릅니다.

5. 셸을 열고 다음 설치 실행 파일 중 하나로 이동합니다.

   ```
   ca-adminui-version-cr-linux.bin
   ca-adminui-version-cr-sol.bin
   ```

6. 해당 모드에 맞는 명령을 입력합니다.

   GUI 모드

   ```
   ./installation_media
   ```

   콘솔 모드

   ```
   ./installation_media –i console
   ```

7. 프롬프트에 따라 관리 UI 업그레이드를 확인합니다.
8. 설치 설정을 검토하고 "설치"를 클릭합니다.
9. 관리 UI 를 호스팅 중인 응용 프로그램 서버를 시작합니다.

   참고: 포함된 JBoss 응용 프로그램 서버의 시작 및 중지에 대한 자세한 내용은 r12.x *정책 서버 설치 안내서*를 참조하십시오. 기존 응용 프로그램 서버 중지에 대한 자세한 내용은 해당 공급업체의 설명서를 참조하십시오.

   관리 UI 가 업그레이드됩니다.

r12.x 보고서 서버 업그레이드

r12.0 SP3 CR4 이전 버전의 보고서 서버를 사용하는 경우 12.52 SP1 보고 환경을 구축하는 가장 간단한 방법은 설치된 버전을 제거한 다음 12.52 SP1 보고 구성 요소를 설치 및 구성하는 것입니다.

보고서 서버 r12.0 SP3 CR4 이상을 사용하는 경우에는 업그레이드가 필요하지 않습니다. 그러나 지역화된 보고서를 사용하려는 경우에는 12.52 SP1 보고 템플릿이 필요합니다. 따라서 보고 템플릿을 사용하려면 12.52 SP1 버전의 보고서 서버 구성 마법사를 실행하십시오.

보고서 서버는 정책 저장소 및 SiteMinder 감사 데이터베이스의 데이터를 사용하여 정책 분석 및 감사 기반 보고서를 컴파일합니다. 보고서 데이터베이스에는 이러한 보고서에 필요한 정보가 들어 있지 않습니다. 따라서 r12.x 보고서 데이터베이스에서 12.52 SP1 보고서 데이터베이스로 마이그레이션할 필요가 없습니다.

다음 절차에 따라 12.52 SP1 보고 구성 요소를 설치 및 구성하십시오.

1. (선택 사항) 기존 보고서를 내보냅니다.

   중요! 기존 보고서는 보고서 데이터베이스에 저장되어 있습니다. 기록 용도로 기존 보고서가 필요한 경우 관리 UI를 사용하여 보고서를 확인한 후 임시 위치로 해당 보고서를 내보내십시오. 보고서 보기에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

2. 보고서 서버와 관리 UI 간의 연결을 삭제합니다.

   참고: 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

3. r12.x 보고서 서버를 제거합니다.

   참고: 자세한 내용은 r12 SP2 *정책 서버 설치 안내서*를 참조하십시오. 보고서 서버를 제거해도 보고서 데이터베이스에 있는 테이블은 제거되지 않습니다. 보고서 데이터베이스에 액세스하여 수동으로 모든 테이블을 제거하십시오.

4. 12.52 SP1 보고 기능을 설치 및 구성합니다. 여기에는 다음과 같은 작업이 포함됩니다.

   a. 보고서 서버 설치

   b. SiteMinder 보고서 템플릿 설치

   c. 보고서 서버 등록

   d. 보고서 서버와 SiteMinder 감사 데이터베이스 간의 연결 구성

   참고: 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

r12.x 병렬 업그레이드 작동 방법

기존 r12.x 환경을 12.52 SP1 환경으로 마이그레이션할 필요는 없습니다. 대신 기존 배포에서 병렬 12.52 SP1 환경을 구성할 수 있습니다.

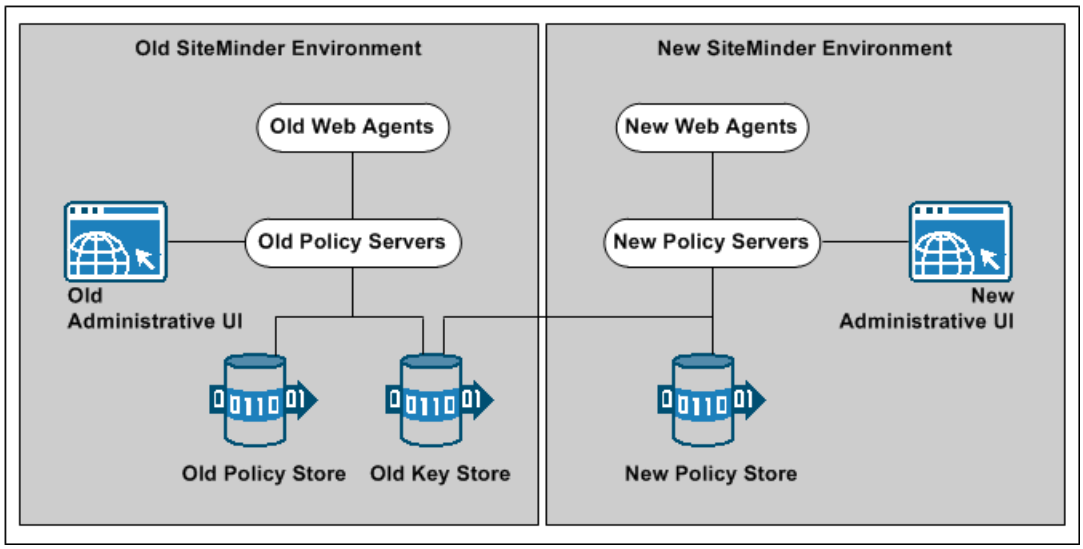
다음 그림에서는 간단한 병렬 업그레이드와 상세 정보를 보여 줍니다.

- r12.x 환경 - 기존 리소스를 계속해서 보호합니다.
- r12.x 관리 UI - r12.x 정책 저장소에서 SiteMinder 개체를 관리하는 데 사용됩니다.
- 12.52 SP1 환경 - 새 리소스를 보호합니다.

- 12.52 SP1 관리 UI - 12.52 SP1 정책 저장소에서 SiteMinder 개체를 관리하는 데 사용됩니다.
- 공통 r12.x 키 저장소. 공용 키 저장소를 사용하여 두 환경 간에서 싱글 사인온을 사용할 수 있습니다.

  참고: 설명에 나와 있지 않지만 다중 키 저장소를 사용하여 두 환경 간에서 싱글 사인온을 사용할 수 있습니다.

그림 12: r12.x 병렬 업그레이드 개요



r12.x 병렬 환경을 구성하는 방법

병렬 환경을 구성하는 절차는 다음과 같습니다.

1. 병렬 환경 키 관리 옵션을 검토하여 싱글 사인온을 구축하는 방법을 결정합니다.
2. 12.52 SP1 환경을 생성합니다.
3. 다음 작업 중 하나를 수행하십시오.
   - 두 환경 모두가 공통 키 저장소 싱글 사인온 요구 사항을 충족하는지 확인합니다.
   - 두 환경 모두가 다중 키 저장소 싱글 사인온 요구 사항을 충족하는지 확인합니다.

4. r12.x 정책 저장소 데이터를 마이그레이션합니다. XPSImport 유틸리티의 12.52 SP1 버전에서 다음 명령을 사용하여 12.52 SP1 의 기본 정책 개체를 12.x 정책 저장소로 가져옵니다.

   ```
   XPSImport smpolicy.xml –npass
   ```

5. r12.x 환경에 smkeydatabase 가 포함된 경우:
   a. 모든 인스턴스를 동기화합니다.
   b. smkeydatabase 의 콘텐츠를 12.52 SP1 인증서 데이터 저장소로 마이그레이션합니다.
6. r12.x 환경에서 레거시 페더레이션(Federation Security Services) 개체를 관리하는 경우 어설션 발급자 ID 를 마이그레이션합니다.
7. 사용자 디렉터리 싱글 사인온 요구 사항을 검토합니다.

추가 정보:

인증서 데이터 관리 (페이지 29)
키 데이터베이스 인스턴스 동기화 (페이지 50)

병렬 환경 키 관리 옵션

병렬 업그레이드에 성공하려면 SiteMinder 키를 관리하여 기존 환경과 12.52 SP1 환경 간의 싱글 사인온을 유지해야 합니다. 두 가지 SiteMinder 키 관리 옵션을 사용할 수 있습니다. 배포 옵션은 두 환경 모두에서 키 저장소를 하나 이상 구현하는 방법에 따라 달라집니다. 옵션에는 다음이 포함됩니다.

- 공용 키 저장소를 사용하는 여러 정책 저장소
- 개별 키 저장소를 사용하는 여러 정책 저장소

공용 키 저장소 배포

모든 정책 서버가 키 롤오버에 대해 단일 키 저장소를 사용할 수 있습니다. 다음 그림을 참조하십시오.

- r12.x 정책 서버는 r12.x 정책 저장소에 연결합니다.
- 12.52 SP1 정책 서버는 12.52 SP1 정책 저장소에 연결합니다.

- 공용 r12.x 키 저장소는 모든 정책 서버에 대한 키 데이터를 유지 관리합니다. 공용 키 저장소를 사용하면 모든 정책 서버에 연결된 에이전트가 키를 공유할 수 있습니다. 키를 공유하면 두 환경 간에서 싱글 사인온을 사용할 수 있습니다.

  중요! r12.x 정책 저장소와 별도로 r12.x 키 저장소를 구성해야 합니다.

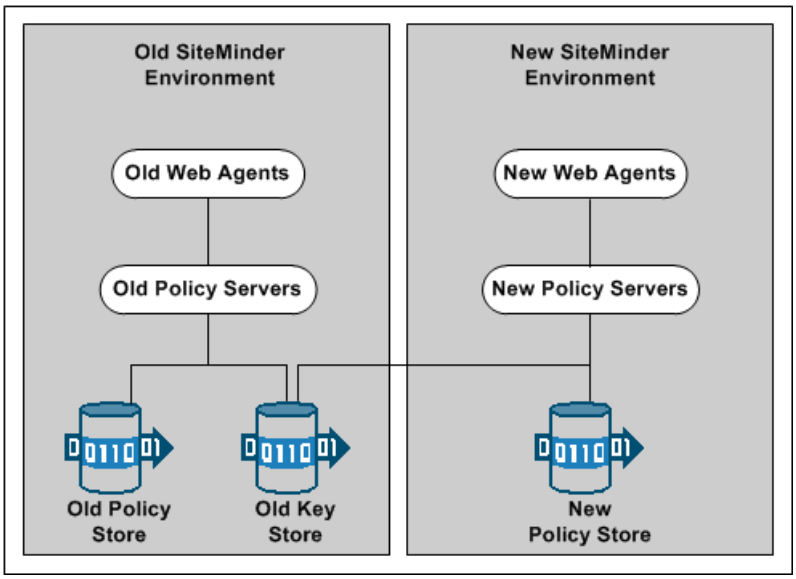
- 모든 정책 서버는 공용 키 저장소에 연결하여 새 키를 검색합니다.

  중요! 12.52 SP1 정책 서버에 r12.x 키 저장소가 구성되어 있어야 합니다. r12.x 정책 서버는 12.52 SP1 키 저장소와 통신할 수 없습니다.

- 모든 웹 에이전트는 해당하는 정책 서버를 폴링하여 새 키를 검색합니다.

참고: 설명에 나와 있지 않지만 장애 조치를 위해 정책 저장소 및 키 저장소 데이터를 복제할 수 있습니다. 데이터베이스 또는 디렉터리 서버 유형에 따라 데이터를 복제하는 방법이 결정됩니다. 마스터/슬레이브 환경의 키 관리에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오. 데이터 복제에 대한 자세한 내용은 공급업체별 설명서를 참조하십시오.

그림 13: r12.x 공용 키 저장소 배포



다중 키 저장소 배포

기존 r12.x 정책 서버는 키 롤오버를 위해 r12.x 키 저장소를 사용하고, 12.52 SP1 정책 서버는 키 롤오버를 위해 12.52 SP1 키 저장소를 사용할 수 있습니다. 다음 그림을 참조하십시오.

- r12.x 정책 서버는 r12.x 정책 저장소에 연결합니다.
- 12.52 SP1 정책 서버는 12.52 SP1 정책 저장소에 연결합니다.
- r12.x 정책 서버는 r12.x 키 저장소에 연결하여 새 키를 검색합니다.
- 12.52 SP1 정책 서버는 12.52 SP1 키 저장소에 연결하여 새 키를 검색합니다.
- SiteMinder 관리자는 관리 UI 를 사용하여 각 키 저장소에 대한 정적 에이전트 및 세션 키를 구성합니다.

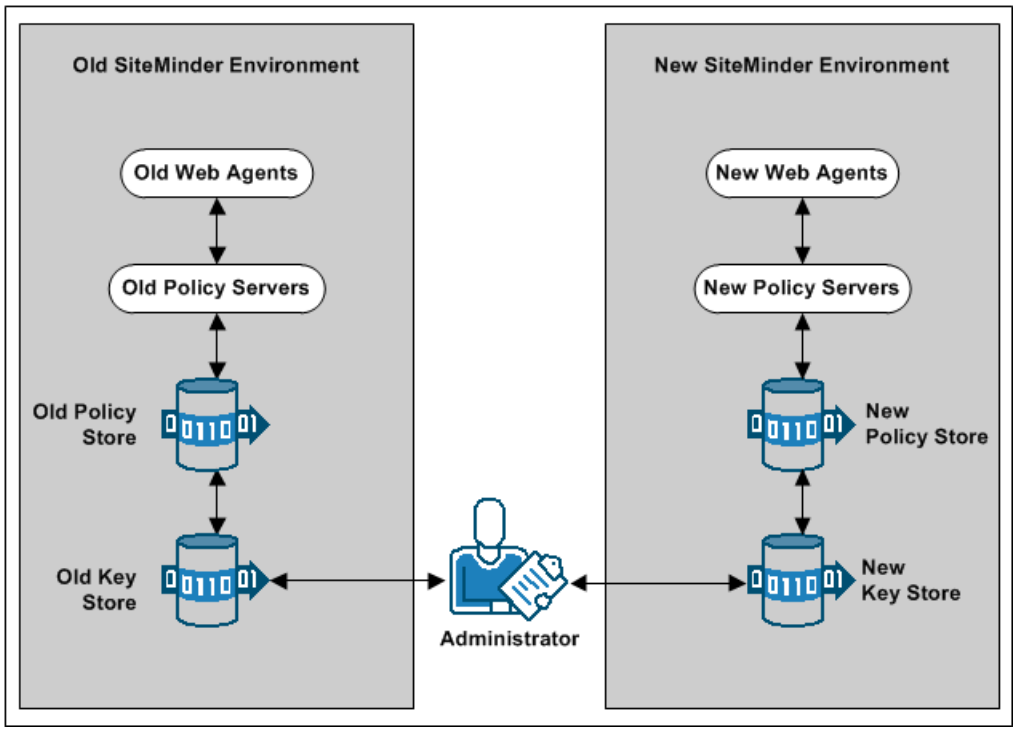
  중요! 모든 키 저장소가 동일한 에이전트 및 세션 키를 사용하지 않으면 싱글 사인온에 실패합니다.

r12.x 웹 에이전트는 해당 r12.x 정책 서버를 폴링하여 새 키를 검색합니다.

- 12.52 SP1 웹 에이전트는 해당하는 12.52 SP1 정책 서버를 폴링하여 새 키를 검색합니다.

참고: 설명에 나와 있지 않지만 장애 조치를 위해 정책 저장소 및 키 저장소 데이터를 복제할 수 있습니다. 데이터베이스 또는 디렉터리 서버 유형에 따라 데이터를 복제하는 방법이 결정됩니다. 마스터/슬레이브 환경의 키 관리에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오. 데이터 복제에 대한 자세한 내용은 공급업체별 설명서를 참조하십시오.

그림 14: r12.x 다중 키 저장소 배포



12.52 SP1 환경 만들기

기존 환경과는 독립적으로 12.52 SP1 환경을 구성할 수 있습니다. 다음 순서로 12.52 SP1 구성 요소를 설치하고 구성하십시오.

1. 정책 서버 하나 이상

   중요! 공통 키 저장소로 싱글 사인온을 유지하는 경우 모든 정책 서버에서 동일한 암호화 키를 사용해야 합니다. 암호화 키 값을 알 수 없는 경우에는 정책 저장소의 r12.x 값을 재설정할 수 있습니다. 12.52 SP1 정책 서버를 설치할 때 새 값을 사용하십시오.

   참고: 정책 저장소 암호화 키의 재설정에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

2. 정책 저장소 하나
3. 관리 UI 하나
4. 웹 에이전트 하나 이상
5. 보고서 서버 하나

참고: 정책 서버, 정책 저장소, 관리 UI 및 보고서 서버 설치에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오. 웹 에이전트 설치에 대한 자세한 내용은 *웹 에이전트 설치 안내서*를 참조하십시오.

공용 키 저장소의 싱글 사인온 요구 사항

공용 키 저장소를 배포하는 경우 다음을 수행하지 않으면 싱글 사인온에 실패합니다.

- r12.x 정책 저장소와 키 저장소가 별도로 구성되어 있는지 확인합니다.
  - r12.x 환경에 별도의 키 저장소가 구성되어 있으면 키 저장소 버전을 r12.x 로 유지합니다. 12.52 SP1 정책 서버는 r12.x 키 저장소와 통신할 수 있지만 r12.x 정책 서버는 12.52 SP1 키 저장소와 통신할 수 없습니다.
  - r12.x 환경에 배치된 정책/키 저장소가 구성되어 있는 경우 r12.x 키를 별도의 r12.x 키 저장소로 분리합니다.
- 키 저장소 버전을 r12.x 로 유지합니다. 12.52 SP1 정책 서버는 r12.x 키 저장소와 통신할 수 있지만 r12.x 정책 서버는 12.52 SP1 키 저장소와 통신할 수 없습니다.
- 모든 정책 서버가 공용 r12.x 키 저장소를 사용하도록 구성합니다.

- 모든 정책 서버가 동일한 암호화 키를 사용하는지 확인합니다. 암호화 키 값을 알 수 없는 경우에는 정책 저장소의 r12.x 값을 재설정할 수 있습니다. 12.52 SP1 정책 서버를 설치할 때 이 새 값을 사용합니다.

  참고: 정책 저장소 암호화 키의 재설정에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

- 동적 에이전트 키를 생성하는 단일 정책 서버를 지정합니다. 나머지 정책 서버에 대한 에이전트 키 생성이 사용되지 않도록 설정합니다.

  참고: 에이전트 키 동적 생성에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

정책 저장소에서 키 저장소를 분리하는 방법

정책 저장소에서 키 저장소를 분리하려면 다음 단계를 수행하십시오.

1. 설정 정책 서버를 설치하거나 찾습니다. 설정 정책 서버는 배치된 정책/키 저장소가 구성되지 않은 정책 서버입니다.
   - 정책 서버에 배치된 저장소가 구성되어 있다면 해당 정책 서버를 새 키 저장소 인스턴스를 구성하는 데 사용할 수 없습니다. 이 경우 정책 서버 호스트 시스템에서 제공되는 필수 SiteMinder 유틸리티가 배치된 저장소를 관리할 수 있도록 구성됩니다.
   - 설정 정책 서버에서는 별도의 필수 유틸리티 집합을 사용할 수 있습니다. 별도의 집합을 사용하면 배치된 저장소에 영향을 주지 않고 키 저장소를 구성할 수 있습니다.
2. 설정 정책 서버 호스트 시스템을 사용하여 별도의 r12.x 키 저장소 인스턴스를 만듭니다. 다음 사항을 고려하십시오.
   - 키 저장소에는 기본 정책 저장소 스키마만 필요합니다. 별도의 키 저장소 구성에 대한 자세한 내용은 r12.0 SP3 *정책 서버 설치 안내서*를 참조하십시오.
   - 키 저장소의 경우 다음을 수행할 필요가 없습니다.
     - SiteMinder 슈퍼 사용자 암호를 설정합니다.
     - 기본 정책 저장소 개체를 가져옵니다.
3. r12.x 환경에서 동적 에이전트 키 생성이 사용되지 않도록 설정합니다.

   참고: 환경에서 정적 키를 사용하는 경우 이 단계가 필요하지 않습니다. 그러나 정책 저장소에서 키를 내보낸 후에는 SiteMinder 관리자가 임의 에이전트 키를 생성하지 않도록 확인해야 합니다.

4. r12.x 정책/키 저장소에서 에이전트 키를 내보냅니다.
5. r12.x 키 저장소로 에이전트 키를 가져옵니다.
6. 모든 정책 서버가 별도의 키 저장소를 사용하도록 구성합니다.
7. 동적 에이전트 키 생성이 사용되지 않도록 설정한 경우 다시 사용하도록 설정합니다.

동적 에이전트 키 생성 사용 안 함

키 저장소 분리를 완료하기 전에는 r12.x 환경이 두 개의 키 저장소를 사용하여 작동합니다.

- 일부 정책 서버는 배치된 정책/키 저장소에 있는 에이전트 키를 사용합니다.
- 일부 정책 서버는 별도의 키 저장소에 있는 에이전트 키를 사용합니다.

별도의 저장소로 키를 내보낸 후 동적 에이전트 키 생성이 사용되지 않도록 설정하면 정책 서버가 키를 생성하는 것을 방지할 수 있습니다. 정책 서버가 키를 생성하지 못하도록 설정하면 모든 저장소에서 키가 동기화되지 않을 때 발생할 수 있는 싱글 사인온 문제를 막을 수 있습니다.

다음 단계를 수행하십시오.

1. r12.x 관리 UI 에 로그인합니다.
2. "관리", "정책 서버"를 차례로 클릭합니다.
3. "키 관리", "에이전트 키 관리"를 차례로 클릭합니다.
4. "정적 에이전트 키 사용" 옵션을 선택합니다.
5. "제출"을 클릭합니다.

   정책 서버가 정적 키를 사용하도록 구성됩니다. 정책 서버가 키를 자동으로 생성하지 않습니다.

에이전트 키 내보내기

배치된 정책/키 저장소에서 키를 내보내 별도의 키 저장소에서 키가 사용되도록 설정할 수 있습니다.

다음 단계를 수행하십시오.

1. r12.x 정책 서버 호스트 시스템에 로그인합니다. 이 정책 서버에 배치된 정책/키 저장소가 구성되어 있는지 확인합니다.
2. 다음 명령을 실행하여 정책 저장소에서 키만 내보냅니다.

   ```
   smkeyexport -dadministrator -wpassword -ofile_name
   ```

   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.

   참고: 이 유틸리티에 대한 자세한 내용은 r12.x *정책 서버 관리 안내서*를 참조하십시오.

   예:

   ```
   smkeyexport -dsuperuser -wpassword -oagentkeys
   ```

   배치된 정책/키 저장소에서 에이전트 키를 내보냈습니다.
3. 에이전트 키가 들어 있는 파일을 설정 정책 서버 호스트 시스템에 복사합니다.

에이전트 키 가져오기

배치된 정책/키 저장소에서 키를 가져와 별도의 키 저장소에서 키가 사용되도록 설정할 수 있습니다.

다음 단계를 수행하십시오.

1. r12.x 단독 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 명령을 실행하여 에이전트 키를 별도의 키 저장소로 가져옵니다.

   ```
   smobjimport -ffile_name -k
   ```

   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.

참고: 이 명령의 모드와 인수에 대한 자세한 내용은 r12.x *정책 서버 관리 안내서*를 참조하십시오.

예:

```
smobjimport -fagentkeys -k
```

에이전트 키를 별도의 키 저장소로 가져옵니다.

모든 정책 서버가 키 저장소를 사용하도록 구성

병렬 환경의 모든 정책 서버가 공용 r12.x 키 저장소를 사용하도록 구성하여 두 환경 간에서 싱글 사인온을 유지합니다.

다음 단계를 수행하십시오.

1. 에이전트 키를 동적으로 생성하도록 지정된 정책 서버를 파악합니다. 가장 마지막에 이 정책 서버에서 키 저장소를 구성합니다.
2. 환경의 다른 모든 정책 서버에 대해 다음 단계를 수행하십시오.
   a. 정책 서버 호스트 시스템에 로그인합니다.
   b. 정책 서버 관리 콘솔을 엽니다.
   c. "데이터" 탭을 클릭합니다.
   d. 데이터베이스 목록에서 키 저장소를 선택하고 "정책 저장소 데이터베이스 사용" 옵션을 해제합니다.
   e. 저장소 목록에서 키 저장소 유형을 선택합니다.
   f. 다음 단계 중 하나를 완료하십시오.
      - (LDAP) "LDAP 키 저장소" 섹션에 필수 연결 정보를 입력합니다.
      - (ODBC) "데이터 원본 정보" 섹션에 데이터 원본 정보를 입력합니다.
   g. 연결을 테스트합니다.
   h. "확인"을 클릭합니다.
   i. 정책 서버를 다시 시작하여 정책 서버가 키 저장소를 사용하도록 구성합니다.
3. 에이전트 키를 생성하도록 지정된 정책 서버가 키 저장소를 사용하도록 구성합니다.

동적 에이전트 키 생성을 사용하도록 다시 설정

동적 에이전트 키 생성이 사용되지 않도록 설정한 경우 에이전트 키를 생성하도록 지정된 정책 서버에서 이 기능을 다시 사용하도록 설정합니다. 환경의 모든 정책 서버가 새 키 저장소를 사용하도록 구성된 후에만 이 절차를 완료하십시오.

다음 단계를 수행하십시오.

1. r12.x 관리 UI 에 로그인합니다.
2. "관리", "정책 서버"를 차례로 클릭합니다.
3. "키 관리", "에이전트 키 관리"를 차례로 클릭합니다.
4. "동적 에이전트 키 사용" 옵션을 선택합니다.
5. "제출"을 클릭합니다.

   지정된 정책 서버가 키를 동적으로 생성하도록 설정됩니다.

정책 저장소에서 키 저장소를 분리하는 데 필요한 태스크를 완료했습니다.

여러 키 저장소의 싱글 사인온 요구 사항

여러 키 저장소를 배포하는 경우 다음을 수행하십시오. 그러지 않으면 싱글 사인온에 실패합니다.

- 모든 정책 서버에 대해 동적 에이전트 키 생성이 사용되지 않도록 설정하십시오.
- r12.x 및 12.52 SP1 키 저장소에 동일한 정적 에이전트 키와 동일한 세션 티켓을 지정하는 데 필요한 관리 UI 권한이 SiteMinder 관리자에게 있는지 확인하십시오.

  참고: 관리자 권한 위임에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.
- r12.x 및 12.52 SP1 키 저장소에 동일한 정적 에이전트 키와 동일한 세션 티켓이 구성되어 있는지 확인하십시오.

  참고: 정적 에이전트 키 및 세션 티켓 구성에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

키 및 인증서 마이그레이션

환경에 하나 이상의 smkeydatabase 가 포함된 경우 해당 내용을 12.52 SP1 인증서 데이터 저장소로 마이그레이션합니다.

다음 단계를 수행하십시오.

1. 모든 r12.x smkeydatabase 가 동기화 (페이지 50)되었는지 확인합니다.
2. r12.x 정책 서버 호스트 시스템에 로그인하고 다음 위치로 이동합니다.

   siteminder_home\config\properties

   siteminder_home

   정책 서버 설치 경로를 지정합니다.
3. 다음 파일을 복사합니다.

   smkeydatabase.properties
4. 12.52 SP1 정책 서버 호스트 시스템에 로그인하고 다음 단계를 완료합니다.
   a. 다음 위치로 이동합니다.

      siteminder_home\config\properties

   b. smkeydatabase 속성 파일의 12.52 SP1 버전의 이름을 다음 값으로 변경합니다.

      newsmkeydatabase.properties

   c. 디렉터리에 r12.x 버전의 속성 파일을 추가합니다.

   d. 12.52 SP1 및 r12.x 속성 파일을 텍스트 편집기에서 엽니다.

   e. r12.x 버전의 데이터베이스 위치 경로를 12.52 SP1 버전의 경로와 일치하도록 편집합니다.

      예:

      r12.x 파일이 다음 경로를 참조합니다.

      DBLocation=C\:/Program Files/netegrity/siteminder/smkeydatabase

      12.52 SP1 파일은 다음 경로를 참조합니다.

      DBLocation=C:/Program Files/CA/siteminder/smkeydatabase

      다음 경로를 참조하도록 r12.x 파일을 업데이트합니다.

      DBLocation=C\:/Program Files/CA/siteminder/smkeydatabase

f. r12.x 속성 파일을 저장하고 12.52 SP1 속성 파일을 닫습니다.

g. 정책 서버 설치 루트에 다음 디렉터리를 생성합니다.

```
smkeydatabase
```

예:

```
C:\Program Files\CA\SiteMinder\smkeydatabase
```

5. r12.x 정책 서버 호스트 시스템으로 돌아가서 smkeydatabase 디렉터리의 내용을 복사합니다.

   참고: 이 디렉터리의 기본 위치는 *siteminder_home* 입니다.

6. 12.52 SP1 정책 서버 호스트 시스템으로 돌아가서 다음 단계를 완료합니다.

   a. r12.x smkeydatabase 디렉터리의 내용을 앞에서 생성한 12.52 SP1 smkeydatabase 디렉터리에 추가합니다.

   b. 다음 마이그레이션 유틸리티를 사용하여 smkeydatabase 를 인증서 데이터 저장소로 마이그레이션합니다.

```
smmigratecds
```

   c. 마이그레이션에 성공하면 smkeydatabase 속성 파일과 smkeydatabase 디렉터리를 제거합니다.

   마이그레이션이 완료되었습니다.

추가 정보:

SiteMinder 키 데이터베이스 수동 마이그레이션 (페이지 177)

어설션 발급자 ID 마이그레이션

r12.x 환경에서 Federation Security Services(레거시 페더레이션) 개체를 관리하는 경우 어설션 발급자 ID 를 r12.x Producer 에서 12.52 SP1 Producer 로 마이그레이션하십시오. ID 를 마이그레이션하면 SAML 1.1 트랜잭션이 서비스 공급자에서 실패하지 않습니다.

다음 단계를 수행하십시오.

1. r12.x 정책 서버 호스트 시스템에 로그인하고 다음 위치로 이동합니다.

   siteminder_home\config\properties

   siteminder_home

   정책 서버 설치 경로를 지정합니다.

2. 다음 파일을 복사합니다.

   AMAssertionGenerator.properties

3. 12.52 SP1 정책 서버 호스트 시스템에 로그인하고 다음 위치로 이동합니다.

   siteminder_home\config\properties

4. 12.52 SP1 버전의 어설션 생성기 속성 파일의 이름을 다음 값으로 변경합니다.

   newAMAssertionGenerator.properties

5. 디렉터리에 r12.x 버전의 속성 파일을 추가합니다.

   마이그레이션이 완료되었습니다.

r12.x 정책 마이그레이션

12.52 SP1 배포를 사용하여 r12.x 리소스를 보호하려는 경우 정책 저장소 데이터를 12.52 SP1 정책 저장소로 마이그레이션하는 것이 좋습니다.

반드시 필요한 것은 아니지만 12.52 SP1 정책 저장소의 관리를 시작하기 전에 정책 저장소 데이터를 마이그레이션하면 중복 개체와 관련된 충돌 가능성을 방지할 수 있습니다.

정책을 마이그레이션하려면

1. r12.x 버전의 XPSExport 유틸리티를 사용하여 r12.x 정책 저장소 데이터를 내보냅니다. r12.x 버전의 XPSExport 에 대한 자세한 내용은 r12.x *정책 서버 관리 안내서*를 참조하십시오.
2. 12.52 SP1 버전의 XPSImport 유틸리티를 사용하여 정책 데이터를 12.52 SP1 정책 저장소로 가져옵니다. 12.52 SP1 버전의 XPSImport 에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

업그레이드나 정책 마이그레이션의 일부로 한 환경의 SiteMinder 정책을 다른 환경으로 이동할 경우 환경과 관련된 일부 개체가 내보내기 파일에 포함됩니다. 이러한 개체에는 다음이 포함됩니다.

- 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.

참고: XPSExport 내보내기 모드에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

사용자 디렉터리 싱글 사인온 요구 사항

두 환경 모두에서 생성한 SiteMinder 사용자 디렉터리 개체의 이름이 동일한지 확인하십시오. 다른 이름을 사용하여 r12.x 및 12.52 SP1 정책 서버를 동일한 사용자 저장소에 연결할 경우 싱글 사인온에 실패합니다.

제 4 장: FIPS 호환 알고리즘 사용

이 섹션은 다음 항목을 포함하고 있습니다.

FIPS 140-2 마이그레이션 개요

정책 서버는 인증된 FIPS(Federal Information Processing Standard) 140-2 호환 암호화 라이브러리를 사용합니다. FIPS 는 AES(Advanced Encryption Standard)를 충족하는 암호화 모듈을 인가하는 데 사용되는 미국 정부의 컴퓨터 보안 표준입니다. 이러한 라이브러리는 SiteMinder 환경에서 중요한 데이터를 암호화하는 데 FIPS 호환 알고리즘만 사용하는 경우 FIPS 작동 모드를 제공합니다. SiteMinder 환경은 다음과 같은 FIPS 작동 모드 중 하나에서 작동할 수 있습니다.

- FIPS 호환성
- FIPS 마이그레이션
- FIPS 전용

기본적으로 12.52 SP1 버전으로 업그레이드된 환경은 FIPS 호환성 모드에서 작동합니다. 이 환경은 FIPS 호환성 모드에서 이전 버전 SiteMinder 의 기존 알고리즘을 사용하여 중요한 데이터를 암호화하며 이전 버전의 SiteMinder 와 호환됩니다. 조직에서 FIPS 호환 알고리즘을 사용할 필요가 없는 경우 이 환경은 추가 구성 없이 FIPS 호환성 모드에서 작동할 수 있습니다.

FIPS 호환 알고리즘만 사용하도록 환경을 마이그레이션하는 과정은 두 단계로 이루어집니다.

1. **기존의 중요한 데이터 다시 암호화** - 1 단계에서는 FIPS 마이그레이션 모드에서 작동하도록 환경을 구성합니다. FIPS 마이그레이션 모드에서는 FIPS 호환성 모드에서 실행 중인 12.52 SP1 환경을 FIPS 전용 모드로 전환할 수 있습니다. FIPS 마이그레이션 모드의 12.52 SP1 환경에서는 FIPS 호환 알고리즘을 사용하여 기존의 중요한 데이터를 다시 암호화할 때 기존 SiteMinder 암호화 알고리즘이 계속 사용됩니다.
2. **FIPS 전용 모드 구성** - 2 단계에서는 FIPS 전용 모드에서 작동하도록 환경을 구성합니다. FIPS 전용 모드의 환경에서는 중요한 데이터를 암호화하는 데 FIPS 호환 알고리즘만 사용합니다.

   중요! FIPS 전용 모드에서 실행 중인 환경은 다음을 포함하여 12.x 이전의 SiteMinder 버전과 상호 운용될 수 없으며 호환되지도 않습니다.

   - 모든 에이전트
   - 이전 버전의 에이전트 API 를 사용하는 사용자 지정 소프트웨어
   - PM API 를 사용하거나 정책 서버가 노출하는 다른 API 를 사용하는 사용자 지정 소프트웨어

   FIPS 전용 모드에 필요한 지원을 받으려면 이러한 모든 소프트웨어를 해당하는 SDK 의 12.52 SP1 버전과 다시 연결하십시오.

FIPS 140-2 마이그레이션 요구 사항

FIPS 호환 알고리즘만 사용하도록 환경을 마이그레이션하기 전에 사용 환경이 최소 요구 사항을 충족하는지 확인하십시오. 다음 내용을 인쇄하여 검사 목록으로 사용할 수도 있습니다.

- ☐ SDK 를 포함한 전체 SiteMinder 환경이 12.52 SP1 로 업그레이드되었는지 확인하십시오.
- ☐ 환경에 사용자 지정 에이전트가 포함되어 있는 경우 해당 에이전트가 각 SDK 에 다시 연결되었는지 확인하십시오.

  참고: 사용자 지정 에이전트를 다시 연결하는 방법에 대한 자세한 내용은 *API Reference Guide for C*(C 용 API 참조 안내서) 및 *API Reference Guide for Java*(Java 용 API 참조 안내서)를 참조하십시오.

- ☐ 환경에서 적어도 하나의 정책 서버가 에이전트 키 생성을 사용하도록 구성되어 있는지 확인하십시오.

  참고: 에이전트 키 생성이 사용되도록 설정하는 방법에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

- ☐ 환경에서 X.509 클라이언트 인증서 인증 체계를 사용하는 경우 사용자 인증서가 FIPS 호환 알고리즘만 사용하여 생성되는지 확인하십시오.
- ☐ 정책 서버가 SSL 을 통해 정책 저장소 및/또는 사용자 저장소에 연결되는 경우 정책 서버 및 디렉터리 저장소에서 연결에 사용되는 인증서가 FIPS 호환 인증서인지 확인하십시오.

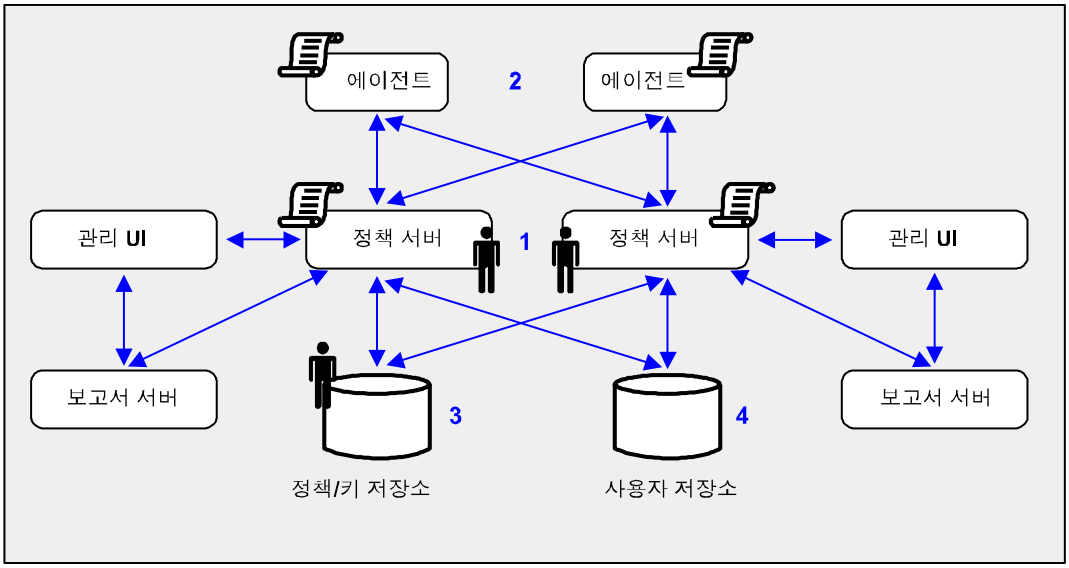
마이그레이션 로드맵 - 중요한 데이터 다시 암호화

FIPS 전용 모드에서 작동하는 환경을 설정하려면 먼저 다음을 수행해야 합니다.

- FIPS 마이그레이션 모드에서 작동하는 특정 구성 요소를 설정합니다.
- FIPS 호환 알고리즘을 사용하여 기존 중요한 데이터를 다시 암호화합니다.

다음 그림에서는 예제 12.52 SP1 환경 및 다음과 같은 상세 정보를 보여 줍니다.

- FIPS 마이그레이션 모드에서 작동하도록 구성 요소를 구성하는 순서.
- 다시 암호화해야 하는 기존 중요한 데이터.



1. 환경의 각 정책 서버는 FIPS 마이그레이션 모드에서 작동하도록 설정됩니다.

   - 정책 저장소 키는 FIPS 와 호환되지 않는 알고리즘을 사용하여 암호화됩니다. 환경을 FIPS 전용 모드로 구성하기 전에 환경의 각 정책 서버에 대해 이 키를 다시 암호화합니다. 정책 저장소 키는 EncryptionKey.txt 파일에 있습니다.
   - 정책 저장소 관리자 암호는 FIPS 와 호환되지 않는 알고리즘을 사용하여 암호화됩니다. 환경을 FIPS 전용 모드로 구성하기 전에 이 암호를 다시 암호화합니다.

     중요! 키 저장소, 감사 로그, 토큰 데이터 또는 세션 저장소에 대해 별도의 데이터베이스를 구성한 경우 이러한 암호는 FIPS 와 호환되지 않는 알고리즘을 사용하여 암호화됩니다. 환경을 FIPS 전용 모드로 구성하기 전에 이러한 암호를 다시 암호화합니다.
   - SiteMinder 슈퍼 사용자 암호는 FIPS 와 호환되지 않는 알고리즘을 사용하여 암호화됩니다. 환경을 FIPS 전용 모드로 구성하기 전에 이 암호를 다시 암호화합니다.

     참고: 이 암호는 기본 SiteMinder 관리자 계정의 암호입니다. 관리 UI 에 직접 액세스할 필요가 없는 모든 관리 태스크에 이 계정이 사용됩니다. 암호는 슈퍼 사용자 권한이 있는 관리 UI 관리자 계정의 암호가 아닙니다.

2. 사용자 지정 에이전트를 비롯한 환경의 각 SiteMinder 에이전트는 FIPS 마이그레이션 모드에서 작동하도록 설정됩니다.

   정책 서버 및 에이전트가 암호화된 통신 채널을 설정하기 위해 사용하는 공유 암호는 FIPS 와 호환되지 않는 알고리즘을 사용하여 암호화됩니다. 환경을 FIPS 전용 모드로 구성하기 전에 공유 암호를 다시 암호화합니다.

3. 키 및 중요 정책 저장소 데이터는 다시 암호화됩니다.

   참고: 이전 그림의 단일 데이터베이스 인스턴스는 정책/키 저장소를 나타냅니다. 환경에서 개별 정책 및 키 저장소에 대해 별도의 데이터베이스를 사용할 수 있습니다.

   정책 저장소 또는 정책 및 키 저장소에 저장된 중요한 데이터는 FIPS 와 호환되지 않는 알고리즘을 사용하여 암호화됩니다. 환경을 FIPS 전용 모드로 구성하기 전에 키 및 중요 정책 저장소 데이터를 다시 암호화합니다.

4. (선택 사항) 환경에서 기본 암호 서비스를 사용하는 경우 해당 사용자가 인증을 시도할 때 FIPS 마이그레이션 모드에서 작동하는 정책 서버가 각 암호 Blob 을 FIPS 호환 알고리즘으로 다시 암호화합니다. 사용자의 암호 기록이 손실되고 사용자가 잠기는 일을 방지하려면 정책 서버가 다시 암호화하지 않은 암호 Blob 을 확인하여 해당 사용자에게 로그인하거나 암호를 변경하도록 알리십시오.

   참고: 암호 정책의 구성 방식에 따라 정책 서버에서 암호 Blob 을 다시 암호화하는 시기가 결정됩니다.

   - 암호 정책이 성공하거나 실패한 로그인을 추적하도록 구성된 경우 정책 서버에서는 사용자가 로그인할 때 암호 Blob 을 다시 암호화합니다.
   - 암호 정책이 로그인을 추적하도록 구성되지 않은 경우 정책 서버에서는 사용자가 암호를 변경할 때 암호 Blob 을 다시 암호화합니다.

기존의 중요한 데이터를 다시 암호화하는 방법

FIPS 호환 알고리즘을 사용하여 기존의 중요한 데이터를 다시 암호화하려면 다음 절차를 완료하십시오.

1. 환경 정보를 수집합니다.
2. 모든 정책 서버에 대해 FIPS 마이그레이션 모드를 설정합니다.
3. 정책 저장소 키를 다시 암호화합니다.
4. 정책 저장소 관리자 암호를 다시 암호화합니다.
5. SiteMinder 슈퍼 사용자 암호를 다시 암호화합니다.
6. 모든 에이전트에 대해 FIPS 마이그레이션 모드를 설정합니다.
7. 정책 및 키 저장소 데이터를 다시 암호화합니다.
8. (선택 사항) 사용 환경에서 기본 암호 서비스를 사용하는 경우 암호 Blob 이 다시 암호화되었는지 확인합니다.

환경 정보 수집

정책 서버가 FIPS 마이그레이션 모드에서 작동 중일 때 기존의 중요한 데이터를 다시 암호화하려면 특정 환경 정보가 필요합니다.

- **정책 저장소 키** - 환경의 각 정책 서버에 대해 EncryptionKey.txt 파일의 정책 저장소 암호화 키를 복사한 후 복사 가능한 단일 위치에 저장합니다. EncryptionKey.txt 파일은 *policy_server_home*\bin 에 있습니다.

  policy_server_home

  정책 서버 설치 경로를 지정합니다.

- **슈퍼 사용자 계정 이름 및 암호** - 슈퍼 사용자 계정의 이름과 암호를 식별합니다. SiteMinder 도구를 사용하여 데이터를 다시 암호화하려면 이 정보가 필요합니다.

  참고: 이 계정은 관리 UI 에 직접 액세스할 필요가 없는 모든 관리 태스크에 사용되는 계정입니다. 이러한 정보는 슈퍼 사용자 권한이 있는 관리 UI 관리자 계정의 자격 증명이 아닙니다.

- **정책 저장소 관리자 암호** - 정책 저장소 관리자 암호를 식별합니다. 이 암호는 정책 저장소와 정책 서버 간의 연결을 구성할 때 지정한 암호입니다.

정책 서버를 FIPS 마이그레이션 모드로 설정

FIPS 호환 알고리즘을 사용하여 기존 중요한 데이터를 다시 암호화할 때 환경에서 기존 SiteMinder 암호화 알고리즘을 계속 사용할 수 있도록 정책 서버를 FIPS 마이그레이션 모드로 설정하십시오.

다음 단계를 수행하십시오.

1. 정책 서버를 호스팅하는 컴퓨터에서 명령 프롬프트를 열고 다음 명령을 실행합니다.

   ```
   setFIPSmigration
   ```

   명령 창에 MIGRATION 가 나타납니다.

2. 정책 서버를 중지합니다.

   참고: 정책 서버 중지 및 시작에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

3. 다음 단계 중 하나를 완료하십시오.
   - 정책 서버가 Windows 시스템에 설치되어 있는 경우 시스템을 재부팅합니다.
   - 정책 서버가 UNIX 시스템에 설치되어 있는 경우 다음 단계를 완료합니다.
     a. 정책 서버를 시작할 때 사용한 사용자로 로그인합니다.
     b. 명령 프롬프트를 엽니다.
     c. *policy_server_home* 으로 이동합니다.
     d. 다음 명령을 실행합니다.

     ```
     . ./ca_ps_env.ksh
     ```
4. 정책 서버를 시작합니다.
5. smps.log 파일을 열고 다음 행이 표시되는지 확인합니다.

   ```
   Policy Server migrating from classic SiteMinder to FIPS-140 cryptographic algorithms.
   ```
6. 로그 파일을 닫습니다.

   정책 서버가 FIPS 마이그레이션 모드에서 작동하도록 설정됩니다.
7. 환경의 각 정책 서버에 대해 이전 단계를 반복합니다.

이제 환경의 각 정책 서버에 대해 정책 저장소 키를 다시 암호화할 수 있습니다.

정책 저장소 키 다시 암호화

기존 키를 FIPS 호환 알고리즘을 사용하여 암호화된 버전으로 바꾸려면 정책 저장소 키를 다시 암호화합니다.

정책 저장소 키를 다시 암호화하려면

1. 정책 서버를 호스트하는 컴퓨터에서 명령 프롬프트를 열고 다음 명령을 실행합니다.

   ```
   smreg -cf MIGRATE -key key_value
   ```

   -cf MIGRATE

   smreg 가 FIPS 마이그레이션 모드에서 실행되도록 지정합니다.

   참고: smreg 가 FIPS 마이그레이션 모드에서 실행되면 정책 저장소 키가 FIPS 호환 알고리즘을 사용하여 다시 생성됩니다.

-key *key value*

현재 정책 저장소 키를 지정합니다.

smreg 는 새 정책 저장소 키를 생성하고 FIPS 호환 알고리즘을 사용하여 해당 키를 암호화합니다.

2. EncryptionKey.txt 파일을 연 다음, 새 암호화 키가 있고 FIPS 호환 알고리즘이 접두사로 추가되어 있는지 확인합니다.

   접두사 예: {AES}

   정책 저장소 키가 다시 암호화됩니다.

3. 환경의 각 정책 서버에 대해 후반 단계를 반복합니다.

이제 정책 저장소 관리자 암호를 다시 암호화할 수 있습니다.

정책 저장소 관리자 암호 다시 암호화

데이터가 FIPS 호환 알고리즘을 사용하여 암호화되도록 정책 저장소 관리자 암호를 다시 암호화합니다.

다음 단계를 수행하십시오.

1. 정책 서버 관리 콘솔을 시작하고 "데이터" 탭을 클릭합니다.

   참고: 정책 서버 관리 콘솔 시작에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

2. "암호" 필드에 관리자 암호를 다시 입력하고 "적용"을 클릭합니다.

   관리자 암호가 FIPS 호환 알고리즘을 사용하여 암호화됩니다.

3. (선택 사항) 다음 저장소 중 하나 이상에 대해 별도의 데이터베이스를 구성한 경우 해당 관리자 암호를 다시 암호화하십시오.

   - 키 저장소
   - 감사 로그
   - 토큰 데이터
   - 세션 저장소

   중요! FIPS 전용 모드에서 작동하는 정책 서버는 FIPS 와 호환되지 않는 알고리즘을 사용하여 암호화된 상태로 유지된 데이터베이스 암호를 암호 해독할 수 없습니다.

이제 SiteMinder 슈퍼 사용자 암호를 다시 암호화할 수 있습니다.

SiteMinder 슈퍼 사용자 암호 다시 암호화

SiteMinder 슈퍼 사용자 암호를 다시 암호화하면 데이터가 FIPS 호환 알고리즘을 사용하여 암호화됩니다.

참고: 이 암호는 기본 관리자 계정의 암호입니다. 이 계정은 관리 UI 에 직접 액세스할 필요가 없는 모든 관리 태스크에 사용됩니다. 이 암호는 슈퍼 사용자 권한이 있는 관리 UI 관리자 계정의 암호가 아닙니다.

SiteMinder 슈퍼 사용자 암호를 재설정하려면 명령 프롬프트를 열고 다음 명령을 실행하십시오.

```
smreg -cf MIGRATE -su password
```

-cf MIGRATE

smreg 가 FIPS 마이그레이션 모드에서 실행되도록 지정합니다.

참고: smreg 가 FIPS 마이그레이션 모드에서 실행되면 기존 슈퍼 사용자 암호가 FIPS 호환 알고리즘을 사용하여 저장됩니다.

암호

기존 슈퍼 사용자 암호를 지정합니다.

참고: 새 암호를 지정할 필요가 없습니다. 동일한 암호를 입력하면 FIPS 호환 알고리즘을 사용하여 데이터가 암호화됩니다.

SiteMinder 슈퍼 사용자 암호가 FIPS 호환 알고리즘을 사용하여 암호화됩니다.

이제 환경의 각 에이전트를 FIPS 마이그레이션 모드로 설정할 수 있습니다.

에이전트를 FIPS 마이그레이션 모드로 설정

FIPS 호환 알고리즘을 사용하여 중요한 데이터를 다시 암호화할 때 환경에서 기존 SiteMinder 암호화 알고리즘을 계속 사용할 수 있도록 에이전트를 FIPS 마이그레이션 모드로 설정하십시오.

에이전트의 FIPS 모드를 변경하려면

1. 텍스트 편집기에서 SmHost.conf 파일을 엽니다.

   이 파일에는 다음 줄이 표시됩니다.

   ```
   fipsmode="COMPAT"
   ```

2. 이 행을 다음과 같이 편집합니다.

   ```
   fipsmode="MIGRATE"
   ```

3. 파일을 저장한 후 닫습니다.
4. 에이전트를 호스트하는 컴퓨터를 다시 시작합니다.

   에이전트가 FIPS 마이그레이션 모드에서 작동합니다.

5. 트러스트된 호스트가 등록된 환경의 각 컴퓨터에 대해 이전 단계를 반복합니다.

이제 에이전트 공유 암호를 암호화할 수 있습니다.

클라이언트 공유 암호 다시 암호화

에이전트 공유 암호를 다시 암호화하면 기존 암호가 FIPS 호환 알고리즘을 사용하여 암호화된 암호로 바뀝니다. 다음 중 한 가지 방법으로 공유 암호를 다시 암호화합니다.

- 관리 UI 에서 수동으로 공유 암호 롤오버
- FIPS 마이그레이션 모드에서 smreghost 사용

  참고: 트러스트된 호스트를 등록할 때 에이전트에 공유 암호 롤오버를 구성하지 않은 경우에는 smreghost 만 사용해야 합니다.

관리 UI 를 사용하여 공유 암호 다시 암호화

관리 UI 에서 공유 암호를 롤오버하려면

1. 관리 UI 에 로그인하고 "관리", "정책 서버", "공유 암호 롤오버"를 차례로 클릭합니다.

   "공유 암호 롤오버" 창이 나타납니다.

2. "다음마다 공유 암호 롤오버" 라디오 단추를 선택합니다.

   "지금 롤오버"가 활성화됩니다.

3. "지금 롤오버"를 클릭합니다.

   공유 암호 롤오버를 허용하도록 구성된 모든 트러스트된 호스트의 공유 암호가 롤오버됩니다.

이제 정책 저장소에 있는 중요한 정책 및 키 데이터를 다시 암호화할 수 있습니다.

smreghost 를 사용하여 공유 암호 다시 암호화

smreghost 를 사용하여 공유 암호를 다시 암호화하려면

1. 명령 프롬프트를 열고 다음 명령을 실행합니다.

   ```
   smreghost -i policy_server_ip_address -u administrator_user_name
   -p administrator_password -hn hostname_for_registration -hc host_config_object
   -f path_to_host_config_file -o -cf MIGRATE
   ```

   -i *policy server ip address*

   트러스트된 호스트를 등록할 정책 서버의 IP 주소를 지정합니다.

   -u *administrator user name*

   트러스트된 호스트를 등록할 수 있는 권한이 있는 SiteMinder 관리자의 이름을 지정합니다.

   - p *administrator password*

   트러스트된 호스트를 등록할 수 있는 관리자의 암호를 지정합니다.

   -hn *hostname for registration*

   등록된 호스트의 현재 이름을 지정합니다.

   -hc *host configuration object*

   정책 서버에 구성된 호스트 구성 개체를 지정합니다.

-f *path to host config file*

등록 데이터가 들어 있는 파일의 전체 경로를 지정합니다. 기본 파일 이름은 SmHost.conf 입니다.

참고: 파일 경로를 지정하지 않으면 업데이트된 파일이 smreghost 를 실행 중인 위치에 저장됩니다.

-o

기존의 트러스트된 호스트를 덮어씁니다. 이 인수를 사용하지 않을 경우 사용자가 관리 UI 를 사용하여 기존의 트러스트된 호스트를 삭제해야 합니다. 이 인수와 함께 smreghost 를 사용하는 것이 좋습니다.

-cf MIGRATE

smreghost 가 FIPS 마이그레이션 모드에서 실행되도록 지정합니다.

참고: smreghost 가 FIPS 마이그레이션 모드에서 실행되면 공유 암호가 FIPS 호환 알고리즘을 사용하여 생성되고 암호화됩니다.

smreghost 는 트러스트된 호스트를 다시 등록하고 FIPS 승인 알고리즘을 사용하여 암호화된 새 공유 암호가 생성됩니다.

2. 트러스트된 호스트 등록 데이터가 들어 있는 파일을 연 다음, 새 공유 암호가 있고 FIPS 승인 알고리즘이 접두사로 추가되어 있는지 확인합니다.

   공유 암호가 FIPS 호환 알고리즘을 사용하여 암호화됩니다.

   접두사 예: {AES}

이제 정책 저장소에 있는 중요한 정책 및 키 데이터를 다시 암호화할 수 있습니다.

정책 및 키 저장소 데이터 다시 암호화

기존 SiteMinder 알고리즘으로 암호화된 중요한 데이터가 FIPS 호환 알고리즘으로 암호화되도록 하려면 정책 및 키 저장소 데이터를 다시 암호화합니다.

정책 및 키 저장소 데이터를 다시 암호화하기 위한 옵션

다음 세 가지 방법으로 정책 및 키 저장소 데이터를 다시 암호화할 수 다음을 수행할 수 있습니다.

- 기존 정책 저장소의 정책 및 키 저장소 데이터를 다시 암호화합니다.
- 기존 정책 저장소의 정책 데이터와 기존 키 저장소의 키 데이터를 다시 암호화합니다.
- 정책 및 키 저장소 데이터를 다시 암호화하고 해당 데이터를 각각 새 12.52 SP1 정책 저장소나 정책 및 키 저장소로 마이그레이션합니다.

이 안내서에서는 기존 저장소의 정책 및 키 저장소 데이터를 다시 암호화하는 단계를 자세히 설명합니다.

새 12.52 SP1 정책 저장소나 정책 및 키 저장소를 생성하려면 다음과 같이 하십시오.

1. smkeyexport 를 사용하여 키 데이터를 내보냅니다.

   참고: XPSExport 로는 정책 또는 키 저장소에 저장된 키를 내보낼 수 없습니다. smkeyexport 사용에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

2. XPSExport 를 사용하여 정책 저장소 데이터를 내보냅니다.

   참고: XPSExport 사용에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

3. 12.52 SP1 정책 저장소나 정책 및 키 저장소를 생성합니다.

   참고: 정책 및 키 저장소 생성에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

4. smkeyimport 를 사용하여 키 데이터를 새 정책 저장소나 새 키 저장소(생성한 경우)로 가져옵니다.

   참고: smkeyimport 사용에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

5. XPSImport 를 사용하여 정책 저장소 데이터를 새 정책 저장소로 가져옵니다.

   참고: XPSImport 사용에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

정책 또는 키 저장소에 저장된 키 다시 암호화

정책 또는 키 저장소에 저장된 키를 다시 암호화하여 기존 키를 FIPS 호환 알고리즘으로 암호화된 버전으로 바꿀 수 있습니다.

정책 또는 키 저장소에 저장된 키를 다시 암호화하려면

1. 정책 서버를 호스트하는 컴퓨터에서 명령 프롬프트를 열고 다음 명령을 실행합니다.

   ```
   smkeyexport -dadmin_name -wadmin_password -ooutput_file_name -l -v -t -cf
   ```

   -d*admin_name*

   SiteMinder 관리자 계정의 이름을 지정합니다.

   -w*admin_password*

   SiteMinder 관리자 계정의 암호를 지정합니다.

   -o*output_file_name*

   (선택 사항) 내보낸 파일의 이름을 지정합니다. 파일 이름을 지정하지 않으면 기본 파일 이름인 stdout.smdif 로 지정됩니다.

   참고: 파일 이름에는 .smdif 확장명을 포함해야 합니다.

   예: pskeys.smdif

   -l

   로그 파일을 생성하도록 지정합니다.

   -v

   (선택 사항) 문제 해결을 위한 세부 정보 표시 모드가 사용되도록 설정합니다.

   -t

   (선택 사항) 문제 해결을 위한 추적이 사용되도록 설정합니다.

-cf

smkeyexport 가 FIPS 마이그레이션 모드에서 실행되도록 지정합니다.

참고: smkeyexport 가 FIPS 마이그레이션 모드에서 실행되면 정책 저장소에 저장된 키가 FIPS 호환 알고리즘을 사용하여 내보내지고 다시 암호화됩니다.

smkeyexport 는 다시 암호화된 키가 들어 있는 smdif 파일을 내보냅니다.

2. 다음 명령을 실행합니다.

```
smkeyimport -iinput_file_name -dadmin_name -wadmin_password -l -v -t -cf
```

-iinput_file_name

생성한 출력 파일의 이름을 지정합니다.

참고: 지정하는 파일 이름에는 .smdif 확장명을 포함해야 합니다.

-dadmin_name

SiteMinder 관리자 계정의 이름을 지정합니다.

-wadmin_password

SiteMinder 관리자 계정의 암호를 지정합니다.

-l

로그 파일을 생성하도록 지정합니다.

-v

(선택 사항) 문제 해결을 위한 세부 정보 표시 모드가 사용되도록 설정합니다.

-t

(선택 사항) 문제 해결을 위한 추적이 사용되도록 설정합니다.

-cf

smkeyimport 가 FIPS 마이그레이션 모드에서 실행되도록 지정합니다.

smkeyimport 는 다시 암호화된 키를 해당 저장소로 가져옵니다.

이제 정책 저장소 데이터를 다시 암호화할 수 있습니다.

정책 저장소 데이터 다시 암호화

정책 저장소 데이터를 다시 암호화하려면

1. 정책 서버를 호스팅하는 시스템에서 명령 프롬프트를 열고 정책 저장소 데이터 파일을 내보낼 위치로 이동합니다.
2. 다음 명령을 실행합니다.

   ```
   XPSExport outputfile -xe -xp -pass <passphrase> -vT -vI -vW -vE -vF -e file_name
   -l log_file
   ```

   참고: XPSExport 를 사용하여 하나 이상의 세부 개체를 내보낼 수 있지만 이 절차에서는 모든 정책 저장소 데이터를 내보내는 인수를 제공합니다. 이 인수를 사용하면 내보내기에 모든 중요한 데이터가 포함됩니다. 하나 이상의 세부 개체 내보내기에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

   outputfile

   XML 출력 파일의 이름을 지정합니다.

   참고: 파일 이름이 고유해야 합니다. 같은 이름의 파일이 존재하면 내보내기에 실패합니다.

   예: psdata

   -xe

   실행 환경과 관련된 개체 유형을 내보냅니다.

   -xp

   정책과 관련된 개체 유형을 내보냅니다.

   -pass <passphrase>

   중요한 데이터 암호화에 필요한 암호를 지정합니다. 중요한 데이터를 정책 저장소로 다시 가져올 때 필요하므로 이 값을 기록해 두십시오.

   제한: 암호는 다음을 포함해야 합니다.

   - 8 자 이상의 문자
   - 숫자 하나(1)
   - 대문자 하나(1)
   - 소문자 하나(1)

   참고: 암호에 공백이 포함된 경우 암호를 큰따옴표(")로 묶으십시오.

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(치명적 오류)로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(치명적 오류)로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)(기본값)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(치명적 오류)로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(치명적 오류)로 설정합니다.

-l *log_path*

(선택 사항) 지정된 경로에 로그를 출력합니다.

-e *file_name*

(선택 사항) 오류 및 예외가 로깅되는 파일을 지정합니다. 생략할 경우 stderr 가 사용됩니다.

XPSExport 는 정책 저장소 데이터를 내보내고 도구를 실행한 디렉터리에 데이터 파일을 저장합니다.

3. 다음 명령을 실행합니다.

```
XPSImport input_file -pass <passphrase> -vT -vI -vW -vE -vF -l log_path
```

input_file

입력 XML 파일을 지정합니다.

-pass <passphrase>

중요한 데이터 암호 해독에 필요한 암호를 지정합니다.

제한: 암호는 내보내기 중에 지정한 암호와 일치해야 합니다. 그렇지 않으면 암호 해독에 실패합니다.

-vT

(선택 사항) 세부 정보 표시 수준을 "TRACE"(치명적 오류)로 설정합니다.

-vI

(선택 사항) 세부 정보 표시 수준을 "INFO"(치명적 오류)로 설정합니다.

-vW

(선택 사항) 세부 정보 표시 수준을 "WARNING"(경고)(기본값)으로 설정합니다.

-vE

(선택 사항) 세부 정보 표시 수준을 "ERROR"(치명적 오류)로 설정합니다.

-vF

(선택 사항) 세부 정보 표시 수준을 "FATAL"(치명적 오류)로 설정합니다.

-l *log_path*

(선택 사항) 지정된 경로에 로그를 출력합니다.

-e *file_name*

(선택 사항) 오류 및 예외가 로깅되는 파일을 지정합니다. 생략할 경우 stderr 가 사용됩니다.

XPSImport 는 정책 저장소로 데이터를 가져옵니다. 중요한 데이터는 FIPS 호환 알고리즘을 사용하여 암호화됩니다.

환경에서 기본 암호 서비스를 사용하는 경우 이제 암호 Blob 이 FIPS 승인 알고리즘을 사용하여 다시 암호화되었는지 확인할 수 있습니다.

암호 Blob 이 다시 암호화되었는지 확인

사용자가 암호 기록을 손실하고 암호 서비스에 의해 잠기지 않도록 정책 서버에서 사용자 저장소의 모든 암호 Blob 을 다시 암호화했는지 확인해야 합니다.

암호 정책에 대한 사용자 저장소 연결을 구성할 때 암호 데이터 사용자 프로필 특성을 지정한 상태입니다. 이 값은 암호 Blob 이 사용자 저장소에 저장되는 위치를 나타내며, 다시 암호화되지 않은 암호 Blob 을 식별하는 데 사용됩니다.

암호 Blob 이 다시 암호화되었는지 확인하려면

1. 디렉터리 서버 또는 데이터베이스 관련 도구를 사용하여 다음과 같은 접두사가 없는 암호 데이터 항목을 검색합니다.

   {AES}

   예: 사용자 저장소 연결을 구성할 때 "암호 데이터" 필드 값으로 "audio"를 지정한 경우 {AES} 접두사가 없는 "audio"에 저장된 모든 항목을 검색합니다.

2. 암호 Blob 에 {AES} 접두사가 없는 사용자를 확인합니다. 이러한 암호 Blob 은 정책 서버에서 다시 암호화하지 않은 것입니다.

3. 해당 사용자에게 로그인하거나 암호를 변경해야 한다는 것을 알려 줍니다.

   참고: 암호 정책의 구성 방식에 따라 정책 서버에서 암호 Blob 을 다시 암호화하는 시기가 결정됩니다.

   - 암호 정책이 성공하거나 실패한 로그인을 추적하도록 구성된 경우 정책 서버에서는 사용자가 로그인할 때 암호 Blob 을 다시 암호화합니다.
   - 암호 정책이 로그인을 추적하도록 구성되지 않은 경우 정책 서버에서는 사용자가 암호를 변경할 때 암호 Blob 을 다시 암호화합니다.

중요! 정책 서버가 FIPS 전용 모드에서 작동할 때 암호 서비스는 암호 Blob 이 다시 암호화되지 않은 사용자를 잠급니다. 관리자가 암호 Blob 을 삭제하고 비활성화된 모든 플래그를 지울 때까지 사용자는 액세스 권한을 다시 얻을 수 없습니다. 암호 Blob 을 삭제하면 사용자의 암호 기록이 손실됩니다.

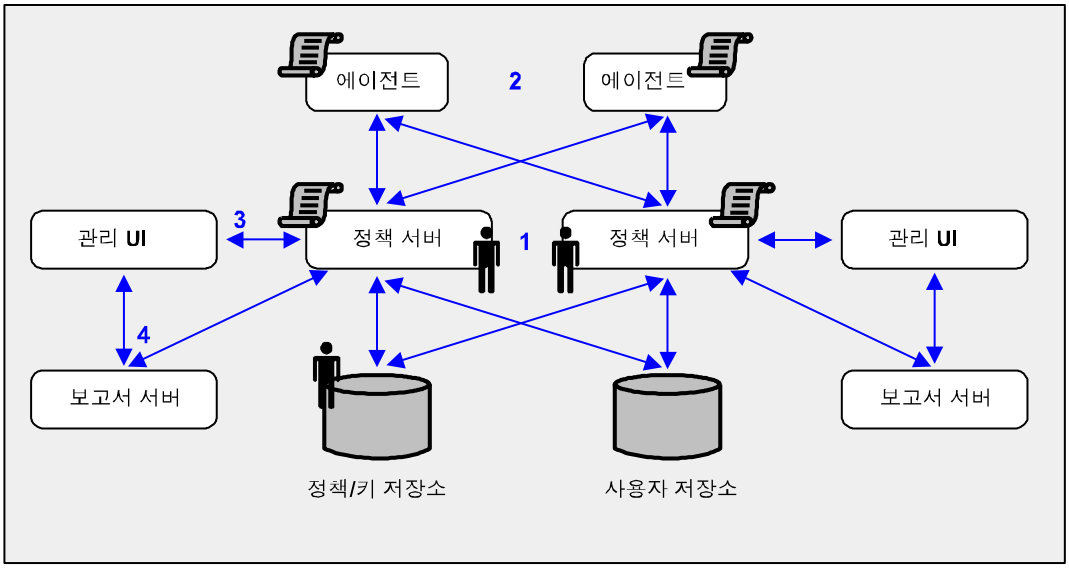
마이그레이션 로드맵 - FIPS 전용 모드 구성

다음 다이어그램에서는 FIPS 마이그레이션 모드에서 작동하는 샘플 12.52 SP1 환경을 보여 주고, FIPS 전용 모드에서 작동하도록 각 구성 요소 및 연결을 구성하는 순서를 나열합니다.

음영 처리된 구성 요소는 FIPS 승인 알고리즘을 사용하여 다시 암호화해야 하는 중요한 데이터를 나타냅니다. 다음을 수행하기 전까지는 마이그레이션 프로세스를 계속하지 마십시오.

- 환경의 각 정책 서버에 대한 정책 저장소 키 다시 암호화
- 정책 저장소 관리자 암호 다시 암호화
- SiteMinder 슈퍼 사용자 암호 다시 암호화
- 환경의 각 에이전트에 대한 공유 암호 다시 암호화
- 정책 저장소 데이터 다시 암호화
- 환경에서 기본 암호 서비스를 사용하는 경우 정책 서버에서 사용자 저장소의 모든 사용자 암호 Blob 을 다시 암호화했는지 확인

  중요! 정책 서버가 FIPS 전용 모드에서 작동할 때 암호 서비스는 암호 Blob 이 다시 암호화되지 않은 사용자를 잠급니다. 관리자가 암호 Blob 을 삭제하고 비활성화된 모든 플래그를 지울 때까지 사용자는 액세스 권한을 다시 얻을 수 없습니다. 암호 Blob 을 삭제하면 사용자의 암호 기록이 손실됩니다.



1. 환경의 각 정책 서버를 FIPS 전용 모드에서 작동하도록 설정합니다.
2. 사용자 지정 에이전트를 포함한 각 SiteMinder 웹 에이전트를 FIPS 전용 모드에서 작동하도록 설정합니다.

3. 각 관리 UI 와 해당 정책 서버 간의 기존 연결을 FIPS 호환 알고리즘이 아닌 알고리즘을 사용하여 암호화합니다. 각 관리 UI 를 해당 정책 서버에 다시 등록하여 FIPS 호환 알고리즘으로 연결을 암호화합니다.
4. 보고서 서버와 정책 서버 간의 기존 연결을 FIPS 호환 알고리즘이 아닌 알고리즘을 사용하여 암호화합니다. 각 보고서 서버를 해당 정책 서버에 다시 등록하여 FIPS 호환 알고리즘으로 연결을 암호화합니다.

FIPS 전용 모드를 구성하는 방법

사용 환경에서 FIPS 호환 알고리즘만 사용하여 중요한 데이터를 암호화하도록 하려면 다음 절차를 완료하십시오.

1. 환경의 각 에이전트를 FIPS 전용 모드로 설정합니다.
2. 환경의 각 정책 서버를 FIPS 전용 모드로 설정합니다.
3. 관리 UI 를 해당 정책 서버에 다시 등록합니다. 다음 사항을 고려하십시오.
   - 등록 프로세스 중에는 관리 UI 를 사용할 수 없습니다. 그러나 정책 서버에서는 등록 프로세스 중에도 액세스 제어를 계속 제공하고 감사 정보가 들어 있는 로그 파일을 생성합니다.
   - 관리 UI 에 내부 또는 외부 관리자 인증을 구성할 수 있습니다.
     - 내부 인증이 구성된 관리 UI 에서는 관리자 자격 증명의 원본으로 정책 저장소를 사용합니다.
     - 외부 인증이 구성된 관리 UI 에서는 관리자 자격 증명의 원본으로 외부 사용자 저장소를 사용합니다.

     관리 UI 를 다시 등록하기 위한 프로세스는 SiteMinder 관리자를 인증하는 방식에 따라 달라집니다.

   참고: 모든 관리 UI 연결이 다시 등록될 때까지 이 단계를 반복하십시오.
4. 보고서 서버를 해당 정책 서버에 다시 등록합니다.

   참고: 모든 보고서 서버 연결이 다시 등록될 때까지 이 단계를 반복하십시오.

에이전트를 FIPS 전용 모드로 설정

에이전트를 FIPS 전용 모드로 설정하면 에이전트가 FIPS 호환 알고리즘을 사용하여 암호화된 세션 키, 에이전트 키 및 공유 암호만 허용하도록 할 수 있습니다.

에이전트를 FIPS 전용 모드로 설정하려면

1. 텍스트 편집기에서 SmHost.conf 파일을 엽니다.

   이 파일에는 다음 줄이 표시됩니다.

   ```
   fipsmode="MIGRATE"
   ```

2. 이 행을 다음과 같이 편집합니다.

   ```
   fipsmode="ONLY"
   ```

3. 파일을 저장한 후 닫습니다.
4. 에이전트를 호스트하는 컴퓨터를 다시 시작합니다.

   에이전트가 FIPS 마이그레이션 모드에서 작동합니다.

5. 트러스트된 호스트로 등록된 환경의 각 컴퓨터에 대해 이전 단계를 반복합니다.

이제 FIPS 전용 모드에서 작동하도록 정책 서버를 구성할 수 있습니다.

정책 서버를 FIPS 전용 모드로 설정

정책 서버를 FIPS 전용 모드로 설정하여 정책 서버가 암호화된 정보를 읽고 쓸 때 FIPS 호환 알고리즘만 사용하도록 구성합니다.

중요! 정책 서버가 FIPS 전용 모드에서 작동할 때 암호 서비스는 암호 Blob 이 다시 암호화되지 않은 사용자를 잠급니다. 관리자가 암호 Blob 을 삭제하고 비활성화된 모든 플래그를 지울 때까지 사용자는 액세스 권한을 다시 얻을 수 없습니다. 암호 Blob 을 삭제하면 사용자의 암호 기록이 손실됩니다.

참고: 다시 암호화되지 않은 암호 Blob 을 식별하는 것에 대한 자세한 내용은 암호 Blob 이 다시 암호화되었는지 확인 (페이지 152)을 참조하십시오.

다음 단계를 수행하십시오.

1. 정책 서버 호스트 시스템에서 명령 프롬프트를 열고 다음 명령을 실행합니다.

   ```
   setFIPSonly
   ```

   명령 창에 ONLY 가 나타납니다.

2. 정책 서버를 중지합니다.

   참고: 정책 서버 중지 및 시작에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

3. 다음 단계 중 하나를 수행합니다.

   - 정책 서버가 Windows 시스템에 설치되어 있는 경우 시스템을 재부팅합니다.
   - 정책 서버가 UNIX 시스템에 설치되어 있는 경우 다음 단계를 수행하십시오.

     a. 정책 서버를 시작할 때 사용한 사용자로 로그인합니다.

     b. 명령 프롬프트를 엽니다.

     c. *policy_server_home* 으로 이동합니다.

     d. 다음 명령을 실행합니다.

     ```
     ./ca_ps_env.ksh
     ```

4. 정책 서버를 시작합니다.

5. smps.log 파일을 열고 다음 행이 표시되는지 확인합니다.

   ```
   Policy Server employing only FIPS-140 cryptographic algorithms.
   ```

6. 로그 파일을 닫습니다.

   정책 서버가 FIPS 전용 모드에서 작동하도록 설정됩니다.

7. 환경의 각 정책 서버에 대해 후반 단계를 반복합니다.

이제 각 관리 UI 를 해당 정책 서버에 등록할 수 있습니다.

내부 인증이 구성된 관리 UI 를 다시 등록하는 방법

관리 UI 와 정책 서버에서 암호화된 연결을 설정하는 데 사용하는 공유 암호는 아직 기존 SiteMinder 알고리즘으로 암호화되고 있습니다. 관리 UI 를 다시 등록하면 FIPS 호환 알고리즘을 사용하여 암호화된 새 공유 암호가 생성됩니다.

내부 인증이 구성된 관리 UI 를 다시 등록하려면 다음 절차를 완료하십시오.

1. 응용 프로그램 서버를 중지합니다.
2. 관리 UI 데이터 디렉터리를 삭제합니다.
3. 관리 UI 등록 창을 재설정합니다.
4. 응용 프로그램 서버를 시작합니다.
5. 관리 UI 를 등록합니다.

응용 프로그램 서버 중지

응용 프로그램 서버를 중지하려면

1. 관리 UI 호스트 시스템에 로그인합니다.
2. 다음 작업 중 하나를 수행하십시오.
   - 독립 실행형 설치 옵션을 사용하여 관리 UI 를 설치한 경우 SiteMinder 관리 UI 서비스를 중지합니다.
   - 기존 응용 프로그램 서버 인프라에 관리 UI 를 설치한 경우 해당 응용 프로그램 서버를 중지합니다.

   참고: 응용 프로그램 서버 중지에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

관리 UI 데이터 디렉터리 삭제

관리 UI 와 정책 서버 간의 기존 트러스트된 연결을 제거하려면 관리 UI 데이터 디렉터리를 삭제하십시오.

관리 UI 데이터 디렉터리를 삭제하려면

1. 관리 UI 호스트 시스템에 로그인합니다.
2. 다음 작업 중 하나를 수행하십시오.
   - (독립 실행형) 독립 실행형 설치 옵션을 사용하여 관리 UI 를 설치한 경우

     administrative_ui_home/CA/SiteMinder/adminui/server/default 로 이동하여 다음 폴더를 삭제합니다.

     data

     administrative_ui_home

     관리 UI 설치 경로를 지정합니다.
   - (JBoss) 기존 JBoss 인프라에 관리 UI 를 설치한 경우

     JBoss_home/server/default/data 로 이동합니다.

     JBoss_home

     JBoss 설치 경로를 지정합니다.

     data 폴더에는 apacheds, derby 및 siteminder 폴더가 있습니다.

     a. siteminder 폴더를 삭제합니다.

     b. apacheds 폴더를 열고 siteminder 폴더를 삭제합니다.

     c. derby 폴더를 열고 siteminder 폴더를 삭제합니다.
   - (WebLogic) 기존 WebLogic 인프라에 관리 UI 를 설치한 경우

     WebLogic_domain_folder 로 이동하여 다음 폴더를 삭제합니다.

     data

     WebLogic_domain_folder

     관리 UI 에 대해 생성된 WebLogic 도메인의 경로를 지정합니다.

- (WebSphere) 기존 WebSphere 인프라에 관리 UI 를 설치한 경우 *WebSphere_home*/profiles/*profile* 로 이동하여 다음 폴더를 삭제합니다.

  data

  WebSphere_home

  WebSphere 가 설치된 전체 경로를 지정합니다.

  profile

  관리 UI 에 사용되는 프로필의 이름을 지정합니다.

관리 UI 데이터 사전이 삭제됩니다.

관리 UI 등록 창 재설정

정책 저장소에 있는 모든 슈퍼 사용자의 자격 증명을 제출하려면 등록 창을 재설정하십시오. 정책 서버에서는 이러한 자격 증명을 사용하여 등록 요청이 유효하고 관리 UI 와 정책 서버 간의 관계를 트러스트할 수 있는지 확인합니다.

관리 UI 등록 창을 재설정하려면

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

```
XPSRegClient siteminder_administrator[:passphrase] -adminui-setup -t timeout -r
retries -c comment -cp -l
log_path -e error_path -vT -vI -vW -vE -vF
```

siteminder_administrator

슈퍼 사용자 권한이 있는 SiteMinder 관리자를 지정합니다.

참고: 슈퍼 사용자 계정을 사용할 수 없는 경우에는 smreg 유틸리티를 사용하여 기본 SiteMinder 계정을 생성하십시오.

passphrase

SiteMinder 관리자 계정의 암호를 지정합니다.

참고: passphrase 를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고 확인하라는 메시지가 표시됩니다.

-adminui-setup

정책 서버에 관리 UI 를 다시 등록하도록 지정합니다.

-t *timeout*

(선택 사항) 관리 UI 를 설치할 때부터 정책 서버에 로그인하고 정책 서버와의 트러스트 관계를 생성할 때까지 할당된 시간을 지정합니다. 이 시간 만료 값을 초과할 경우 정책 서버에서는 등록 요청을 거부합니다.

측정 단위: 분

기본값: 240(4 시간)

최소 제한: 1

최대 제한: 1440(24 시간)

-r *retries*

(선택 사항) 관리 UI 를 등록할 때 허용되는 시도 실패 횟수를 지정합니다. 등록 프로세스를 완료하기 위해 관리 UI 에 로그인할 때 올바르지 않은 SiteMinder 관리자 자격 증명을 제출할 경우 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 유틸리티에서 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 내보내야 하는 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.

3. Enter 키를 누릅니다.

   XPSRegClient 가 정책 서버에 관리자 자격 증명을 제공합니다. 정책 서버에서는 관리 UI 에 로그인할 때 이러한 자격 증명을 사용하여 등록 요청을 확인합니다.

응용 프로그램 서버 시작

응용 프로그램 서버를 시작하려면

1. 관리 UI 호스트 시스템에 로그인합니다.
2. 다음 작업 중 하나를 수행하십시오.
   - 독립 실행형 설치 옵션을 사용하여 관리 UI 를 설치한 경우 SiteMinder 관리 UI 서비스를 시작합니다.
   - 기존 응용 프로그램 서버 인프라에 관리 UI 를 설치한 경우 해당 응용 프로그램 서버를 시작합니다.

참고: 응용 프로그램 서버 시작에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

관리 UI 등록

FIPS 호환 알고리즘을 사용하여 암호화된 새 공유 암호를 생성하려면 관리 UI 를 등록하십시오.

참고: 관리 UI 등록에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

외부 인증이 구성된 관리 UI 를 다시 등록하는 방법

관리 UI 와 정책 서버에서 암호화된 연결을 설정하는 데 사용하는 공유 암호는 아직 기존 SiteMinder 알고리즘으로 암호화되고 있습니다. 관리 UI 를 다시 등록하면 FIPS 호환 알고리즘을 사용하여 암호화된 새 공유 암호가 생성됩니다.

외부 인증이 구성된 관리 UI 를 다시 등록하려면 다음 절차를 완료하십시오.

1. 관리 UI 와 정책 서버 간의 기존 연결을 삭제합니다.
2. 관리 UI 등록 도구를 실행합니다.
3. 등록 정보를 수집합니다.
4. 관리 UI 와 정책 서버의 연결을 구성합니다.
5. 이전의 트러스트된 호스트를 삭제합니다.

관리 UI 와 정책 서버의 연결 삭제

관리 UI 와 정책 서버의 연결을 삭제하여 연결을 다시 등록할 수 있습니다.

관리 UI 와 정책 서버의 연결을 삭제하려면

1. 관리 UI 에 로그인하고 "관리", "관리 UI"를 차례로 클릭합니다.
   연결 유형 목록이 나타납니다.
2. "정책 서버 연결", "정책 서버 연결 삭제"를 차례로 클릭합니다.
   "정책 서버 연결 삭제" 창이 나타납니다.
3. 검색 조건을 입력하고 "검색"을 클릭합니다.
   조건과 일치하는 연결이 나타납니다.

4. 삭제할 연결을 선택하고 "선택"을 클릭합니다.

   요청을 확인하라는 메시지가 표시됩니다.

5. "예"를 클릭합니다.

   관리 UI 와 정책 서버 간의 연결이 삭제됩니다.

관리 UI 등록 도구 실행

관리 UI 등록 도구를 실행하여 클라이언트 이름 및 암호를 생성하십시오. 클라이언트 이름 및 암호 쌍은 등록할 관리 UI 를 정책 서버에서 식별하는 데 사용되는 값입니다. 관리 UI 에서 클라이언트 및 암호 값을 제출하여 등록 프로세스를 완료하십시오.

등록 도구를 실행하려면

1. 정책 서버 호스트 시스템에서 명령 프롬프트를 엽니다.
2. 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.

3. Enter 키를 누릅니다.

   클라이언트 이름 및 암호 쌍이 생성됩니다.

이제 관리 UI 를 정책 서버에 등록할 수 있습니다. 관리 UI 에서 등록 프로세스를 완료하십시오.

등록 정보 수집

관리 UI 는 사용자가 정책 서버에서 등록할 수 있도록 등록 프로세스로부터 특정 정보가 필요합니다.

관리 UI 에 로그인하기 전에 다음 정보를 수집하십시오.

- **클라이언트 이름** - XPSRegClient 도구를 사용하여 지정한 클라이언트 이름입니다.
- **암호** - XPSRegClient 도구를 사용하여 지정한 암호입니다.
- **정책 서버 호스트** - 정책 서버 호스트 시스템의 IP 주소 또는 이름입니다.
- **정책 서버 인증 포트** - 정책 서버가 인증 요청을 수신 대기하는 포트입니다.

  기본값: 44442

정책 서버에 대한 연결 구성

SiteMinder 관리자가 관리 UI 를 사용하여 정책 서버를 통해 정책 정보를 관리할 수 있도록 관리 UI 와 정책 서버의 연결을 구성할 수 있습니다. 관리 UI 에서 연결을 구성합니다.

관리 UI 와 정책 서버의 연결을 구성하려면

1. 지원되는 웹 브라우저를 열고 다음을 입력합니다.

   http://*host.domain*/iam/siteminder/adminui

   관리 UI 로그인 화면이 표시됩니다.
2. 슈퍼 사용자로 로그인합니다.
3. "관리", "관리 UI"를 차례로 클릭합니다.
4. "정책 서버 연결", "정책 서버 연결 등록"을 차례로 클릭합니다.

   "정책 서버 연결 등록" 창이 열립니다.

   참고: "도움말"을 클릭하면 해당되는 각 요구 사항과 제한을 포함하여 설정과 컨트롤에 대한 설명을 볼 수 있습니다.
5. "일반" 그룹 상자의 "이름" 필드에 연결 이름을 입력합니다.
6. "정책 서버 호스트" 필드에 정책 서버 호스트 시스템의 이름이나 IP 주소를 입력합니다.

7. "정책 서버 포트" 필드에 정책 서버 인증 포트를 입력합니다.

   참고: 이 값은 정책 서버 관리 콘솔의 "설정" 탭에 있는 "인증 포트(TCP)" 필드 값과 일치해야 합니다. 기본 인증 포트는 44442 입니다.

8. "일반" 그룹 상자의 필드에 등록 도구를 사용하여 생성한 클라이언트 이름 및 암호를 입력합니다.

9. "FIPS 전용" 모드 라디오 단추를 선택합니다.

10. "제출"을 클릭합니다.

    관리 UI 와 정책 서버 간의 연결이 구성됩니다. 관리 UI 와 정책 서버에서 암호화된 연결을 설정하는 데 사용하는 공유 암호는 FIPS 승인 알고리즘을 사용하여 암호화됩니다.

관리 UI 를 다시 등록하기 위한 프로세스를 완료했습니다.

이전의 트러스트된 호스트 삭제

관리 UI 를 정책 서버에 다시 등록하면 새 트러스트된 호스트가 생성됩니다. 이전의 트러스트된 호스트는 더 이상 필요하지 않으므로 삭제해야 합니다.

트러스트된 호스트 연결을 삭제하려면

1. 관리 UI 에 로그인하고 "인프라", "호스트"를 차례로 클릭합니다.
2. "트러스트된 호스트", "트러스트된 호스트 삭제"를 차례로 클릭합니다.

   "트러스트된 호스트 삭제" 창이 나타납니다.

3. 이전의 트러스트된 호스트 연결을 검색하여 선택합니다.

   참고: 관리 UI 등록 프로세스의 결과로 생성된 트러스트된 호스트에는 "Generated by XPSRegClient"(XPSRegClient 에서 생성됨)라는 설명이 있습니다.

4. "선택"을 클릭합니다.

   선택 항목을 확인하라는 메시지가 표시됩니다.

   중요! 새 트러스트된 호스트가 아니라 마지막으로 관리 UI 를 등록할 때 생성된 트러스트된 호스트를 삭제해야 합니다.

5. "예"를 클릭합니다.

   트러스트된 호스트 연결이 삭제됩니다.

보고서 서버 연결을 다시 등록하는 방법

보고서 서버를 다시 등록하면 보고서 서버와 정책 서버 간의 연결이 FIPS 승인 알고리즘을 사용하여 암호화됩니다.

보고서 서버를 다시 등록하려면 다음 단계를 완료하십시오.

1. 보고서 서버 클라이언트의 이름과 암호를 생성합니다.
2. 등록 정보를 수집합니다.
3. 보고서 서버를 정책 서버에 등록합니다.

클라이언트 이름 및 암호 만들기

XPSRegClient 유틸리티를 실행하여 클라이언트 이름 및 암호를 생성하십시오. 클라이언트 이름 및 암호의 용도는 다음과 같습니다.

- 등록할 보고서 서버를 정책 서버에서 식별하는 데 사용됩니다.
- XPSRegClient 도구로 보고서 서버를 정책 서버에 등록하는 데 사용됩니다.

등록 도구를 실행하려면

1. 정책 서버 호스트 시스템에서 명령줄 창을 엽니다.
2. *siteminder_home*/bin 으로 이동합니다.

   siteminder_home

   정책 서버 설치 경로를 지정합니다.
3. 다음 명령을 실행합니다.

   ```
   XPSRegClient client_name[:passphrase] -report -t timeout -r retries
   -c comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

   client_name

   등록할 보고서 서버의 이름을 식별합니다.

   제한: 이 값은 고유해야 합니다. 예를 들어 이전에 reportserver1 을 사용했으면 reportserver2 를 입력합니다.

   참고: 이 값을 기록해 두십시오. 이 값은 보고서 서버 호스트 시스템에서 등록 프로세스를 완료하는 데 필요합니다.

passphrase

보고서 서버 등록을 완료하는 데 필요한 암호를 지정합니다.

제한: 암호는 다음 조건을 충족해야 합니다.

- 6 자 이상을 포함해야 합니다.
- 암호에 앰퍼샌드(&)나 별표(*)는 포함할 수 없습니다.
- 암호에 공백이 포함되어 있는 경우 암호를 따옴표로 묶어야 합니다.

이 단계에서 암호를 지정하지 않으면 XPSRegClient 에서 암호를 입력하고 확인하라는 메시지가 표시됩니다.

참고: 이 값을 기록해 두십시오. 이 값은 보고서 서버 호스트 시스템에서 등록 프로세스를 완료하는 데 필요합니다.

-report

보고서 서버를 등록하도록 지정합니다.

-t *timeout*

(선택 사항) 보고서 서버 호스트 시스템에서 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) 보고서 서버 호스트 시스템에서 등록 프로세스를 완료할 때 허용되는 시도 실패 횟수를 지정합니다. 등록 중 정책 서버에 제출한 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 내보내야 하는 위치를 지정합니다.

기본값: siteminder_home\log. 여기서 siteminder_home 은 정책 서버가 설치된 위치입니다.

-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 표시됩니다. 암호를 제공하지 않은 경우 암호를 묻는 메시지가 표시됩니다.

4. Enter 키를 누릅니다.

   클라이언트 이름 및 암호가 생성됩니다.

이제 보고서 서버를 정책 서버에 등록할 수 있습니다. 보고서 서버 호스트 시스템에서 등록 프로세스를 완료합니다.

등록 정보 수집

보고서 서버와 정책 서버 간의 등록 프로세스를 완료하려면 특정 정보가 필요합니다. 보고서 서버 호스트 시스템에서 XPSRegClient 유틸리티를 실행하기 전에 다음 정보를 수집하십시오.

- **클라이언트 이름** - XPSRegClient 도구를 사용하여 지정한 클라이언트 이름입니다.
- **암호** - XPSRegClient 도구를 사용하여 지정한 암호입니다.
- **정책 서버 호스트** - 정책 서버 호스트 시스템의 IP 주소 또는 이름입니다.

정책 서버에 보고서 서버 등록

정책 서버에 보고서 서버를 등록하여 두 구성 요소 간에 트러스트 관계를 생성하십시오. 보고서 서버 등록 도구를 사용하여 보고서 서버 호스트 시스템에서 연결을 구성하십시오.

정책 서버에 대한 연결을 구성하려면

1. 보고서 서버 호스트 시스템에서 명령줄 창을 열고 *report_server_home/external/scripts* 로 이동합니다.

   report_server_home

   보고서 서버 설치 위치를 지정합니다.

   기본값: (Windows) C:\Program Files\CA\SC\CommonReporting3

   기본값: (UNIX) /opt/CA/SharedComponents/CommonReporting3

2. 다음 명령 중 하나를 실행합니다.

   - (Windows)

     ```
     regreportserver.bat -pshost host_name -client client_name -passphrase passphrase
     -psport portnum -fipsmode 0|1
     ```

     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)

     ```
     regreportserver.sh -pshost host_name -client client_name -passphrase passphrase
     -psport portnum -fipsmode 0|1
     ```

-pshost *host_name*

보고서 서버를 등록하는 정책 서버 호스트 시스템의 IP 주소 또는 이름을 지정합니다.

-client *client_name*

클라이언트 이름을 지정합니다. 클라이언트 이름은 등록하려는 보고서 서버를 식별합니다.

참고: 이 값은 정책 서버 호스트 시스템에서 보고서 서버를 등록할 때 XPSRegClient 유틸리티를 사용하여 지정한 클라이언트 이름과 일치해야 합니다.

예: XPSRegClient 유틸리티를 사용할 때 "reportserver1"을 지정한 경우 "reportserver1"을 입력합니다.

-passphrase *passphrase*

클라이언트 이름과 쌍을 이루는 암호를 지정합니다. 클라이언트 이름은 등록하려는 보고서 서버를 식별합니다.

참고: 이 값은 정책 서버 호스트 시스템에서 보고서 서버를 등록할 때 XPSRegClient 유틸리티를 사용하여 지정한 암호와 일치해야 합니다.

예: XPSRegClient 유틸리티를 사용할 때 SiteMinder 를 지정한 경우 SiteMinder 를 입력합니다.

-psport *portnum*

(선택 사항) 정책 서버가 등록 요청을 수신 대기하는 포트를 지정합니다.

fipsmode

보고서 서버와 정책 서버 간의 통신이 암호화되는 방식을 지정합니다.

- 0 은 FIPS 호환성 모드를 지정합니다.
- 1 은 FIPS 전용 모드를 지정합니다.

기본값: 0

3. Enter 키를 누릅니다.

등록했음을 알리는 메시지가 표시됩니다. 정책 서버에 보고서 서버를 다시 등록하는 작업을 완료했습니다. 보고서 서버와 정책 서버 간의 연결이 FIPS 호환 알고리즘을 사용하여 암호화됩니다.

제 5 장: SiteMinder 키 데이터베이스 마이그레이션 문제 해결

SiteMinder 키 데이터베이스 마이그레이션의 상태를 알 수 없음

증상

정책 서버가 업그레이드되었다는 것은 알고 있습니다. 하지만 인증서 데이터 저장소로의 smkeydatabase 마이그레이션이 성공했는지 여부가 불확실합니다.

해결 방법

마이그레이션이 성공했는지 확인하려면 smkeydatabase 마이그레이션 유틸리티(smmigratecds)를 사용하십시오.

참고: 이 유틸리티의 기본 위치는 *siteminder_home*\bin 입니다.

siteminder_home

정책 서버 설치 경로를 지정합니다.

다음 단계를 수행하십시오.

1. smkeydatabase 와 같은 곳에 배치된 정책 서버 호스트 시스템에 로그인합니다.
2. 다음 단계 중 하나를 수행합니다.
   - (Windows) 명령 프롬프트를 열고 다음 명령을 입력합니다.

     ```
     smmigratecds.bat –isComplete
     ```

     -isComplete

     이전 마이그레이션이 성공했는지 확인합니다.

   - (UNIX) 셸을 열고 다음 명령을 실행합니다.

     ```
     smmigratecds.sh –isComplete
     ```

마이그레이션에 성공한 경우 시스템이 이미 마이그레이션되었다는 메시지가 표시됩니다. 마이그레이션에 실패한 경우에는 시스템을 마이그레이션해야 한다는 메시지가 표시됩니다.

인증서 데이터 저장소 오류 발생

증상

인증서 데이터 저장소가 구성되지 않았다는 메시지가 표시됩니다.

해결 방법

다음 단계를 수행하십시오.

1. r6.x 에서 업그레이드하는 경우에는 정책 저장소 스키마를 확장 (페이지 37)합니다.
2. 정책 서버 호스트 시스템에 로그인합니다.
3. 다음 명령을 실행합니다.

   ```
   XPSDDInstall CDSObjects.xdd
   ```

   정책 저장소 스키마가 인증서 데이터 저장소를 지원하도록 확장됩니다.
4. 다음 단계 중 하나를 수행합니다.
   - (Windows) 명령 프롬프트를 열고 다음 명령을 입력합니다.

     ```
     smmigratecds.bat –validateInstall
     ```

     validateInstall

     인증서 데이터 저장소가 올바르게 설치되었는지 확인합니다.
   - (UNIX) 셸을 열고 다음 명령을 실행합니다.

     ```
     smmigratecds.sh -validateInstall
     ```

     인증서 저장소가 올바르게 구성된 경우 설치가 유효하다는 메시지가 표시됩니다. 인증서 데이터 저장소 설치가 실패한 경우에는 설치가 유효하지 않다는 메시지가 표시됩니다.
5. SiteMinder 키 데이터베이스를 수동으로 마이그레이션합니다.

추가 정보:

SiteMinder 키 데이터베이스 수동 마이그레이션 (페이지 177)

마이그레이션 실패 오류 발생

증상

smkeydatabase 마이그레이션이 실패했다는 메시지가 표시됩니다.

해결 방법

마이그레이션 유틸리티(smmigratecds)는 smkeydatabase 의 콘텐츠를 인증서 데이터 저장소와 비교하여 하나 이상의 데이터 불일치를 찾아냅니다. 데이터 불일치의 예는 서로 다른 인증서에 동일한 별칭이 매핑된 경우입니다.

이러한 불일치가 있으면 마이그레이션이 실패합니다.

다음 단계를 수행하십시오.

1. smkeydatabase 마이그레이션 로그(smkeydatabaseMigration.log)를 사용하여 문제를 찾습니다.

   로그는 *siteminder_home*\log 에 있습니다.

   siteminder_home

   정책 서버 설치 경로를 지정합니다.

2. 액세스 레거시 키 저장소 플래그(–accessLegacyKS)로 smkeytool 유틸리티를 사용하여 smkeydatabase 에 액세스합니다.
3. 실패의 원인이 된 데이터 불일치를 해결합니다.

   참고: smkeytool 사용에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

4. smkeydatabase 를 수동으로 마이그레이션합니다.

SiteMinder 키 데이터베이스 수동 마이그레이션

증상

smkeydatabase 인증서 데이터를 인증서 데이터 저장소로 수동으로 마이그레이션하고자 합니다.

해결 방법

smkeydatabase 마이그레이션 유틸리티(smmigratecds)를 사용하십시오.

다음 단계를 수행하십시오.

1. 모든 smkeydatabase 인스턴스가 동기화 (페이지 50)되었는지 확인합니다.
2. smkeydatabase 와 같은 곳에 배치된 정책 서버 호스트 시스템에 로그인합니다.
3. 다음 단계 중 하나를 수행하여 인증서 데이터 저장소가 올바르게 구성되었는지 확인합니다.
   - (Windows) 명령 프롬프트를 열고 다음 명령을 입력합니다.

     ```
     smmigratecds.bat –validateInstall
     ```

     -validateInstall

     인증서 데이터 저장소가 올바르게 설치되었는지 확인합니다.
   - (UNIX) 셸을 열고 다음 명령을 실행합니다.

     ```
     smmigratecds.sh -validateInstall
     ```
4. 다음 단계 중 하나를 수행하여 smkeydatabase 의 콘텐츠를 인증서 데이터 저장소와 비교합니다. 콘텐츠를 비교하면 마이그레이션 실패의 원인이 될 수 있는 데이터 불일치를 확인할 수 있습니다.
   - (Windows) 다음 명령을 실행합니다.

     ```
     smmigratecds.bat –validate -log log_file
     ```

     -validate

     smkeydatabase의 내용을 인증서 데이터 저장소와 비교합니다.

     -log

     확인 결과를 로그로 보냅니다.

     log_file

     유틸리티가 로그를 보낼 로그 파일의 이름과 위치를 지정합니다.

     예: -log "C:\Progam Files\Sample\Logs"
   - (UNIX) 다음 명령을 실행합니다.

     ```
     smmigratecds.sh -validate -log log_file
     ```
5. (선택 사항) 데이터 불일치가 존재하는 경우 로그 파일을 사용하여 문제를 찾습니다.

6. 다음 단계 중 하나를 수행하여 마이그레이션을 시작합니다.
   - (Windows) 다음 명령을 실행합니다.

     `smmigratecds.bat -migrate -log log_file`

     -migrate

     smkeydatabase를 인증서 데이터 저장소로 마이그레이션합니다.

     -log

     마이그레이션 결과를 로그로 보냅니다.

     log_file

     유틸리티가 로그를 보낼 로그 파일의 이름과 위치를 지정합니다.

     예: -log "C:\Progam Files\Sample\Logs"

   - (UNIX) 다음 명령을 실행합니다.

     `smmigratecds.sh -migrate -log log_file`

7. (선택 사항) 마이그레이션에 실패한 경우 로그 파일을 사용하여 원인을 파악합니다.