# SiteMinder

# 구현 안내서

**12.52 SP1**

ca technologies

# CA Technologies 제품 참조

이 문서는 다음 CA Technologies 제품을 참조합니다 :

- CA RiskMinder<tm>(이전의 CA Arcot RiskFort)
- CA AuthMinder®(이전의 CA Arcot WebFort)
- CA SiteMinder® Federation
- CA Directory
- CA DataMinder®(이전의 CA DLP) Content Classification Service
- 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

이 설명서가 마지막으로 릴리스된 이후에 다음과 같이 업데이트되었습니다.

- 정기적인 유지 관리 태스크 (페이지 216)-XPS 스위퍼 유틸리티 실행 지침이 업데이트되었습니다(169270, 168658, 21175885:01).

# 목차

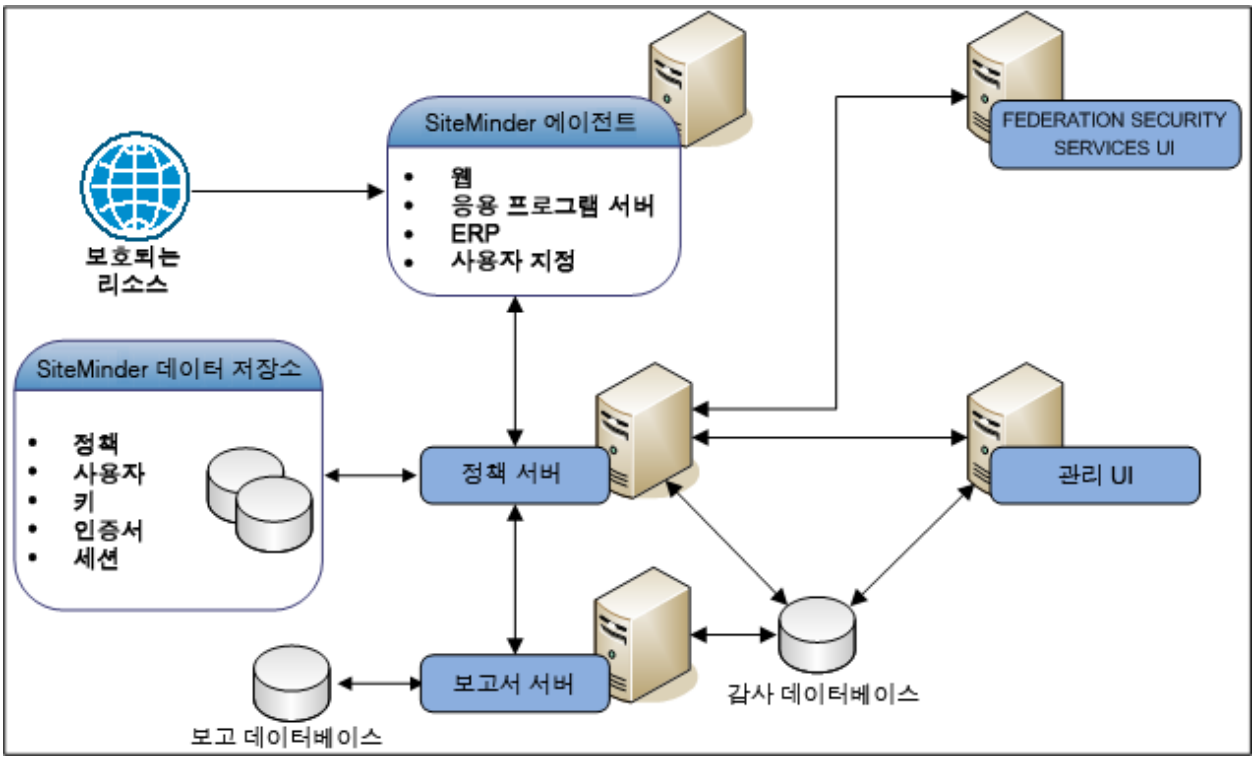
# 제 1 장: SiteMinder 구성 요소 및 저장소

## 구성 요소 및 저장소

SiteMinder 환경에는 여러 구성 요소가 포함되어 있습니다. 일부 구성 요소는 리소스의 보안을 위해 필요하며, 일부는 선택 사항이거나 특정 기능을 구축할 때만 필요하기도 합니다. 이러한 구성 요소는 조직의 리소스, 응용 프로그램, 디렉터리 및 데이터베이스와 함께 작동하여 전체 네트워크의 리소스에 대한 보안 액세스를 지원합니다.

모든 SiteMinder 구성 요소는 여러 운영 환경에서 지원됩니다. SiteMinder 구현은 배포된 환경의 영향을 크게 받습니다. 실제 구현이 다음 다이어그램을 반영할 필요는 없습니다. 다음 다이어그램의 목적은 SiteMinder 환경의 주요 구성 요소 및 각 구성 요소 간의 일반적인 관계를 보여 주려는 것입니다.

*그림 1: 제품 구성 요소 개요*



이 안내서에서 설명하는 아키텍처 질문을 고려할 때는 앞의 다이어그램과 다음의 구성 요소 설명을 참조하십시오.

## 정책 서버

(필수) SiteMinder 정책 서버는 PDP(정책 결정 지점)의 역할을 합니다. 정책 서버의 목적은 SiteMinder 에이전트로 통신하는 액세스 제어 정책을 평가하고 적용하는 것입니다. 정책 서버는 다음을 제공합니다.

- 정책에 기반한 사용자 관리
- 인증 서비스
- 권한 부여 서비스
- 암호 서비스
- 세션 관리
- 감사 서비스

정책 서버는 다른 모든 주요 구성 요소와 상호 작용하여 이러한 태스크를 수행합니다.

## SiteMinder 에이전트

(필수) SiteMinder 에이전트는 웹 서버, J2EE 응용 프로그램 서버, ERP(엔터프라이즈 리소스 계획) 시스템 또는 사용자 지정 응용 프로그램에 있을 수 있습니다. 에이전트는 PEP(정책 적용 지점)로 작동하여 사용자의 리소스 요청을 가로채 정책 서버와 통신하여 리소스가 보호되는지 확인합니다.

리소스가 보호되지 않는 경우 에이전트는 액세스를 허용합니다. 리소스가 보호되는 경우 에이전트는 정책 서버와 계속 통신하여 사용자를 인증하고 권한을 부여합니다. 권한 부여에 성공하면 에이전트는 리소스 요청이 서버로 진행되도록 허용합니다. 또한 에이전트는 다음을 수행합니다.

- 콘텐츠 개인화가 가능하도록 웹 응용 프로그램에 정보를 제공
- 리소스에 더 빠르게 액세스할 수 있도록 인증된 사용자 및 보호된 리소스에 대한 정보를 캐시
- SSO(싱글 사인온) 사용

## eTrust SOA Security Manager 에이전트

(eTrust SOA Security Manager 에 필수) eTrust SOA Security Manager(WSS) 에이전트는 다음 플랫폼에서 작동하는 PEP(정책 적용 지점)의 역할을 합니다.

- 웹 서버
- J2EE Application Server
- 사용자 지정 응용 프로그램

WSS 에이전트는 "대규모" SOAP 기반 웹 서비스에 대한 요청을 가로챕니다. 그런 다음 WSS 에이전트는 정책 서버와 통신하여 리소스가 보호되는지 여부를 확인합니다.

**참고:** JBoss 용 SiteMinder 에이전트에는 SiteMinder 및 WSS 에이전트 기능이 포함되어 있습니다. .

리소스가 보호되지 않는 경우 에이전트는 액세스를 허용합니다. 리소스가 보호되는 경우 에이전트는 정책 서버와 계속 통신하여 사용자를 인증하고 권한을 부여합니다. 권한 부여에 성공하면 에이전트는 리소스 요청이 서버로 진행되도록 허용합니다.

에이전트는 다음과 같은 기타 기능들도 수행합니다.

- 리소스에 더 빠르게 액세스할 수 있도록 인증된 사용자 및 보호된 리소스에 대한 정보를 캐시
- SSO(싱글 사인온) 사용

## CA Business Intelligence

(선택 사항) CA Business Intelligence 는 다양한 CA 제품에서 정보 제공과 비즈니스 결정 지원을 위한 용도로 사용하는 보고 및 분석 소프트웨어 집합입니다. CA 제품에서는 CA Business Intelligence 를 사용하여 효율적인 엔터프라이즈 IT 관리에 필요한 정보를 통합하고 분석한 다음 다양한 보고 옵션을 사용하여 표현합니다.

CA Business Intelligence 에는 정보 관리, 보고, 쿼리, 분석을 위한 완전한 도구 세트인 SAP BusinessObjects Enterprise 가 포함되어 있습니다. CA Business Intelligence 는 SAP BusinessObjects Enterprise 를 독립 실행형 구성 요소로 설치합니다. 이 안내서에서는 이 독립 실행형 구성 요소를 보고서 서버라고 합니다. 보고서 서버 설치는 전체 SiteMinder 설치 프로세스에 속하는 별도의 단계입니다. SiteMinder 관련 구성 요소와 별도로 보고서 서버를 설치하기 때문에 다른 CA 제품이 동일한 Business Intelligence 서비스를 공유할 수 있습니다.

보고서 서버는 보고서를 컴파일하여 SiteMinder 환경을 쉽게 분석할 수 있도록 도와줍니다. 이 구성 요소의 용도는 다음과 같은 유형의 보고서를 생성하는 것입니다.

- Audit
- 정책 분석

보고서 서버는 다음과 같은 구성 요소와 통신하여 보고서를 컴파일합니다.

- CMS(중앙 관리 서버) 데이터베이스(보고서 데이터베이스)
- 관리 UI
- 정책 서버
- SiteMinder 감사 데이터베이스

# 데이터 저장소

SiteMinder 구현에는 여러 개의 데이터 저장소가 포함됩니다. 그중에는 필수인 저장소도 있고 선택 사항이거나 특정 기능을 구현하는 데만 필요한 저장소도 있습니다.

여기에서는 다음에 대해 자세히 설명합니다.

- 저장소가 필수인지 선택 사항인지 여부
- 저장소의 용도

## 정책 저장소

(필수) SiteMinder 정책 저장소(정책 저장소)는 LDAP 디렉터리 서버 또는 ODBC 데이터베이스에 있는 권한 저장소입니다. 이 구성 요소의 용도는 다음을 비롯한 모든 정책 관련 개체를 저장하는 것입니다.

- SiteMinder 가 보호하는 리소스
- 이러한 리소스를 보호하는 데 사용되는 메서드
- 이러한 리소스에 액세스하거나 액세스할 수 없는 사용자 또는 그룹
- 보호되는 리소스에 대한 액세스 권한을 사용자에게 부여 또는 거부할 때 수행되어야 하는 작업

정책 서버는 EPM(Enterprise Policy Management) 응용 프로그램 또는 SiteMinder 정책이라고 통칭하는 이러한 정보를 사용하여 리소스가 보호되는지 여부와 인증된 사용자에게 요청된 리소스에 대한 액세스 권한이 부여되었는지 여부를 확인합니다.

## 사용자 저장소

(필수) SiteMinder 사용자 저장소 연결은 엔터프라이즈 네트워크에서 기존 사용자 디렉터리 또는 데이터베이스에 대한 연결입니다. 독자적인 SiteMinder 사용자 저장소를 사용할 필요는 없습니다. 사용자 저장소 연결의 용도는 정책 서버가 다음을 포함하는 사용자 데이터를 사용할 수 있도록 하는 것입니다.

- 조직 정보
- 사용자 및 그룹 특성
- 암호와 같은 사용자 자격 증명
- 이름 및 성과 같은 사용자 특성

정책 서버는 이 연결을 사용하여 다음을 수행합니다.

- 에이전트가 보호된 리소스에 대한 요청을 제출할 때 사용자 자격 증명을 확인
- 특정 사용자 데이터를 필요로 하는 SiteMinder 기능에 대한 사용자 특성 검색

**참고:** 사용자 저장소 연결에 대한 자세한 내용은 설명서 로드맵을 참조하십시오.

## 외부 관리자 저장소

(선택 사항) 기본적으로 관리 UI 에서는 정책 저장소를 SiteMinder 관리자 자격 증명의 원본으로 사용합니다. 이 기본 구성을 사용하면 정책 저장소를 구성하고 관리 UI 를 설치한 후에 바로 환경을 관리할 수 있습니다. 정책 저장소를 구성할 때 기본 SiteMinder 슈퍼 사용자 계정(siteminder)이 생성됩니다. 이 계정은 최대 시스템 권한을 가지며 관리 UI 에 처음 액세스하고 추가적인 SiteMinder 관리자를 생성하는 데 사용됩니다.

관리 UI 가 외부 관리자 저장소(예: 회사 디렉터리)를 사용하도록 구성할 수 있습니다. 외부 관리자 저장소는 엔터프라이즈 네트워크의 LDAP 디렉터리 서버 또는 ODBC 데이터베이스에 대한 연결입니다. 다음 사항을 고려하십시오.

- 관리 UI 는 하나의 외부 관리자 저장소에만 연결할 수 있습니다.
- 관리 UI 는 여러 정책 서버를 관리하도록 구성될 수 있습니다. 관리 UI 에서 여러 정책 서버를 관리하려면 외부 관리자 저장소에 대한 연결이 필요합니다.
- 고가용성을 위해 둘 이상의 관리 UI 를 구성하는 경우 동일한 외부 관리자 저장소를 사용하면 각 관리 UI 에서 모든 관리자를 사용할 수 있습니다.

**참고:** SiteMinder 관리자 및 외부 관리자 저장소 구성에 대한 자세한 내용은 설명서 로드맵을 참조하십시오.

## 키 저장소

(필수) 이 구성 요소의 용도는 정책 서버 및 에이전트에서 중요한 데이터를 암호화하는 데 사용하는 다음과 같은 암호화 키를 저장하는 것입니다.

- 에이전트에서 SiteMinder 쿠키를 암호화하는 데 사용하는 키
- 정책 서버에서 관리자 암호와 같은 중요한 정책 저장소 정보를 암호화하는 데 사용하는 키
- 정책 서버에서 자격 증명 및 사용자 세션과 관련된 기타 정보를 포함하는 SiteMinder 세션 티켓을 암호화하는 데 사용하는 키

키 저장소를 정책 저장소와 함께 배치하거나 암호화 키를 별도의 디렉터리 또는 데이터베이스에 저장할 수 있습니다. 별도의 키 저장소를 배포해야 하는 필요성은 다음에 따라 결정됩니다.

- 정책 서버와 정책 저장소를 구현하는 방법
- 싱글 사인온 요구 사항

**참고:** 정책 서버 구성 마법사를 사용하여 정책 저장소를 구성하는 경우 정책 저장소가 자동으로 정책 저장소와 함께 배치됩니다.

## 인증서 데이터 저장소

(선택 사항) SiteMinder CDS(인증서 데이터 저장소)는 SiteMinder 환경에서 다음과 같은 구성 요소 및 기능을 사용할 수 있도록 지원합니다.

- CA(인증 기관) 인증서
- 공개 키 및 개인 키
- CRL(인증서 해지 목록)
- OCSP 해지 검사

**참고:** SiteMinder 페더레이션 기능은 인증서 데이터 저장소를 사용합니다. X.509 인증서 인증 체계가 인증을 위해 사용하는 사용자 인증서는 인증서 데이터 저장소에 저장되지 않습니다. 이러한 사용자 인증서는 LDAP/AD 사용자 디렉터리 또는 ODBC 저장소에 저장됩니다.

기본적으로 인증서 데이터 저장소는 자동으로 구성되고 정책 서버와 같은 곳에 설치됩니다. 따라서 다음 사항이 적용됩니다.

- 별도의 외부 저장소가 필요하지 않습니다.
- 동일한 정책 저장소에 대한 공통의 뷰를 공유하는 모든 정책 서버는 동일한 키, 인증서 및 인증서 해지 목록에 액세스할 수 있습니다.
- 동일한 정책 저장소를 관리하는 모든 SiteMinder 관리자는 관리 UI 를 사용하여 인증서 데이터 저장소를 중앙에서 관리할 수 있습니다.

## SiteMinder 감사 데이터베이스

(선택 사항) 기본적으로 정책 서버는 정책 서버 로그라고 하는 텍스트 파일에 감사 이벤트를 씁니다. 감사 로그의 용도는 다음과 같은 모든 사용자 활동에 대한 정보를 추적하는 것입니다.

- 성공한 모든 인증
- 실패한 모든 인증
- 성공한 모든 권한 부여 시도
- 실패한 모든 권한 부여 시도
- 모든 관리 로그인 시도
- 관리자 암호 변경, 정책 저장소 개체 생성 및 정책 저장소 개체 변경과 같은 모든 관리 활동

하지만 독립 실행형 SiteMinder 감사 데이터베이스(감사 데이터베이스)를 구성할 수 있습니다. 감사 이벤트를 저장할 위치를 결정할 때는 다음 사항을 고려하십시오.

- 보고서 서버는 감사 기반 보고서를 생성하기 위해 감사 데이터베이스에 대한 연결을 필요로 합니다. 보고서 서버는 텍스트 파일에 기록된 정책 서버 로그를 바탕으로 감사 기반 보고서를 생성할 수 없습니다.
- 감사 로그를 텍스트 파일에 로깅하는 것보다 데이터베이스에 저장하는 것이 훨씬 안전합니다.
- 지원되는 경우 정책 저장소는 감사 데이터베이스의 역할도 할 수 있습니다.

**참고:** 감사 데이터베이스 구성에 대한 자세한 내용은 설명서 로드맵을 참조하십시오.

## 세션 저장소

(선택 사항) SiteMinder 가 사용자를 인증할 때 정책 서버는 세션 티켓을 발급합니다. 세션 티켓에는 해당 사용자에 대한 기본 정보 및 인증 정보가 포함됩니다. 기본적으로 SiteMinder 에서는 비영구 세션을 통해 세션 관리를 구현합니다. 비영구 세션이 사용되는 경우 에이전트는 세션 티켓을 사용자 브라우저의 쿠키에 씁니다. 하지만 일부 SiteMinder 기능에는 영구 세션이 필요합니다.

영구 세션이 사용되는 경우 에이전트는 세션 티켓을 독립 실행형 데이터베이스에 써야 합니다.

SiteMinder 세션 저장소를 배포하는 기본적인 이유는 다음과 같습니다.

- SiteMinder 로그오프 URI 가 구현된 경우 세션 저장소가 있으면 사용자가 로그오프한 후에 SiteMinder 세션이 다시 사용되지 않습니다.
- 영구 사용자 세션이 필요한 기능을 지원하기 위해서입니다.

에이전트는 이 정보를 사용하여 사용자를 식별하고 정책 서버에 세션 정보를 제공합니다.

**참고:** 세션 저장소 구성에 대한 자세한 내용은 설명서 로드맵을 참조하십시오.

## SiteMinder 관리 UI

(필수) SiteMinder 관리 UI(관리 UI)는 정책 서버와 독립적으로 설치되는 웹 기반 관리 콘솔입니다. 관리 UI 는 액세스 제어, 보고 및 정책 분석과 관련된 모든 태스크를 관리하기 위해 사용됩니다.

# 제 2 장: 아키텍처 고려 사항

이 섹션은 다음 항목을 포함하고 있습니다.



## 엔터프라이즈 환경

SiteMinder 구현은 배포되는 환경에 크게 영향을 받습니다. 구현을 엔터프라이즈에 적합한 여러 단계로 분할하는 계획을 세우는 것이 좋습니다. 배포 계획을 세울 때는 몇 가지 질문을 고려해야 합니다.

이러한 질문에 대한 답변은 SiteMinder 구현 계획을 수립하는 데 매우 중요합니다.

### 운영 체제

SiteMinder 구성 요소는 여러 플랫폼에서 지원됩니다. 이러한 플랫폼에 대한 자세한 내용은 "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)에 나와 있습니다. 다음 중 회사에 배포된 운영 체제는 무엇입니까?

- Microsoft® Windows®
- Oracle® Solaris™
- Red Hat® Enterprise Linux®
- Novell® SUSE® Linux
- HP-UX(Hewlett-Packard Company UNIX)
- IBM® AIX®
- IBM z/OS®

**참고:** 지원되는 운영 체제 버전에 대한 자세한 내용은 "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)를 참조하십시오.

다음 표를 참조하여 회사에 배포된 운영 체제가 현재 필요한 SiteMinder 구성 요소에 대해 지원되는지 확인하십시오.

| 구성 요소 | 필수 | 운영 체제 |
|---|---|---|
| 정책 서버 | 예 | |
| 에이전트 | 예 | |
| 관리 UI | 예 | |
| 보고서 서버 | 아니요 | |

**참고:** 이와 같은 구성 요소에는 플랫폼 요구 사항 외에도 최소 메모리 요구 사항 등의 다른 요구 사항이 있습니다. 정책 서버, 관리 UI 및 보고서 서버와 관련된 플랫폼 이외의 요구 사항에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오. 에이전트와 관련된 플랫폼 이외의 요구 사항에 대한 자세한 내용은 해당 SiteMinder 에이전트 설명서를 참조하십시오.

## 웹 서버 공급업체

웹 서버의 리소스를 보호하도록 SiteMinder 에이전트를 설치하고 구성할 수 있습니다. 다음의 지원되는 서버 공급업체 중 엔터프라이즈에 배포된 것은 무엇입니까?

- Apache™ HTTP Server
- Apache Tomcat
- Hewlett-Packard Company(HP) Apache
- IBM HTTP Server
- IBM Lotus® Domino
- Microsoft IIS
- Oracle® HTTP Server
- Red Hat Apache
- Sun Java™ System

**참고:** 지원되는 웹 서버의 구체적인 버전은 SiteMinder Platform Support Matrix(SiteMinder 플랫폼 지원표)를 참조하십시오.

여기에 나열되지 않은 다른 웹 서버를 사용하는 경우 웹 서버의 리소스를 보호하기 위해 CA SiteMinder for Secure Proxy Server 를 사용하는 방법을 고려하십시오.

## 응용 프로그램 서버 공급업체

J2EE 응용 프로그램 서버의 리소스를 보호하도록 SiteMinder 에이전트를 설치하고 구성할 수 있습니다. 다음의 지원되는 서버 공급업체 중 엔터프라이즈에 배포된 것은 무엇입니까?

- Oracle WebLogic®
- IBM WebSphere®
- RedHat JBoss®

**참고:** 지원되는 응용 프로그램 서버의 구체적인 버전은 SiteMinder Platform Support Matrix(SiteMinder 플랫폼 지원표)를 참조하십시오.

## ERP(Enterprise Resource Planning) 시스템

ERP 시스템의 리소스를 보호하도록 에이전트를 설치하고 구성할 수 있습니다. 다음의 지원되는 ERP 공급업체 중 엔터프라이즈에 배포된 것은 무엇입니까?

- Oracle PeopleSoft®
- Oracle Siebel®
- SAP®

**참고:** 지원되는 ERP 시스템의 구체적인 버전은 SiteMinder Platform Support Matrix(SiteMinder 플랫폼 지원표)를 참조하십시오.

## 디렉터리 서버와 데이터베이스

SiteMinder 데이터 저장소는 여러 디렉터리 서버 및 데이터베이스에서 지원됩니다. 다음 중 회사에 배포된 항목은 무엇입니까?

**참고:** 자세한 내용은 "Platform Support Matrix"(플랫폼 지원표)를 참조하십시오.

다음 표를 통해 회사에 배포된 디렉터리 서버 및 데이터베이스 유형이 구현에 필요한 구성 요소에 대해 지원되는지 확인할 수 있습니다.

| 구성 요소 | 필수 | LDAP | 데이터베이스 |
|---|---|---|---|
| 정책 저장소 | 예 | | |
| 사용자 저장소 연결 | 예 | | |
| 관리자 저장소 | 아니요 | | |
| 감사 데이터베이스 | 아니요 | 해당 없음 | |
| 키 저장소 | 아니요 | | |
| 세션 저장소 | 아니요 | 해당 없음 | |

# 아키텍처 사용 사례

다음 사용 사례는 SiteMinder 아키텍처를 고가용성과 성능의 관점에서 생각해 보도록 하기 위한 것입니다. 사용 사례는 간단한 배포에서 시작하여 점점 더 복잡한 시나리오로 발전합니다. 각 사례는 논리적 SiteMinder 구성 요소 "블록"의 개념을 기반으로 하며 다음과 같은 아키텍처 고려 사항을 해결하기 위해 환경에 여러 개의 블록이 포함되는 방식을 보여 줍니다.

- 중복성
- 장애 조치
- 용량 및 규모
- 여러 쿠키 도메인

이 사용 사례를 바탕으로 필요한 인프라를 도출하여 다음을 수행할 수 있습니다.

- SiteMinder 구성 요소 간에 중복성 및 고가용성을 구현하는 방법을 결정
- 여러 데이터 센터를 구현하는 방법을 결정
- 용량 계획에서 수집한 사용량 메트릭을 지원
- 구현 고려 사항을 지원
- 환경의 성능 조정을 위한 반복적인 프로세스를 시작

**추가 정보:**

용량 계획 소개 (페이지 103)
성능 조정 소개 (페이지 149)
중복성 및 고가용성 (페이지 39)

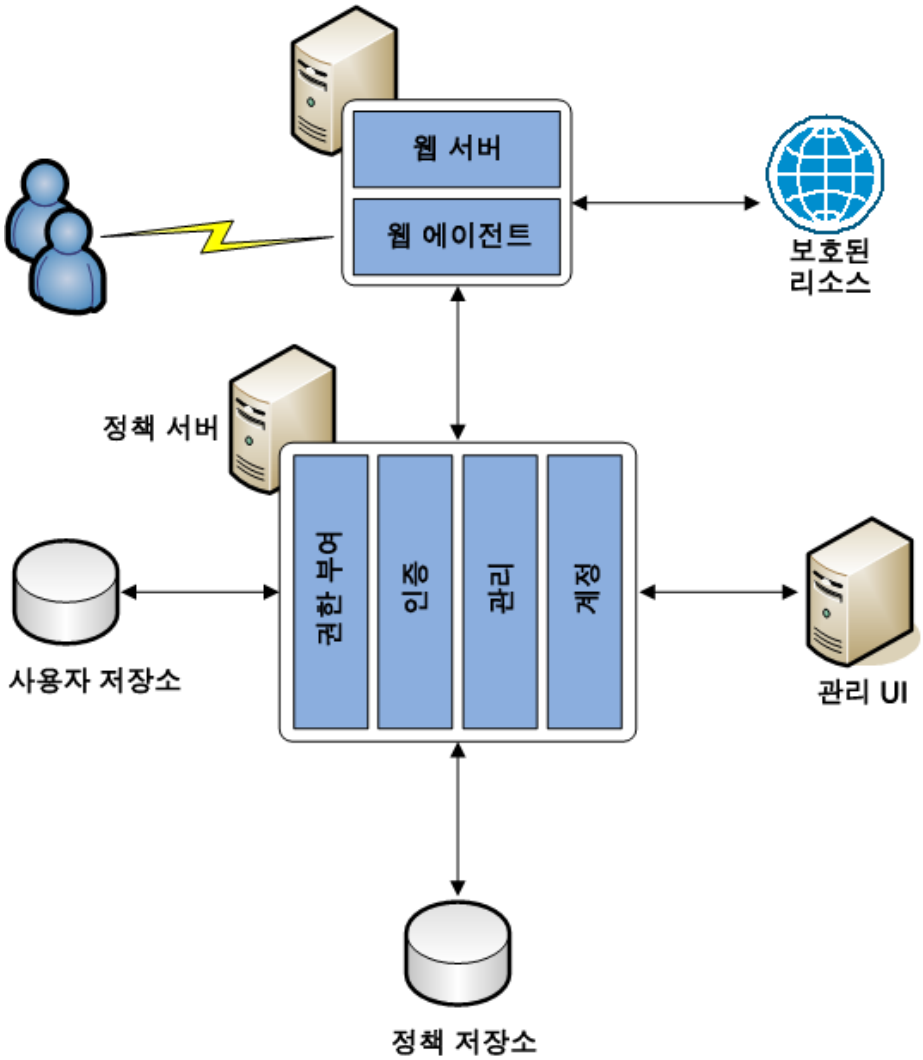
## 간단한 배포

가장 간단한 SiteMinder 배포에는 구성 요소로 이루어진 "블록" 한 개가 필요합니다. 구성 요소 블록은 다음을 포함하는 종속적 구성 요소의 논리적 조합입니다.

- 웹 에이전트
- 정책 서버
- 사용자 저장소
- 정책 저장소
- 관리 UI

최소한 하나의 블록을 배포하여 웹 기반 리소스를 보호합니다.

다음은 간단한 배포를 보여 주는 다이어그램입니다.




각 구성 요소마다 리소스 보호와 관련한 특정 역할이 있습니다.

**참고:** 각 구성 요소의 주된 용도에 대한 자세한 내용은 "SiteMinder 구성 요소"를 참조하십시오.

## 선택적 구성 요소를 사용한 간단한 배포

선택적 SiteMinder 구성 요소를 사용하여 간단한 배포의 기능을 확장할 수 있습니다. 선택적 구성 요소의 구현은 엔터프라이즈에 필요한 SiteMinder 기능에 따라 결정됩니다. 예를 들면 다음과 같습니다.

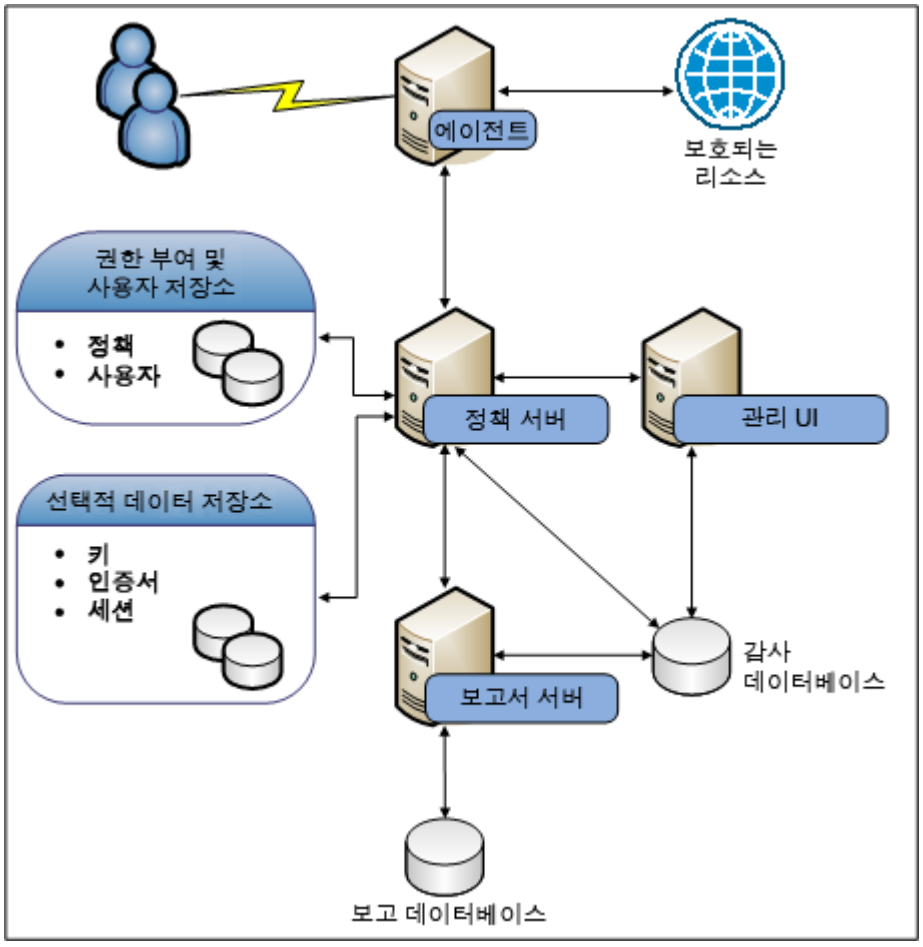
- 페더레이션 기반 기능을 구축할 계획인 경우에는 환경에 인증서 데이터 저장소와 세션 저장소가 필요합니다.
- 감사 기반 보고서를 작성할 계획인 경우에는 환경에 보고서 서버와 감사 데이터베이스가 필요합니다.

다음 다이어그램은 선택적 구성 요소와 이에 필요한 종속성을 보여 줍니다.

- 보고서 서버 하나
- 보고서 데이터베이스
- 감사 데이터베이스
- 키 저장소

- 세션 저장소
- 인증서 데이터 저장소

*그림 2: 선택적 구성 요소를 사용한 간단한 배포*




각 구성 요소에는 리소스 보호와 관련한 특정 역할이 있습니다.

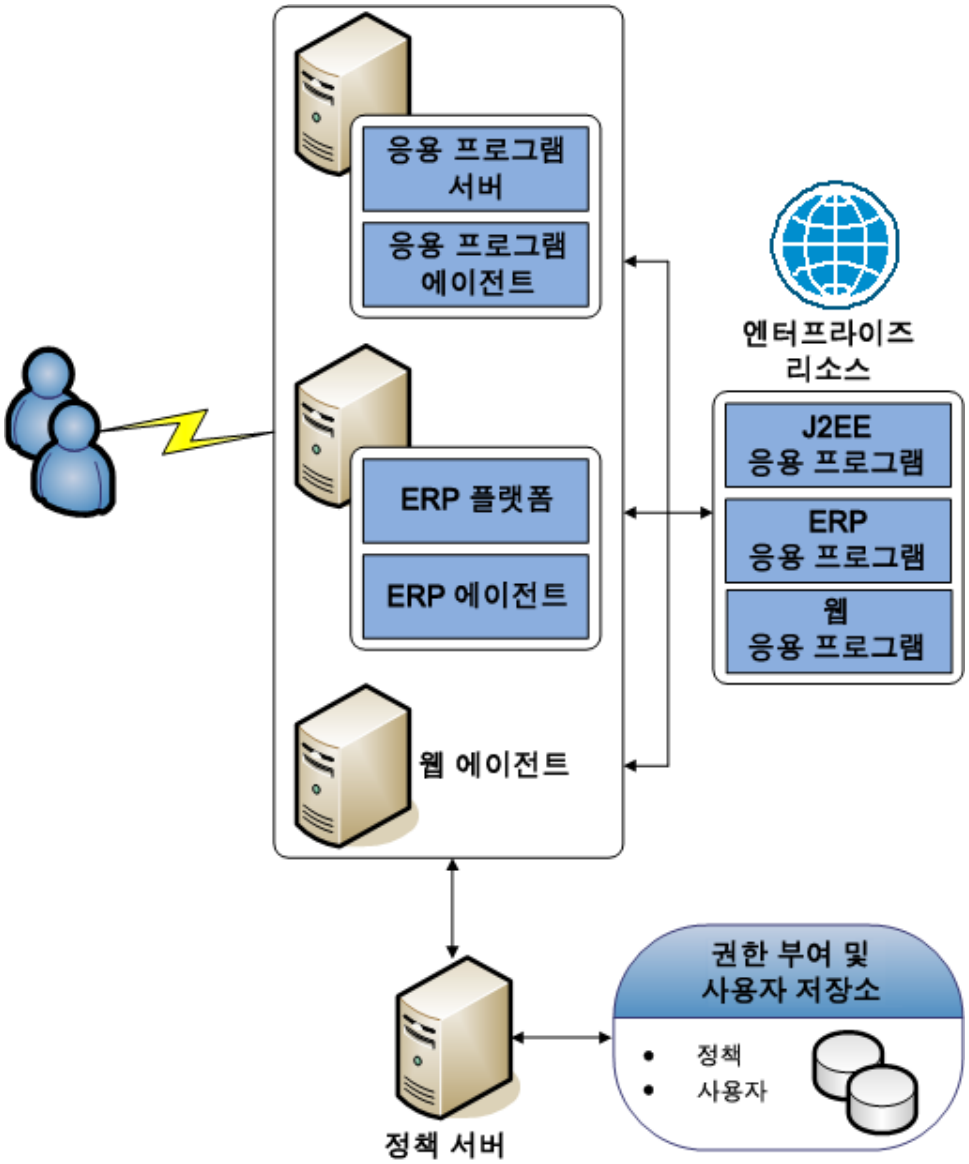
**참고:** 각 구성 요소의 주된 용도에 대한 자세한 내용은 "SiteMinder 구성 요소"를 참조하십시오.

## 선택적 에이전트를 사용한 간단한 배포

환경에서 간단한 배포의 기능을 확장하여 웹 서버에 있지 않은 리소스를 보호할 수 있습니다. 예를 들어 환경에서 리소스를 호스트하는 위치에 따라 다음과 같이 구분됩니다.

- 응용 프로그램 서버에서 리소스를 호스트하는 경우 응용 프로그램 서버 에이전트를 구현하여 리소스를 보호할 수 있습니다.
- ERP 시스템에서 리소스를 호스트하는 경우 ERP 에이전트를 구현하여 리소스를 보호할 수 있습니다.

다음 다이어그램에서는 선택적 에이전트를 보여 줍니다.




각 구성 요소마다 리소스 보호와 관련한 특정 역할이 있습니다.

**참고:** 각 구성 요소의 기본 용도에 대한 자세한 내용은 "SiteMinder 구성 요소"를 참조하십시오.

# 작업 연속성을 위한 다중 구성 요소

다음 사용 사례에서는 아래와 같은 방법을 사용하는 환경에 중복성과 장애 조치를 구축하기 위해 다중 구성 요소 블록을 구현하는 방법을 보여 줍니다.

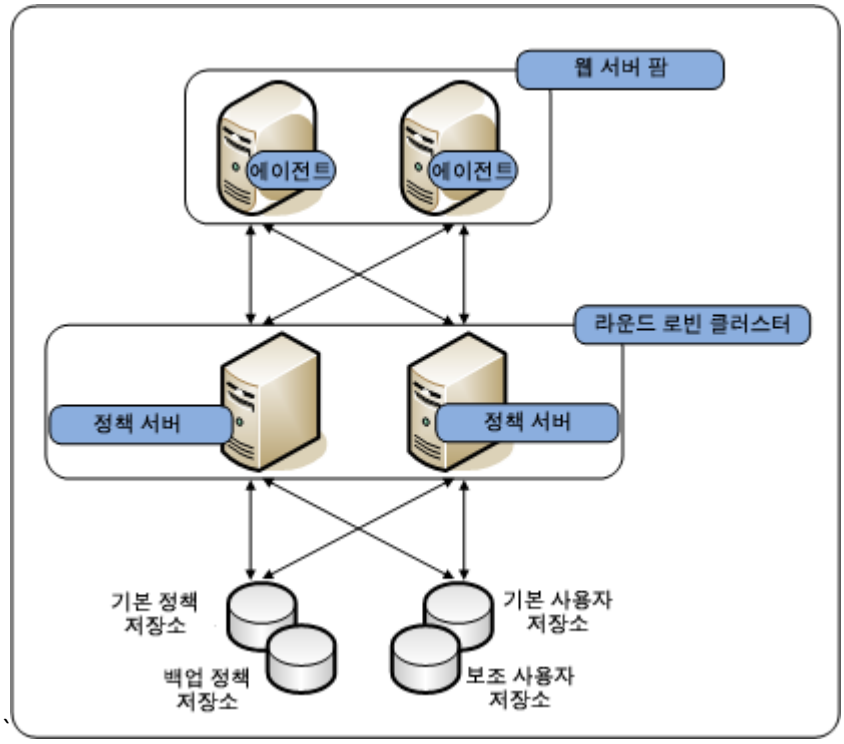
- SiteMinder 라운드 로빈 부하 분산
- 하드웨어 부하 분산 장치

## 작업 연속성을 위한 다중 구성 요소 - SiteMinder 부하 분산 사용

SiteMinder 라운드 로빈 부하 분산을 사용하는 환경에 중복성과 장애 조치를 구축하기 위해 다중 구성 요소 블록을 구현할 수 있습니다. 이 사용 사례에서는 간단한 배포 환경을 기반으로 작업 연속성 계획을 시작하는 방법을 설명합니다. 다음 다이어그램에서 보여 주는 항목은 아래와 같습니다.

- 사용자 요청을 가로채는 다중 에이전트 인스턴스. 그림에 나와 있는 것처럼, 각 에이전트는 기본 정책 서버에서 초기화와 통신을 수행하고 보조 정책 서버로 장애 조치되도록 구성됩니다.
- 액세스 제어 정책을 평가하고 적용하는 정책 서버 클러스터. 부하는 클러스터의 각 정책 서버 간에 동적으로 분산됩니다.
- 다중 사용자 저장소 연결. 각 정책 서버는 기본 사용자 저장소와 통신하도록 구성됩니다. 기본 사용자 저장소 연결은 보조 사용자 저장소 연결과 함께 구성됩니다. 정책 서버는 사용자 정보 요청의 부하를 두 연결 간에 분산시킵니다. 기본 연결을 사용할 수 없게 되면 정책 서버가 보조 연결로 장애 조치됩니다.

- 단일 정책 저장소 인스턴스. 각 정책 서버는 정책 정보의 공통 보기를 위해 동일한 정책 저장소에 연결합니다. 기본 정책 저장소 연결과 함께 정책 서버가 장애 조치될 수 있는 보조 연결이 구성됩니다.




각 구성 요소마다 리소스 보호와 관련한 특정 역할이 있습니다.

**참고:** 각 구성 요소의 주된 용도에 대한 자세한 내용은 "SiteMinder 구성 요소"를 참조하십시오. SiteMinder 중복성 및 고가용성에 대한 자세한 내용은 "중복성 및 고가용성"을 참조하십시오.

**추가 정보:**

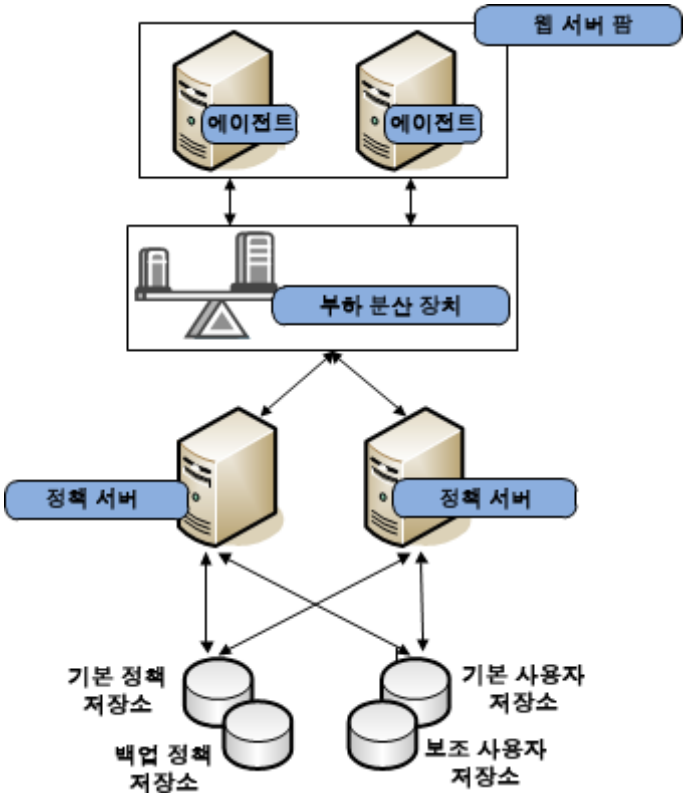
중복성 및 고가용성 (페이지 39)

## 작업 연속성을 위한 다중 구성 요소 - 하드웨어 부하 분산 사용

하드웨어 부하 분산을 사용하는 환경에 중복성과 장애 조치를 구축하기 위해 다중 구성 요소 블록을 구현할 수 있습니다. 이 사용 사례에서는 간단한 배포 환경을 기반으로 작업 연속성 계획을 시작하는 방법을 설명합니다. 다음 다이어그램에서 보여 주는 항목은 아래와 같습니다.

- 사용자 요청을 가로채는 다중 에이전트 인스턴스. 그림에 나와 있는 것처럼, 각 에이전트는 기본 정책 서버에서 초기화와 통신을 수행하고 보조 정책 서버로 장애 조치되도록 구성됩니다.
- 하드웨어 부하 분산 장치는 VIP(가상 IP 주소)를 통해 다중 정책 서버를 노출하도록 구성됩니다. 하드웨어 부하 분산 장치는 해당 VIP 에 연결된 모든 정책 서버 간에 동적으로 부하를 분산시킵니다.
- 액세스 제어 정책을 평가하고 적용하는 다중 정책 서버
- 다중 사용자 저장소 연결. 각 정책 서버는 기본 사용자 저장소와 통신하도록 구성됩니다. 기본 사용자 저장소 연결은 보조 사용자 저장소 연결과 함께 구성됩니다. 정책 서버는 사용자 정보 요청의 부하를 두 연결 간에 분산시킵니다. 기본 연결을 사용할 수 없게 되면 정책 서버가 보조 연결로 장애 조치됩니다.

- 단일 정책 저장소 인스턴스. 각 정책 서버는 정책 정보의 공통 보기를 위해 동일한 정책 저장소에 연결합니다. 기본 정책 저장소 연결과 함께 정책 서버가 장애 조치될 수 있는 보조 연결이 구성됩니다.




각 구성 요소마다 리소스 보호와 관련한 특정 역할이 있습니다.

**참고:** 각 구성 요소의 주된 용도에 대한 자세한 내용은 "SiteMinder 구성 요소"를 참조하십시오. SiteMinder 중복성 및 고가용성에 대한 자세한 내용은 "중복성 및 고가용성"을 참조하십시오.

**추가 정보:**

중복성 및 고가용성 (페이지 39)

## 확장을 위한 클러스터된 구성 요소

확장하여 처리량을 늘릴 때 높은 성능 수준을 유지할 수 있도록 추가 클러스터를 구현할 수 있습니다. 이 사용 사례에서는 작업 연속성을 위한 다중 구성 요소 사용 사례를 기반으로 확장 측면에서 아키텍처 계획을 시작하는 방법을 설명합니다.

다이어그램의 초기 배포 부분에서는 다음을 보여 줍니다.

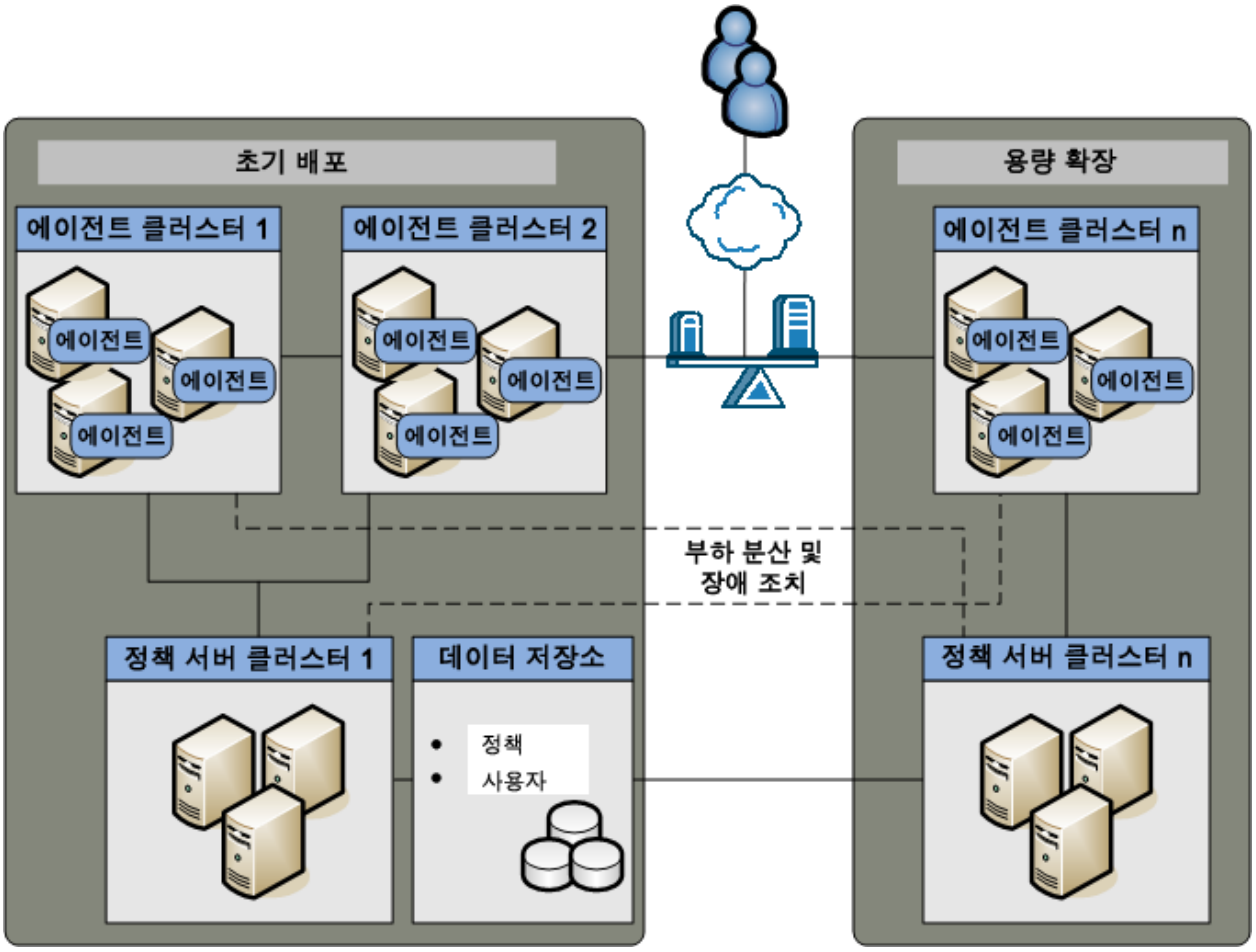
- 사용자 요청을 전체 다중 에이전트 클러스터에 분산시키는 부하 분산 장치
- 특정 응용 프로그램에 대한 사용자 요청을 가로채는 다중 에이전트 인스턴스. 에이전트는 클러스터의 기본 정책 서버에서 초기화와 통신을 수행하도록 구성됩니다. 클러스터에서 충분한 정책 서버를 사용할 수 없게 되면 에이전트가 다른 정책 서버 클러스터로 장애 조치됩니다.

  **참고:** 에이전트와 정책 서버의 중복성 및 고가용성에 대한 자세한 내용은 "중복성 및 고가용성"을 참조하십시오.
- 액세스 제어 정책을 평가하고 적용하는 정책 서버 클러스터. 부하는 클러스터의 각 정책 서버 간에 동적으로 분산됩니다.
- 다중 사용자 저장소 연결. 각 정책 서버는 기본 사용자 저장소에 연결되도록 구성됩니다. 기본 사용자 저장소 연결은 보조 사용자 저장소 연결과 함께 구성됩니다. 정책 서버는 사용자 정보 요청의 부하를 두 연결 간에 분산시킵니다. 기본 연결을 사용할 수 없게 되면 정책 서버가 보조 연결로 장애 조치됩니다.

  **참고:** 정책 서버와 사용자 저장소의 중복성 및 고가용성에 대한 자세한 내용은 "중복성 및 고가용성"을 참조하십시오.

- 단일 정책 저장소 인스턴스. 클러스터의 각 정책 서버는 정책 정보의 공통 보기를 위해 동일한 정책 저장소에 연결합니다. 기본 정책 저장소 연결과 함께 정책 서버가 장애 조치될 수 있는 보조 연결이 구성됩니다.

  **참고:** 정책 서버와 정책 저장소의 중복성에 대한 자세한 내용은 "중복성 및 고가용성"을 참조하십시오.




각 구성 요소마다 리소스 보호와 관련한 특정 역할이 있습니다.

**참고:** 각 구성 요소의 주된 용도에 대한 자세한 내용은 "SiteMinder 구성 요소"를 참조하십시오.

다이어그램의 용량 확장 부분에는 다른 구성 요소 블록이 나와 있으며 다음을 보여 줍니다.

- 요청을 새 에이전트 클러스터로 분산시키는 부하 분산 장치
- 사용자 요청을 가로채는 다중 에이전트 인스턴스. 각 에이전트는 클러스터 n 의 정책 서버에 연결되도록 구성될 뿐만 아니라 환경의 임의 정책 서버로 장애 조치되도록 구성됩니다. 점선으로 표시된 것처럼, 에이전트 클러스터 n 의 에이전트는 정책 서버 클러스터 1 의 정책 서버로 장애 조치되도록 구성됩니다.
- 액세스 제어 정책을 평가하고 적용하는 정책 서버 클러스터. 점선으로 표시된 것처럼, 각 정책 서버 클러스터에는 장애 조치 임계값이 구성됩니다. 사용 가능한 정책 서버의 수가 지정된 임계값 아래로 떨어지면 장애가 발생한 정책 서버가 서비스를 제공하지 못한 모든 요청이 다른 클러스터로 전달됩니다.

  **참고:** 정책 서버 클러스터의 장애 조치 임계값에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

**추가 정보:**

중복성 및 고가용성 (페이지 39)
작업 연속성을 위한 다중 구성 요소 - SiteMinder 부하 분산 사용 (페이지 33)
작업 연속성을 위한 다중 구성 요소 - 하드웨어 부하 분산 사용 (페이지 35)

## 중복성 및 고가용성

SiteMinder 구성 요소의 논리적 블록 간에 중복성 및 고가용성을 구성하여 시스템 가용성과 성능을 유지 관리할 수 있습니다.

### 에이전트와 정책 서버 간 통신

SiteMinder 에이전트를 구성하면 호스트 서버에 호스트 구성 파일(기본 이름: SmHost.conf)이 생성됩니다. 에이전트는 이 호스트 구성 파일의 연결 정보를 사용하여 정책 서버와의 초기 연결을 생성합니다.

초기 연결이 설정된 후 에이전트는 정책 서버의 HCO(호스트 구성 개체)에서 후속 정책 서버 연결 정보를 가져옵니다.

다중 정책 서버를 포함하도록 HCO 를 구성하고 에이전트가 다중 정책 서버 간에 요청을 분산시키기 위해 사용하는 방법을 지정할 수 있습니다.

SiteMinder 에이전트는 다음과 같은 방식으로 다중 정책 서버 간에 요청을 분산시킬 수 있습니다.

- 장애 조치
- 라운드 로빈 부하 분산
- 하나 이상의 정책 서버 클러스터에 대한 라운드 로빈 부하 분산

또는, 하드웨어 부하 분산 장치에 구성되어 있으며 다중 정책 서버를 노출하는 단일 가상 IP 주소를 포함하도록 HCO 를 구성할 수도 있습니다. 이 경우 에이전트 소프트웨어 대신 부하 분산 장치가 장애 조치 및 부하 분산을 담당합니다.

**추가 정보:**

SiteMinder 에이전트 (페이지 14)

## 장애 조치

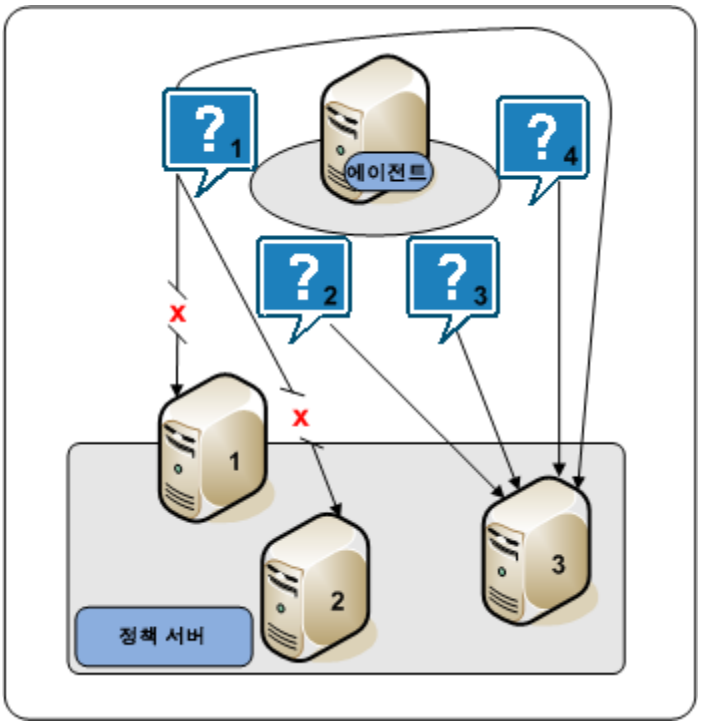
장애 조치는 기본 HCO 설정입니다. 장애 조치 모드에서 SiteMinder 에이전트는 HCO 가 나열되는 첫 번째 정책 서버로 모든 요청을 전송하고 다음과 같이 진행합니다.

1. 첫 번째 정책 서버가 응답하지 않으면 에이전트는 이를 사용할 수 없는 것으로 간주하고 요청을 리디렉션합니다. 그리고 이후의 모든 요청은 HCO 가 나열하는 다음 정책으로 리디렉션합니다.
2. 처음 두 개의 정책 서버가 응답하지 않으면 에이전트는 둘 다 사용할 수 없는 것으로 간주하고 요청을 리디렉션합니다. 그리고 이후의 모든 요청은 HCO 가 나열하는 다음 정책으로 리디렉션합니다.

**참고:** 여러 정책 서버를 사용하여 HCO 를 구성하는 방법에 대해서는 *정책 서버 구성 안내서*를 참조하십시오.

응답하지 않는 정책 서버가 복구되면(에이전트가 주기적으로 폴링하여 확인함) 정책 서버는 자동으로 HCO 목록의 원래 위치로 돌아가서 모든 에이전트 요청을 수신하기 시작합니다.

다음 다이어그램은 에이전트 장애 조치 프로세스를 보여 줍니다.




## 라운드 로빈 부하 분산

라운드 로빈 부하 분산은 선택적 HCO 설정입니다. 라운드 로빈 부하 분산은 요청을 정책 서버 집합 전체에 균등하게 분산시키므로

- 사용자 인증 및 권한 부여가 더 효율적으로 수행됩니다.
- 에이전트 요청으로 인하여 하나의 정책 서버에 과부하가 발생하는 일이 방지됩니다.

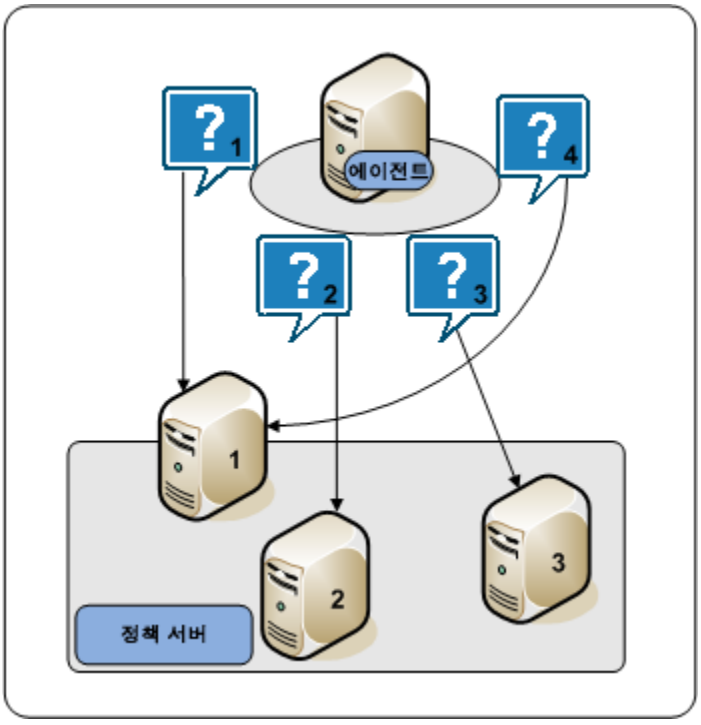
**참고:** HCO 를 라운드 로빈 부하 분산을 위해 구성하는 방법에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

라운드 로빈 모드에서 에이전트는 요청을 HCO 가 나열하는 모든 정책 서버에 분산시킵니다. 에이전트는 다음을 수행합니다.

1. HCO 가 나열하는 첫 번째 정책 서버로 요청을 전송합니다.
2. HCO 가 나열하는 두 번째 정책 서버로 요청을 전송합니다.
3. HCO 가 나열하는 세 번째 정책 서버로 요청을 전송합니다.
4. 에이전트는 사용 가능한 모든 정책 서버로 요청을 전송할 때까지 계속해서 이러한 방식으로 요청을 전송합니다. 사용 가능한 모든 정책 서버로 요청을 전송한 후에 에이전트는 첫 번째 정책 서버로 돌아가서 주기를 다시 시작합니다.

정책 서버가 응답하지 않으면 에이전트는 HCO 가 나열하는 다음 정책 서버로 요청을 리디렉션합니다. 응답하지 않는 정책 서버가 복구되면(에이전트가 주기적으로 폴링하여 확인함) 정책 서버는 자동으로 HCO 목록의 원래 위치로 돌아갑니다.

다음 다이어그램은 라운드 로빈 프로세스를 보여 줍니다.



## 정책 서버 클러스터

라운드 로빈 부하 분산은 SiteMinder 에이전트 요청을 HCO 가 나열하는 모든 정책 서버로 균등하게 분산시킵니다. 이는 시스템 가용성과 응답 시간을 향상시키는 효율적인 방법이지만 다음을 고려해야 합니다.

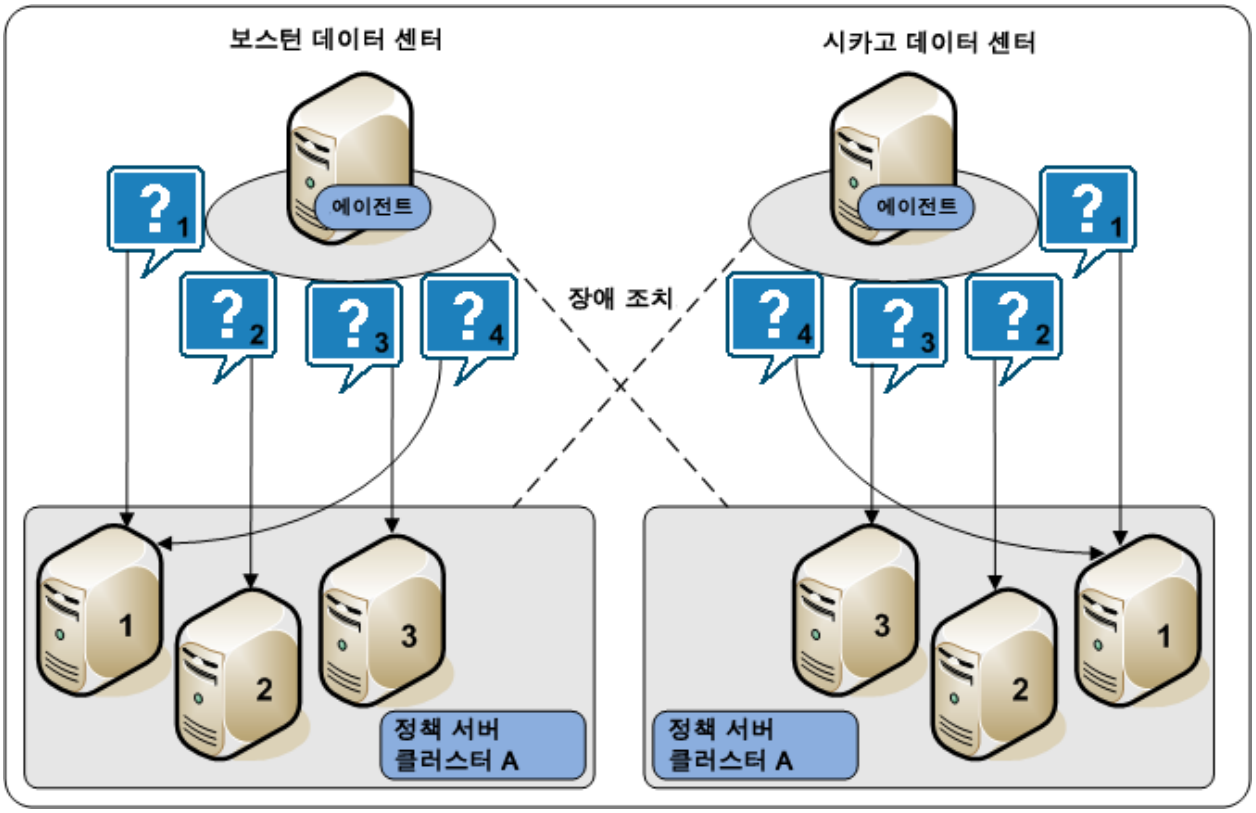
- 라운드 로빈 부하 분산은 컴퓨팅 용량이 서로 다른 이종 환경에서는 가장 효율적인 분배 방법이 아닙니다. 각 정책 서버는 용량에 관계없이 동일한 수의 요청을 받게 됩니다.
- 다른 지리적 위치에 있는 정책 서버로 라운드 로빈 부하 분산을 수행하면 성능이 저하될 수 있습니다. 특정 로캘 외부에 있는 정책 서버로 에이전트 요청을 전송하면 네트워크 통신 오버헤드 및 네트워크 경합이 증가할 수 있습니다.

정책 서버 클러스터는 에이전트가 요청을 분산시킬 수 있는 정책 서버 그룹입니다. 정책 서버 클러스터는 라운드 로빈 부하 분산에 대하여 다음과 같은 이점을 제공합니다.

- 클러스터에 특정 데이터 센터의 정책 서버만 포함되도록 구성할 수 있습니다. 고유한 정책 서버 클러스터를 사용하여 에이전트를 그룹화하면 지리적으로 분산된 여러 지역으로 부하를 분산시킬 때 발생하는 네트워크 오버헤드를 방지할 수 있습니다. 네트워크 오버헤드는 에이전트가 다른 정책 서버 클러스터로 장애 조치될 때만 발생합니다.
- 클러스터를 정책 서버 장애 조치 임계값에 기반하여 다른 클러스터로 장애 조치할 수 있습니다.
- 에이전트가 요청을 균등하게 분산시키는 대신 응답 시간에 기반하여 모든 정책 서버에 동적으로 분산시킵니다.

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

다음 다이어그램은 두 개의 정책 서버 클러스터를 보여 줍니다. 각 클러스터는 라운드 로빈 부하 분산과 관련될 수 있는 네트워크 오버헤드를 피하기 위해 지리적으로 분리되어 있습니다.

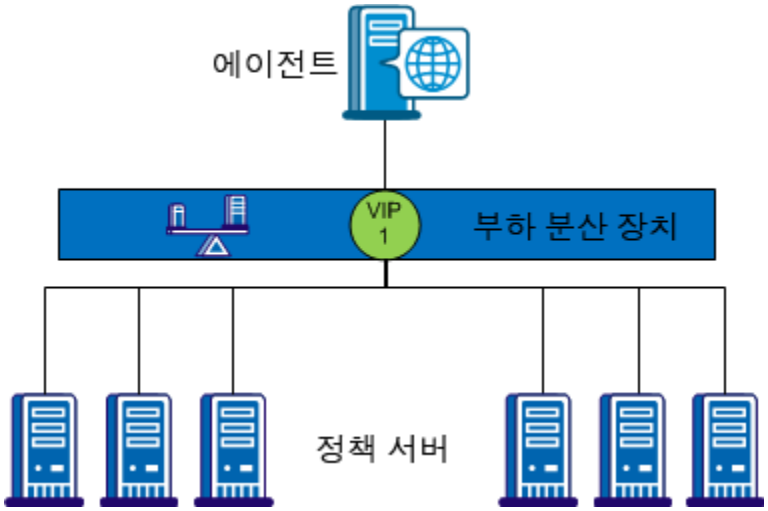



## 하드웨어 부하 분산

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

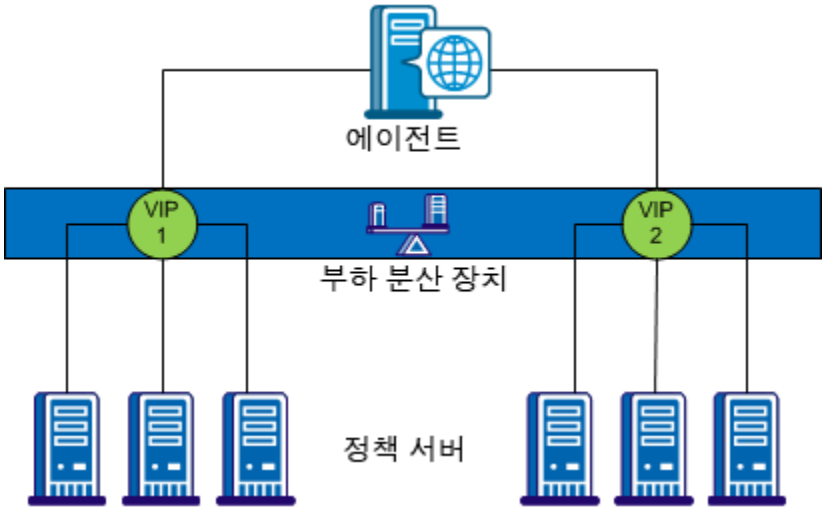
- 단일 VIP 와 VIP 별로 노출되는 다중 정책 서버
- 다중 VIP 와 VIP 별로 노출되는 다중 정책 서버

**단일 VIP, VIP 별 다중 정책 서버**




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

**다중 VIP, VIP 별 다중 정책 서버**



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

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

## 정책 서버에서 사용자 저장소로의 통신

정책 서버는 다음을 사용하기 위해 쿼리를 여러 LDAP 또는 ODBC 사용자 저장소로 분산시킬 수 있습니다.

- 장애 조치
- 라운드 로빈 부하 분산

**참고:** 사용자 저장소 연결 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

**추가 정보:**

사용자 저장소 (페이지 17)

## 장애 조치

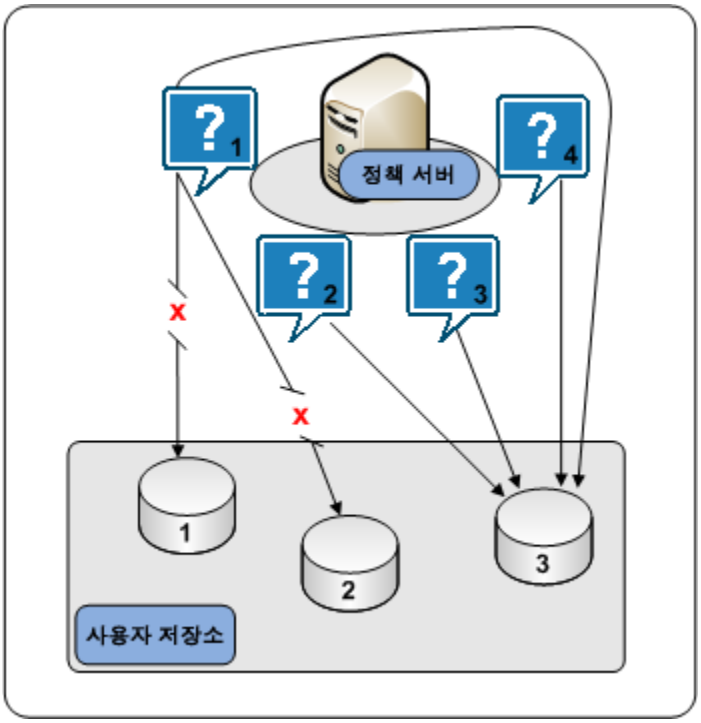
장애 조치는 SiteMinder 사용자 저장소 개체의 선택적 설정입니다. 장애 조치 모드에서 정책 서버는 모든 요청을 기본 사용자 저장소로 분산시키고 다음과 같이 처리합니다.

1. 기본 사용자 저장소가 응답하지 않으면 정책 서버는 이를 사용할 수 없는 것으로 간주하고 요청을 리디렉션합니다. 그리고 이후의 모든 요청을 SiteMinder 사용자 저장소 개체가 나열하는 다음 사용자 저장소로 리디렉션합니다.
2. 첫 번째 및 두 번째 사용자 저장소가 응답하지 않으면 정책 서버는 둘 다 사용할 수 없는 것으로 간주하고 요청을 리디렉션합니다. 그리고 이후의 모든 요청을 SiteMinder 사용자 저장소 개체가 나열하는 다음 사용자 저장소로 리디렉션합니다.

**참고:** 사용자 저장소 장애 조치 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

응답하지 않는 사용자 저장소가 복구되면 사용자 저장소가 자동으로 장애 조치 목록의 원래 위치로 돌아가고 모든 정책 서버 요청을 수신하기 시작합니다.

다음 다이어그램은 사용자 저장소 장애 조치 프로세스를 보여 줍니다.



## 라운드 로빈 부하 분산

라운드 로빈 부하 분산은 선택적 SiteMinder 사용자 저장소 개체 설정입니다. 라운드 로빈 부하 분산은 요청을 사용자 저장소 집합 전체에 균등하게 분산시키므로 다음과 같은 효과가 있습니다.

- 사용자 저장소 쿼리의 효율성이 향상됩니다.
- 단일 사용자 저장소가 정책 서버 요청으로 인해 오버로드되는 것을 방지합니다.

**참고:** 다음 사항을 고려하십시오.

- LDAP 사용자 저장소 간의 부하 분산 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.
- 관리 UI 에는 ODBC 사용자 저장소 간의 라운드 로빈 부하 분산을 구성하기 위한 설정이 포함되어 있지 않습니다. 하지만 정책 서버 설치에는 다음이 포함됩니다.
  - SiteMinder Oracle 유선 프로토콜. 이 프로토콜은 여러 Oracle 저장소에 대한 부하 분산을 지원합니다. 데이터 원본 수준에서 Oracle 사용자 저장소 부하 분산을 구성할 수 있습니다.
  - SiteMinder SQL Server 유선 프로토콜. 이 프로토콜은 SQL Server 또는 SQL Server Cluster Enterprise 를 구성하기 위해 사용할 수 있습니다. 데이터베이스 수준에서 SQL Server 사용자 저장소 부하 분산을 구성할 수 있습니다.

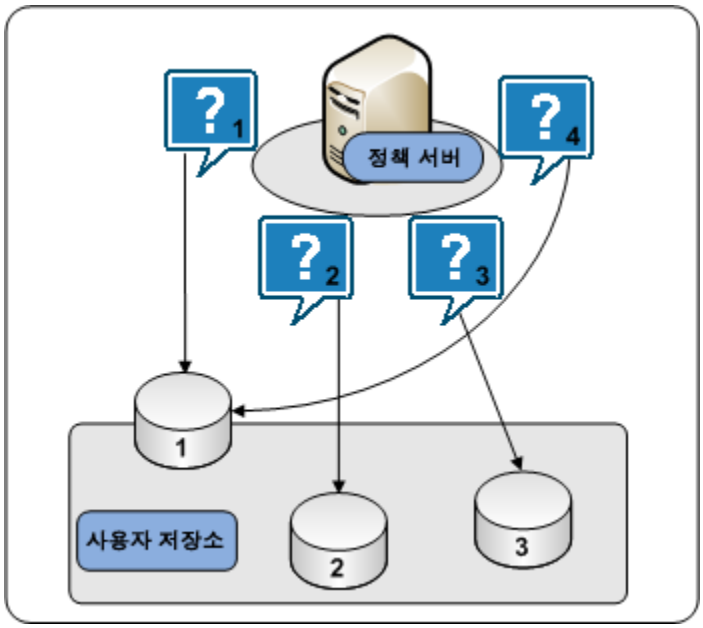
라운드 로빈 모드에서 정책 서버는 요청을 SiteMinder 사용자 저장소 개체가 나열하는 모든 사용자 저장소로 분산시킵니다. 정책 서버는 다음을 수행합니다.

1. 사용자 저장소 개체가 나열하는 첫 번째 사용자 저장소로 요청을 전송합니다.
2. 사용자 저장소 개체가 나열하는 두 번째 사용자 저장소로 요청을 전송합니다.
3. 사용자 저장소 개체가 나열하는 세 번째 사용자 저장소로 요청을 전송합니다.

4. 정책 서버는 사용 가능한 모든 정책 서버로 요청을 전송할 때까지 계속해서 이러한 방식으로 요청을 전송합니다. 사용 가능한 모든 사용자 저장소로 요청을 전송한 후에 정책 서버는 첫 번째 사용자 저장소로 돌아가서 주기를 다시 시작합니다.

**참고:** 사용자 저장소가 실패할 경우 중복성의 이점을 추가하는 장애 조치를 포함하여 부하 분산을 구성하십시오. 부하 분산 및 장애 조치 구성에 대한 자세한 내용은 정 *책*서버 구성 안내서를 참조하십시오.

다음 다이어그램은 사용자 저장소 라운드 로빈 프로세스를 보여 줍니다.




## 정책 서버에서 정책 저장소로의 통신

정책 정보에 대한 공통의 뷰를 위해 모든 정책 서버가 동일한 정책 저장소에 연결되어야 합니다. 하지만 배포에는 정책 서버가 장애 조치할 수 있는 여러 개의 "핫" 정책 저장소가 포함되는 것이 좋습니다.

다음은 정책 저장소 장애 조치 시나리오입니다.

- 복제된 버전과 함께 구성된 마스터 정책 저장소
- 다중 마스터 정책 저장소

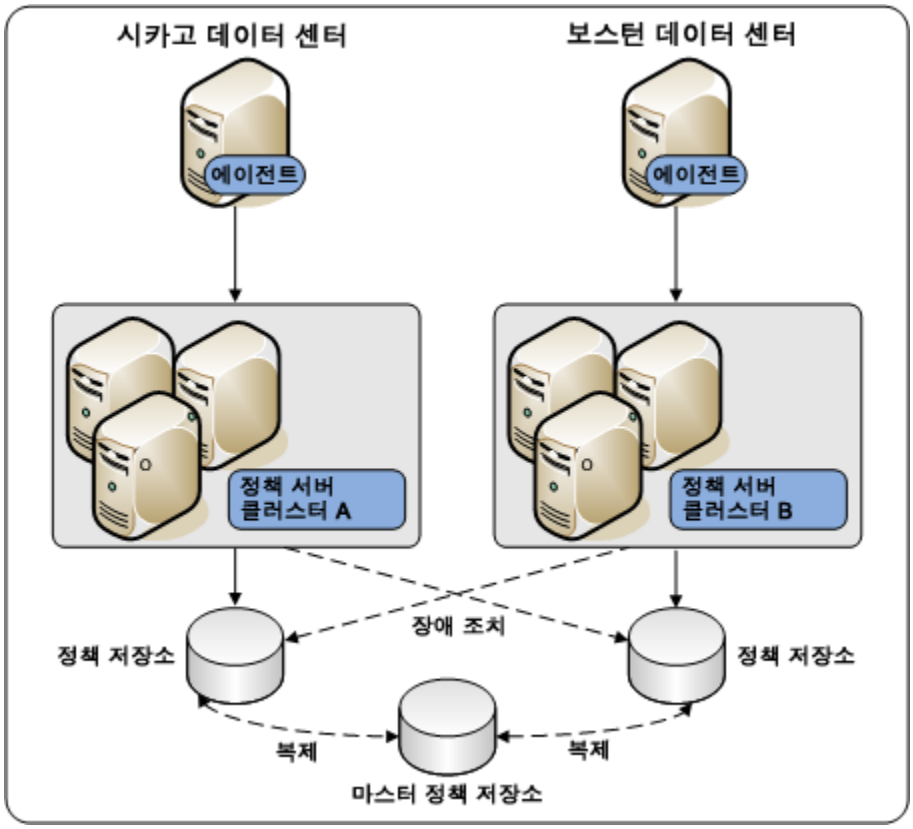
## 마스터 정책 저장소

마스터 정책 저장소를 복제된 버전과 함께 배포하면 정책 저장소의 중복성을 구현할 수 있습니다. 단일 마스터 정책 저장소를 통해 각 정책 서버는 가장 가까운 복제된 버전과 통신할 수 있습니다. 이러한 통신 방법의 특성은 다음과 같습니다.

- 지리적으로 분산된 정책 서버의 성능을 향상시킵니다. 정책 서버 요청을 특정 로캘 외부의 정책 저장소로 보내면 네트워크 통신 오버헤드 및 네트워크 경합이 증가할 수 있습니다.
- 장애 조치를 허용합니다. 기본 정책 저장소가 실패하면 정책 서버가 보조 저장소로 장애 조치됩니다.

**참고:** 복제 구성에 대한 자세한 내용은 해당 공급업체의 설명서를 참조하십시오. 정책 저장소 장애 조치 구성에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

다음 다이어그램은 단일 마스터 정책 저장소 환경을 보여 줍니다.



## 다중 마스터 정책 저장소

다중 마스터 기술을 사용하여 LDAP 디렉터리를 배포하면 정책 저장소 중복성을 구현할 수 있습니다. 다중 마스터 정책 저장소를 통해 각 정책 서버는 가장 가까운 복제된 버전과 통신할 수 있습니다. 이러한 통신 방법의 특성은 다음과 같습니다.

- 지리적으로 분산된 정책 서버의 성능을 향상시킵니다. 정책 서버 요청을 특정 로캘 외부의 정책 저장소로 보내면 네트워크 통신 오버헤드 및 네트워크 경합이 증가할 수 있습니다.
- 장애 조치를 허용합니다. 기본 정책 저장소가 실패하면 정책 서버가 보조 저장소로 장애 조치됩니다.

다중 마스터 모드에서 LDAP 정책 저장소를 구성할 때는 다음과 같은 구성이 권장됩니다.

- 모든 관리에 단일 마스터를 사용해야 합니다.
- 키 저장소에 단일 마스터를 사용해야 합니다.

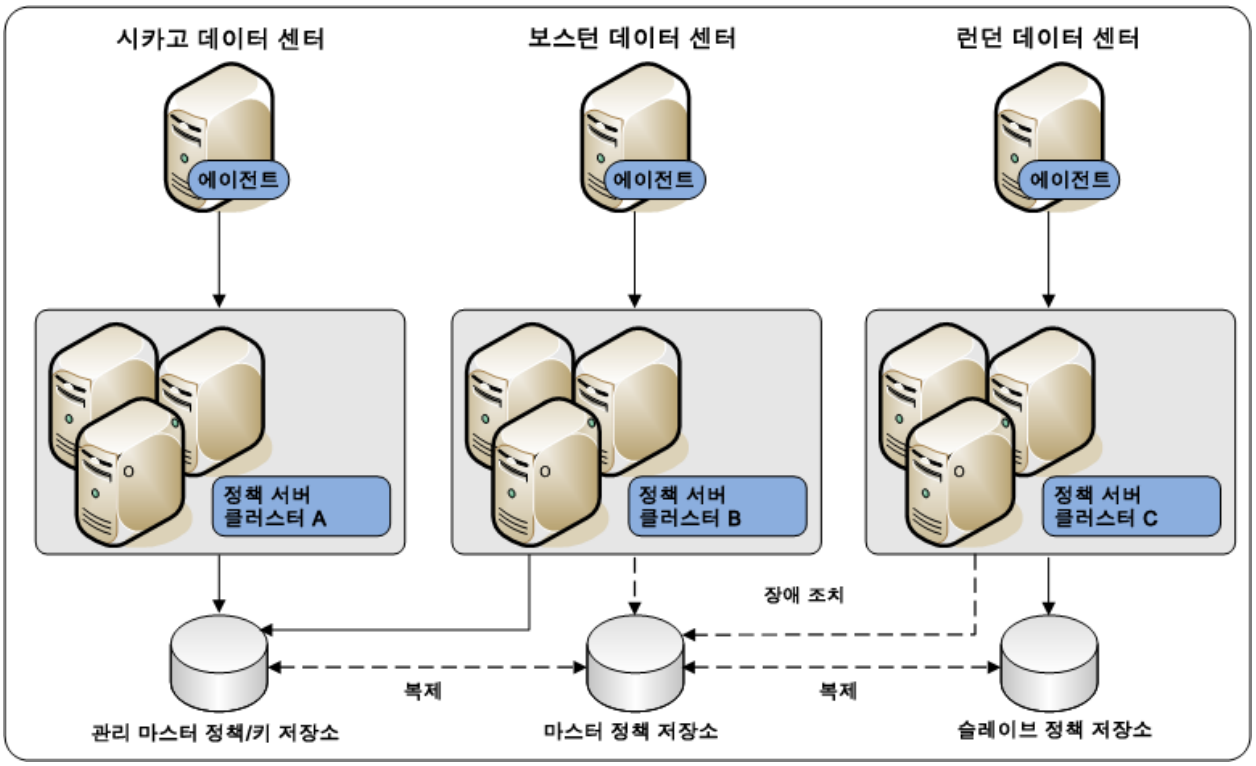
  이 마스터는 관리에 사용되는 마스터와 동일하지 않아도 됩니다. 그러나 키와 관리 모두에 동일한 마스터 저장소를 사용하는 것이 좋습니다. 이 구성에서 모든 키 저장소 노드는 복제본이 아니라 마스터에 연결되어야 합니다.

  **참고:** 키 저장소에 관리용 마스터와는 다른 마스터를 사용하는 경우 모든 키 저장소에서 동일한 키 저장소 값을 사용해야 합니다. 키 저장소가 정책 저장소와 키 저장소의 역할을 모두 담당하도록 구성하면 안 됩니다.
- 다른 모든 정책 저장소 마스터는 장애 조치 모드용으로 설정되어야 합니다.

다른 구성에서는 동기화 문제가 발생할 수 있으므로 정책 저장소가 손상되거나 에이전트 키가 동기화되지 않는 등의 일관되지 않은 결과를 초래할 수 있습니다.

다른 구성과 관련한 지원은 SiteMinder 지원부에 문의하십시오.

다음 다이어그램은 다중 마스터 정책 저장소 환경을 보여 줍니다.



## 정책 서버에서 감사 저장소로의 통신

기본적으로 각 정책 서버는 감사 정보를 텍스트 파일에 저장합니다. 이 텍스트 파일을 정책 서버 로그라고 합니다. 감사 데이터를 데이터베이스에 직접 로깅하도록 정책 서버를 구성할 수 있습니다.

SiteMinder 감사 로그는 일반적으로 감사 및 규정 준수의 용도로 사용됩니다. 다음 사항을 고려하십시오.

- 중앙에서 모든 데이터를 한 번에 쿼리할 수 있도록 모든 정책 서버가 중앙화된 감사 저장소에 쓰도록 구성하는 것이 좋습니다. 중앙화된 감사 저장소를 배포할 경우에는 고가용성 배포를 사용하는 것이 좋습니다.

  **참고:** 감사 저장소 구성에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오. 장애 조치 구성에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

  **중요!** 동기 감사를 사용하는 경우에는 감사 저장소 중단으로 인해 모든 정책 서버 인증과 권한 부여가 중지되는 것을 방지하도록 장애 조치를 구성하는 것이 좋습니다. 정책 서버는 레코드가 감사 데이터베이스에 저장되기 전에는 에이전트 인증 및 권한 부여 요청의 결과를 반환하지 않습니다. 레코드가 저장되기 전에는 사용자가 인증되거나 권한을 부여받지 않습니다. 장애 조치 구성에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

- 배포에서 정책 서버가 중앙화된 감사 저장소에 쓰는 것을 허용하지 않는 경우에는 smauditimport 유틸리티를 사용하여 개별 정책 서버 로그를 중앙화된 감사 저장소로 가져올 수 있습니다.

  **참고:** 정책 서버 로깅 및 smauditimport 도구에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

**추가 정보:**

SiteMinder 감사 데이터베이스 (페이지 20)

## 정책 서버에서 세션 저장소로의 통신

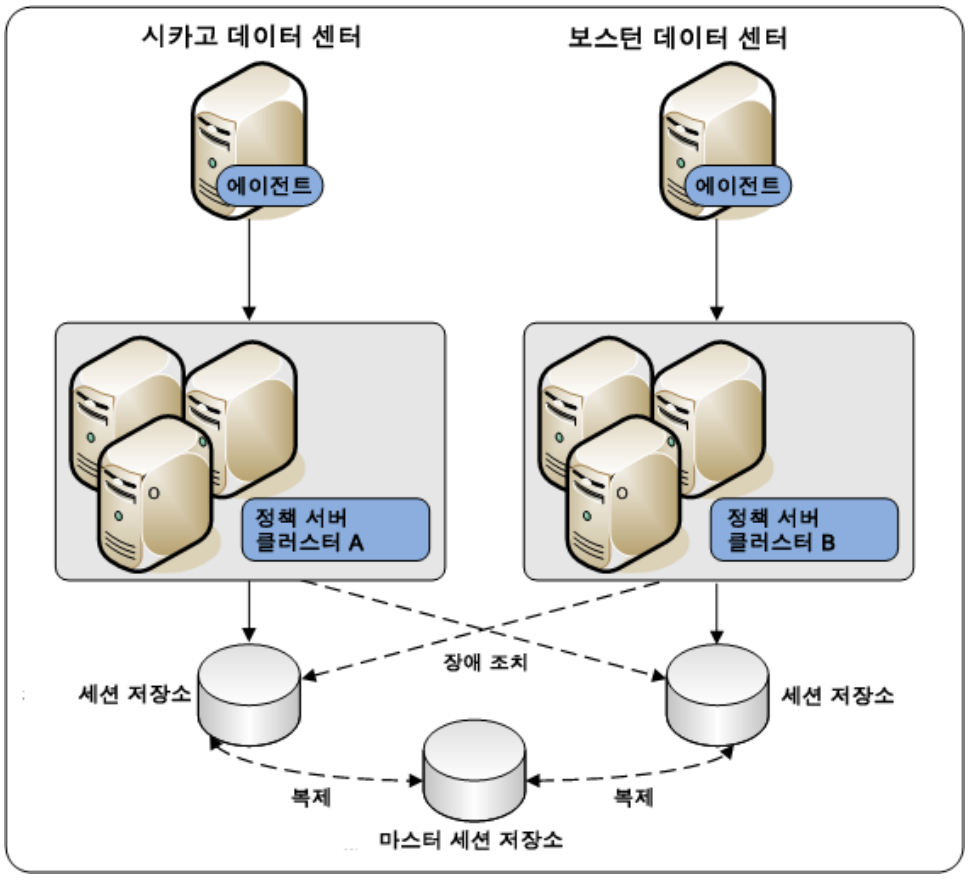
세션 저장소를 배포하는 경우 환경의 모든 정책 서버는 동일한 세션 저장소 데이터베이스를 사용해야 합니다.

마스터 세션 저장소를 배포하면 세션 저장소 중복성을 구현할 수 있습니다. 마스터 세션 저장소를 통해 각 정책 서버는 가장 가까운 복제된 버전과 통신할 수 있습니다. 이러한 통신 방법의 특성은 다음과 같습니다.

- 지리적으로 분산된 정책 서버의 성능을 향상시킵니다. 정책 서버 요청을 특정 로캘 외부의 중앙화된 세션 저장소로 보내면 네트워크 통신 오버헤드 및 네트워크 경합이 증가할 수 있습니다.
- 장애 조치를 허용합니다. 기본 세션 저장소가 실패하면 정책 서버가 보조 세션 저장소로 장애 조치됩니다.

**참고:** 복제 구성에 대한 자세한 내용은 해당 공급업체의 설명서를 참조하십시오. 세션 저장소 장애 조치 구성에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

다음 다이어그램은 세션 저장소에 대한 공통의 뷰를 공유하는 모든 정책 서버를 보여 줍니다.




**추가 정보:**

세션 저장소 (페이지 21)

# 고급 세션 보증 아키텍처와 성능 고려 사항

고급 세션 보증 기능은 세션 가로채기와 재생을 방지합니다. 사용자가 로그인할 때 최종 사용자 장치에 대한 지문을 생성하도록 DeviceDNA™ 확인이 수행됩니다. 기본적으로 5 분 간격으로 지문을 생성하고 새 지문과 로그인 중에 생성된 원래 지문을 비교하여 장치를 확인합니다.

초기 지문 생성 및 이후의 재확인 작업으로 인해 SiteMinder 아키텍처의 필요성이 커지고 있습니다. 특히, 고급 세션 보증 흐름 응용 프로그램을 실행하는 SiteMinder 정책 서버와 CA SiteMinder for Secure Proxy Server 인스턴스에 영향을 줍니다. 지문 재확인이 필요한 경우 리소스에 대한 액세스 권한을 부여하는 데 걸리는 시간이 늘어나는 것처럼 사용자 인증에 걸리는 시간도 늘어납니다. 인증하는 동안 늘어나는 실제 지연 시간은 네트워크 연결 속도, 서버 용량, 최종 사용자 장치 등 여러 가지 요인에 의해 결정되며 그 밖의 다른 요인도 영향을 미칩니다. 내부 테스트에 따르면, 고급 세션 보증이 구성된 응용 프로그램의 인증 지연 시간은 60%까지 증가할 수 있습니다. DeviceDNA™ 수집 및 계산에서 추가적인 리디렉션이 발생하고 처리 시간이 늘어나기 때문입니다. 각 환경에서 실제 증가 비율은 현재 인증 지연 시간, 네트워크, 리소스에 액세스하는 컴퓨터의 속도에 따라 달라집니다. 또한 고급 세션 보증 트랜잭션에서 고급 세션 보증을 사용하지 않는 경우 이 트랜잭션에 참여하는 SiteMinder 제품군 구성 요소를 호스트하는 시스템의 리소스 소비(예: CPU 사용률)가 높아집니다.

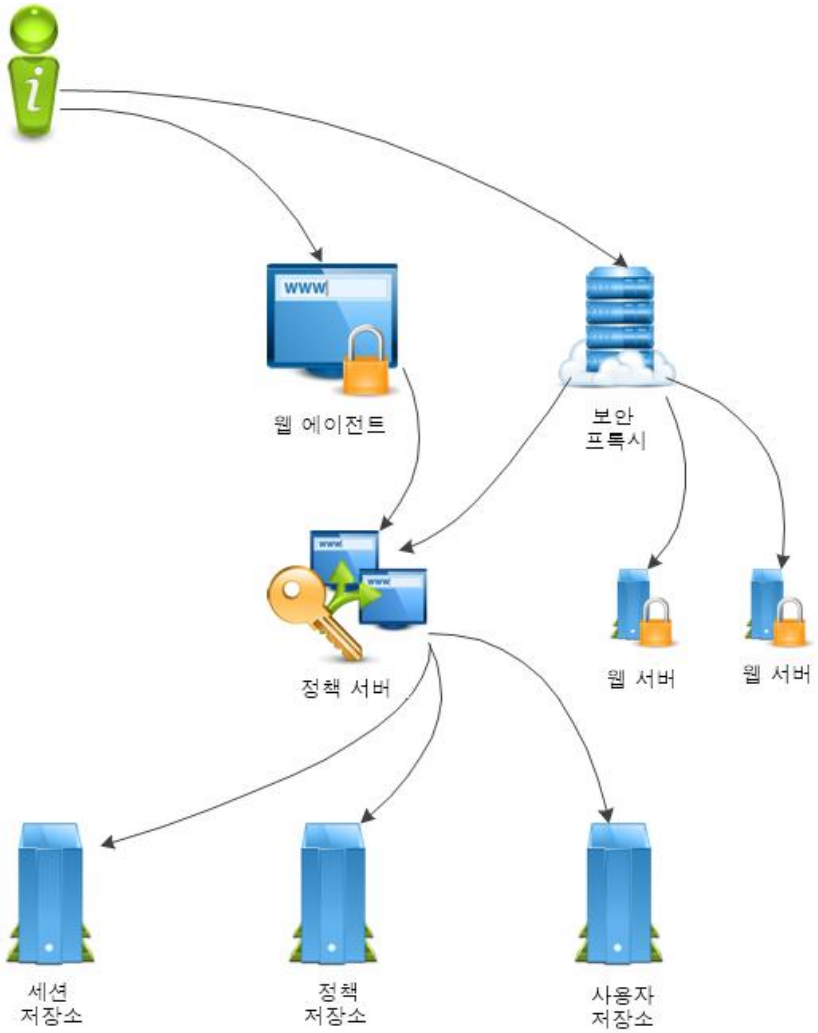
DeviceDNA 확인을 구동하는 응용 프로그램은 CA SiteMinder for Secure Proxy Server 인스턴스에서 호스트됩니다. 이러한 인스턴스는 웹 프록시 등의 표준 CA SiteMinder for Secure Proxy Server 기능 또는 SAML 페더레이션 기능을 수행하는 CA SiteMinder for Secure Proxy Server 인스턴스이거나 고급 세션 보증 트랜잭션 처리를 전담하는 별도의 독립 실행형 CA SiteMinder for Secure Proxy Server 인스턴스일 수 있습니다. CA SiteMinder for Secure Proxy Server 플랫폼의 성능도 초당 인증 및 권한 부여 트랜잭션 수, 현재 환경 내 인증 대비 권한 부여의 비율, 사용자 세션의 길이, 재확인 빈도 등의 요인과 그 밖의 다양한 요인에 의해 결정됩니다.

이 단원에서는 SiteMinder 고급 세션 보증 기능을 배포하는 데 사용할 수 있는 여러 가지 아키텍처를 소개하고, 해당 환경에서 이 기능을 사용하지 않는 기존 SiteMinder 응용 프로그램에 미치는 성능 영향을 최소화하는 몇 가지 옵션에 대해 설명합니다.

배포하려고 선택한 아키텍처에 관계없이 고급 세션 보증을 단계적으로 도입하는 것이 매우 중요합니다. 가장 좋은 방법은 이 기능을 개발 환경에서 설치한 후 다양한 응용 프로그램 또는 영역에 대해 단계적으로 사용하도록 설정하고 해당 환경에 미치는 성능 영향을 측정하면서 테스트하는 것입니다.

## 기본 아키텍처

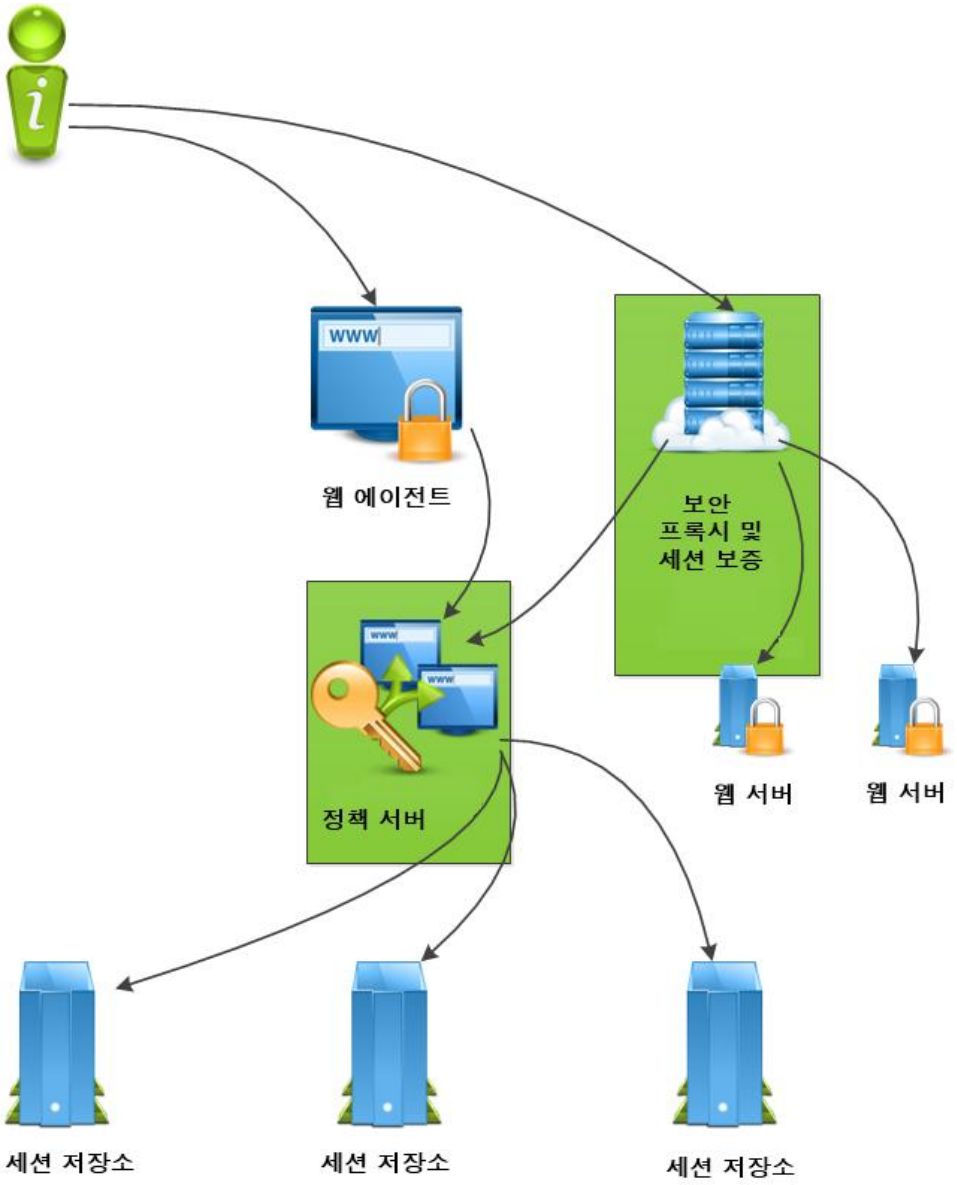
다음 다이어그램에서는 고급 세션 보증을 사용하지 않는 간략한 기본 SiteMinder 아키텍처 다이어그램을 보여 줍니다.




이 아키텍처에서는 웹 에이전트와 CA SiteMinder for Secure Proxy Server 를 모두 사용하여 다른 웹 응용 프로그램에 대한 프록시 연결을 구성합니다.

## 가능한 아키텍처 1 - 기존 구성 요소 사용

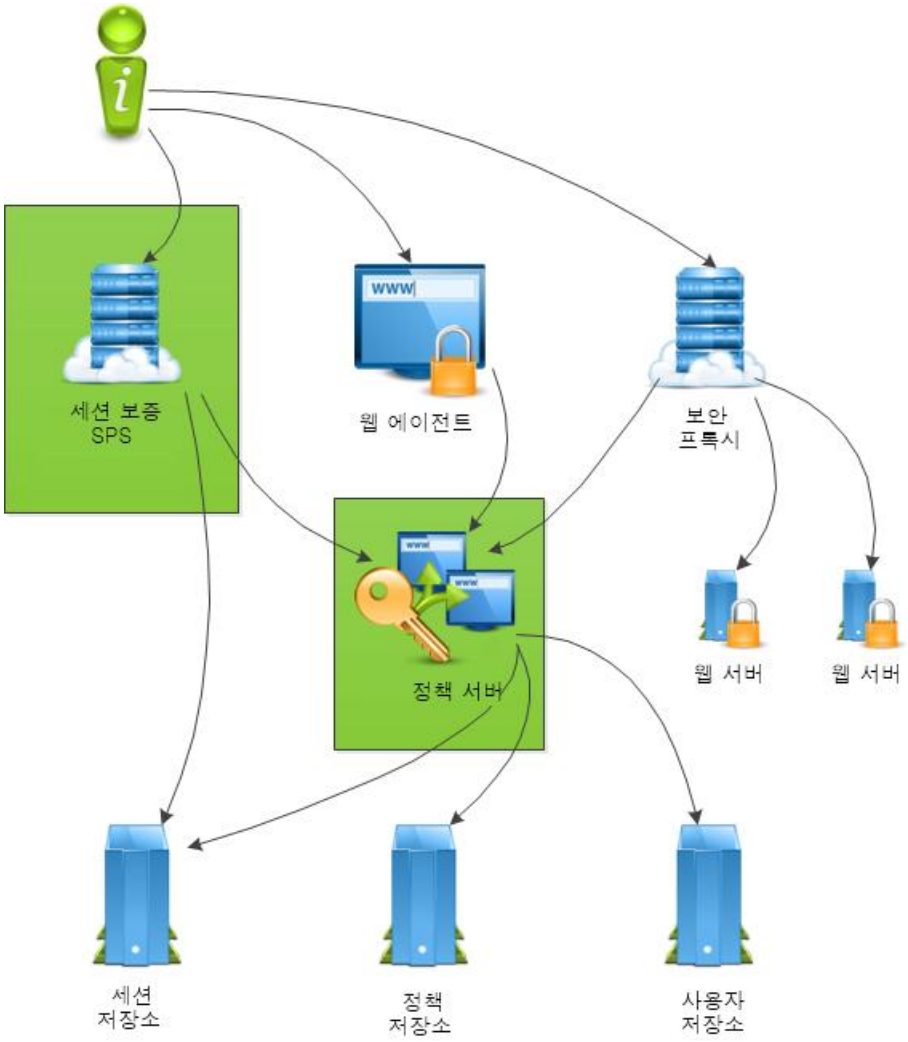
다음 다이어그램에서는 기존 구성 요소를 사용하여 고급 세션 보증을 배포하는 SiteMinder 아키텍처를 보여 줍니다.



이 아키텍처에서 녹색으로 표시된 정책 서버와 CA SiteMinder for Secure Proxy Server 를 고급 세션 보증에 사용할 수 있습니다. 기존 정책 서버와 CA SiteMinder for Secure Proxy Server 를 사용하면 이 기능을 배포하는 데 추가 하드웨어가 필요하지 않습니다. 하지만 이 아키텍처에서는 고급 세션 보증의 로드가 증가할 때 정책 서버 및 CA SiteMinder for Secure Proxy Server 의 CPU 사용률이 증가합니다. 두 구성 요소 중 하나의 스레드가 완전히 사용되거나 CPU 가 로드를 감당할 수 없을 때까지 로드가 증가하면 모든 SiteMinder 트랜잭션은 해당 트랜잭션이 고급 세션 보증을 사용하도록 구성되었는지 여부에 관계없이 부정적인 영향을 받게 됩니다.

## 가능한 아키텍처 2 - 기존 정책 서버 사용

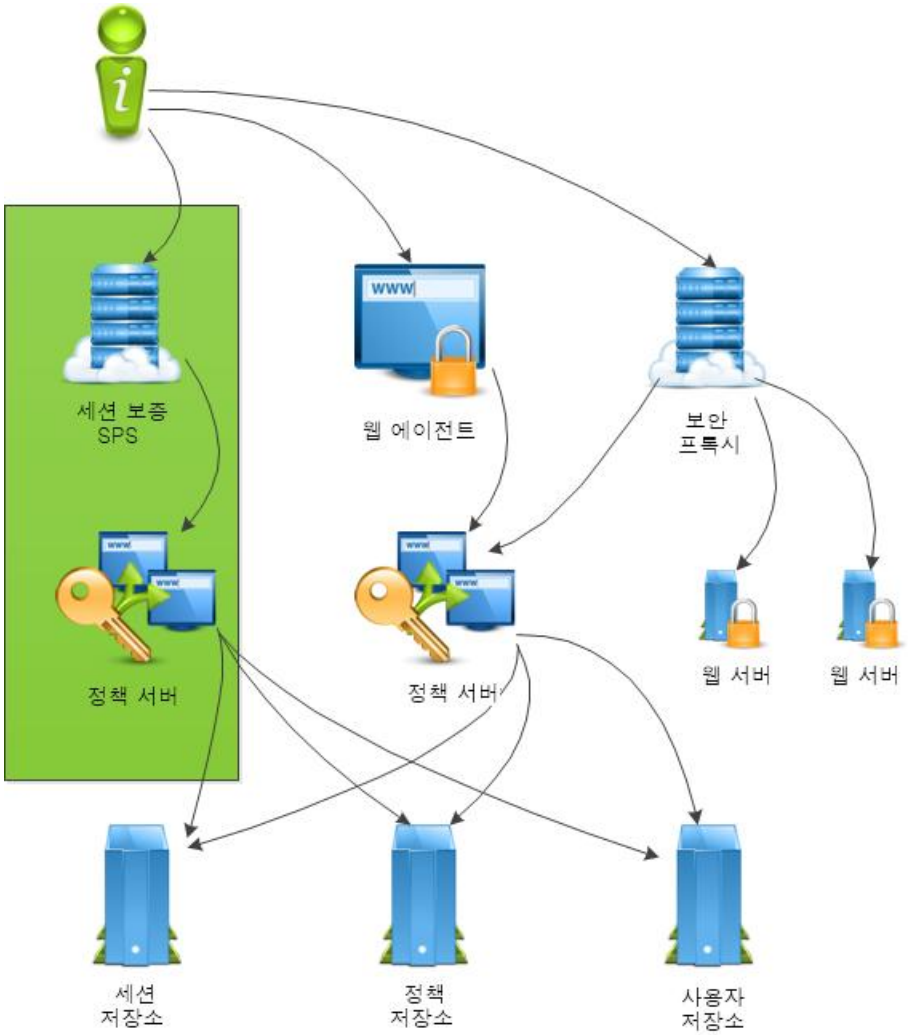
다음 다이어그램에서는 새 CA SiteMinder for Secure Proxy Server 인스턴스를 사용하여 고급 세션 보증을 배포하는 SiteMinder 아키텍처를 보여 줍니다.



이 아키텍처에서는 녹색으로 표시된 CA SiteMinder for Secure Proxy Server 가 새로 도입되었습니다. 이 CA SiteMinder for Secure Proxy Server 는 모든 고급 세션 보증 태스크를 수행하여 CPU 사용률 증가를 방지하거나 프록시 연결을 통해 요청을 백엔드 웹 서버에 전달하는 데 사용되는 다른 CA SiteMinder for Secure Proxy Server 인스턴스의 성능 저하를 방지합니다. 하지만 고급 세션 보증 흐름 응용 프로그램을 실행하는 CA SiteMinder for Secure Proxy Server 인스턴스와 다른 에이전트 및 CA SiteMinder for Secure Proxy Server 인스턴스에서 모두 같은 정책 서버를 공유하기 때문에 정책 서버 사용 수요가 서버 용량을 초과하게 되면 응용 프로그램 및 에이전트의 모든 SiteMinder 트랜잭션이 영향을 받게 됩니다.

## 가능한 아키텍처 3 - 세션 보증 구성 요소의 완전한 분리

다음 다이어그램에서는 새로운 정책 서버와 CA SiteMinder for Secure Proxy Server 를 사용하여 고급 세션 보증을 배포하는 가능한 SiteMinder 아키텍처를 보여 줍니다.



이 아키텍처에서는 특별히 고급 세션 보증을 호스트하기 위해 새 CA SiteMinder for Secure Proxy Server 인스턴스가 배포됩니다. 새 CA SiteMinder for Secure Proxy Server 는 새 정책 서버와 통신합니다. 이 아키텍처를 사용하면 해당 환경에서 하드웨어가 늘어나지만 기존 정책 서버 로드와 성능이 가능한 한 기본 아키텍처와 비슷하게 유지됩니다.

고급 세션 보증을 신속하게 배포하려는 대규모 조직의 경우 이 아키텍처를 사용하는 것이 좋습니다. 이 아키텍처는 고급 세션 보증이 CPU 사용률을 증가시키거나 일반적인 요청 처리에 필요한 스레드를 독점 사용하는 문제를 최소화합니다.

# 제 3 장: SiteMinder 구현 계획

## 구현 계획 개요

SiteMinder 를 구현하는 방법은 다음에 따라 결정됩니다.

- 응용 프로그램을 SiteMinder 액세스 관리 모델에 매핑하는 방식
- 사용하려는 SiteMinder 기능
- SiteMinder 정책 서버와 에이전트를 관리할 방법

SiteMinder 를 배포하고 구성하기 전에 이 단원의 정보를 고려하는 것이 좋습니다.

## 정책 관리 모델

SiteMinder 정책 관리 모델을 사용하면 웹 리소스에 대한 액세스 권한과 각 권한에 해당하는 사용자 집단을 정의할 수 있습니다. 정책 관리 모델에 따라 다음과 같은 사항이 결정됩니다.

- 보호되는 리소스
- 리소스에 액세스할 수 있는 사용자
- 사용자 집단이 갖는 액세스 권한의 유형
- SiteMinder 가 리소스에 대한 액세스를 부여하는 경우 발생하는 결과
- SiteMinder 가 리소스에 대한 액세스를 거부하는 경우 발생하는 결과

사용하는 모델에 관계없이 모든 SiteMinder 기능을 사용할 수 있습니다. 모델 간의 주요한 차이는 각 모델을 구성하는 데 필요한 SiteMinder 관련 지식의 수준입니다. 다음 관리 UI 개체는 정책 관리 모델을 나타냅니다.

- 응용 프로그램
- 정책 도메인 및 도메인 개체

**참고:** 응용 프로그램 개체 또는 도메인 정책을 구성하려면 다음과 같은 SiteMinder 핵심 개체가 필요합니다.

- 호스트 구성 개체
- 에이전트 구성 개체
- 에이전트 개체
- 사용자 디렉터리 개체

  **참고:** 이러한 개체에 대한 자세한 내용은 *정책* 서버 구성 안내서를 참조하십시오.

## 응용 프로그램 개체를 사용한 정책 관리

응용 프로그램 개체는 웹 응용 프로그램, 웹 사이트 또는 웹 서비스에 대한 완전한 보안 정책을 정의할 수 있는 직관적인 방법을 제공합니다. 응용 프로그램은 리소스를 사용자 역할과 연결하여 사용자별로 액세스할 수 있는 리소스를 결정하는 권한 정책을 지정합니다.

**참고:** 응용 프로그램 개체는 정책 도메인 및 하위 개체에서 구성할 수 있는 정책 정보(즉, 영역, 규칙, 규칙 그룹, 응답 및 정책)를 정의합니다. 다음 표는 이러한 관계를 요약하여 보여 줍니다.

| 응용 프로그램 대화 상자 및 그룹 상자 | 그에 상응하는 도메인 구성 요소 |
|---|---|
| 일반 설정 | 정책 도메인 및 보호된 리소스의 루트 위치 |
| 구성 요소 | 보안 요구 사항이 동일한 응용 프로그램 내에서의 리소스 영역 및 위치 |
| 리소스 | 규칙과 필요한 인증 또는 권한 부여 작업 |
| 응용 프로그램 역할 | 사용자 디렉터리 조회 |

**참고:** 응용 프로그램을 사용한 정책 관리에 대한 자세한 내용은 *정책* 서버 구성 안내서를 참조하십시오.

## 정책 도메인 및 도메인 개체를 사용한 정책 관리

SiteMinder r12.0 전에는 정책 도메인 및 도메인 개체(영역, 규칙, 응답, 정책 등)가 리소스를 보호하는 유일한 방법이었습니다. 이미 이전 릴리스에 익숙한 정책 서버 관리자의 경우 여전히 정책 도메인과 도메인 개체를 사용하여 리소스에 대한 보안 정책을 구성할 수 있습니다.

SiteMinder 정책은 다음과 같은 개별 SiteMinder 개체로 구성됩니다.

- 도메인
- 도메인의 최소 하나의 영역
- 도메인의 최소 하나의 규칙 또는 규칙 그룹
- (선택 사항) 도메인의 하나 이상의 응답 또는 응답 그룹

정책 개체는 이러한 핵심 개체를 바인딩하여 리소스, 사용자 집단, 그리고 SiteMinder 가 리소스에 대한 액세스를 허용하거나 거부할 때 필요한 작업을 식별합니다. 따라서 SiteMinder 정책을 구성하려면 각 개체에 대한 이해가 필요합니다.

**참고:** 이러한 각 개체와 각 개체의 개별적인 SiteMinder 정책 역할에 대한 자세한 내용은 정 *책*서버 구성 안내서를 참조하십시오.

# 보안을 적용할 응용 프로그램 식별

보안을 적용하려고 계획하는 응용 프로그램은 무엇입니까? 이러한 응용 프로그램은 SiteMinder 액세스 관리 모델에 어떻게 매핑됩니까?

우선 동일한 수준의 보호를 필요로 하는 각 응용 프로그램 내의 개별 리소스(URL)와 조직 내의 개별 응용 프로그램에 대해 생각해 보십시오. 다음을 식별하는 것이 좋습니다.

- 하나 이상의 사용자 집단과 연결된 리소스의 논리적 그룹(개별 응용 프로그램인 경우가 많음). 이러한 논리적 그룹은 SiteMinder 정책 도메인 또는 EPM 응용 프로그램의 리소스 필터에 매핑됩니다. SiteMinder 정책 도메인 또는 EPM 응용 프로그램의 리소스 필터는 응용 프로그램의 루트 위치를 나타냅니다.
- 응용 프로그램 내에서 보안(인증 및 권한 부여) 요구 사항이 동일한 개별 리소스(URL)의 집합. 요구 사항이 동일한 리소스의 집합은 SiteMinder 정책 영역 또는 EPM 응용 프로그램 구성 요소로 매핑됩니다.

이런 방식으로 리소스를 그룹화하면 응용 프로그램을 SiteMinder 액세스 관리 모델로 매핑하는 데 도움이 됩니다.

각 응용 프로그램에 대한 정보를 수집할 때는 정보를 체계적으로 구성할 수 있도록 다음과 비슷한 리소스 표를 사용하십시오.

| 리소스 | 도메인/응용 프로그램 리소스 필터 | 영역/구성 요소 리소스 필터 |
|---|---|---|
| **예:** 회사 포털 | **예:** 성과 관리 응용 프로그램 | **예:** 관리자 리소스 |

**참고:** 보호가 필요한 응용 프로그램을 식별하면 용량 계획 수립에도 도움이 됩니다.

**추가 정보:**

용량 계획 소개 (페이지 103)
확장명 무시 매개 변수 (페이지 166)

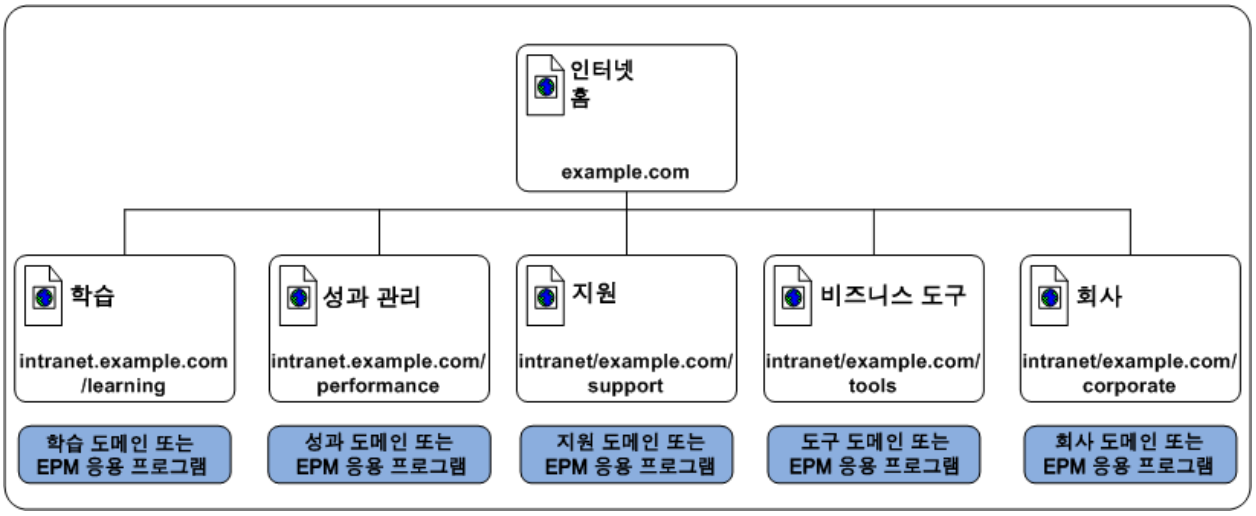
## 리소스를 도메인 또는 EPM 응용 프로그램으로 그룹화

SiteMinder 정책 도메인 또는 EPM 응용 프로그램을 정의하려면 하나 이상의 사용자 집단과 연결된 리소스의 논리적 그룹(개별 응용 프로그램인 경우가 많음)을 식별해야 합니다. 리소스를 이 수준에서 그룹화하면 응용 프로그램 내에서 보안 요구 사항이 동일한 개별 리소스(URL) 집합을 식별하는 데 도움이 됩니다.

**참고:** SiteMinder 정책 도메인 또는 EPM 응용 프로그램에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

이러한 요구 사항을 결정하기 위한 전략은 조직의 사이트 맵을 검토하는 것입니다.

예를 들어 가상의 회사에 다음과 같은 사이트 맵으로 표현되는 회사 인트라넷이 있다고 가정하겠습니다.




이 예에서 회사 포털은 다음과 같은 논리적 리소스 그룹으로 구분됩니다.

- 학습
- 성과 관리
- 지원
- 비즈니스 도구
- 회사

회사 인트라넷의 리소스 표는 다음과 비슷합니다.

| 리소스 | 도메인/EPM 응용 프로그램 필터 | 영역/구성 요소 필터 |
|---|---|---|
| 회사 인트라넷 | intranet.example.com | 해당 없음 |
| 학습 | intranet.example.com/learning | 해당 없음 |
| 성과 관리 | intranet.example.com/performance | 해당 없음 |
| 지원 | intranet.example.com/support | 해당 없음 |
| 비즈니스 도구 | intranet.example.com/tools | 해당 없음 |
| 회사 | intranet.example.com/corporate | 해당 없음 |

**추가 정보:**

도메인 및 인증 성능 (페이지 182)

## 리소스를 영역 또는 EPM 응용 프로그램으로 그룹화

SiteMinder 정책 영역 또는 EPM 구성 요소를 정의하려면 SiteMinder 정책 도메인 또는 EPM 응용 프로그램 내에서 보안 또는 개인화 요구 사항이 동일한 개별 리소스(URL)의 집합을 식별해야 합니다. 영역 또는 EPM 구성 요소의 내용은 동일한 인증 체계를 공유합니다. 그 결과 프로세스 초기에 이러한 리소스를 식별하면 개별 보안 요구 사항을 충족하는 데 필요한 인증 체계를 결정하는 데 도움이 될 수 있습니다.

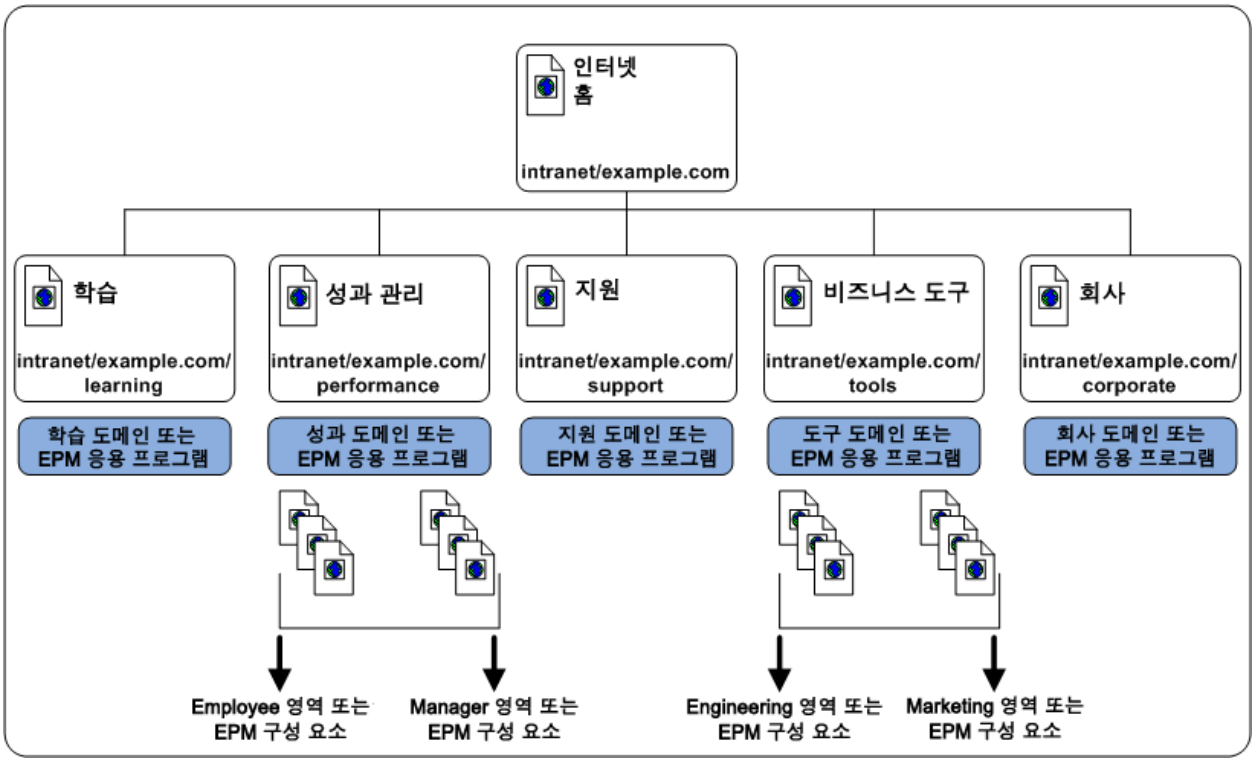
**참고:** SiteMinder 정책 영역 및 EPM 구성 요소에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

예를 들어 성과 관리 및 비즈니스 도구 응용 프로그램은 특정 사용자 집단이 응용 프로그램의 루트에 액세스하는 것을 허용하지만, 각 응용 프로그램에는 리소스에 적절한 수준의 보안 또는 개인화를 제공하기 위한 추가적인 SiteMinder 정책 영역 또는 EPM 구성 요소가 포함됩니다.

- 성과 관리 응용 프로그램에는 상근직 직원만 액세스할 수 있는 리소스와 관리자만 액세스할 수 있는 리소스가 포함되어 있습니다.

- 비즈니스 도구 응용 프로그램에는 연구 개발 직원만 액세스할 수 있는 리소스와 마케팅 직원만 액세스할 수 있는 리소스가 포함되어 있습니다.

**참고:** 여기에는 나와 있지 않지만 SiteMinder 정책 규칙 및 EPM 리소스는 특정 웹 에이전트, 인증 및 권한 부여 이벤트를 제어하는 데 사용됩니다. 자세한 내용은 정 *책*서버 구성 안내서를 참조하십시오.




응용 프로그램의 리소스 표는 다음과 비슷합니다.

| 리소스 | 도메인/EPM 응용 프로그램 필터 | 영역/구성 요소 필터 |
|---|---|---|
| 회사 인트라넷 | intranet.example.com | 해당 없음 |
| 학습 | intranet.example.com/learning | 해당 없음 |
| 성과 관리 | intranet.example.com/performance | /employee<br>/manager |
| 지원 | intranet.example.com/support | 해당 없음 |
| 비즈니스 도구 | intranet.example.com/tools | /engineering |

| 리소스 | 도메인/EPM 응용 프로그램 필터 | 영역/구성 요소 필터 |
|---|---|---|
| | | /marketing |
| 회사 | intranet.example.com/corporate | 해당 없음 |

# 사용자 저장소 식별

SiteMinder 는 엔터프라이즈 네트워크의 기존 사용자 저장소에 대한 하나 이상의 연결을 통해 사용자를 인증하고, 권한을 부여할 수 있습니다. 보안을 적용할 응용 프로그램 (페이지 67)을 식별한 후에는 다음 질문을 고려하십시오.

- 응용 프로그램이 인증을 위해 중앙화된 사용자 저장소를 사용합니까? 아니면 개별적인 사용자 저장소를 사용합니까?
- 응용 프로그램이 별도의 저장소를 사용하는 경우 이 프로젝트에 사용자 ID 를 하나의 저장소로 중앙화하기 위한 태스크가 포함됩니까?
- 응용 프로그램이 사용자를 인증하고 권한을 부여하는 데 동일한 저장소를 사용합니까? 아니면 인증에 사용되는 별도의 저장소가 있습니까?

각 응용 프로그램에서 사용하는 저장소를 식별하면 다음을 수행하는 데 도움이 됩니다.

- 리소스를 보호하기 위해 SiteMinder 관리자가 SiteMinder 정책 도메인에서 구성해야 하는 사용자 저장소 연결을 식별합니다.

  **참고:** 도메인 내에서 사용자 저장소 연결을 구성하는 방법에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

- 환경에 SiteMinder 디렉터리 매핑 기능이 필요한지 결정합니다. 기본적으로 SiteMinder 에서는 사용자가 동일한 사용자 저장소에 대해 인증되고 권한이 부여된다고 가정합니다. 하지만 SiteMinder 정책 도메인을 구성하여 하나 이상의 저장소에 대해 인증하고 다른 저장소에 대해 권한을 부여할 수 있습니다.

  **참고:** 디렉터리 매핑에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

각 응용 프로그램에 대한 정보를 수집할 때는 정보를 체계화할 수 있도록 다음과 비슷한 표를 사용하십시오.

| 사용자 저장소 이름 | 사용자 저장소 유형 | 인증? | 권한 부여? |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

# 인증 방법 식별

SiteMinder 는 리소스에 필요한 다양한 수준의 보호를 충족하기 위해 여러 가지 인증 방법을 지원합니다.

- 기본
- 양식 기반 사용자 ID 및 암호
- RSA® Ace/SecurID® 등과 같은 하드웨어 및 소프트웨어 토큰 기반
- IWA(Windows 통합 인증)
- Microsoft Windows CardSpace 와 같은 ICAS(정보 카드 인증 체계)
- MIT Kerberos
- RADIUS 및 SafeWord 와 같은 서버 기반
- X.509 인증서 기반
- SiteMinder SDK 를 사용하여 생성한 사용자 지정 인증 체계

보안을 적용할 응용 프로그램 (페이지 67)을 식별한 후에는(보안 요구 사항이 동일한 리소스(URL) 집합을 식별하는 것이 바람직함) 다음 질문을 고려하십시오.

- 특정 리소스 유형에 대하여 조직에서 충족해야 하는 인증 지침, 규정 또는 법규가 있습니까?
- 정보가 얼마나 민감하고 중요합니까?
- 이 정보에는 어떤 유형의 사용자가 액세스합니까?
- 이러한 사용자에게 필요한 보안 유형은 무엇입니까?

이러한 유형의 질문에 대한 답변은 다음을 수행하는 데 도움이 됩니다.

- 환경에 필요한 인증 방법을 식별
- 특정 리소스를 보호하기 위해 SiteMinder 관리자가 구성해야 하는 인증 체계를 식별

  **참고:** 인증 체계 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

각 리소스에 대한 정보를 수집할 때는 보안을 적용할 계획이 있는 응용 프로그램별로 정보를 구성하는 것이 좋습니다. 예를 들어 다음 표에서는 보안을 적용할 응용 프로그램 (페이지 67)에서 설명한 대로 응용 프로그램이 개별 도메인 및 영역으로 그룹화된다고 가정합니다.

| 리소스 | URL | 영역 | 인증 방법 |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# 암호 관리 옵션 식별

조직에서 사용자 암호를 관리해야 하는 보안 정책이 있습니까? 향후 사용자 암호를 관리해야 할 것으로 예상됩니까?

SiteMinder 암호 정책을 사용하여 엔터프라이즈의 암호 요구 사항을 적용할 수 있습니다. 암호 정책은 사용자의 암호를 수락하기 전에 다음과 같은 유형의 특성에 대하여 암효의 유효성을 검사합니다.

**조합**

최소 또는 최대 길이, 허용된 문자 유형 및 이러한 문자가 암호에서 반복될 수 있는지 여부와 그 빈도를 확인합니다.

**기간**

동일한 암호를 사용할 수 있는 기간, 암호를 변경하기 전에 비활성 상태로 유지할 수 있는 기간 및 만료된 암호를 다시 사용할 수 있는 기간 또는 빈도와 관련된 시간 제한을 확인합니다. 암호가 만료된 사용자에 대해 다음 응답 중 하나를 지정할 수 있습니다.

- 계정 비활성화
- 암호를 변경하도록 강제

**시도 횟수**

사용자가 이전에 잘못된 암호를 입력한 횟수를 기록하고 이 횟수가 초과될 경우 다음 작업 중 하나를 수행하십시오.

- 계정을 비활성화합니다.
- 한 번의 로그인 시도 또는 계정 다시 활성화를 허용하기 전에 지정된 기간 동안 기다립니다.

**참고:** 자세한 내용은 *SiteMinder 정책 서버 구성 안내서*를 참조하십시오.

## 암호 정책 고려 사항

기업에서 암호 정책을 구현하려는 경우에는 다음 사항을 고려하십시오.

- SiteMinder 에 사용자 디렉터리에 대한 읽기/쓰기 권한이 있어야 합니다. 이러한 권한에는 해당 디렉터리 내의 일부 특성을 단독으로 사용하여 암호 및 암호 관련 정보를 저장할 수 있는 권한이 포함됩니다.
- 암호의 유효성을 검사하려면 추가 사용자 디렉터리 검색이 필요하므로 암호 정책은 SiteMinder 성능에 영향을 줄 수 있습니다. 사용자 디렉터리 전체가 아니라 일부만 검색하도록 구성된 암호 정책도 성능에 영향을 줄 수 있습니다.
- 사용자 디렉터리에 네이티브 암호 정책이 있는 경우 이 정책은 다음 조건을 충족해야 합니다.
  - SiteMinder 암호 정책보다 덜 제한적임
  - 사용 안 함

  그렇지 않으면 네이티브 암호 정책이 SiteMinder 에 알리지 않고 암호를 수락하거나 거부할 수 있습니다. 따라서 SiteMinder 가 해당 암호를 관리할 수 없습니다.
- 기본적으로 사용자가 암호를 변경할 때 잘못된 정보를 입력하면 SiteMinder 는 일반적인 오류 메시지를 반환합니다. 이 메시지에 오류 원인은 포함되지 않습니다. 이 기본 동작을 변경하여 변경에 실패한 이유를 사용자에게 알려 주려면 DisallowForceLogin 레지스트리 키를 생성하여 사용하십시오.
- 여러 정책 서버에서 암호 정책을 사용하는 경우에는 모든 서버의 시스템 시간을 동기화하십시오. 시간을 동기화하면 계정이 비활성화되거나 강제 암호 변경이 중간에 종료되지 않도록 할 수 있습니다.

  **참고:** 자세한 내용은 *SiteMinder 정책 서버 구성 안내서*를 참조하십시오.

# 웹 에이전트를 관리할 사람을 식별

웹 에이전트는 시작할 때 정책 서버에 연결합니다. 정책 서버에는 연결된 웹 에이전트를 구성 매개 변수의 위치로 보내는 ACO(에이전트 구성 개체)가 포함되어 있습니다.

응용 프로그램이 조직 전체에 배포되는 방식을 고려하면 SiteMinder 웹 에이전트에 대한 구성 매개 변수를 저장하는 가장 효율적인 방법을 결정하는 데 도움이 됩니다. 다음 질문을 고려하십시오.

1. 대부분의 웹 응용 프로그램이 보안 요구 사항이 동일한 대규모 서버 팜에 배포되어 있습니까?
2. 대부분의 웹 응용 프로그램을 중앙의 사람 또는 그룹이 관리합니까?
3. 대부분의 웹 응용 프로그램이 보안 요구 사항이 서로 다른 별도의 웹 서버에 배포되어 있습니까?
4. 대부분의 웹 응용 프로그램을 서로 다른 부서 또는 물리적 위치에 있는 서로 다른 사람이 관리합니까?

앞의 목록에서 하나 또는 두 개의 질문에 예라고 답한 경우에는 다음 구성 방법을 사용해 보십시오.

- 중앙 구성

  정책 서버에 상주하는 ACO(에이전트 구성 개체)에서 하나 이상의 에이전트에 대한 매개 변수를 관리합니다. 중앙 에이전트 구성을 사용하면 여러 에이전트의 매개 변수 설정을 동시에 업데이트할 수 있습니다. 일반적으로 각기 다른 웹 응용 프로그램은 웹 응용 프로그램을 보호하는 모든 에이전트 사이에 설정이 공유되는 별개의 ACO 를 사용합니다. 예를 들어 하나의 회계 응용 프로그램을 보호하는 에이전트가 5 개 있을 경우 이 응용 프로그램에 대해 원하는 설정을 포함하는 ACO 를 하나 생성할 수 있습니다. 그러면 5 개의 에이전트는 모두 동일한 ACO 의 매개 변수 설정을 사용하게 됩니다.

  각 응용 프로그램에 대해 별도의 에이전트 구성 개체를 사용하는 것이 좋습니다. 예를 들어 더 엄격한 보안 요구 사항으로 인사 관리 응용 프로그램을 보호하려는 경우 이 응용 프로그램에 대해 별도의 ACO 를 생성합니다.

  에이전트는 시작 시 관련 ACO 에서 AllowLocalConfig 매개 변수의 값을 읽습니다. 이 값이 no 로 설정되어 있으면 에이전트는 해당 ACO 의 매개 변수 설정을 사용합니다(에이전트 로그 및 추적 파일 설정 제외). 에이전트 로그 파일과 추적 파일은 ACO 설정에 관계없이 항상 로컬로 제어할 수 있습니다.

  **참고:** 가능하면 항상 중앙 에이전트 구성을 사용하는 것이 좋습니다. 그러면 에이전트 구성과 유지 관리가 간소해집니다.

앞의 목록에서 세 개 또는 네 개의 질문에 예라고 답한 경우에는 다음 구성 방법을 사용해 보십시오.

- 로컬 구성

  웹 서버 자체에 설치된 파일을 사용하여 각 웹 에이전트를 개별적으로 관리합니다. 웹 에이전트가 시작되면 에이전트는 관련 ACO(에이전트 구성 개체)에서 AllowLocalConfig 매개 변수의 값을 읽습니다. 이 값이 yes 로 설정되어 있으면 웹 에이전트는 웹 서버에 있는 LocalConfig.conf 파일의 매개 변수 설정을 사용합니다. LocalConfig.conf 파일의 매개 변수 설정은 정책 서버의 ACO 에 저장된 모든 설정을 무시합니다.

다음 질문은 로컬 에이전트 구성이 엔터프라이즈의 요구 사항을 더 잘 충족하는 다른 상황을 식별하는 데 도움이 됩니다.

- 엔터프라이즈에서 리버스 프록시 서버에 웹 에이전트 일부를 배포할 계획입니까?

  예를 들어 몇 군데 위치에 리버스 프록시 서버를 구현하고 웹 에이전트의 대규모 그룹으로 내부 리소스를 보호하려는 경우가 있습니다. 이 경우 로컬 구성을 사용하여 리버스 프록시 웹 에이전트를 관리할 수 있습니다.

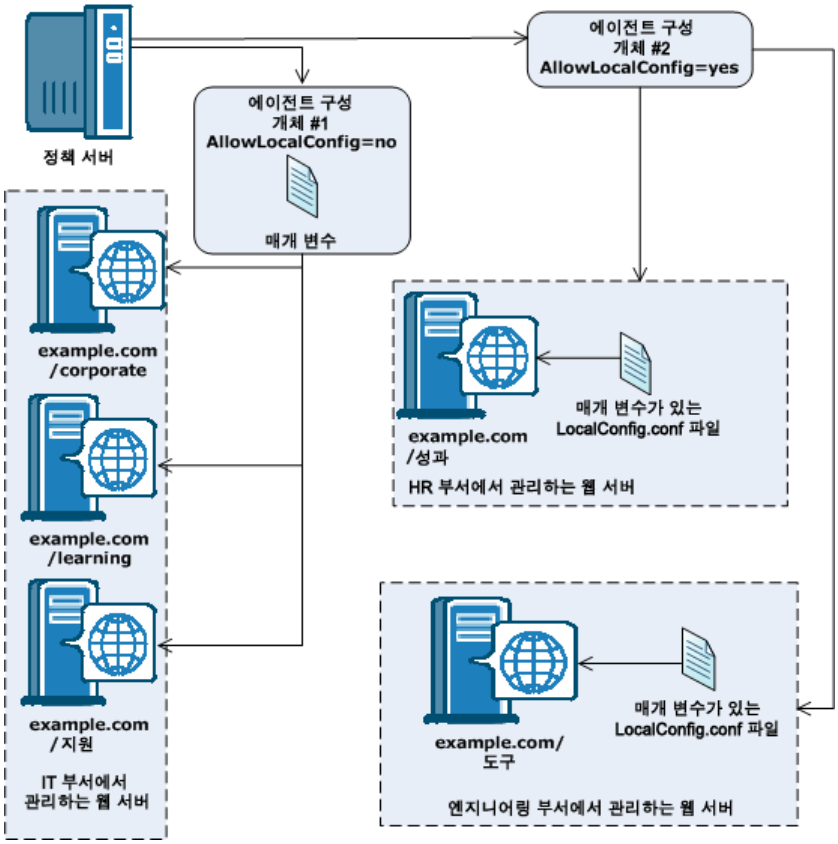
- 로컬 웹 서버 관리자가 웹 에이전트 구성 설정의 일부만 변경할 수 있고 다른 설정은 변경하지 못하게 만들려고 하십니까?

  예를 들어 조직에서 SiteMinder 를 사용하여 보안 정책을 관리하고 적용하지만 원격 사무소의 웹 서버 관리자에게 로그온 및 로그오프 페이지를 사용자 지정할 수 있게 허용하는 경우가 있습니다. ACO 의 AllowLocalConfig 매개 변수의 값에 개별 매개 변수를 추가하여 관리자가 사용자 지정된 페이지의 설정만 변경할 수 있고 다른 설정은 변경하지 못하게 만들 수 있습니다.

  **참고:** 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

## 중앙 구성과 로컬 구성의 조합

또한 필요에 따라 중앙 및 로컬 구성의 조합을 사용할 수도 있습니다. 예를 들어 세 개의 비슷한 웹 서버는 중앙 구성으로 관리하고 다른 두 개의 서버는 로컬 구성으로 관리할 수 있습니다. 다음 그림을 예로 참조하십시오.



# 데이터 센터 식별

여러 데이터 센터에서 SiteMinder 구성 요소를 구현하는 방법을 결정하는 데는 뒤에서 설명할 여러 가지 요소가 영향을 미칩니다. SiteMinder 구성 요소를 구현하는 방법을 결정할 때 데이터 센터를 식별하고 각 데이터 센터가 SiteMinder 환경에서 수행하는 역할을 파악하면 보다 자세한 정보를 바탕으로 결정할 수 있습니다. 다음 질문을 고려하십시오.

- 배포에 포함된 데이터 센터는 몇 개이며 각 데이터 센터의 위치는 어디입니까?
- 데이터 센터가 여러 개인 경우:
  - 모두 활성입니까? 아니면 일부는 재난 복구나 백업 전용입니까?
  - 보호되는 각 응용 프로그램이 단일 데이터 센터에 있습니까? 아니면 여러 센터에 분산되어 있습니까?
  - 장애 조치를 데이터 센터 수준에서 구성할 계획입니까? 아니면 여러 데이터 센터에 걸쳐 구성할 계획입니까?
  - 데이터 센터 간의 대역폭과 처리량은 어느 정도입니까?

각 데이터 센터에 대한 정보를 수집할 때는 다음과 비슷한 리소스 표를 사용하여 결과를 구성하십시오.

| 데이터 센터 이름 | 위치 | 용도 |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

**추가 정보:**

다중 데이터 센터 (페이지 130)

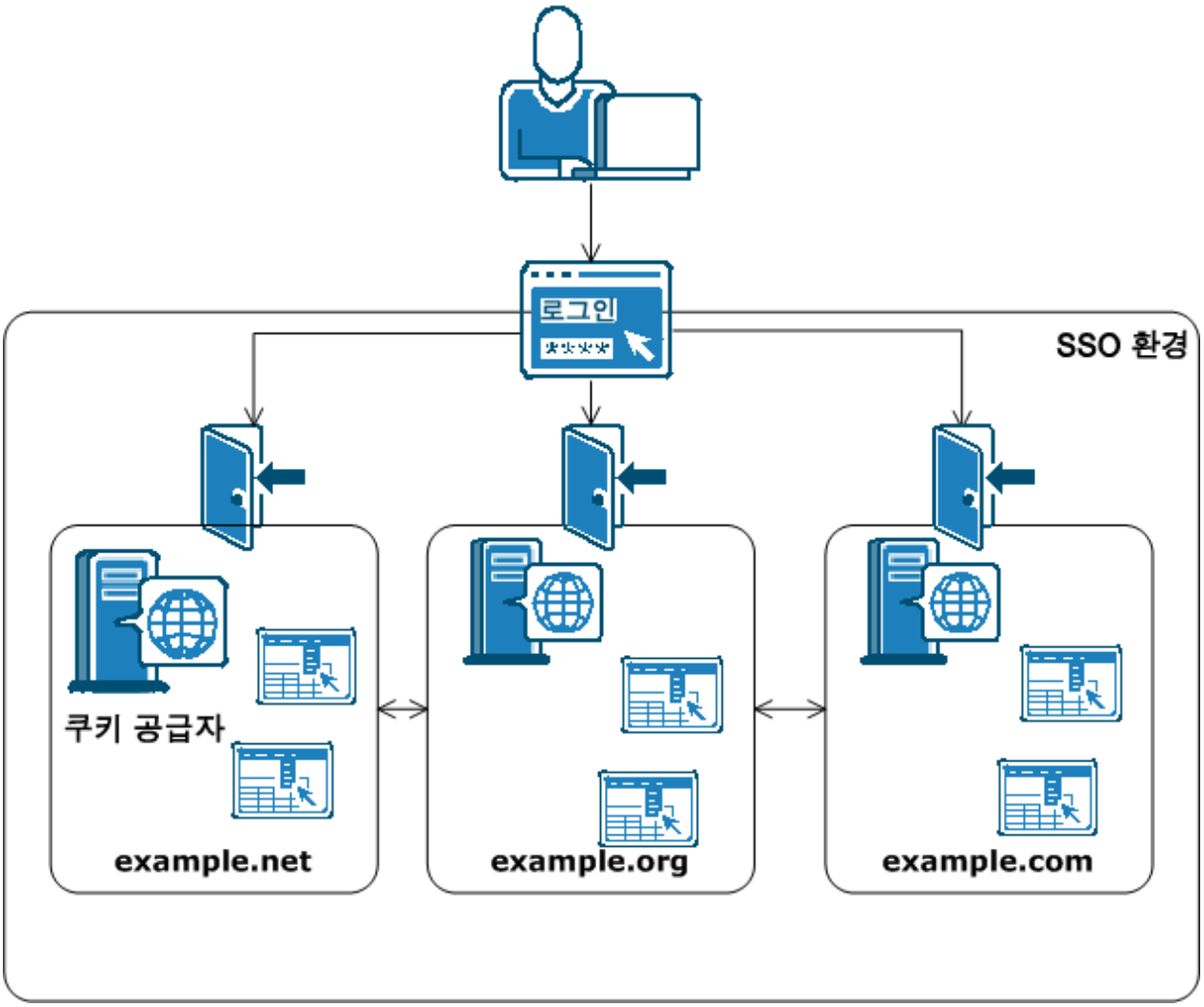
# 여러 쿠키 도메인으로 보안을 적용할 리소스 식별

엔터프라이즈의 싱글 사인온 환경이 여러 쿠키 도메인으로 확장될 계획입니까?

SiteMinder 는 쿠키 공급자로 구성된 SiteMinder 웹 에이전트를 사용하여 여러 쿠키 도메인에 대해 싱글 사인온을 구현합니다.

쿠키 공급자 웹 에이전트가 있는 쿠키 도메인을 쿠키 공급자 도메인이라고 합니다. 싱글 사인온 환경 내에서 다른 쿠키 도메인의 다른 모든 웹 에이전트는 하나의 쿠키 공급자를 가리킵니다.

다음 그림은 여러 쿠키 도메인을 사용하는 SSO 환경의 예를 보여 줍니다.

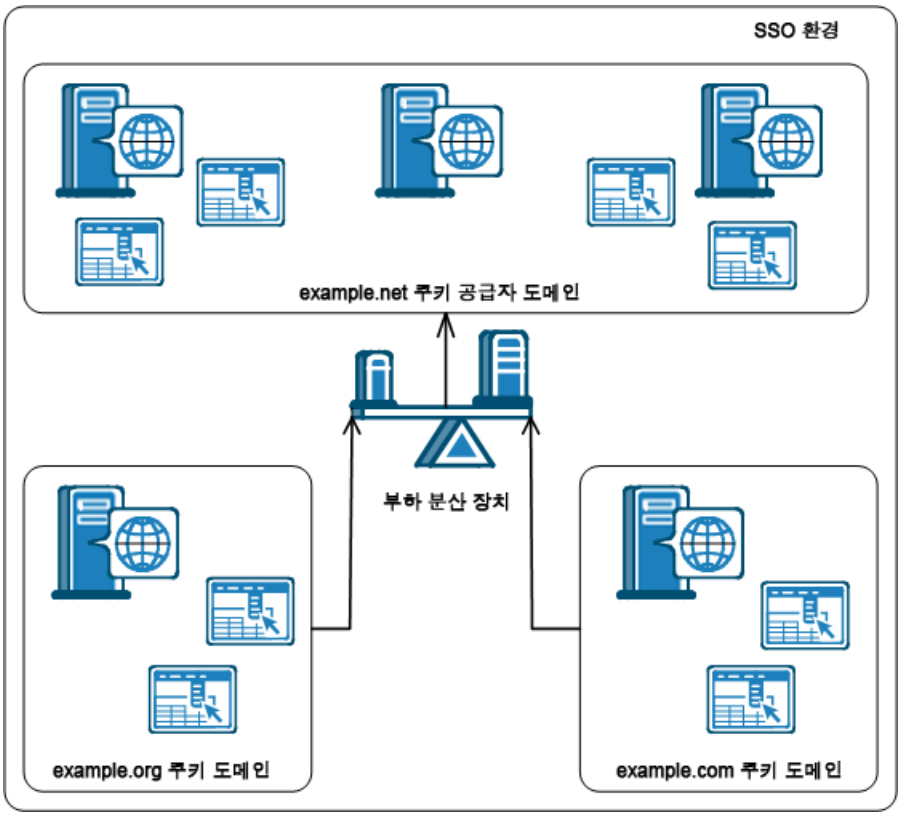


**참고**: 쿠키 공급자에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

## SSO 를 위해 쿠키 공급자 도메인과 다른 쿠키 도메인 간의 부하 분산

싱글 사인온 환경의 에이전트는 부하 분산 기능을 사용합니까?

SSO 환경의 모든 에이전트는 단일 쿠키 공급자 도메인을 참조해야 합니다. 쿠키 공급자 도메인의 웹 서버와 SSO 환경의 다른 쿠키 도메인 사이에 부하 분산 장치를 추가하십시오. 다음 그림은 이러한 예를 보여 줍니다.




example.org 쿠키 도메인의 웹 에이전트와 example.com 쿠키 도메인의 웹 에이전트는 둘 다 example.net 이라는 같은 쿠키 공급자 도메인을 가리킵니다. 부하 분산 장치는 example.net 쿠키 공급자 도메인의 모든 웹 서버 사이에 균등하게 트래픽을 배분합니다.

# 파트너 관계에 CA SiteMinder® Federation 이 필요한지 여부 확인

기존 또는 계획된 B2B 파트너 관계를 위해 조직에서 아이덴티티 정보를 파트너와 안전하게 공유해야 합니까?

CA SiteMinder?Federation 을 통해 아이덴티티 페더레이션을 구현하여 SiteMinder 기능을 파트너 사이트로 확장할 수 있습니다. CA SiteMinder?Federation 은 레거시 페더레이션 및 파트너 관계 페더레이션의 두 가지 배포 옵션을 제공합니다.

파트너 조직 간의 페더레이션된 트랜잭션을 통해 조직은 다음을 수행할 수 있습니다.

- 사용자 아이덴티티 정보를 안전한 방식으로 파트너 간에 교환
- 파트너 측의 사용자 아이덴티티와 회사 측의 사용자 아이덴티티 간에 링크 설정
- 여러 도메인의 파트너 웹 사이트에서 싱글 사인온 사용
- 파트너 사이트 간에 파트너 웹 사이트 전체에서 싱글 로그아웃 또는 파트너 웹 사이트마다 별도의 세션 등 여러 가지 사용자 세션 모델 처리
- 파트너에서 수신한 사용자 정보를 기반으로 리소스에 대한 액세스 제어
- 이기종 환경에서 상호 운용성 허용

CA SiteMinder?Federation 을 통해 기업은 어설션을 생성 또는 소비하거나 두 작업을 모두 할 수 있습니다. CA SiteMinder?Federation 은 다음 표준 및 프로토콜을 지원합니다.

- SAML 1.0(레거시 페더레이션만)
- SAML 1.1 및 2.0
- Microsoft ADFS/WS-페더레이션(레거시 페더레이션만)

- SAML 브라우저 아티팩트 프로토콜
- SAML POST 프로토콜
- WS-페더레이션 피동 요청자 프로필 프로토콜(레거시 페더레이션만)

**참고:** CA SiteMinder® Federation 는 SiteMinder 와 별도로 라이선스가 필요합니다. 라이선스에 대한 자세한 내용은 CA 고객 담당자에게 문의하십시오. 페더레이션에 대한 자세한 내용은 *CA SiteMinder® Federation 레거시 페더레이션 안내서* 또는 *CA SiteMinder® Federation 파트너 관계 페더레이션 안내서*를 참조하십시오.

조직에서 페더레이션 구현을 계획하는 경우 다음 표와 유사한 표를 참조하여 아이덴티티 페더레이션을 사용하기 위한 파트너와 가능한 방법을 파악하십시오.

| 파트너 | 표준 | 프로토콜 |
|---|---|---|
| | | |
| | | |
| | | |

# AES(Advanced Encryption Standards)가 필요한지 여부 결정

조직에서 FIPS(Federal Information Processing Standard) 140-2 호환 알고리즘을 사용해야 합니까?

AES(Advanced Encryption Standard)의 SiteMinder 구현은 FIPS 140-2 표준을 지원합니다. FIPS 는 AES 를 충족하는 암호화 모듈을 인가하는 데 사용되는 미국 정부의 컴퓨터 보안 표준입니다.

정책 서버는 인증된 FIPS 140-2 호환 암호화 라이브러리를 사용합니다. 이러한 암호화 라이브러리는 SiteMinder 환경에서 중요한 데이터를 암호화하는 데 AES 호환 알고리즘만 사용하는 경우에 FIPS 작동 모드를 지원합니다. SiteMinder 환경은 다음과 같은 FIPS 작동 모드 중 하나에서 작동할 수 있습니다.

- FIPS 호환성
- FIPS 마이그레이션
- FIPS 전용

**참고:** SiteMinder 에서 사용하는 암호화 라이브러리와 FIPS 전용 모드에서 중요한 데이터를 암호화하는 데 사용되는 AES 알고리즘에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오. FIPS 작동 모드 및 정책 서버를 설치할 때 사용할 모드에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

FIPS 전용 모드를 통한 AES 암호화를 구현할 경우에는 다음 사항을 고려하십시오.

- 디렉터리 서버, 데이터베이스 및 드라이버를 포함한 모든 타사 구성 요소는 FIPS 호환 알고리즘을 지원하도록 구성되어야 합니다.

  **참고:** 공급업체가 FIPS 140-2 표준을 지원하는지 여부에 대한 자세한 내용은 공급업체의 설명서를 참조하십시오.

- 환경에서 X.509 클라이언트 인증서 인증 체계를 사용하는 경우 사용자 인증서가 FIPS 호환 알고리즘만 사용하여 생성되어야 합니다.
- 정책 서버를 SSL 을 사용하여 정책 저장소 또는 사용자 저장소에 연결할 경우에는 정책 서버와 디렉터리 저장소가 FIPS 호환 인증서를 사용하는지 확인하십시오.
- SiteMinder r12.x 와 함께 제공되는 모든 웹 에이전트는 FIPS 와 호환됩니다. 에이전트가 FIPS 와 호환되는지 여부를 확인하려면 에이전트의 설명서를 참조하십시오.

**중요!** FIPS 전용 모드로 실행 중인 환경은 이전 버전의 SiteMinder 와 함께 운용될 수 없으며 이전 버전의 SiteMinder 와 호환되지도 않습니다. 이 요구 사항에는 모든 에이전트, 이전 버전의 에이전트 API 를 사용하는 사용자 지정 소프트웨어, 그리고 PM API 나 정책 서버에서 노출하는 그 밖의 모든 API 를 사용하는 사용자 지정 소프트웨어가 포함됩니다. FIPS 전용 모드에 필요한 지원을 받으려면 이러한 모든 소프트웨어를 해당하는 SDK 의 현재 버전과 다시 연결하십시오.

# 가상화 사용 여부 결정

SiteMinder 를 가상 환경으로 구현할 계획입니까?

SiteMinder 를 가상 환경으로 구현하기 전에 다음 사항을 고려하십시오.

- CA policy on virtualization (가상화에 대한 CA 정책)을 검토하십시오.
- 다음을 확인하십시오.
  - 호스트 시스템이 응용 프로그램에 부과할 수 있는 성능 오버헤드와 가상 환경을 이해하십시오.
  - 성능 오버헤드가 최대한 제거되도록 가상 환경을 조정하십시오.

    **참고:** 가상 환경의 성능 조정에 대한 자세한 내용은 공급업체의 설명서를 참조하십시오.
- CPU, 디스크 공간 및 메모리의 크기를 가상 환경에 맞게 조정해야 합니다. 각 SiteMinder 설치 안내서에서 설명하는 시스템 요구 사항을 사용하여 시스템 전체에 배포할 구성 요소의 양을 결정하십시오.
- 클록 동기화 및 다중 운영 체제와 관련된 문제를 파악하십시오. 클록이 동기화되지 않으면 예기치 않은 SiteMinder 동작이 발생할 수 있습니다.
- 구성 요소 배포 위치를 고려할 때:
  - 정책 서버를 가상 환경에 배포하는 것이 좋습니다. 정책 서버에 자체 이더넷 포트가 있는 것이 좋습니다. SiteMinder 는 사용 가능한 대역폭을 두고 가상 호스트와 경쟁하므로 전용 포트를 사용하면 요청이 누락되는 것을 방지할 수 있습니다.
  - 웹 에이전트는 가상화된 웹 서버에 배포하는 것이 좋습니다.
  - SiteMinder 데이터 저장소는 모두 물리적 하드웨어 및 운영 체제에 배포하는 것이 좋습니다. 디렉터리 서버 및 데이터베이스는 리소스의 영향을 크게 받을 수 있습니다. 가상화된 환경에 배포될 경우 이러한 영향 때문에 성능이 저하될 수 있습니다.

# 정책 서버 관리 방법 결정

각 비즈니스 단위가 정책 서버의 관리를 책임져야 합니까? 아니면 하나의 비즈니스 단위가 중앙에서 모든 정책 서버를 관리할 수 있습니까?

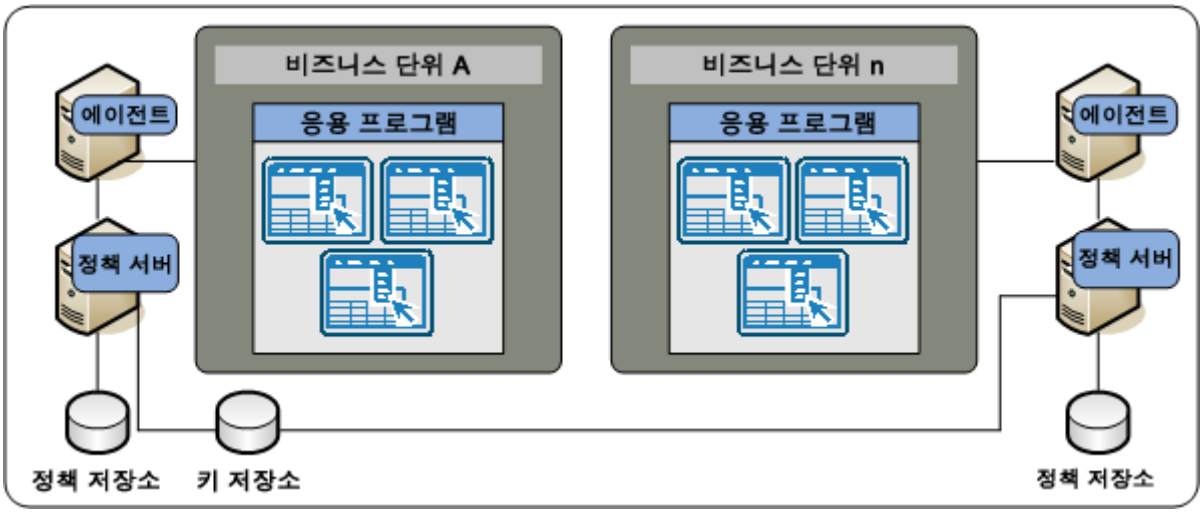
## 로컬 정책 서버 관리

각 비즈니스 단위가 정책 서버와 정책 저장소를 로컬로 관리하는 경우에는 로컬 정책 서버 관리가 다음과 같은 특징이 있다는 점을 고려하십시오.

- 각 비즈니스 단위가 개별적인 필요에 따라 보안 요구 사항을 직접 관리할 수 있게 됩니다.
- SiteMinder 인프라의 복잡성이 증가할 수 있습니다.
  - 로컬 정책 서버 관리를 사용하면 관리하고 업그레이드해야 할 정책 서버와 정책 저장소의 수가 늘어날 수 있습니다.
  - 싱글 사인온이 필요한 경우 로컬 정책 서버 관리를 사용하면 추가적인 SiteMinder 구성이 필요합니다. 그림과 같이 두 비즈니스 단위의 정책 서버는 모든 SiteMinder 에이전트가 동일한 키를 공유할 수 있도록 키 저장소를 공유해야 합니다.

    **참고:** 이 그림에서는 싱글 사인온 요구 사항을 설명하기 위해 공유 키 저장소를 보여 줍니다. 공유 키 저장소는 싱글 사인온을 구현하는 유일한 방법이 아니며 추가 요구 사항이 존재합니다. 싱글 사인온 사용을 위한 키 관리 시나리오에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.
- SiteMinder 관리자가 서로 다른 비즈니스 단위에 있기 때문에 SiteMinder 핵심 개체, 정책 및 EPM 응용 프로그램의 일관된 구현과 관리가 더 까다로워질 수 있습니다.

다음 그림에서는 정책 서버를 로컬에서 관리하는 두 비즈니스 단위를 보여 줍니다.



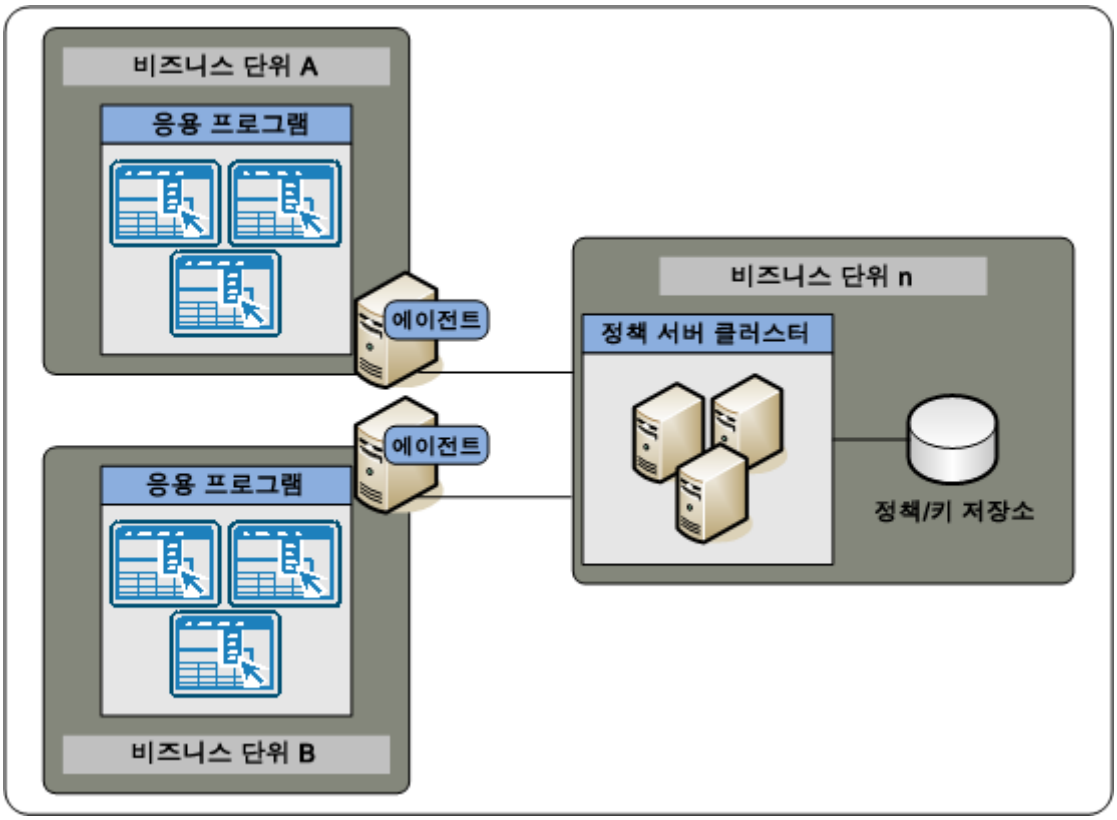
## 중앙 정책 서버 관리

단일 비즈니스 단위가 정책 서버를 로컬로 관리할 경우 중앙 정책 서버 관리에는 다음과 같은 특징이 있다는 점을 고려하십시오.

- 모든 SiteMinder 관리자가 동일한 비즈니스 단위에 있으므로 SiteMinder 핵심 개체, 정책 및 EPM 응용 프로그램을 일관성 있게 구현하기가 용이합니다.
- 모든 SiteMinder 관리자가 동일한 비즈니스 단위에 있기 때문에 이러한 개체를 관리하기가 더 용이합니다.

  **참고:** 그림에서처럼 개별 비즈니스 단위는 응용 프로그램을 보호하면서 SiteMinder 에이전트를 계속 관리할 수 있습니다.
- SiteMinder 인프라를 단순화할 수 있습니다. 중앙 관리를 사용하면 관리하고 업그레이드해야 할 정책 서버와 정책 저장소의 수가 줄어듭니다.
- 관리자가 SiteMinder 성능을 중앙에서 모니터링할 수 있습니다.

다음 그림은 모든 정책 서버를 관리하는 단일 비즈니스 단위를 보여 줍니다.



# 웹 에이전트 관리 방법 결정

동일하게 구성할 여러 개의 웹 에이전트가 있는 경우 정책 서버에서 에이전트 구성 개체를 사용하면 웹 에이전트를 더 쉽게 관리할 수 있습니다. 단일 에이전트 구성 개체를 공유할 수 있는 웹 에이전트 수에는 제한이 없습니다. 정책 서버에서 구성을 변경하면 변경 내용은 구성 개체를 사용하는 모든 웹 에이전트에 자동으로 적용됩니다.

**참고:** 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

# 제 4 장: eTrust SOA Security Manager 구현 계획

## 정책 관리 모델

eTrust SOA Security Manager 액세스 관리 모델을 사용하면 응용 프로그램에 대한 액세스 권한과 각 권한에 해당하는 사용자 집단을 정의할 수 있습니다. 액세스 관리 모델에 따라 다음과 같은 사항이 결정됩니다.

- 보호되는 리소스
- 리소스에 액세스할 수 있는 사용자
- 사용자 집단이 갖는 액세스 권한의 유형
- SiteMinder 가 리소스에 대한 액세스를 부여하는 경우 발생하는 결과
- SiteMinder 가 리소스에 대한 액세스를 거부하는 경우 발생하는 결과

사용하는 모델에 관계없이 거의 모든 eTrust SOA Security Manager 기능을 사용할 수 있습니다. 모델 간의 주요한 차이는 각 모델을 구성하는 데 필요한 SiteMinder 관련 지식의 수준입니다. 다음 관리 UI 개체는 정책 관리 모델을 나타냅니다.

- 응용 프로그램 개체
- 정책 도메인 및 정책 개체

**참고:** 응용 프로그램 개체 또는 SiteMinder 도메인 정책을 구성하려면 다음과 같은 SiteMinder 핵심 개체가 필요합니다.

- 호스트 구성 개체
- 에이전트 구성 개체
- 에이전트 개체
- 사용자 디렉터리 개체

  이러한 개체에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

## 응용 프로그램 개체를 사용한 정책 관리

사용자 eTrust SOA Security Manager 환경에 적합한 새 보안 정책을 생성하고 관리하기 위해 권장되는 방법은 하나 이상의 관련 웹 서비스를 나타내는 응용 프로그램 개체를 정의한 다음 연결된 WSDL 파일에서 보호할 항목을 정의하는 구성 요소 및 리소스 설정을 생성하는 것입니다.

**참고:** 응용 프로그램 개체는 변수 개체를 사용하는 정책 식을 지원하지 않습니다. 변수를 사용하는 콘텐츠 기반 권한 부여는 정책 도메인과 정책을 사용하여 구현해야 합니다.

## 정책 도메인 및 정책을 사용한 정책 관리

CA SOA Security Manager 또는 SiteMinder 에 이미 익숙한 정책 서버 관리자의 경우 여전히 정책 도메인 및 도메인 개체(영역, 규칙, 응답, 정책 등)를 사용하여 웹 서비스 리소스에 대한 보안 정책을 수동으로 구성할 수 있습니다.

다음과 같은 경우에도 도메인 및 도메인 개체를 사용해야 합니다.

- 기존 방법으로 생성되고 이전 CA SOA Security Manager 배포에서 마이그레이션된 정책을 수정하는 경우
- 변수를 사용하여 콘텐츠 기반 권한 부여를 구현하는 경우

# 보호할 웹 서비스 식별

보호하려는 웹 서비스는 무엇입니까? 이러한 웹 서비스는 eTrust SOA Security Manager 정책 관리 방법에 어떻게 매핑됩니까?

우선 동일한 수준의 보호 기능을 필요로 하는 각 웹 서비스 내의 작업 집합과 조직 내의 개별 웹 서비스에 대해 생각해 보십시오. 다음을 식별하는 것이 좋습니다.

- 하나 이상의 사용자 집단과 연결된 리소스의 논리적 그룹(개별 웹 서비스를 통해 제공되는 경우가 많음)
- 웹 서비스 내에서 보안(인증 및 권한 부여) 요구 사항이 동일한 개별 작업 집합

**참고:** 보호가 필요한 웹 서비스를 식별하면 용량 계획 수립에도 도움이 됩니다.

**추가 정보:**

용량 계획 소개 (페이지 119)

# 사용자 저장소 식별

eTrust SOA Security Manager 는 엔터프라이즈 네트워크의 기존 사용자 저장소에 대한 하나 이상의 연결을 통해 사용자를 인증하고, 권한을 부여할 수 있습니다. 보호할 웹 서비스를 식별한 후에는 다음 질문을 고려하십시오.

- 웹 서비스가 인증을 위해 중앙화된 사용자 저장소를 사용합니까? 아니면 개별적인 사용자 저장소를 사용합니까?
- 웹 서비스가 별도의 저장소를 사용하는 경우 이 프로젝트에 사용자 ID 를 하나의 저장소로 중앙화하기 위한 태스크가 포함됩니까?
- 웹 서비스가 사용자 인증 및 권한 부여에 동일한 저장소를 사용합니까? 아니면 인증에 사용되는 별도의 저장소가 있습니까?

각 웹 서비스에서 사용하는 저장소를 식별하면 다음을 수행하는 데 도움이 됩니다.

- 리소스를 보호하기 위해 SiteMinder 관리자가 SiteMinder 정책 도메인에서 구성해야 하는 사용자 저장소 연결을 식별합니다.

  **참고:** 도메인 내에서 사용자 저장소 연결을 구성하는 방법에 대한 자세한 내용은 정 *책*서버 구성 안내서를 참조하십시오.

- 환경에 SiteMinder 디렉터리 매핑 기능이 필요한지 결정합니다. 기본적으로 SiteMinder 에서는 사용자가 동일한 사용자 저장소에 대해 인증되고 권한이 부여된다고 가정합니다. 하지만 SiteMinder 정책 도메인을 구성하여 하나 이상의 저장소에 대해 인증하고 다른 저장소에 대해 권한을 부여할 수 있습니다.

  **참고:** 디렉터리 매핑에 대한 자세한 내용은 정 *책*서버 구성 안내서를 참조하십시오.

각 웹 서비스에 대한 정보를 수집할 때는 정보를 체계화할 수 있도록 다음과 비슷한 표를 사용하십시오.

| 사용자 저장소 이름 | 사용자 저장소 유형 | 인증? | 권한 부여? |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

**추가 정보:**

보호할 웹 서비스 식별 (페이지 92)

# 인증 방법 식별

eTrust SOA Security Manager 는 리소스에 필요한 다양한 수준의 보호를 충족하기 위해 여러 가지 인증 방법을 지원합니다.

**XML 문서 자격 증명 수집기**

문서 내의 필드를 사용자 디렉터리 내의 필드에 매핑함으로써 메시지에서 수집된 자격 증명을 사용하여 XML 메시지의 유효성을 검사합니다.

**XML 디지털 서명**

올바른 X.509 인증서로 디지털 서명된 XML 문서의 유효성을 검사합니다.

**WS-보안**

수신 메시지의 SOAP 봉투에 있는 WS-Security 헤더에서 수집된 자격 증명을 사용하여 XML 메시지의 유효성을 검사합니다.

eTrust SOA Security Manager 는 -WS-Security 토큰을 생성 및 소비할 수 있으므로 사용자가 WSSecurity 인증 체계를 사용하여 페더레이션된 사이트에 여러 웹 서비스 구현을 배포할 수 있습니다.

**SAML 세션 티켓**

메시지 HTTP 헤더, SOAP 봉투 또는 쿠키에 있는 eTrust SOA Security Manager 동기화 세션 SAML 어설션(CA SiteMinder 세션 티켓 및 CA SiteMinder 사용자 공개 키의 암호화된 조합 포함)에서 가져온 자격 증명을 사용하여 XML 메시지의 유효성을 검사합니다.

eTrust SOA Security Manager 는 SAML 세션 티켓 어설션을 생성 및 소비할 수 있습니다. 따라서 사용자는 SAML 세션 티켓 인증 체계를 사용하여 단일 정책 서버 도메인 내에 여러 웹 서비스 구현을 배포할 수 있습니다.

보호할 웹 서비스를 식별한 후에는(보안 요구 사항이 동일한 웹 서비스 작업을 식별하는 것이 바람직함) 다음 질문을 고려하십시오.

- 특정 리소스 유형에 대하여 조직에서 충족해야 하는 인증 지침, 규정 또는 법규가 있습니까?
- 정보가 얼마나 민감하고 중요합니까?
- 이 정보에는 어떤 유형의 사용자가 액세스합니까?
- 이러한 사용자에게 필요한 보안 유형은 무엇입니까?

이러한 유형의 질문에 대한 답변은 다음을 수행하는 데 도움이 됩니다.

- 환경에 필요한 인증 방법을 식별
- 특정 리소스를 보호하기 위해 SiteMinder 관리자가 구성해야 하는 인증 체계를 식별

  **참고:** 인증 체계 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

**추가 정보:**

보호할 웹 서비스 식별 (페이지 92)

# SiteMinder WSS 에이전트를 관리할 사람 식별

SiteMinder WSS 에이전트는 시작 시 정책 서버에 연결합니다. 정책 서버에는 연결된 SiteMinder WSS 에이전트를 구성 매개 변수의 위치로 보내는 ACO(에이전트 구성 개체)가 포함되어 있습니다.

웹 서비스가 조직 전체에 배포되는 방식을 고려하면 SiteMinder WSS 에이전트에 대한 구성 매개 변수를 저장하는 가장 효율적인 방법을 결정하는 데 도움이 됩니다. 다음 질문을 고려하십시오.

1. 대부분의 웹 서비스가 보안 요구 사항이 동일한 대규모 서버 팜에 배포되어 있습니까?
2. 대부분의 웹 서비스를 중앙의 한 사람 또는 그룹이 관리합니까?
3. 대부분의 웹 서비스가 보안 요구 사항이 서로 다른 별도의 웹 서버에 배포되어 있습니까?
4. 대부분의 웹 서비스를 서로 다른 부서 또는 물리적 위치에 있는 서로 다른 사람이 관리합니까?

eTrust SOA Security Manager 는 다음과 같은 구성 방법을 제공합니다.

### 중앙 구성

앞의 목록에서 한 개 또는 두 개의 질문에 예라고 답한 경우에는 정책 서버에 있는 ACO(에이전트 구성 개체)에서 하나 이상의 SiteMinder WSS 에이전트를 관리하는 중앙 구성을 사용해 보십시오. 중앙 구성을 사용하면 여러 SiteMinder WSS 에이전트의 매개 변수 설정을 동시에 업데이트할 수 있습니다. 일반적으로 각기 다른 웹 서비스는 웹 서비스를 보호하는 모든 SiteMinder WSS 에이전트 사이에 설정이 공유되는 별개의 ACO 를 사용합니다. 예를 들어 하나의 회계 웹 서비스를 보호하는 SiteMinder WSS 에이전트가 5 개 있을 경우 이 웹 서비스에 대한 설정을 포함하는 ACO 를 하나 생성할 수 있습니다. 그러면 5 개의 SiteMinder WSS 에이전트는 모두 동일한 ACO 의 매개 변수 설정을 사용하게 됩니다.

각 응용 프로그램에 대해 별도의 에이전트 구성 개체를 사용하는 것이 좋습니다. 예를 들어 더 엄격한 보안 요구 사항으로 인사 관리 웹 서비스를 보호하려는 경우 이 웹 서비스에 대해 별도의 ACO 를 생성합니다.

SiteMinder WSS 에이전트는 시작 시 관련 ACO 에서 AllowLocalConfig 매개 변수의 값을 읽습니다. 이 값이 no 로 설정되어 있으면 SiteMinder WSS 에이전트는 해당 ACO 의 매개 변수 설정을 사용합니다.

**참고:** 가능하면 항상 중앙 에이전트 구성을 사용하는 것이 좋습니다. 그러면 에이전트 구성과 유지 관리가 간소해집니다.

### 로컬 구성

앞의 목록에서 세 개 또는 네 개의 질문에 예라고 답한 경우에는 각 SiteMinder WSS 에이전트가 서버 자체에 설치된 파일을 사용하여 관리되는 로컬 구성을 사용해 보십시오. SiteMinder WSS 에이전트가 시작되면 에이전트는 관련 ACO(에이전트 구성 개체)에서 AllowLocalConfig 매개 변수의 값을 읽습니다. 이 값이 yes 로 설정되어 있으면 SiteMinder WSS 에이전트는 응용 프로그램 또는 웹 서버에 있는 LocalConfig.conf 파일의 매개 변수 설정을 사용합니다. LocalConfig.conf 파일의 매개 변수 설정은 정책 서버의 ACO 에 저장된 모든 설정보다 우선합니다. 앞의 목록에서 세 개 또는 네 개의 질문에 예라고 답한 경우에는 다음 구성 방법을 사용해 보십시오.

**참고:** 응용 프로그램 또는 웹 서버에서 LocalConfig.conf 파일이 있는 위치에 대한 자세한 내용은 해당하는 SiteMinder WSS 에이전트 안내서를 참조하십시오.

또한 필요에 따라 중앙 및 로컬 구성의 조합을 사용할 수도 있습니다. 예를 들어 세 개의 비슷한 웹 서버는 중앙 구성으로 관리하고 다른 두 개의 서버는 로컬 구성으로 관리할 수 있습니다.

다음 질문은 로컬 에이전트 구성이 엔터프라이즈의 요구 사항을 더 잘 충족하는 다른 상황을 식별하는 데 도움이 됩니다.

- 엔터프라이즈에서 XML 게이트웨이에 사용자 지정 SiteMinder WSS 에이전트를 배포할 계획입니까?

  예를 들어 몇 군데 위치에 XML 게이트웨이를 구현하고 대규모 SiteMinder WSS 에이전트 그룹으로 내부 리소스를 보호하려는 경우가 있습니다. 이 경우 로컬 구성을 사용하여 XML 게이트웨이의 사용자 지정 SiteMinder WSS 에이전트를 관리할 수 있습니다.

- 로컬 서버 관리자가 SiteMinder WSS 에이전트 구성 설정의 일부만 변경할 수 있고 다른 설정은 변경하지 못하게 하려고 합니까?

  예를 들어 조직에서 SiteMinder 를 사용하여 보안 정책을 관리하고 적용하지만 원격 사무소의 응용 프로그램 및 웹 서버 관리자에게 로그온 및 로그오프 페이지를 사용자 지정할 수 있게 허용하는 경우가 있습니다. ACO 의 AllowLocalConfig 매개 변수의 값에 개별 매개 변수를 추가하여 관리자가 사용자 지정된 페이지의 설정만 변경할 수 있고 다른 설정은 변경하지 못하게 만들 수 있습니다.

# 데이터 센터 식별

여러 데이터 센터에서 SiteMinder 구성 요소를 구현하는 방법을 결정하는 데는 뒤에서 설명할 여러 가지 요소가 영향을 미칩니다. SiteMinder 구성 요소를 구현하는 방법을 결정할 때 데이터 센터를 식별하고 각 데이터 센터가 SiteMinder 환경에서 수행하는 역할을 파악하면 보다 자세한 정보를 바탕으로 결정할 수 있습니다. 다음 질문을 고려하십시오.

- 배포에 포함된 데이터 센터는 몇 개이며 각 데이터 센터의 위치는 어디입니까?
- 데이터 센터가 여러 개인 경우:
  - 모두 활성입니까? 아니면 일부는 재난 복구나 백업 전용입니까?
  - 보호되는 각 응용 프로그램이 단일 데이터 센터에 있습니까? 아니면 여러 센터에 분산되어 있습니까?
  - 장애 조치를 데이터 센터 수준에서 구성할 계획입니까? 아니면 여러 데이터 센터에 걸쳐 구성할 계획입니까?
  - 데이터 센터 간의 대역폭과 처리량은 어느 정도입니까?

각 데이터 센터에 대한 정보를 수집할 때는 다음과 비슷한 리소스 표를 사용하여 결과를 구성하십시오.

| 데이터 센터 이름 | 위치 | 용도 |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

**추가 정보:**

다중 데이터 센터 (페이지 130)

# AES(Advanced Encryption Standards)가 필요한지 여부 결정

조직에서 FIPS(Federal Information Processing Standard) 140-2 호환 알고리즘을 사용해야 합니까?

AES(Advanced Encryption Standard)의 SiteMinder 구현은 FIPS 140-2 표준을 지원합니다. FIPS 는 AES 를 충족하는 암호화 모듈을 인가하는 데 사용되는 미국 정부의 컴퓨터 보안 표준입니다.

정책 서버는 인증된 FIPS 140-2 호환 암호화 라이브러리를 사용합니다. 이러한 암호화 라이브러리는 SiteMinder 환경에서 중요한 데이터를 암호화하는 데 AES 호환 알고리즘만 사용하는 경우에 FIPS 작동 모드를 지원합니다. SiteMinder 환경은 다음과 같은 FIPS 작동 모드 중 하나에서 작동할 수 있습니다.

- FIPS 호환성
- FIPS 전용

**참고:** SiteMinder 에서 사용하는 암호화 라이브러리와 FIPS 전용 모드에서 중요한 데이터를 암호화하는 데 사용되는 AES 알고리즘에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오. FIPS 작동 모드 및 정책 서버를 설치할 때 사용할 모드에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

FIPS 전용 모드를 통한 AES 암호화를 구현할 경우에는 다음 사항을 고려하십시오.

- 디렉터리 서버, 데이터베이스 및 드라이버를 포함한 모든 타사 구성 요소는 FIPS 호환 알고리즘을 지원하도록 구성되어야 합니다.

  **참고:** 공급업체가 FIPS 140-2 표준을 지원하는지 여부에 대한 자세한 내용은 공급업체의 설명서를 참조하십시오.
- 환경에서 X.509 클라이언트 인증서 인증 체계를 사용하는 경우 사용자 인증서가 FIPS 호환 알고리즘만 사용하여 생성되어야 합니다.

- 정책 서버를 SSL 을 사용하여 정책 저장소 또는 사용자 저장소에 연결할 경우에는 정책 서버와 디렉터리 저장소가 FIPS 호환 인증서를 사용하는지 확인하십시오.
- SiteMinder 12.x 와 함께 제공되는 모든 SiteMinder WSS 에이전트는 FIPS 와 호환됩니다. 에이전트가 FIPS 와 호환되는지 여부를 확인하려면 에이전트의 설명서를 참조하십시오.

**중요!** FIPS 전용 모드로 실행 중인 환경은 이전 버전의 SiteMinder 와 함께 운용될 수 없으며 이전 버전의 SiteMinder 와 호환되지도 않습니다. 이 요구 사항에는 모든 에이전트, 이전 버전의 eTrust SOA Security Manager SDK 를 사용하는 사용자 지정 소프트웨어가 포함됩니다. FIPS 전용 모드에 필요한 지원을 받으려면 이러한 모든 소프트웨어를 SDK 의 현재 버전과 다시 연결하십시오.

# 가상화 사용 여부 결정

SiteMinder 를 가상 환경으로 구현할 계획입니까?

SiteMinder 를 가상 환경으로 구현하기 전에 다음 사항을 고려하십시오.

- CA policy on virtualization (가상화에 대한 CA 정책)을 검토하십시오.
- 다음을 확인하십시오.
  - 호스트 시스템이 응용 프로그램에 부과할 수 있는 성능 오버헤드와 가상 환경을 이해하십시오.
  - 성능 오버헤드가 최대한 제거되도록 가상 환경을 조정하십시오.

    **참고:** 가상 환경의 성능 조정에 대한 자세한 내용은 공급업체의 설명서를 참조하십시오.
- CPU, 디스크 공간 및 메모리의 크기를 가상 환경에 맞게 조정해야 합니다. 각 SiteMinder 설치 안내서에서 설명하는 시스템 요구 사항을 사용하여 시스템 전체에 배포할 구성 요소의 양을 결정하십시오.
- 클록 동기화 및 다중 운영 체제와 관련된 문제를 파악하십시오. 클록이 동기화되지 않으면 예기치 않은 SiteMinder 동작이 발생할 수 있습니다.

- 구성 요소 배포 위치를 고려할 때:
  - 정책 서버를 가상 환경에 배포하는 것이 좋습니다. 정책 서버에 자체 이더넷 포트가 있는 것이 좋습니다. SiteMinder 는 사용 가능한 대역폭을 두고 가상 호스트와 경쟁하므로 전용 포트를 사용하면 요청이 누락되는 것을 방지할 수 있습니다.
  - 웹 에이전트는 가상화된 웹 서버에 배포하는 것이 좋습니다.
  - SiteMinder 데이터 저장소는 모두 물리적 하드웨어 및 운영 체제에 배포하는 것이 좋습니다. 디렉터리 서버 및 데이터베이스는 리소스의 영향을 크게 받을 수 있습니다. 가상화된 환경에 배포될 경우 이러한 영향 때문에 성능이 저하될 수 있습니다.

# 정책 서버 관리 방법 결정

각 비즈니스 단위가 정책 서버의 관리를 책임져야 합니까? 아니면 하나의 비즈니스 단위가 중앙에서 모든 정책 서버를 관리할 수 있습니까?

**로컬 정책 서버 관리**

각 비즈니스 단위가 정책 서버와 정책 저장소를 로컬로 관리하는 경우에는 로컬 정책 서버 관리가 다음과 같은 특징이 있다는 점을 고려하십시오.

- 각 비즈니스 단위가 개별적인 필요에 따라 보안 요구 사항을 직접 관리할 수 있게 됩니다.
- SiteMinder 인프라의 복잡성이 증가할 수 있습니다. 로컬 정책 서버 관리를 사용하면 관리하고 업그레이드해야 할 정책 서버와 정책 저장소의 수가 늘어날 수 있습니다.
- SiteMinder 관리자가 서로 다른 비즈니스 단위에 있기 때문에 SiteMinder 핵심 개체, 정책 및 응용 프로그램 개체의 일관된 구현과 관리가 더 까다로워질 수 있습니다.

### 중앙 정책 서버 관리

단일 비즈니스 단위가 정책 서버를 로컬로 관리할 경우 중앙 정책 서버 관리에는 다음과 같은 특징이 있다는 점을 고려하십시오.

- 모든 SiteMinder 관리자가 동일한 비즈니스 단위에 있으므로 SiteMinder 핵심 개체, 정책 및 응용 프로그램 개체를 일관성 있게 구현하기가 용이합니다.
- 모든 SiteMinder 관리자가 동일한 비즈니스 단위에 있기 때문에 이러한 개체를 관리하기가 더 용이합니다.

  **참고:** 그림에서처럼 개별 비즈니스 단위는 응용 프로그램을 보호하면서 SiteMinder 에이전트를 계속 관리할 수 있습니다.
- SiteMinder 인프라를 단순화할 수 있습니다. 중앙 관리를 사용하면 관리하고 업그레이드해야 할 정책 서버와 정책 저장소의 수가 줄어듭니다.
- 관리자가 SiteMinder 성능을 중앙에서 모니터링할 수 있습니다.

# SiteMinder WSS 에이전트 관리 방법 결정

동일하게 구성할 여러 개의 SiteMinder WSS 에이전트가 있는 경우 정책 서버에서 에이전트 구성 개체를 사용하면 에이전트를 더 쉽게 관리할 수 있습니다. 단일 에이전트 구성 개체를 공유할 수 있는 SiteMinder WSS 에이전트 수에는 제한이 없습니다. 정책 서버에서 구성을 변경하면 변경 내용은 구성 개체를 사용하는 모든 SiteMinder WSS 에이전트에 자동으로 적용됩니다.

**참고:** 에이전트 관련 개체를 구성하는 방법에 대한 자세한 내용은 *eTrust SOA Security Manager Policy Configuration Guide*(eTrust SOA Security Manager 정책 구성 안내서)와 사용 중인 SiteMinder WSS 에이전트 유형에 해당하는 SiteMinder WSS 에이전트 안내서를 참조하십시오.

# 제 5 장: SiteMinder 용량 계획

이 섹션은 다음 항목을 포함하고 있습니다.



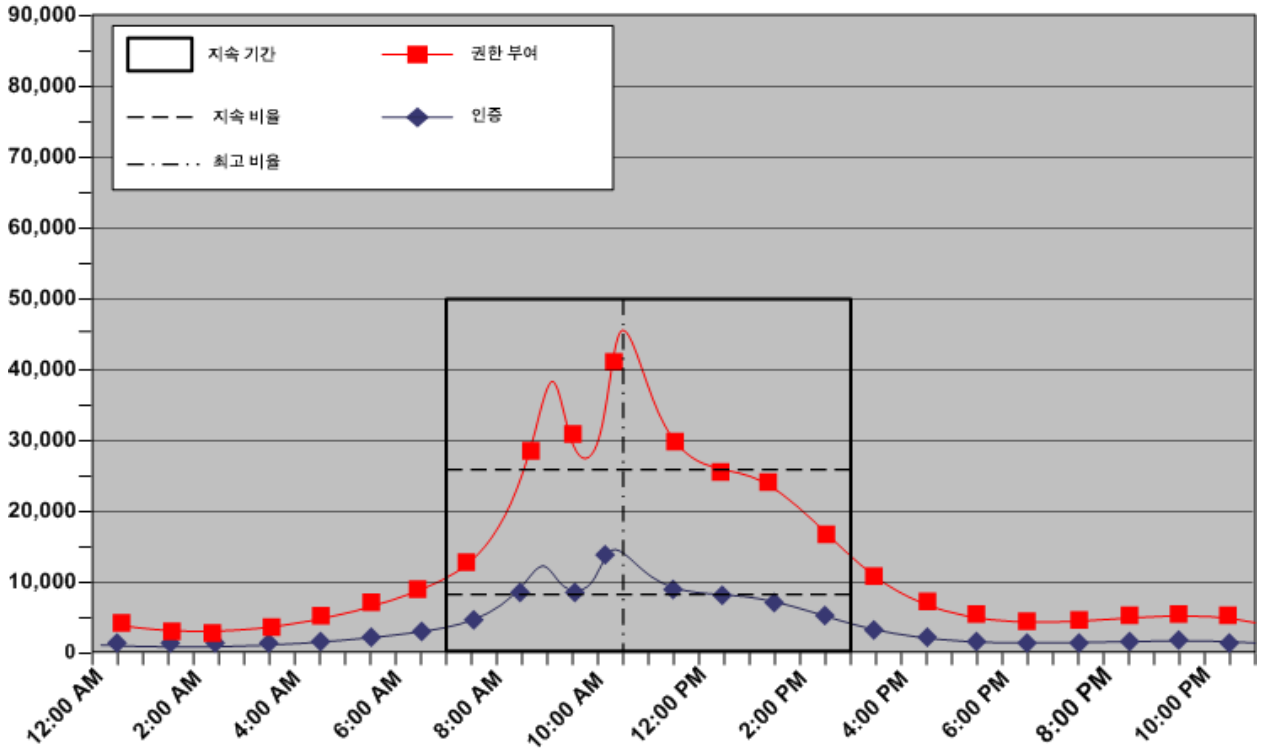
## 용량 계획 소개

성능을 염두에 두고 SiteMinder 배포 계획을 수립하는 것은 높은 수준의 엔터프라이즈 가용성과 성능 표준을 유지 관리하기 위한 첫 단계입니다. 이를 위한 좋은 접근 방법은 응용 프로그램 하나마다 SiteMinder 가 처리해야 하는 예상 인증 및 권한 부여의 수를 추정하는 것입니다. SiteMinder 의 성능에 영향을 미치는 일반적인 요소는 다음과 같습니다.

- 지속적 인증 및 권한 부여 비율. 사용자가 응용 프로그램에 대해 인증을 받고 보호된 리소스를 요청하는 비율은 업무일 내내 크게 변화합니다. 어떤 시간대에는 인증 요청이 생성되는 수가 비교적 적고 따라서 권한 부여 요청의 수도 비교적 적지만 다른 시간대에는 요청이 더 많이 생성됩니다. 지속적 인증 및 권한 부여 비율은 SiteMinder 가 평균적인 숫자의 인증 및 권한 부여 요청을 처리해야 하는 지속적인 기간을 나타냅니다.
- 최고 인증 및 권한 부여 비율. 지속적 활동 기간 동안 사용자 활동이 급증할 수 있습니다. 최고 인증 및 권한 부여 비율은 SiteMinder 가 가장 많은 수의 인증 및 권한 부여 요청을 처리해야 하는 기간을 나타냅니다.

  **참고:** 성능 조정 및 네트워크 대역폭과 같은 여러 가지 다른 요소가 SiteMinder 성능에 영향을 미칠 수 있지만, 앞에서 언급한 요소들은 정책 서버와 에이전트를 구현할 때 그리고 기존 사용자 저장소가 예상 SiteMinder 작업 부하를 처리할 수 있는지를 결정할 때 보다 풍부한 정보를 바탕으로 결정을 내리는 데 도움이 됩니다.

다음 그림은 하루 동안 인증 및 권한 부여 비율이 변동하는 모습, 특정 기간 동안 일정하게 유지되는 모습 및 그 기간 동안의 최고 지점을 보여 줍니다.




**참고:** 사용자를 인증하고 사용자에게 권한을 부여하면 많은 수의 읽기가 수행되며 암호 정책이 활성화되면 사용자 저장소에 많은 쓰기가 수행됩니다. 지속 비율과 최고 비율을 파악하면 사용자 저장소가 정책 서버 요청을 처리하기 위해 작동하는 데 가해지는 부하를 알 수 있습니다.

**추가 정보:**

성능 조정 소개 (페이지 149)

# 사용 사례: 용량 계획 수립

다음 사용 사례는 가상의 조직이 응용 프로그램 사용을 모델링하여 용량 계획을 수립하는 방법을 보여 주기 위한 것입니다. 이 사용 사례는 이 장 전체에서 예제로 사용합니다.

회사에서 SiteMinder 를 배포할 계획입니다. 현재 하나의 사용자 저장소에 100,000 명의 사용자가 있습니다. 이 저장소에는 암호 서비스가 활성화되어 있습니다.

어떤 사용자는 포털 응용 프로그램에 하루에 한 번 로그인하지만 다른 사용자는 하루에 세 번 로그인하기도 합니다.

# 지속적 인증 비율을 추정하는 방법

응용 프로그램의 지속적 인증 비율을 추정할 때는 다음을 확인해야 합니다.

- 업무일 중 총 인증 요청 수의 변동
- 인증 요청을 초당 인증 수로 변환하는 방법

응용 프로그램의 지속적 인증 비율을 추정하려면 다음 단계를 완료하십시오.

1. 일별 인증 수를 추정합니다.
2. 지속적 인증 비율을 추정합니다.

## 일별 인증 수 추정

응용 프로그램에 대한 대략적인 일별 인증 수를 추정해 보겠습니다.

사용자의 수는 일별 인증 수(인증 부하)에 직접적인 영향을 미칩니다. 사용자가 응용 프로그램에 로그인할 때 SiteMinder 가 해당 사용자를 인증합니다. 따라서 응용 프로그램의 인증 부하는 일별 총 로그인 수라고 생각할 수 있습니다.

**참고:** 인증 부하를 확인할 때는 24 시간 단위의 평가 기간으로 시작하는 것이 좋습니다. 하지만 엔터프라이즈의 요구 사항에 따라 하루 동안의 결과를 몇 주 또는 몇 개월 동안 비교하면 연중 사용 처리량을 더 정확하게 파악할 수 있습니다.

모든 사용자가 매일 응용 프로그램에 로그인할 가능성은 거의 없으므로 총 로그인 수의 추정은 하루에 한 번 로그인하는 사용자의 비율을 확인하는 데서 시작하며, 계산 방법은 다음과 같습니다.

(*total_users* * *percentage_users*) * (*number_of_logins*) = *daily_logins*

***total_users***

응용 프로그램에 액세스할 수 있는 총 사용자 수를 나타냅니다.

***percentage_users***

하루에 같은 횟수로 로그인하는 사용자의 비율을 나타냅니다.

***number_of_logins***

특정 사용자 집합이 로그인하는 횟수를 나타냅니다.

***daily_logins***

특정 사용자 집합이 수행하는 로그인 횟수를 나타냅니다.

**예 1:** 회사의 사용자 수는 100,000 명이며 그중 75 %가 하루에 한 번 로그인합니다.

(100,000 * 0.75) x (1) = 75,000 회 로그인

하지만 일부 사용자는 응용 프로그램에 하루에 두 번 이상 로그인할 가능성이 더 많습니다.

**예 2:** 회사의 사용자 수는 100,000 명이며 그중 5 %가 하루에 두 번 로그인하고 1 %는 하루에 세 번 로그인합니다.

(100,000 * 0.05) x (2) = 10,000 회 로그인

(100,000 * 0.01) x (3) = 3,000 회 로그인

하루의 총 로그인 수는 각 로그인 계산의 합계입니다.

**예 3:** 회사의 사용자 수는 100,000 명이며

- 그중 75 %가 하루에 한 번 로그인하여 총 75,000 회의 로그인을 생성합니다.
- 그중 5 %는 하루에 두 번 로그인하여 10,000 회의 로그인을 생성합니다.
- 그중 1 %는 하루에 세 번 로그인하여 3,000 회의 로그인을 생성합니다.

포털 응용 프로그램의 인증 부하는 88,000 회의 로그인입니다.

**참고:** 모든 사용자가 매일 응용 프로그램에 로그인하는 것이 아니기 때문에 로그인하는 사용자의 백분율이 100 %일 필요는 없습니다.

다음 표는 앞에 나온 각각의 예를 보여 줍니다.

| 총 사용자 수 | 총 사용자 수의 비율 | 일별 로그인 수 | 로그인 수 |
|---|---|---|---|
| 100,000 | 75 | 1 | 75,000 |
| 100,000 | 5 | 2 | 10,000 |
| 100,000 | 1 | 3 | 3,000 |
| **인증 부하** | | | **88,0000** |

회사에서는 인증 부하를 사용하여 지속적 인증 비율을 추정합니다.

## 지속적 인증 비율 추정

응용 프로그램에 대한 지속적 인증 비율을 추정해 보겠습니다.

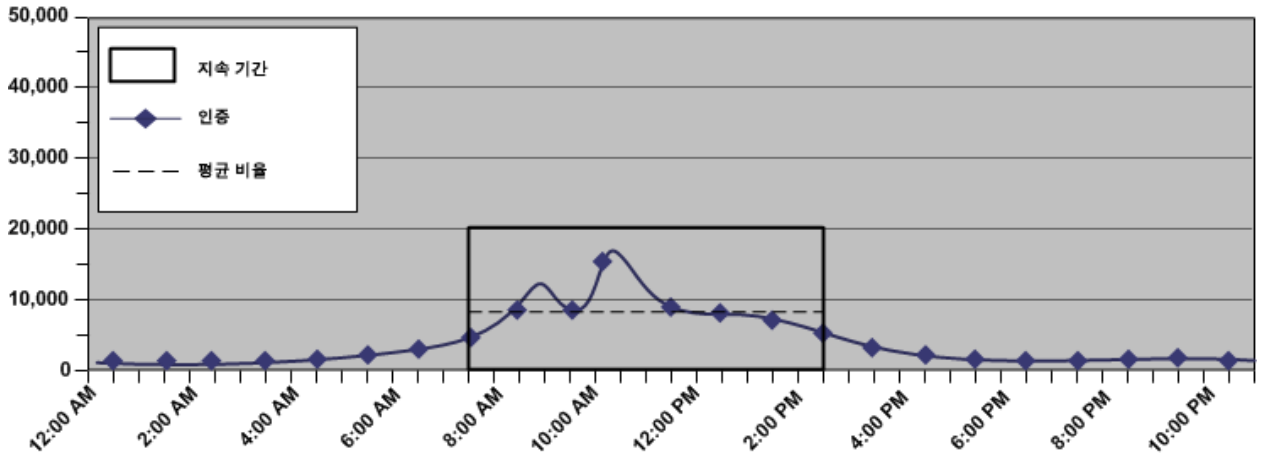
지속적 인증 비율은 인증 부하를 기반으로 합니다. 구체적으로 말하면 인증이 일어나는 시기와 비율을 의미합니다. 인증 부하가 업무일 동안 균등하게 분산될 가능성은 거의 없습니다. 대신 요청이 발생하는 비율은 지속 기간 동안 가장 낮은 수준과 가장 높은(최고) 수준 내에서 크게 변동합니다. 지속적 인증 비율을 추정하려면 시스템이 평균적인 양의 인증 요청을 처리하는 지속 기간을 식별해야 합니다.

지속적 인증 비율을 추정할 때는 일별 인증 부하를 사용하여 다음을 파악하는 것이 좋습니다.

- 업무일 동안 인증 요청이 발생하는 비율

  **참고:** 1 시간 단위로 분할된 24 시간의 평가 기간부터 시작하는 것이 좋습니다. 하지만 엔터프라이즈의 요구 사항에 따라 하루 동안의 결과를 몇 주 또는 몇 개월 동안 비교하면 연중 사용 처리량을 더 정확하게 파악할 수 있습니다.
- 시스템이 평균적인 수의 인증 요청을 처리하는 지속 기간
- 지속 기간 동안 발생하는 대략적인 인증 요청 수

다음 그림은 이러한 메트릭의 예입니다.




이러한 메트릭을 식별하면 사용자가 인증하는 평균 비율을 유지하기 위해 SiteMinder 가 처리해야 하는 초당 인증 요청 수를 추정할 수 있습니다. 계산 방법은 다음과 같습니다.

(*authentication_load* * *percentage_of_authentication_requests*) / *number_of_sustained_hours* / 3600 = *sustained_authentication_rate*

***authentication_load***

응용 프로그램에 대한 일별 인증 수를 나타냅니다.

***percentage_of_authentication_requests***

시스템이 지속 수준에서 작동할 때 발생하는 인증 요청의 백분율을 나타냅니다.

**예:** 인증 부하가 50,000 회의 로그인이고 지속 기간 동안 32,000 회의 로그인이 발생할 경우 값은 64 %(0.64)입니다.

***number_of_sustained_hours***

시스템이 지속 수준에서 작동하는 시간을 나타냅니다.

**참고:** 3,600 은 1 시간에 해당하는 초를 나타냅니다.

***sustained_authentication_rate***

지속 활동 기간 동안 SiteMinder 가 처리해야 하는 초당 인증 요청 수를 나타냅니다.

### 예: 지속 인증 비율 추정

회사에서 응용 프로그램 포털의 인증 부하가 88,000 회의 로그인임을 확인했습니다. 응용 프로그램 포털은 고객이 연중 무휴로 하루 24 시간 사용할 수 있습니다. 시스템 활동 보고서를 사용하여 일반적인 일일 결과를 분석한 결과는 다음과 같습니다.

- 시스템은 약 5 시간(오전 9 시 - 오후 2 시) 동안 지속 수준에서 작동합니다.
- 지속 수준에서 시간당 약 9,000 개의 인증 요청이 발생합니다.
- 이 시간 동안 약 45,000(9,000 * 5)회의 인증 요청 또는 일별 인증 부하의 51 %(45,000/88,000)가 발생합니다.

(88,000 * 0.51) / 5 / 3600 = 초당 2.49 회의 인증.

포털 응용 프로그램의 지속 인증 비율은 초당 2.49 회의 인증입니다.

## 최고 인증 비율 추정

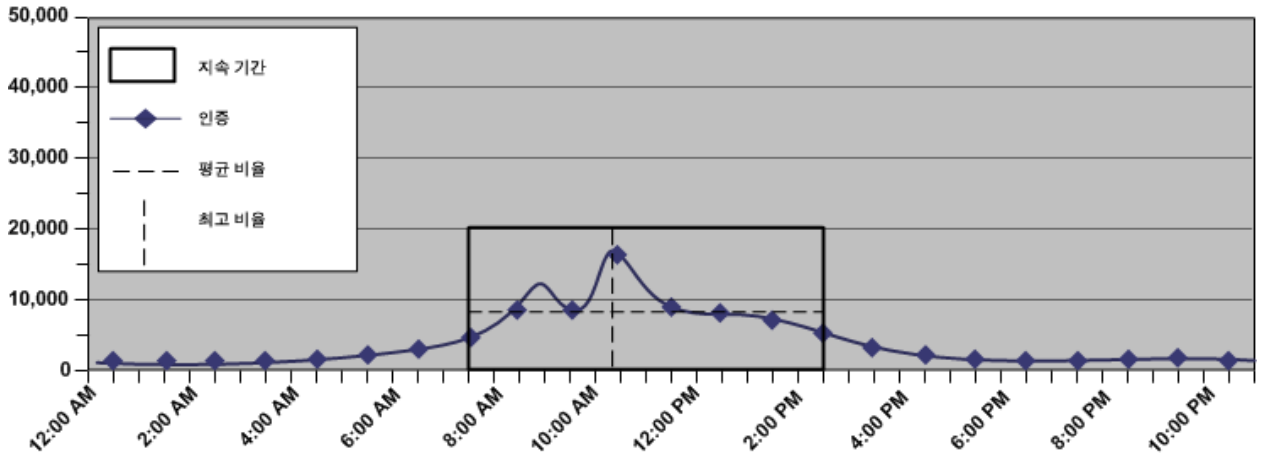
응용 프로그램에 대한 최고 권한 부여 비율을 추정해 보겠습니다.

최고 인증 비율은 지속 인증 비율, 즉 시스템이 최고 수준으로 작동하는 시기와 비율을 기반으로 합니다. 최고 인증 비율을 추정하려면 시스템이 최고 수준의 인증 요청을 처리하는 시점을 식별해야 합니다.

최고 인증 비율을 추정할 때는 지속 인증 비율을 확인할 때 수집한 메트릭을 사용하여 다음을 확인하는 것이 좋습니다.

- 시스템이 가장 많은 수의 인증 요청을 처리하는 시간
- 이 기간 동안 발생하는 대략적인 인증 요청 수

다음 그림은 이러한 메트릭의 예입니다.




이러한 메트릭을 식별하면 사용자가 인증하는 최고 비율을 유지하기 위해 SiteMinder 가 처리해야 하는 초당 인증 요청 수를 추정할 수 있습니다. 계산 방법은 다음과 같습니다.

(*authentication_load* x *percentage_of_transactions*) / *number_of_hours* / 3600 = *peak_authentication_rate*

**참고**: 이 비율은 가장 작업량이 많은 1 시간을 기반으로 합니다. 최고 인증 비율이 시간별 계산을 초과하는 기간이 있을 수 있습니다.

***authentication_load***

응용 프로그램에 대한 일별 인증 수를 나타냅니다.

***percentage_of_transactions***

시스템이 최고 수준에서 작동할 때 발생하는 트랜잭션의 백분율을 나타냅니다.

***number_of_hours***

시스템이 최고 수준에서 작동하는 시간을 나타냅니다.

**참고:** 3,600 은 1 시간에 해당하는 초를 나타냅니다.

***peak_authentication_rate***

응용 프로그램에 대한 최고 인증 비율을 나타냅니다.

### 예: 최고 인증 비율 추정

회사에서 포털 응용 프로그램의 일별 인증 비율이 88,000 회의 로그인임을 확인했습니다. 시스템 활동 보고서에는 하루 중 가장 작업량이 많은 1 시간 동안 18,000 회의 인증 요청이 발생한 것으로 보고됩니다. 이 숫자는 인증 부하의 약 20 %를 나타냅니다.

18,000 / 1 / 3600 = 초당 5 회 인증

포털 응용 프로그램의 최고 인증 비율은 초당 5 회의 인증입니다.

**참고**: 이 예는 가장 작업량이 많은 1 시간을 기반으로 합니다. 시간 중 최고 인증 비율이 초당 5 회 인증을 초과하는 기간이 있을 수 있습니다.

**추가 정보:**

에이전트에서 사용 가능한 소켓의 양 늘리기 (페이지 156)

## 지속적 권한 부여 비율을 추정하는 방법

응용 프로그램에 대한 지속적 권한 부여 비율을 추정하려면 다음을 확인해야 합니다.

- 하루 중 총 권한 부여 요청 수가 변동하는 상태
- 권한 부여 요청을 초당 요청 수로 변환하는 방법

응용 프로그램의 최고 권한 부여 비율을 추정하려면 다음 단계를 완료하십시오.

1. 일별 권한 부여 수를 추정합니다.
2. 지속적 권한 부여 비율을 추정합니다.

## 일별 권한 부여 수 추정

응용 프로그램에 대한 대략적인 일별 권한 부여 수를 추정해 보겠습니다.

총 로그인 수(인증 부하) 및 각 인증된 사용자의 페이지 "방문 횟수"가 일별 권한 부여 수(권한 부여 부하)에 직접적인 영향을 미칩니다. 웹 페이지 "방문 횟수"에는 일반적으로 권한 부여가 필요합니다. 따라서 응용 프로그램의 권한 부여 부하를 일별 총 권한 부여 수라고 생각할 수 있습니다.

**참고:** 권한 부여 부하를 추정할 때는 24 시간의 평가 간격으로 시작하는 것이 좋습니다. 하지만 엔터프라이즈의 요구 사항에 따라 하루 동안의 결과를 몇 주 또는 몇 개월의 기간 동안 비교하면 연중 사용 처리량을 더 정확하게 파악할 수 있습니다.

모든 사용자가 로그인할 때마다 동일한 수의 페이지를 요청할 가능성은 거의 없으므로 총 권한 부여 수의 계산은 하나의 페이지 방문 횟수를 생성하는 로그인의 백분율을 확인하는 작업부터 시작합니다. 계산 방법은 다음과 같습니다.

*authentication_load * percentage_of_authenticated_users * page_visits = daily_authorizations*

***authentication_load***

응용 프로그램에 대한 대략적인 일별 인증 수를 나타냅니다.

***percent_of_authenticated_users***

로그인 후 동일한 수의 페이지를 방문하는 인증된 사용자의 백분율을 나타냅니다.

***page_visits***

특정한 인증된 사용자 집합이 로그인 후 방문하는 페이지 수를 나타냅니다.

**참고:** 페이지에 여러 개의 개체가 포함되어 있기 때문에 GET/POST 가 여러 개 발생할 수 있습니다. 페이지당 총 권한 부여 수는 GET 요청의 수에 POST 요청의 수를 더한 값에 웹 에이전트가 무시하는 확장의 수를 뺀 값입니다. 이 안내서에서 다음의 각 예에서는 한 번의 페이지 방문이 하나의 GET/POST 를 생성한다고 가정합니다. 정책을 확인하지 않고 특정 리소스 유형에 대한 액세스를 허용하도록 웹 에이전트를 구성하는 방법에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

***daily_authorizations***

인증된 사용자의 특정 집합에 필요한 권한 부여의 수를 나타냅니다.

### 예 1: 일별 권한 부여 수 추정

일별 인증 수 추정 (페이지 105)에서 설명한 것처럼 포털 응용 프로그램의 인증 부하는 88,000 회의 로그인입니다. 이중에서 25 %가 로그인 후 1 개의 페이지를 방문합니다.

88,000 * 0.25 * 1 = 22,000 회의 권한 부여

하지만 일부 로그인은 두 개 이상의 페이지 방문 횟수를 생성할 가능성이 더 많습니다.

### 예 2: 일별 권한 부여 수 추정

포털 응용 프로그램의 인증 부하는 88,000 회의 로그인입니다.

- 이중에서 50 %는 로그인 후 10 개의 페이지를 방문합니다.
- 이중에서 25 %는 로그인 후 15 개의 페이지를 방문합니다.

88,000 * 0.5 * 10 = 440,000 회의 권한 부여

88,000 * 0.25 * 15 = 330,000 회의 권한 부여

일별 총 권한 부여 수(권한 부여 부하)는 각 권한 부여 계산의 합입니다.

### 예 3: 일별 권한 부여 수 추정

포털 응용 프로그램의 인증 부하는 88,000 회의 로그인입니다.

- 이중에서 25 %는 로그인 후 1 개의 페이지 방문 횟수를 생성하여 22,000 회의 권한 부여를 생성합니다.
- 이중에서 50 %는 로그인 후 10 개의 페이지 방문 횟수를 생성하여 440,000 회의 권한 부여를 생성합니다.
- 이중에서 25 %는 로그인 후 15 개의 페이지 방문 횟수를 생성하여 330,000 회의 권한 부여를 생성합니다.

**참고:** 인증된 각 사용자는 최소 하나의 페이지 방문 횟수를 생성하므로 인증된 사용자의 백분율은 100 %여야 합니다.

따라서 포털 응용 프로그램의 권한 부여 부하는 792,000 회입니다.

다음 표는 앞에 나온 각각의 예를 보여 줍니다.

| 페이지 방문 횟수 | 총 로그인의 백분율 | 인증 부하 | 권한 부여 |
|---|---|---|---|
| 1 | 25 | 88,000 | 22,000 |
| 10 | 50 | 88,000 | 440,000 |
| 15 | 25 | 88,000 | 330,000 |
| **권한 부여 부하** | | | **792,000** |

회사에서는 권한 부여 부하를 사용하여 지속적 권한 부여 비율을 추정합니다.

## 지속적 권한 부여 비율 추정

응용 프로그램에 대한 지속적 권한 부여 비율을 추정해 보겠습니다.

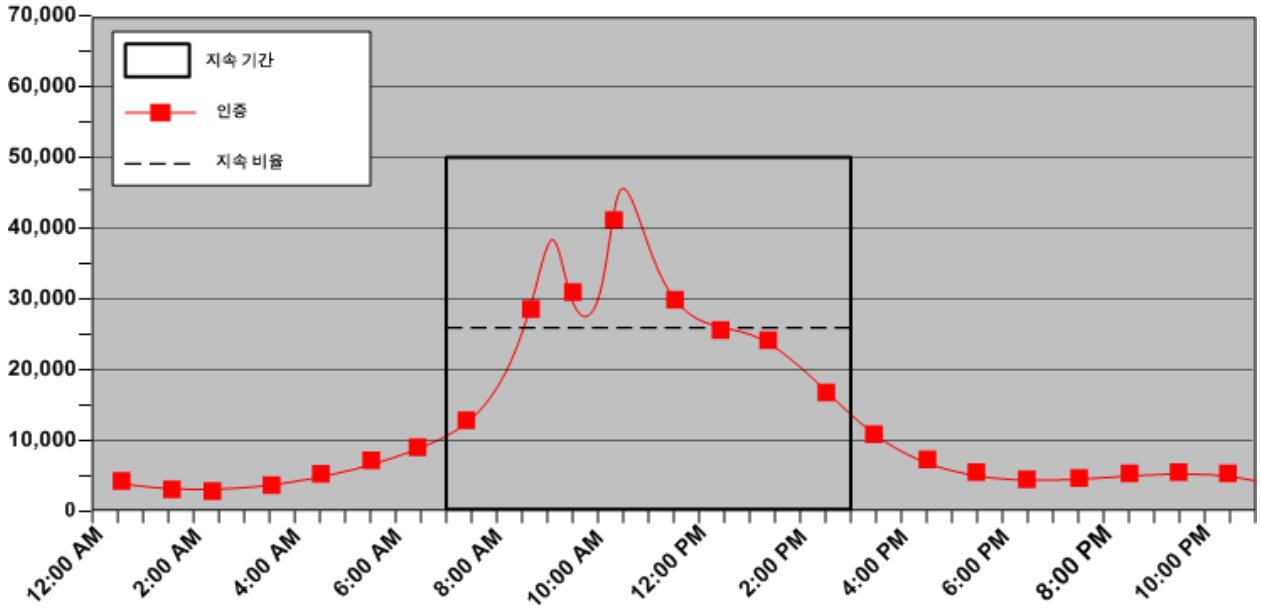
지속적 권한 부여 비율은 권한 부여 부하, 즉 권한 부여가 일어나는 시기와 비율을 기반으로 합니다. 권한 부여 부하가 업무일 동안 균등하게 분산될 가능성은 거의 없습니다. 대신 요청이 발생하는 비율은 지속 기간 동안 가장 낮은 수준과 가장 높은(최고) 수준 내에서 크게 변동합니다. 지속적 권한 부여 비율을 추정하려면 시스템이 평균적인 양의 권한 부여 요청을 처리하는 지속 기간을 식별해야 합니다.

지속적 권한 부여 비율을 추정할 때는 일별 권한 부여 부하를 사용하여 다음을 확인하는 것이 좋습니다.

- 영업일 중 권한 부여 요청이 발생하는 비율

  **참고:** 1 시간 단위로 분할된 24 시간의 평가 기간부터 시작하는 것이 좋습니다. 하지만 엔터프라이즈의 요구 사항에 따라 하루 동안의 결과를 몇 주 또는 몇 개월 동안 비교하면 연중 사용 처리량을 더 정확하게 파악할 수 있습니다.
- 시스템이 평균적인 양의 권한 부여 요청을 처리하는 지속 기간
- 지속 기간 동안 발생하는 대략적인 권한 부여 요청 수

다음 그림은 이러한 메트릭의 예입니다.




이러한 메트릭을 식별하면 권한 부여 요청이 발생하는 평균 비율을 유지하기 위해 SiteMinder 가 처리해야 하는 초당 권한 부여 요청 수를 추정하는 데 도움이 됩니다. 계산 방법은 다음과 같습니다.

(*authorization_load* * *percentage_of_authorization_requests*) / *number_sustained_hours* / 3600 = *sustained_authorization_rate*

***authorization_load***

응용 프로그램에 대한 일별 권한 부여 수를 나타냅니다.

***percentage_of_authorization_requests***

시스템이 지속 수준에서 작동할 때 발생하는 권한 부여 요청의 백분율을 나타냅니다.

**예:** 권한 부여 부하가 500,000 회의 요청이고 지속 기간 동안 320,000 회의 요청이 발생할 경우 값은 64 %(0.64)입니다.

***number_of_sustained_hours***

시스템이 지속 수준에서 작동하는 시간을 나타냅니다.

**참고:** 3,600 은 1 시간에 해당하는 초를 나타냅니다.

***sustained_authentication_rate***

지속 활동 기간 동안 SiteMinder 가 처리해야 하는 초당 권한 부여 요청 수를 나타냅니다.

### 예: 지속적 권한 부여 비율 추정

일별 권한 부여 수 추정 (페이지 112)에서 설명한 것처럼 포털 응용 프로그램의 권한 부여 부하는 792,000 회입니다. 응용 프로그램 포털은 고객이 연중 무휴로 하루 24 시간 사용할 수 있습니다. 시스템 활동 보고서를 사용하여 일반적인 일일 결과를 분석한 결과는 다음과 같습니다.

- 시스템은 약 5 시간(오전 9 시 - 오후 2 시) 동안 지속 수준에서 작동합니다.
- 지속 수준에서 시간당 약 75,000 회의 권한 부여 요청이 발생합니다.
- 이 시간 동안 약 375,000(75,000 * 5)회의 권한 부여 요청 또는 일별 권한 부여 부하의 47 %(375,000/792,000)가 발생합니다.

(762,000 * 0.47) / 5 / 3600 = 초당 19.90 회의 권한 부여

포털 응용 프로그램의 지속 권한 부여 비율은 초당 19.90 회의 권한 부여입니다.

## 최고 권한 부여 비율 추정

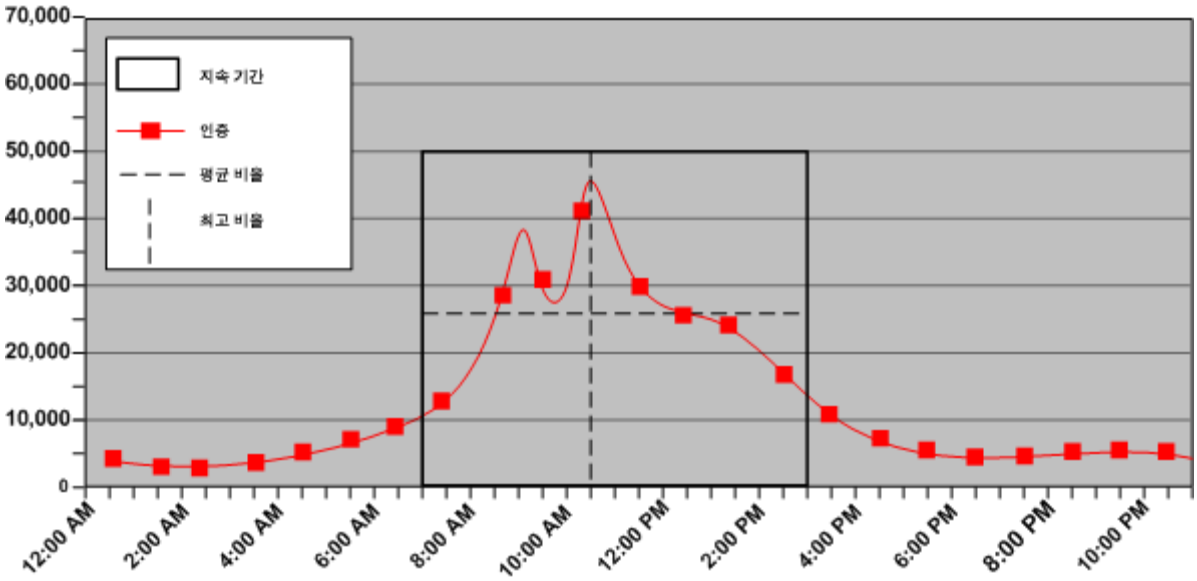
응용 프로그램에 대한 최고 권한 부여 비율을 추정해 보겠습니다.

최고 권한 부여 비율은 지속 권한 부여 비율, 즉 시스템이 최고 수준으로 작동하는 시기와 비율을 기반으로 합니다. 최고 권한 부여 비율을 추정하려면 시스템이 최고 수준의 권한 부여 요청을 처리하는 시기를 식별해야 합니다.

최고 권한 부여 비율을 추정할 때는 지속 권한 부여 비율을 확인할 때 수집한 메트릭을 사용하여 다음을 파악하는 것이 좋습니다.

- 시스템이 가장 많은 수의 권한 부여 요청을 처리하는 시간
- 이 기간 동안 발생하는 대략적인 권한 부여 요청 수

다음 그림은 이러한 메트릭의 예입니다.




이러한 메트릭을 식별하면 사용자가 인증하는 최고 비율을 유지하기 위해 SiteMinder 가 처리해야 하는 초당 인증 요청 수를 추정할 수 있습니다. 계산 방법은 다음과 같습니다.

(*authorization_load* * *percentage_of_transactions*) / *number_of_hours* / 3600 = *peak_authorization_rate*

**참고**: 이 비율은 가장 작업량이 많은 1 시간을 기반으로 합니다. 최고 권한 부여 비율이 시간별 계산을 초과하는 기간이 있을 수 있습니다.

***authorization_load***

응용 프로그램에 대한 일별 권한 부여 수를 나타냅니다.

***percentage_of_transactions***

시스템이 최고 수준에서 작동할 때 발생하는 트랜잭션의 백분율을 나타냅니다.

***number_of_hours***

시스템이 최고 수준에서 작동하는 시간을 나타냅니다.

***peak_authorization_rate***

응용 프로그램에 대한 최고 권한 부여 비율을 나타냅니다.

### 예: 최고 권한 부여 비율 추정

일별 권한 부여 수 추정 (페이지 112)에서 설명한 것처럼 포털 응용 프로그램의 권한 부여 부하는 792,000 회입니다. 시스템 활동 보고서에는 하루 중 가장 작업량이 많은 1 시간 동안 260,000 회의 권한 부여 요청이 발생한 것으로 보고됩니다. 이 숫자는 권한 부여 부하의 약 33 %입니다.

(792,000 * 0.33) / 1 / 3600 = 초당 72.6 회의 권한 부여

포털 응용 프로그램의 최고 인증 비율은 초당 72.6 회의 권한 부여입니다.

# 제 6 장: eTrust SOA Security Manager 용량 계획

이 섹션은 다음 항목을 포함하고 있습니다.



## 용량 계획 소개

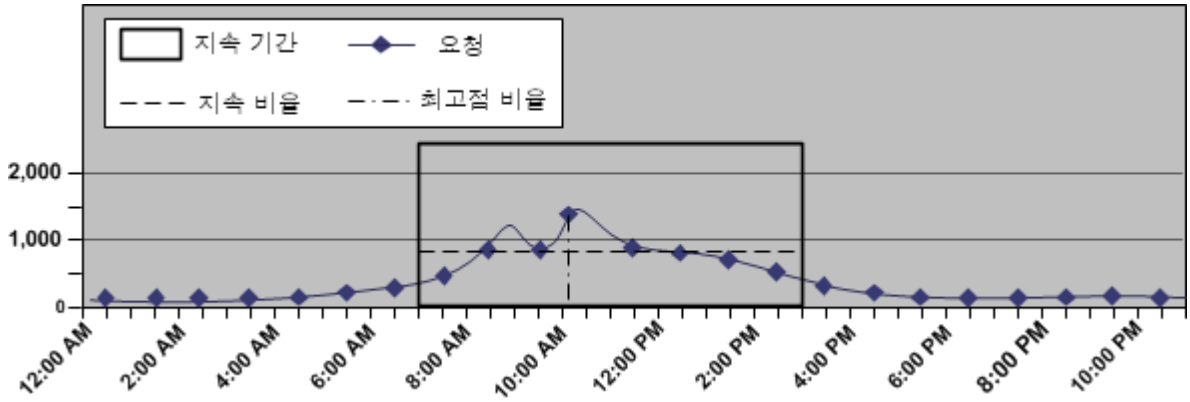
성능을 염두에 두고 eTrust SOA Security Manager 배포 계획을 수립하는 것은 높은 수준의 엔터프라이즈 가용성과 성능 표준을 유지 관리하기 위한 첫 단계입니다. 이를 위한 좋은 접근 방법은 웹 서비스 하나마다 SiteMinder 가 처리해야 하는 예상 요청의 수를 추정하는 것입니다. SiteMinder 성능에 영향을 미치는 가장 중요한 요인은 다음과 같습니다.

- 지속적 요청 비율. 웹 서비스 클라이언트가 보호된 웹 서비스 리소스에 대한 요청을 보내는 비율은 업무일 내내 크게 변화합니다. 어떤 시간대에는 요청이 생성되는 수가 비교적 적고 따라서 필요한 인증 및 권한 부여 수도 비교적 적지만 다른 시간대에는 요청이 더 많이 생성됩니다. 지속적 요청 비율은 SiteMinder 가 평균적인 숫자의 인증 및 권한 부여 요청을 처리해야 하는 지속적인 기간을 나타냅니다.

  **참고:** 각 웹 서비스 요청은 인증 및 권한 부여 이벤트를 각각 하나씩 트리거합니다.

- 최고 요청 비율. 지속적 활동 기간 동안 웹 서비스 클라이언트 활동이 급증할 수 있습니다. 최고 요청 비율은 SiteMinder 가 가장 많은 수의 인증 및 권한 부여 요청을 처리해야 하는 기간을 나타냅니다.

다음 그림은 하루 동안 요청 비율이 변동하는 모습, 특정 기간 동안 일정하게 유지되는 모습 및 그 기간 동안의 최고 지점을 보여 줍니다.




**참고:** 인증 및 권한 부여 요청을 수행하면 사용자 저장소에서 많은 읽기가 발생합니다. 지속 비율과 최고 비율을 파악하면 사용자 저장소가 정책 서버 요청을 처리하기 위해 작동하는 데 가해지는 부하를 알 수 있습니다.

**추가 정보:**

성능 조정 소개 (페이지 149)

# 사용 사례: 용량 계획 수립

다음 사용 사례는 서비스 이행 조직인 example.com 에서 조직의 주문 이행 웹 서비스 사용을 모델링하여 용량 계획을 수립하는 방법을 보여 주기 위한 것입니다. 이 사용 사례는 이 장 전체에서 예제로 사용합니다.

회사에서 eTrust SOA Security Manager 를 배포하여 웹 서비스를 보호할 계획입니다. 현재 단일 사용자 저장소에 10,000 명의 사용자가 있습니다.

일부 웹 서비스 클라이언트는 하루에 한 번 웹 서비스의 인벤토리 작업에 대한 단일 상태 요청을 보내는 반면, 다른 웹 서비스 클라이언트는 이행 작업에 대한 일괄 처리 주문 요청을 하루에 네 개씩 보낼 수 있습니다.

# 지속적 요청 비율을 추정하는 방법

웹 서비스에 대한 지속적 요청 비율을 추정하려면 다음을 확인해야 합니다.

- 업무일 중 총 요청 수의 변동
- 요청을 초당 요청 수로 변환하는 방법

웹 서비스의 지속적 요청 비율을 추정하려면 다음 단계를 수행하십시오.

1. 일별 요청 수 추정
2. 지속적 요청 비율 추정

## 일별 요청 수 추정

웹 서비스에 대한 대략적인 일별 요청 수를 추정해 보겠습니다.

웹 서비스 클라이언트의 수는 일별 요청(요청 부하)에 직접적인 영향을 미칩니다. 웹 서비스 클라이언트가 요청을 웹 서비스에 보내면 SiteMinder 가 해당 요청을 인증합니다. 따라서 웹 서비스의 요청 부하는 일별 총 요청 수라고 생각할 수 있습니다.

**참고:** 요청 부하를 확인할 때는 24 시간 단위의 평가 기간으로 시작하는 것이 좋습니다. 하지만 엔터프라이즈의 요구 사항에 따라 하루 동안의 결과를 몇 주 또는 몇 개월 동안 비교하면 연중 사용 처리량을 더 정확하게 파악할 수 있습니다.

모든 웹 서비스 클라이언트가 매일 웹 서비스에 요청을 보낼 가능성은 거의 없으므로 총 요청 수의 추정은 하루에 한 번 요청을 보내는 웹 서비스 클라이언트의 비율을 확인하는 데서 시작하며, 계산 방법은 다음과 같습니다.

(*total_clients* * *percentage_clients*) * (*number_of_requests*) = *daily_logins*

***total_clients***

응용 프로그램에 액세스할 수 있는 총 클라이언트 수를 나타냅니다.

***percentage_clients***

하루에 같은 횟수로 요청을 보내는 클라이언트의 백분율을 나타냅니다.

***number_of_requests***

특정 클라이언트 집합이 요청을 보내는 횟수를 나타냅니다.

***daily_logins***

특정 클라이언트 집합이 생성하는 로그인 횟수를 나타냅니다.

### 예

회사의 사용자 수는 10,000 명이며, 그중 60%가 하루에 한 번 인벤토리 상태 요청을 보냅니다.

(10,000 * 0.6) x (1) = 6,000 회 로그인

또한, 사용자의 30%는 매일 1 회의 주문 이행 요청을 보내고, 20%는 매일 2 회의 주문 이행 요청을 보내며, 매일 3 회 및 4 회의 주문 이행 요청을 보내는 사용자도 각각 10%에 달합니다.

(10,000 * 0.3) x (1) = 3,000 회 로그인

(10,000 * 0.2) x (2) = 4,000 회 로그인

(10,000 * 0.1) x (3) = 3,000 회 로그인

(10,000 * 0.1) x (4) = 4,000 회 로그인

하루의 총 요청 수는 계산된 각 요청 수의 합계입니다. 따라서 이행 웹 서비스에 대한 요청 부하는 20,000 회의 로그인입니다.

**참고:** 모든 클라이언트가 반드시 매일 서비스 요청을 보내지는 않으므로 요청하는 클라이언트의 백분율이 반드시 100%가 되지는 않습니다.

회사에서는 요청 부하를 사용하여 지속적 요청 비율을 추정합니다.

## 지속적 요청 비율 추정

웹 서비스에 대한 지속적 요청 비율을 추정해 보겠습니다.

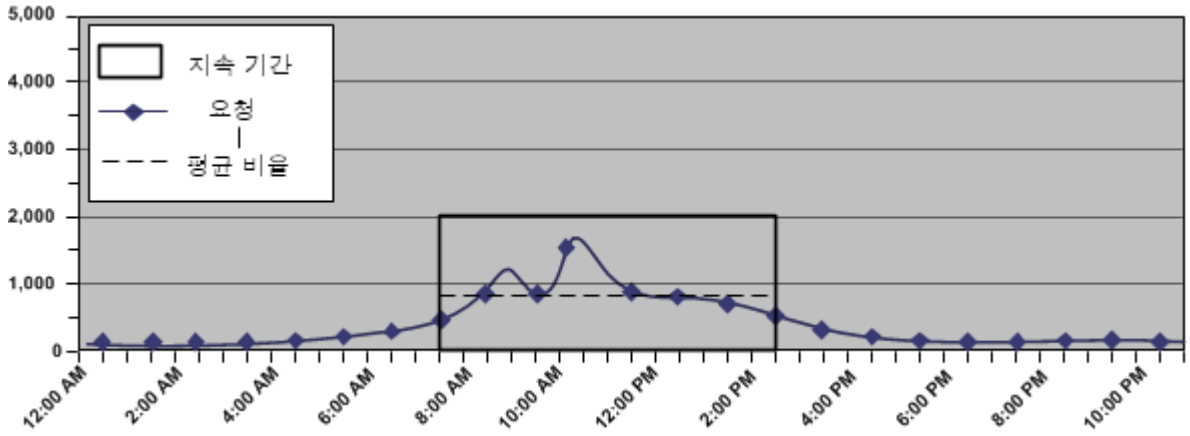
지속적 요청 비율은 요청 부하를 기반으로 합니다. 구체적으로 말하면 요청이 발생하는 시기와 비율을 의미합니다. 요청 부하가 업무일 동안 균등하게 분산될 가능성은 거의 없습니다. 대신 요청이 발생하는 비율은 지속 기간 동안 가장 낮은 수준과 가장 높은(최고) 수준 내에서 크게 변동합니다. 지속적 요청 비율을 추정하려면 시스템이 평균적인 수의 요청을 처리하는 지속 기간을 식별해야 합니다.

지속적 요청 비율을 추정할 때는 일별 요청 부하를 사용하여 다음을 파악하는 것이 좋습니다.

- 업무일 동안 요청이 발생하는 비율

  **참고:** 1 시간 단위로 분할된 24 시간의 평가 기간부터 시작하는 것이 좋습니다. 하지만 엔터프라이즈의 요구 사항에 따라 하루 동안의 결과를 몇 주 또는 몇 개월 동안 비교하면 연중 사용 처리량을 더 정확하게 파악할 수 있습니다.
- 시스템이 평균적인 수의 요청을 처리하는 지속 기간
- 지속 기간 동안 발생하는 대략적인 요청 수

다음 그림은 이러한 메트릭의 예입니다.



이러한 메트릭을 식별하면 사용자가 인증하는 평균 비율을 유지하기 위해 SiteMinder 가 처리해야 하는 초당 요청 수를 추정할 수 있습니다. 계산 방법은 다음과 같습니다.

(*request_load* * *percentage_of_requests*) / *number_of_sustained_hours* / 3600 = *sustained_request_rate*

***request_load***

응용 프로그램에 대한 일별 요청 수를 나타냅니다.

***percentage_of_requests***

시스템이 지속 수준에서 작동할 때 발생하는 요청의 백분율을 나타냅니다.

**예:** 요청 부하가 5,000 회의 로그인이고 지속 기간 동안 3,000 회의 로그인이 발생할 경우 값은 64 %(0.64)입니다.

***number_of_sustained_hours***

시스템이 지속 수준에서 작동하는 시간을 나타냅니다.

**참고:** 3,600 은 1 시간에 해당하는 초를 나타냅니다.

***sustained_request_rate***

지속 활동 기간 동안 SiteMinder 가 처리해야 하는 초당 요청 수를 나타냅니다.

## 예: 지속적 요청 비율 추정

회사에서 웹 서비스의 요청 부하가 2,000 회의 로그인임을 확인했습니다. 웹 서비스는 고객이 연중 무휴로 하루 24 시간 사용할 수 있습니다. 시스템 활동 보고서를 사용하여 일반적인 일일 결과를 분석한 결과는 다음과 같습니다.

- 시스템은 약 5 시간(오전 9 시 - 오후 2 시) 동안 지속 수준에서 작동합니다.
- 지속 수준에서 시간당 약 2,500 회의 요청이 발생합니다.
- 이 시간 동안 약 1,250(250 * 5)회의 요청 또는 일별 요청 부하의 62.5%(1,250/2,000)가 발생합니다.

(2,000 * 0.625) / 5 / 3600 = 초당 0.0694 회 요청

이행 웹 서비스의 지속적 요청 비율은 초당 0.694 회입니다.

# 최고 요청 비율 추정

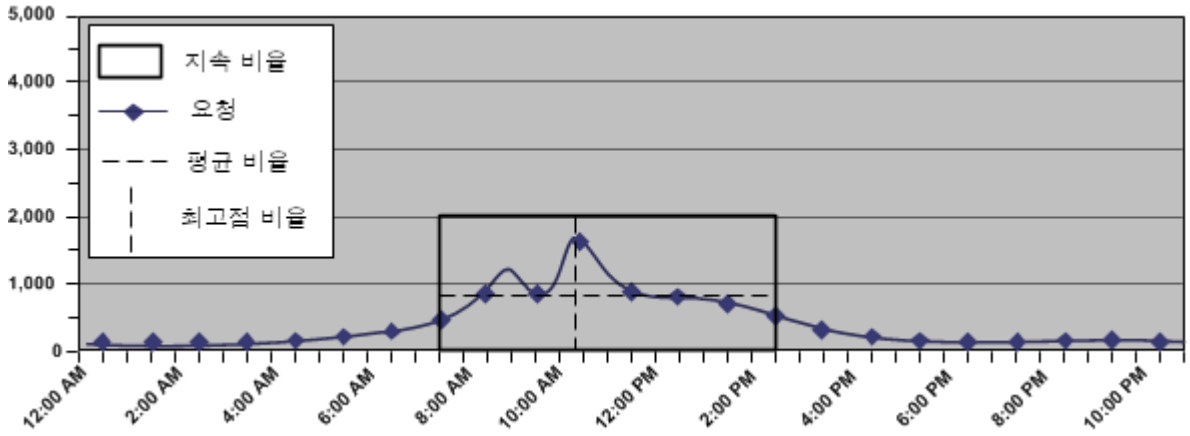
웹 서비스에 대한 최고 요청 비율을 추정해 보겠습니다.

최고 요청 비율은 지속적 요청 비율, 즉 시스템이 최고 수준으로 작동하는 시기와 비율을 기반으로 합니다. 최고 요청 비율을 추정하려면 시스템이 최고 수준의 요청을 처리하는 시기를 식별해야 합니다.

최고 요청 비율을 추정할 때는 지속적 요청 비율을 확인할 때 수집한 메트릭을 사용하여 다음을 확인하는 것이 좋습니다.

- 시스템이 가장 많은 수의 요청을 처리하는 시간
- 이 기간 동안 발생하는 대략적인 요청 수

다음 그림은 이러한 메트릭의 예입니다.




이러한 메트릭을 식별하면 웹 서비스 클라이언트의 최고 인증 비율을 유지하기 위해 SiteMinder 가 처리해야 하는 초당 요청 수를 추정할 수 있습니다. 계산 방법은 다음과 같습니다.

(*request_load* x *percentage_of_transactions*) / *number_of_hours* / 3600 = *peak_request_rate*

**참고**: 이 비율은 가장 작업량이 많은 1 시간을 기반으로 합니다. 최고 요청 비율이 시간별 계산을 초과하는 기간이 있을 수 있습니다.

***request_load***

웹 서비스에 대한 일별 요청 수를 나타냅니다.

***percentage_of_transactions***

시스템이 최고 수준에서 작동할 때 발생하는 트랜잭션의 백분율을 나타냅니다.

***number_of_hours***

시스템이 최고 수준에서 작동하는 시간을 나타냅니다.

**참고:** 3,600 은 1 시간에 해당하는 초를 나타냅니다.

***peak_request_rate***

응용 프로그램에 대한 최고 요청 비율을 나타냅니다.

### 예: 최고 요청 비율 추정

회사에서 웹 서비스의 일별 요청 부하가 8,800 회임을 확인했습니다. 시스템 활동 보고서에는 하루 중 가장 작업량이 많은 1 시간 동안 1,800 회의 요청이 발생한 것으로 보고됩니다. 이 숫자는 요청 부하의 약 20%를 나타냅니다.

1,800 / 1 / 3600 = 초당 0.5 회 요청

이행 웹 서비스의 최고 요청 비율은 초당 5 회입니다.

**참고**: 이 예는 가장 작업량이 많은 1 시간을 기반으로 합니다. 시간 중 최고 요청 비율이 초당 5 회 요청을 초과하는 기간이 있을 수 있습니다.

**추가 정보:**

에이전트에서 사용 가능한 소켓의 양 늘리기 (페이지 156)

# 용량 계획 시 고려해야 할 다른 요인

eTrust SOA Security Manager 용량 계획을 결정할 때 가장 중요한 요인은 요청 비율이지만 다른 요인, 특히 웹 서비스를 보호하는 데 사용되는 인증 체계도 SiteMinder 성능에 영향을 미칠 수 있습니다.

따라서 용량 계획 프로세스에서는 성능 조정 및 네트워크 대역폭도 고려하십시오.

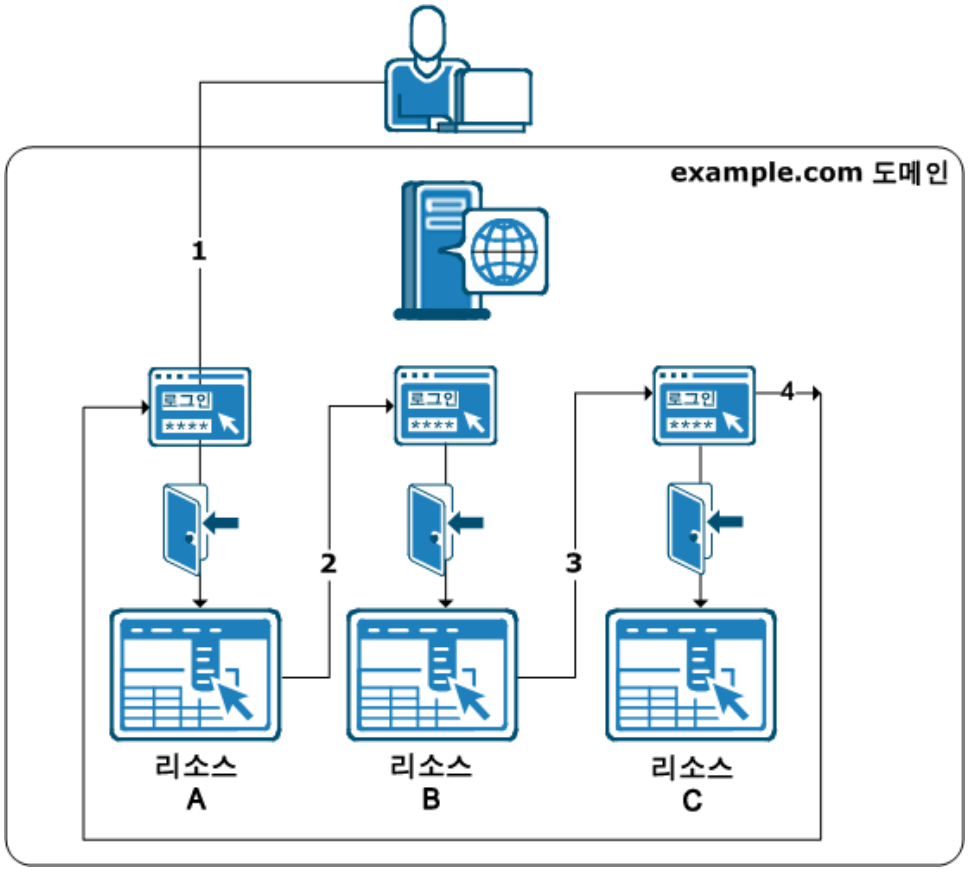
# 제 7 장: 구성 고려 사항

이 섹션은 다음 항목을 포함하고 있습니다.

# 보안 영역

보안 영역은 SiteMinder 웹 에이전트가 보호하는 단일 쿠키 도메인에 있는 리소스 그룹입니다. 사용자는 한 번 인증한 후 다시 인증을 하지 않고 영역의 다른 리소스(권한 부여된)에 액세스할 수 있습니다.

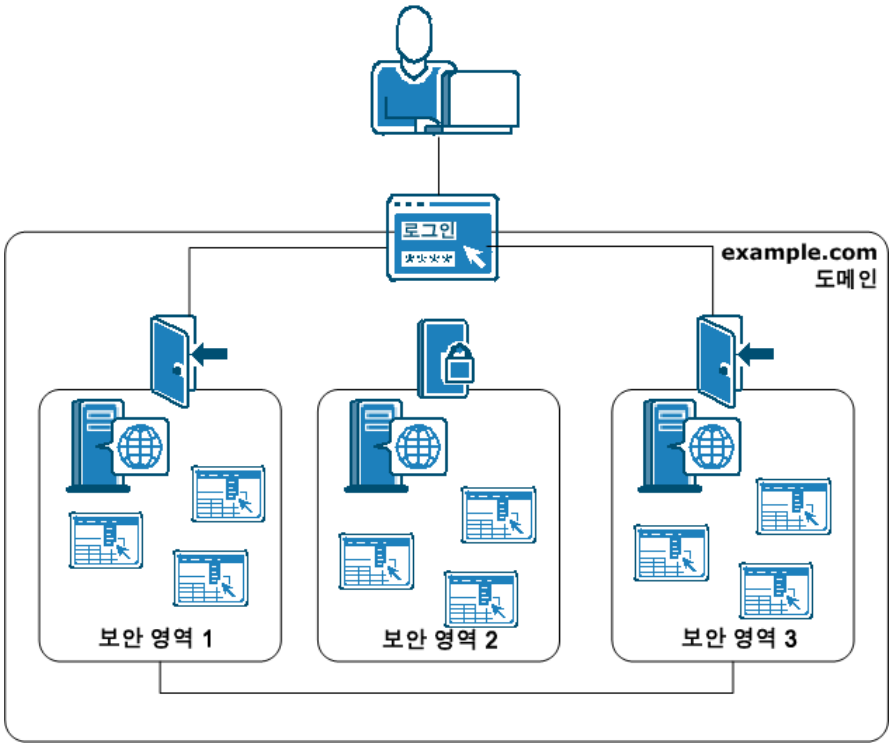
보안 영역이 없다면 사용자는 쿠키 도메인의 다른 리소스에 대해 이전에 SiteMinder 에서 인증된 경우라도 동일한 쿠키 도메인에 있는 보호된 리소스에 액세스할 때마다 인증해야 할 수 있습니다. 다음 그림은 이러한 예를 보여 줍니다.



다음과 같은 경우에는 보안 영역의 구현을 고려하십시오.

- 쿠키 도메인에 여러 개의 리소스가 있는데 이러한 리소스에 서로 다른 액세스 제한을 적용하지 않으려는 경우
- 동일한 쿠키 도메인에 있는 여러 리소스 간에 SSO 를 활성화하려는 경우
- 여러 쿠키 도메인에 걸쳐 있는 리소스 그룹을 생성하고 이 그룹 간에 SSO 를 허용하려는 경우
- 단일 쿠키 도메인이 있는 대규모 조직이 있고 조직의 리소스를 보호하기 위해 여러 SiteMinder 인스턴스를 사용하는 경우 보안 영역을 사용하면 리소스를 분리하여 단일 쿠키 도메인 내의 액세스를 제어할 수 있습니다. 보안 영역이 없다면 두 인스턴스에 대한 쿠키 도메인 이름이 동일하기 때문에 하나의 SiteMinder 인스턴스에서 사용되는 쿠키가 다른 SiteMinder 인스턴스의 쿠키를 덮어쓸 수 있습니다(쿠키 스톰핑).

다음 그림은 보안 영역을 사용하여 한 번의 로그인만으로 사용자에게 보안 영역 1 및 3 의 리소스에 대한 액세스를 허용하고 보안 영역 2 의 권한 없는 리소스에 대한 액세스는 차단하는 방법을 보여 줍니다.




**참고:** 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

# 다중 데이터 센터

SiteMinder 에서는 전역 배포를 같은 대륙에 있는 여러 데이터 센터와 동일하게 취급합니다. 따라서 SiteMinder 외부의 요소가 다중 데이터 센터 배포의 성능에 영향을 미칩니다. 다음의 핵심 요소가 포함됩니다.

- 네트워크 지연
- 회복성

다중 데이터 센터 배포를 계획할 때는 다음과 같은 외부 요소를 고려하는 것이 좋습니다.

- 네트워크 인프라
- 응용 프로그램 위치
- 사용자 위치
- 사용자 저장소 공급업체 및 제약 사항(예: 허용되는 마스터의 수)

## 모범 사례

데이터 센터를 구성할 때 다음 사항을 고려하십시오.

- 다음의 구성 요소를 각 데이터 센터에 함께 배치하면 네트워크 지연 및 회복성이 SiteMinder 성능에 미치는 영향을 줄일 수 있습니다.
  - SiteMinder 에이전트
  - 정책 서버
  - 사용자 저장소

    **참고:** 암호 서비스와 같은 SiteMinder 기능에 쓰기 가능한 저장소가 필요한 경우 각 데이터 센터마다 쓰기 가능한 저장소를 설치하는 것이 좋습니다.
- 모든 구성 요소를 동일한 데이터 센터에 둘 수 없는 경우 최소한 정책 서버와 사용자 저장소는 동일한 데이터 센터에 배치하는 것이 좋습니다.

## 아키텍처 고려 사항

SiteMinder 데이터 센터를 계획할 때 다음 아키텍처 요소를 고려하십시오.

- SiteMinder 암호 서비스는 인증할 때마다 사용자 계정에 LDAP 쓰기를 수행하려고 시도합니다.

  **참고:** 암호 서비스에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

- SiteMinder 는 읽기 전용 소비자 디렉터리와 통신할 때 LDAP 쓰기 조회를 따릅니다.

- 마스터 정책 저장소를 복제된 버전과 함께 배포하는 경우에는 정책 서버 호스트 시스템(LDAP)의 로컬 호스트 파일 또는 ODBC 데이터 원본을 사용하여 정책 서버를 로컬 정책 저장소로 연결하는 방법을 고려하십시오. 이 방법을 사용하면 모든 정책 서버가 동일한 정책 저장소를 공유하며 모든 정책 서버가 WAN 을 통해 정책 저장소와 통신해야 할 때 발생 가능한 지연을 방지할 수 있습니다.

- 마스터/소비자 사용자 저장소를 배포하는 경우에는 정책 서버 호스트 시스템(LDAP)의 로컬 호스트 파일 또는 ODBC DSN(데이터 원본 이름)을 사용하여 정책 서버를 로컬 소비자에 연결하는 방법을 고려하십시오. 이 방법을 사용하면 모든 정책 서버가 동일한 사용자 저장소를 읽게 되며 모든 정책 서버가 WAN 을 통해 사용자 계정 정보를 읽어야 할 때 발생 가능한 지연을 방지할 수 있습니다.

### 예: 정책 서버를 로컬 소비자 사용자 저장소에 연결하는 로컬 호스트 파일

두 개의 지리적으로 떨어진 데이터 센터에 myusers 라는 이름의 소비자 사용자 저장소에 연결되는 정책 서버가 포함되어 있습니다.

- 데이터 센터 1 의 로컬 소비자는 111.11.111.1 에서 사용할 수 있습니다.
- 데이터 센터 2 의 로컬 소비자는 222.22.222.2 에서 사용할 수 있습니다.

**정책 서버를 로컬 소비자에 연결하려면**

1. 데이터 센터 1 의 정책 서버 호스트 시스템에서 로컬 호스트 파일을 사용하여 myusers 를 111.11.111.1 에 매핑합니다.
2. 데이터 센터 2 의 정책 서버 호스트 시스템에서 로컬 호스트 파일을 사용하여 myusers 를 222.22.222.2 에 매핑합니다.

## 여러 데이터 센터 사용 사례

다음 사용 사례는 SiteMinder 데이터 센터를 네트워크 지연과 회복성의 관점에서 생각해 보도록 하기 위한 것입니다. 사용 사례는 간단한 배포에서 시작하여 점점 더 복잡한 시나리오로 발전합니다.

이 사용 사례는 전역 아키텍처의 일부로 사용할 수 있는 기술을 파악하기 위한 것이며 최종 아키텍처로 사용하기 위한 것이 아닙니다. 이 사례에서 필요한 인프라를 도출하여 조직에 가장 적합한 데이터 센터를 구성하십시오.

### 모든 구성 요소가 단일 데이터 센터에 포함됨

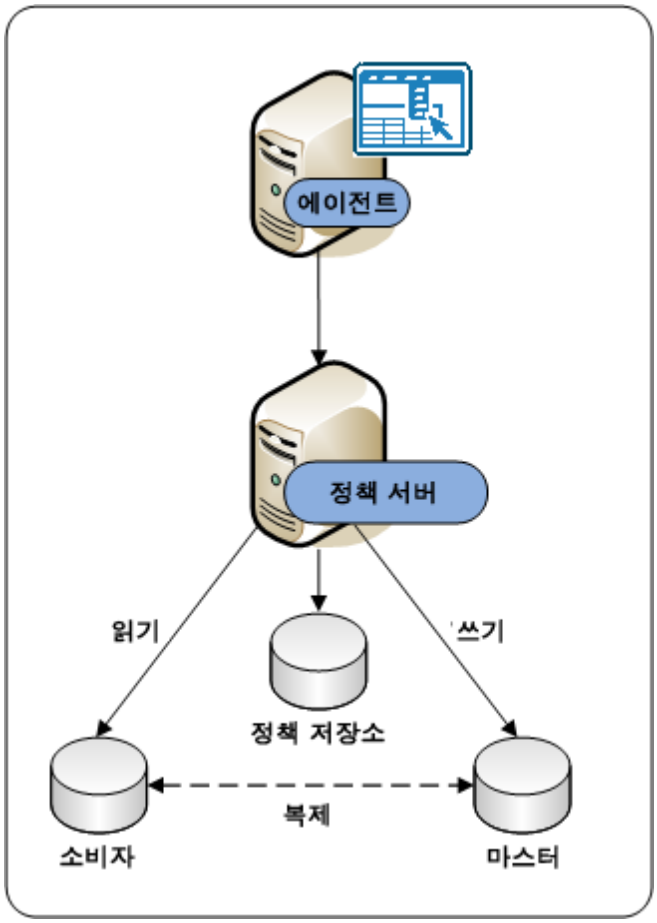
가장 간단한 배포에서는 필요한 모든 SiteMinder 구성 요소가 하나의 데이터 센터에 포함됩니다.

다음 다이어그램에서 보여 주는 항목은 아래와 같습니다.

- 모든 응용 프로그램이 단일 데이터 센터에 있습니다.
- 정책 서버가 마스터 사용자 저장소에 쓰기를 수행합니다. SiteMinder 암호 서비스는 인증할 때마다 사용자 계정에 LDAP 쓰기를 수행하려고 시도합니다.

  **중요!** 다중 마스터 LDAP 사용자 저장소 지원의 제한 사항에 대한 자세한 내용은 *정책 서버 릴리스 정보*를 참조하십시오.

- SiteMinder 는 소비자 사용자 저장소를 읽습니다.




다음 사항을 고려하십시오.

- 여기에는 나와 있지 않지만 SiteMinder 는 쓰기 및 읽기 전용 트랜잭션에 대해 구성된 데이터베이스 클러스터를 지원합니다.
- 작업 연속성, 중복성 및 고가용성을 위해 하나의 데이터 센터에 여러 구성 요소를 구성할 수 있습니다.

**추가 정보:**

중복성 및 고가용성 (페이지 39)

## 모든 구성 요소가 여러 데이터 센터에 포함됨

여러 데이터 센터를 배포하여 SiteMinder 환경을 확장할 수 있습니다. 여러 데이터 센터를 구현하기 위한 결정에 영향을 미치는 요소는 다음과 같습니다.

- 네트워크 인프라
- 응용 프로그램의 위치
- 사용자의 위치

다음 다이어그램에서 보여 주는 항목은 아래와 같습니다.

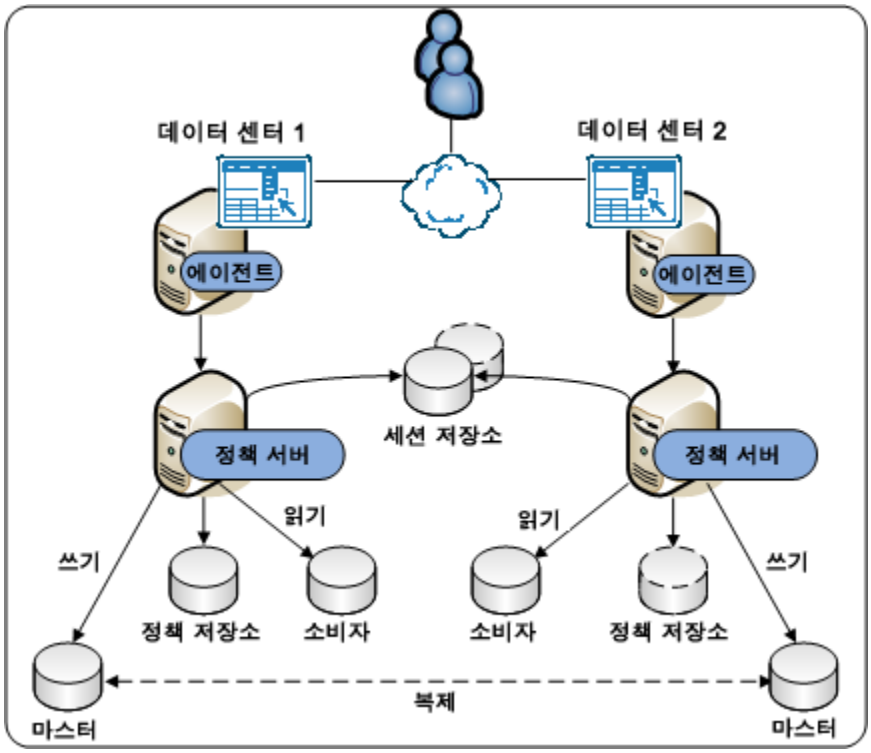
- 응용 프로그램이 여러 데이터 센터에 있습니다.
- 각 데이터 센터가 자체 정책 저장소를 사용합니다. 데이터 센터 1 에는 기본 정책 저장소가 포함되어 있습니다. 데이터 센터 2 에는 점선으로 표시된 복제된 버전이 포함되어 있습니다.

  **참고:** 배포의 모든 정책 서버는 동일한 정책 저장소에 대한 공통의 뷰를 공유해야 합니다. 정책 저장소 중복성에 대한 자세한 내용은 정책 서버에서 정책 저장소로의 통신 (페이지 49)을 참조하십시오.

- 각 데이터 센터가 자체 마스터/소비자 사용자 저장소를 사용합니다.

  **중요!** 다중 마스터 LDAP 사용자 저장소 지원의 제한 사항에 대한 자세한 내용은 *정책 서버 릴리스 정보*를 참조하십시오.

- 중앙화된 복제된 세션 저장소는 모든 응용 프로그램 간에 싱글 사인온을 활성화합니다.




**추가 정보:**

정책 서버에서 정책 저장소로의 통신 (페이지 49)
모든 구성 요소가 단일 데이터 센터에 포함됨 (페이지 132)

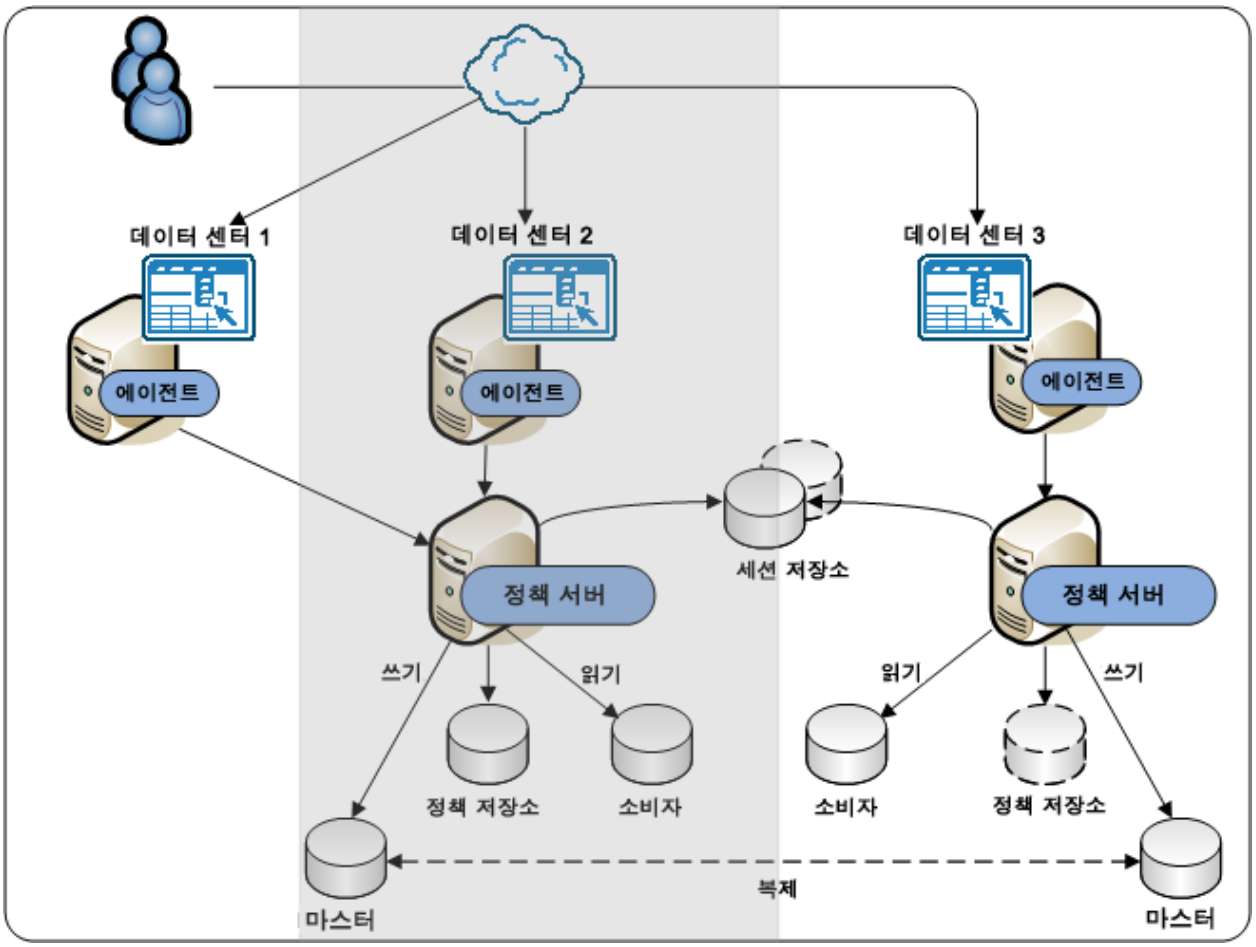
## 데이터 센터를 통해 통신하는 SiteMinder 에이전트

모든 구성 요소를 동일한 데이터 센터에 둘 수 없는 경우 최소한 정책 서버와 사용자 저장소는 동일한 데이터 센터에 배치하는 것이 좋습니다.

다음 다이어그램에서 보여 주는 항목은 아래와 같습니다.

- 응용 프로그램이 여러 데이터 센터에 있습니다.
- 데이터 센터 1 에는 웹 서버와 SiteMinder 에이전트만 포함되어 있습니다. 에이전트는 WAN 을 통해 데이터 센터 2 에 있는 정책 서버와 통신합니다.

- 데이터 센터 2 및 3:
  - 마스터/복제된 정책 저장소 (페이지 50)를 통해 정책 저장소에 대한 공통의 뷰를 공유합니다.
  - 자체 마스터/소비자 사용자 저장소 (페이지 132)를 사용합니다.
  - 모든 응용 프로그램 간에 싱글 사인온을 활성화하는 중앙화된 복제된 세션 저장소를 사용합니다.




**추가 정보:**

정책 서버에서 정책 저장소로의 통신 (페이지 49)

## 데이터 센터를 통해 통신하는 정책 서버

모든 구성 요소를 동일한 데이터 센터에 둘 수 없는 경우 최소한 정책 서버와 사용자 저장소는 동일한 데이터 센터에 배치하는 것이 좋습니다.

다음 다이어그램에서 보여 주는 항목은 아래와 같습니다.

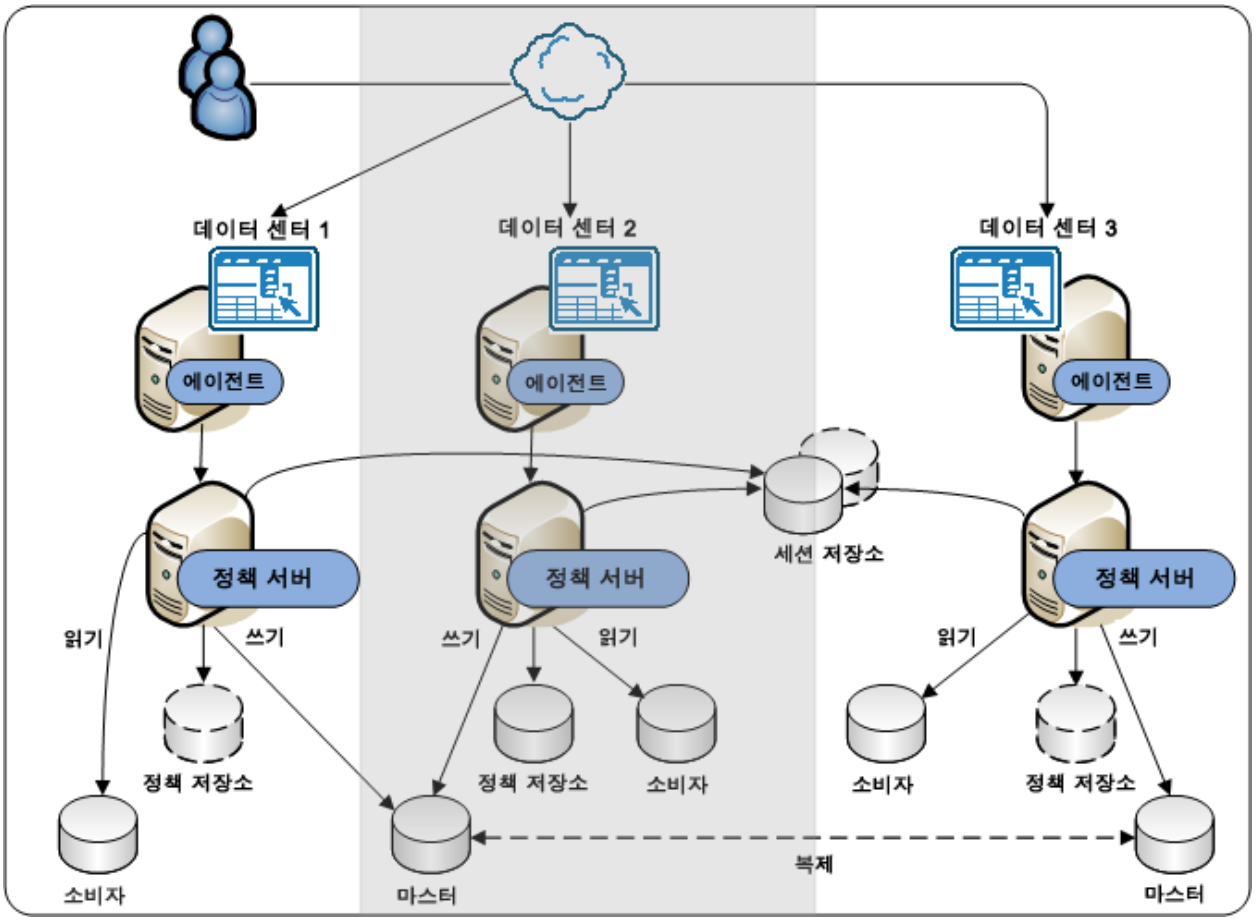
- 응용 프로그램이 여러 데이터 센터에 있습니다.
- 데이터 센터 1 에는 에이전트와 정책 서버만 포함되어 있습니다. 정책 서버는 WAN 을 통해서만 통신하여 데이터 센터 2 의 마스터 사용자 저장소에 LDAP 쓰기를 수행합니다.

  **중요!** 정책 서버가 LDAP 읽기 및 쓰기를 수행하기 위해 WAN 을 통해 통신하도록 구성되는 것은 권장하지 않습니다.

- 모든 데이터 센터:
  - 마스터/복제된 정책 저장소 (페이지 50)를 통해 정책 저장소에 대한 공통의 뷰를 공유합니다.
  - 모든 응용 프로그램 간에 싱글 사인온을 활성화하는 중앙화된 복제된 세션 저장소를 사용합니다.

- 데이터 센터 2 및 3 은 자체 마스터/소비자 사용자 저장소 (페이지 132)를 사용합니다.

  **중요!** 다중 마스터 LDAP 사용자 저장소 지원의 제한 사항에 대한 자세한 내용은 *정책 서버 릴리스 정보*를 참조하십시오.




**추가 정보:**

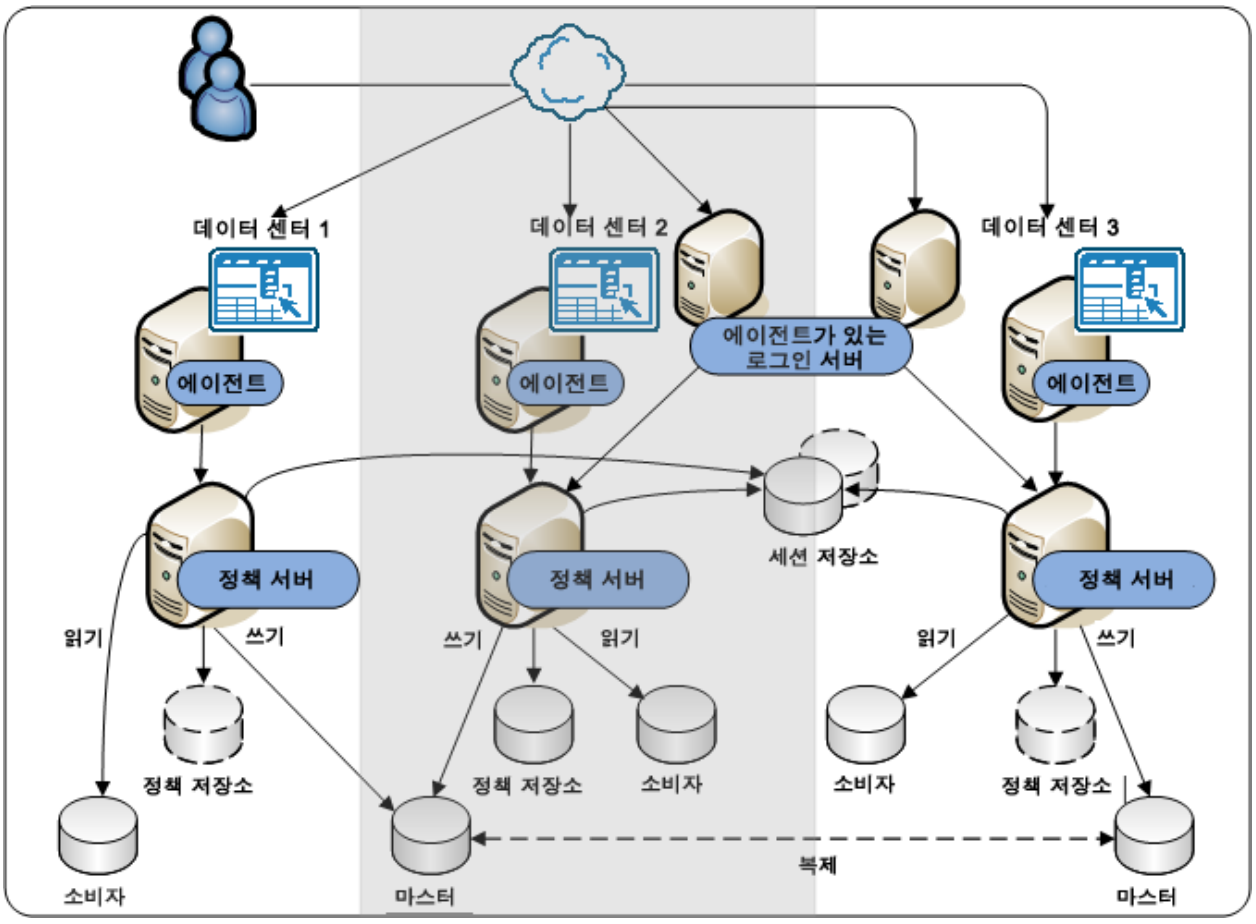
정책 서버에서 정책 저장소로의 통신 (페이지 49)
마스터 정책 저장소 (페이지 50)
모든 구성 요소가 단일 데이터 센터에 포함됨 (페이지 132)

## 사용자 저장소 쓰기를 제어하는 로그인 서버

LDAP 쓰기 가능 마스터의 위치에 따라 SiteMinder 배포가 제한될 수 있습니다. 각 데이터 센터마다 쓰기 가능한 마스터를 사용해야 하는 요구 사항을 제거하기 위해 하나 이상의 중앙화된 로그인 서버를 사용하는 방법을 고려하십시오.

다음 다이어그램에서 보여 주는 항목은 아래와 같습니다.

- 여러 데이터 센터 배포:
  - 데이터 센터 1 의 정책 서버가 WAN 을 통해 통신하여 LDAP 쓰기를 수행 (페이지 137)합니다.
  - 나머지 데이터 센터에는 모든 구성 요소 (페이지 134)가 포함되어 있습니다.
- 데이터 센터 2 와 데이터 센터 3 에 로그인 서버가 있습니다.



사용자가 데이터 센터 1 의 보호된 URL 에 대한 액세스를 요청할 경우:

1. 웹 에이전트가 요청을 데이터 센터 2 의 로그온 서버로 리디렉션합니다. 리디렉션은 리소스를 보호하는 인증 체계를 기반으로 합니다.

   **참고:** 인증 체계에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

2. 데이터 센터 2 의 정책 서버는 사용자를 인증하고 마스터 사용자 저장소에 씁니다.

3. 정책 서버는 SiteMinder 세션 티켓을 생성하고 이를 다시 원래의 보호된 URL 로 전달합니다.

   **참고:** 사용자 세션에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

4. 웹 에이전트는 SiteMinder 세션 티켓을 쿠키에 저장합니다. 웹 에이전트는 다음 상황 중 하나가 발생할 때까지 쿠키를 사용하여 데이터 센터에서 이후의 인증 및 권한 부여 요청을 처리합니다.

   - 사용자가 추가 자격 증명을 필요로 하는 다른 리소스를 요청합니다.
   - 세션이 만료됩니다.

# 인증 및 중앙화된 로그인 서버

SiteMinder 배포에는 일반적으로 인증(로그인) 요구 사항이 다른 여러 응용 프로그램이 포함됩니다. 이러한 요구 사항 때문에 개별 응용 프로그램 소유자가 관리해야 하는 로그인 페이지가 무수히 많이 발생할 수 있습니다. 이러한 로그인 페이지를 로컬에서 관리하면 페이지 디자인이나 오류 메시지 표시 등에서 일관성이 없는 부분이 발생하여 전반적인 인증 환경에 영향을 미칠 수 있습니다.

다음과 같은 이점을 위하여 로그인 페이지를 중앙 관리하는 것이 좋습니다.

- 응용 프로그램 간에 일관성을 유지할 수 있습니다. 하나의 SiteMinder 팀이 모든 로그인 페이지를 소유하면 이 팀에서 모든 로그인 페이지를 일관성 있게 구현하고 더 쉽게 관리할 수 있습니다.
- 로그인 페이지의 수를 최소화할 수 있습니다. 응용 프로그램 진입점의 수를 최소화하면 사용자에게 개별 응용 프로그램이 아니라 중앙화된 인프라에 로그인한다는 느낌을 줄 수 있습니다.

로그인 페이지를 구성할 때는 다음 사항을 고려하십시오.

- 동일한 인증 체계를 공유하고 동일한 로그인 페이지를 재사용하는 응용 프로그램을 식별하십시오.
- 모든 로그인 페이지를 호스트하는 중앙화된 로그인 서버를 사용하십시오.
- 사용자에게 다음과 같은 경우를 알리는 로그인 페이지를 구성하십시오.
  - 사용자가 올바른 자격 증명을 제공하지 못한 경우
  - 로그인 시도 횟수가 너무 많아 인증이 실패한 경우

## 로그인 페이지 중앙화

응용 프로그램의 로그인 요구 사항은 기본적인 사용자 이름/암호 인증에서 양식 기반 인증이나 디지털 인증서에 이르기까지 다양합니다. 가능하면 다음과 같은 방법을 사용하는 것이 좋습니다.

- 모든 웹 응용 프로그램에서 중복을 방지하기 위해 모든 로그인 페이지를 중앙 로그인 서버에서 관리합니다.
- 암호 서비스 페이지, 오류 페이지 및 이용 약관 페이지와 같은 다른 모든 시스템 전반 리소스를 중앙 서버에서 관리합니다.

**참고:** 인증 체계에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

로그인 페이지를 중앙에서 관리하려면 로그인 요구 사항이 동일한 응용 프로그램을 식별해야 합니다. 인증을 구성할 때 다음 사항을 고려하십시오.

- 응용 프로그램마다 별도의 로그인 페이지를 생성하지 않도록 하십시오. SiteMinder 를 채택하는 수가 증가함에 따라 응용 프로그램마다 별도의 로그인 페이지를 관리하기가 어렵기 때문입니다.
- 인증 요구 사항이 동일한 응용 프로그램을 식별하십시오. 가능하면 이러한 응용 프로그램의 진입점으로 하나의 로그인 페이지를 사용하십시오.

다음과 비슷한 표를 사용하여 응용 프로그램을 인증 요구 사항별로 그룹화하십시오.

| 인증 체계 이름 | 유형 | 로그인 페이지 서버 | 로그인 페이지 URL |
|---|---|---|---|
| | | | |

| 인증 체계 이름 | 유형 | 로그인 페이지 서버 | 로그인 페이지 URL |
|---|---|---|---|
| | | | |
| | | | |

### 예: 응용 프로그램을 인증 요구 사항별로 그룹화

SiteMinder 환경에서 10 개의 응용 프로그램을 보호합니다.

- 5 개의 응용 프로그램에는 양식 기반 인증이 필요합니다.
- 3 개의 응용 프로그램에는 Windows 기반 인증이 필요합니다.
- 2 개의 응용 프로그램에는 기본 사용자 이름/암호 인증이 필요합니다.

인증 요구 사항이 동일한 응용 프로그램을 식별하면 다음 표와 같이 8 개의 페이지를 3 개의 로그인 페이지로 대체할 수 있습니다.

| 인증 체계 이름 | 유형 | 로그인 페이지 서버 | 로그인 페이지 URL |
|---|---|---|---|
| Auth1 | 양식 | login.acme.com | /login.asp |
| Auth2 | Windows | login.acme.com | /smgetcrd.ntc |
| Auth3 | 기본 | login.acme.com | 해당 없음 |

## 모범 사례

로그인 페이지를 구성할 때는 다음 사항을 고려하십시오.

- 사용자가 적절한 인증에 실패할 경우 오류 메시지를 표시합니다.
- 사용자를 로그인 시도 횟수가 초과되었음을 알리는 메시지를 표시하는 페이지로 리디렉션합니다.
- 양식 기반 인증을 사용하여 사용자를 리디렉션하는 것이 좋습니다. 양식 기반 인증을 사용할 수 없는 경우 SiteMinder OnAuthAttempt 및 OnAuthReject 응답을 사용하여 사용자를 리디렉션할 수 있습니다.

  **참고:** 응답에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

- 양식 기반 인증을 구성하는 경우 login.asp 와 같은 동적 페이지를 생성하여 기존 인프라와 긴밀하게 통합하는 것을 고려하십시오.
- 동적 페이지를 생성할 수 없는 경우 웹 에이전트 설치에 포함된 샘플 로그인 FCC 파일(login.fcc)을 사용하여 로그인 FCC 파일을 구성하십시오. 샘플 파일의 기본 위치는 *web_agent_home*\samples_default\forms 입니다. forms 디렉터리는 FCC(양식 자격 증명 수집기)가 처리하는 파일의 기본 위치입니다.

  ***web_agent_home***

  웹 에이전트 설치 경로를 지정합니다.

  **참고:** 양식 기반 인증에 적용되는 로그인 FCC 에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오. 웹 에이전트와 함께 로그인 FCC 를 구성하는 방법과 FCC 가 요청을 처리하는 방식에 대해서는 *웹 에이전트 구성 안내서*를 참조하십시오.

- 모든 로그인 페이지마다 웹 에이전트 호스트 시스템에 별도의 디렉터리를 만드는 것이 좋습니다. forms 디렉터리 이외의 위치를 사용하면 샘플 파일을 실수로 덮어쓰는 것을 방지할 수 있습니다.
- 사용자가 성공적으로 로그아웃한 후에 사용자 지정 로그오프 페이지를 표시합니다.

  **참고:** 로그오프 페이지 구성에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

## 로그인 페이지 사용 사례

다음 사용 사례는 SiteMinder 인증의 구성에 대해 생각해 보도록 하기 위한 것입니다.

이 사용 사례는 모범 사례를 반영한 것이며 전역 아키텍처의 일부로 사용할 수 있는 기술을 파악할 수 있도록 작성되었습니다. 이 사용 사례는 최종 아키텍처로 사용하기 위한 것이 아닙니다. 이 사례에서 필요한 인프라를 도출하여 조직에 가장 적합한 로그인 페이지를 구성하십시오.

## 독립 실행형 로그인 페이지

이 사용 사례에서 SiteMinder 는 사용자가 보호된 리소스를 요청할 때 사용자를 독립 실행형 로그인 페이지로 리디렉션합니다. 구체적인 사항은 다음과 같습니다.

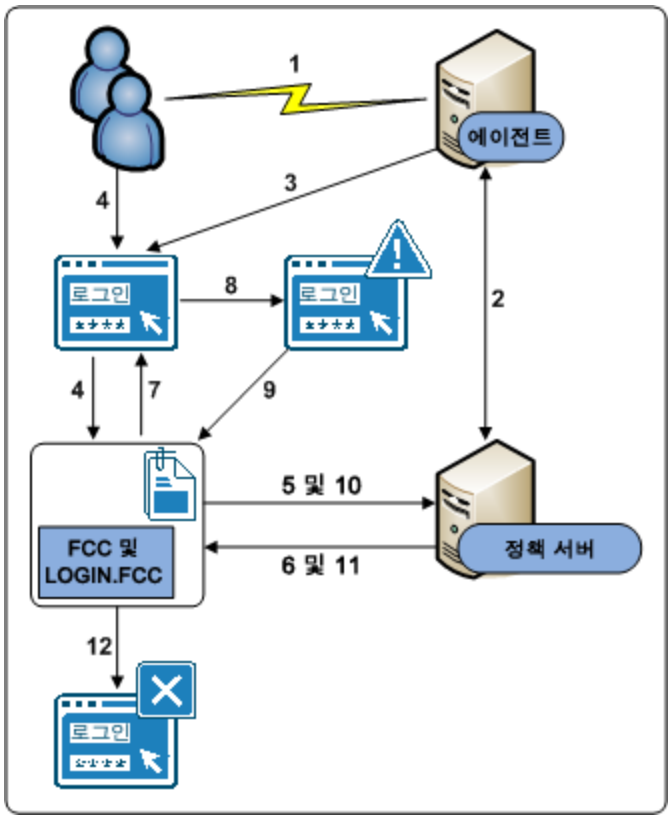
- 동적 로그인 페이지(login.asp)가 웹 에이전트 호스트 시스템에 배포됩니다.
- 동적 로그인 페이지가 다음을 수행하도록 코딩됩니다.
  - 로그인 FCC 파일(login.fcc)에 포스트합니다.
  - 사용자의 웹 브라우저에 SMTRYNO 쿠키가 있는 경우 오류 메시지를 표시합니다.

    **참고:** SMTRYNO 쿠키에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.
- 로그인 FCC 파일은 인증 시도가 두 번 실패하면 사용자를 실패한 인증 페이지(login.unauth)로 리디렉션하도록 @directive(@smretries)를 사용하여 구성됩니다.

  **참고:** @directives 로 FCC 파일을 구성하는 방법에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.
- SiteMinder 관리자는 Auth1 이라는 양식 기반 인증 체계를 구성했습니다. Auth1 의 대상은 login.asp 입니다.

  **참고:** 인증 체계 구성에 대한 자세한 내용은 정 *책*서버 구성 안내서를 참조하십시오.

다음 다이어그램은 이 사용 사례의 인증 프로세스를 보여 줍니다.




1. 사용자가 보호된 리소스를 요청합니다.
2. 웹 에이전트가 정책 서버에 연결하고 여기에서 리소스가 보호되어 있음을 확인합니다.
3. 웹 에이전트가 사용자 요청을 login.asp 로 리디렉션합니다.
4. 사용자가 올바르지 않은 자격 증명을 제출합니다. 자격 증명이 login.fcc 파일로 포스트되고 FCC 가 이를 처리합니다.
5. FCC 는 자격 증명을 정책 서버로 전달합니다.
6. 정책 서버는 자격 증명이 올바르지 않음을 확인하고 이를 FCC 에 알립니다.
7. FCC 는 사용자의 웹 브라우저에 SMTRYNO 쿠키를 삽입하고 사용자를 로그인 페이지로 리디렉션합니다.
8. 오류 메시지가 표시되면서 로그인 페이지가 새로 고쳐집니다. 올바르지 않은 자격 증명이 제공되었으며 다시 시도하라는 오류 메시지가 표시됩니다.

9. 사용자가 올바르지 않은 자격 증명을 제출합니다. 자격 증명이 login.fcc 파일로 포스트되고 FCC 가 이를 처리합니다.
10. FCC 는 자격 증명을 정책 서버로 전달합니다.
11. 정책 서버는 자격 증명이 여전히 올바르지 않음을 확인하고 이를 FCC 에 알립니다.
12. 사용자가 실패한 인증 시도의 최대 횟수를 초과하여 실패한 인증 메시지가 표시되는 페이지로 리디렉션됩니다.

## 웹 포털에 포함된 양식

이 사용 사례에서는 양식이 웹 포털 홈 페이지에 포함됩니다. 사용자는 양식에 자격 증명을 입력하고 인증 시 보호된 리소스로 리디렉션됩니다. 구체적인 사항은 다음과 같습니다.

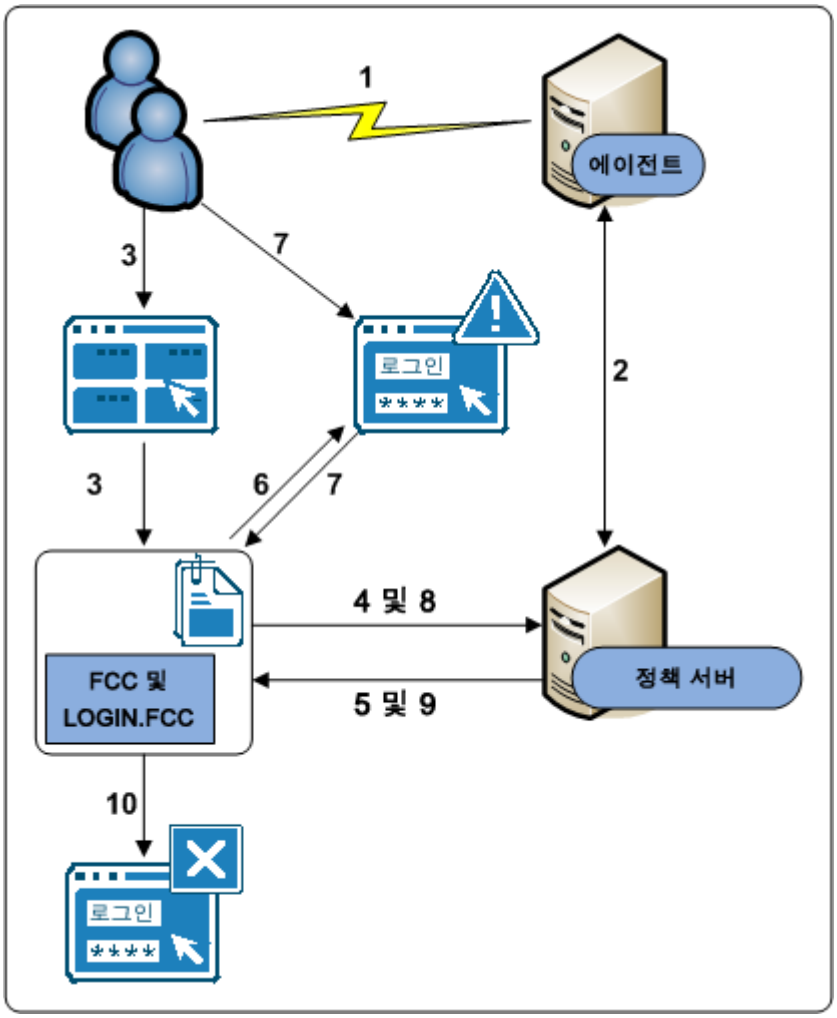
- 웹 포털 홈 페이지(portal.asp)에 사용자의 자격 증명을 묻는 포함된 양식이 포함되어 있습니다. 홈 페이지는 다음과 같습니다.
  - 보호된 리소스를 가리키는 대상 변수가 포함되어 있습니다.
  - 로그인 FCC 파일(login.fcc)에 포스트합니다.
- 독립 실행형 로그인 페이지(login.asp)가 웹 에이전트 호스트 시스템에 배포됩니다. 사용자가 보호된 리소스에 직접 액세스하려고 하면 이 페이지에서 사용자에게 자격 증명을 묻습니다. 로그인 페이지는 다음을 수행합니다.
  - 로그인 FCC 파일에 포스트합니다.
  - 사용자의 웹 브라우저에 SMTRYNO 쿠키가 있는 경우 오류 메시지를 표시합니다.

    **참고:** SMTRYNO 쿠키에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.
- 로그인 FCC 파일은 인증 시도가 두 번 실패하면 사용자를 실패한 인증 페이지(login.unauth)로 리디렉션하도록 @directive(@smretries)를 사용하여 구성됩니다.

  **참고:** @directives 로 FCC 파일을 구성하는 방법에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.
- SiteMinder 관리자는 Auth1 이라는 양식 기반 인증 체계를 구성했습니다. Auth1 의 대상은 login.asp 입니다.

  **참고:** 인증 체계 구성에 대한 자세한 내용은 정*책* 서버 구성 안내서를 참조하십시오.

다음 다이어그램은 이 사용 사례의 인증 프로세스를 보여 줍니다.




1. 사용자가 웹 포털 홈 페이지로 이동합니다.
2. 웹 에이전트가 정책 서버에 연결하고 여기에서 리소스가 보호되지 않음을 확인합니다.
3. 사용자가 올바르지 않은 자격 증명을 제출합니다. 자격 증명이 login.fcc 파일로 포스트되고 FCC 가 이를 처리합니다.
4. FCC 는 자격 증명을 정책 서버로 전달합니다.
5. 정책 서버는 자격 증명이 올바르지 않음을 확인하고 이를 FCC 에 알립니다.

6. FCC 는 사용자의 웹 브라우저에 SMTRYNO 쿠키를 삽입하고 사용자를 로그인 페이지로 리디렉션합니다. 오류 메시지와 함께 로그인 페이지가 표시됩니다. 올바르지 않은 자격 증명이 제공되었으며 다시 시도하라는 오류 메시지가 표시됩니다.

   **참고:** 여기에는 나와 있지 않지만 사용자가 보호된 리소스에 직접 액세스하면 웹 브라우저에 SMTRYNO 쿠키가 없기 때문에 오류 메시지가 없는 로그인 페이지가 표시됩니다.

7. 사용자가 올바르지 않은 자격 증명을 제출합니다. 자격 증명이 login.fcc 파일로 포스트되고 FCC 가 이를 처리합니다.

8. FCC 는 자격 증명을 정책 서버로 전달합니다.

9. 정책 서버는 자격 증명이 여전히 올바르지 않음을 확인하고 이를 FCC 에 알립니다.

10. 사용자가 실패한 인증 시도의 최대 횟수를 초과하여 실패한 인증 메시지가 표시되는 페이지로 리디렉션됩니다.

# 제 8 장: 성능 조정

이 섹션은 다음 항목을 포함하고 있습니다.



## 성능 조정 소개

정책 서버는 다음 세 가지 기본 요청을 처리하여 액세스 제어 정책을 평가하고 적용합니다.

- IsProtected - 요청된 리소스가 보호됩니까?
- IsAuthenticated - 리소스를 요청하는 사용자가 ID 를 확인하는 자격 증명을 제시했습니까?
- IsAuthorized - 인증된 사용자에게 보호된 리소스를 볼 수 있는 권한이 부여되었습니까?

이러한 각 요청을 처리하기 위해 SiteMinder 구성 요소 간에 트랜잭션이 생성됩니다. SiteMinder 성능 조정은 다음과 같은 방법으로 처리량을 늘리고 지연 시간을 줄이는 반복적인 프로세스입니다.

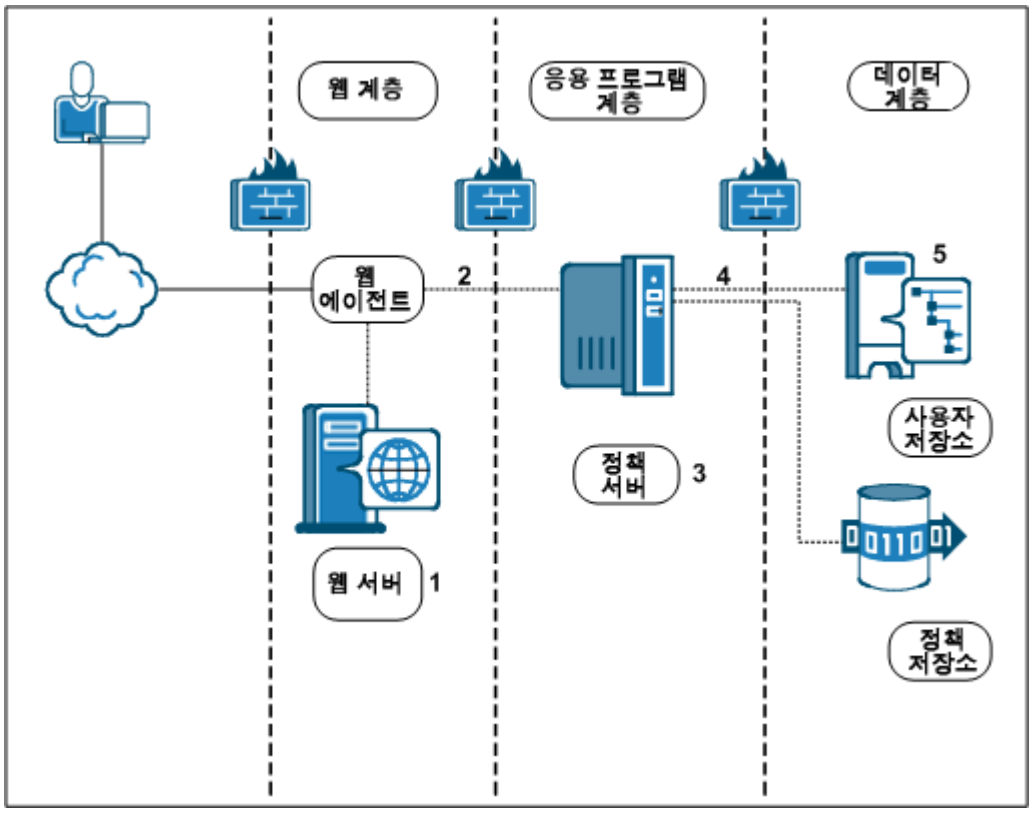
- 이러한 트랜잭션이 수행되는 시점과 위치를 파악
- 성능에 영향을 미치는 SiteMinder 설정 및 기능을 식별
- 타사 및 SiteMinder 도구를 사용하여 성능을 측정하고 인프라 병목 지점을 식별

웹, 응용 프로그램 및 데이터 계층에서 성능 요소를 검사하는 것이 좋습니다.

**참고:** SiteMinder 는 미들웨어이며 독립적으로 배포되지 않습니다. 다음 단원에서는 웹 및 응용 프로그램 계층에서 SiteMinder 구성 요소의 조정을 집중적으로 살펴보며 실제 웹, 응용 프로그램 또는 데이터 계층 자체를 조정하는 방법은 다루지 않습니다. 환경의 웹 서버, 디렉터리 서버 및 데이터베이스를 조정하는 방법에 대한 자세한 내용은 해당 공급업체의 설명서를 참조하십시오.

# 성능 조정 로드맵

성능 조정은 반복적인 프로세스이며 따라서 웹, 응용 프로그램 및 데이터 계층을 개별적으로 처리하여 각 계층이 전반적인 성능에 어떤 영향을 미치는지 파악하는 것이 중요합니다. 경우에 따라 SiteMinder 에이전트, 정책 서버 또는 SiteMinder 정책 개체 자체의 구성 설정을 변경하여 성능을 향상시킬 수도 있습니다. 다음 다이어그램은 표준 배포를 나타내며 성능에 중요한 영향을 미치는 개별 구성 요소를 자세히 보여 줍니다.



1. 환경에 배포된 웹 및 응용 프로그램 서버의 유형은 SiteMinder 에이전트와 정책 서버의 통신 방법에 영향을 미칠 수 있습니다.
2. 사용할 수 있는 소켓 수는 에이전트와 정책 서버 간 통신의 효율성에 영향을 미칠 수 있습니다.
3. SiteMinder 정책 설계는 정책 서버 서비스 인증 및 권한 부여 요청의 효율성에 영향을 미칠 수 있습니다.
4. 정책 서버는 일련의 서비스를 수행하여 사용자를 인증하고, 권한을 부여합니다. 이러한 서비스의 결과로 사용자 디렉터리에 대한 여러 개의 읽기 및 쓰기가 발생하며 이를 통칭하여 요청이라고 합니다. 지속적 작업 기간 및 최고 작업 기간에 사용자 디렉터리가 이러한 작업 부하를 처리할 수 있는지 여부를 파악하면 SiteMinder 성능에 도움이 됩니다.
5. 사용자 디렉터리 자체가 SiteMinder 성능에 영향을 미칠 수 있습니다.

**추가 정보:**

사용자 저장소 용량 계획 (페이지 194)
SiteMinder 정책 설계 및 성능 (페이지 173)
서버 성능 (페이지 153)
에이전트와 정책 서버 간 트래픽 줄이기 (페이지 159)
데이터 계층 지침 (페이지 192)
웹 계층 소켓 사용 (페이지 155)

# 웹 계층 성능

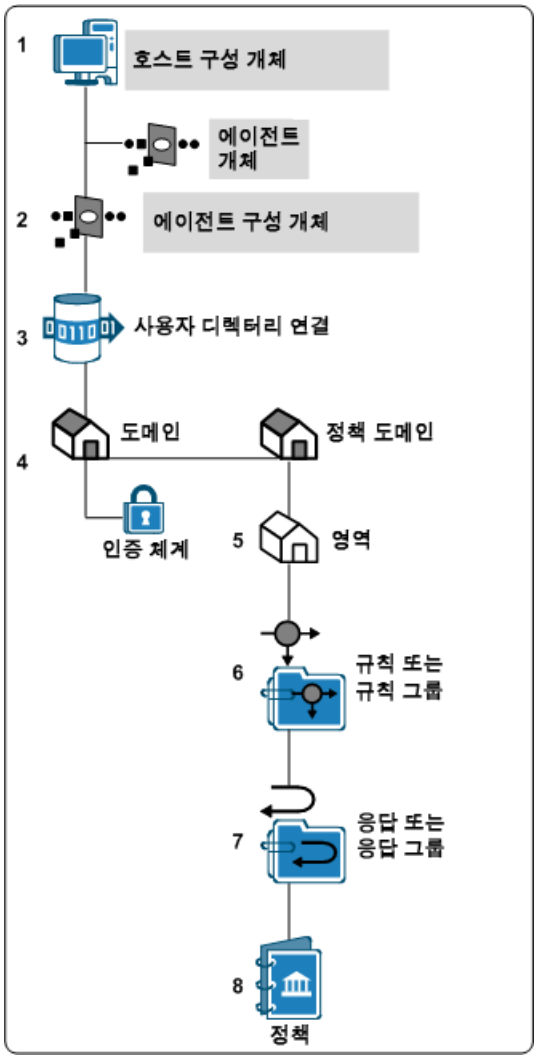
SiteMinder 에이전트가 웹 또는 응용 프로그램 서버로 전송된 요청을 가로챌 때 에이전트는 SiteMinder 정책 서버에 대해 다음 호출을 실행합니다.

- isProtected
- isAuthenticated
- isAuthorized

이러한 각 호출에 의해 웹 계층의 에이전트와 응용 프로그램 계층의 정책 서버 간에 트래픽이 생성됩니다. 다음 설정이 웹 계층의 성능을 조정하는 데 도움이 될 수 있습니다.

- 정책 서버 요청의 시간 만료 간격을 변경합니다.
- 에이전트가 정책 서버 연결에 사용할 수 있는 소켓 수를 변경합니다.
- 에이전트 캐시를 사용하여 에이전트가 정책 서버에 대해 수행하는 호출 수를 줄입니다.

다음 그림에 음영으로 표시된 항목에는 웹 계층의 성능에 영향을 주는 설정이 포함되어 있습니다.




## 서버 성능

지원되는 여러 웹 및 응용 프로그램 서버에 SiteMinder 에이전트를 설치할 수 있습니다. 호스팅 서버의 성능에 따라 SiteMinder 웹 계층의 성능이 결정됩니다. SiteMinder 와 함께 작동하는 웹 서버의 성능에 영향을 미치는 항목은 다음과 같습니다.

- 웹 서버의 프로세서 속도
- 웹 서버의 메모리 양

## SiteMinder 에이전트 성능

SiteMinder 웹 에이전트 성능에 영향을 미치는 요소는 다음과 같습니다.

- 웹 또는 응용 프로그램 서버 CPU 및 사용 가능한 메모리
- 정책 서버 지연(정책 서버가 에이전트 요청에 응답하는 속도)

요청 수를 처리하는 데 사용할 수 있는 웹 서버의 수가 너무 적으면 다음과 같은 유형의 문제가 발생할 수 있습니다.

- 사용자 로그인이 지연되거나 불가능합니다.
- 사용자가 요청한 리소스를 수신할 때 지연이 발생합니다.
- CPU 사용량이 최대 용량이거나 최대 용량에 근접합니다.

최고 기간에 각 웹 또는 응용 프로그램 서버에서 처리하는 요청 수를 예측하면 SiteMinder 환경에 적합한 웹 서버 수를 결정하는 데 도움이 됩니다.

요청 수를 추정하려면 다음 방법 중 하나를 사용하십시오.

- 용량 계획을 세웁니다.
- 환경의 각 에이전트에 대한 SiteMinder 작업 보고서를 생성합니다.
- 웹 서버에 대한 성능 보고서를 생성합니다.

  **참고:** 자세한 내용은 웹 서버 공급업체에서 제공하는 설명서를 참조하십시오.

**추가 정보:**

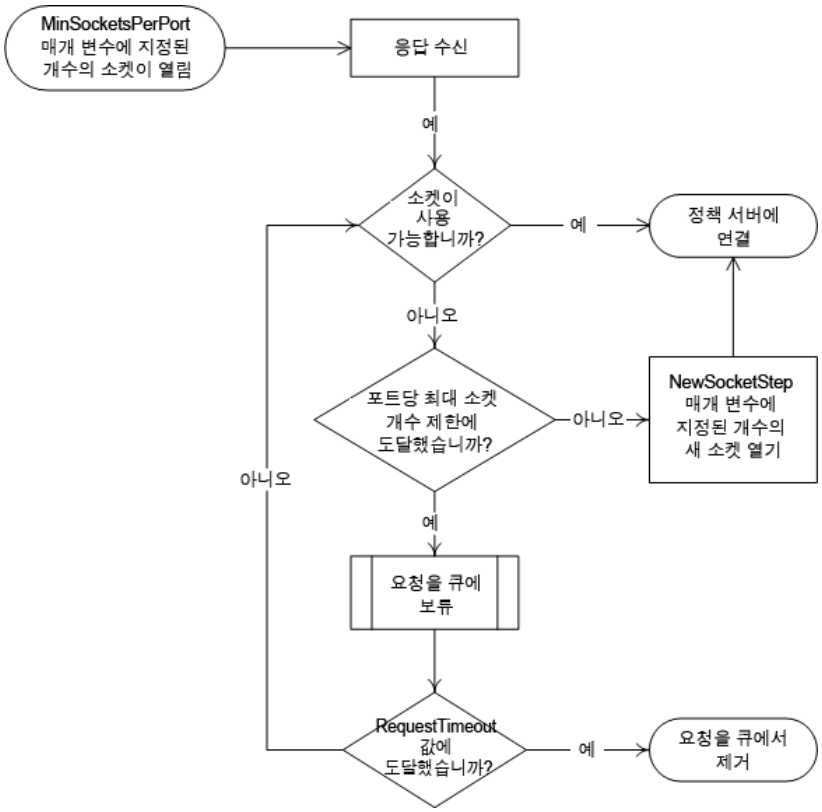
최고 인증 비율 추정 (페이지 109)
최고 권한 부여 비율 추정 (페이지 116)

## 웹 계층 소켓 사용

SiteMinder 에이전트는 시작할 때 정책 서버에서 호스트 구성 개체의 MinSocketsPerPort 매개 변수로 지정된 수의 소켓을 엽니다. 더 많은 요청이 수신되면 에이전트는 최대 소켓 수에 도달할 때까지 지정된 수의 새 소켓을 연결 풀에 추가합니다. 모든 소켓이 사용되면 다음 이벤트 중 하나가 발생할 때까지 추가 요청(최대 300 개)이 큐에 유지됩니다.

- 소켓 쌍이 사용할 수 있게 되고 요청이 정책 서버로 전송됩니다.
- 요청 시간이 초과되고 사용자가 리소스 액세스를 다시 시도해야 합니다.

다음 그림은 이러한 프로세스를 보여 줍니다.




정책 서버의 호스트 구성 개체에는 사용되는 소켓의 수를 제어하는 매개 변수가 포함되어 있습니다.

## 부하가 높을 때 요청 시간 만료 간격 늘리기

네트워크가 다음 조건 중 하나라도 해당하는 경우 SiteMinder 에이전트의 요청이 정책 서버 큐에 유지되는 시간을 늘리는 방법을 고려하십시오.

- 트래픽 양이 많음
- 연결 속도가 느림

정책 서버 호스트 구성 개체의 RequestTimeout 매개 변수는 에이전트가 정책 서버의 응답을 기다리는 시간을 제어합니다. 간격이 너무 짧으면 요청이 시간 만료되고 사용자에게 오류 메시지가 표시됩니다.

**참고:** 자세한 내용은 *SiteMinder 정책 서버 구성 안내서*를 참조하십시오.

## 에이전트에서 사용 가능한 소켓의 양 늘리기

용량 계획의 추정에 따라 SiteMinder 에이전트당 사용자 요청의 수가 특정 순간 60 개(처리 중인 요청 20 개 및 큐의 요청 40 개)를 초과할 것으로 예상되는 경우에는 MaxSocketsPerPort 매개 변수의 값을 늘리십시오.

관리 UI 에서 MaxSocketsPerPort 매개 변수의 값을 늘린 후에는 정책 서버 관리 콘솔의 "최대 연결 수" 설정이 SiteMinder 환경의 모든 에이전트 프로세스를 수용할 수 있을 정도로 충분히 높은지 확인하십시오. 이 설정에 따라 특정 정책 서버에서 사용할 수 있는 최대 연결 수가 결정됩니다.

**참고:** 프리포크(pre-fork) 모드의 Apache 기반 서버와 같은 다중 프로세스 웹 서버의 경우 이 소켓의 수를 하나로 줄일 수 있습니다. 각 프로세스에서는 하나의 스레드만 사용하여 SiteMinder 정책 서버와 통신하기 때문에 소켓이 하나만 필요합니다.

**추가 정보:**

최고 요청 비율 추정 (페이지 125)

## NewSocketStep 설정 늘리기

최고 부하 상태에서 SiteMinder 에이전트에 연결 풀의 추가 소켓이 필요한 경우 매번 가져오는 소켓의 수는 NewSocketStep 매개 변수에 의해 결정됩니다.

NewSocketStep 매개 변수의 값이 너무 낮게 설정되면 에이전트가 소켓 연결을 만드는 데 더 많은 시간이 소요되므로 최고 부하 상태의 응답 시간이 느려집니다.

응답 시간이 느려지는 것을 방지하려면 용량 계획을 통해 에이전트가 처리하는 요청의 수를 파악한 다음 그에 따라 NewSocketStep 매개 변수의 값을 늘리십시오.

이 매개 변수의 이상적인 값은 웹 또는 응용 프로그램 서버의 부하가 증가함에 따라 에이전트가 요청을 위한 소켓을 만드는 데 너무 많은 시간을 소비하지 않을 정도의 값입니다.

SiteMinder 환경에서 가장 적합하게 작동할 때까지 여러 설정을 실험해 보는 것이 좋습니다.

**참고:** 프리포크(pre-fork) 모드의 Apache 기반 서버와 같은 다중 프로세스 웹 서버의 경우 이 소켓의 수를 하나로 줄일 수 있습니다. 각 프로세스에서는 하나의 스레드만 사용하여 SiteMinder 정책 서버와 통신하기 때문에 소켓이 하나만 필요합니다.

**추가 정보:**

최고 인증 비율 추정 (페이지 109)
최고 요청 비율 추정 (페이지 125)

## 포트당 최소 소켓 설정

SiteMinder 에이전트는 시작할 때 정책 서버에서 호스트 구성 개체의 MinSocketsPerPort 매개 변수로 지정된 수의 소켓을 엽니다. 이 소켓은 정책 서버에 대한 지속적인 연결을 유지 관리합니다.

웹 및 응용 프로그램 서버 유형 대부분에 대해(Worker 모드의 Apache 기반 서버를 포함하여) 이 매개 변수를 기본 설정으로 두는 것이 좋습니다. 이 매개 변수를 늘리면 에이전트가 리소스 요청을 수신하지 않을 때도 소켓이 열려 있으므로 추가적인 소켓이 불필요하게 점유됩니다.

**참고:** 프리포크(pre-fork) 모드의 Apache 기반 서버와 같은 다중 프로세스 웹 서버의 경우 이 소켓의 수를 하나로 줄일 수 있습니다. 각 프로세스에서는 하나의 스레드만 사용하여 SiteMinder 정책 서버와 통신하기 때문에 소켓이 하나만 필요합니다.

## 소켓 설정 간 관계의 예

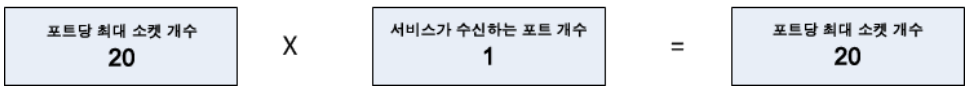
사용 중인 웹 서버의 유형에 따라 정책 서버의 소켓 할당 매개 변수 간의 관계가 결정됩니다.

단일 프로세스 다중 스레드 웹 서버는 다중 프로세스 단일 스레드 웹 서버와 다르게 작동하므로 웹 서버 유형에 따라 정책 서버에서 소켓의 할당이 달라집니다.

**참고**: 웹 서버의 유형을 확인하려면 공급업체의 설명서를 참조하십시오.

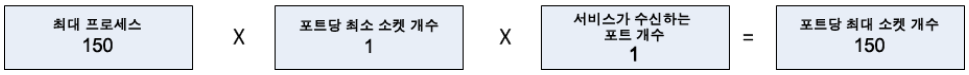
다음 그림은 단일 프로세스 다중 스레드 웹 서버에 대한 공식을 보여 줍니다.

**단일 프로세스/다중 스레드 웹 서버를 위한 소켓 설정 공식**

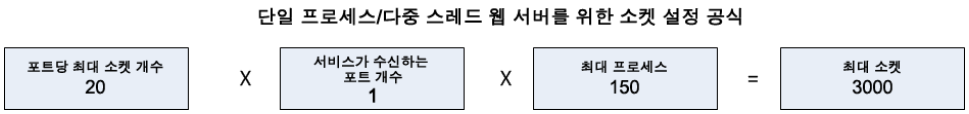



다음 그림은 다중 프로세스 단일 스레드 웹 서버에 대한 공식을 보여 줍니다.

**단일 프로세스/다중 스레드 웹 서버를 위한 소켓 설정 공식**



다음 그림은 다중 프로세스 다중 스레드 웹 서버에 대한 공식을 보여 줍니다.




소켓 설정을 조정할 때 앞의 공식을 지침으로 사용하십시오.

## 에이전트와 정책 서버 간 트래픽 줄이기

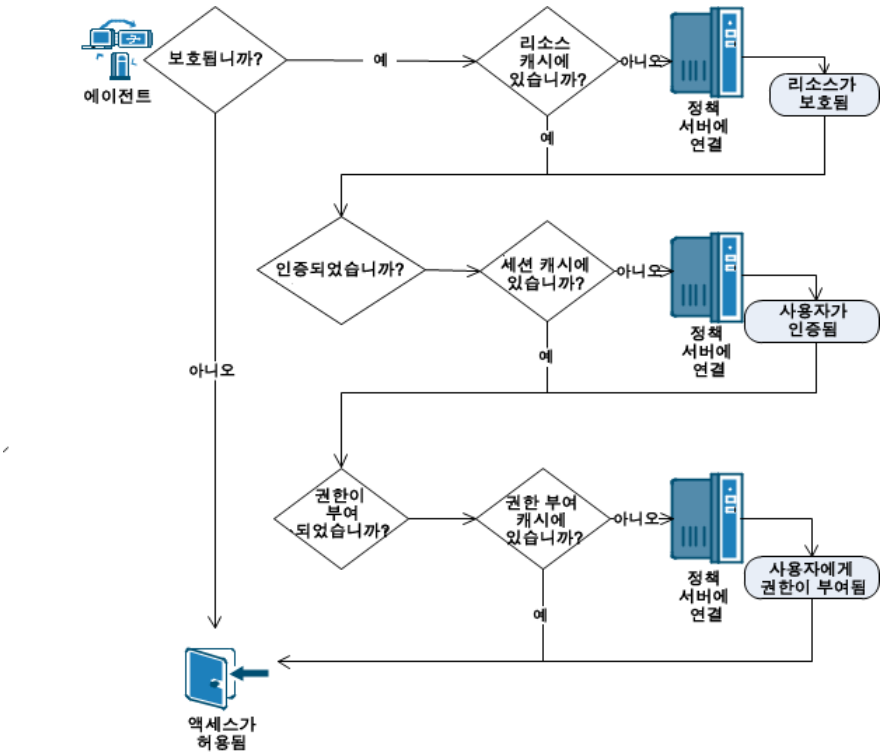
SiteMinder 에이전트에는 함께 사용하여 에이전트와 정책 서버 간 트래픽 양을 줄일 수 있는 여러 개의 캐시 및 구성 매개 변수가 있습니다. 일반적으로 이러한 설정은 정책 및 URI 가 대개 정적인 SiteMinder 환경에서 가장 효율적입니다.

## 에이전트 캐시 작동 방식

SiteMinder 에이전트는 SiteMinder 정책 서버에 연결하기 전에 다음 캐시에서 필요한 정보를 검색합니다.

- 리소스 캐시
- 세션 캐시
- 권한 부여 캐시

정책 서버에 연결하는 것보다 캐시에서 정보를 검색하는 것이 더 빠르기 때문에 성능이 향상됩니다. 다음 그림은 이러한 프로세스를 보여 줍니다.



## 리소스 캐시

각 SiteMinder 에이전트는 리소스 캐시를 사용하여 정책 서버에서 받는 다음과 같은 정보를 임시로 저장합니다.

- 리소스가 보호되는지 여부
- 정책에 포함된 추가 응답 특성

에이전트는 리소스 캐시를 검색하여 정책 서버에 연결하기 전에 리소스가 보호되는지 여부를 확인합니다. 리소스가 캐시에 있을 경우 에이전트가 정책 서버에 대해 IsProtected 호출을 실행하지 않으므로 정책 서버에 대한 트래픽이 줄어듭니다.

리소스 캐시에는 두 가지 에이전트 구성 매개 변수가 영향을 줍니다. SiteMinder 배포를 계획할 때 다음 사항을 고려하십시오.

**리소스 캐시 시간 만료**

용량 계획 테스트 결과를 기반으로 에이전트 리소스 캐시의 시간 만료 간격을 지정하는 것이 좋습니다. 시간 만료 간격이 너무 작으면 리소스 캐시의 효율성이 제한됩니다. 에이전트 구성의 ResourceCacheTimeout 매개 변수 값이 리소스 캐시의 시간 만료 간격을 결정합니다.

**리소스 캐시 크기**

사용자가 요청할 것으로 예상되는 최대 URI 개수보다 10% 크게 리소스 캐시를 사용하는 것이 좋습니다. 동적 URL(예: 쿼리 문자열이 포함된 URL)을 사용하는 응용 프로그램을 보호하는 경우 리소스 캐시의 크기를 조정하는 대신 IgnoreQueryData 매개 변수를 사용해 보십시오. MaxResourceCacheSize 에이전트 구성 매개 변수의 값이 리소스 캐시의 크기를 결정합니다.

**참고:** 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

## 리소스 캐시 및 URL 쿼리 문자열

URL 쿼리 문자열을 사용하는 응용 프로그램을 보호하려면 쿼리 문자열의 데이터를 무시하도록 웹 에이전트를 구성하여 리소스 캐시의 장점을 활용할 수 있습니다. 쿼리 문자열 데이터가 무시되면 잘려진 URL 이 리소스 캐시에 저장됩니다. 웹 에이전트 구성의 IgnoreQueryData 매개 변수 값을 설정하여 쿼리 문자열을 무시할 수 있습니다.

**중요!** URL 쿼리 데이터를 사용하는 정책이 있을 경우 이 설정을 활성화하지 마십시오.

다음 표에서는 URL 의 쿼리 문자열을 무시하여 리소스 캐시에서 해당 항목이 사용되는지, 아니면 웹 에이전트가 정책 서버에 연결해야 하는지 여부를 확인하는 방법을 보여 줍니다.

| 쿼리 문자열과 함께 요청된 URL | 캐시에 저장된 잘린 URL | 캐시된 항목이 사용됨 | 정책 서버가 연결됨 |
|---|---|---|---|
| /exampleapplication/page1.html ?user=firstuser | /exampleapplication/ page1.html | 아니요 | 예 |
| /exampleapplication/page1.html ?user=seconduser | | 예 | 아니요 |
| /exampleapplication/page2.html ?user=seconduser | /exampleapplication/ page2.html | 아니요 | 예 |

**참고:** 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

## 세션 캐시(인증)

각 SiteMinder 에이전트는 세션 캐시를 사용하여 정책 서버가 이미 인증한 사용자의 인증 정보를 저장합니다.

에이전트는 인증을 위해 정책 서버에 연결하기 전에 세션 캐시를 검색하여 사용자가 인증되었는지 확인합니다. 세션 캐시는 정책 서버에 대한 인증 호출의 수를 줄여서 성능을 향상시킵니다.

사용자에 대한 인증은 다음 이벤트 중 하나가 발생할 때 종료됩니다.

- 사용자가 로그아웃합니다.
- 사용자와 관련된 세션이 만료됩니다.
- 캐시에 있는 항목의 기간이 60 분을 초과합니다.

그러면 인증 정보가 세션 캐시에서 제거되고 삭제됩니다.

## 권한 부여 캐시

각 SiteMinder 에이전트는 권한 부여 캐시를 사용하여 정책 서버가 이미 권한을 부여한 사용자의 권한 부여 ID 를 저장합니다.

에이전트는 권한 부여를 위해 정책 서버에 연결하기 전에 권한 부여 캐시를 검색하여 사용자에게 권한이 부여되었는지 확인합니다. 권한 부여 캐시는 정책 서버에 대한 권한 부여 호출의 수를 줄여서 성능을 향상시킵니다.

사용자에 대한 권한 부여는 다음 이벤트 중 하나가 발생할 때 종료됩니다.

- 사용자가 로그아웃합니다.
- 사용자와 관련된 세션이 만료됩니다.

그러면 권한 부여 ID 가 캐시에서 제거되고 삭제됩니다.

## 세션 및 권한 부여 캐시 설정

정책 서버 설정과 에이전트 구성 매개 변수의 조합을 통해 세션 캐시와 권한 부여 캐시를 제어할 수 있습니다. 용량 계획의 결과를 지침으로 사용하여 SiteMinder 배포에서 다음 설정에 가장 적합한 값을 결정하십시오.

**세션 시간 만료**

다음과 같이 세션 시간 만료를 설정하는 것이 좋습니다.

- 최대 수의 사용자가 보호되는 응용 프로그램에 액세스하는 지속 기간에 맞춰 최대 세션 시간 만료를 설정하십시오.
- 유휴 세션 시간 만료를 다음 조건을 모두 충족하는 간격으로 설정하십시오.
  - 사용자가 작업하는 동안 로그아웃되지 않을 정도로 충분히 긴 시간
  - 사용자가 로그아웃하지 않고 컴퓨터에서 벗어나는 등 응용 프로그램이 사용되지 않을 경우 사용자를 자동으로 로그아웃하기에 충분할 정도로 짧은 시간

정책 서버 설정이 시간 만료 간격을 결정합니다.

### 세션 캐시 크기

세션 시간 만료 간격 중에 지속된 기간 동안 리소스에 액세스할 것으로 예상되는 사용자의 수를 기반으로 이 캐시의 크기를 지정하십시오. 크기 추정에 세션 시간 만료 기간 동안 로그아웃했다가 다시 로그인한 사용자를 포함하십시오. 요청 수가 비교적 적을 것으로 예상되는 사용자는 크기 추정에 포함하지 마십시오. 이러한 사용자는 세션 캐시 및 권한 부여 캐시에 거의 영향을 주지 않기 때문입니다. MaxSessionCacheSize 라는 웹 에이전트 구성 매개 변수가 세션 캐시와 권한 부여 캐시 모두의 크기를 결정합니다.

**추가 정보:**

지속적 인증 비율을 추정하는 방법 (페이지 105)

## 캐싱 및 익명 사용자

SiteMinder 에서 제공하는 익명 인증 체계는 이 체계를 통해 보호되는 리소스에 대한 액세스 제어를 제공하지 *않습니다*. 익명 인증 체계에서는 네트워크에서 식별되지 않은 사용자에 대해 다음 동작이 허용됩니다.

- 사용자가 사이트로 돌아오는 빈도를 추적합니다.
- 특정 사용자가 사이트를 방문하는 동안 수행하는 작업(예: 사용자가 방문 중에 열어본 페이지)을 추적합니다.
- 특정 사용자를 위해 개인화된 콘텐츠를 표시합니다.

사용자가 익명 인증 체계로 보호되는 리소스를 요청하면 정책 서버는 GUID(전역 고유 식별자)를 할당하고 이를 관련된 사용자의 브라우저에 저장합니다. SiteMinder 는 이 GUID 를 사용하여 사용자를 식별합니다.

익명 인증 체계를 사용할 계획인 경우 다음 항목을 구현하면 SiteMinder 환경에서 성능을 향상시킬 수 있습니다.

- 익명 요청을 처리하는 웹 서버를 분리합니다.
- CacheAnonymous 매개 변수를 설정하여 익명 요청을 캐싱하도록 분리된 각 웹 서버에서 웹 에이전트를 구성합니다.

익명 사용자에 대해 별도의 웹 서버와 웹 에이전트를 사용하면 보호된 리소스에 대한 요청을 처리하는 다른 웹 서버의 캐시가 너무 자주 플러시되는 것을 방지할 수 있습니다.

**참고:** 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

## 웹 에이전트 성능에 영향을 미치는 다른 매개 변수

다음 매개 변수도 웹 에이전트 성능에 영향을 미칩니다.

- PSPollInterval
- IgnoreExt
- IgnoreURL

## 정책 서버 폴 간격 매개 변수

SiteMinder 에이전트는 정책 서버에 주기적으로 연결하여 업데이트된 정책 또는 암호화 키를 수신합니다. 정책 서버에 연결하는 간격은 PSPollInterval 에이전트 구성 매개 변수를 변경하여 조정할 수 있습니다.

시간 간격을 늘리면 에이전트와 정책 서버 간의 불필요한 트래픽을 줄일 수 있습니다. SiteMinder 환경에 다음과 같은 특성이 있는 경우 간격을 늘리는 것을 고려하십시오.

- 에이전트의 수가 많은 경우
- SiteMinder 정책의 대부분이 정적이고 자주 변경되지 않는 경우

  **참고:** 자세한 내용은 에이전트에 대한 *에이전트 구성 안내서* 또는 *에이전트 안내서*를 참조하십시오.

**중요!** PSPollInterval 매개 변수를 늘리면 에이전트가 SiteMinder 정책 변경을 실행하는 시간에도 영향을 줍니다. 예를 들어 해고된 직원에 대한 액세스 권한을 해지하도록 10 시 30 분에 정책을 변경하고 PSPollInterval 매개 변수의 값이 3600(초)이라고 가정합니다. 웹 에이전트는 11 시 30 분이 될 때까지 변경된 정책을 실행하지 않습니다.

## 확장명 무시 매개 변수

SiteMinder 로 보호하려는 리소스에 보호를 *원하지 않는* 이미지나 파일이 많이 포함된 경우에는 특정 파일 확장명을 무시하도록 웹 에이전트를 구성하여 웹 에이전트와 정책 서버 간의 트래픽을 줄일 수 있습니다.

웹 에이전트가 정책 서버에 대해 다음 호출을 하지 *않으므로* 성능이 향상됩니다.

- IsProtected
- IsAuthenticated
- IsAuthorized
- 로그인

관련 리소스에 대한 요청이 직접 웹 서버로 전달되고 사용자에게 액세스 권한이 부여됩니다.

보호할 리소스를 먼저 식별하면 웹 에이전트에서 무시할 파일 확장명(있는 경우)을 결정하는 데 도움이 됩니다.

웹 에이전트 구성의 IgnoreExt 매개 변수에 무시할 파일 확장명을 추가합니다.

**참고:** 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

**추가 정보:**

보안을 적용할 응용 프로그램 식별 (페이지 67)

### URL 무시 매개 변수

특정 하위 디렉터리의 리소스를 보호하지 않는 상태로 두려면 특정 URI(Uniform Resource Identifiers)를 무시하도록 웹 에이전트를 구성할 수 있습니다.

예를 들어 각 웹 서버에 pictures 라는 하위 디렉터리가 있고 이 디렉터리를 보호하려면 웹 에이전트 구성에서 IgnoreURL 매개 변수를 설정할 수 있습니다.

웹 에이전트가 정책 서버에 대해 다음 호출을 하지 *않으므로* 성능이 향상됩니다.

- IsProtected
- IsAuthenticated
- IsAuthorized
- 로그인

관련 리소스에 대한 요청이 직접 웹 서버로 전달되고 사용자에게 액세스 권한이 부여됩니다.

## 부하 분산을 통해 에이전트 성능 향상

SiteMinder 에이전트 및 정책 서버가 여러 개 있는 경우 동적 부하 분산을 사용하면 에이전트가 모든 정책 서버에 요청을 분산시키므로 지연이 줄어들고 처리량이 향상됩니다. 동적 부하 분산을 통해 에이전트가 정책 서버에 보다 빠르게 액세스할 수 있게 되고 인증 및 권한 부여가 훨씬 효율적으로 수행됩니다.

SiteMinder 는 다중 정책 서버 통신에 대한 소프트웨어 기반 장애 조치와 부하 분산 기능을 제공합니다. 호스트 구성 개체의 EnableFailover 매개 변수에서 다음 값 중 하나를 사용하여 웹 에이전트 연결의 처리 방법을 결정합니다.

- 이 값을 yes 로 설정하면 에이전트가 항상 호스트 구성 개체에 처음 나열된 정책 서버(왼쪽에서 오른쪽)에 연결을 시도합니다. 정책 서버가 여러 개 있는 경우 모든 에이전트가 첫 번째 정책 서버에 연결을 시도합니다. 목록의 첫 번째 서버를 사용할 수 없는 상태가 아니라면 목록의 다른 서버에 연결되지 않습니다. 일부 정책 서버가 많은 연결을 처리하고 다른 정책 서버는 훨씬 적은 수의 연결을 처리한다는 점에서 대규모 환경에서는 이 구성이 부하 분산보다 효율성이 떨어집니다.
- 이 값을 no 로 설정하면 부하 분산이 사용됩니다. 에이전트가 호스트 구성 개체에 나열되어 있는 모든 정책 서버에 라운드 로빈 방식으로 요청을 분산시킵니다. 다중 정책 서버를 사용할 경우 더 높은 처리량을 얻으려면 이 설정을 사용하는 것이 좋습니다. 부하 분산 정책 서버 중 하나를 사용할 수 없어도 장애 조치는 계속 수행됩니다.

  **참고:** 자세한 내용은 *SiteMinder 정책 서버 구성 안내서*를 참조하십시오.

또한, SiteMinder 는 SiteMinder 에이전트 및 정책 서버 간의 연결에서 고성능 동적 부하 분산을 제공하는 하드웨어 부하 분산 장치를 사용할 수 있도록 지원합니다. 가상 IP 주소를 통해 다중 정책 서버를 노출하도록 구성한 경우 하드웨어 부하 분산 장치가 해당 가상 주소에 연결된 모든 정책 서버 간 부하 분산을 처리합니다. 에이전트가 장애 조치나 부하 분산을 처리할 필요가 없으므로 EnableFailover 매개 변수를 yes 로 설정하여 SiteMinder 부하 분산이 사용되지 않도록 설정합니다. 호스트 구성 개체에서 정책 서버 그룹을 노출하는 단일 또는 다중 VIP 를 구성합니다.

## 다중 스레드 웹 및 응용 프로그램 서버에서 SiteMinder 장애 조치 및 부하 분산

Sun Java 시스템, IIS, 작업자 모드의 Apache 기반 서버, WebSphere 응용 프로그램 서버 등과 같은 다중 스레드 웹 및 응용 프로그램 서버에서 실행되는 SiteMinder 에이전트는 시작 시 정책 서버에 대해 최소 개수의 소켓을 엽니다.

정책 서버 간 장애 조치나 부하 분산이 수행되도록 환경을 구성한 경우 에이전트는 시작 시 각 정책 서버에 대해 최소 개수의 소켓을 엽니다. 부하 분산 정책 서버의 경우 각 정책 서버가 전체 요청의 절반만 처리하기 때문에 각 정책 서버에 대해 훨씬 적은 수의 소켓이 열리지만 정책 서버에 대한 연결은 동일한 방식으로 처리됩니다.

장애 조치가 구성되어 있고 에이전트와 기본 정책 서버 간에 오류가 발생하면 장애 조치 정책 서버에 대한 연결이 사용됩니다. 장애 조치는 서비스별로 발생하기 때문에 기본 정책 서버와 장애 조치 정책 서버 모두에 대한 연결이 동시에 활성화될 수 있습니다. 기본 정책 서버가 복구된 후에도 장애 조치 서버에 대해 열린 소켓이 그대로 유지됩니다. 모든 새 소켓은 기본 정책 서버에 대해 열립니다.

**추가 정보:**

Apache 기반 웹 서버 Worker 모드를 사용하는 웹 에이전트 및 정책 서버의 상호 작용 (페이지 171)

## 다중 프로세스 웹 및 응용 프로그램 서버에서 SiteMinder 장애 조치 및 부하 분산

프리포크(pre-fork) 모드의 Apache 기반 서버와 같은 다중 프로세스 웹 또는 응용 프로그램 서버에서 실행되는 SiteMinder 에이전트는 장애 조치가 발생했는지 여부와 관계없이 구성된 *모든* 정책 서버에 대해 동일한 수의 연결을 엽니다.

자식 프로세스마다 정책 서버에 대한 고유한 연결이 있기 때문에 장애 조치가 발생할 경우 각 자식에 대해 독립적으로 처리됩니다. 결과적으로 장애 조치가 발생하면 각 소켓에서 500 오류가 발생합니다. 기본 정책 서버가 복구된 후에도 장애 조치 서버에 대해 열린 소켓이 열린 상태로 그대로 유지됩니다. 모든 새 소켓은 기본 정책 서버에 대해 열립니다.

**추가 정보:**

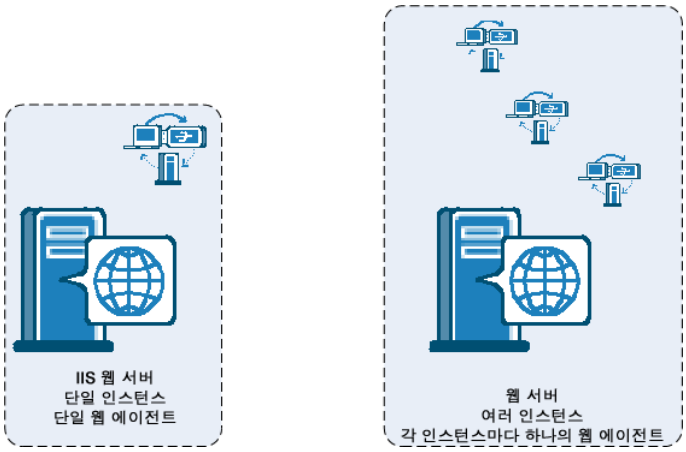
Apache 기반 웹 서버 프리포크(Pre-Fork) 모드를 사용하는 웹 에이전트 및 정책 서버의 상호 작용 (페이지 171)

# 웹 서버, 웹 에이전트 및 웹 서버 프로세스

각 SiteMinder 에이전트마다 자체 웹 서버 인스턴스가 필요합니다. 예를 들어 IIS 웹 서버는 IIS 웹 서버가 설치된 컴퓨터의 단일 인스턴스를 사용하여 작동합니다. IIS 에이전트의 수는 IIS 웹 서버의 수와 동일합니다.

컴퓨터 한 대에 여러 인스턴스를 지원하는 다른 웹 서버의 경우 각 인스턴스별로 하나의 SiteMinder 에이전트를 설치하고 구성할 수 있습니다. 예를 들어 하나의 컴퓨터에서 세 개의 개별적인 웹 서버 인스턴스를 실행하는 경우가 있습니다. 각 인스턴스마다 자체 에이전트가 있습니다. 따라서 하나의 컴퓨터에서 세 개의 SiteMinder 에이전트가 작동합니다.

다음 그림은 이러한 예를 보여 줍니다.




Apache 웹 서버의 경우 다음과 같은 MRM(다중 처리 모듈)이 SiteMinder 에이전트 프로세스가 정책 서버에 연결하는 방식에 영향을 미칩니다.

**프리포크(pre-fork) 모드**

추가 요청을 처리할 자식 프로세스를 생성합니다.

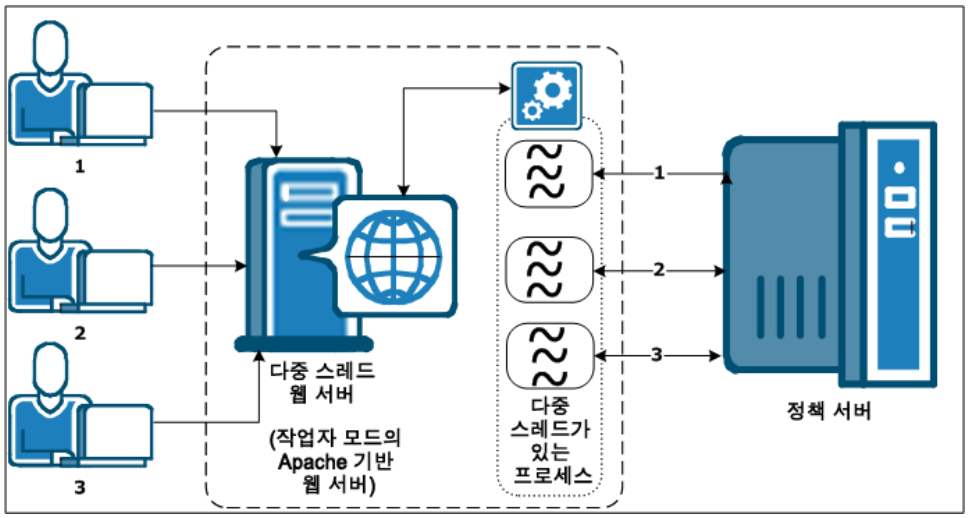
**Worker 모드**

추가 요청을 처리하기 위해 연결 풀에서 추가 스레드를 가져옵니다.

## Apache 기반 웹 서버 Worker 모드를 사용하는 웹 에이전트 및 정책 서버의 상호 작용

Worker 모드의 Apache 기반 웹 서버는 스레드를 사용하여 SiteMinder 정책 서버 연결을 처리합니다. 부하가 높을 때 정책 서버에 대한 추가 연결을 생성하기 위하여 연결 풀에서 필요에 따라 스레드를 가져옵니다.

다음 그림은 이러한 프로세스를 보여 줍니다.



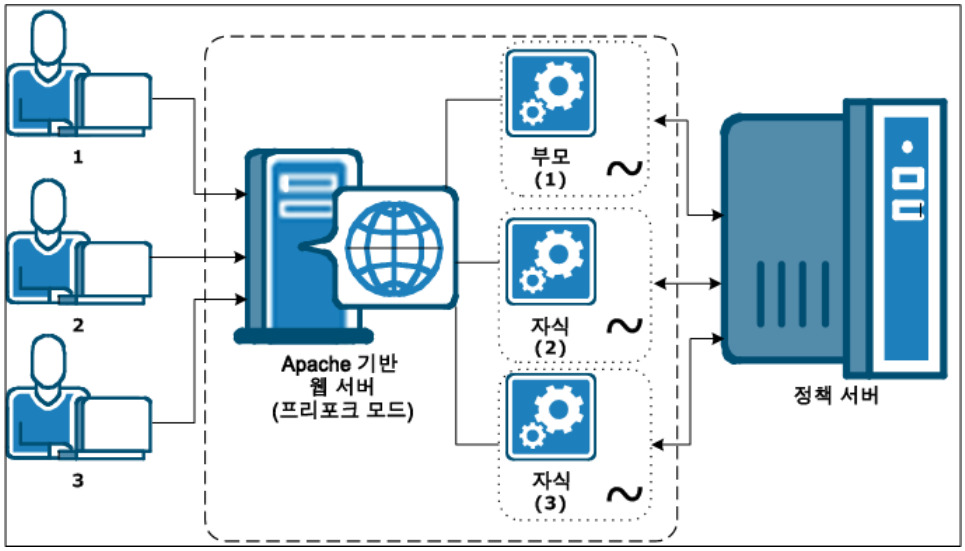

**추가 정보:**

다중 스레드 웹 및 응용 프로그램 서버에서 SiteMinder 장애 조치 및 부하 분산 (페이지 168)

## Apache 기반 웹 서버 프리포크(Pre-Fork) 모드를 사용하는 웹 에이전트 및 정책 서버의 상호 작용

프리포크(Pre-Fork) 모드의 Apache 기반 웹 서버가 요청을 수신하면 웹 서버는 SiteMinder 정책 서버와 통신하기 위해 자식 프로세스를 생성합니다. 더 많은 요청이 수신될수록 이를 처리하기 위해 더 많은 자식 프로세스가 생성됩니다. Apache 기반 웹 서버가 생성한 각 자식 프로세스는 SiteMinder 정책 서버에 대하여 고유한 독립적인 연결을 갖습니다.

다음 그림은 이러한 프로세스를 보여 줍니다.




Apache 기반 웹 서버의 경우 httpd.conf 파일에 있는 MaxClients 매개 변수의 값에 따라 웹 서버에서 생성하는 자식 프로세스의 수가 결정됩니다. Apache 기반 웹 서버의 부모 프로세스가 자식 프로세스를 생성할 때 자식 프로세스는 SiteMinder 정책 서버에 대한 초기 연결을 엽니다.

웹 에이전트의 수와 웹 에이전트 프로세스의 수 사이에는 중요한 차이가 있습니다. 각 웹 에이전트마다 자체 웹 서버 인스턴스가 필요합니다. 예를 들어 IIS 웹 서버는 단일 인스턴스로만 작동하기 때문에 IIS 웹 에이전트의 수는 IIS 웹 서버의 수와 동일합니다. 다른 유형의 서버에는 하나의 물리적 웹 서버 내에서 여러 포트를 수신하는 여러 서버 인스턴스가 있을 수 있습니다.

Apache 기반 웹 서버에서 SiteMinder 정책 서버로 열린 최대 소켓 수는 MaxClients 매개 변수의 값에 웹 에이전트 프로세스 수를 곱한 값과 같습니다. 예를 들어 서버의 MaxClients 매개 변수 값이 150 으로 설정되어 있고 웹 에이전트 프로세스가 다섯 개인 경우에 가능한 열린 소켓 수의 최대값은 750 입니다.

다중 프로세스 웹 서버를 사용하면 SiteMinder 환경에서 정책 서버에 대한 웹 에이전트 프로세스의 비율에 영향을 미칩니다. 초당 트랜잭션 수가 아니라 웹 에이전트 프로세스와 정책 서버 간의 연결 수가 제한 요소가 되는 경우가 많습니다.

웹 에이전트를 배포하기 전에 요청을 수신하는 SiteMinder 정책 서버가 관련 웹 서버가 열 수 있는 최대 연결 수를 처리할 수 있는지 확인하십시오.

**추가 정보:**

다중 프로세스 웹 및 응용 프로그램 서버에서 SiteMinder 장애 조치 및 부하 분산 (페이지 169)

# 응용 프로그램 계층 성능

정책 서버는 응용 프로그램 계층의 정책과 데이터 계층의 사용자 자격 증명 및 특성을 평가하여 리소스를 보호합니다. 응용 프로그램 계층의 성능을 조정할 때 다음 지침을 고려하십시오.

- 사용자를 인증하는 데 필요한 시스템 리소스의 양은 성능에 영향을 미칩니다.
- 사용자에게 권한을 부여하는 데 필요한 시스템 리소스의 양은 성능에 영향을 미칩니다.
- 인증 및 권한 부여 중에 수행되는 SiteMinder 사용자 디렉터리에 대한 정책 서버 요청의 수는 성능에 영향을 미칩니다.

## SiteMinder 정책 설계 및 성능

SiteMinder 정책은 사용자가 리소스와 상호 작용하는 방식을 정의합니다. 관리 UI 에서 SiteMinder 정책을 생성할 때는 사용자, 리소스 및 리소스와 연결된 작업을 식별하는 개체를 함께 연결(바인딩)합니다.

특정 SiteMinder 구성 요소를 구성하는 방식을 통해 또는 선택적 기능을 활성화하도록 선택하여 성능을 향상시키거나 저하시킬 수 있습니다. 성능 전략은 다음과 같습니다.

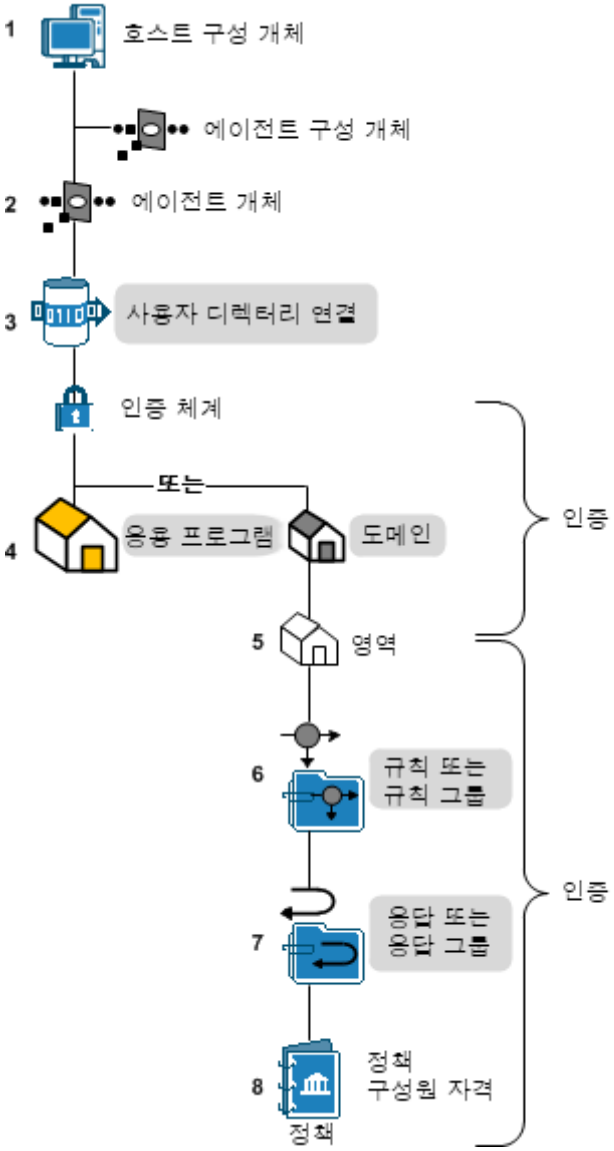
- 성능에 영향을 미칠 수 있는 SiteMinder 정책 개체를 식별
- 사용자 인증에 영향을 미치는 SiteMinder 매개 변수 및 기능을 식별
- 사용자 권한 부여에 영향을 미치는 SiteMinder 매개 변수 및 기능을 식별

엔터프라이즈의 비즈니스 규칙 및 보안 요구 사항이 궁극적으로 SiteMinder 정책 설계에 반영되어야 합니다. 다음은 이러한 요구 사항을 충족하는 동시에 SiteMinder 성능의 균형을 유지하는 데 사용할 수 있는 지침입니다.

## SiteMinder 정책 개체 및 성능 로드맵

SiteMinder 에서는 핵심 SiteMinder 정책 개체를 특정한 순서로 구성해야 합니다. 다음 다이어그램은 이러한 순서를 나타내며 여기에서 음영으로 표시된 항목은 사용자 인증 또는 권한 부여 중에 성능에 영향을 미치는 개체를 나타냅니다.

**참고:** HCO(호스트 구성 개체) 및 ACO(에이전트 구성 개체)는 웹 계층의 성능에 영향을 미칩니다.



**추가 정보:**

웹 계층 성능 (페이지 152)

## 응용 프로그램

응용 프로그램을 구성하는 방식에 따라 인증 및 권한 부여 동안의 성능이 향상되거나 저하될 수 있습니다.

응용 프로그램은 하나 이상의 관련 웹 서비스에 대한 완전한 보안 정책을 정의하는 정책 서버 개체입니다. 응용 프로그램은 웹 서비스 리소스를 사용자 역할과 연결하여 웹 서비스 사용자별로 액세스할 수 있는 웹 서비스 응용 프로그램 리소스를 결정하는 권한 정책을 지정합니다.

응용 프로그램을 생성할 때는 정책 서버가 사용자 인증을 시도하는 하나 이상의 사용자 디렉터리 연결에 해당 응용 프로그램을 바인딩합니다. 따라서 디렉터리 연결의 수와 디렉터리 연결이 나열되는 순서는 인증하는 동안 SiteMinder 성능에 직접적인 영향을 미칩니다.

응용 프로그램에 보호된 리소스로 정의된 웹 서비스 포트 및 작업의 수는 권한 부여 중의 SiteMinder 성능과 관련이 있습니다.

리소스를 하나 이상의 응답에 바인딩할 수 있습니다. 리소스가 액세스될 때는 연결된 응답이 사용자 특성, DN 특성, 정적 텍스트, 사용자 지정 활성 응답 등의 정보를 에이전트에 반환합니다.

웹 서비스 리소스에 바인딩하는 응답의 유형은 권한 부여 중의 SiteMinder 성능과 직접적으로 관련이 있습니다.

## 도메인

도메인을 구성하는 방식에 따라 인증할 때 성능이 향상되거나 저하될 수 있습니다.

SiteMinder 정책 도메인은 하나 이상의 사용자 디렉터리와 연결된 리소스의 논리적 그룹입니다. 도메인을 생성할 때는 하나 이상의 사용자 디렉터리 연결을 도메인에 바인딩합니다.

정책 서버는 이 디렉터리 연결을 사용하여 사용자 인증을 시도합니다. 따라서 디렉터리 연결의 수와 디렉터리 연결이 나열되는 순서는 인증하는 동안 SiteMinder 의 성능과 직접적인 관련이 있습니다.

**참고:** 도메인 구성에 대한 자세한 내용은 정 *책*서버 구성 안내서를 참조하십시오.

**추가 정보:**

리소스를 도메인 또는 EPM 응용 프로그램으로 그룹화 (페이지 68)
도메인 및 인증 성능 (페이지 182)

## 영역

영역을 구성하는 방식에 따라 인증할 때의 성능이 향상되거나 저하될 수 있습니다.

도메인의 리소스를 하나 이상의 영역으로 그룹화합니다. 영역은 공통된 보안(인증) 요구 사항을 갖는 리소스(URL) 집합입니다. 사용자가 정의하는 리소스 필터 및 선택하는 인증 체계는 인증하는 동안의 성능과 직접적인 관련이 있습니다.

- 리소스 필터는 보호된 리소스의 루트 역할을 합니다. 요청된 리소스가 보호되는지 확인하려면 정책 서버에서 리소스 필터를 평가해야 합니다(IsProtected?).
- 영역과 연결된 인증 체계에 따라 사용자가 영역의 리소스에 액세스하기 위해 제시해야 하는 자격 증명의 유형이 결정됩니다(IsAuthenticated?).

또한 영역 설정에 따라 다음이 결정됩니다.

- SiteMinder 가 사용자 세션을 처리하는 방법. SiteMinder 는 사용자가 인증되는 영역의 컨텍스트에서 사용자 세션을 생성합니다.
- 인증 도중 작업을 제어하기 위해 영역을 사용할 수 있는지 여부.

**참고:** 영역에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오. 인증 체계에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

**추가 정보:**

리소스를 영역 또는 EPM 응용 프로그램으로 그룹화 (페이지 70)
영역 및 인증 성능 (페이지 183)

## 규칙 및 규칙 그룹

영역을 구성하는 방식에 따라 권한을 부여할 때의 성능이 향상되거나 저하될 수 있습니다.

규칙 또는 규칙 그룹은 영역의 컨텍스트에서 생성합니다. 규칙

- 보호가 필요한 영역 내에서 특정 리소스를 식별합니다.
- 특정 인증 또는 권한 부여 이벤트에 기반하여 리소스에 대한 액세스를 허용하거나 거부하기 위해 사용할 수 있습니다.

규칙에 정의하는 리소스 필터(영역 필터가 접두어로 추가됨)는 보호가 필요한 리소스를 식별합니다.

정책 서버는 규칙을 평가하여 요청된 리소스와 가장 일치하는 리소스 필터를 결정합니다. 일치할 경우 정책 서버는 규칙이 바인딩된 정책을 실행하여 사용자에게 리소스에 액세스할 권한이 있는지 확인합니다.

영역 내에 있는 규칙의 수와 각 리소스 필터를 정의하는 방식은 권한 부여를 수행하는 동안 SiteMinder 의 성능과 직접적인 관련이 있습니다.

**참고:** 규칙에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

**추가 정보:**

규칙 및 권한 부여 성능 (페이지 184)

## 응답

응답을 구성하는 방식에 따라 권한을 부여하는 동안의 성능이 향상되거나 저하될 수 있습니다.

응답 또는 응답 그룹은 특정한 규칙 또는 규칙 그룹에 바인딩됩니다. 규칙이 실행될 때 응답은 다음을 수행할 수 있습니다.

- 사용자 세션이 유효한 상태로 유지되는 시간을 사용자 지정합니다.
- 사용자를 다른 리소스로 리디렉션합니다.
- 사용자 디렉터리에 포함된 특성에 기반하여 사용자가 받는 콘텐츠를 사용자 지정합니다.
- 정적 텍스트, 사용자 특성, DN 특성, 사용자 지정된 활성 응답 또는 정의된 변수의 런타임 값을 정책 서버에서 SiteMinder 에이전트로 전달합니다.
- SiteMinder WSS 에이전트에 WS-Security 헤더 및 SAML 세션 티켓을 생성하도록 지시하십시오.

정책 규칙을 하나 이상의 응답에 바인딩할 수 있습니다. SiteMinder 정책 규칙에 바인딩하는 응답의 유형은 권한을 부여하는 동안의 SiteMinder 의 성능과 직접적인 관련이 있습니다.

**참고:** 응답에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

**추가 정보:**

응답 및 권한 부여 성능 (페이지 185)

## 인증 지침

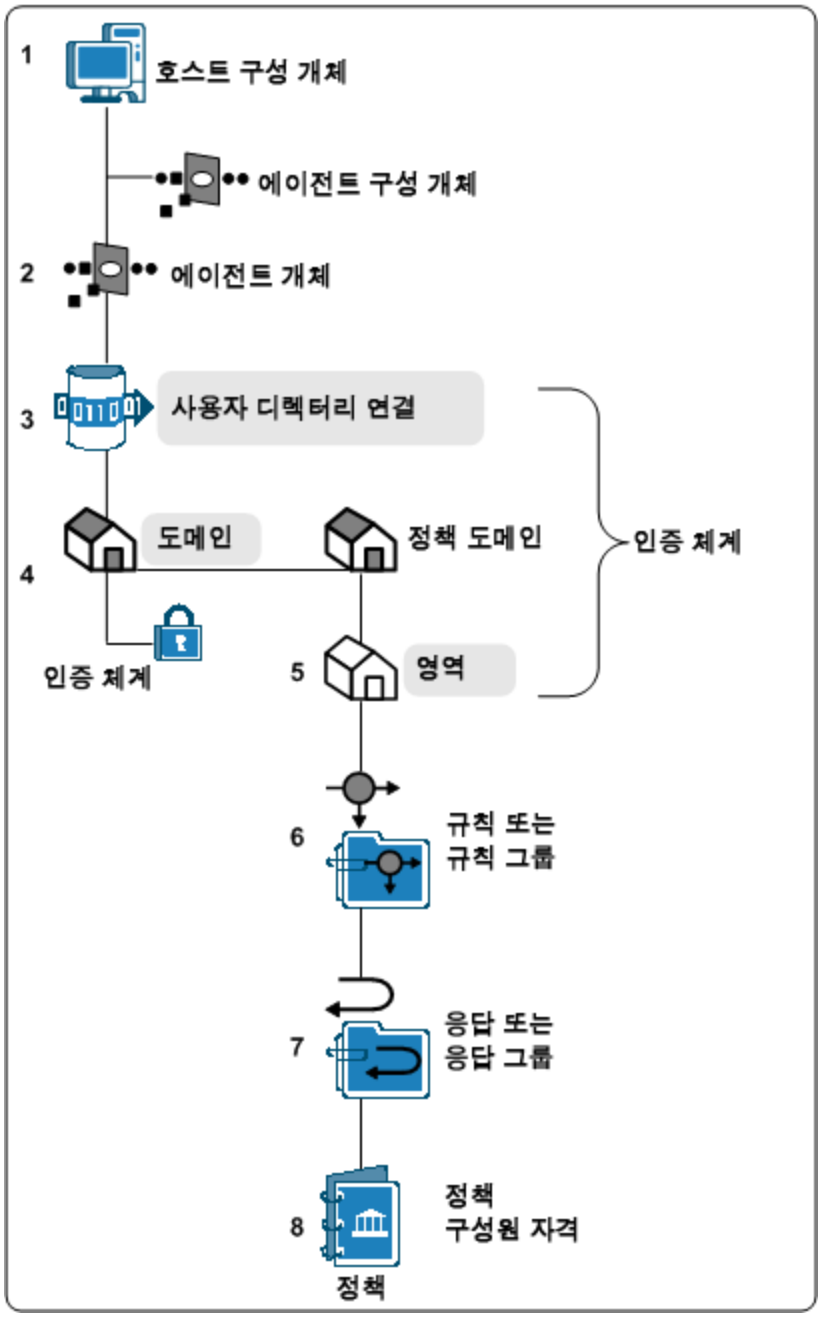
인증(IsAuthenticated?) 단계 중 SiteMinder 의 성능은 일반적으로 다음과 관련이 있습니다.

- 인증 요청을 처리하는 데 사용되는 시스템 리소스
- 정책 서버가 인증 요청을 처리하기 위해 SiteMinder 사용자 디렉터리에 수행하는 읽기/쓰기(통칭하여 요청)의 수

## SiteMinder 정책 개체 및 성능 로드맵

특정 SiteMinder 정책 개체를 구성하는 방식을 통해 또는 그러한 개체와 연결된 선택적 기능을 활성화하도록 선택하여 인증 성능을 향상시키거나 저하시킬 수 있습니다.

SiteMinder 에서는 핵심 SiteMinder 정책 개체를 특정한 순서로 구성해야 합니다. 다음 다이어그램은 이러한 순서를 나타내며 여기에서 음영으로 표시된 항목은 사용자 인증 시 성능에 영향을 미치는 개체를 나타냅니다.


1
호스트 구성 개체
에이전트 구성 개체
2
에이전트 개체
3
사용자 디렉터리 연결
4
도메인
정책 도메인
인증 체계
인증 체계
5
영역
6
규칙 또는
규칙 그룹
7
응답 또는
응답 그룹
8
정책
구성원 자격
정책

## 사용자 디렉터리 및 인증 성능

도메인을 구성하려면 하나 이상의 사용자 디렉터리 연결을 도메인에 바인딩해야 합니다. 정책 서버는 사용자 디렉터리 연결에 지정된 검색 조건을 사용하여 인증 단계에서 사용자 자격 증명을 확인합니다.

**참고:** 사용자 디렉터리 연결 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

디렉터리 수준에서 사용자 인증 성능에 영향을 미치는 요소는 다음과 같습니다.

- 검색 식 및 쿼리 - LDAP 식 또는 ODBC 쿼리가 복잡할수록 정책 서버가 사용자를 인증하기 위해 조건을 확인하는 데 걸리는 시간이 길어집니다.
- 암호 서비스 - SiteMinder 사용자 디렉터리에 암호 정책을 적용할 수 있습니다. 암호 정책을 구현하기 전에 다음 사항을 고려하십시오.
  - 정책 서버는 암호 정책에 연결된 특성을 읽고 이를 업데이트해야 할 수 있습니다. 특성을 업데이트하려면 정책 서버는 사용자 디렉터리에 써야 합니다.
  - 암호 정책이 로그인 상세 정보를 추적하도록 구성된 경우에는 인증할 때마다 추가적인 사용자 디렉터리 쓰기가 필요합니다.
  - 정책 서버는 전체 디렉터리보다 디렉터리 내 특정 사용자 그룹에만 적용되는 암호 정책을 확인하는 데 더 많은 시간을 소비합니다.

## eTrust SOA Security Manager 인증 체계 및 인증 성능

각 eTrust SOA Security Manager 인증 체계는 서로 다른 수준의 WSS 에이전트 처리 오버헤드를 발생시키며 이는 WSS 에이전트 유형 간에도 달라질 수 있습니다.

일반적으로 디지털 서명 확인 또는 페이로드 기밀성이 필요하지 않은 인증 체계의 경우에 인증 처리량이 더 높습니다.

디지털 서명 확인은 웹 서버용 WSS 에이전트에서 더 많은 CPU 와 데이터를 사용하지만 응용 프로그램 서버용 WSS 에이전트에도 약간의 영향을 미칩니다.

## 도메인 및 인증 성능

도메인(또는 전체 응용 프로그램 개체) 수준에서 사용자 인증 성능에 영향을 미치는 요소는 다음과 같습니다.

- 도메인의 디렉터리 연결 수 - 정책 서버는 사용자 자격 증명의 유효성을 확인할 수 있을 때까지 도메인의 각 사용자 디렉터리를 검색합니다. 사용자 디렉터리 연결의 수가 많을수록 정책 서버가 사용자를 인증하는 데 걸리는 시간이 길어집니다.

  도메인의 디렉터리 연결 수를 줄이는 방법을 찾아서 불필요한 정책 서버 요청을 방지하십시오. 다음 사항을 고려하십시오.

  - 도메인 내의 리소스를 요청하는 사용자 및 해당 정보가 저장된 디렉터리
  - 조직을 SiteMinder 배포에 추가할 때 사용자 디렉터리를 결합

- 사용자 디렉터리 연결이 나열되는 순서 - 정책 서버는 사용자 디렉터리를 도메인에서 나열하는 순서대로 검색합니다. 연결 순서를 결정할 때는 인증 우선 순위를 평가하십시오. 다음 사항을 고려하십시오.

  - 특정 디렉터리에서 응용 프로그램에 액세스하는 사용자의 비율이 더 높은지 여부
  - 인증 우선 순위가 더 높은, 더 작은 규모의 사용자 그룹이 있는지 여부

## 영역 및 인증 성능

영역(또는 응용 프로그램 개체 구성 요소) 수준에서 사용자 인증 성능에 영향을 미치는 요소는 다음과 같습니다. 영역을 구성할 때 다음 사항을 고려하십시오.

- 자격 증명 수집 - 영역은 특정한 인증 체계와 연관되며 일부 인증 체계에는 자격 증명 수집기를 사용해야 합니다. 이러한 유형의 인증 체계를 사용하여 리소스를 보호하는 에이전트는 사용자를 자격 증명 수집기로 리디렉션하여 자격 증명을 수집합니다. 자격 증명을 수집하면 인증 프로세스에 추가적인 단계가 추가됩니다.

  **참고:** 인증 체계 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오. 자격 증명 수집기 사용에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오.

- 영구 세션 - SiteMinder 가 사용자를 인증할 때 정책 서버는 세션 티켓을 발행합니다. 세션 티켓에는 사용자에 대한 기본 정보와 사용자의 인증 컨텍스트가 포함됩니다. 기본적으로 SiteMinder 는 에이전트가 사용자 웹 브라우저의 쿠키에 세션 티켓을 쓰는 비영구 세션을 통해 세션 관리를 구현합니다.

  일부 SiteMinder 기능에는 영구 세션이 필요합니다. 영구 세션에 대한 영역을 구성할 수 있습니다. 이 영역의 리소스를 보호하는 에이전트는 SiteMinder 세션 저장소에 세션 티켓을 쓰기 때문에 각 인증마다 세션 저장소에 대한 추가적인 요청이 생성됩니다.

  **중요!** 영구 세션은 성능에 큰 영향을 미칠 수 있습니다.

  **참고:** 사용자 세션에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

- 인증 이벤트 - 기본적으로 영역은 인증 이벤트를 처리하도록 구성됩니다. 이 설정을 통해 사용자가 인증되거나 인증에 실패할 경우 실행할 규칙을 정의할 수 있습니다. 정책 평가 논리는 인증 이벤트를 처리하도록 구성된 모든 영역에 적용됩니다. 이 논리는 시스템 리소스를 소비하며 사용자 디렉터리 요청을 생성할 수 있습니다.

  사용자가 리소스에 대한 액세스를 얻기 위해 인증할 때 발생하는 이벤트 작업의 필요성을 평가하십시오. 인증 작업이 필요하지 않은 경우 영역의 인증 이벤트가 사용되지 않도록 설정하여 인증 단계의 속도를 높이십시오.

  **참고:** 영역에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

# 권한 부여 지침

권한 부여 도중 SiteMinder 의 성능은 일반적으로 다음과 관련이 있습니다.

- 권한 부여 요청을 처리하는 데 사용되는 시스템 리소스
- 정책 서버가 권한 부여 요청을 처리하기 위해 SiteMinder 사용자 디렉터리에 수행하는 읽기/쓰기(통칭하여 요청)의 수

SiteMinder 정책 설계의 복잡성이 이러한 각 영역에 영향을 미칩니다.

## 정책 개체 및 성능

특정 SiteMinder 정책 개체를 구성하는 방식을 통해 또는 이러한 개체와 연결된 선택적 기능을 활성화하도록 선택하여 인증 성능을 향상시키거나 저하시킬 수 있습니다. 다음 정책 개체는 사용자 권한 부여 과정에서 성능에 영향을 미칠 수 있습니다.

- 규칙 (페이지 184)
- 응답 (페이지 185)
- 정책 구성원 자격 (페이지 186)

## 규칙 및 권한 부여 성능

규칙(또는 응용 프로그램 개체 리소스) 수준에서 사용자 권한 부여 성능에 영향을 미치는 요소는 다음과 같습니다.

- 단일 영역에서 규칙 수가 많으면 권한 부여 결정 속도가 느려질 수 있습니다. 사용자가 특정 영역에 대해 인증된 경우 정책 서버는 사용자가 요청하는 특정 리소스(URL)와 가장 일치하는 리소스 필터를 확인하기 위해 영역 내의 모든 규칙을 평가해야 합니다.
- 리소스 필터의 유형은 정책 서버가 리소스 일치를 평가하는 속도에 영향을 미칩니다.

**참고:** 규칙에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

다음 필터는 성능에 미치는 영향이 가장 작은 순서대로 나열한 것입니다.

- 정확히 일치 - 특정 리소스를 사용하여 리소스 필터를 정의하면 성능에 미치는 영향이 가장 적습니다. 정책 서버는 리소스 필터를 요청된 리소스의 URL 과 비교하기만 하면 됩니다.

  **예:** 회사에서 사용자 지정 영역(/customer)을 생성하고 포털 응용 프로그램의 특정 페이지(lending_home.html)를 사용하여 규칙을 지정합니다. 그 결과 생성되는 리소스 필터는 /customer/lending_home.html 입니다. 이 경우 요청된 리소스와 규칙 간의 일치를 평가하려면 정책 서버가 요청된 리소스를 리소스 필터와 비교하여 일치 여부를 확인하기만 하면 됩니다.

- 정확한 접두사 - 접두사를 사용하여 리소스 필터를 정의하면 정확한 일치에 비해 성능에 더 큰 영향을 미칩니다. 정책 서버는 요청된 리소스가 리소스의 루트(영역) 내에 포함되어 있는지 여부를 확인해야 하기 때문입니다.

  **예:** 회사에서 직원 영역(/employee)을 생성하고 "*.html"을 사용하여 규칙을 지정합니다. * 접두사는 직원 영역의 모든 html 파일이 보호된다는 것을 나타냅니다. 그 결과 생성되는 리소스 필터는 /employee /*.html 입니다. 이 경우 요청된 리소스와 리소스 필터 간의 일치를 평가하려면 정책 서버는 요청된 리소스가 직원 디렉터리의 일부이고 HTML 파일인지를 평가해야 합니다.

- 정규식 - 정규식을 사용하여 리소스 필터를 정의하면 성능에 가장 큰 영향을 미칩니다. 정책 서버는 식을 평가하여 그 결과를 요청된 리소스와 비교해야 합니다. 식이 복잡할수록 성능에 미치는 영향이 더 큽니다.

## 응답 및 권한 부여 성능

SiteMinder 정책의 규칙에 바인딩된 응답 특성의 유형은 성능에 영향을 미칩니다. 다음 응답 유형은 성능에 미치는 영향이 가장 작은 순서대로 나열한 것입니다.

- 정적 - 정적 특성을 정의하면 일관된 데이터가 반환됩니다.
- 사용자 특성 - 사용자 특성을 정의하면 사용자 디렉터리에 있는 사용자 항목의 프로필 정보가 반환됩니다.

  **참고:** 이러한 유형의 응답을 위해서는 정책 서버가 사용자 디렉터리를 검색해야 합니다.

- DN 특성 - DN 특성을 정의하면 사용자가 연관된 디렉터리 개체와 연결된 정보가 반환됩니다. 특성을 DN 특성으로 취급할 수 있는 디렉터리 개체의 예로는 사용자가 속한 그룹과 사용자 DN 의 일부인 조직 단위(OU)가 있습니다.

  **참고:** 이러한 유형의 응답을 위해서는 정책 서버가 사용자 디렉터리를 검색해야 합니다.

## SiteMinder 정책 구성원 자격 및 권한 부여 성능

정책 구성원 자격은 정책에 적용할 사용자를 지정하는 SiteMinder 정책의 일부입니다. SiteMinder 정책은 도메인에 저장되므로 SiteMinder 정책 구성원 자격을 도메인에 바인딩된 사용자 디렉터리에 저장된 모든 사용자에게 적용하려면 필터를 사용합니다. 정의하는 필터의 유형에 따라 정책 서버가 SiteMinder 정책 구성원 자격을 평가하는 방법이 결정됩니다.

**참고:** SiteMinder 정책에 사용자를 추가하는 방법에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

다음 필터는 성능에 미치는 영향이 가장 작은 순서대로 나열한 것입니다.

- 모두 - "모두"는 성능에 가장 작은 영향을 미칩니다.

  SiteMinder 이 사용자를 인증할 때 정책 서버는 세션 티켓을 발행합니다. 세션 티켓은 사용자가 저장되어 있는 사용자 디렉터리를 식별합니다. 정책 서버는 정책이 사용자에게 적용되는지 결정할 때 SiteMinder 정책에 바인딩된 디렉터리에 세션 티켓을 비교하기만 하면 됩니다.

  **참고:** 사용자 세션에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

- 고유 이름 - DN(고유 이름)은 "모두"보다 성능에 더 큰 영향을 미칩니다.

  인증된 사용자의 DN 이 포함된 조직 또는 조직 단위는 세션 티켓에 저장됩니다. 정책 서버는 세션 티켓 정보와 SiteMinder 정책 구성원 자격 필터를 비교하여 정책이 사용자에게 적용되는지 여부를 확인해야 합니다.

- 그룹 구성원 자격 또는 검색 식 - 이러한 유형의 필터는 고유 이름에 비해 성능에 더 큰 영향을 미칩니다. 그룹 구성원 자격 및 검색 식은 추가적인 시스템 리소스를 소비하며 사용자 디렉터리 검색을 수행해야 합니다. 정책 서버는 다음을 수행해야 합니다.

  a. 그룹 구성원 자격 또는 검색 식을 확인합니다.

  b. 사용자 디렉터리를 검색하여 SiteMinder 정책이 사용자에게 적용되는지 확인합니다.

- 중첩된 그룹 - 중첩된 그룹을 사용하여 SiteMinder 정책 구성원 자격을 정의하면 성능에 가장 큰 영향을 미칩니다.

  정책 서버는 SiteMinder 정책이 사용자에게 적용되는지 확인할 때 디렉터리의 각 사용자 그룹 및 모든 하위 그룹을 검색해야 합니다.

  **중요!** 디렉터리의 그룹 계층 구조가 깊으면 정책 서버가 정책 구성원 자격을 평가할 때 걸리는 시간에 영향이 미칠 수 있습니다.

**참고:** 사용자 권한 부여 캐시를 활성화하면 정책 서버가 정책 구성원 자격을 확인하기 위해 사용자 디렉터리에 수행하는 요청의 수를 줄일 수 있습니다.

**추가 정보:**

사용자 권한 부여 캐시 (페이지 187)

## 사용자 권한 부여 캐시

사용자 권한 부여 캐시는 사용자와 정책 간의 관계를 저장하여 SiteMinder 정책 구성원 자격을 확인하기 위한 사용자 디렉터리 요청의 수를 감소시킵니다.

**참고:** 사용자 권한 부여 캐시는 사용자에 대한 데이터를 저장하거나, 사용자 특성 값을 저장하거나, 사용자 항목을 캐시하지 않습니다.

예를 들어 사용자 A 가 속한 "Administrator" 그룹에 세 개의 정책이 적용되도록 구성되어 있습니다. 정책 서버는 처음으로 SiteMinder 정책 구성원 자격을 평가할 때 그룹 구성원 자격을 확인하고 사용자 디렉터리에 세 번의 요청을 수행하여(각 정책마다 한 번씩) 각 SiteMinder 정책이 적용되는지 확인해야 합니다.

정책 서버는 이 결과를 사용자 권한 부여 캐시에 씁니다. 이후의 정책 평가에서는 정책 서버가 사용자 디렉터리 요청을 수행할 필요가 없습니다. 그 대신 정책 서버는 캐시된 권한 부여 정보를 사용하여 정책 구성원 자격을 확인합니다.

**참고:** 정책 서버는 주기적으로 정책 업데이트를 폴링합니다. 기본 간격은 60 초입니다. 정책 구성원 자격이 변경되면 정책 서버는 정책을 다시 로드하고 업데이트된 정책과 관련된 캐시 항목을 제거합니다.

**추가 정보:**

SiteMinder 정책 구성원 자격 및 권한 부여 성능 (페이지 186)

## 사용자 권한 부여 캐시 효율성

사용자 권한 부여 캐시는 다음과 같은 경우에 가장 효율적입니다.

- 세션 중에 모든 사용자 요청이 일관되게 동일한 서버로 전송(지속)됩니다.
- 모든 SiteMinder 에이전트가 라운드 로빈 부하 분산이 아니라 정책 서버 장애 조치를 위해 구성되어 있습니다.

이러한 요소가 충족되지 않으면 사용자 권한 부여 캐시의 효율이 감소합니다.

### 예: 라운드 로빈 부하 분산을 위해 구성된 사용자 권한 부여 캐시 및 에이전트

SiteMinder 에이전트 라운드 로빈 풀에 있는 정책 서버의 수가 많을수록 사용자 권한 부여 캐시의 효율이 감소할 가능성이 높아집니다.

단일 SiteMinder 에이전트가 두 개의 정책 서버 간에 라운드 로빈되도록 구성된 경우 보호된 리소스에 대한 첫 번째 요청에 따라 정책 서버 중 하나에 사용자 권한 부여 캐시 항목이 생성됩니다. 캐시 항목이 없는 정책 서버가 두 번째 요청을 처리해야 하는 확률은 약 50 %입니다. 하지만 더 진행되면 두 정책 서버 모두가 이후 요청을 위해 데이터를 캐시하게 됩니다.

이제 10 개의 정책 서버 간에 라운드 로빈되도록 구성된 단일 에이전트의 효과에 대해 생각해 보겠습니다. 정책 서버가 사용자에게 권한을 부여하고 결과를 권한 부여 캐시에 입력한 후에 동일한 정책 서버가 다음 요청을 처리해야 하는 확률은 10 %에 불과합니다. 이 구성에서 캐시 적중 확률이 50 %가 되려면 5 건의 캐시 누락이 발생해야 합니다.

**참고:** 정책 서버 클러스터는 사용자 권한 부여 캐시에 대한 라운드 로빈 부하 분산의 효과를 줄일 수 있습니다.

## 사용자 권한 부여 캐시의 크기 추정

사용자 권한 부여 캐시의 기본 크기는 10 MB 입니다. 사용자 권한 부여 캐시에 필요한 공간을 추정하고 정책 서버 관리 콘솔을 사용하여 기본 크기를 조정할 수 있습니다.

### 사용자 권한 부여 캐시의 크기를 추정하려면

1. 캐시 항목의 개수를 추정하려면 다음 공식을 사용하십시오.

   *expected_users* * *number_of_policies_per_session* = *entries*

   ***expected_users***

   SiteMinder 가 보호하는 응용 프로그램에 대하여 인증되는 총 사용자 수를 지정합니다.

   ***number_of_policies_per_session***

   세션 중에 사용자에게 적용되는 SiteMinder 정책의 평균 개수를 지정합니다.

   **참고:** 각 SiteMinder 정책이 사용자 권한 부여 캐시에 고유한 항목을 입력할 가능성이 있습니다.

   ***entries***

   권한 부여가 생성할 수 있는 캐시 항목 수를 지정합니다.

2. 캐시의 크기를 추정하려면 다음 공식을 사용하십시오.

   (*entries* * .000062) + 1

   **참고:** .000062 는 대략적인 캐시 항목의 크기(MB 단위)를 나타냅니다.

## 감사 및 성능

기본적으로 정책 서버는 감사 이벤트를 텍스트 파일에 쓰며 이 파일을 정책 서버 로그라고 합니다. 원하는 경우 이벤트를 감사 데이터베이스에 로깅하도록 정책 서버를 구성할 수 있습니다.

**참고:** 이벤트를 감사 데이터베이스에 로깅하도록 정책 서버를 구성하는 방법에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오. 감사 데이터베이스 구성에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

이벤트를 감사 데이터베이스에 로깅하도록 결정한 경우에는 다음 사항을 고려하십시오.

- SiteMinder 는 모든 인증 및 권한 부여 결정을 데이터베이스에 로깅하므로 인증 및 권한 부여와 관련된 성능에 영향을 미칩니다.
- (선택 사항) 동기식 로깅 - 영역 수준에서 동기식 로깅을 구성할 수 있습니다. 이를 구성하면 정책 서버는 레코드가 감사 데이터베이스에 저장될 때까지 각 인증 및 권한 부여 요청의 결과를 차단합니다. 레코드가 저장되기 전에는 사용자가 인증되거나 권한을 부여받지 않습니다.

## 응용 프로그램 계층 부하 분산

다양한 SiteMinder 에이전트 매개 변수를 조정하고 SiteMinder 정책 설계 지침을 따르더라도 정책 서버가 인증 및 권한 부여 요청에 처리하는 데 걸리는 시간이 크게 향상되지 않을 수 있습니다.

에이전트와 정책 서버가 여러 개인 경우 동적 부하 분산을 적용하면 에이전트가 요청을 모든 정책 서버로 분산하므로 지연 시간이 감소하고 처리량이 향상됩니다.

**추가 정보:**

중복성 및 고가용성 (페이지 39)

# 데이터 계층 성능

SiteMinder 데이터 저장소, 특히 사용자 디렉터리와 연관된 성능 저하는 SiteMinder 성능 저하의 가장 일반적인 원인 중 하나입니다. 데이터 계층 성능은 일반적으로 다음 두 가지 일반 영역과 관련이 있습니다.

- 데이터 계층 자체. 적절하게 조정되지 않았거나 시스템 리소스가 부족한 사용자 디렉터리로 인해 SiteMinder 성능이 저하될 수 있습니다.
- 사용자 디렉터리가 작동해야 하는 용량. SiteMinder 인증 및 권한 부여 서비스 때문에 사용자 디렉터리에 대해 많은 수의 읽기 및 쓰기(통칭하여 요청)가 수행됩니다. SiteMinder 작업 부하를 처리할 수 있도록 사용자 디렉터리 자체에 대한 용량 계획 수립을 수행하십시오.

성능 전략은 다음과 같습니다.

- 데이터 계층 자체가 성능 저하의 주요 원인이 아닌지 확인합니다.
- 특정 기간 동안 SiteMinder 가 처리해야 하는 인증 및 권한 부여의 수를 식별합니다.

  **참고:** 사용자 인증 및 권한 부여가 발생하는 지속적 비율 및 최고 비율을 계산할 수 있습니다.
- 각각의 사용자 인증 및 이후의 권한 부여가 생성하는 사용자 디렉터리 요청의 수를 추정합니다.

**추가 정보:**

용량 계획 소개 (페이지 103)
용량 계획 소개 (페이지 119)

# 데이터 계층 지침

정책 서버는 표준 프로토콜을 사용하여 데이터 계층과 상호 작용합니다. 디렉터리 서버 및 데이터베이스가 일반적인 클라이언트에서 최대한의 성능을 발휘하도록 조정된 경우에는 이러한 조정을 통해 SiteMinder 성능이 향상됩니다.

**참고:** 조정 지침은 해당 공급업체의 설명서를 참조하십시오.

SiteMinder 성능은 사용자 디렉터리의 성능과 연관되므로 그 성능을 향상시키기 위한 몇 가지 일반적인 고려 사항이 있습니다. 다음 영역을 확인하십시오.

- 사용자 디렉터리가 사용할 수 있는 시스템 리소스와 이러한 리소스를 사용하기 위해 경합할 수 있는 모든 외부 리소스
- SSL(Secure Socket Layer)의 사용
- SiteMinder 가 사용자 디렉터리를 검색할 수 있는 효율성
- 정적 IP 주소의 사용
- 복제의 사용

## 시스템 리소스

사용자 디렉터리가 사용할 수 있는 시스템 리소스는 SiteMinder 의 성능과 직접적으로 관련이 있습니다. 사용자 디렉터리가 높은 수준의 사용률로 작동 중인 경우에는 SiteMinder 를 조정하여 성능을 향상시킬 수 없습니다.

사용자 디렉터리를 호스트하는 시스템의 성능이 다음 사항으로 인해 저하되지 않는지 확인하십시오.

- 느린 CPU 또는 I/O 시스템
- 메모리 부족
- 올바르지 않게 구성된 버퍼 캐시
- 부족하거나 단편화된 디스크 공간

## SSL(Secure Socket Layer) 및 사용자 디렉터리

SiteMinder 환경에 SSL 을 구성할 계획이라면 다음 사항을 고려하십시오.

- 정책 서버와 LDAP 사용자 디렉터리가 SSL 을 통해 통신하도록 구성하면 성능이 저하됩니다. 보안 요구 사항을 검토하여 SSL 이 필수인지 확인하십시오.
- SSL 을 구성하기로 결정한 경우에는 정책 서버와 디렉터리 서버 사이에 SSL 가속기를 배치하지 마십시오. 그렇지 않으면 정책 서버가 디렉터리의 단일 인스턴스를 가정합니다. 이 경우 가속기 뒤의 여러 사용자 디렉터리 간에 일관되지 않은 쓰기가 발생할 수 있습니다.

## 정적 IP 주소 및 사용자 디렉터리

관리 UI 에서 사용자 디렉터리 연결을 구성할 때 호스트 이름 대신 정적 IP 주소를 사용하는 방법을 고려하십시오. 정책 서버가 호스트 이름을 확인하는 데 걸리는 시간은 무시해도 좋은 정도지만 정적 IP 주소를 사용하면 DNS(Domain Naming Services) 종속성이 제거됩니다.

## 사용자 디렉터리 검색

SiteMinder 가 사용자 디렉터리를 효율적으로 검색할 수 있도록 하면 성능에 직접적인 영향을 미칩니다. 다음 사항을 고려하십시오.

- 디렉터리 인덱싱을 사용하여 SiteMinder 의 검색 결과를 향상시킵니다.
  - LDAP - 검색에 사용되는 다른 모든 특성에 더하여 objectClass 특성도 인덱스해야 합니다.

    **참고:** Microsoft 에서는 objectClass 대신 objectCategory 특성을 사용할 것을 권장합니다. Active Directory 에서 objectClass 특성을 인덱스하지 못하면 성능이 크게 저하될 수 있습니다.
  - ODBC - SiteMinder 스키마 쿼리에서 검색 조건으로 정의된 모든 필드는 인덱스되어야 합니다.

    **참고:** 인덱싱에 대한 자세한 내용은 공급업체 설명서를 참조하십시오.
- 관리 가능한 사용자 그룹 집합을 반환하도록 쿼리를 설계합니다.

  **참고:** 쿼리를 최적화할 수 없는 경우 최대 검색 결과 매개 변수를 설정하여 너무 큰 결과 집합으로 인해 전체 성능이 저하되는 것을 방지하십시오.
- 표준 SQL 분석기로 ODBC 에 대한 SQL 쿼리 체계를 최적화합니다.

### 복제

복제는 다음 상황에서 성능을 저하시킬 수 있습니다.

- 마스터-슬레이브 복제에서 마스터 복제본만 쓰기 요청을 허용하는 경우. 일반적으로 암호 서비스를 사용할 때는 각 인증마다 암호 Blob 특성을 업데이트해야 합니다. 마스터 복제본만 쓰기를 처리할 수 있는 경우에는 각 쓰기 요청이 마스터로 리디렉션됩니다.

  이 리디렉션으로 인해 인증 단계에서 시간이 더 소요되며 마스터-복제본이 쓰기가 발생하는 속도를 수용하지 못할 수 있습니다.

- LDAP 조회가 사용되는 경우. LDAP 조회의 경우 각 요청에 디렉터리에 대한 둘 이상의 요청이 수반될 수 있으므로 성능을 저하시킬 수 있습니다.

## 사용자 저장소 용량 계획

정책 서버는 일련의 서비스를 수행하여 사용자를 인증하고, 권한을 부여합니다. 이러한 서비스의 결과로 사용자 디렉터리에 대한 여러 개의 읽기 및 쓰기가 발생하며 이를 통칭하여 요청이라고 합니다. 지속적 작업 및 최고 작업 기간 중 사용자 디렉터리가 이러한 작업 부하를 처리할 수 있는지 여부를 파악하면 SiteMinder 성능에 큰 도움이 됩니다.

SiteMinder 의 성능에 영향을 미치는 일반적인 요소는 다음과 같습니다.

- 총 작업 수 및 지속적 사용자 디렉터리 검색 비율 - 총 작업 수는 인증 및 권한 부여 요청을 처리할 때 정책 서버가 처리해야 하는 조합된 요청 수입니다. 이러한 작업이 발생하는 비율은 업무일 동안 크게 변동할 수 있습니다.

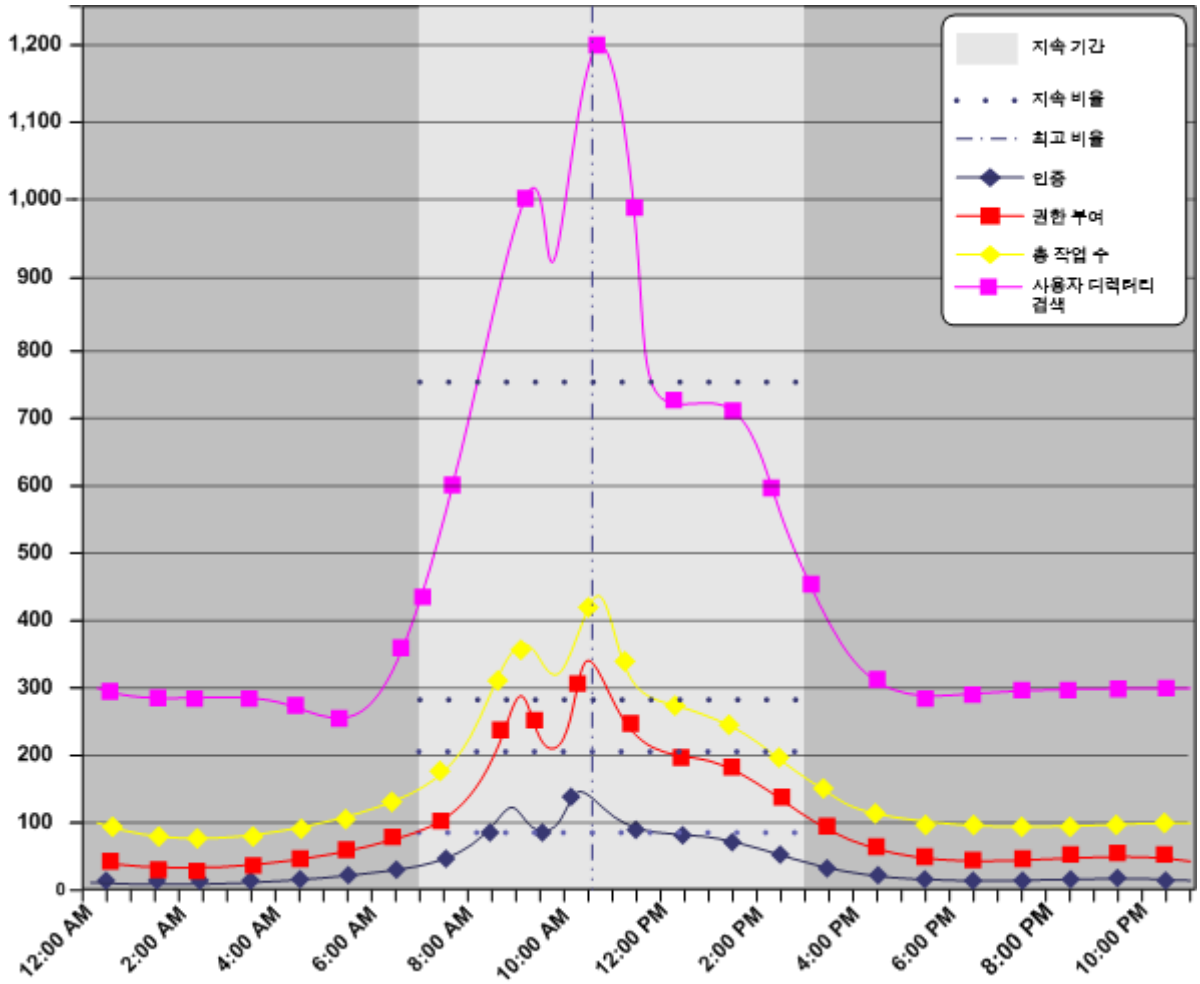
  이에 따라 정책 서버가 작업을 처리하기 위해 사용자 디렉터리 요청을 생성하는 속도가 변동합니다. 어떤 기간에는 비교적 적은 수의 사용자 디렉터리 요청이 생성되지만 다른 기간에는 더 많은 수가 생성됩니다.

  지속적 사용자 디렉터리 검색 비율은 정책 서버가 평균적인 숫자의 작업을 처리하기 위해 평균적인 숫자의 사용자 디렉터리 요청을 생성하는 기간을 나타냅니다.

- 총 작업 및 최고 사용자 디렉터리 검색 비율 - 지속적 활동 기간 중에 사용자 활동이 급증할 수 있습니다. 최고 사용자 디렉터리 검색 비율은 정책 서버가 최고 작업 수를 처리하기 위해 가장 높은 수의 사용자 디렉터리 요청을 생성하는 기간을 나타냅니다.

다음 그림은 다음 사항을 보여 줍니다.

- 총 작업과 사용자 디렉터리 검색 비율 간의 관계
- 각 비율이 하루 동안 변동하는 상황, 특정 기간 동안 지속되는 상황 및 해당 기간 중 최고 비율을 나타내는 상황




사용자 디렉터리가 작동해야 하는 부하를 추정할 때는 다음 지침을 사용하는 것이 좋습니다. 부하를 추정한 후에는 표준 도구를 사용하여 디렉터리에 부하를 생성하고 그 결과를 추적할 수 있습니다.

**참고:** 여러 요소로 인해 필요한 수치를 달성하지 못할 수 있습니다. 조정 지침은 해당 공급업체의 설명서를 참조하십시오.

**추가 정보:**

정책 서버 (페이지 14)
지속적 인증 비율을 추정하는 방법 (페이지 105)
지속적 권한 부여 비율을 추정하는 방법 (페이지 111)

## 사용자 저장소 용량 계획 검사 목록

인증 및 권한 부여 요청을 처리하기 위해 정책 서버가 수행해야 하는 사용자 디렉터리 요청의 수를 추정하려면 특정 정보가 필요합니다. 사용자 저장소 용량 계획을 시작하기 전에 다음 정보를 수집하십시오.

- ☐ 응용 프로그램에 대한 일별 총 인증 수(인증 부하)
- ☐ 응용 프로그램에 대한 일별 총 권한 부여 수(권한 부여 부하)
- ☐ 사용자가 응용 프로그램에 인증되고 보호된 리소스를 요청하는 지속적 기간 및 최고 기간

  **참고:** 용량 계획을 수립하면 사용자 활동의 인증 부하, 권한 부여 부하 및 지속적 수준과 최고 수준에 관련된 메트릭을 식별하는 데 도움이 됩니다.
- ☐ 활성화된 정책의 총 숫자. 각 SiteMinder 정책에 대해 다음을 확인하십시오.
  - SiteMinder 정책 구성원 자격 필터로 인해 하나 이상의 사용자 디렉터리 검색이 수행되는지 여부
  - SiteMinder 정책에 바인딩된 응답으로 인해 하나 이상의 사용자 디렉터리 검색이 수행되는지 여부

**추가 정보:**

용량 계획 소개 (페이지 103)
SiteMinder 정책 구성원 자격 및 권한 부여 성능 (페이지 186)
응답 및 권한 부여 성능 (페이지 185)

## 지속적 사용자 디렉터리 검색 비율을 추정하는 방법

지속적 사용자 디렉터리 검색 비율을 추정하려면 다음을 확인해야 합니다.

- 업무일 중 총 사용자 디렉터리 요청 수의 변동
- 사용자 디렉터리 요청이 지속 기간 동안 초당 요청 수로 해석되는 방식

지속적 사용자 디렉터리 검색 비율을 추정하려면 다음 단계를 완료하십시오.

1. 인증 지침을 사용하여 인증 부하가 생성하는 사용자 디렉터리 요청의 수를 추정합니다.
2. 권한 부여 지침을 사용하여 권한 부여 부하가 생성하는 사용자 디렉터리 요청의 수를 추정합니다.
3. 지속적 사용자 디렉터리 검색 비율을 추정합니다.

## 인증 지침을 사용하여 디렉터리 검색 추정

정책 서버는 각 인증 요청을 처리하기 위해 많은 수의 사용자 디렉터리 요청을 생성합니다. 사용자 디렉터리 요청 중 일부는 필요하지만 다른 일부는 회피할 수 있습니다.

다음 지침을 사용하여 각 인증으로 인해 생성되는 정책 서버 요청 수를 추정하십시오.

(필수) 각 사용자를 인증하기 위한 두 개의 검색:

- 사용자를 식별하기 위한 저장소당 하나의 검색/쿼리
- 사용자 자격 증명을 확인하기 위한 하나의 검색/쿼리

(선택 사항) 정책을 설계한 방식과 암호 서비스를 활성화했는지 여부에 따라 추가 검색이 필요할 수 있습니다.

- 사용자가 인증될 때 수행되는 규칙(OnAuth 규칙)에 바인딩된 각 SiteMinder 정책에 대한 하나의 검색/쿼리

  **참고:** 규칙 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오. 규칙과 SiteMinder 정책 간의 관계에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

- 사용자 특성을 반환하는 응답에 바인딩된 각 SiteMinder 정책마다 하나의 검색/쿼리

  **참고:** 응답 및 응답과 규칙의 관계에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

- 암호 서비스에 대해 활성화된 사용자 저장소당 하나의 쓰기/업데이트. 암호 서비스가 SiteMinder 정책 도메인의 사용자 디렉터리에 적용되지 않는 경우 쓰기/업데이트는 필수가 아닙니다.

  **참고:** 암호 서비스에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

다음 사용 사례에서는 각 지침을 사용하여 인증 부하로 인해 생성되는 총 사용자 디렉터리 검색 수를 확인하는 방법을 자세히 설명합니다.

## 사례 1: 사용자 인증 및 디렉터리 요청

회사에서 다음을 완료했습니다.

- 뱅킹 응용 프로그램을 위한 하나의 사용자 디렉터리를 배포했습니다.
- 용량 계획을 수립했습니다. 그 결과 사용자가 88,000 회의 로그인으로 인증 부하를 생성하는 것으로 확인되었습니다.

회사에서는 다음 공식을 사용하여 정책 서버가 인증 부하를 처리하기 위해 사용자 디렉터리로 전송하는 요청 수를 추정하기 시작합니다.

*authentication_load * 2 * number_of_user_stores = requests_for_authentication*

***authentication_load***

응용 프로그램에 대한 일별 인증 수를 지정합니다.

**참고:** 2 는 상수입니다. 사용자를 인증할 때 두 회의 요청이 생성됩니다. 사용자를 식별하기 위한 검색 하나와 자격 증명을 확인하기 위한 바인딩 하나입니다.

***number_of_user_stores***

구현의 사용자 저장소 수를 지정합니다.

***requests_for_authentication***

인증 부하가 생성하는 사용자 디렉터리 요청의 수를 지정합니다.

**결과:** 88,000 * 2 * 1 = 176,000 회의 요청

회사는 이 추정을 사용하여 일별 인증 부하를 처리하기 위해 필요한 총 사용자 디렉터리 요청 수를 결정합니다.

## 사례 2: 정책 설계 및 사용자 디렉터리 요청

회사는 응용 프로그램 포털을 보호하기 위해 네 개의 정책을 구성했으며, 그중 하나는 인증 성공 시 수행되는 규칙에 바인딩됩니다.

회사에서는 다음 공식을 사용하여 정책 서버가 인증 부하를 처리하기 위해 사용자 디렉터리로 전송하는 요청 수의 추정을 계속합니다.

*authentication_load* * (*percent_of_policies* * *number_of_searches*) = *requests_for_authentication*

***authentication_load***

응용 프로그램에 대한 일별 인증 수를 지정합니다.

***percent_of_policies***

활성화된 정책의 총 수를 지정하며, 백분율로 표현되고 특성은 다음과 같습니다.

- onAuth 규칙에 바인딩됩니다.
- 동일한 수의 사용자 디렉터리 검색을 생성합니다.

**예:** 활성화된 SiteMinder 정책이 4 개 있습니다. 하나는 OnAuth 규칙에 바인딩됩니다. 이 정책은 정책 구성원 자격을 확인하기 위해 하나의 사용자 디렉터리 검색을 생성합니다. 활성화된 정책의 25 %가 인증 시 실행되며 하나의 사용자 저장소 검색을 생성합니다. 나머지 정책은 인증 도중에 실행되지 않습니다.

***number_of_searches***

SiteMinder 정책이 인증된 각 사용자에게 적용되는지를 확인하기 위해 정책 서버가 수행하는 요청의 수를 지정합니다.

***requests_for_authentication***

인증 부하가 생성하는 사용자 디렉터리 요청의 수를 지정합니다.

**결과:** 88,000 * 0.25 * 1 = 22,000 회의 요청

회사는 이 추정을 사용하여 일별 인증 부하를 처리하기 위해 필요한 총 사용자 디렉터리 요청 수를 결정합니다.

## 사례 3: 응답 및 사용자 디렉터리 요청

회사에서 OnAuth 규칙을 사용하여 하나의 SiteMinder 정책을 정의했습니다. 이 정책에 따르면 정책이 실행될 때 CN(일반 이름) 특성 응답이 반환되어야 합니다. 회사는 이 값을 반환하기 위한 웹 에이전트 응답을 정의하고 이를 SiteMinder 정책 규칙에 바인딩합니다.

회사에서는 다음 공식을 사용하여 정책 서버가 인증 부하를 처리하기 위해 사용자 디렉터리로 전송하는 요청 수의 추정을 계속합니다.

*authentication_load* * *percent_of_policies* * *number_of_responses_per_policy* = *requests_for_authentication*

***authentication_load***

응용 프로그램에 대한 일별 인증 수를 지정합니다.

***percent_of_policies***

사용자 특성을 반환하는 특정한 수의 응답에 바인딩된, 활성화된 정책의 전체 수(백분율로 표현)를 지정합니다.

**예:** 활성화된 정책이 네 개이고 그중 하나가 응답을 사용하여 사용자 특성을 반환할 경우 정책의 25 %에 사용자 디렉터리 검색이 필요합니다.

***number_of_responses_per_policy***

SiteMinder 정책에 바인딩된 응답의 수를 지정합니다.

***requests_for_authentication***

인증 부하가 생성하는 사용자 디렉터리 요청의 수를 지정합니다.

**결과:** 88,000 * 0.25 * 1 = 22,000 회의 요청

회사는 이 추정을 사용하여 일별 인증 부하를 처리하기 위해 필요한 총 사용자 디렉터리 요청 수를 결정합니다.

## 사례 4: 암호 서비스 및 디렉터리 요청

회사에서 사용자 저장소에 대해 암호 서비스를 활성화했습니다.
회사에서는 다음 공식을 사용하여 정책 서버가 인증 부하를 처리하기 위해 사용자 디렉터리로 전송하는 요청 수의 추정을 계속합니다.

*authentication_load* * 1 = *requests_for_authentication*

***authentication_load***

응용 프로그램에 대한 일별 인증 수를 나타냅니다.

**참고:** 1 은 상수입니다. 사용자 로그인 상세 정보를 추적하려면 각 인증마다 하나의 사용자 디렉터리 쓰기가 필요합니다.

***requests_for_authentication***

인증 부하가 생성하는 사용자 디렉터리 요청의 수를 나타냅니다.

**결과:** 88,000 * 1 = 88,000 회의 요청

회사는 이 추정을 사용하여 일별 인증 부하를 처리하기 위해 필요한 총 사용자 디렉터리 요청 수를 결정합니다.

## 사례 5: 인증에 대한 총 디렉터리 요청 수

회사에서는 각 사용 사례의 개별적인 총계를 사용하여 정책 서버가 인증 부하를 처리하기 위해 사용자 저장소에 전송하는 총 요청 수를 확인합니다.

- 88,000 명의 고유한 사용자와 이들의 자격 증명을 식별하기 위한 176,000 회의 요청
- OnAuth SiteMinder 정책이 해당 사용자에게 적용되는지 확인하기 위한 22,000 회의 요청
- 인증 시 일반 이름 특성을 반환하기 위한 22,000 회의 요청
- 암호 정책에 대한 88,000 회의 요청

**결과:** 176,000 + 22,000 + 22,000 + 88,000 = 322,080 회의 요청

회사는 이 결과와 권한 부여에 기반한 결과를 사용하여 사용자 저장소가 정책 서버 요청을 처리해야 하는 지속적 비율을 추정합니다.

## 권한 부여 지침을 사용하여 디렉터리 검색 추정

정책 서버는 사용자에게 권한을 부여하기 위해 몇 개의 사용자 디렉터리 요청을 수행합니다. 어떤 사용자 디렉터리 요청은 SiteMinder 정책 구성원 자격을 확인하기 위해 필요하지만 다른 요청은 SiteMinder 정책 설계에 따라 다릅니다. 다음 지침을 사용하면 각 권한 부여로 인해 생성되는 정책 서버 요청 수를 추정할 수 있습니다.

- 정책 도메인의 각 SiteMinder 정책마다 하나의 검색/쿼리

  **참고:** 이 지침은 구성원 자격 필터의 결과로 하나 이상의 사용자 디렉터리 요청이 생성되는 정책에만 적용됩니다. SiteMinder 정책 구성원 자격과 사용자 디렉터리 요청의 관계에 대한 자세한 내용은 "Policy Membership and Authorization Requests"(정책 구성원 자격 및 권한 부여 요청)을 참조하십시오.

- 사용자 특성을 반환하는 응답에 바인딩된 각 SiteMinder 정책마다 하나의 검색/쿼리

  **참고:** 응답과 사용자 디렉터리 요청의 관계에 대한 자세한 내용은 "응답 및 권한 부여 성능"을 참조하십시오.

다음 사용 사례에서는 각 지침을 사용하여 권한 부여 부하로 인해 생성되는 총 사용자 디렉터리 검색 수를 확인하는 방법을 자세히 설명합니다.

**참고:** 사용자 권한 부여 캐시를 통해 사용자 디렉터리에 대한 권한 부여 관련 요청의 수를 크게 줄일 수 있습니다.

**추가 정보:**

SiteMinder 정책 구성원 자격 및 권한 부여 성능 (페이지 186)
응답 및 권한 부여 성능 (페이지 185)
사용자 권한 부여 캐시 (페이지 187)

## 사례 1: 정책 구성원 자격 및 사용자 디렉터리 요청

회사에서 포털 응용 프로그램을 보호하는 세 개의 정책을 활성화했습니다.

- 정책 A 에는 SiteMinder 정책 구성원 자격을 확인하기 위해 하나의 사용자 디렉터리 요청이 필요합니다.
- 정책 B 에는 SiteMinder 정책 구성원 자격을 확인하기 위해 최대 두 개의 사용자 디렉터리 요청이 필요합니다.
- 정책 C 에는 SiteMinder 정책 구성원 자격을 확인하기 위해 최대 세 개의 사용자 디렉터리 요청이 필요합니다.

또한 용량 계획 수립 결과 응용 프로그램의 권한 부여 부하가 726,000 회인 것으로 확인되었습니다.

회사에서는 다음 공식을 사용하여 정책 서버가 권한 부여 부하를 처리하기 위해 사용자 디렉터리로 전송하는 요청 수의 추정을 시작합니다.

*authorization_load* x *percent_of_policies* * *number_of_searches* = *daily_authorization_requests*

***authorization_load***

응용 프로그램에 대한 일별 권한 부여 수를 지정합니다.

***percent_of_policies***

SiteMinder 정책 구성원 자격을 확인하기 위해 동일한 숫자의 사용자 디렉터리 요청을 생성할 수 있는 활성화된 정책의 수(백분율로 표현)를 지정합니다.

**참고:** 총 백분율은 100 %여야 합니다.

***number_of_searches***

정책 서버가 SiteMinder 정책 구성원 자격을 확인하기 위해 수행할 수 있는 사용자 디렉터리 요청의 수를 지정합니다.

***daily_authorization_requests***

권한 부여 요청을 처리하기 위한 사용자 디렉터리 요청의 수를 지정합니다.

**결과:**

- 정책 A - 792,000 * 0.33 * 1= 261,360 회의 요청
- 정책 B 및 C - 792,000 * 0.66 * 2= 1,045,440 회의 요청
- 총 사용자 디렉터리 요청-158,000 + 1,045,440= 1,306,880 회의 요청

회사는 이 추정을 사용하여 일별 권한 부여 부하를 처리하기 위해 필요한 총 사용자 디렉터리 요청 수를 결정합니다.

**추가 정보:**

사용자 권한 부여 캐시 (페이지 187)

## 사례 2: 응답 및 사용자 디렉터리 검색

회사에서 포털 응용 프로그램을 보호하기 위해 세 개의 정책을 활성화했으며 그중 두 개는 사용자 특성을 반환하는 응답에 바인딩되어 있습니다.

- 정책 A 는 실행될 때 하나의 사용자 특성을 반환합니다.
- 정책 B 는 실행될 때 두 개의 사용자 특성을 반환합니다.
- 정책 C 는 사용자 특성을 반환하는 응답에 바인딩되어 있지 않습니다.

회사는 다음 공식을 사용하여 정책 서버가 사용자 특성을 반환하는 응답을 확인하기 위해 수행하는 사용자 디렉터리 요청의 수를 추정합니다.

*authorization_load * percent_of_policies * number_of_responses= daily_authorization_requests*

***authorization_load***

응용 프로그램에 대한 일별 권한 부여 수를 지정합니다.

***percent_of_policies***

사용자 특성을 반환하는 응답 때문에 동일한 수의 사용자 디렉터리 요청을 생성하는 활성화된 정책의 수(백분율로 표현)를 지정합니다.

**참고:** 총 백분율은 100 %여야 합니다.

***number_of_responses***

SiteMinder 정책에 바인딩된 응답의 수를 지정합니다.

***daily_authorization_requests***

권한 부여 요청을 처리하기 위한 사용자 디렉터리 요청의 수를 지정합니다.

**결과:**

- 정책 A - 792,000 * 0.2 x 1= 158,000
- 정책 B - 792,000 * 0.2 x 2= 316,800
- 정책 C - 792,000 * 0.6 x 0= 0
- 총 사용자 디렉터리 요청 - 158,000 + 316,800 + 0= 526,000

회사는 이 추정을 사용하여 일별 권한 부여 부하를 처리하기 위해 필요한 총 사용자 디렉터리 요청 수를 결정합니다.

### 사례 3: 권한 부여에 대한 총 디렉터리 요청 수

회사에서는 각 사용 사례의 개별적인 총계를 사용하여 정책 서버가 권한 부여 부하를 처리하기 위해 사용자 디렉터리에 전송하는 총 요청 수를 확인합니다.

- SiteMinder 정책 구성원 자격을 확인하기 위한 1,203,440 회의 요청
- 응답과 연결된 사용자 특성을 반환하기 위한 526,000 회의 요청

**결과:** 1,203,440 + 526,000= 1,729,440 회의 요청

회사는 이 결과와 인증에 기반한 결과를 사용하여 사용자 저장소가 정책 서버 요청을 처리해야 하는 지속적 비율을 추정합니다.

## 지속적 사용자 디렉터리 검색 비율 추정

지속적 사용자 디렉터리 검색 비율은 총 작업 수(인증 부하 더하기 권한 부여 부하), 즉 이러한 요청이 발생하는 시기와 비율을 기반으로 합니다. 이러한 요청이 업무일 동안 균등하게 분산될 가능성은 거의 없습니다. 대신 이러한 요청이 발생하는 비율은 지속 기간 중 가장 낮은 수준과 가장 높은(최고) 수준 내에서 크게 변동합니다.

지속적 사용자 디렉터리 검색 비율을 추정하려면 다음을 확인해야 합니다.

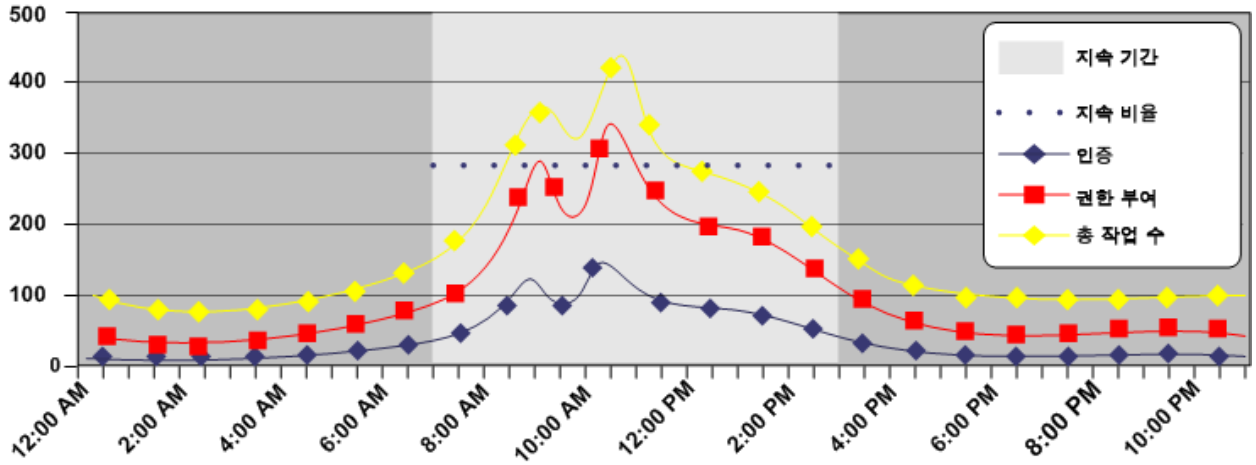
- 시스템이 평균적인 수의 작업을 처리하는 지속 기간
- 이러한 요청이 사용자 디렉터리 검색으로 변환되는 방식

지속적 사용자 디렉터리 검색 비율을 추정할 때는 일일 인증 부하 및 권한 부여를 사용하여 다음을 식별하는 것이 좋습니다.

- 하루 중 총 작업이 수행되는 비율

  **참고:** 1 시간 단위로 분할된 24 시간의 평가 기간부터 시작하는 것이 좋습니다. 하지만 엔터프라이즈의 요구 사항에 따라 하루 동안의 결과를 몇 주 또는 몇 개월 동안 비교하면 연중 사용 처리량을 더 정확하게 파악할 수 있습니다.
- 시스템이 평균적인 수의 요청을 처리하는 지속 기간
- 지속 기간 동안 발생하는 대략적인 요청 수

다음 그림은 이러한 메트릭의 예입니다.




## 사례: 지속적 사용자 디렉터리 검색 비율 추정

회사에서 다음을 확인했습니다.

- 응용 프로그램에 대한 일별 인증 부하 및 권한 부여 부하로 인해 약 888,000 개의 총 작업이 발생합니다.
- 총 작업은 약 2,051,520 개의 사용자 디렉터리 요청으로 이어집니다.
- 시스템은 약 5 시간(오전 9 시 - 오후 2 시) 동안 지속 수준에서 작동합니다.
- 지속 수준 중 시간당 약 84,000 개의 작업이 발생합니다.
- 이 시간 동안 약 420,000(84,000 * 5)개의 작업 또는 총 작업의 48 %(420,000 / 880,000)가 수행됩니다.

회사는 다음 공식을 사용하여 지속적 사용자 저장소 검색 비율을 추정합니다.

(*total_user_directory_requests* * *percentage_of_requests*) / *number_of_hours* / 3600 = *sustained_user_directory_search_rate*

***total_user_directory_requests***

정책 서버가 인증 및 권한 부여 요청을 처리하기 위해 사용자 디렉터리에 수행하는 일별 요청 수를 나타냅니다.

***percentage_of_requests***

시스템이 지속 수준에서 작동할 때 발생하는 총 작업의 백분율을 나타냅니다.

***number_of_hours***

시스템이 지속적 비율로 작동하는 시간을 나타냅니다.

***sustained_user_directory_search_rate***

정책 서버가 지속적 작업 비율을 유지하기 위해 사용자 디렉터리에 수행하는 초당 요청 수를 나타냅니다.

**결과:** (2,051,520 * 0.48) / 5 /3600 = 초당 54.7 개의 사용자 디렉터리 요청 수

정책 서버는 지속적 작동 수준 도중 인증 및 권한 부여 요청을 처리하기 위해 사용자 디렉터리에 대해 초당 54.7 회의 요청을 생성합니다.

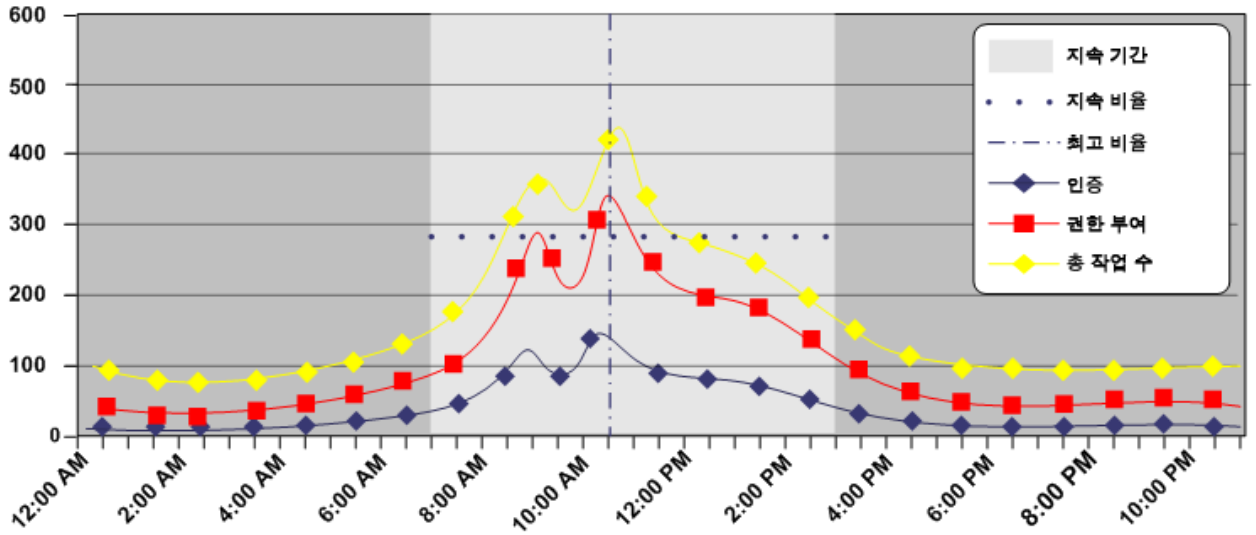
## 최고 사용자 디렉터리 검색 비율 추정

최고 사용자 디렉터리 검색 비율은 총 작업 수(인증 부하 더하기 권한 부여 부하), 즉 시스템이 최고 수준에서 작동하는 시기와 비율을 기반으로 합니다. 최고 사용자 디렉터리 검색 비율을 추정할 때는 시스템이 최고 수준의 작업을 처리하는 시기와 이러한 요청이 사용자 디렉터리 검색으로 이어지는 방식을 식별해야 합니다.

최고 권한 부여 비율을 추정할 때는 지속 권한 부여 비율을 확인할 때 수집한 메트릭을 사용하여 다음을 파악하는 것이 좋습니다.

- 시스템이 가장 높은 수의 작업을 처리하는 시간
- 이 기간 중 발생하는 대략적인 작업의 수

다음 그림은 이러한 메트릭의 예입니다.



## 사례: 최고 사용자 디렉터리 검색 비율 추정

회사에서는 응용 프로그램의 일별 총 작업 수가 888,000 개인 것으로 확인했습니다. 이 작업은 약 2,051,520 개의 사용자 디렉터리 검색으로 이어집니다. 용량 계획 수립 중 수집된 메트릭을 사용하여 회사는 업무 시간 1 시간 동안 약 278,000 개의 작업 또는 총 작업의 31 %가 수행되는 것으로 확인했습니다.

회사는 다음 공식을 사용하여 최고 사용자 저장소 검색 비율을 추정합니다.

(*total_user_directory_requests* * *percentage_of_requests*) / *number_of_hours* / 3600 = *peak_authentication_request_rate*

***total_authentication_requests***

정책 서버가 사용자 저장소로 보내는 총 요청 수를 나타냅니다.

***percentage_of_requests***

시스템이 최고 수준에서 작동할 때 발생하는 작업의 백분율을 나타냅니다.

***number_of_hours***

시스템이 최고 수준에서 작동하는 시간을 나타냅니다.

***peak_user_directory_request_rate***

정책 서버가 최고 인증 비율을 유지하기 위해 사용자 저장소에 수행하는 초당 요청 수를 나타냅니다.

**결과:** (2,051,520 * 0.31) / 1 / 3600 = 초당 176.6 회의 요청

정책 서버는 최고 작업 수준에서 인증 및 권한 부여 요청을 처리하기 위해 사용자 디렉터리에 대해 초당 176.6 회의 요청을 생성합니다.

## 사용자 저장소 용량 계획

정책 서버는 일련의 서비스를 수행하여 웹 서비스 요청 메시지를 인증하고 권한을 부여합니다. 이러한 서비스의 결과로 사용자 디렉터리에 대한 여러 개의 읽기 및 쓰기가 발생하며 이를 통칭하여 요청이라고 합니다. 지속적 작업 및 최고 작업 기간 중 사용자 디렉터리가 이러한 작업 부하를 처리할 수 있는지 여부를 파악하면 eTrust SOA Security Manager 성능에 큰 도움이 됩니다.

eTrust SOA Security Manager 의 성능에 영향을 미치는 일반적인 요소는 다음과 같습니다.

- 총 웹 서비스 요청 수 및 지속적 사용자 디렉터리 검색 비율 - 정책 서버는 수신되는 각 웹 서비스 요청에 대해 인증 및 권한 부여 작업을 처리해야 합니다. 이러한 요청이 발생하는 비율은 업무일 동안 크게 변동할 수 있습니다.

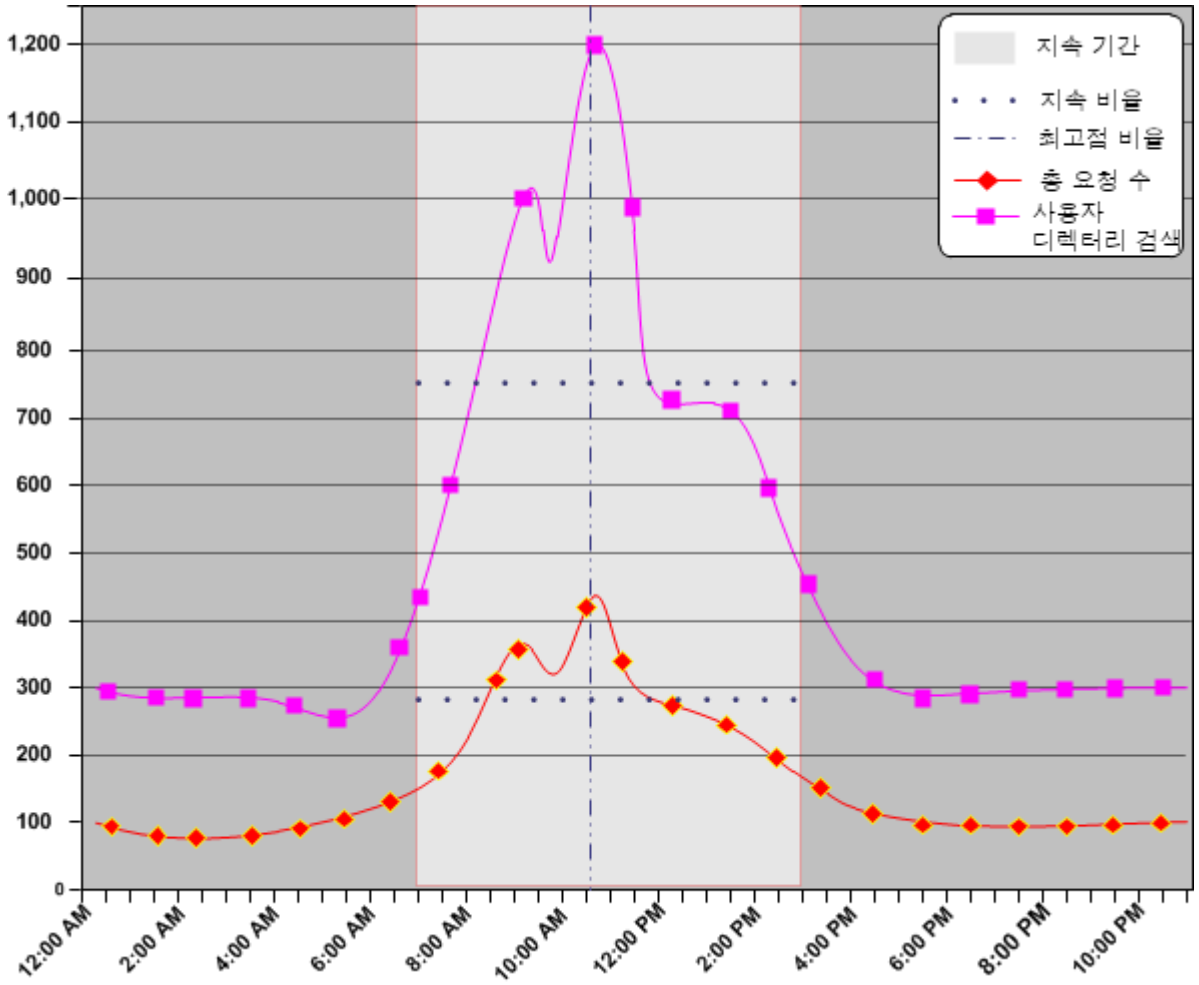
  이에 따라 정책 서버가 작업을 처리하기 위해 사용자 디렉터리 요청을 생성하는 속도가 변동합니다. 어떤 기간에는 비교적 적은 수의 사용자 디렉터리 요청이 생성되지만 다른 기간에는 더 많은 수가 생성됩니다.

  지속적 사용자 디렉터리 검색 비율은 정책 서버가 평균적인 숫자의 작업을 처리하기 위해 평균적인 숫자의 사용자 디렉터리 요청을 생성하는 기간을 나타냅니다.

- 총 요청 및 최고 사용자 디렉터리 검색 비율 - 지속적 활동 기간 중에 웹 서비스 요청 활동이 급증할 수 있습니다. 최고 사용자 디렉터리 검색 비율은 정책 서버가 최고 인증 및 권한 부여 작업 수를 처리하기 위해 가장 높은 수의 사용자 디렉터리 요청을 생성하는 기간을 나타냅니다.

다음 그림은 다음 사항을 보여 줍니다.

- 총 요청과 사용자 디렉터리 검색 비율 간의 관계
- 각 비율이 하루 동안 변동하는 상황, 특정 기간 동안 지속되는 상황 및 해당 기간 중 최고 비율을 나타내는 상황




사용자 디렉터리가 작동해야 하는 부하를 추정할 때는 다음 지침을 사용하는 것이 좋습니다. 부하를 추정한 후에는 표준 도구를 사용하여 디렉터리에 부하를 생성하고 그 결과를 추적할 수 있습니다.

**참고:** 여러 요소로 인해 필요한 수치를 달성하지 못할 수 있습니다. 조정 지침은 해당 공급업체의 설명서를 참조하십시오.

**추가 정보:**

정책 서버 (페이지 14)
지속적 요청 비율을 추정하는 방법 (페이지 121)

## 사용자 저장소 용량 계획 검사 목록

웹 서비스 요청을 처리하기 위해 정책 서버가 수행해야 하는 사용자 디렉터리 요청의 수를 추정하려면 특정 정보가 필요합니다. 사용자 저장소 용량 계획을 시작하기 전에 다음 정보를 수집하십시오.

- 웹 서비스에 대한 일별 총 웹 서비스 요청 수(요청 부하)
- 웹 서비스 클라이언트가 웹 서비스에 요청을 보내는 지속적 기간 및 최고 기간
- 활성화된 정책의 총 숫자. 각 SiteMinder 정책에 대해 다음을 확인하십시오.
  - 정책 구성원 자격 필터로 인해 하나 이상의 사용자 디렉터리 검색이 수행되는지 여부
  - 정책에 바인딩된 응답으로 인해 하나 이상의 사용자 디렉터리 검색이 수행되는지 여부

**추가 정보:**

SiteMinder 정책 구성원 자격 및 권한 부여 성능 (페이지 186)
용량 계획 소개 (페이지 119)

## 지속적 사용자 디렉터리 검색 비율을 추정하는 방법

지속적 사용자 디렉터리 검색 비율을 추정하려면 다음을 확인해야 합니다.

- 업무일 중 총 사용자 디렉터리 요청 수의 변동
- 사용자 디렉터리 요청이 지속 기간 동안 초당 요청 수로 해석되는 방식

지속적 사용자 디렉터리 검색 비율을 추정하려면 다음 단계를 완료하십시오.

1. 인증 지침을 사용하여 인증 부하가 생성하는 사용자 디렉터리 요청의 수를 추정합니다.
2. 권한 부여 지침을 사용하여 권한 부여 부하가 생성하는 사용자 디렉터리 요청의 수를 추정합니다.
3. 지속적 사용자 디렉터리 검색 비율을 추정합니다.

## 인증 지침을 사용하여 디렉터리 검색 추정

정책 서버는 각 인증 요청을 처리하기 위해 많은 수의 사용자 디렉터리 요청을 생성합니다. 사용자 디렉터리 요청 중 일부는 필요하지만 다른 일부는 회피할 수 있습니다.

다음 지침을 사용하여 각 인증으로 인해 생성되는 정책 서버 요청 수를 추정하십시오.

(필수) 각 사용자를 인증하기 위한 두 개의 검색:

- 사용자를 식별하기 위한 저장소당 하나의 검색/쿼리
- 사용자 자격 증명을 확인하기 위한 하나의 검색/쿼리

(선택 사항) 정책 설계 방식에 따라 추가 검색이 필요할 수 있습니다.

- 사용자가 인증될 때 수행되는 규칙(OnAuth 규칙)에 바인딩된 각 SiteMinder 정책에 대한 하나의 검색/쿼리

  **참고:** 규칙 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오. 규칙과 SiteMinder 정책 간의 관계에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

- 사용자 특성을 반환하는 응답에 바인딩된 각 SiteMinder 정책마다 하나의 검색/쿼리

  **참고:** 응답 및 응답과 규칙의 관계에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

## 권한 부여 지침을 사용하여 디렉터리 검색 추정

정책 서버는 사용자에게 권한을 부여하기 위해 몇 개의 사용자 디렉터리 요청을 수행합니다. 어떤 사용자 디렉터리 요청은 SiteMinder 정책 구성원 자격을 확인하기 위해 필요하지만 다른 요청은 SiteMinder 정책 설계에 따라 다릅니다. 다음 지침을 사용하면 각 권한 부여로 인해 생성되는 정책 서버 요청 수를 추정할 수 있습니다.

- 응용 프로그램 또는 정책 도메인의 각 SiteMinder 정책마다 하나의 검색/쿼리

  **참고:** 이 지침은 구성원 자격 필터의 결과로 하나 이상의 사용자 디렉터리 요청이 생성되는 정책에만 적용됩니다. SiteMinder 정책 구성원 자격과 사용자 디렉터리 요청의 관계에 대한 자세한 내용은 "Policy Membership and Authorization Requests"(정책 구성원 자격 및 권한 부여 요청)을 참조하십시오.

- 사용자 특성을 반환하는 응답에 바인딩된 각 SiteMinder 정책마다 하나의 검색/쿼리

  **참고:** 응답과 사용자 디렉터리 요청의 관계에 대한 자세한 내용은 "응답 및 권한 부여 성능"을 참조하십시오.

**참고:** 사용자 권한 부여 캐시를 통해 사용자 디렉터리에 대한 권한 부여 관련 요청의 수를 크게 줄일 수 있습니다.

**추가 정보:**

사용자 권한 부여 캐시 (페이지 187)

## 지속적 사용자 디렉터리 검색 비율 추정

지속적 사용자 디렉터리 검색 비율은 총 작업 수(인증 부하 더하기 권한 부여 부하), 즉 이러한 요청이 발생하는 시기와 비율을 기반으로 합니다. 이러한 요청이 업무일 동안 균등하게 분산될 가능성은 거의 없습니다. 대신 이러한 요청이 발생하는 비율은 지속 기간 중 가장 낮은 수준과 가장 높은(최고) 수준 내에서 크게 변동합니다.

지속적 사용자 디렉터리 검색 비율을 추정하려면 다음을 확인해야 합니다.

- 시스템이 평균적인 수의 작업을 처리하는 지속 기간
- 이러한 요청이 사용자 디렉터리 검색으로 변환되는 방식

지속적 사용자 디렉터리 검색 비율을 추정할 때는 일일 인증 부하 및 권한 부여를 사용하여 다음을 식별하는 것이 좋습니다.

- 하루 중 총 작업이 수행되는 비율

  **참고:** 1 시간 단위로 분할된 24 시간의 평가 기간부터 시작하는 것이 좋습니다. 하지만 엔터프라이즈의 요구 사항에 따라 하루 동안의 결과를 몇 주 또는 몇 개월 동안 비교하면 연중 사용 처리량을 더 정확하게 파악할 수 있습니다.
- 시스템이 평균적인 수의 요청을 처리하는 지속 기간
- 지속 기간 동안 발생하는 대략적인 요청 수

## 사례: 지속적 사용자 디렉터리 검색 비율 추정

회사에서 다음을 확인했습니다.

- 응용 프로그램에 대한 일별 인증 부하 및 권한 부여 부하로 인해 약 888,000 개의 총 작업이 발생합니다.
- 총 작업은 약 2,051,520 개의 사용자 디렉터리 요청으로 이어집니다.
- 시스템은 약 5 시간(오전 9 시 - 오후 2 시) 동안 지속 수준에서 작동합니다.
- 지속 수준 중 시간당 약 84,000 개의 작업이 발생합니다.
- 이 시간 동안 약 420,000(84,000 * 5)개의 작업 또는 총 작업의 48 %(420,000 / 880,000)가 수행됩니다.

회사는 다음 공식을 사용하여 지속적 사용자 저장소 검색 비율을 추정합니다.

(*total_user_directory_requests* * *percentage_of_requests*) / *number_of_hours* / 3600 = *sustained_user_directory_search_rate*

***total_user_directory_requests***

정책 서버가 인증 및 권한 부여 요청을 처리하기 위해 사용자 디렉터리에 수행하는 일별 요청 수를 나타냅니다.

***percentage_of_requests***

시스템이 지속 수준에서 작동할 때 발생하는 총 작업의 백분율을 나타냅니다.

***number_of_hours***

시스템이 지속적 비율로 작동하는 시간을 나타냅니다.

***sustained_user_directory_search_rate***

정책 서버가 지속적 작업 비율을 유지하기 위해 사용자 디렉터리에 수행하는 초당 요청 수를 나타냅니다.

**결과:** (2,051,520 * 0.48) / 5 /3600 = 초당 54.7 개의 사용자 디렉터리 요청 수

정책 서버는 지속적 작동 수준 도중 인증 및 권한 부여 요청을 처리하기 위해 사용자 디렉터리에 대해 초당 54.7 회의 요청을 생성합니다.

## 최고 사용자 디렉터리 검색 비율 추정

최고 사용자 디렉터리 검색 비율은 총 작업 수(인증 부하 더하기 권한 부여 부하), 즉 시스템이 최고 수준에서 작동하는 시기와 비율을 기반으로 합니다. 최고 사용자 디렉터리 검색 비율을 추정할 때는 시스템이 최고 수준의 작업을 처리하는 시기와 이러한 요청이 사용자 디렉터리 검색으로 이어지는 방식을 식별해야 합니다.

최고 권한 부여 비율을 추정할 때는 지속 권한 부여 비율을 확인할 때 수집한 메트릭을 사용하여 다음을 파악하는 것이 좋습니다.

- 시스템이 가장 높은 수의 작업을 처리하는 시간
- 이 기간 중 발생하는 대략적인 작업의 수

## 사례: 최고 사용자 디렉터리 검색 비율 추정

회사에서는 응용 프로그램의 일별 총 작업 수가 888,000 개인 것으로 확인했습니다. 이 작업은 약 2,051,520 개의 사용자 디렉터리 검색으로 이어집니다. 용량 계획 수립 중 수집된 메트릭을 사용하여 회사는 업무 시간 1 시간 동안 약 278,000 개의 작업 또는 총 작업의 31 %가 수행되는 것으로 확인했습니다.

회사는 다음 공식을 사용하여 최고 사용자 저장소 검색 비율을 추정합니다.

(*total_user_directory_requests* * *percentage_of_requests*) / *number_of_hours* / 3600 = *peak_authentication_request_rate*

***total_authentication_requests***

정책 서버가 사용자 저장소로 보내는 총 요청 수를 나타냅니다.

***percentage_of_requests***

시스템이 최고 수준에서 작동할 때 발생하는 작업의 백분율을 나타냅니다.

***number_of_hours***

시스템이 최고 수준에서 작동하는 시간을 나타냅니다.

***peak_user_directory_request_rate***

정책 서버가 최고 인증 비율을 유지하기 위해 사용자 저장소에 수행하는 초당 요청 수를 나타냅니다.

**결과:** (2,051,520 * 0.31) / 1 / 3600 = 초당 176.6 회의 요청

정책 서버는 최고 작업 수준에서 인증 및 권한 부여 요청을 처리하기 위해 사용자 디렉터리에 대해 초당 176.6 회의 요청을 생성합니다.

# 정기적인 유지 관리 태스크

다음 목록에는 일반적인 SiteMinder 유지 관리를 위해 수행할 수 있는 태스크가 정리되어 있습니다. CA Services 구현 팀에서는 일반적으로 특정 환경을 기준으로 다음과 같은 태스크에 대한 세부 사항을 다룹니다.

- 운영 체제 패치 적용

  **빈도:** 매월 또는 필요 시

- SiteMinder 누적 패치 적용

  **빈도:** 매월 또는 필요 시

- SiteMinder OneView Monitor, CA Wily 또는 유사 도구를 사용하여 SiteMinder 성능 모니터링

  **빈도:** 지속적

- 백엔드 리포지토리 성능 모니터링

  **빈도:** 지속적

- 네이티브 또는 SiteMinder 도구를 사용하여 백엔드 리포지토리 백업

  **빈도:** 조직의 요구 사항에 따라 다름

- 네이티브 도구를 사용하여 백엔드 리포지토리 유지 관리 이러한 유지 관리의 예로는 다음과 같은 항목이 포함됩니다.
  - 인덱싱
  - 트랜잭션 로그를 백업하여 디스크 공간 사용 절감

  **빈도:** 조직의 요구 사항에 따라 다름

- XPSSweeper 유틸리티를 실행하여 정책 저장소에서 삭제된 개체의 삭제 표시 제거

  **빈도:** 24 시간마다. 이 일정을 사용하면 정책 저장소의 크기를 줄일 수 있습니다.

- SiteMinder 로그 파일 보관

  **빈도:** 조직의 요구 사항에 따라 다름

- SiteMinder 정책 감사 및 필요한 경우 조정/최적화

  **빈도:** 조직의 요구 사항에 따라 다름

- 인증 및 권한 부여 오류 감사 필요한 경우 이벤트 에스컬레이션

  **빈도:** 지속적

# 제 9 장: 구현 문제 진단

이 섹션은 다음 항목을 포함하고 있습니다.



## 문제 진단 소개

SiteMinder 구현 도중 발생할 수 있는 문제는 다양하며 환경마다 서로 다릅니다. 문제는 환경의 전반적인 성능에 대한 개별 구성 요소의 배포와 관련될 수 있습니다.

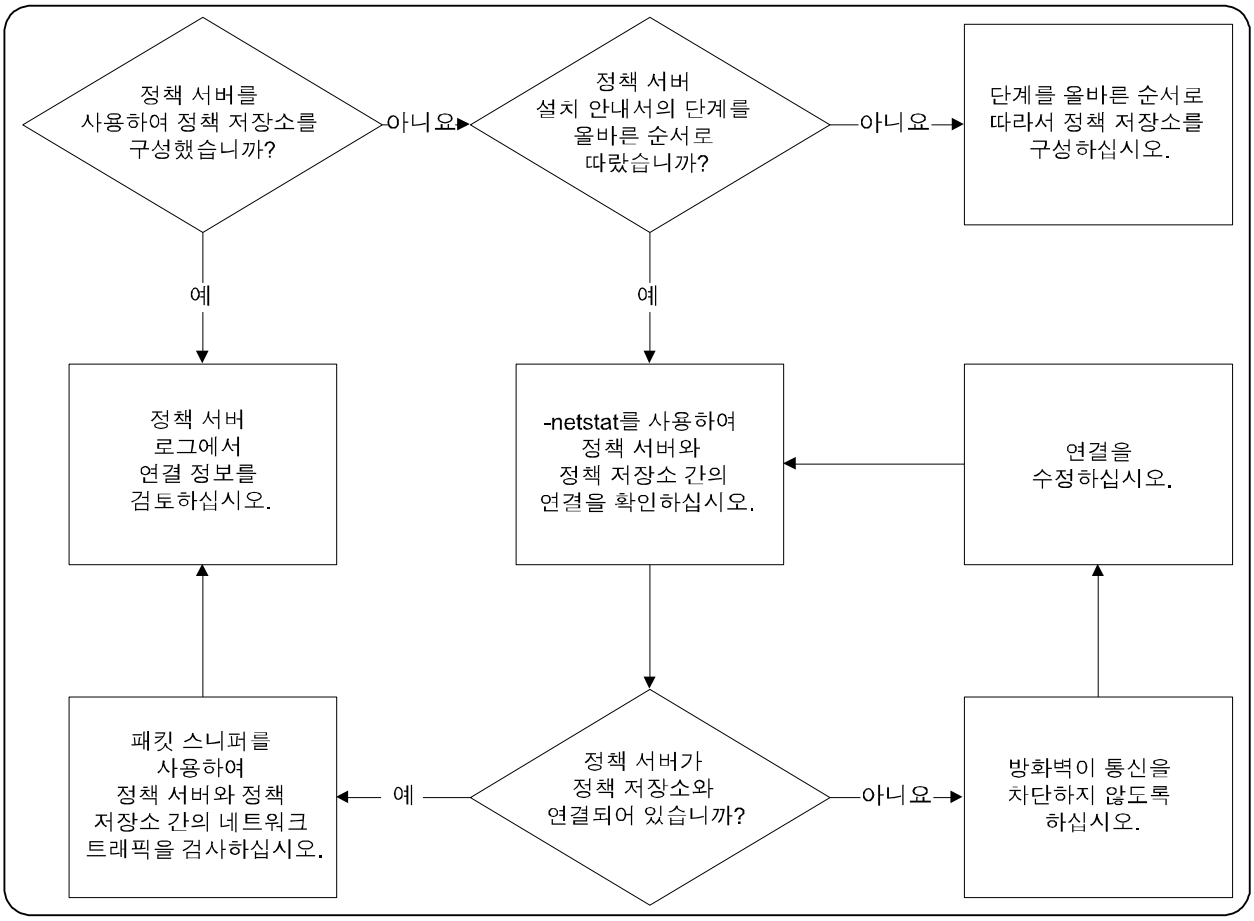
이어지는 단원에서 다루는 내용은 다음과 같습니다.

- 일반적인 구현 문제를 진단하는 방법
- 문제를 효과적으로 해결하기 위해 지원 팀과 협조하는 방법
- 문제 해결에 도움이 되는 추가 SiteMinder 설명서를 찾는 위치
- SiteMinder 성능 측정에 사용할 수 있는 몇 가지 도구

# 정책 서버/정책 저장소 연결 문제

정책 서버와 적절하게 구성된 정책 저장소를 연결할 때 다양한 문제가 연관됩니다. 이러한 문제의 범위는 올바르지 않게 구성된 정책 저장소에서 네트워크 및 데이터베이스 연결에 이르기까지 다양합니다.

다음 순서도를 사용하여 문제를 진단하십시오.




다음 사항을 고려하십시오.

- 정책 서버 호스트 시스템에서 패킷 스니퍼를 사용하면 정책 서버가 정책 서버에 보내는 오류 메시지를 기록할 수 있습니다. 연결 요청에 연결이 거부되었다는 오류 메시지가 포함되어 있으면 정책 저장소 역할을 하는 데이터베이스 또는 디렉터리 서버가 연결을 차단합니다.

- 정책 서버 로그를 검토하면 정책 서버가 시도 중인 연결에 대한 정보를 식별할 수 있습니다. 연결이 실패하는 일반적인 원인에는 다음이 포함됩니다.
  - 정책 서버가 올바르지 않은 관리자 자격 증명을 사용하여 정책 저장소에 액세스합니다.
  - 정책 서버가 사용 중인 관리자 계정에 읽기 액세스 권한이 없습니다.

  **참고:** 정책 서버 로그는 *siteminder_home*/log 에 있습니다.

  ***siteminder_home***

  정책 서버 설치 위치를 지정합니다.

# 지원 팀과 함께 작업

SiteMinder 지원 팀의 지원이 필요한 경우 지원 티켓을 열 때 수집하고 포함할 수 있는 정보가 있습니다. 최대한 많은 정보를 포함하면 지원 팀에서 문제 해결 시간을 단축하는 데 도움이 됩니다.

## 환경 정보

다음 정보를 최대한 많이 수집하여 지원 티켓을 열 때 이를 포함하십시오.

- 정책 서버가 설치된 운영 체제(서비스 팩 수준 포함)

  **예:** Windows 2008 SP2
- SiteMinder 에이전트가 설치된 웹 서버

  **예:** Windows 2008 SP2, IIS 7.0
- 정책 서버의 버전(서비스 팩 및 누적 릴리스(CR) 포함)

  **예:** r12.0 SP2 CR1
- 정책 서버와 통신하는 SiteMinder 에이전트의 버전(서비스 팩 및 CR 포함)

  **예:** r12.0 SP2 CR1
- 정책 저장소 유형(LDAP/ODBC) 및 특정 공급업체와 버전

  **예:** Oracle 10g R2
- 다른 SiteMinder 데이터 저장소의 특정 공급업체 및 버전

- 적용 가능한 경우 SiteMinder 와 통합된 다른 모든 CA 제품 또는 타사 제품
- 환경에 배포된 모든 사용자 지정 코드 또는 타사 인증 체계. 사용자 지정 코드에는 GSE(Global Solutions Engineering)에서 제공하는 코드 또는 각 조직에서 개발한 코드가 포함됩니다.
- SiteMinder 구성 요소 업그레이드 또는 새 하드웨어 등과 같이 환경에서 최근 수행된 모든 변경 내용
- 문제가 시작된 시기

**참고:** SiteMinder Platform Support Matrix(SiteMinder 플랫폼 지원표)를 사용하여 문제가 SiteMinder 에서 지원하지 않는 타사 제품 또는 운영 체제에 관련되지 않음을 확인할 수 있습니다. 자세한 내용은 SiteMinder Platform Support Matrix(SiteMinder 플랫폼 지원표)를 참조하십시오.

## 로그 파일

발생한 문제에 따라 지원 팀에서는 다음 로그 파일 중 하나 이상을 요청할 수 있습니다.

| 구성 요소 | 파일 |
|---|---|
| 정책 서버 | ■ 정책 서버 로그(smps.log)<br>■ 정책 서버 프로파일러 로그(smtracedefault.log)<br>■ 감사 로그(smaccess.log) |
| 웹 에이전트 | ■ 웹 에이전트 로그<br>■ 웹 에이전트 추적 로그<br>■ 웹 서버 오류 로그<br>■ 웹 서버 액세스 로그 |
| WSS 에이전트 | ■ WSS 에이전트 로그<br>■ XML 처리 메시지 로그<br>■ 웹 에이전트 추적 로그(웹 서버용 WSS 에이전트만 해당)<br>■ 응용 프로그램 서버 또는 웹 서버 오류 로그<br>■ 응용 프로그램 서버 또는 웹 서버 액세스 로그 |

다음 사항을 고려하십시오.

- 모든 정책 서버 로그는 *ps_home*\log 에 있습니다.

  ***ps_home***

  정책 서버 설치 경로를 지정합니다.

  **참고:** 정책 서버 프로파일러 구성에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오. 감사에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.

- 웹 및 WSS 에이전트 로그에는 기본 위치 또는 기본 이름이 없습니다.

  **참고:** 웹 에이전트 로깅 구성에 대한 자세한 내용은 *웹 에이전트 구성 안내서*를 참조하십시오. WSS 에이전트 로깅 구성에 대한 자세한 내용은 해당하는 WSS 에이전트 안내서를 참조하십시오.

## 정책 서버 중단

다음 목록은 정책 서버가 중단된 경우 지원 팀이 추가적인 상세 정보를 검색하는 데 도움이 되는 정보입니다. 이 정보가 있어야 지원 티켓을 열 수 있는 것은 아니지만 지원 팀에서 요청할 가능성이 많은 정보입니다. 이 정보를 초기에 제공하면 지원 팀의 문제 해결 시간을 단축할 수 있습니다.

1. 환경 정보를 제공합니다.
2. 문제를 가능한 한 자세하게 설명합니다. 예를 들면 다음과 같습니다.
   - 프로세스가 중단되는 빈도
   - 중단이 발생한 횟수
   - 중단될 때 서버에서 발생한 상황에 대한 설명
   - 중단을 재현하는 단계
3. UNIX 코어 파일 또는 Windows 덤프 파일을 첨부합니다. 이러한 파일을 첨부할 때는 다음 사항을 고려하십시오.
   - (UNIX) 가능한 경우 패키지된 코어를 제공하십시오.
   - (Windows) 이 파일이 프로그램 오류 디버깅 도구에서 생성된 미니 덤프가 아니라 전체 덤프인지 확인하십시오.
4. 정책 저장소 데이터를 첨부합니다.
5. 정책 서버 로그 및 정책 서버 감사 로그를 첨부합니다.

6. 정책 서버 추적 로그 출력을 수정합니다.
7. 정책 서버 프로파일러 로그를 첨부합니다.

   **참고:** 로그 파일을 첨부하려는 경우 해당 파일이 모두 일치하는지 확인하십시오. 또한 모든 파일의 실행된 시간이 동일해야 합니다.

**추가 정보:**

환경 정보 (페이지 221)
로그 파일 (페이지 222)

## 정책 저장소 데이터 첨부

정책 저장소 데이터를 검사하면 지원 팀에서 문제를 식별하기가 더 쉬워집니다. 정책 저장소를 내보내고 SiteMinder 데이터 정보 파일(smdif)을 티켓에 첨부합니다.

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

## 정책 서버 추적 로그 수정

정책 서버 추적 로그를 검사하면 지원 팀에서 문제를 식별하기가 더 쉬워집니다. 정책 서버가 중단된 경우 정책 서버 프로파일러를 사용하여 문제를 캡처할 수 있습니다.

**참고:** 정책 서버가 중지된 경우에는 문제를 캡처하지 못할 수도 있습니다. 이 경우에는 정책 서버 프로파일러를 사용하는 대신 코어 덤프를 수행하십시오.

정책 서버 프로파일러는 기본 구성 파일을 사용하여 정책 서버 작업을 추적 로그에 기록합니다. 기본 설정에는 구성 요소 및 데이터에 대한 정보가 포함됩니다.

- 구성 요소는 정책 서버가 실행하는 작업의 논리적 그룹을 나타냅니다.
- 데이터는 정책 서버가 추적해야 하는 실제 데이터를 나타냅니다.

SiteMinder 지원 팀은 기본 구성 파일에 포함되지 않은 구성 요소와 데이터 설정을 사용하여 문제 해결 프로세스를 시작합니다. 정책 서버 추적 로그를 제출하기 전에 기본 설정을 수정하십시오.

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

### 예: 수정된 구성 요소

기본 추적 구성을 수정하여 다음 구성 요소를 포함합니다.

- 서버

  서버 구성 요소에는 추가적인 하위 구성 요소가 포함됩니다. 서버 구성 요소를 추가한 후에는 다음 하위 구성 요소를 제거하십시오.

  - Policy_Object
  - Policy_Object_Cache
  - Administration
  - Audit_Logging
- Tunnel_Service
- JavaAPI

### 예: 수정된 데이터 형식

기본 추적 구성을 수정하여 다음 데이터 형식을 포함합니다.

**중요!** 데이터 형식이 나열되는 순서에 따라 데이터가 로그되는 순서가 결정됩니다. 데이터 형식을 다음 순서로 나열하십시오.

- Date
- Time
- Precise Time
- Pid
- Tid
- SrcFile
- Function
- AgentName
- TransactionName

- TransactionID
- Resource
- Realm
- Rule
- Domain
- Group
- Policy
- User
- Directory
- AgentType
- ReturnValue
- ErrorString
- ErrorValue
- AuthStatus
- AuthReason
- AuthScheme
- ClusterID
- RequestIPAddr
- Returns
- Result
- Message

## 에이전트 중단

다음 목록은 에이전트가 중단된 경우 지원 팀에서 추가적인 상세 정보를 검색하는 데 도움이 되는 정보입니다. 이 정보가 있어야 지원 티켓을 열 수 있는 것은 아니지만 지원 팀에서 요청할 가능성이 많은 정보입니다. 이 정보를 초기에 제공하면 지원 팀의 문제 해결 시간을 단축할 수 있습니다.

1. 환경 정보를 수집합니다.
2. 문제를 가능한 한 자세하게 설명합니다. 예를 들면 다음과 같습니다.
   - 프로세스가 중단되는 빈도
   - 중단이 발생한 횟수
   - 중단될 때 서버에서 발생한 상황에 대한 설명
   - 중단을 재현하는 단계
3. UNIX 코어 파일 또는 Windows 덤프 파일을 첨부합니다. 이러한 파일을 첨부할 때는 다음 사항을 고려하십시오.
   - (UNIX) 가능한 경우 패키지된 코어를 제공하십시오.
   - (Windows) 이 파일이 프로그램 오류 디버깅 도구에서 생성된 미니 덤프가 아니라 전체 덤프 파일인지 확인하십시오.
4. 에이전트 로그와 웹 또는 응용 프로그램 서버 오류 로그를 첨부합니다.

   **참고:** 로그 파일을 첨부하려는 경우 해당 파일이 모두 일치하는지 확인하십시오. 또한 모든 파일의 실행된 시간이 동일해야 합니다.
5. 웹 서버 바이너리 디렉터리의 tar 또는 zip 을 첨부합니다.

   **참고:** IIS 웹 서버에서 실행 중인 에이전트에는 이 단계가 적용되지 않습니다.
6. 웹 서버용 웹 에이전트 또는 WSS 에이전트의 경우 웹 에이전트 추적 로그와 웹 서버 액세스 로그를 첨부합니다.

**추가 정보:**

환경 정보 (페이지 221)
로그 파일 (페이지 222)

## 리소스 누수

다음은 메모리, 파일 핸들, 네트워크 연결, 소켓 또는 디스크 공간과 같은 시스템 리소스가 릴리스되지 않는 경우 지원 팀이 추가적인 상세 정보를 검색하는 데 도움이 되는 정보의 목록입니다. 이 정보가 있어야 지원 티켓을 열 수 있는 것은 아니지만 지원 팀에서 요청할 가능성이 많은 정보입니다. 이 정보를 초기에 제공하면 지원 팀의 문제 해결 시간을 단축할 수 있습니다.

1. 환경 정보를 수집합니다.
2. 문제를 가능한 한 자세하게 설명합니다. 최소한 다음을 포함하십시오.
   - 리소스 누수의 빈도.
   - 리소스 누수의 크기. prstat 와 같이 리소스 할당을 보여줄 수 있는 도구를 사용하여 일정한 시간 동안 리소스 누수를 측정하십시오.
   - 리소스 누수를 측정하는 데 사용한 도구
   - 리소스 누수가 시스템에 미치는 영향

     **예:** 시스템 중단 또는 중지
   - 리소스 누수를 재현하는 단계 또는 응용 프로그램 트래픽에 기반한 재현 테스트
3. 로그를 첨부합니다.
   - (정책 서버) 정책 서버 문제가 발생한 경우 정책 서버 로그 및 정책 서버 감사 로그를 첨부합니다.
   - (SiteMinder 에이전트) 에이전트 문제가 발생한 경우 에이전트 로그 및 웹 서버 또는 응용 프로그램 서버 오류 로그를 첨부합니다.

   **참고:** 로그 파일을 첨부하려는 경우 해당 파일이 모두 일치하는지 확인하십시오. 또한 모든 파일의 실행된 시간이 동일해야 합니다.

**추가 정보:**

환경 정보 (페이지 221)
로그 파일 (페이지 222)

# 기능 문제

기능 문제는 SiteMinder 가 설명서에 명시된 대로 수행되지 않는 문제라고 정의할 수 있습니다. 다음은 기능 문제가 발생하는 경우 지원 팀이 추가적인 상세 정보를 검색하는 데 도움이 되는 정보의 목록입니다. 이 정보가 있어야 지원 티켓을 열 수 있는 것은 아니지만 지원 팀에서 요청할 가능성이 많은 정보입니다. 이 정보를 초기에 제공하면 지원 팀의 문제 해결 시간을 단축할 수 있습니다.

1. 환경 정보를 수집합니다.
2. 문제를 재현하는 단계를 포함하여 문제를 가능한 한 자세히 설명합니다.
3. 로그를 첨부합니다.
   - (정책 서버) 정책 서버 문제가 발생한 경우 정책 서버 로그 및 정책 서버 감사 로그를 첨부합니다.
   - (SiteMinder 에이전트) 에이전트 문제가 발생한 경우 에이전트 로그 및 해당 웹 서버 또는 응용 프로그램 서버 오류 로그를 첨부합니다.

   **참고:** 로그 파일을 첨부하려는 경우 해당 파일이 모두 일치하는지 확인하십시오. 또한 모든 파일의 실행된 시간이 동일해야 합니다.
4. 정책 저장소를 SiteMinder 데이터 정보 파일(smdif)로 내보내고 파일을 첨부합니다.

   **참고:** 정책 저장소 내보내기에 대한 자세한 내용은 *정책 서버 관리 안내서*를 참조하십시오.
5. 로그를 첨부합니다.
   - (정책 서버) 정책 서버 문제가 발생하는 경우 정책 서버 프로파일러 로그를 첨부합니다.
   - (SiteMinder 에이전트) 에이전트 문제가 발생한 경우 모든 에이전트 로그 및 웹 서버 또는 응용 프로그램 서버 액세스 로그를 첨부합니다.

**추가 정보:**

환경 정보 (페이지 221)
로그 파일 (페이지 222)

## 임의 문제

임의 문제는 산발적으로 발생하며 기능적 특성이 있지만 재현 가능한 패턴이 없는 문제라고 정의됩니다. 다음은 임의 문제가 발생하는 경우 지원 팀이 추가적인 상세 정보를 검색하는 데 도움이 되는 정보의 목록입니다. 이 정보가 있어야 지원 티켓을 열 수 있는 것은 아니지만 지원 팀에서 요청할 가능성이 많은 정보입니다. 이 정보를 초기에 제공하면 지원 팀의 문제 해결 시간을 단축할 수 있습니다.

1. 환경 정보를 수집합니다.
2. 문제를 가능한 한 자세하게 설명합니다. 예를 들면 다음과 같습니다.
   - 문제가 시작된 시점
   - 문제의 빈도
   - 문제가 시스템에 미치는 영향

     **예:** 트랜잭션이 평소보다 오래 걸립니다.
3. 로그를 첨부합니다.
   - (정책 서버) 정책 서버 문제가 발생하는 경우:
     - 실패 시점 정책 서버 로그, 실패 시점 정책 서버 감사 로그 및 실패 시점 정책 서버 프로파일러 로그를 첨부합니다.
     - 시스템이 정상 작동할 때의 정책 서버 프로파일러 로그를 첨부합니다.
   - (SiteMinder 에이전트) 에이전트 문제가 발생하는 경우:
     - 실패 시점의 모든 에이전트 로그를 첨부합니다.
     - 시스템이 정상 작동할 때의 모든 에이전트 로그를 첨부합니다.

   **참고:** 로그 파일을 첨부하려는 경우 해당 파일이 모두 일치하는지 확인하십시오. 또한 모든 파일의 실행된 시간이 동일해야 합니다.

**추가 정보:**

환경 정보 (페이지 221)
로그 파일 (페이지 222)

# 기술 자료 문서 찾기

SiteMinder 북셸프는 사용 가능한 유일한 리소스입니다. SiteMinder 기술 자료(KB) 문서는 CA 기술 지원 사이트에 있습니다. 이 문서에서는 SiteMinder 환경의 관리 및 문제 해결에 관련된 다양한 항목을 다룹니다.

**SiteMinder KB 문서를 찾으려면**

1. 기술 지원 사이트에 로그인합니다.
2. "Support by Product"(제품별 지원)를 클릭합니다.

   "Support by Product"(제품별 지원) 페이지가 표시됩니다.
3. 제품 목록에서 SiteMinder 를 찾아 링크를 클릭합니다.

   SiteMinder 제품 페이지가 표시됩니다.
4. "Search Support"(지원 검색) 아래에서 검색 조건을 입력합니다. "Search Support"(지원 검색)는 화면 오른쪽에 있습니다.

   검색 조건에 일치하는 정보가 나타납니다.

# SiteMinder 성능 측정

SiteMinder 성능 측정은 배포의 여러 구성 요소가 어떻게 작동하는지를 반영하는 메트릭을 수집하는 반복적 프로세스입니다. 각 구성 요소 쌍 사이의 라운드트립 시간을 측정하여 성능 표준이 충족되는지 확인하고 잠재적 병목 지점을 식별하는 것이 좋습니다.

**참고:** CPU 사용량과 같은 전통적 성능 메트릭을 SiteMinder 배포 조정을 위한 유일한 결정 요소로 사용하지 않도록 하십시오. 예를 들어 정책 서버를 호스트하는 시스템은 부하가 높을 때 낮은 CPU 사용량으로 실행될 수 있지만 이것이 정책 서버가 최적 성능에 도달했음을 확인해 주는 요소는 아닙니다.

SiteMinder 성능 측정에 사용할 수 있는 도구는 다음과 같습니다.

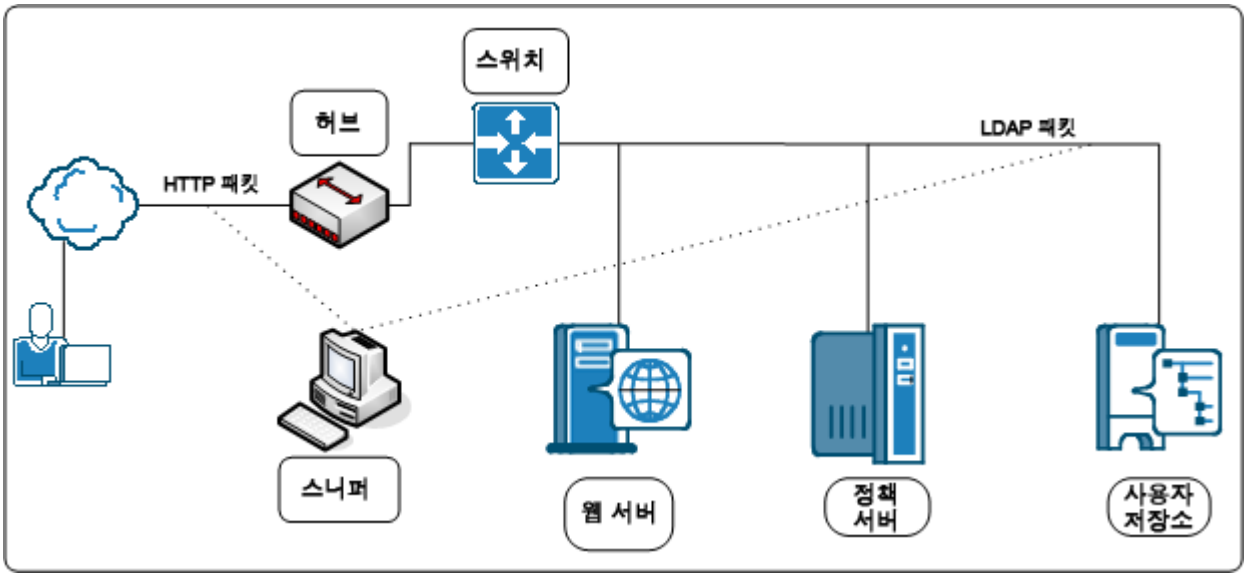
- 네트워크 스니퍼
- SiteMinder OneView 모니터
- SiteMinder 테스트 도구
- 디렉터리 서버 유틸리티 및 SQL 분석기

## 네트워크 스니퍼

타사 네트워크 스니퍼를 사용하여 테스트 결과에 영향을 주지 않고 암호화되지 않은 데이터에 대한 요청의 크기와 콘텐츠를 보여 주는 정보를 수집할 수 있습니다. 또한 스니퍼는 추가적인 패킷의 전송, 부하 분산 간의 긴 지연 시간 및 로그만으로 캡처할 수 없는 리디렉션 기술에 대한 알림도 제공할 수 있습니다.

**참고:** 네트워크가 스위칭되는 허브 구성으로 설정된 경우에는 클라이언트와 클라이언트측 허브의 서버 사이에 스니퍼를 배치하십시오.

다음 다이어그램은 표준 SiteMinder 배포의 네트워크 스니퍼를 보여 줍니다.




## SiteMinder OneView 모니터

SiteMinder OneView 모니터를 사용하여 성능 병목 지점을 식별하고 SiteMinder 배포의 리소스 사용에 대한 메트릭을 수집할 수 있습니다. 또한 OneView 모니터는 다음의 SiteMinder 구성 요소에서 작업 데이터를 수집하여 구성 요소 실패와 같은 특정 이벤트가 발생할 때 알림을 표시합니다.

- 정책 서버
- SiteMinder 에이전트

OneView 모니터는 다음과 같은 메트릭을 제공하여 SiteMinder 에이전트와 정책 서버 간의 성능 병목 지점을 식별할 수 있습니다.

- 평균 인증 시도 횟수 및 사용자 인증에 걸리는 평균 시간
- 평균 권한 부여 시도 횟수 및 사용자 권한 부여에 걸리는 평균 시간
- 캐시 적중 및 누락 수

**참고:** OneView 모니터가 제공할 수 있는 데이터 형식의 전체 목록은 *정책 서버 관리 안내서*를 참조하십시오. OneView 모니터 설치에 대한 자세한 내용은 *정책 서버 설치 안내서*를 참조하십시오.

## SiteMinder 테스트 도구

SiteMinder 테스트 도구 유틸리티를 사용하여 SiteMinder 에이전트와 정책 서버 간의 상호 작용을 테스트할 수 있습니다. 테스트 도구는 웹 에이전트를 에뮬레이션하므로 이를 사용하면 정책 서버 성능을 분리하여 파악할 수 있습니다.

테스트 도구는 다음 세 가지 유형의 테스트를 수행할 수 있습니다.

**기능 테스트**

정책이 올바르게 구성되었는지 테스트합니다.

**재발 테스트**

정책 저장소 마이그레이션 또는 새 기능 구현과 같은 변경 내용이 배포에 영향을 미치는지 여부를 테스트합니다.

**스트레스 테스트**

여러 요청을 수신할 때 정책 서버의 성능을 테스트합니다.

**참고:** 테스트 도구 유틸리티에 대한 자세한 내용은 *테스트 도구 도움말*을 참조하십시오.

## 디렉터리 서버 유틸리티 및 SQL 분석기

디렉터리 서버 유틸리티를 사용하면 디렉터리 서버 또는 데이터베이스에 대한 정책 서버 요청을 시뮬레이트하여 쿼리 지체 시간을 분리하여 파악할 수 있습니다. 또한 SQL 분석기를 사용하여 정책 서버와 사용자 디렉터리 간의 응답 시간을 분석할 수 있습니다.

# 제 10 장: 제품 통합

이 섹션은 다음 항목을 포함하고 있습니다.



## CA Arcot WebFort 및 RiskFort 통합

CA Arcot Adapter™(Adapter)를 사용하여 SiteMinder 를 CA Arcot WebFort 강력한 인증 솔루션 및 CA Arcot RiskFort 어댑티브(adaptive) 인증 솔루션의 온 프레미스 구현 환경과 통합할 수 있습니다.

시작하기 전에 다음 사항을 고려하십시오.

- 통합을 위해서는 최소 버전의 Adapter 및 CA Arcot RiskFort 가 필요합니다.
- 통합을 위해서는 최소 버전의 CA Arcot WebFort 가 필요합니다.

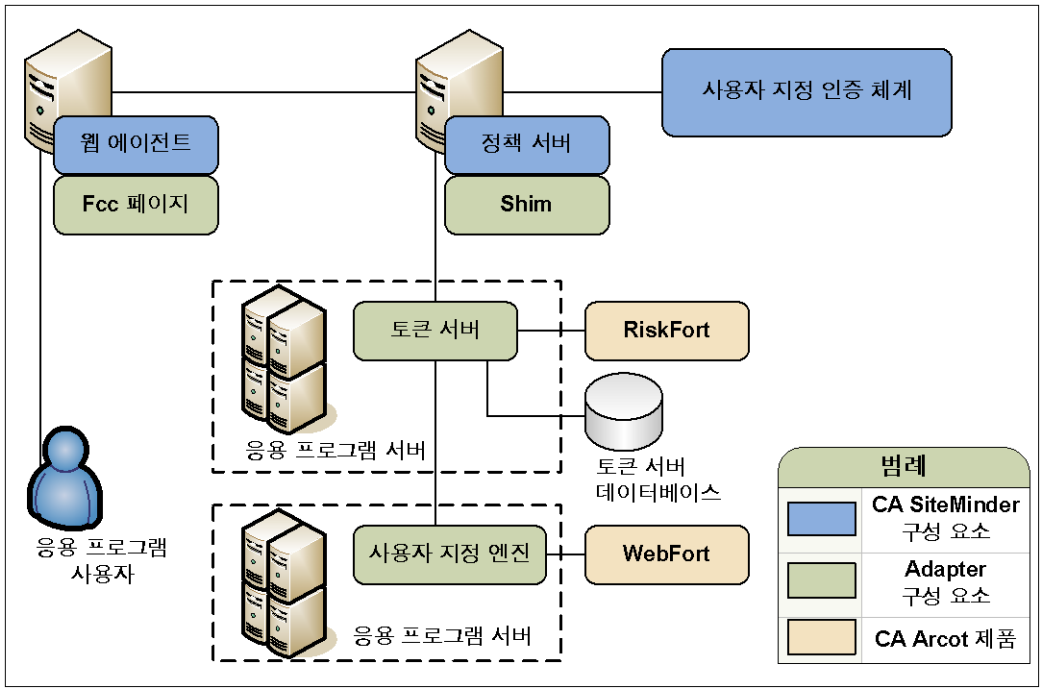
**참고:** 지원되는 버전에 대한 자세한 내용은 "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)를 참조하십시오.

다음 다이어그램의 용도는 다음과 같습니다.

- Adapter 와 그 구성 요소, CA Arcot RiskFort 및 CA Arcot WebFort 가 SiteMinder 환경에서 통합되는 방식을 보여 줍니다.
- 주요 구성 요소와 각 구성 요소의 일반적인 관계를 자세히 알려 줍니다. 이 다이어그램은 워크플로 다이어그램이 아닙니다.

**참고:** 모든 CA Arcot 구성 요소를 설치 및 구성하는 방법에 대한 자세한 내용은 CA Arcot 설명서를 참조하십시오.

*그림 3: CA SiteMinder 및 CA Arcot 통합 아키텍처*




## 온 프레미스 Arcot 통합에서의 인증

CA Arcot 는 인증(CA Arcot WebFort) 및 위험 평가(CA Arcot RiskFort) 프로세스를 안내하는 방식으로 통합 환경에서 인증 서비스를 제공합니다. 인증 프로세스는 다음과 같이 진행됩니다.

- CA Arcot WebFort 가 SiteMinder 의 보호를 받는 리소스를 요청하는 사용자의 ID 가 적합한지 확인할 수 있는 강력한 인증을 제공합니다.

  **참고:** 강력한 인증에 대한 자세한 내용은 *CA Arcot WebFort Installation and Deployment Guide*(CA Arcot WebFort 설치 및 배포 안내서)를 참조하십시오. 지원되는 인증 방법을 구성하는 방법에 대한 자세한 내용은 *CA Arcot WebFort Administration Guide*(CA Arcot WebFort 관리 안내서)를 참조하십시오.

- CA Arcot RiskFort 가 각 트랜잭션과 관련된 위험 수준을 결정하는 위험 평가를 완료하기 위해 다양한 데이터를 수집합니다.

  **참고:** 위험 평가 및 위험 점수에 대한 자세한 내용은 *CA Arcot RiskFort Installation and Deployment Guide*(CA Arcot RiskFort 설치 및 배포 안내서)를 참조하십시오. 위험 점수 부여를 구성하는 방법에 대한 자세한 내용은 *CA Arcot RiskFort Administration Guide*(CA Arcot RiskFort 관리 안내서)를 참조하십시오.

위험 평가의 결과로 위험 점수와 해당 권고 사항이 생성되는데, 이 권고 사항은 인증 허용 또는 거부와 같은 권장 작업입니다.

CA Arcot 는 권고 사항을 정책 서버에 전달하고, 정책 서버는 필요한 경우 자체의 권한 부여 서비스를 계속합니다.

**참고:** 인증 과정에서 Adapter 워크플로 및 각 CA Arcot 구성 요소의 역할에 대한 자세한 내용은 *CA Arcot Adapter for CA SiteMinder Installation and Configuration Guide*(CA Arcot Adapter for CA SiteMinder 설치 및 구성 안내서)를 참조하십시오.

## 신뢰 수준 및 SiteMinder 권한 부여

정책 서버는 통합 환경에서 권한 부여 서비스를 유지 관리하며 위험 점수를 권한 부여 결정에 적용할 수 있습니다. 위험 점수는 인증 프로세스 (페이지 236)에서 생성됩니다.

정책 서버는 위험 점수를 SiteMinder 신뢰 수준(신뢰 수준)으로 적용합니다. 신뢰 수준은 위험 점수를 기반으로 하므로, 마찬가지로 해당 트랜잭션이 안전할 가능성을 나타내는 정수로 표현됩니다.

다음과 같이 신뢰 수준을 두 가지 액세스 관리 모델에 모두 적용할 수 있습니다.

- 정책을 사용하여 리소스를 보호하는 경우 신뢰 수준을 다음 개체에 적용할 수 있습니다.
  - 정책 영역
  - 활성 정책 식

- EPM 응용 프로그램을 사용하여 리소스를 보호하는 경우 신뢰 수준을 다음 개체에 적용할 수 있습니다.
  - 응용 프로그램 구성 요소
  - SM_USER_CONFIDENCE_LEVEL SiteMinder 생성 특성을 참조하는 명명된 식으로 구성된 응용 프로그램 역할

**참고:** 신뢰 수준을 정책 영역이나 응용 프로그램 구성 요소에 적용하려면 신뢰 수준 지원을 활성화 (페이지 240)해야 합니다. 활성 정책 식 또는 응용 프로그램 역할을 사용하여 신뢰 수준을 적용하는 기능은 이전 릴리스부터 계속 지원되므로 기본적으로 활성화되어 있습니다. 신뢰 수준을 정책 및 응용 프로그램에 적용하는 방법에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

다음 예제 워크플로는 두 값 사이의 관계를 자세히 설명하고 정책 서버가 신뢰 수준을 권한 부여 결정에 적용하는 방식을 보여 줍니다.

1. 사용자가 성공적으로 인증되면 Adapter 가 아래의 대수 공식을 사용하여 위험 점수를 신뢰 수준으로 변환합니다.

   `(100 - 위험 점수) * 10 = 신뢰 수준`

2. Adapter 가 신뢰 수준을 SiteMinder 세션 티켓에 삽입합니다.

   **참고:** 세션 티켓에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

3. 사용자가 보호되는 리소스를 요청하면 정책 서버가 세션 티켓의 신뢰 수준을 정책 또는 응용 프로그램에 구성된 신뢰 수준과 비교합니다.

4. 다음 작업이 수행될 수 있습니다.

   - 정책 규칙이 액세스를 허용하도록 구성되고 사용자의 신뢰 수준이 정책 영역 또는 활성 정책 식에 구성된 신뢰 수준 이상일 경우 정책 규칙이 트리거됩니다.

     **참고:** 사용자의 신뢰 수준이 정책에 구성된 신뢰 수준보다 낮으면 SiteMinder 가 액세스를 거부합니다.

   - 정책 규칙이 액세스를 거부하도록 구성되고 사용자의 신뢰 수준이 정책 영역 또는 활성 정책 식에 구성된 값보다 낮을 경우 정책 규칙이 트리거됩니다.

- 사용자의 신뢰 수준이 응용 프로그램 역할에 구성된 신뢰 수준보다 낮을 경우 사용자가 역할 구성원 자격에서 제외되고 SiteMinder 가 액세스를 거부합니다.
- 사용자의 신뢰 수준이 응용 프로그램 구성 요소에 구성된 신뢰 수준 이상일 경우 SiteMinder 가 액세스를 허용합니다.

**추가 정보:**

정책 관리 모델 (페이지 65)

## 위험 점수와 신뢰 수준 비교

위험 점수와 신뢰 수준이 모두 트랜잭션이 안전한지 확인하는 데 도움이 되지만 두 값 사이에는 몇 가지 차이가 있습니다. 권한 부여 결정을 계획할 때는 다음과 같은 차이점을 고려하십시오.

| CA Arcot 위험 점수 | SiteMinder 신뢰 수준 |
|---|---|
| 0~100 사이의 숫자로 위험 점수가 표현됩니다. | 0~1000 사이의 숫자로 신뢰 수준이 표현됩니다. |
| 위험 점수가 낮을수록 트랜잭션이 안전할 가능성이 커집니다. | 신뢰 수준이 높을수록 트랜잭션이 안전할 가능성이 커집니다.<br>**참고:** 값이 영(0)이면 전혀 신뢰할 수 없음을 나타냅니다. 전혀 신뢰할 수 없으면 SiteMinder 가 요청된 리소스에 대한 액세스를 거부합니다. |

다음 예제 워크플로는 위험 점수와 신뢰 수준 간의 역관계를 자세히 보여 줍니다.

1. 사용자가 SiteMinder 로 보호되는 리소스를 요청하고 인증을 위해 CA Arcot 로 전달됩니다.
2. Adapter 가 인증 및 위험 분석 프로세스를 안내합니다. CA Arcot 평가와 점수 부여 규칙에 따라 사용자가 인증되고 위험 점수가 30 으로 지정됩니다. 위험 점수가 낮을수록 트랜잭션이 안전함을 의미합니다.

   **참고:** 위험 평가 및 점수 부여 규칙에 대한 자세한 내용은 *CA Arcot RiskFort Administration Guide*(CA Arcot RiskFort 관리 안내서)를 참조하십시오.
3. Adapter 가 다음을 수행합니다.
   a. 인증 결정을 정책 서버에 전달합니다.
   b. 아래의 대수 공식을 사용하여 위험 점수를 신뢰 수준으로 변환합니다.

      `(100 - 위험 점수) * 10 = 신뢰 수준`

      이 예제에서는 Adapter 가 아래의 대수 공식을 사용하여 위험 점수를 신뢰 수준으로 변환합니다.

      `(100 - 30) * 10 = 700`

      신뢰 수준이 높을수록 트랜잭션이 안전함을 의미합니다.
4. Adapter 가 신뢰 수준을 사용자의 세션 티켓에 삽입합니다.
5. 사용자가 700 이상의 신뢰 수준을 요구하는 정책 또는 응용 프로그램에 의해 보호되는 리소스를 요청합니다.
6. 정책 서버가 해당 리소스에 대한 액세스를 허용합니다.

## 권한 부여 결정에 신뢰 수준 지원 사용

필요한 경우 신뢰 수준을 권한 부여 결정에 적용할 수 있습니다. 다음 사항을 고려하십시오.

- 신뢰 수준을 다음 개체에 적용할 수 있습니다.
  - 정책 영역
  - 활성 정책 식

- 응용 프로그램 구성 요소
- SM_USER_CONFIDENCE_LEVEL SiteMinder 생성 특성을 참조하는 명명된 식을 포함하는 응용 프로그램 역할

**참고:** 신뢰 수준을 정책 및 응용 프로그램에 적용하는 방법에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

- 신뢰 수준을 영역 또는 응용 프로그램 구성 요소에 적용하려면 신뢰 수준 지원만 활성화하면 됩니다. 활성 정책 식 또는 응용 프로그램 역할을 사용하여 신뢰 수준을 적용하는 기능은 이전 릴리스부터 계속 지원되므로 기본적으로 활성화되어 있습니다.

**다음 단계를 수행하십시오.**

1. SiteMinder 환경에서 정책 서버 호스트 시스템에 로그인합니다.
2. XPSConfig 유틸리티를 시작합니다.

   XPSConfig 에서 옵션을 묻는 메시지를 표시합니다.
3. SM 을 입력하고 Enter 키를 누릅니다.

   XPSConfig 에서 옵션을 묻는 메시지를 표시합니다.
4. 15 를 입력하고 Enter 키를 누릅니다.

   ConfidenceLevelSupportEnabled 매개 변수가 나타납니다.
5. C 를 입력하고 Enter 키를 누릅니다.

   매개 변수에 대한 보류 중인 값이 True 로 표시됩니다.
6. XPSConfig 유틸리티를 종료합니다.
7. 정책 서버를 다시 시작합니다.

   신뢰 수준 지원이 활성화됩니다.

## CA Arcot 통합 사용 사례

다음 사용 사례는 SiteMinder 와 CA Arcot 강력한 인증 및 위험 평가를 통합하는 방법을 자세히 알려 줍니다. 이 사용 사례는 간단한 통합에서 시작해서 좀 더 복잡한 시나리오로 진행됩니다.

## CA Arcot 인증 및 위험 분석

가장 간단한 배포에는 Adapter 및 모든 관련 구성 요소를 SiteMinder 와 통합하는 과정이 포함됩니다.

Adapter 는 인증 중에 위험 점수 (페이지 236)를 적용하도록 인증(CA Arcot WebFort) 및 위험 평가(CA Arcot RiskFort) 프로세스를 안내합니다.

**다음 단계를 수행하십시오.**

1. CA Arcot RiskFort 와 CA Arcot WebFort 가 설치 및 구성되어 있어야 합니다.

   **참고:** 자세한 내용은 각각의 CA Arcot 설치 및 배포 안내서를 참조하십시오.

2. CA Arcot Adapter 와 모든 관련 구성 요소를 설치 및 배포합니다. 이러한 구성 요소에는 양식 자격 증명 수집기 파일 집합이 포함됩니다. 이 파일을 통해 Adapter HTML 양식 인증 체계를 사용하여 사용자 자격 증명을 수집할 수 있습니다.

   **참고:** Adapter 와 모든 관련 구성 요소를 설치 및 구성하는 방법에 대한 자세한 내용은 *CA Arcot Adapter for CA SiteMinder Installation and Configuration Guide*(CA Arcot Adapter for CA SiteMinder 설치 및 구성 안내서)를 참조하십시오.

3. 다음 단계를 수행하십시오.

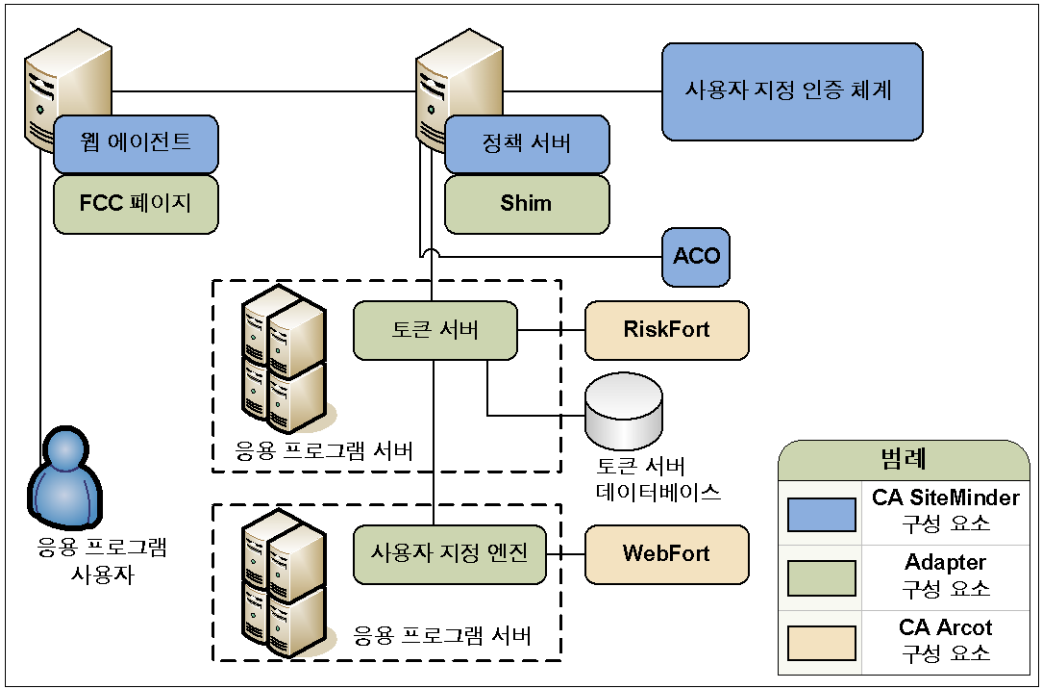
   a. Adapter 라이브러리를 호출하도록 SiteMinder 사용자 지정 인증 체계를 구성합니다.

   b. CA Arcot 통합에 포함할 웹 에이전트를 결정합니다. 통합을 지원하기 위한 각 ACO(에이전트 구성 개체)를 구성합니다.

   **참고:** 필요한 사용자 지정 인증 체계 및 ACO 설정에 대한 자세한 내용은 *CA Arcot Adapter for CA SiteMinder Installation and Configuration Guide*(CA Arcot Adapter for CA SiteMinder 설치 및 구성 안내서)를 참조하십시오. 인증 체계 및 ACO 매개 변수 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

다음 다이어그램은 이러한 배포 시나리오를 보여 줍니다.

*그림 4: CA Arcot 인증 및 위험 분석*




## SiteMinder 인증 및 CA Arcot 위험 분석

SiteMinder 인증 체계를 통합하는 방식을 통해서만 위험 평가에 대해 Adapter 를 구성할 수 있습니다. 통합에 포함되는 SiteMinder 인증 체계를 배킹 인증이라고 합니다.

배킹 인증인 SiteMinder 인증 체계를 사용하는 경우 Shim 이 SiteMinder 와 SiteMinder 인증 체계 간의 인터페이스로 작동합니다.

**참고:** 배킹 인증에 대한 자세한 내용은 *CA Arcot Adapter for CA SiteMinder Installation and Configuration Guide*(CA Arcot Adapter for CA SiteMinder 설치 및 구성 안내서)를 참조하십시오. 모든 SiteMinder 인증 체계가 배킹 인증에 지원되는 것은 아닙니다. 자세한 내용은 SiteMinder Platform Support Matrix(SiteMinder 플랫폼 지원표)를 참조하십시오.

**다음 단계를 수행하십시오.**

1. CA Arcot 인증 및 위험 분석 (페이지 242)에 나열된 단계를 완료합니다.

   **중요!** 통합을 위해서는 SiteMinder 사용자 지정 인증 체계가 구성되어야 합니다. SiteMinder 사용자 지정 인증 체계는 필요한 Adapter 라이브러리를 호출합니다. 이 라이브러리는 배킹 인증을 배포하는 경우에도 필요합니다.

2. 올바른 CA Arcot 매개 변수를 사용하여 SiteMinder 사용자 지정 인증 체계를 구성해야 합니다. 이 매개 변수는 배킹 인증으로 작동하는 SiteMinder 인증 체계를 지원하는 사용자 흐름을 나타내야 합니다. 이 값을 "매개 변수" 필드에 입력하십시오.

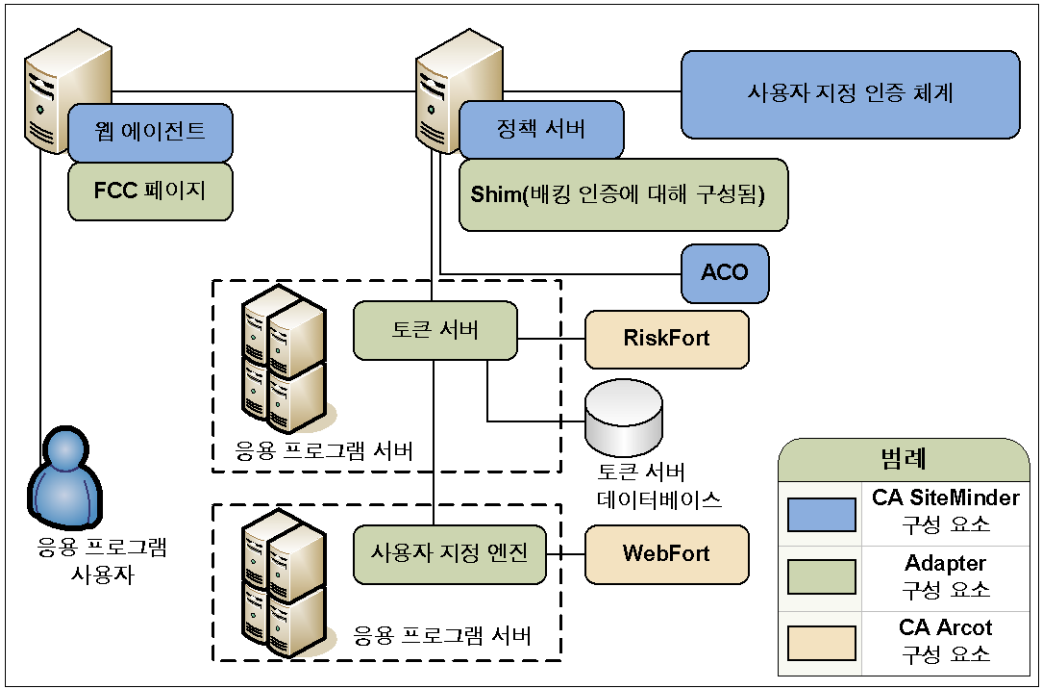
   **참고:** 사용자 흐름 및 해당 매개 변수 값에 대한 자세한 내용은 *CA Arcot Adapter for CA SiteMinder Installation and Configuration Guide*(CA Arcot Adapter for CA SiteMinder 설치 및 구성 안내서)를 참조하십시오. SiteMinder 사용자 지정 인증 체계 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

3. SiteMinder 인증 체계를 배킹 인증으로 사용하도록 Shim 을 구성합니다.

   **참고:** 배킹 인증 체계 구성에 대한 자세한 내용은 *CA Arcot Adapter for CA SiteMinder Installation and Configuration Guide*(CA Arcot Adapter for CA SiteMinder 설치 및 구성 안내서)를 참조하십시오.

다음 다이어그램은 이러한 배포 시나리오를 보여 줍니다.

*그림 5: CA SiteMinder 인증 및 CA Arcot 위험 분석*




## SiteMinder 권한 부여 및 신뢰 수준

신뢰 수준 (페이지 237)을 두 가지 액세스 관리 모델 모두에 추가하여 정책 서버 권한 부여 서비스를 확장할 수 있습니다.

신뢰 수준을 추가하면 CA Arcot 위험 분석 결과를 권한 부여 결정에 적용할 수 있습니다.

**다음 단계를 수행하십시오.**

1. CA Arcot 인증 및 위험 분석 (페이지 242) 또는 SiteMinder 인증 및 CA Arcot 위험 분석 (페이지 243)의 단계를 완료합니다.
2. (선택 사항) 신뢰 수준을 정책 영역 또는 응용 프로그램 구성 요소에 적용할 계획이라면 신뢰 수준 지원을 활성화합니다 (페이지 240). 활성 정책 식 또는 응용 프로그램 역할을 사용하여 신뢰 수준을 적용하는 기능은 이전 릴리스부터 계속 지원되므로 기본적으로 활성화되어 있습니다.

3. 다음 단계 중 하나를 수행합니다.
   - 정책을 사용하여 리소스를 보호하는 경우 신뢰 수준을 하나 이상의 정책 영역 또는 활성 정책 식에 추가합니다.
   - 응용 프로그램을 사용하여 리소스를 보호하는 경우 신뢰 수준을 하나 이상의 응용 프로그램 구성 요소 또는 응용 프로그램 역할에 추가합니다.

     **참고:** 신뢰 수준을 정책 및 응용 프로그램에 적용하는 방법에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

**추가 정보:**

정책 관리 모델 (페이지 65)

## 사용자 저장소 고려 사항

통합이 적용되는 모든 SiteMinder 사용자를 CA Arcot WebFort 데이터베이스에서 사용할 수 있어야 합니다.

도움이 필요한 경우 CA Arcot 지원부에 문의하십시오.

**참고:** 연락처 정보는 *CA Arcot Adapter for CA SiteMinder Installation and Configuration Guide*(CA Arcot Adapter for CA SiteMinder 설치 및 구성 안내서)를 참조하십시오.

# CA Arcot A-OK 통합

CA Arcot A–OK Adapter™(A–OK Adapter)를 사용하여 SiteMinder 를 호스트되는 CA Arcot A–OK 서비스와 통합할 수 있습니다.

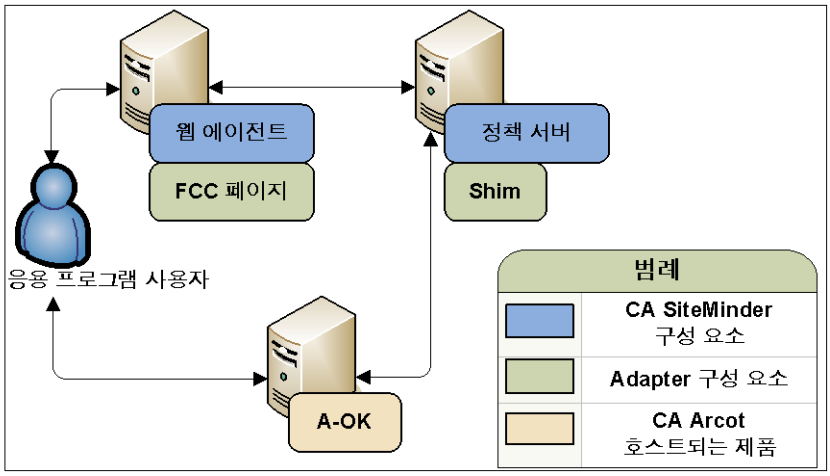
**참고:** 통합을 위해서는 최소 버전의 A–OK Adapter 가 필요합니다. 지원되는 버전에 대한 자세한 내용은 "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)를 참조하십시오.

다음 다이어그램의 용도는 다음과 같습니다.

- SiteMinder 환경에서 A–OK Adapter 와 그 구성 요소가 통합되는 방식을 보여 줍니다.
- 주요 구성 요소와 각 구성 요소의 일반적인 관계를 자세히 알려 줍니다. 이 다이어그램은 워크플로 다이어그램이 아닙니다.

**참고:** A–OK Adapter 설치 및 구성에 대한 자세한 내용은 *CA Arcot A–OK Adapter for CA SiteMinder Installation and Configuration Guide*(CA Arcot A–OK Adapter for CA SiteMinder 설치 및 구성 안내서)를 참조하십시오.

*그림 6: CA SiteMinder 및 CA Arcot A-OK 통합 아키텍처*




## 호스트되는 CA Arcot 통합에서의 인증

CA Arcot A–OK 는 인증 및 위험 평가 프로세스를 안내하는 방식으로 통합 환경에서 인증 서비스를 제공합니다. CA Arcot A–OK 는 일련의 SAML 요청과 응답을 통해 인증 워크플로의 각 단계를 진행합니다.

**참고:** 인증 워크플로에 대한 자세한 내용은 *CA Arcot A–OK Adapter for CA SiteMinder Installation and Configuration Guide*(CA Arcot A–OK Adapter for CA SiteMinder 설치 및 구성 안내서)를 참조하십시오.

위험 평가의 결과로 위험 점수와 해당 권고 사항이 생성되는데, 이 권고 사항은 인증 허용 또는 거부와 같은 권장 작업입니다.

CA Arcot A–OK 는 권고 사항을 정책 서버에 전달하고, 정책 서버는 필요한 경우 자체의 권한 부여 서비스를 계속합니다.

**참고:** 사용자 자격 증명을 관리하고 위험 평가 프로세스와 관련된 규칙을 구성하는 방법에 대한 자세한 내용은 *CA Arcot A–OK User Administration Guide*(CA Arcot A–OK 사용자 관리 안내서)를 참조하십시오.

## 신뢰 수준 및 SiteMinder 권한 부여

정책 서버는 통합 환경에서 권한 부여 서비스를 유지 관리하며 위험 점수를 권한 부여 결정에 적용할 수 있습니다. 위험 점수는 인증 프로세스 (페이지 247)에서 생성됩니다.

정책 서버는 위험 점수를 SiteMinder 신뢰 수준으로 적용합니다. 신뢰 수준은 위험 점수를 기반으로 하므로, 마찬가지로 해당 트랜잭션이 안전할 가능성을 나타내는 정수로 표현됩니다.

다음과 같이 신뢰 수준을 두 가지 액세스 관리 모델에 모두 적용할 수 있습니다.

- 정책을 사용하여 리소스를 보호하는 경우 신뢰 수준을 다음 개체에 적용할 수 있습니다.
  - 정책 영역
  - 활성 정책 식
- EPM 응용 프로그램을 사용하여 리소스를 보호하는 경우 신뢰 수준을 다음 개체에 적용할 수 있습니다.
  - 응용 프로그램 구성 요소
  - SM_USER_CONFIDENCE_LEVEL SiteMinder 생성 특성을 참조하는 명명된 식으로 구성된 응용 프로그램 역할

**참고:** 신뢰 수준을 정책 영역이나 응용 프로그램 구성 요소에 적용하려면 신뢰 수준 지원을 활성화 (페이지 251)해야 합니다. 활성 정책 식 또는 응용 프로그램 역할을 사용하여 신뢰 수준을 적용하는 기능은 이전 릴리스부터 계속 지원되므로 기본적으로 활성화되어 있습니다. 신뢰 수준을 정책 및 응용 프로그램에 적용하는 방법에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

다음 예제 워크플로는 두 값 사이의 관계를 자세히 설명하고 정책 서버가 신뢰 수준을 권한 부여 결정에 적용하는 방식을 보여 줍니다.

1. 사용자가 성공적으로 인증되면 A–OK Adapter 가 아래의 대수 공식을 사용하여 위험 점수를 신뢰 수준으로 변환합니다.

   ```
   (100 - 위험 점수) * 10 = 신뢰 수준
   ```

2. A–OK Adapter 가 신뢰 수준을 SiteMinder 세션 티켓에 삽입합니다.

   **참고:** 세션 티켓에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

3. 사용자가 보호되는 리소스를 요청하면 정책 서버가 세션 티켓의 신뢰 수준을 정책 또는 응용 프로그램에 구성된 신뢰 수준과 비교합니다.

4. 다음 작업이 수행될 수 있습니다.

   - 정책 규칙이 액세스를 허용하도록 구성되고 사용자의 신뢰 수준이 정책 영역 또는 활성 정책 식에 구성된 신뢰 수준 이상일 경우 정책 규칙이 트리거됩니다.

     **참고:** 사용자의 신뢰 수준이 정책에 구성된 신뢰 수준보다 낮으면 SiteMinder 가 액세스를 거부합니다.

   - 정책 규칙이 액세스를 거부하도록 구성되고 사용자의 신뢰 수준이 정책 영역 또는 활성 정책 식에 구성된 값보다 낮을 경우 정책 규칙이 트리거됩니다.

   - 사용자의 신뢰 수준이 응용 프로그램 역할에 구성된 신뢰 수준보다 낮을 경우 사용자가 역할 구성원 자격에서 제외되고 SiteMinder 가 액세스를 거부합니다.

   - 사용자의 신뢰 수준이 응용 프로그램 구성 요소에 구성된 신뢰 수준 이상일 경우 SiteMinder 가 액세스를 허용합니다.

## 위험 점수와 신뢰 수준 비교

위험 점수와 신뢰 수준이 모두 트랜잭션이 안전한지 확인하는 데 도움이 되지만 두 값 사이에는 몇 가지 차이가 있습니다. 권한 부여 결정을 계획할 때는 다음과 같은 차이점을 고려하십시오.

| CA Arcot 위험 점수 | SiteMinder 신뢰 수준 |
|---|---|
| 0~100 사이의 숫자로 위험 점수가 표현됩니다. | 0~1000 사이의 숫자로 신뢰 수준이 표현됩니다. |

| CA Arcot 위험 점수 | SiteMinder 신뢰 수준 |
| --- | --- |
| 위험 점수가 낮을수록 트랜잭션이 안전할 가능성이 커집니다. | 신뢰 수준이 높을수록 트랜잭션이 안전할 가능성이 커집니다.<br>**참고:** 값이 영(0)이면 전혀 신뢰할 수 없음을 나타냅니다. 전혀 신뢰할 수 없으면 SiteMinder 가 요청된 리소스에 대한 액세스를 거부합니다. |

다음 예제 워크플로는 위험 점수와 신뢰 수준 간의 역관계를 자세히 보여 줍니다.

1. 사용자가 SiteMinder 로 보호되는 리소스를 요청하고 인증을 위해 CA Arcot A–OK 로 전달됩니다.
2. A–OK Adapter 가 인증 및 위험 분석 프로세스를 안내합니다. CA Arcot A–OK 평가와 점수 부여 규칙에 따라 사용자가 인증되고 위험 점수가 30 으로 지정됩니다. 위험 점수가 낮을수록 트랜잭션이 안전함을 의미합니다.

   **참고:** 사용자 자격 증명을 관리하고 위험 평가 프로세스와 관련된 규칙을 구성하는 방법에 대한 자세한 내용은 *CA Arcot A–OK User Administration Guide*(CA Arcot A–OK 사용자 관리 안내서)를 참조하십시오.
3. A–OK Adapter 가 다음을 수행합니다.
   a. 인증 결정을 정책 서버에 전달합니다.
   b. 아래의 대수 공식을 사용하여 위험 점수를 신뢰 수준으로 변환합니다.

      ```
      (100 - 위험 점수) * 10 = 신뢰 수준
      ```

      이 예제에서는 A–OK Adapter 가 아래의 대수 공식을 사용하여 위험 점수를 신뢰 수준으로 변환합니다.

      ```
      (100 - 30) * 10 = 700
      ```

      신뢰 수준이 높을수록 트랜잭션이 안전함을 의미합니다.
4. A–OK Adapter 가 신뢰 수준을 사용자의 세션 티켓에 삽입합니다.
5. 사용자가 700 이상의 신뢰 수준을 요구하는 정책 또는 응용 프로그램에 의해 보호되는 리소스를 요청합니다.
6. 정책 서버가 해당 리소스에 대한 액세스를 허용합니다.

## 신뢰 수준 지원 활성화

필요한 경우 신뢰 수준을 권한 부여 결정에 적용할 수 있습니다. 다음 사항을 고려하십시오.

- 신뢰 수준을 다음 개체에 적용할 수 있습니다.
  - 정책 영역
  - 활성 정책 식
  - 응용 프로그램 구성 요소
  - SM_USER_CONFIDENCE_LEVEL SiteMinder 생성 특성을 참조하는 명명된 식을 포함하는 응용 프로그램 역할

  **참고:** 신뢰 수준을 정책 및 응용 프로그램에 적용하는 방법에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.
- 신뢰 수준을 영역 또는 응용 프로그램 구성 요소에 적용하려면 신뢰 수준 지원만 활성화하면 됩니다. 활성 정책 식 또는 응용 프로그램 역할을 사용하여 신뢰 수준을 적용하는 기능은 이전 릴리스부터 계속 지원되므로 기본적으로 활성화되어 있습니다.

**다음 단계를 수행하십시오.**

1. SiteMinder 환경에서 정책 서버 호스트 시스템에 로그인합니다.
2. XPSConfig 유틸리티를 시작합니다.

   XPSConfig 에서 옵션을 묻는 메시지를 표시합니다.
3. SM 을 입력하고 Enter 키를 누릅니다.

   XPSConfig 에서 옵션을 묻는 메시지를 표시합니다.
4. 15 를 입력하고 Enter 키를 누릅니다.

   ConfidenceLevelSupportEnabled 매개 변수가 나타납니다.
5. C 를 입력하고 Enter 키를 누릅니다.

   매개 변수에 대한 보류 중인 값이 True 로 표시됩니다.
6. XPSConfig 유틸리티를 종료합니다.
7. 정책 서버를 다시 시작합니다.

   신뢰 수준 지원이 활성화됩니다.

# CA Arcot A-OK 통합 사용 사례

다음 사용 사례는 SiteMinder 와 CA Arcot A-OK 강력한 인증 및 위험 평가를 통합하는 방법을 자세히 알려 줍니다. 이 사용 사례는 간단한 통합에서 시작해서 좀 더 복잡한 시나리오로 진행됩니다.

## CA Arcot A–OK 인증 및 위험 분석

가장 간단한 배포에는 A–OK Adapter 및 모든 관련 구성 요소를 SiteMinder 와 통합하는 과정이 포함됩니다.

A–OK Adapter 는 인증 프로세스 (페이지 247) 중에 위험 점수를 적용하도록 인증 및 위험 평가 프로세스를 안내합니다.

**다음 단계를 수행하십시오.**

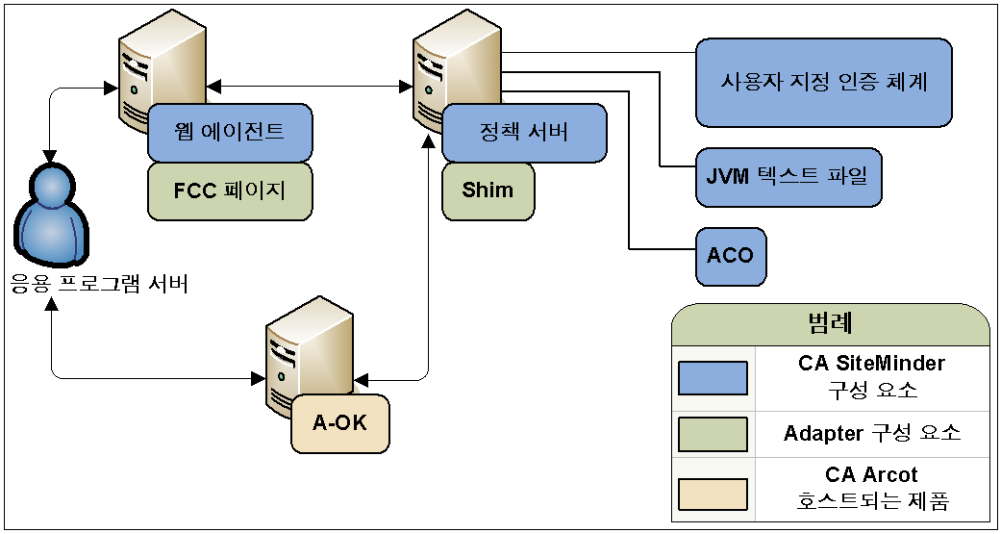
1. CA Arcot A–OK 서비스를 사용할 수 있는지 확인합니다.
2. A–OK Adapter 와 모든 관련 구성 요소를 설치 및 배포합니다. 이러한 구성 요소에는 양식 자격 증명 수집기 파일 집합이 포함됩니다. 이 파일을 통해 A–OK Adapter HTML 양식 인증 체계를 사용하여 사용자 자격 증명을 수집할 수 있습니다.

   **참고:** A–OK Adapter 와 모든 관련 구성 요소의 설치 및 구성에 대한 자세한 내용은 *CA Arcot A–OK Adapter for CA SiteMinder Installation and Configuration Guide*(CA Arcot A–OK Adapter for CA SiteMinder 설치 및 구성 안내서)를 참조하십시오.
3. 다음 단계를 완료합니다.
   a. A–OK Adapter 라이브러리를 호출하도록 SiteMinder 사용자 지정 인증 체계를 구성합니다.
   b. CA Arcot A–OK 통합에 포함할 웹 에이전트를 결정합니다. 통합을 지원하기 위한 각 ACO(에이전트 구성 개체)를 구성합니다.
   c. A–OK Adapter JAR 파일, 인증서 및 속성 파일을 정책 서버의 JVM(Java Virtual Machine) 파일(JVMOptions.txt)에 추가합니다.

   **참고:** 필요한 사용자 지정 인증 체계, ACO 설정 및 정책 서버 JVM 파일의 편집에 대한 자세한 내용은 *CA Arcot A–OK Adapter for CA SiteMinder Installation and Configuration Guide*(CA Arcot A–OK Adapter for CA SiteMinder 설치 및 구성 안내서)를 참조하십시오. 인증 체계 및 ACO 매개 변수 구성에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

다음 다이어그램은 이러한 배포 시나리오를 보여 줍니다.

*그림 7: CA Arcot A-OK 인증 및 위험 분석*




## SiteMinder 권한 부여 및 신뢰 수준

신뢰 수준 (페이지 248)을 두 가지 액세스 관리 모델 모두에 추가하여 정책 서버 권한 부여 서비스를 확장할 수 있습니다.

신뢰 수준을 추가하면 CA Arcot A–OK 위험 분석 결과를 권한 부여 결정에 적용할 수 있습니다.

**다음 단계를 수행하십시오.**

1. CA Arcot A–OK 인증 및 위험 분석 (페이지 252)에 나열된 단계를 완료합니다.
2. (선택 사항) 신뢰 수준을 정책 영역 또는 응용 프로그램 구성 요소에 적용할 계획이라면 신뢰 수준 지원을 활성화합니다 (페이지 251). 활성 정책 식 또는 응용 프로그램 역할을 사용하여 신뢰 수준을 적용하는 기능은 이전 릴리스부터 계속 지원되므로 기본적으로 활성화되어 있습니다.
3. 다음 단계 중 하나를 완료하십시오.
   - 정책을 사용하여 리소스를 보호하는 경우 신뢰 수준을 하나 이상의 정책 영역 또는 활성 정책 식에 추가합니다.

- 응용 프로그램을 사용하여 리소스를 보호하는 경우 신뢰 수준을 하나 이상의 응용 프로그램 구성 요소 또는 응용 프로그램 역할에 추가합니다.

  **참고:** 신뢰 수준을 정책 및 응용 프로그램에 적용하는 방법에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

**추가 정보:**

정책 관리 모델 (페이지 65)

## 사용자 저장소 고려 사항

통합이 적용되는 모든 SiteMinder 사용자를 CA Arcot A–OK 에서 호스트되는 서비스에서 사용할 수 있어야 합니다.

도움이 필요한 경우 CA Arcot 지원부에 문의하십시오.

**참고:** 연락처 정보는 *CA Arcot A–OK Adapter for CA SiteMinder Installation and Configuration Guide*(CA Arcot A–OK Adapter for CA SiteMinder 설치 및 구성 안내서)를 참조하십시오.

# [assign the value for dlp in your book] Content Classification Service 통합

이제 SiteMinder 와 [assign the value for dlp in your book] Content Classification Service(CCS)가 통합되어 정책 서버가 CCS 의 콘텐츠 평가를 기반으로 콘텐츠 인식 권한 부여를 결정할 수 있습니다.

시작하기 전에 다음 사항을 고려하십시오.

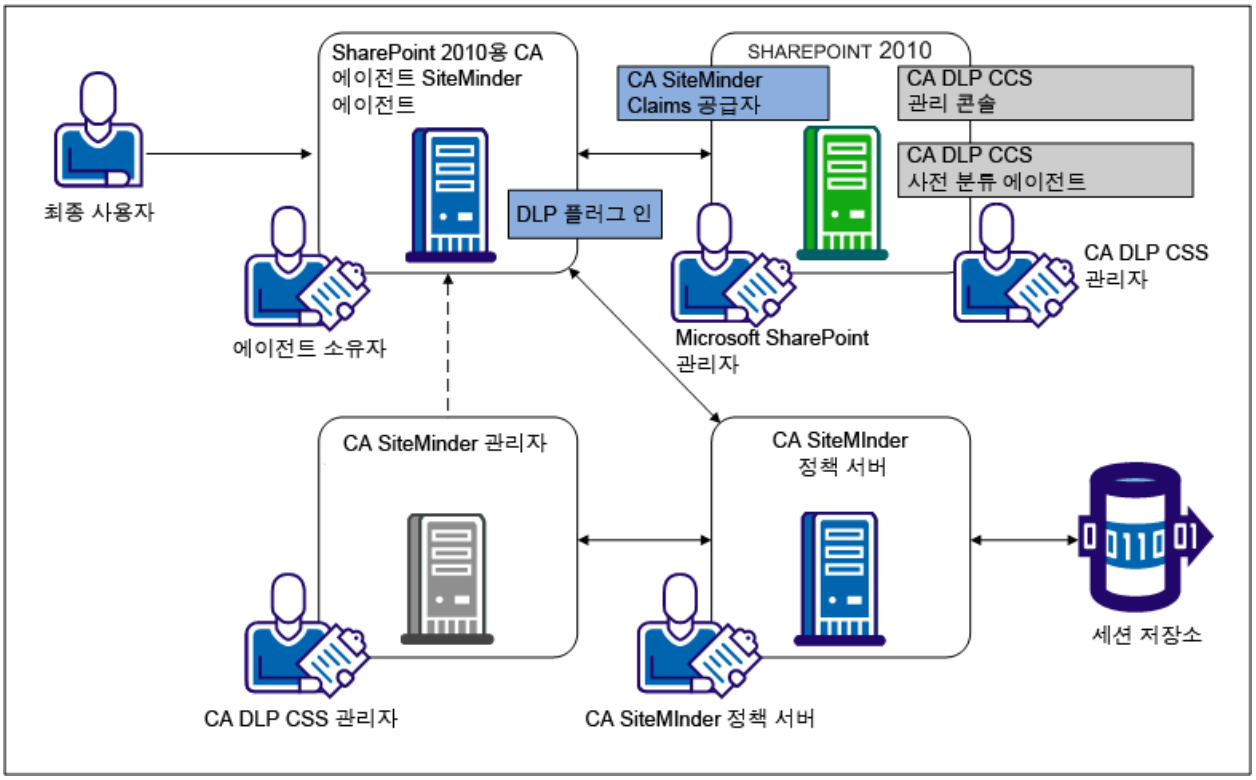
- 통합을 위해서는 최소 버전의 SiteMinder, CCS 및 SharePoint 용 SiteMinder 에이전트가 필요합니다.

  **참고:** 자세한 내용은 "SiteMinder Platform Support Matrix"(SiteMinder 플랫폼 지원표)를 참조하십시오.
- 통합을 사용하려면 여러 조직 역할이 필요합니다. 다음 담당자와 협력하여 통합 작업을 진행하십시오.
  - CCS 관리자

- SiteMinder 관리자
- SharePoint 용 SiteMinder 에이전트의 소유자

다음 다이어그램의 용도는 다음과 같습니다.

- 통합 환경에서 CCS 와 SiteMinder 구성 요소 간의 일반적인 관계를 보여 줍니다. 통합 환경에 배포된 구성 요소나 워크플로가 이 다이어그램에 모두 나와 있지는 않습니다.
- 필요한 구성 요소의 설치나 구성을 담당하는 개별 담당자 간의 연관 관계를 보여 줍니다.




## [assign the value for dlp in your book] Content Classfication Service

통합 환경에서 CCS 는 미리 정의된 콘텐츠 분류를 SiteMinder 정책 서버에 제공하는 역할을 합니다. 분류는 기업 환경에서 일반적으로 사용되는 문서 유형에 해당합니다. 정책 서버는 분류를 사용하여 콘텐츠 인식 권한 부여를 결정합니다.

[assign the value for dlp in your book] Content Classification Service (페이지 254)에 점선으로 표시된 것처럼, 정책 서버가 권한 부여 결정 시 콘텐츠 분류를 사용할 수 없는 경우 CCS 가 직접 리소스 분류 또는 재분류 요청을 할 수 있습니다. CCS 는 다음 작업을 수행합니다.

- 정책 서버가 권한 부여를 결정할 수 있도록 결과를 정책 서버에 전달합니다.
- 이후 권한 부여 결정에 사용할 수 있도록 결과를 CCS 분류 캐시에 추가합니다.

**참고:** CCS 및 콘텐츠 분류에 대한 자세한 내용은 *[assign the value for dlp in your book] Content Classification Service Integration Guide([assign the value for dlp in your book] Content Classification Service 통합 안내서)*를 참조하십시오. 이 안내서는 [assign the value for dlp in your book] Content Classification Service 북셸프에 포함되어 있습니다.

## [assign the value for dlp in your book] Content Classification Service 사전 분류 에이전트

통합 환경에서 [assign the value for dlp in your book] CCS 사전 분류 에이전트는 오프라인으로 SharePoint 문서를 검색하고 분류하는 역할을 합니다. 문서를 오프라인으로 분류하면 정책 서버가 권한 부여를 결정하는 과정에서 문서 분류를 가져올 필요가 없습니다.

**참고:** 사전 분류 에이전트 및 분류 서비스 검색에 대한 자세한 내용은 *[assign the value for dlp in your book] Content Classification Service Integration Guide([assign the value for dlp in your book] Content Classification Service 통합 안내서)*를 참조하십시오. 이 안내서는 [assign the value for dlp in your book] Content Classification Service 북셸프에 포함되어 있습니다.

## SiteMinder 정책 서버

통합 환경에서 SiteMinder 정책 서버는 PDP(정책 결정 지점)의 역할을 합니다. 정책 서버는 다음 작업을 수행합니다.

- 통합 환경 내의 모든 인증 및 권한 부여 서비스를 유지 관리합니다.
- SharePoint 용 SiteMinder 에이전트와 통신하여 보호된 문서의 리소스 정보를 가져옵니다.

- [assign the value for dlp in your book] CCS 와 통신하여 보호된 문서의 콘텐츠 분류를 가져옵니다. 정책 서버는 이러한 결과를 사용하여 콘텐츠 인식 권한 부여를 결정합니다.

해당 기능이 구성된 경우 정책 서버는 [assign the value for dlp in your book] CCS 를 위한 일회용 보안 토큰을 생성할 수 있습니다. [assign the value for dlp in your book] CCS 는 이 토큰을 사용하여 직접 리소스를 요청합니다. CCS 는 권한 부여 결정의 일부로 리소스를 분류하거나 재분류해야 할 경우 리소스를 요청합니다.

**참고:** EPM(Enterprise Policy Management) 응용 프로그램에 콘텐츠 분류를 적용하는 방법에 대한 자세한 내용은 *정책 서버 구성 안내서*를 참조하십시오.

## SharePoint 용 SiteMinder 에이전트

통합 환경에서 SharePoint 용 SiteMinder 에이전트는 PEP(정책 적용 지점)의 역할을 합니다. SharePoint 용 에이전트는 다음 작업을 수행합니다.

- SharePoint 문서에 대한 요청을 가로챕니다.
- 문서에서 리소스 정보를 추출합니다.
- 리소스 정보를 정책 서버에 전달합니다.

## SiteMinder 세션 저장소

SiteMinder 세션 저장소는 일회용 보안 토큰을 클러스터 환경의 모든 정책 서버에 제공하는 역할을 합니다. 해당 기능이 구성된 경우 정책 서버는 [assign the value for dlp in your book] CCS 를 위한 보안 토큰을 생성합니다. 이 토큰은 [assign the value for dlp in your book] CCS 가 보호된 문서에 액세스해야 할 때 자격 증명으로 사용됩니다.

[assign the value for dlp in your book] CCS 는 정책 서버에 콘텐츠 분류를 제공할 수 없는 경우 보호된 문서에 액세스해야 합니다. 리소스 요청을 통해 CSS 는 다음 작업을 수행할 수 있습니다.

- 문서를 분류하거나 재분류합니다.
- 정책 서버에 콘텐츠 분류를 제공합니다.
- 이후 정책 서버 권한 부여 요청에 사용할 수 있도록 콘텐츠 분류를 [assign the value for dlp in your book] 분류 캐시에 추가합니다.

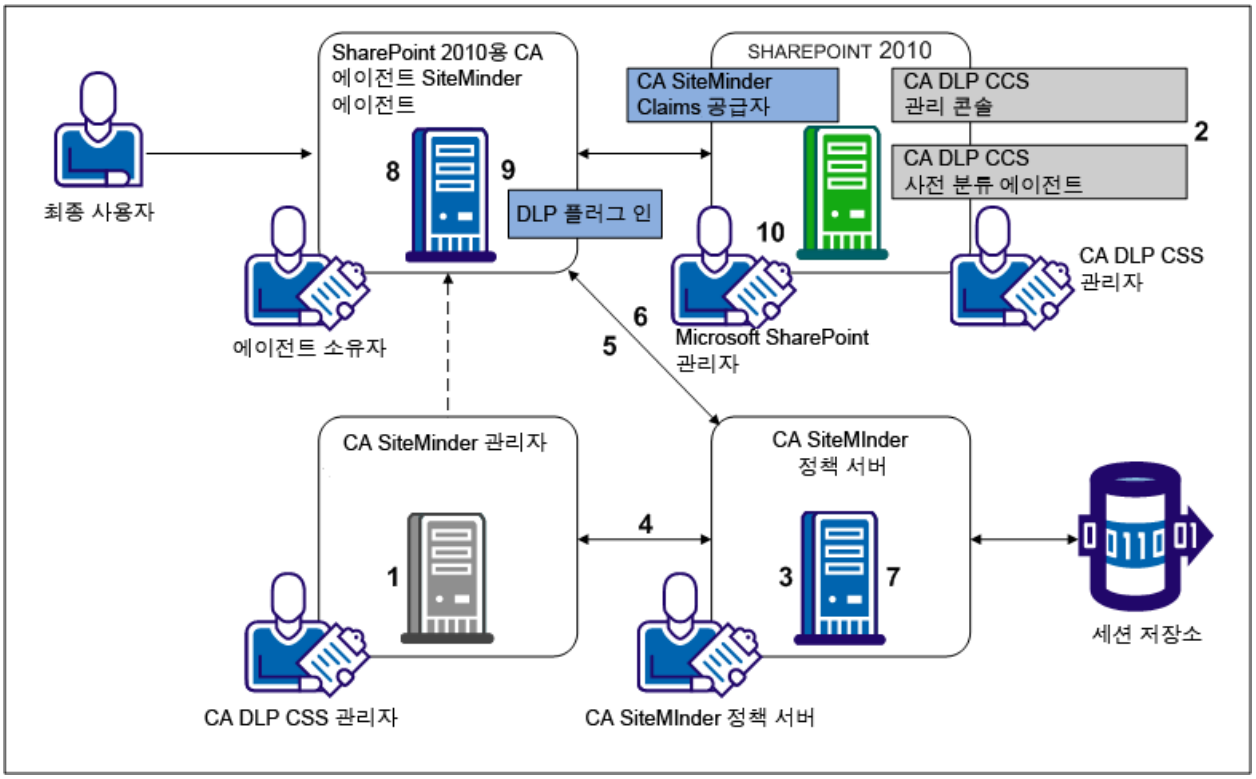
이 과정 중에 SharePoint 용 에이전트는 토큰을 정책 서버에 반환하여 신뢰성을 검사할 수 있도록 합니다. SharePoint 용 에이전트가 토큰을 생성하지 않은 정책 서버로 유효성 검사 요청을 보낼 경우의 결과는 다음과 같습니다.

- 세션 저장소가 포함된 환경의 경우 정책 서버는 토큰을 가져와 유효성을 검사한 후 [assign the value for dlp in your book] CCS 에 대해 권한을 부여합니다.
- 세션 저장소가 포함되지 않은 환경의 경우 정책 서버는 토큰 유효성을 검사할 수 없으며 권한 부여 요청을 거부합니다.

## [assign the value for dlp in your book] Content Classification Service 통합 로드맵

다음 다이어그램의 용도는 다음과 같습니다.

- [assign the value for dlp in your book]와 SiteMinder 통합의 샘플을 보여 줍니다.
- 각 구성 요소의 설치 또는 구성 순서를 보여 줍니다.



다음 표에는 그림에 나온 각 단계와 해당 태스크의 담당자가 나와 있습니다.

| 단계 | 작업 | 담당자 |
|---|---|---|
| 1 | [assign the value for dlp in your book] CCS 를 설치하고 SSL 을 통해 통신하도록 구성합니다. (페이지 259) | [assign the value for dlp in your book] CCS 관리자 |
| 2 | [assign the value for dlp in your book] 사전 분류 에이전트를 설치 및 구성합니다. (페이지 259) | [assign the value for dlp in your book] CCS 관리자 |
| 3 | 통합에 SSL 이 사용되도록 설정합니다. (페이지 260) | SiteMinder 관리자 |
| 4 | [assign the value for dlp in your book] CCS 에 대한 연결을 구성합니다. (페이지 261) | SiteMinder 관리자 |
| 5 | SharePoint 용 에이전트의 에이전트 구성 개체를 수정합니다. (페이지 262) | SiteMinder 관리자 |
| 6 | DLP 제외 목록 매개 변수가 사용되도록 설정합니다. (페이지 263) | SiteMinder 관리자 |
| 7 | 권한 부여 오류 메시지가 사용되도록 설정합니다. (페이지 264) | SiteMinder 관리자 |
| 8 | SharePoint 다중 인증에 대한 프록시 규칙을 수정합니다. (페이지 265) | SharePoint 에이전트 소유자 |
| 9 | DLP 플러그인이 사용되도록 설정합니다. (페이지 268) | SharePoint 에이전트 소유자 |
| 10 | [assign the value for dlp in your book] CCS 에 SharePoint 응용 프로그램에 대한 읽기 권한을 제공합니다. (페이지 269) | SharePoint 관리자 |

## [assign the value for dlp in your book] CCS 관리자 태스크

[assign the value for dlp in your book] CCS 관리자가 담당하는 작업은 다음과 같습니다.

- [assign the value for dlp in your book] Content Classification Service 를 하나 이상 설치하고 각 인스턴스가 SSL 을 통해 통신하도록 구성합니다. 통합을 위해서는 [assign the value for dlp in your book] Content Classification Service 와 SiteMinder 정책 서버가 안전하게 통신해야 합니다.

정책 서버 호스트 시스템에서 SSL 이 사용되도록 설정하려면 SiteMinder 관리자에게 CCS 서버 인증서 파일이 있어야 합니다.

**중요!** CCS 인스턴스가 안전하게 통신하도록 구성할 때 모든 CCS 인스턴스에 대해 동일한 인증서와 암호를 사용하십시오.

- SharePoint 환경에 [assign the value for dlp in your book] CCS 사전 분류 에이전트를 설치하고 분류 서비스 검색을 예약합니다. 사전 분류 에이전트와 함께 [assign the value for dlp in your book] CCS 관리 콘솔이 설치됩니다.

**참고:** 자세한 내용은 *[assign the value for dlp in your book] Content Classification Service Integration Guide([assign the value for dlp in your book] Content Classification Service 통합 안내서)*를 참조하십시오. 이 안내서는 [assign the value for dlp in your book] Content Classification Service 북셸프에 포함되어 있습니다.

## SiteMinder 관리자 태스크

SiteMinder 관리자는 SiteMinder 환경을 통합할 수 있도록 설정하는 작업을 담당합니다. 다음 순서에 따라 통합 단계를 완료하십시오.

1. 통합에 SSL 이 사용되도록 설정합니다.
2. [assign the value for dlp in your book] CCS 에 대한 연결을 구성합니다.
3. SharePoint 에이전트 구성 개체를 수정합니다.
4. DLP 제외 목록 매개 변수가 사용되도록 설정합니다.
5. 권한 부여 오류 메시지가 사용되도록 설정합니다.

## 통합에 SSL 사용

통합을 위해서는 [assign the value for dlp in your book] CCS 와 SiteMinder 정책 서버가 안전하게 통신해야 합니다.

- [assign the value for dlp in your book] CCS 관리자는 모든 [assign the value for dlp in your book] CCS 인스턴스가 안전하게 통신하도록 구성해야 합니다. 시작하기 전에 [assign the value for dlp in your book] 관리자에게 CCS 서버 인증서를 요청하십시오. 통합에 SSL 이 사용되도록 설정하려면 서버 인증서가 필요합니다.
- SSL 이 사용되도록 설정하는 것은 로컬 설정입니다. SharePoint 문서를 보호하고 있는 각 정책 서버에 대해 다음 절차를 완료하십시오.

**다음 단계를 수행하십시오.**

1. 클라이언트 인증서 체인 파일을 생성합니다. 체인 파일은 인증서 파일과 해당 개인 키를 포함하는 단일 파일입니다.

   **중요!** 이 파일은 PEM 형식이어야 합니다.

2. 정책 서버 호스트 시스템에 로그인합니다.
3. CCS 서버 인증서 및 클라이언트 인증서 체인 파일을 배포합니다.
4. *siteminder_home*\bin\thirdparty\axis2c 로 이동합니다.
5. 다음 파일을 엽니다.

   `axis2.xml`

6. SERVER_CERT 매개 변수를 찾습니다. 샘플 값을 CCS 서버 인증서 파일의 경로로 바꿉니다.
7. KEY_FILE 매개 변수를 찾습니다. 샘플 값을 클라이언트 인증서 체인 파일의 경로로 바꿉니다.
8. SSL_PASSPHRASE 매개 변수를 찾습니다. 샘플 값을 클라이언트 인증서 체인 파일의 개인 키를 암호화하는 데 사용된 암호로 바꿉니다.
9. 파일을 저장합니다.

## [assign the value for dlp in your book] Content Classification Service 에 대한 연결 구성

다음 작업을 수행하려면 정책 서버에서 [assign the value for dlp in your book] CCS 에 연결해야 합니다.

- 보호된 문서의 콘텐츠 분류를 가져옵니다.
- 콘텐츠 분류를 사용하여 콘텐츠 인식 권한 부여를 결정합니다.

연결을 구성하는 것은 로컬 설정입니다. SharePoint 문서를 보호하고 있는 모든 정책 서버에 대해 다음 절차를 완료하십시오.

**다음 단계를 수행하십시오.**

1. 슈퍼 사용자 관리자 계정으로 관리 UI 에 로그인합니다.
2. "정책", "DLP 구성"을 차례로 클릭합니다.
3. "SiteMinder DLP 통합 사용" 목록에서 "True"를 선택합니다.
4. 기본 [assign the value for dlp in your book] CCS 의 IP 주소나 정규화된 도메인 이름을 입력합니다.

5. (선택 사항) 추가 구성 매개 변수를 입력합니다.

   **참고:** 매개 변수에 대한 자세한 내용을 보려면 "도움말"을 클릭하십시오.

6. "저장"을 클릭합니다.
7. 정책 서버를 다시 시작하여 정책 서버에서 통합이 사용되도록 설정하고 [assign the value for dlp in your book] CCS 에 대한 연결을 구성합니다.
8. 다시 시작된 정책 서버에 등록된 관리 UI 를 다시 시작합니다.

## SharePoint 에이전트 구성 개체 수정

SharePoint 에이전트 구성 개체를 수정하면 에이전트가 보호된 문서에서 리소스 정보를 추출하도록 구성됩니다. 에이전트는 권한 부여 프로세스 중에 이 정보를 정책 서버에 전달합니다.

**다음 단계를 수행하십시오.**

1. 관리 UI 에 로그인합니다.
2. "인프라", "에이전트 구성 개체"를 차례로 클릭합니다.
3. SharePoint 2010 에이전트의 에이전트 구성 개체를 찾습니다.
4. 편집 아이콘을 클릭하여 개체를 엽니다.
5. DLPSupportEnabled 매개 변수에 대해 다음 값을 입력합니다.

   `SHAREPOINT`

6. "제출"을 클릭합니다.

   에이전트 구성 개체가 통합이 사용되도록 설정됩니다.

7. SharePoint 용 에이전트의 소유자에게 연락합니다. 에이전트 구성 개체는 웹 에이전트 구성 파일에 해당하는 정책 서버 측 요소입니다. SharePoint 용 에이전트에 대한 통합을 완료하려면 웹 계층에서 별도의 절차를 수행해야 합니다. 이 태스크는 SharePoint 용 에이전트의 소유자가 완료해야 합니다.

## DLP 제외 목록 매개 변수가 사용되도록 설정

SharePoint 2010 에이전트 구성 개체에는 DLP 제외 목록 매개 변수가 포함되어 있습니다. 이 매개 변수는 정책 서버가 [assign the value for dlp in your book] CCS 콘텐츠 분류에서 제외하는 기본 리소스 집합을 포함합니다. 콘텐츠 분류에서 리소스를 제외하면 해당 리소스는 자동으로 권한이 부여될 수 있다는 알림이 SharePoint 에이전트에 전달됩니다.

통합을 위해서는 이 매개 변수가 사용되도록 설정해야 합니다.

**다음 단계를 수행하십시오.**

1. 관리 UI 에 로그인합니다.
2. "인프라", "에이전트 구성 개체"를 차례로 클릭합니다.
3. SharePoint 2010 에이전트의 에이전트 구성 개체를 찾습니다.
4. 편집 아이콘을 클릭하여 개체를 엽니다.
5. 다음 매개 변수를 찾습니다.

   `#DlpExclusionList`
6. 편집 아이콘을 클릭하여 매개 변수를 엽니다.
7. 매개 변수 이름에서 파운드 기호를 제거합니다.
8. 추가 리소스를 콘텐츠 분류에서 제외하려면 해당 확장명을 기본 집합에 추가합니다.

   **참고:** 값을 쉼표로 구분하십시오.
9. "확인"을 클릭합니다.
10. "제출"을 클릭합니다.

    에이전트 구성 개체가 사용되도록 설정됩니다.

## 권한 부여 오류 메시지가 사용되도록 설정

기본적으로 권한 부여 중에 사용자가 DLP 콘텐츠 검사에 실패하면 표준 HTTP 403 오류 메시지가 표시됩니다.

사용자에게 친숙한 대체 메시지를 반환하려면 권한 부여 실패 메시지를 사용하십시오.

**다음 단계를 수행하십시오.**

1. 텍스트 파일이나 HTML 파일을 사용하여 사용자 지정 오류 페이지를 생성합니다. 다음 사항을 고려하십시오.
   - 사용자 리디렉션은 사용자 지정 오류 페이지로만 할 수 있습니다. 응용 프로그램은 지원되지 않습니다.
   - 사용 환경에서 Internet Explorer 를 사용하는 경우 사용자 지정 HTML 파일을 배포하려면 다음 항목을 포함하십시오.
     - head 요소에 style 요소를 포함하십시오.
     - body 요소를 닫기 전에 후행 행을 포함하십시오.

     Internet Explorer 에서 사용자 지정 페이지 대신 표준 오류 메시지가 표시되지 않도록 하려면 HTML 파일에 이러한 항목이 있어야 합니다.
2. 관리 UI 에 로그인합니다.
3. "인프라", "에이전트 구성 개체"를 차례로 클릭합니다.
4. SharePoint 2010 에이전트의 에이전트 구성 개체를 찾습니다.
5. 편집 아이콘을 클릭하여 개체를 엽니다.
6. 다음 매개 변수를 찾습니다.

   ```
   #DlpErrorFile
   ```
7. 편집 아이콘을 클릭하여 매개 변수를 엽니다.
8. 매개 변수 이름에서 파운드 기호를 제거합니다.
9. "값" 필드에 사용자 지정 오류 페이지의 위치를 입력합니다.

   **예:**

   ```
   C:\custompages\dlperror.txt
   ```

10. "확인"을 클릭합니다.
11. "제출"을 클릭합니다.

    사용자에게 친숙한 메시지가 사용되도록 설정됩니다.

## SharePoint 용 CA 에이전트 소유자 태스크

SharePoint 용 CA 에이전트 관리자는 SharePoint 에이전트 환경을 통합할 수 있도록 설정하는 작업을 담당합니다. 다음 순서에 따라 통합 단계를 완료하십시오.

1. SharePoint 가 다중 인증 모드로 구성되어 있는 경우 프록시 규칙을 수정합니다.
2. DLP 플러그인이 사용되도록 설정합니다.

## SharePoint 다중 인증에 대한 프록시 규칙 수정

SharePoint 가 다중 인증으로 구성되어 있는 경우 [assign the value for dlp in your book] CCS 가 SharePoint 리소스를 제대로 분류할 수 있도록 하려면 특정 CA SiteMinder Agent for SharePoint 프록시 규칙이 필요합니다.

Sharepoint 관리자에게 문의하여 다중 인증이 구성되어 있는지 여부를 확인하십시오. 다중 인증이 구성되어 있는 경우 다음 절차를 완료하십시오.

**중요!** SharePoint 환경이 다중 인증으로 구성되어 있는 경우 다른 프록시 규칙 설정은 사용하지 마십시오. CA SiteMinder Agent for SharePoint 가 [assign the value for dlp in your book] CCS 의 리소스 요청을 제대로 전달할 수 있도록 이 요청에는 HTTP 헤더가 사용됩니다. CA SiteMinder Agent for SharePoint 가 다음 프록시 규칙을 사용하여 이러한 요청을 제대로 전달하지 않을 경우 보호된 정보에 대한 무단 액세스 및 정보 노출이 발생할 수 있습니다.

**다음 단계를 수행하십시오.**

1. CA SiteMinder Agent for SharePoint 에서 다음 파일을 찾습니다.

   *Agent-for-SharePoint_home*\proxy-engine\conf\proxyrules.xml

2. 다음 예와 유사한 이름을 사용하여 이 파일의 이름을 바꿉니다.

   proxyrules_xml_default.txt

3. CA SiteMinder Agent for SharePoint 에 있는 다음 파일을 텍스트 편집기에서 엽니다.

   *Agent-for-SharePoint_home*\proxy-engine\examples\proxyrules\proxyrules_example2.xml

4. 이 파일을 다음 위치에 새 파일로 저장합니다.

   *Agent-for-SharePoint_home*\proxy-engine\conf\proxyrules.xml

5. 업데이트된 proxyrules.xml 파일에서 다음 텍스트를 찾습니다.

   ```
   :///$$PROXY_RULES_DTD$$"
   ```

6. 이 텍스트를 다음 텍스트로 바꿉니다.

   ```
   :///C:\Program Files\CA\Agent-for-SharePoint\proxy-engine\conf\dtd\proxyrules.dtd"
   ```

7. 다음 텍스트를 찾습니다.

   ```
   http://www.company.com
   ```

8. 이 텍스트를 조직의 도메인으로 변경합니다. 다음 예를 참조하십시오.

   ```
   http:www.example.com
   ```

9. 다음 행을 찾습니다.

   ```
   <nete:cond type="header" criteria="equals" headername="HEADER">
   ```

10. 이 행을 다음 행과 일치하도록 편집합니다.

    ```
    <nete:cond type="header" headername="SMSERVICETOKEN">
    ```

11. 다음 행을 찾습니다.

    ```
    <nete:case value="value1">
    ```

12. 이 행을 다음 행과 일치하도록 편집합니다.

    ```
    <nete:case value="DLP">
    ```

13. 이 행 뒤에 행을 하나 추가합니다.

14. 다음 xml 구문을 복사하여 새 행에 붙여 넣습니다.

```
<nete:xprcond>

<nete:xpr>

<nete:rule>^/_login/default.aspx\?ReturnUrl=(.*)</nete:rule>
<nete:result>http://sharepoint.example.com:port_number/_trust/default.aspx?tr
ust=siteminder_trusted_identity_provider&amp;ReturnUrl=$1</nete:result>
</nete:xpr>

<nete:xpr-default>

<nete:forward>http://sharepoint.example:port_number$0</nete:forward>

</nete:xpr-default>

</nete:xprcond>
```

15. 앞의 섹션에 있는 두 개의 **sharepoint.example:***port_number* 인스턴스를 다음 값 중 *하나*로 바꿉니다.
    - 하드웨어 부하 분산 기능의 호스트 이름, 도메인 및 포트 번호. 이 하드웨어 부하 분산 기능은 CA SiteMinder Agent for SharePoint 서버와 SharePoint 서버 사이에서 작동합니다.
    - 단일 웹 프런트엔드의 호스트 이름, 도메인 및 포트 번호. 이 컨텍스트에서 이 WFE(웹 프런트엔드)는 "백엔드" SharePoint 서버의 앞쪽에서 작동하는 웹 서버를 나타냅니다.
16. 앞의 섹션에 있는 *siteminder_trusted_identity_provider* 인스턴스를 SiteMinder 트러스트된 아이덴티티 공급자 이름으로 바꿉니다.
17. 파일에서 다음 행을 찾습니다.

```
<nete:forward>http://home.company.com</nete:forward>
```

18. 이 행의 **home.company.com** 을 다음 값 중 *하나*로 바꿉니다.
    - 하드웨어 부하 분산 기능의 호스트 이름, 도메인 및 포트 번호. 이 하드웨어 부하 분산 기능은 CA SiteMinder Agent for SharePoint 서버와 SharePoint 서버 사이에서 작동합니다.
    - 단일 웹 프런트엔드의 호스트 이름, 도메인 및 포트 번호. 이 컨텍스트에서 이 WFE(웹 프런트엔드)는 "백엔드" SharePoint 서버의 앞쪽에서 작동하는 웹 서버를 나타냅니다.
19. 파일을 저장하고 텍스트 편집기를 닫습니다.

    프록시 규칙이 설정됩니다.

## DLP 플러그인이 사용되도록 설정

DLP 플러그인이 사용되도록 설정하면 에이전트가 보호된 문서에서 리소스 정보를 추출하도록 구성됩니다. 에이전트는 권한 부여 프로세스 중에 이 정보를 정책 서버에 전달합니다.

**중요!** 통합이 사용되도록 설정하려면 응용 프로그램 계층에서 별도의 절차를 수행해야 합니다. SharePoint 에이전트 구성 개체를 수정하기 전에 웹 에이전트 구성 파일을 수정하지 마십시오. 이 태스크는 SiteMinder 관리자가 완료해야 합니다.

**다음 단계를 수행하십시오.**

1. CA SiteMinder Agent for SharePoint 를 호스트하는 시스템에 로그인합니다.
2. 다음 위치로 이동합니다.

   *Agent-for-SharePoint_Home*\proxy-engine\conf\defaultagent

   **Agent-for-SharePoint_Home**

   CA SiteMinder Agent for SharePoint 가 설치된 디렉터리를 나타냅니다.

   **기본값**: (Windows) [32-비트] C:\Program Files\CA\Agent-for-SharePoint

   **기본값**: (Windows) [64-비트] C:\CA\Agent-for-SharePoint
   **기본값**: (UNIX/Linux) /opt/CA/Agent-for-SharePoint
3. 다음 파일을 엽니다.

   WebAgent.conf
4. 명확성 플러그인을 로드하는 행의 주석 처리를 제거(왼쪽의 # 기호 제거)합니다.

   **예:** (Windows [32-비트]) LoadPlugin="C:\Program Files\CA\Agent-for-SharePoint\agentframework\bin\DisambiguatePlugin.dll"

   **예:** (Windows [64-비트]) LoadPlugin="C:\CA\Agent-for-SharePoint\agentframework\bin\DisambiguatePlugin.dll"

   **예:** (UNIX/Linux) LoadPlugin="/opt/CA/Agent-for-SharePoint/agentframework/bin/DisambiguatePlugin.so"

5. 파일을 저장합니다.
6. 웹 서버를 다시 시작합니다.

   CA SiteMinder Agent for SharePoint 가 [assign the value for dlp in your book] 통합이 가능하도록 구성됩니다.

## Microsoft SharePoint 관리자 태스크

SharePoint 관리자는 SiteMinder 가 보호하는 SharePoint 응용 프로그램에 대한 읽기 권한을 [assign the value for dlp in your book] CCS 에 제공하는 작업을 담당합니다. [assign the value for dlp in your book] CCS 가 보호된 문서에 포함된 콘텐츠의 유형을 확인하려면 읽기 권한이 필요합니다.

[assign the value for dlp in your book] CCS 에 읽기 권한을 제공하는 작업은 응용 프로그램 단위로 수행해야 합니다. SiteMinder 가 보호하는 모든 응용 프로그램에 대해 다음 절차를 완료하십시오.

### 다음 단계를 수행하십시오.

1. CA SiteMinder Claims 공급자가 구성되어 있는 경우 SharePoint 루프백 검색 기능이 필요합니다. 이 기능이 사용되지 않도록 설정되어 있는 경우 다음 단계를 수행하십시오.
   a. "시작", "모든 프로그램", "Microsoft SharePoint 2010 제품", "SharePoint 2010 관리 셸"을 차례로 클릭합니다.
   b. 관리 셸에서 다음 디렉터리로 이동합니다.

      ```
      C:\Program Files\CA\SharePointClaimsProvider\scripts
      ```

   c. 다음 명령을 입력합니다.

      ```
      .\Set-SMClaimProviderConfiguration.ps1 -EnableLoopBackSearch
      ```

   d. 루프백 검색이 사용되도록 설정됩니다.
2. SharePoint 중앙 관리에 로그인합니다.
3. "응용 프로그램 관리" 섹션을 찾은 다음 "웹 응용 프로그램 관리"를 클릭합니다.

   응용 프로그램 목록이 나타납니다.
4. 응용 프로그램을 선택하고 "웹 응용 프로그램" 리본 메뉴에서 "사용자 정책"을 클릭합니다.

   "웹 응용 프로그램 정책" 대화 상자가 나타납니다.

5. "사용자 추가"를 클릭합니다.

   "사용자 추가" 마법사가 나타납니다.

6. "표준 시간대"를 선택하고 "다음"을 클릭합니다.

7. "사용자" 필드를 찾은 다음 찾아보기 아이콘을 클릭합니다.

   "사용자 및 그룹 선택 - 웹 페이지" 대화 상자가 나타납니다.

8. SiteMinder 트러스트된 아이덴티티 공급자를 찾습니다. 이 트러스트된 아이덴티티 공급자 아래에서 관련 식별자 클레임을 클릭합니다.

9. "찾기" 필드에 다음 값을 입력하고 검색 아이콘을 클릭합니다.

   `caservice`

10. 다음 사용자 아이콘을 두 번 클릭하고 "확인"을 클릭합니다.

    `caservice`

    "사용자 추가" 대화 상자가 나타납니다.

11. 다음 권한을 선택하고 "마침"을 클릭합니다.

    `전체 읽기 - 전체 읽기 권한이 있습니다.`

    "웹 응용 프로그램 정책" 대화 상자가 나타납니다.

12. "확인"을 클릭합니다.

    이제 [assign the value for dlp in your book] CCS 에 응용 프로그램에 대한 읽기 권한이 있습니다.

# CA Identity Manager 역할 및 액세스 제어

CA Identity Manager 와 통합하면 CA Identity Manager 역할을 사용한 정책 기반 액세스 제어를 구현할 수 있습니다. 이러한 역할을 사용하면 외부 응용 프로그램에서 사용자 권한을 중앙 집중식으로 관리할 수 있습니다.

**참고:** 통합 구성에 대한 자세한 내용은 CA Identity Manager 설명서를 참조하십시오.

통합 요구 사항은 다음과 같습니다.

- 정책 서버 설치의 다음 위치에 CA Identity Manager 통합을 위한 필수 데이터 정의가 들어 있어야 합니다.

  *siteminder_home*\xps\dd

  **siteminder_home**

  정책 서버 설치 경로를 지정합니다.

- 파일 이름은 다음과 같습니다.

  IdmSmObjects.xdd

  **중요!** CA Identity Manager 통합을 완료한 후에 이 파일을 정책 저장소로 가져오십시오. 통합을 완료하기 전에 데이터 정의를 가져오면 정책 서버가 미확정 상태가 될 수 있습니다. CA Identity Manager 관리자와 함께 통합을 조정하십시오.

- CA Identity Manager 관리자가 CA Identity Manager 의 환경과 역할을 관리하여 SiteMinder 가 보호하는 응용 프로그램에 대한 사용자 액세스를 결정합니다. SiteMinder 관리 UI 에서는 이러한 환경을 IDM 환경이라고 합니다.

  **참고:** 환경 및 역할에 대한 자세한 내용은 CA Identity Manager 설명서를 참조하십시오.

- SiteMinder 관리자가 관리 UI 를 사용하여 하나 이상의 IDM 환경을 정책 도메인 및 사용자 디렉터리에 연결합니다. SiteMinder 관리자는 IDM 환경을 생성하거나 관리할 수 없습니다.

- SiteMinder 관리자가 관리 UI 를 사용하여 정책을 생성하고 IDM 환경에서 사용할 수 있는 하나 이상의 역할에 연결합니다. SiteMinder 관리자는 CA Identity Manager 역할을 생성하거나 관리할 수 없습니다.

  **참고:** 사용자가 CA Identity Manager 역할을 엔터프라이즈 관리 응용 프로그램에 적용할 수 없습니다.

SiteMinder 가 보호된 응용 프로그램에서 CA Identity Manager 사용자에게 지정된 권한에 대한 상세 정보를 제공할 수도 있습니다. 다음 그림에 나와 있는 것처럼, SiteMinder 관리자는 응답을 정책의 액세스 규칙에 연결합니다. 응답에는 SiteMinder 생성 사용자 특성을 지정하는 응답 특성이 들어 있습니다.

SiteMinder 생성 사용자 특성은 CA Identity Manager 에서 태스크 정보를 가져옵니다. 정책 서버는 이 정보를 HTTP 헤더 변수나 쿠키로 웹 에이전트에 전달합니다. 웹 에이전트는 헤더 변수나 쿠키를 보호된 응용 프로그램에서 정밀한 액세스 제어에 사용할 수 있게 만듭니다.

*그림 8: CA Identity Manager 및 세부 액세스 제어*