IBM® WebSphere Commerce®

액세스 제어 안내서

버전 5.4

IBM® WebSphere Commerce®

액세스 제어 안내서

버전 5.4

주!

이 책 및 이 책이 지원하는 제품을 사용하기 전에 반드시 주의사항의 일반 정보를 읽으십시오.

초판(2002년 3월), 제 2 판(2002년 4월)

이 개정판은 다음 제품에 적용됩니다.

Windows NT 및 Windows 2000용 IBM WebSphere Commerce Business Edition, 버전 5.4
AIX용 IBM WebSphere Commerce Business Edition, 버전 5.4
Solaris Operating Environment Software용 IBM WebSphere Commerce Business Edition, 버전 5.4
Windows NT 및 Windows 2000용 IBM WebSphere Commerce Studio, Business Developer Edition, 버전 5.4
Windows NT 및 2000용 IBM WebSphere Commerce Professional Edition, 버전 5.4
AIX용 IBM WebSphere Commerce Professional Edition, 버전 5.4
Solaris Operating Environment Software용 IBM WebSphere Commerce Professional Edition, 버전 5.4
Windows NT 및 Windows 2000용 IBM WebSphere Commerce Studio, Professional Developer Edition, 버전 5.4

새 개정판에서 별도로 명시하지 않는 한, 위 제품의 모든 후속 릴리스와 수정에 적용됩니다. 제품 레벨에 맞는 올바른 버전을 사용하고 있는지 확인하십시오.

책에 대한 주문은 한국 IBM 담당자 또는 해당 지역의 IBM 지방 사무소로 문의하십시오. 다음 주소에서는 책을 구비하고 있지 않습니다.

IBM은 여러분의 의견을 환영합니다. 다음 중 한 가지 방법으로 의견을 보내실 수 있습니다.

1. 아래로 전자 우편을 보내십시오.

   ibmkspoe@kr.ibm.com

2. 우편으로 보내실 경우에는 다음 주소로 우송해 주십시오.

   137-270
   서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
   한국 아이.비.엠 주식회사
   고객만족센터

IBM에 정보를 보내는 경우, IBM은 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다.

참조 정보

WebSphere Commerce™에는 전체적인 전자상거래 솔루션에 대해 설명하는 온라인 및 하드카피 정보가 포함됩니다. 또한 WebSphere Commerce에 번들로 제공되는 소프트웨어 제품들은 소프트웨어 특정 기능을 자세하게 제공합니다. 여기서는 여러 가지 유형의 정보를 찾는 방법에 대해 간단하게 설명합니다.

WebSphere Commerce 서적

- *IBM™® WebSphere Commerce 기본 정보, 버전 5.4*
- *IBM™ WebSphere Commerce 프로그래머 안내서, 버전 5.4*
- *Windows NT™® 및 Windows™® 2000용 IBM™ WebSphere Commerce 빠른 시작, 버전 5.4*
- *Windows NT™ 및 Windows™ 2000용 IBM™ WebSphere Commerce Studio Business Developer Edition 설치 안내서, 버전 5.4*
- *IBM™ WebSphere Commerce 이주 안내서, 버전 5.4*

이 문서들에 대한 갱신은 다음 웹 주소를 참조하십시오.
`http://www.ibm.com/software/webservers/commerce/wc_be/lit-tech-general.html`

WebSphere Commerce 온라인 도움말

WebSphere Commerce 온라인 도움말은 웹 브라우저를 사용하여 볼 수 있는 온라인 정보로 구성됩니다. 온라인 정보에서 발췌한 것은 PDF 문서의 연관된 주제 영역으로 컴파일되었습니다.

온라인 도움말은 다음 주소에서 Internet Explorer, 버전 5.5 이상의 웹 브라우저에서 볼 수 있습니다.

`http://`*`host_name`*`/wchelp/`.
여기서 *`host_name`*은 WebSphere Commerce 시스템의 이름입니다.

또한 Windows에서는 다음과 같이 **시작** 메뉴에서 도움말에 액세스할 수 있습니다.

시작 -> 프로그램 -> IBM® WebSphere Commerce -> 문서

웹에서 사용 가능한 기타 정보

지원

뉴스 그룹, FAQ, 기술적 주석, 문제점 해결 및 다운로드를 포함한 지원 정보를 찾으려면 다음 웹 주소를 방문하십시오.

Business

http://www.ibm.com/software/webservers/commerce/wc_be/support.html

Professional

http://www.ibm.com/software/webservers/commerce/wc_pe/support.html

소프트웨어 협력업체

WebSphere Commerce를 향상시키기 위해 제품 및 서비스를 제공하는 많은 소프트웨어 협력업체가 있습니다. 이들 파트너들에 대한 정보는, 다음 웹 주소를 방문하십시오. http://www.ibm.com/software/webservers/commerce/community 및 Software Developers 링크를 누르십시오.

Redbooks™

고급 기술 정보를 찾으려면 http://www.ibm.com/redbooks에 위치한 Redbooks™ 웹 사이트를 방문하여 WebSphere Commerce를 검색하십시오.

시작하기 전에

*IBM WebSphere Commerce 버전 5.4 액세스 제어 안내서*는 WebSphere Commerce 사이트 액세스를 관리하고자 하는 사이트 운영자를 위한 것입니다. 상점 운영자는 역할을 수행하는 조직 엔티티에 대해 제한된 액세스 관리를 수행할 수 있습니다.

이 안내서는 조직 및 사용자, 액세스 제어 정책, 계층과 관계 및 상품에 포함된 기본 정책에 대한 개요를 포함하는 액세스 관리에 대한 소개를 제공합니다. 이 안내서는 기존 정책의 기초적인 사용자 정의를 하고자 하는 사이트 운영자를 돕기 위한 광범위한 시나리오와 함께 수정한 정책의 테스트 및 성능 고려사항에 대한 지시사항을 제공합니다.

이 책은 다음과 같이 나누어집니다.

제 1 장: 개요 WebSphere Commerce의 액세스 제어 시스템에 대한 핵심 기능의 요약 개요 및 이전 WebSphere Commerce의 출고 이후 변경된 항목에 대한 설명

제 2 장: 시작하기 조직 및 사용자 정의 방법, 조직 및 사용자의 액세스 제어 정책과의 관계, 액세스 제어 정책의 기본 구조, WebSphere Commerce 관리 콘솔 및 XML에서 정책의 주요 부분을 읽고 식별하는 방법 등 액세스 관리에 대한 소개

제 3 장: 액세스 제어 개념 조직과 그 하위 조직 구조의 개념 설명, 사용자에게 시스템에 대한 액세스를 부여하는 방법, 기본 역할 및 관련 용어 설명

제 4 장: 액세스 제어 정책 사용자 정의 자원 레벨 및 역할 기반 정책과 그들의 관계 및 계층에 대한 심화 검토

제 5 장: 액세스 제어 시나리오 WebSphere Commerce와 함께 제공된 기본 액세스 제어 정책의 기초적인 수정 방법을 표시하는 다양한 시나리오

제 6 장: XML 파일을 사용하여 액세스 제어 정책 사용자 정의 XML을 사용하여 액세스 제어 정책 일부의 사용자 정의 검토 이는 정책 정보를 XML 파일에서 액세스 제어 데이터베이스 테이블로 로드하고 XML 파일로 액세스 제어 데이터베이스 테이블에서 정책 정보를 추출하는 단계별 절차 포함

부록: 기본 액세스 제어 정책의 테이블 설치시 시스템에 로드되는 모든 기본 액세스 제어 정책에 대한 완전한 목록

전제

이 안내서는 사이트에 IBM WebSphere Commerce, 버전 5.4를 설치 및 구성하였으며 사이트 운영자가 WebSphere Commerce 관리 콘솔 도구에 액세스할 수 있음을 전제로 합니다. 상점 운영자는 WebSphere Commerce 관리 콘솔 도구를 사용하여 조직 엔티티의 액세스 제어 정책을 관리할 수 있지만 정책의 구성요소(예: 조치 그룹 및 자원 그룹)는 시스템 범위의 엔티티이므로 관리할 수 없습니다.

또한 이 안내서는 시스템이 WebSphere Commerce를 실행하기 위한 모든 소프트웨어 및 하드웨어 요구사항을 충족하고 있음을 전제로 합니다. 전제 조건을 포함한 WebSphere Commerce를 설치하기 위한 자세한 정보는 *IBM WebSphere Commerce 버전 5.4 설치 안내서*를 참조하십시오.

이 책에 사용된 규칙

이 책은 다음과 같은 규칙을 사용합니다.

굵은체는 필드, 아이콘 또는 메뉴 선택사항의 이름과 같이 GUI(Graphical User Interface) 제어를 나타냅니다.

모노체는 디렉토리 경로 및 정확하게 입력해야 하는 텍스트의 예를 나타냅니다.

*기울임꼴*은 값을 입력해야 하는 변수 및 강조의 의미로 사용됩니다.

태스크를 완료하는 데 도움이 되는 추가 정보를 표시합니다.

NT Windows NT®용 WebSphere Commerce 고유의 정보를 표시합니다.

2000 Windows® 2000용 WebSphere Commerce 고유의 정보를 표시합니다.

AIX AIX®용 WebSphere Commerce 고유의 정보를 표시합니다.

Solaris Solaris Operating Environment Software용 WebSphere Commerce 고유의 정보를 표시합니다.

Linux Linux용 WebSphere Commerce 고유의 정보를 표시합니다.

400 IBM Eserver iSeries™ 400®(이전 AS/400®)용 WebSphere Commerce 고유의 정보를 표시합니다.

Professional WebSphere Commerce Professional Edition 고유의 정보를 표시합니다.

Business WebSphere Commerce Business Edition 고유의 정보를 표시합니다.

목차

제 1 장 액세스 제어 소개

전자 상거래의 역할은 기업의 비즈니스 방식을 변화시켰을 뿐만 아니라 고객 및 비즈니스 파트너들로부터 기대할 수 있는 관계의 종류를 극적으로 증가시켰습니다. 웹은 기존 고객에게 향상된 가치를 제공하고 인터넷의 힘과 증가된 효율성으로부터 이익을 얻고자 하는 새 고객에게 다가가는 핵심 요소입니다. 웹을 통한 비즈니스 방식의 명백한 이점 및 고객 기반을 늘릴 수 있는 엄청난 잠재력과 함께 비즈니스 플로우 및 거래 패턴을 관리하면서도 높은 보안 환경을 유지하고, 적절한 트랜잭션에 권한을 부여하며 작업 프로세스를 간소화해야 하게 되었습니다.

액세스 제어의 특징은 사용자가 시스템에 참여하는 방식을 관리함으로써 사용자의 활동 및 상품, 서비스와의 비즈니스 관계를 기반으로 작업 프로세스를 감독하는 능력입니다. 예를 들어, 사이트에 등록한 고객이 상점의 경매 상품을 보고 입찰할 수 있도록 할 수 있습니다. 마찬가지로 그래픽 디자이너에게 상점 페이지를 사용자 정의하는 권한은 부여하지만, 상품 카탈로그의 실제 컨텐츠를 관리하는 것은 제한할 수 있습니다.

WebSphere Commerce는 인스턴스 작성시 시스템으로 자동 로드되는 200개 이상의 기본 액세스 제어 정책을 포함시켜서 액세스 관리에 적합한 도구를 제공합니다. 이 정책은 비즈니스가 필요로 하는 많은 일반적 액세스 제어 요구 사항에 대응하기 위해 설계된 것으로, 고유의 전자 상거래 솔루션에 적합하도록 사용자 정의할 수 있습니다.

전자 상거래 활동에 대한 액세스 관리는 사이트의 승인된 구성원간의 안전한 비즈니스 트랜잭션을 보장하고 온라인 조작의 적법성을 검증함으로써 회사의 재정적 자산 및 자원을 보호하는 데 있어서 불가결한 부분입니다. 액세스 제어는 특히 전자 상거래의 경우 매우 중대하며, 여기에서는 웹을 통해 시작되는 고객 관계에 의해 비즈니스로의 진입이 크게 영향을 받습니다.

WebSphere Commerce 버전 5.4의 새로운 기능

WebSphere Commerce에 추가된 다른 새로운 기능 및 개선점 목록은 *IBM WebSphere Commerce, 버전 5.4 새로운 기능 안내서*를 참조하십시오.

사용자 인터페이스 강화

관리 콘솔의 액세스 관리 메뉴에서 접근 가능한 정책 편집 페이지에 더하여, WebSphere Commerce는 정책 및 그것과 연관된 조치 그룹, 액세스 그룹 및 자원 그룹을 보기 위한 보기 페이지를 추가로 제공합니다. 정책 보기 페이지는 관리 콘솔 사용자 인터페이스와 완전히 통합되었으며 기존 정책 편집 페이지에 추가된 버튼을 이용하여 액세스 가능합니다.

세부 제어

이전 버전의 WebSphere Commerce Suite는 정밀하지 않은 액세스 제어를 제공하는데, 이를 통해 시스템에서 누가 어느 함수를 호출할 수 있는지 정의할 수 있습니다. 예를 들어, 이전 릴리스의 WebSphere® Commerce Suite에서는 구매자에게 주문 취소를 허용하기 위해 `cancel order` 함수를 호출하는 정밀하지 않은 액세스 제어를 사용했을 것입니다.

이제, WebSphere Commerce는 또한 세부 액세스 제어를 통해 어떤 비즈니스 오브젝트 인스턴스(자원이라고도 함)에 대해 누가, 어떤 함수들을 호출할 수 있는지 정의할 수 있게 합니다. 즉, 구매자에게 주문 취소를 허용하되 구매자가 다른 사용자들의 주문이 아닌 자신의 주문에 대해서만 주문 취소 함수를 호출할 수 있도록 제한할 수 있습니다.

정밀하지 않은 액세스 제어에 세부 액세스 제어가 결합된 부가적인 장점으로 인해 더 광범위한 액세스 관리가 가능하며 사이트 활동을 보다 세밀하게 사용자에게 허가할 수 있습니다.

구성요소 별도 관리

이전 릴리스의 WebSphere Commerce Suite에서는 세부 액세스 제어가 시스템 코드 내에 작성되었는데 여기에는 자원 레벨에서 정책을 사용자 정의하기 위해 코드의 변경이 필요했습니다.

이제, WebSphere Commerce는 관리 콘솔 도구에 포함된 정책 표시기 인터페이스나 표준 텍스트 편집기를 이용하여 수정 가능한 XML 파일에 액세스 제어 정책을 정리함으로써 정밀하지 않은 액세스 제어 및 세부 액세스 제어를 외형화하였습니다.

정밀하지 않은 액세스 제어 정책 및 세부 액세스 제어 정책은 이제 상품 코드와 별도로 사용 가능하므로, 비즈니스 요구사항에 맞게 액세스 관리를 고치려면 상품 코드가 아니라 XML 파일에 포함된 정보를 변경해야 합니다.

새로운 비즈니스 프로세스에 적용 가능

지속적으로 변화하는 오늘날의 시장에서 신속하게 비즈니스 환경을 조정해나가는 것은 경쟁력을 유지하고, 시장 변화 및 새로운 비즈니스 프로세스에 적응하는 데 있어 중요한 역할을 합니다. 정밀하지 않은 정책 및 세부 정책을 외형화함으로써, 시스템에 액세스하는 수준을 코드의 사용자 정의가 아닌 정책 수정으로 신속하고 쉽게 변경할 수 있습니다. 보다 중요한 것은, 이전에는 담당 서비스팀만 사용 가능했던 세부 정책을 외부에 둠으로써 자체적으로 기초적인 정책 수정을 많이 할 수 있으며, 또한 사용자의 웹 사이트를 위해 WebSphere Commerce를 사용자 정의하는 추가 비용을 줄일 수 있게 되었습니다.

조정성

시간이 가면서 조직이 변화하고 성장함에 따라, 시스템에 대한 액세스 또한 그러한 변화들을 수용해야 합니다. 새 직원들이 합류하고 역할과 의무가 바뀜에 따라, 그들의 액세스 레벨 또한 필요한 활동을 할 수 있도록 적절하게 변경되어야 합니다. 아직까지 각 개별 사용자의 활동을 추적하는 것은 시간이 걸리고 어려우며 비현실적이기까지 합니다.

하지만, WebSphere Commerce는 ID가 아닌 공유 *속성* 세트로 멤버쉽을 정의하는 액세스 그룹을 이용함으로써 시스템 액세스 허용 관리가 암시적으로 이루어집니다. 사용자에게는 역할이 할당되고 그 역할에 따라 액세스가 주어집니다. 예를 들어, 적절한 액세스 제어 정책을 사용하여 사용자 A, B 및 C에 구매자 역할을 지정하고 모든 구매자는 운송되지 않은 모든 주문을 취소할 수 있습니다. 만약 사용자 A가 조직을 떠나면 사용자 A의 역할 정보는 삭제되는 반면 구매자 역할과 연관된 주문 취소 액세스 제어 정책은 사용자 B와 C를 위해 그대로 유지됩니다.

암시적으로 사용자에게 액세스를 허용하는 능력은, 활동을 관리하는 강력한 방법이며, 훨씬 더 적은 시간과 노력만을 필요로 합니다. 또한, 액세스 제어 관리에 필요한 노력은 변경하려는 정책 수의 요소이지 시스템의 *크기*, 조직에 속한 사용자 수 또는 수행하고자 하는 비즈니스 활동 수의 요소는 아닙니다. 시스템에서 실행되는 액세스 제어 정책은 소규모 조직과 대규모 조직에도 비슷하게 적용될 수 있습니다. 그 결과 WebSphere Commerce에서 실행되는 액세스 제어 정책의 조정성은 운영 구조나 효율성을 저해하지 않으면서도 회사가 계속 변화하고 성장할 수 있게 합니다.

액세스 제어의 의의

액세스 제어는 비즈니스 워크플로우를 관리할 수 있게 해주며 사용자가 그들의 역할 및 의무에 맞는 활동들만 수행하도록 합니다. WebSphere Commerce는 즉시 사용 가능한 기본 정책을 제공할 뿐만 아니라, 비즈니스 요구 사항에 맞게 정책을 사용자 정의할 수 있는 도구 및 기능을 제공합니다.

다음 테이블은 간단한 수정으로 비즈니스 환경 액세스를 사용자 정의하는 방법에 대한 몇 가지 예를 요약한 것입니다.

기본적으로 사용자에게 허용되는 항목	사용자 정의 후 사용자에게 허용되는 항목
고객은 스스로 등록할 수 있습니다.	판매자 관리자만 새 고객을 등록할 수 있습니다.
구매자는 자신이 작성한 RFQ를 표시할 수 있습니다.	RFQ 결과 계약이 체결된 경우, 판매자만이 RFQ를 표시할 수 있습니다.
주문이 보류 상태일 경우 고객만이 자신이 작성한 주문을 취소할 수 있습니다.	전체 상품 가격이 $1000 미만인 경우, 고객 서비스 영업대표는 보류 상태인 주문도 취소할 수 있습니다.
주문은 주문을 작성한 사람이 수정할 수 있습니다.	구매자 조직 중 구매자 역할을 가진 사용자만이 작성된 주문을 수정할 수 있습니다.
회계 담당은 모든 계정을 표시할 수 있습니다.	회계 담당은 활성화된 계정만을 표시할 수 있습니다.

물류 관리자 역할의 직원은 서비스 센터를 작성하고 수정할 수 있습니다.	물류 관리자 역할의 직원은 서비스 센터를 작성할 수 있지만 수정할 수는 없습니다.

다음 장에서는 조직 및 사용자를 작성하는 방법과 액세스 제어 정책에 대해 자세히 다룹니다.

제 2 장 시작하기

앞 장에서는, 전자 상거래에서 액세스 제어 정책이 하는 중요한 역할과 웹상의 비즈니스 수행시 효율성과 신뢰성을 향상시키는 주요 이점들을 배웠습니다.

이 장에서는 WebSphere Commerce의 액세스 관리 기초를 논하는데, 예를 들면 조직 및 사용자 정의, 액세스 제어 정책을 이용하여 시스템에서 수행하는 조직 및 사용자의 활동 관리 방법과 같은 것입니다. 조직 및 사용자를 설정할 때 수행해야 할 단계를 간략히 요약한 후, 액세스 제어 정책 및 WebSphere Commerce에서의 역할을 좀 더 깊이 살펴보고 자세하게 설명합니다.

이 장은 다음 절로 나누어집니다.

- 조직 및 사용자 정의
- 액세스 제어 정보
- 액세스 제어 사용 시작

조직 및 사용자 정의

사이트 운영자의 경우, WebSphere Commerce 설치 및 구성 후 첫 번째 태스크는 전자 상거래 사이트에 대한 액세스를 설정하고 관리하는 것입니다. 여기에는 사이트에 참가할 조직을 작성하고 그 조직들의 구성원을 정의하는 것이 포함됩니다.

어떤 경우에는 사이트에 합류하는 조직이 구매자 조직 또는 다른 조직일 수 있으며, 등록하려는 고객 중 B2C 관계에 있는 고객이 있을 수도 있습니다. B2C 혹은 B2B 중 어느 사이트를 관리하든지, 사이트의 조직 구조를 정의하는 것은 구성원들이 시스템에 대해 가질 수 있는 액세스 유형을 관리하는 데 있어서 중요한 단계입니다.

이 절에서는 사이트의 구조를 정의하기 위해 수행해야 할 상위 레벨 단계를 제공합니다. 만일 조직 및 사용자를 이미 설정한 경우, 액세스 제어의 다음 장으로 건너뛰어도 됩니다. 그렇지 않은 경우, 사전 계획의 안내서로서 이 절을 이용하십시오.

조직, 사용자, 역할을 작성하는 것에 대한 보다 자세한 내용은 기술 라이브러리 페이지의 온라인 도움말을 참조하십시오.

Business

http://www.ibm.com/software/webservers/commerce/wc_be/lit-tech-general.html

Professional

http://www.ibm.com/software/webservers/commerce/wc_pe/lit-tech-general.html

또한 *IBM WebSphere Commerce 기본 정보, 버전 5.4*를 참조하시기 바랍니다.

판매자 조직 정의

보통, 판매자 조직은 WebSphere Commerce 사이트에서 하나 이상의 상점을 소유한 조직입니다. 판매자 조직은 하부 조직이나 부서를 가질 수 있는데, 이들은 각자 하나 이상의 상점을 소유할 수 있습니다. 예를 들어, 견본 상점 InFashion은 패션 상품들을 판매하며, 여기에는 별개의 온라인 상점을 가지는 여성용 부서나 남성용 부서가 있을 수 있습니다.

지금은 하부 조직이 없는 판매자 조직을 설정한다고 가정합니다. 다음은 판매자 조직을 설정하기 위해 수행할 내용을 요약한 것입니다.

1. 새 조직 작성. 새 조직을 만드는 경우 그 조직에 대해 새 프로파일을 작성하게 되며, 여기에는 조직 이름, 설명, 주소, 담당자 및 조직 유형이 포함됩니다.
2. (선택적) 판매자 조직 내에서 승인이 필요한 작업(예: 주문 처리나 사용자 등록)을 정의합니다. 이 단계는 B2B 사이트에서만 필요합니다. 승인에 대한 내용은 제품 온라인 도움말 문서를 참조하십시오.
3. 새 조직에 역할 지정. 조직은 해당 상위 조직에서 지정한 역할만 맡을 수 있습니다. 루트 조직은 모든 다른 조직의 상위이기 때문에 모든 가능한 역할을 지정해야 합니다. WebSphere Commerce는 바로 사용할 수 있는 기본 역할 세트를 제공합니다. 판매자 조직을 작성하고 있으므로 지정할 일반적 역할에는 판매자 관리자, 상점 운영자, 상점 개발자, 판매자 등이 포함됩니다. 기본 역할 목록은 14 페이지의 『역할』을 참조하십시오.
4. 사용자 작성. 조직과 마찬가지로, 각 사용자별로 사용자 이름, 연락처 정보 및 지정된 역할이 포함된 프로파일을 작성합니다. 역할을 지정할 때는, 이전 단계에서 조직에게 지정한 역할 목록에서 선택합니다.

위에서 요약한 모든 단계들은 사이트 운영자가 관리 콘솔의 액세스 관리 메뉴에서 수행할 수 있습니다.

주: WebSphere Commerce Professional Edition에서는 하나의 판매자 조직만 있을 수 있습니다.

구매자 조직 정의

B2B 사이트를 운영하고 있을 경우, 하나 이상의 구매자 조직이 사이트에 속해 있을 수 있습니다(B2C 사이트를 운영하고 있을 경우, 대신 기본 조직에 구매자 각각이 등록됨

니다). 사이트에서 구매 관계에 참여할 비즈니스를 규정하고 나면, 각 비즈니스별로 구매자 조직을 작성해야 합니다. 구매자 조직은 필요한 만큼 가질 수 있습니다.

구매자 조직은 구조적으로 판매자 조직과 유사합니다. 판매자 조직과 마찬가지로, 구매자 조직 또한 하부 조직이나 부서를 가질 수 있으며, 이들은 조직의 다양한 구매 활동을 나타냅니다.

지금은 구매자 조직에 하부 조직이 없다고 가정합니다. 다음은 구매자 조직을 설정하기 위해 수행할 내용을 요약한 것입니다.

1. 판매자 조직을 작성했을 때와 마찬가지로 새 조직을 만들고 필요하다면 승인 가능한 태스크를 정의합니다. 승인 가능한 태스크를 정의하는 것은 B2B 사이트에서만 필요합니다.
2. 새 구매자 조직에 역할 지정. 구매자 조직을 작성하고 있으므로, 지정할 일반적 역할에는 구매자 관리자, 구매자(구매측), 구매자 승인자 등이 포함됩니다.
3. 사용자 작성 및 역할 지정. 역할을 지정할 때는, 이전 단계에서 구매자 조직에게 지정한 역할 목록에서 선택합니다.
4. 사이트에 추가하고자 하는 구매자 조직 각각에 대해 전체 절차를 반복합니다.

위에서 요약한 모든 단계들은 관리 콘솔의 액세스 관리 메뉴에서 이루어집니다.

주: WebSphere Commerce Professional Edition에서는 모든 고객들이 기본 조직에 속합니다.

액세스 제어 이해

전자 상거래 사이트에 참여할 조직 및 사용자 정의를 마치고 나면, 이제 정책 설정을 통해 그들의 활동을 관리할 수 있는데, 이 프로세스를 *액세스 제어*라고 합니다. 다음 절에서는 액세스 제어 정책과 기본 구조를 살펴봅니다.

액세스 제어 정책의 개념

액세스 제어 정책이란 사이트에서 특정 활동을 수행할 수 있도록 권한을 부여받은 사용자 그룹을 설명하는 규칙입니다. 이 활동에는 등록에서 경매 관리, 상품 카탈로그 갱신, 주문 승인 허용까지, 그리고 전자 상거래 사이트를 운영하고 유지보수하는데 필수적인 수백 개의 활동이 포함됩니다.

이 정책들이 사용자에게 사이트 액세스를 허용하게 됩니다. 하나 이상의 액세스 제어 정책을 통해 수행하도록 권한이 부여되어 있지 않은 경우, 사용자는 사이트의 어떤 기능에도 액세스할 수 없습니다.

액세스 재어 정책의 작동 방식

액세스 제어 정책은 다음 4가지 부분으로 구성됩니다. 액세스 그룹, 조치 그룹, 자원 그룹 및 선택적 관계

*액세스 그룹*은 사이트의 기능 세트에 대한 일반 액세스를 공유하는 사용자 그룹입니다. 액세스 그룹에는 일반적으로 같은 부서, 기량 또는 역할 같은 일반 속성을 공유하는 사용자들이 포함됩니다.

*조치 그룹*은 같은 자원에 대해 실행할 수 있는 조치들의 그룹을 말합니다. 일반적으로, 조치 그룹에는 일반 비즈니스 영역과 연관된 조치나 사이트 내 관련 활동 세트가 포함됩니다.

*자원 그룹*에는 정책으로 제어하는 자원이 포함됩니다. 자원 그룹에는 장기 구매 계약이나 관련 명령어 세트 같은 비즈니스 오브젝트들이 포함될 수 있습니다.

어떤 경우에는 자원과 *관계* 있는 사용자만 이에 대해 조치를 취할 수 있습니다. 예를 들어, 장기 구매 계약을 작성한 사용자들만이 이를 수정하도록 할 수 있습니다.

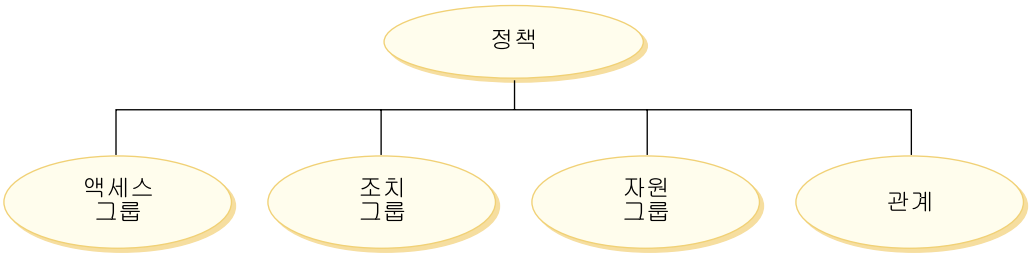


그림 1. 액세스 제어 정책의 4가지 부분

이 4가지 부분이 함께 사용자, 가능한 조치, 조치를 취할 비즈니스 오브젝트 또는 명령어 세트 및 선택적으로 사용자가 자원 그룹에 대해 가지고 있는 관계들을 지정함으로써 WebSphere Commerce에서 정책을 정의하게 됩니다.

액세스 제어 사용 시작 방법

어떤 경우에는 아무것도 할 필요가 없습니다. 그 이유는 WebSphere Commerce의 기본 정책이 일반적인 시스템의 사용자 및 조직에서 그들의 역할과 연관하여 수행하는 활동에 기반을 둔 액세스 제어의 기본 구조를 제공하기 때문입니다. 이 정책들은 광범위한 일반적 비즈니스 활동을 다루며 멤버쉽, 주문 작성 및 처리, 워크플로우 승인 및 경매, 견적 요청, 장기 구매 계약과 같은 거래가 포함됩니다. 조직 및 사용자를 정의한 후 기본 정책을 제공된 그대로 사용할 수도 있고 고객의 개별 요구에 맞게 사용자 정의할 수 있습니다.

하지만, 기본 정책을 사용할 지 혹은 사용자 정의할 지를 결정하기 전에, WebSphere Commerce에서 이들이 어떻게 보일 지를 이해하는 것이 중요합니다. 기본 정책을 자세히 보려면 36 페이지의 『정책 세부사항』을 참조하십시오.

제 3 장 액세스 제어 개념

WebSphere Commerce는 사용자나 응용프로그램이 자원에 액세스할 수 있는 충분한 권한을 가지고 있는지 확인하기 위한 처리로서 액세스 제어를 봅니다. 이 절에서는 WebSphere Commerce 액세스 제어의 몇 가지 측면에 대한 세부사항을 설명합니다.

WebSphere Commerce에서 액세스 제어는 액세스 제어 정책을 사용하여 수행됩니다. 액세스 제어 정책은 자원 세트에 대해 일련의 조치를 수행할 수 있는 사용자 그룹을 설명하는 역할입니다. WebSphere Commerce는 기본 액세스 제어 정책 세트를 제공합니다. 이러한 기본 액세스 제어 정책은 XML 포맷으로 지정되고 e-commerce 사이트에서 필요로 하는 많은 일반적인 액세스 제어 요구사항을 제시하도록 설계됩니다. WebSphere Commerce의 액세스 제어 구성요소에 대해 이해하려면 먼저 e-commerce 사이트의 일반 조직 계층을 알아야 합니다.

조직 계층

WebSphere Commerce 구성원 서브시스템 내의 사용자 및 조직 엔티티는 계층으로 구성됩니다. 이 계층은 조직 및 조직 단위에 대한 항목과 리프 노드의 사용자에 대한 항목이 있는 일반적인 조직 계층과 유사합니다. 계층에는 맨 위에 *루트 조직*이라고 하는 인공의 조직 엔티티가 포함됩니다. 다른 모든 조직 엔티티와 사용자는 이 루트 조직의 최하위 요소입니다. 루트 조직 아래에 하나의 판매자 조직과 몇 개의 구매자 조직이 있을 수 있습니다. 이러한 모든 조직은 하나 이상의 부속 조직을 가질 수 있습니다. 구매자 또는 판매자 관리자는 조직의 우두머리로서 조직을 유지보수해야 합니다. 판매자 조직 측면에서는 각 부속 조직이 조직 내에 하나 이상의 상점을 가질 수 있습니다. 상점 운영자는 상점을 유지보수해야 합니다. 아래 그림은 B2B e-commerce 사이트의 조직 계층을 보여줍니다.

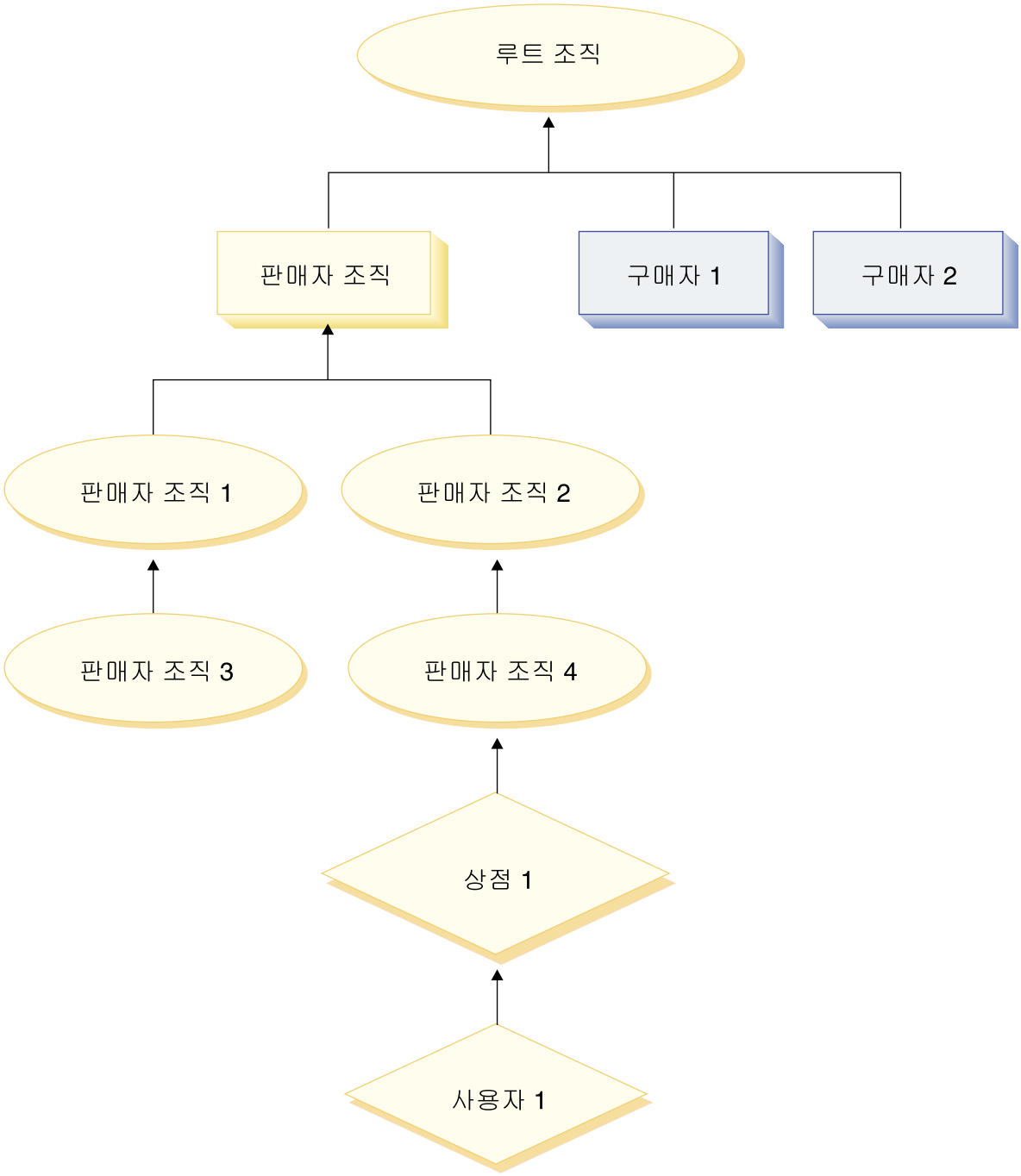


그림 2. B2B 사이트의 조직 계층

루트 조직

루트 조직은 조직 계층의 맨 위에 있습니다. 사이트 운영자는 WebSphere Commerce 내에서 작업을 수행할 수 있는 슈퍼유저 액세스를 갖습니다. 사이트 운영자는 WebSphere Commerce와 이에 연관된 소프트웨어 및 하드웨어를 설치, 구성 및 유지보수합니다. 이 역할은 보통 액세스 및 권한을 제어하고(즉, 구성원 작성 후 적절한 역

할에 지정) 웹 사이트를 관리합니다. 사이트 운영자는 사용자에게 역할을 지정하고 사용자가 역할을 수행하는 조직을 지정할 수 있습니다. 사이트 운영자는 각 운영자에게 암호를 지정하여 권한이 있는 쪽에서만 기밀 정보에 액세스할 수 있도록 해야 합니다. 이렇게 하면 카탈로그 갱신 또는 RFQ 승인과 같은 주요 책임을 제어할 수 있는 방법이 제공됩니다.

주: 사용자는 상위 조직이 아닌 조직에서도 역할을 수행할 수 있습니다.

WebSphere Commerce 사이트에는 하나의 판매자 조직이 있습니다. B2B 사이트에는 하나 이상의 구매자 조직도 있습니다. 사이트 운영자는 판매자 조직(상점을 소유하는)의 액세스 제어 정책과 상점에서 구매하는 각 조직에 대한 액세스 제어 정책을 둘 다 정의할 수 있습니다. B2C 사이트에는 구매자 조직이 없습니다. B2C 고객은 기본 조직의 구성원으로 모델화됩니다.

조직(판매자)

B2B 및 B2C 사이트 둘 다에서 사이트 운영자는 하나의 최상위 레벨 판매자를 작성합니다. 이 판매자 조직 바로 아래에, 다른 부속 조직이나 조직 단위를 작성할 수 있습니다. 이러한 판매측 조직 엔티티는 하나 이상의 상점을 소유할 수 있습니다. 그러면, 사이트 운영자는 판매자 조직에 대한 특수 액세스 제어 정책을 정의하고 조직을 관리할 수 있는 판매자 관리자를 지정합니다. 판매자 관리자는 사용자를 등록하고 해당 조직에 관련된 액세스 제어 정책에 따라 조직의 비즈니스 요구사항에 맞게 서로 다른 역할을 사용자에게 지정합니다.

판매자 관리자의 책임에 대해서는 다음과 같이 요약됩니다.

- 상점을 소유할 수 있는 부속 조직을 작성하십시오. 선택적으로, 조직 내에서 승인을 요구하는 처리를 정의합니다. 이 단계는 B2B 사이트에서만 필요합니다.
- 부속 조직에 역할을 지정합니다.
- 사용자를 작성합니다.
- 사용자에게 역할을 지정합니다.

조직(구매자)

B2B 사이트에서 사이트 운영자는 비즈니스 요구사항에 따라 하나 이상의 구매자 조직을 작성합니다. 그런 다음 구매자 조직에 대한 특수 액세스 제어 정책을 정의하고 구매자 조직을 관리할 수 있는 구매자 관리자를 지정합니다. 구매자 관리자는 사용자를 등록하고 해당 조직에 관련된 액세스 제어 정책에 따라 조직의 비즈니스 요구사항에 맞게 서로 다른 역할을 사용자에게 지정합니다.

구매자 관리자의 책임은 다음과 같이 요약됩니다.

- 구매자 조직 내에 부속 조직을 작성하고 관리합니다. 선택적으로, 조직 내에서 승인을 요구하는 처리를 정의합니다. 이 단계는 B2B 사이트에서만 필요합니다.

- 부속 조직에 역할을 지정합니다.
- 사용자를 작성합니다.
- 사용자에게 역할을 지정합니다.

주: 사이트 운영자는 해당될 경우 구매자 조직의 액세스 제어 정책을 수정하고 관리할 수 있습니다. 사이트 운영자 태스크에 대한 자세한 정보는 15 페이지의 『사이트 운영자』를 참조하십시오.

역할

위에서 언급한 것처럼 WebSphere Commerce는 기본 역할 세트를 제공합니다. 사이트 운영자는 역할에 사용자를 지정하기 전에 모든 조직에 특정 역할을 지정해야 합니다. 조직은 해당 상위 조직에 지정된 역할만 맡을 수 있습니다. 마찬가지로 사용자는 해당 상위 조직에 지정된 역할만 맡을 수 있습니다.

WebSphere Commerce의 모든 역할의 범위는 조직입니다. 예를 들어, 사용자가 조직 X에 대해 상품 관리자 역할을 수행합니다. 이 사용자의 상위 조직도 상품 관리자 역할에 지정되었어야 합니다. 그러면 액세스 제어 정책은 이 사용자가 조직 X와 해당되는 부속 조직의 컨텍스트 내에서만 상품 관리 작업을 수행할 수 있도록 설정할 수 있습니다.

주: 사용자와 조직에 역할을 지정하는 것은 MBRROLE 테이블에서 수행됩니다.

WebSphere Commerce와 함께 제공되는 기본 역할은 다음 카테고리로 그룹화할 수 있습니다.

- 사이트 작업
- 사이트 및 컨텐츠 개발
- 마케팅 관리
- 상품 관리
- 판매 관리
- 물류 및 작업 관리
- 조직 관리

사이트 작업

WebSphere Commerce에서는 다음과 같은 기술 작업 역할이 지원됩니다.

- 사이트 운영자
- 상점 운영자

사이트 운영자

사이트 운영자는 WebSphere Commerce와 이에 연관된 소프트웨어 및 하드웨어를 설치, 구성 및 유지보수합니다. 운영자는 시스템 경고, 경보 및 오류에 응답하고 시스템 문제점을 진단하여 해결합니다. 이 역할은 보통 액세스 및 권한을 제어하고(즉, 구성원 작성 후 적절한 역할에 지정) 웹 사이트를 관리하며 성능 모니터, 로드 밸런싱 태스크를 수행합니다. 사이트 운영자는 또한 테스트, 스테이징 및 생산과 같은 여러 개발 단계에 대한 몇 가지의 서버 구성을 설정 및 유지보수해야 합니다. 이 역할은 중요한 시스템 백업을 처리하고 성능 문제점을 해결해야 할 수도 있습니다.

상점 운영자

상점 운영자는 상점 자원을 관리하고, 세금, 운송 및 상점 정보에 대한 변경사항을 갱신하고 공개합니다. 상점 운영자는 또한 조직에 대한 액세스 제어 정책을 관리할 수 있습니다. 보통 상점 개발 팀을 이끌어 가는 상점 운영자는 상점 아카이브를 공개할 수 있는 권한을 가지고 있는 팀의 유일한 역할입니다(사이트 운영자도 상점 아카이브를 공개할 수 있습니다). 상점 운영자는 보통 웹에 익숙하며 상점의 비즈니스 프로시저에 대한 전체적인 지식을 가지고 있습니다.

사이트 및 컨텐츠 개발

WebSphere Commerce는 상점 개발자 사이트 및 컨텐츠 개발 역할을 지원합니다.

상점 개발자

상점 개발자는 Java™ 서버 페이지 파일과 필요한 사용자 정의된 코드를 작성하고 WebSphere Commerce와 함께 포함된 표준 기능을 수정할 수 있습니다. 상점 아카이브가 작성되었으면, 상점 개발자는 수동으로, 또는 상점 프로파일 노트북과 세금 및 운송 노트북을 사용하여 이 아카이브를 변경할 수 있는 권한을 갖습니다. 상점 개발자는 상점 아카이브를 WebSphere Commerce 서버에 공개할 수 있는 권한은 갖지 않습니다.

물류 및 작업

WebSphere Commerce는 다음과 같은 물류 및 작업 관리 역할을 지원합니다.

- 물류 관리자
- 운영 관리자
- 수령인
- 반품 관리자
- 포장업자

물류 관리자

Business 간혹 운송 관리자로도 불리는 물류 관리자는 운송 회사에서 창고로, 그리고 개인 고객으로의 대량 화물 수송 및 운송을 관리하고 조정합니다. 이 역할은 회사가 회

사 전략에 맞도록 최상의 비용으로 최상의 운송자를 사용할 수 있게 하는 책임을 가지고 있습니다. 운송은 중요한 고객 서비스 측면으로, 온라인 비즈니스에 대한 중요한 성공 요소가 될 수 있습니다.

운영 관리자

B2C 이 역할은 주문이 적절하게 이행되고, 지불이 수령되며, 주문이 운송되도록 주문 처리를 관리합니다. 운영 관리자는 고객 주문 검색, 자세히 보기, 주문 정보 관리, 반품 작성 및 편집을 수행할 수 있습니다.

포장업자

포장업자는 서비스 센터에서 상품을 오더피킹하여 고객에게 운송할 수 있도록 상품을 포장합니다. 포장업자는 또한 출고 요청서와 출고 전표를 관리합니다. 이는 주문 이행 동안 상품 운송을 확인하기 위해 사용됩니다.

수령인

수령인은 서비스 센터에서 재고를 수령하고, 주문된 상품에 대한 예상 재고 레코드 및 임시 수령증을 추적하며, 고객 반품의 결과로 반품된 상품을 수령합니다.

반품 관리자

반품 관리자는 반품된 상품의 처리를 관리합니다.

- 반품 목록
- 반품된 상품 목록
- 반품된 상품 처리

상품 관리

다음 상품 관리 역할이 WebSphere Commerce에서 지원됩니다.

- 구매자(판매자측)
- 카테고리 관리자
- 상품 관리자 또는 판매 계획 관리자

구매자(판매자측)

구매자는 판매 상품을 구입합니다. 구매자는 공급업체나 제공자와의 관계를 처리하고, 운송 및 지불 옵션과 같은 것에 대해 좋은 조건으로 원하는 상품을 확보하기 위해 조정합니다. 구매자는 가격을 설정할 수도 있습니다. 구매자는 구매할 수량을 결정하고 재고가 적절하게 보충하기 위해 재고를 관리합니다.

카테고리 관리자

카테고리 관리자는 카테고리를 작성, 수정 및 삭제하여 카테고리 계층을 관리합니다. 카테고리 계층은 상점에서 제공하는 상품 또는 서비스를 구성합니다. 카테고리 관리자는 또한 상품, 예상 재고 레코드, 공급업체 정보, 재고 및 반품 이유에 대해 관리합니다.

상품 관리자/판매 계획 관리자

Business 판매 계획 또는 B2C 상품 관리자는 고객 구매를 추적하고, 할인을 제안하며, 온라인 상점에서 상품을 표시, 가격 책정 및 판매하기 위한 최상의 방법을 판별합니다.

- 모든 카테고리 관리자 태스크를 수행합니다.
- 모든 마케팅 관리자 태스크를 수행합니다.

판매 관리

다음 비즈니스 관계 관리 역할은 WebSphere Commerce에 의해 지원됩니다.

- 판매 관리자
- 회계 담당
- 고객 서비스 대표
- 고객 서비스 영업대표

판매 관리자

판매 관리자는 고객 모집 및 관리, 판매 예측 충족, 고객 비즈니스 증가에 대한 동기 제공, 장기 구매 계약 관리, 가격 책정 조건 설정, 재고 예측 설정을 위한 상품 관리자와의 작업, 특별 판매를 위한 마케팅 관리자와의 작업 등을 수행합니다.

회계 담당

회계 담당은 관계를 빌드하고 고객 서비스 문제점을 관리하기 위해 개인 계정에 대해 작업합니다. 이들에게는 장기 구매 계약 가격 책정 변경, 장기 구매 계약 조정 및 계정 카테고리별 수익 분석을 수행할 수 있는 권한이 부여될 수도 있습니다.

고객 서비스 대표

이 역할은 모든 고객 서비스 태스크에 대한 액세스를 갖습니다. 고객 서비스 대표는 고객 조회(고객 등록, 주문, 반품 및 경매와 같은)를 관리하고 고객 서비스 영업대표가 액세스할 수 없는 태스크(예: 시스템에서 거부하는 반품 레코드 승인, 지불 예외(신용 카드 권한부여 장애와 같은)에 대해 고객에게 연락)를 완료하기 위한 권한을 갖습니다.

고객 서비스 영업대표Customer Service Representative)

온라인 비즈니스가 고객에게 자체 서비스 기능을 제공하도록 잘 설계되어 있어도, 아무리 웹에 익숙한 고객의 경우에도 개인 연락처를 필요로 하는 특정 유형의 고객이나 경우가 있을 수 있습니다. 대부분의 온라인 비즈니스는 고객을 위해 직접 서비스를 확보하기 위한 전자 우편, 팩스 또는 연락처를 제공합니다. 이는 고객으로부터의 모든 질문을 처리할 고객 서비스 영업대표의 책임입니다.

마케팅 관리

WebSphere Commerce는 마케팅 관리자의 마케팅 관리 역할을 지원합니다.

마케팅 관리자

마케팅 관리자는 마켓 전략 및 브랜드 메시지를 고객에게 알립니다. 이 역할은 고객 행위를 모니터, 분석 및 이해합니다. 또한 마케팅 관리자는 대상 판매에 대한 고객 프로파일을 작성 또는 수정하고 캠페인 및 특별 판매를 작성하고 관리합니다. 캠페인 이벤트 계획은 판매자, 마케팅 관리자 및 판매 계획 관리자로 구성되는 팀에 의해 처리될 수 있습니다.

조직 관리

WebSphere Commerce는 다음 조직 관리 역할을 지원합니다.

- 판매자 관리자
- 구매자 관리자
- 구매자 승인자

판매자 관리자

판매자 관리자는 판매 조직에 대한 정보를 관리합니다. 판매자 관리자는 해당되는 비즈니스 역할 지정을 포함하여, 판매 조직 내의 부속 조직과 판매 조직의 다양한 사용자를 작성 및 관리합니다.

구매자 관리자

구매자 관리자는 판매 조직에 대한 정보를 관리합니다. 구매 조직 내의 부속 조직을 작성 및 관리하고 사용자를 구매자로 승인하는 것을 포함하여 다양한 사용자를 관리합니다. 구매자 승인자 및 추가 구매자 조직 운영자와 같은 다른 구매측 역할을 작성 및 관리할 수도 있습니다.

구매자 승인자

구매자 승인자는 구매 조직에서 판매자에 대해 구매 주문을 제출하기 전에 구매자가 하는 주문을 승인하는 개인입니다.

액세스 제어 정책

액세스 제어 정책은 사용자 그룹에게 WebSphere Commerce 내의 자원 세트에 대해 일련의 조치를 수행할 수 있는 권한을 부여합니다. 하나 이상의 액세스 제어 정책을 통해 권한이 부여되지 않으면, 사용자는 시스템 기능에 대해 어떤 액세스도 갖지 않습니다. 액세스 제어 정책을 이해하려면 네 가지 기본 개념인 사용자, 경매, 자원 및 관계를 이해해야 합니다. 사용자는 시스템을 사용하는 사람입니다. 자원은 시스템에서 보호해야 하는 오브젝트입니다. 조치는 사용자가 자원에 대해 수행할 수 있는 활동입니다. 관계는 사용자와 자원 사이에 존재하는 선택 조건입니다.

액세스 제어 정책의 요소

액세스 제어 정책은 네 개의 요소로 구성됩니다.

액세스 그룹

정책을 적용할 사용자의 그룹.

조치 그룹

자원에서 사용자가 수행하는 조치 그룹.

자원 그룹

정책에 의해 제어되는 자원. 자원 그룹에는 장기 구매 계약이나 주문과 같은 비즈니스 오브젝트나, 특정 역할의 사용자가 수행할 수 있는 모든 명령과 같은 관련 명령 세트가 포함될 수 있습니다.

관계(선택)

각 자원 클래스는 이와 연관되는 관계 세트를 가질 수 있습니다. 각 자원은 각 관계를 이행하는 사용자 세트를 가질 수 있습니다. 예를 들어, 정책은 주문의 작성자만 이를 수정할 수 있도록 지정할 수 있습니다. 이 경우 관계는 작성자이고 사용자와 주문 자원 사이의 관계입니다.

액세스 제어 정책 개념

액세스 제어 정책은 사용자에게 사이트에 대한 액세스 권한을 부여합니다. 하나 이상의 액세스 제어 정책을 통해 수행하도록 권한이 부여되어 있지 않은 경우, 사용자는 사이트의 어떤 기능에도 액세스할 수 없습니다.

각 액세스 제어 정책의 양식은 다음과 같습니다.

```
AccessControlPolicy [AccessGroup,ActionGroup,ResourceGroup,Relationship]
```

액세스 제어 정책의 요소는 특정 액세스 그룹에 속하는 사용자는 자원에 대한 특정 관계를 만족할 경우 지정된 자원 그룹에 속하는 자원에 대해 지정된 조치 그룹의 조치를 수행할 수 있음을 지정합니다. 관계는 필요한 경우에만 지정됩니다. 예를 들어, `[AllUsers,UpdateDoc,doc,creator]`는 문서 작성자인 모든 사용자가 문서를 갱신할 수 있음을 지정합니다.

다음 절에서는 개념적 정보와 액세스 제어와 연관되는 용어를 설명합니다.

구성원 그룹

WebSphere Commerce의 구성원 서브시스템은 다양한 비즈니스 이유에 맞게 카테고리화된 사용자 그룹인 구성원 그룹을 작성할 수 있게 합니다. 그룹은 많은 목적에 사용할 수 있습니다(예를 들어, 액세스 제어 목적, 승인 목적, 할인 및 가격 계산과 상품 표시와 같은 마케팅 목적). 사용자 그룹(-1) 유형의 구성원 그룹은 범용 그룹인 반면, 액세스 그룹(-2) 유형의 구성원 그룹은 액세스 제어 용도입니다. 구성원 그룹은 MBRGRPUSG 테이블에 있는 구성원 그룹 유형과 연관됩니다.

액세스 그룹: 액세스 그룹(-2) 유형의 구성원 그룹은 액세스 제어 목적으로 사용자를 그룹화하기 위한 것입니다. 액세스 그룹은 액세스 제어 정책의 한 요소이며 액세스 제어 목적으로 특별히 정의된 사용자 그룹으로 정의됩니다. 액세스 그룹에서 멤버쉽에 대

한 기준은 보통 역할, 사용자가 속하는 조직 또는 사용자 등록 상태를 기초로 합니다. 예를 들어, 판매자 관리자라고 하는 액세스 그룹은 사용자가 판매자 관리자 역할을 수행하는 그룹입니다.

WebSphere Commerce에는 여러 기본 역할이 포함되며, 각 역할에는 해당 역할을 암시적으로 참조하는 기본 구성원 그룹이 해당됩니다. 역할은 사이트에서 수행하는 활동 유형을 기초로 액세스 그룹에 사용자를 추가하기 위한 속성으로 사용할 수 있습니다. 예를 들어, 기본적으로 판매자 관리자라는 역할과 판매자 관리자라는 해당 액세스 그룹이 있습니다. 사이트 운영자는 WebSphere Commerce 관리 콘솔을 사용하여 사이트에 대한 액세스 그룹을 작성, 유지보수 및 삭제합니다. 구매자 관리자나 판매자 관리자는 WebSphere Commerce 조직 관리 콘솔을 사용하여 사용자에게 역할을 지정하거나 명시적으로 액세스 그룹에 사용자를 지정합니다. 액세스 그룹은 암시적, 명시적 또는 둘 다 가능합니다.

암시적 액세스 그룹: 암시적 액세스 그룹은 기준 세트에 의해 정의됩니다. 기준을 만족하는 사용자는 그룹의 구성원입니다. 기준은 대개 사용자의 역할, 상위 조직 또는 등록 상태를 기초로 합니다. 구성원 그룹에서 멤버쉽을 정의하는 암시적 조건은 MBRGRP 테이블의 CONDITIONS 열에 있습니다. 사용자 속성을 지정하는 암시적 액세스 그룹을 사용하면 명시적으로 개별 사용자를 지정하고 지정을 취소할 필요 없이 유사한 사용자에게 액세스 권한을 부여하는 것이 쉽습니다. 또한 사용자 속성이 변경될 때 그룹 구성원을 갱신하지 않아도 됩니다. 액세스 그룹에 대한 간단한 기준은 사용자가 역할을 수행하는 조직에 관계 없이 특정 역할이 지정된 모든 사용자를 포함하는 것입니다. 더 복잡한 기준으로는 특정 조직에 대해 가능한 역할 세트 중 하나를 수행하는 사용자만 액세스 그룹에 속하도록 지정하는 것이 있습니다.

명시적 액세스 그룹: 구성원 그룹에서 명시적으로 사용자를 추가하거나 제거할 수 있습니다. 이러한 두 명시적 지정은 MBRGRPMBR 테이블을 사용하여 수행될 수 있습니다. 명시적 액세스 그룹에는 일반 속성을 공유할 수도, 공유하지 않을 수도 있는 명시적으로 지정된 사용자들이 포함됩니다. 또한 암시적으로 정의된 그룹에서 포함 조건은 충족하지만 그룹에서 제외하려고 하는 개인을 제외할 수도 있습니다.

사용자 그룹: 사용자 그룹(-1) 유형의 구성원 그룹은 일반적인 관심을 공유하는 사용자 집합으로서 판매자에 의해 정의됩니다. 사용자 그룹은 단골 또는 선호 고객을 위해 대형 상점에서 제공하는 클럽과 유사합니다. 사용자 그룹의 일부가 되면 고객에서 상품을 구매할 수 있도록 할인 또는 기타 보너스를 부여할 수 있습니다. 예를 들어, 시장 조사에서 연장자 고객이 반복적으로 여행 서적 및 가방을 구입하는 것으로 나타난 경우, 이러한 고객에게 연장자 여행 클럽이라는 구성원 그룹을 지정할 수 있습니다. 마찬가지로, 단골 고객에게 비즈니스에 대해 보답하기 위한 사용자 그룹을 작성할 수 있습니다.

조치

일반적으로, 조치는 자원에 대해 수행되는 조작입니다. 제어 명령에 대한 역할 기반 정책에서 조치는 실행이고 자원은 실행되는 명령입니다. 보기에 대한 역할 기반 정책에서 조치는 보기의 이름이고 자원은 com.ibm.commerce.commands.ViewCommand입니다. 자원 레벨 액세스 제어의 경우, 조치는 보통 WebSphere Commerce 명령에 맵핑되고 자원은 보통 보호 EJB(Enterprise Java Bean)의 원격 인터페이스입니다. 예를 들어, 제어기 명령 com.ibm.commerce.order.commands.OrderCancelCmd는 com.ibm.commerce.order.objects.Order 자원에 대해 작동합니다. 마지막으로 Display 조치는 데이터 bean 자원을 활성화하는 데 사용됩니다.

사이트 운영자는 WebSphere Commerce 관리 콘솔을 사용하여 기존 조치를 조치 그룹과 연관시킬 수 있지만 새 조치를 작성할 수는 없습니다. 새 조치는 XML 파일에 정의한 후 데이터베이스로 로드하여 작성할 수 있습니다. 조치는 ACACTION 테이블에 저장됩니다.

조치 그룹

조치 그룹은 관련 조치의 그룹입니다. 조치 그룹의 예로, 다음 명령을 포함하는 AccountManage 그룹을 들 수 있습니다.

- com.ibm.commerce.account.commands.AccountDeleteCmd
- com.ibm.commerce.account.commands.AccountSaveCmd

사이트 운영자만 조치 그룹을 작성, 갱신 및 삭제할 수 있습니다. 이것은 WebSphere Commerce 관리 콘솔과 XML을 통해 수행할 수 있습니다. 조치 그룹은 ACACTGRP 테이블에 저장됩니다. 조치는 ACACTACTGP 테이블에 있는 조치 그룹과 연관됩니다.

자원 카테고리

자원 카테고리는 액세스 제어로 보호해야 하는 자원 클래스를 의미합니다. 자원은 Protectable 인터페이스 정보를 구현해야 합니다. 자원 카테고리는 주문, RFQ 및 경매와 같은 Java 클래스입니다. 자원은 이러한 클래스의 인스턴스입니다. 예를 들어, 경매 운영자 A에 의해 작성된 경매 1이 한 자원이고 경매 운영자 B에 의해 작성된 경매 2는 또다른 자원입니다. 이 두 자원이 자원 카테고리인 경매에 속합니다.

주: Protectable 인터페이스에 대한 자세한 정보는 *IBM WebSphere Commerce 프로그래머 안내서*를 참조하십시오.

자원 카테고리는 ACRESCGRY 테이블에 정의되고 편의상 가끔씩 자원으로 언급됩니다. 사이트 운영자는 WebSphere Commerce 관리 콘솔을 사용하여 기존 자원 카테고리와 자원 그룹을 연관시킬 수 있습니다. 새 자원 카테고리는 XML을 사용하여 작성할 수 있습니다.

자원

자원은 시스템에서 보호해야 하는 오브젝트입니다. 예를 들어, RFQ, 경매, 사용자 및 주문은 WebSphere Commerce에서 보호해야 하는 자원의 일부입니다. 각 자원에는 소유자가 있습니다. 자원 소유권은 적용할 액세스 제어 정책을 판별하기 위해 사용됩니다. 액세스 제어 정책은 조직 엔티티인 소유자를 가지고 있습니다. 정책은 정책을 소유하는 동일 조직 엔티티가 소유하는 자원에만 적용됩니다. 최상위 조직 엔티티가 소유하는 정책도 자원에 적용됩니다.

제어기 명령 자원: 제어기 명령에 대한 역할 기반 액세스 제어의 경우, 정책은 실행 조치가 제어기 명령 자원에서 수행되는 것처럼 구조화됩니다. 이러한 정책은 제어기 명령 실행을 지정된 역할의 사용자로 제한하기 위한 것입니다. 이러한 정책의 액세스 그룹은 보통 단일 역할을 가지고 있는 사람들입니다(예를 들어, 상품 관리자 역할을 가지고 있는 상품 관리자들). 그러면 자원 그룹은 상품 관리자가 실행할 수 있는 제어기 명령 세트가 됩니다.

제어기 명령에 대한 역할 기반 액세스 제어를 실시하는 동안 명령의 소유자를 결정해야 합니다. 이것은 구현된 경우 명령에서 `getOwner()` 메소드를 호출하여 수행됩니다. 대개 이 메소드는 구현되지 않으므로 다음 중 한 가지를 수행하여 WebSphere Commerce Runtime이 이를 확인합니다.

- 현재 명령 컨텍스트에 있는 상점을 소유하는 조직을 사용합니다.
- 명령 컨텍스트에 상점이 없는 경우 루트 조직을 소유자로 사용합니다.

데이터 bean 자원: 모든 데이터 bean이 보호를 요구하지는 않습니다. 기존 WebSphere Commerce 응용프로그램 내에서 보호가 필요한 데이터 bean은 이미 필요한 액세스 제어를 구현해 있습니다. 보호할 데이터 bean은 새 데이터 bean을 작성할 때 정하게 됩니다. 보호할 자원을 결정하는 것은 응용프로그램에 따라 다릅니다. 표시할 정보가 보기에 대한 역할 기반 액세스 제어에 의해 충분히 보호받지 못하는 경우 데이터 bean을 직간접적으로 보호해야 합니다. 이는 데이터 bean을 포함하는 JSP(Java Server Page)에 해당합니다.

데이터 bean이 보호되어야 하고 자체적으로 존재할 수 있는 경우에는 직접적으로 보호해야 합니다. 데이터 bean의 존재가 또다른 데이터 bean의 존재 여부에 달려 있는 경우 보호를 위해 다른 데이터 bean에 위임해야 합니다. 직접 보호하는 데이터 bean의 예로는 `Order` 데이터 bean이 있습니다. 간접적으로 보호되는 데이터 bean의 예로는 `OrderItem` 데이터 bean이 있습니다. 이 데이터 bean은 `Order` 데이터 bean 없이는 존재할 수 없습니다. 데이터 bean 자원을 보호하는 방법에 대한 자세한 정보는 *WebSphere Commerce 5.4 프로그래머 안내서*를 참조하십시오.

데이터 자원: 데이터 자원은 경매, 주문, RFQ 및 사용자와 같이, 조작될 수 있는 비즈니스 오브젝트를 말합니다. 이들은 대개 엔터프라이즈 bean 레벨에서 보호되지만 Protectable 인터페이스를 구현하는 모든 클래스를 보호할 수 있습니다. 데이터 자원은

자원 레벨 액세스 제어 확인을 사용하여 보호됩니다. 이를 수행하는 일반적인 방법은 제어기 또는 태스크 명령의 getResources() 메소드에 있는 데이터 자원을 리턴하는 것입니다. 자세한 정보는 *WebSphere Commerce 5.4 프로그래머 안내서*를 참조하십시오.

자원 그룹

자원 그룹은 관련된 자원 세트를 식별합니다. 자원 그룹에는 장기 구매 계약이나 관련 명령 세트와 같은 비즈니스 오브젝트가 포함될 수 있습니다. 액세스 제어에서 자원 그룹은 액세스 제어 정책이 액세스 권한을 부여하는 자원을 지정합니다.

자원 그룹은 ACRESGRP 테이블에 정의됩니다. 사이트 운영자는 WebSphere Commerce 관리 콘솔을 사용하거나 XML을 사용하여 자원 그룹을 관리하고 자원을 자원 그룹과 연관시킬 수 있습니다.

암시적 자원 그룹: 암시적 자원 그룹은 특정의 속성 세트와 일치하는 자원을 정의합니다. 이러한 속성 중 한 가지는 Java 클래스 이름이어야 합니다. 기타 속성에는 상태, 상점 ID, 가격 등이 포함될 수 있습니다. 예를 들어, 보류 중 상태(ORDERS.STATUS=P)인 모든 주문을 포함하는 암시적 자원 그룹을 작성할 수 있습니다. 암시적 자원 그룹은 대개 자원이 Java 클래스 이름 외에 일반 속성을 공유할 때 자원 레벨 정책에서 사용할 자원을 그룹화하는데 사용합니다.

암시적 자원 그룹은 ACRESGRP 테이블의 CONDITIONS 열을 사용하여 정의됩니다. 단순한 암시적 자원 그룹은 WebSphere Commerce 관리 콘솔을 사용하여 작성할 수 있습니다. XML을 사용하여 점점 더 복잡한 그룹을 작성할 수 있습니다.

명시적 자원 그룹: 명시적 자원 그룹은 하나 이상의 자원 카테고리를 자원 그룹과 연관지어서 지정됩니다. 이러한 연관은 ACRESGPRES 테이블에서 수행됩니다. Java 클래스 이름을 나열하여 그룹에 명시적으로 자원 카테고리를 추가하면 일반 속성을 공유하지 않아도 되는 개인 자원을 그룹화할 수 있습니다.

관계

각 자원은 연관된 특정 종류의 관계를 갖거나, 각 관계를 이행하는 구성원 세트를 가질 수 있습니다. 예를 들어, 모든 자원은 자원 소유자가 이행하는 *소유자* 관계를 갖습니다. 기타 관계는 문서를 받는 사람과 주문 작성자를 포함할 수 있습니다. 이러한 자원 관계는 특정의 자원 인스턴스에서 특정 조치를 수행할 수 있는 사람을 판별할 때 중요합니다. 예를 들어, 문서 작성자는 문서를 삭제할 수 없지만 감사자는 삭제할 수도 있습니다. 마찬가지로, 검토자는 문서를 읽거나 승인할 수 없지만 문서를 전달하거나 다른 조직을 수행할 수는 있습니다.

관계는 ACRELATION 테이블에 저장되고, 선택적으로 ACPOLICY 테이블의 ACRELATION_ID 열을 사용하여 액세스 제어 정책에 지정됩니다. 사용자와 자원 간의 관계를 충족시켜야 하는 정책을 확인할 때 자원에서 fulfills(Long Member, String

relationship) 메소드가 호출되어 확인합니다. 이러한 관계와 관계 그룹을 비교하는 경우 이러한 관계를 종종 단순 관계로 지칭합니다.

관계 그룹: 액세스 제어 정책은 사용자가 액세스할 자원에 대한 특정 관계를 충족해야 한다고 지정하거나 사용자가 관계 그룹에 지정된 조건을 충족해야 한다고 지정할 수 있습니다. 대부분의 경우 관계면 충분합니다. 그러나 보다 복잡한 관계가 요구되는 경우 대신 관계 그룹을 사용할 수 있습니다. 관계 그룹으로 복수 관계와 관계 체인을 지정할 수 있습니다. 이들 모두 관계 체인 구조를 사용하여 수행됩니다. 관계 체인은 단순한 관계(사용자와 자원의 직접적인 관계)를 표현할 수 있는 구조이지만 이를 사용하여 사용자와 자원 간 일련의 관계를 표현할 수도 있습니다. 예를 들어, 사용자가 자원과의 관계(소유자 관계 제외)를 가진 조직에서 역할을 가지고 있어야 한다고 표현하려면 관계 그룹을 사용해야 합니다. 이 예에서 사용자와 조직 간에 역할 관계가 있고 조직과 자원 간에 관계가 있는 것입니다.

관계 및 관계 그룹 비교: 개념적으로 대부분의 관계가 사용자와 자원의 직접적인 관계이므로, 대부분의 경우 관계를 사용하려면 응용프로그램에 대한 액세스 제어 요구사항을 충족시켜야 합니다. 예를 들어, 정책에서 사용자가 자원의 작성자여야 합니다. 그러나 복수 관계를 지정해야 하는 경우 관계 그룹을 사용해야 합니다. 예를 들어, 정책에서 사용자가 자원의 작성자이거나 제출자여야 합니다.

또한 관계 그룹은 사용자와 자원의 관계 체인을 표현해야 합니다. 관계 체인에서 사용자와 자원의 직접적인 관계는 없습니다. 예를 들어, 주문에 지정된 구매 조직에 속한 사용자가 있을 수 있습니다. 이 경우 사용자는 조직과 하위 관계를 가지고 해당 조직은 주문과 구매 관계를 갖습니다.

관계 체인: 각 관계 그룹은 andListCondition 또는 orListCondition 요소별로 그룹화된 하나 이상의 RELATIONSHIP_CHAIN 개방 조건으로 구성됩니다. 관계 체인은 일련의 하나 이상의 관계입니다. 관계 체인의 길이는 구성되는 관계 수로 결정됩니다. 이것은 관계 체인의 XML 표현에서 <parameter name= "X" value="Y"/> 항목 수를 조사하여 판별할 수 있습니다. 다음은 길이가 1인 관계 체인의 예입니다.

```
<openCondition name="RELATIONSHIP_CHAIN">
<parameter name="RELATIONSHIP"
value="aValue"/>
</openCondition>
```

길이가 1인 관계 체인의 경우 <parameter name="Relationshiop" value="something"> 요소는 사용자와 자원의 직접적인 관계를 지정합니다. 값 속성은 사용자와 자원의 관계를 나타내는 문자열입니다. 이것은 또한 보호 가능한 자원에 대한 fulfills() 메소드의 관계 매개변수와 일치해야 합니다.

관계 체인의 길이가 2인 경우 이것은 일련의 두 관계입니다. 첫 번째 <parameter name= "X" value="Y"/> 요소는 사용자와 조직 엔티티 사이에 있습니다. 마지막 <parmeter name= "X" value="Y"/> 요소는 조직 엔티티와 자원 사이에 있습니다. 다음은 길이가 2인 관계 체인의 예입니다.

```
<openCondition name=RELATIONSHIP_CHAIN">
<parameter name="aValue1" value="aValue2"/>
<parameter name="RELATIONSHIP" value="aValue3"/>
</openCondition>
```

aValue1의 가능한 값은 HIERARCHY와 ROLE입니다. HIERARCHY는 멤버쉽 계층 구조에서 사용자와 조직 엔티티 간에 계층 구조 관계가 있음을 지정합니다. ROLE은 사용자가 조직 엔티티에서 역할을 수행함을 지정합니다.

aValue1 값이 HIERARCHY인 경우 가능한 값은 child이며 이것은 사용자가 구성원 계층에서 직접 하위인 조직 엔티티를 리턴합니다. aValue1 값이 ROLE인 경우 가능한 값은 ROLE 테이블의 NAME 열에 있는 임의의 유효한 항목이며 이것은 현재 사용자가 이 역할을 수행하는 모든 조직 엔티티를 리턴합니다.

aValue3 항목은 첫 번째 매개변수와 자원을 확인하여 검색된 하나 이상의 조직 엔티티 간의 관계를 나타내는 문자열입니다. 이 값은 보호 가능한 자원에서 fulfills() 메소드의 관계 매개변수와 일치합니다. aValue1 매개변수를 확인하여 하나 이상의 조직 엔티티가 리턴된 경우 적어도 하나의 이러한 조직 엔티티가 aValue2 매개변수에 지정된 관계를 충족하는 경우 RELATIONSHIP_CHAIN의 이 부분이 충족됩니다.

주: 단일 매개변수 요소가 있는 단일 관계 체인으로 구성된 관계 그룹은 기능적으로 단순 관계와 동일합니다. 이 경우 정책에서 관계 그룹 대신 관계를 사용하는 것이 보다 쉽습니다. 관계 그룹 정의에 대한 자세한 정보는 100 페이지의 『관계 그룹 정의』를 참조하십시오.

자원 및 정책 소유권

모든 정책은 조직 엔티티에서 소유합니다. 모든 액세스 제어 자원도 보통 조직 엔티티라고 하는 소유자를 가지고 있습니다. 예를 들어, 주문은 주문이 제출된 상점을 소유하는 조직에서 소유합니다. 사용자는 또한 자신의 자원을 소유할 수 있습니다. 예를 들어, 등록된 사용자는 자신의 특성을 소유합니다. 자원 및 액세스 제어 정책의 소유권은 특정 자원에 적용할 정책을 판별할 때 중요합니다. 주어진 자원에 대해 소유 조직 엔티티와 해당 소유자의 최상위 엔티티에 속하는 정책이 적용됩니다.

액세스 제어 정책 유형

두 가지 유형의 액세스 제어 정책은 다음과 같습니다.

- 표준 정책
- 템플리트 정책

표준 정책

표준 정책에는 고정 소유자가 있습니다. 예를 들어, 표준 정책을 판매자 조직에서 소유할 경우 그 정책은 판매자 조직에서 소유하는 자원과, 해당 최하위 조직 엔티티에서 소유하는 자원(존재할 경우)에만 적용됩니다. 루트 조직은 WebSphere Commerce에서 다른 모든 조직의 최상위 조직이므로 루트 조직(구성원 ID = -2001)에서 소유하는 정책은 정의에 따라 사이트의 모든 자원에 적용됩니다. 그러므로 루트 조직에서 소유하는 표준 정책은 간혹 사이트 레벨 정책으로 언급됩니다.

루트 조직에서 소유하지 않는 표준 정책을 조직 레벨 정책이라고 하는데, 이는 사이트 전반에 적용되지 않고 정책 소유자나 해당 최하위 조직 엔티티에서 소유하는 자원에만 적용되기 때문입니다. 상점 운영자는 자신의 조직 엔티티와 해당되는 최하위 조직 엔티티에 대한 정책을 관리할 수 있습니다. 사이트 운영자는 모든 정책을 수정할 수 있습니다.

템플리트 정책

템플리트 정책에는 동적 소유자가 있습니다. 템플리트 정책은 자원과 해당 최상위 조직 엔티티를 소유하는 조직 엔티티에 동적으로 적용됩니다. 예를 들어, 루트 조직 아래에 10개의 조직이 있고 각 조직에서는 상점 운영자가 역할을 수행하는 조직에서 소유하는 자원만 수정할 수 있습니다. 이를 설정하는 방법은 두 가지입니다.

1. 액세스하는 자원에 따라 10개의 조직 중 임의의 조직에 동적으로 적용할 하나의 템플리트 정책을 갖습니다. 템플리트 정책에서 액세스 그룹에 대한 기준도 동적이 될 수 있습니다. 예를 들어, 사용자가 조직 3에서 소유하는 자원에 액세스하려고 하고, 템플리트 정책의 소유자가 동적으로 조직 3으로 변경되며, 액세스 그룹 역시 자체 범위를 동적으로 조직 3으로 변경할 경우, 사용자는 조직 3에 대해 상점 운영자 역할을 수행해야 합니다.
2. 10개의 정책을 가지고 있습니다. 각 정책은 10개의 조직 중 하나에서 소유합니다. 조직 1에 대한 액세스 그룹은 사용자가 조직 1에 대한 상점 운영자 역할을 수행해야 함을 지정합니다. 조직 2에 대한 액세스 그룹은 사용자가 조직 2에 대한 상점 운영자 역할을 수행해야 함을 지정하는 등 이후 조직도 이와 마찬가지 방식입니다.

첫 번째 솔루션의 장점은 실제 정책 사본이 단 하나이지만, 논리적 사본은 10개라는 점입니다. 템플리트 정책은 사이트 운영자가 관리할 수 있습니다.

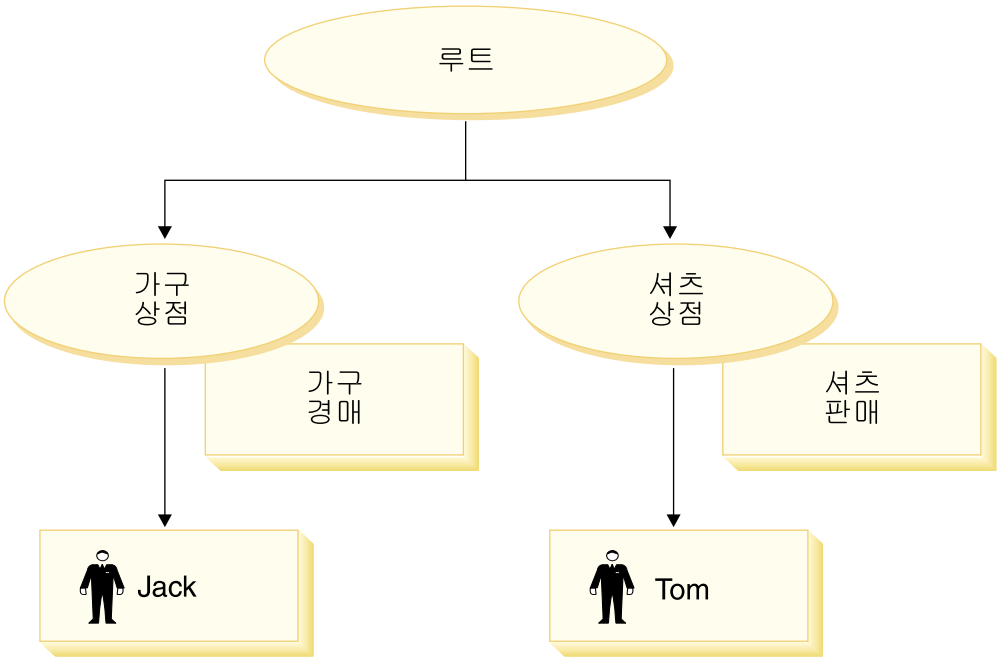
템플리트 정책 대체: 템플리트 정책의 또다른 기능은 지정된 조직 엔티티에 대해 대체가 가능하다는 것입니다. 위의 예로 돌아가서, 11번째 조직 엔티티가 WebSphere Commerce 사이트에 추가되지만 이 최신 조직 엔티티가 위의 템플리트 정책을 적용하려고 하지 않는 경우, 이를 지정할 방법이 있습니다. 항목을 ACORGPOL 테이블에 추가하여, 템플리트 정책의 정책 ID와 11번째 조직의 조직 엔티티 ID를 지정해야 합니다. 이는 상점 운영자가 템플리트 정책을 삭제 또는 갱신할 때 특정 조직의 컨텍스트에서 WebSphere Commerce 관리 콘솔을 통해서도 수행할 수 있습니다.

루트 조직의 최하위 조직에 대한 템플리트 정책을 대체해도 여전히 템플리트 정책은 루트 조직 레벨에서 적용됩니다. 템플리트 정책을 최하위 조직 레벨에서 보다 제한적인 정책으로 대체하는 경우, 루트 조직 레벨에서도 템플리트 정책을 대체해야 합니다. 루트 조직에 대한 템플리트 정책을 대체하는 유일한 방법은 데이터베이스를 통해 다음과 같은 SQL을 실행하는 것입니다.

```
insert into ACORGPOL (acpolicy_id, member_id) values ( (select acpolicy_id from
ACPOLICY where policyname = 'policyToOverride'), -2001)
```

액세스 제어 레벨

WebSphere Commerce에는 광범위하게 두 가지 액세스 제어 레벨인 명령 레벨(역할 기반이라고도 함)과 자원 레벨(인스턴스 레벨이라고도 함)이 있습니다.



명령 레벨 또는 역할 기반 액세스 제어

명령 레벨 또는 역할 기반 액세스 제어는 정밀하지 않은 액세스 제어입니다. 이 액세스 제어는 "누가 무엇을 수행할 수 있는지"를 판별합니다. 역할 기반 액세스 제어를 사용할 경우, 특정 역할의 모든 사용자가 특정 명령을 실행할 수 있음을 지정할 수 있습니다. 판매자가 판매자 명령을 실행할 수 있는 액세스 제어 정책을 고려해 보십시오. 이 정책에서 판매자 명령 중 하나는 `ModifyAuction` 명령입니다. 위 그림에서 Jack과 Tom은 모두 판매자이므로 둘 다 경매를 수정할 수 있습니다.

역할 기반 액세스 제어는 제어기 명령과 보기에 사용합니다. 이러한 유형의 액세스 제어는 명령이 작용하는 데이터 자원을 고려하지 않습니다. 단지 사용자가 특정 제어기 명령 또는 보기를 실행할 수 있는지를 판별합니다.

이러한 레벨의 액세스 제어는 필수이므로 런타임에 의해 시행됩니다. 모든 제어기 명령은 명령 레벨 액세스 제어에 의해 보호해야 합니다. 또한 직접 호출할 수 있거나 다른 명령을 통한 경로 재지정에 의해 실행할 수 있는(보기로 보내어 실행되는 것과 반대로) 보기는 명령 레벨 액세스 제어에 의해 보호해야 합니다.

제어기 명령에 대한 명령 레벨 액세스 제어: 제어기 명령을 실행할 때마다 명령 자원에서 Execute 조치를 수행할 수 있는 권한을 사용자에게 부여하는 액세스 제어 정책이 존재해야 합니다. 자원은 제어기 명령의 인터페이스 이름입니다. 액세스 그룹은 보통 단일 역할에 맞게 조정됩니다. 예를 들어, 회계 담당 역할을 가지고 있는 사용자는 AccountRepresentativesCmdResourceGroup 자원 그룹에서 모든 명령을 실행할 수 있도록 지정할 수 있습니다.

보기에 대한 명령 레벨 액세스 제어: URL에서 직접 보기를 호출하거나, 보기가 명령을 통한 경로 재지정의 결과일 경우, 그 보기는 액세스 제어 정책을 가지고 있어야 합니다. 그러한 정책은 ACACTION 테이블에서 조치로 viewname이 지정되어 있어야 합니다. 그런 다음 이 조치는 ACACTACTGP 테이블을 사용하여 조치 그룹과 연관되어야 합니다. 이 조치 그룹은 ACPOLICY 테이블에서 해당되는 명령 레벨 정책에서 참조되어야 합니다.

인스턴스 레벨 또는 자원 레벨 액세스 제어

인스턴스 레벨 또는 자원 레벨 액세스 제어 정책은 정교한 액세스 제어를 제공하여 누가 어떤 자원에 대해 어떤 명령을 수행할 수 있는지를 판별합니다. 판매자가 경매를 수정할 수 있는 역할 기반 액세스 제어 정책에 대한 이전 예에서 역할 기반 액세스 제어를 보다 세부적으로 조정하여 역할을 수행하는 조직이 소유하는 경매를 판매자가 수정할 수 있습니다. 27에서 Jack은 판매자 조직 1의 판매자 역할을 가지고 있습니다. Tom은 판매자 조직 2의 판매자 역할을 가지고 있습니다. Jack은 가구 상점에서 가구 경매를 작성합니다. Tom은 셔츠 상점에서 셔츠 경매를 작성합니다. Jack은 가구 경매를 수정할 수 있지만 셔츠 경매는 수정할 수 *없습니다*. Tom은 셔츠 경매를 수정할 수 있지만, 가구 경매는 수정할 수 *없습니다*.

요약하면, 먼저 시스템은 명령 레벨 액세스 확인을 수행합니다. 사용자가 명령을 실행할 수 있으면, 후속 자원 레벨 액세스 제어 정책이 수행되어 사용자가 문제의 자원에 액세스할 수 있는지 판별합니다.

자원 레벨 액세스 제어는 명령 및 데이터 bean에 적용됩니다.

명령에 대한 자원 레벨 액세스 제어: 명령 레벨 액세스 제어 확인이 완료된 후, 액세스가 부여되면 다음 두 경우 중 하나에서 자원 레벨 확인이 수행됩니다.

- 명령이 getResources()를 구현합니다. 이 메소드는 현재 조치에 대해 확인해야 하는 자원의 인스턴스를 지정합니다. 여기서 명령은 이제 조치입니다. WebSphere Commerce Runtime은 현재 사용자가 getResources()에 의해 지정된 모든 자원

에 대한 액세스를 갖도록 합니다. 기본적으로 getResources()는 널(Null)값을 리턴합니다. 즉, 어떤 자원 레벨 확인도 수행하지 않습니다.

- 명령이 checkIsAllowed(Object Resource, String Action)를 호출합니다. 이 경우, 명령 작성자는 런타임에 의해 getResources()가 호출될 때 확인해야 하는 자원을 모르므로, 명령이 필요에 따라 이 checkIsAllowed() 메소드를 호출하여 현재 조치 및 자원 쌍에 대한 권한이 있는지 판별할 수 있습니다. 조치는 대개 현재 명령의 인터페이스 이름입니다. 이 메소드가 호출될 때, 액세스가 거부되면 ECApplicationException(ECMessage._ERR_USER_AUTHORITY, ..) 예외가 발생합니다.

데이터 bean에 대한 자원 레벨 액세스 제어: 위에 설명된 대로, 보기는 보통 역할을 기반으로 하는 명령 레벨 정책에 의해 보호됩니다. 예를 들어, 명령 레벨 정책은 판매자 관리자가 특정 보기에 대한 액세스는 갖도록 지정할 수 있습니다. 이는 사용자가 판매자 관리자 역할을 수행하는 조직에 JSP의 데이터 bean이 모두 관련되어 있는지 추가로 확인할 경우에 종종 필요합니다. 이것은 보호(직접 또는 간접적인)가 필요한 모든 데이터 bean이 Delegator 인터페이스를 구현하도록 하여 수행됩니다. 이러한 데이터 bean은 번갈아 Protectable 인터페이스를 구현하는 1차(독립) 데이터 bean에게 위임합니다. 1차 데이터 bean은 자체에게 위임하므로 두 인터페이스를 구현합니다. 그러면 데이터 bean 관리자의 activate() 메소드를 사용하여 데이터 bean을 호출할 때마다, WebSphere Commerce Runtime은 현재 사용자에게 1차 데이터 bean 자원에 대한 Display 조치를 수행할 수 있는 권한을 부여하는 정책이 있는지 확인합니다.

액세스 제어로 권한 없는 조치를 금지하는 방법

이 절에서는 사용자가 권한을 부여 받은 조치만 수행할 수 있도록 정책 기반 액세스 제어가 작동하는 방법에 대해 설명합니다.

사용자 초기화 조치 수행 전에 권한 확인

*정책 관리자*는 현재 사용자가 지정된 자원에 대해 지정된 조치를 실행할 수 있는지 여부를 판별하는 액세스 제어 구성요소입니다. 액세스 제어 정책은 XML 포맷으로 지정됩니다. 인스턴스 작성 중에 기본 정책은 자동으로 해당되는 데이터베이스 테이블에 로드됩니다. WebSphere Commerce Application Server가 시작되면 액세스 제어 정보는 정책 관리자가 사용자 권한을 확인하도록 호출될 때 이를 신속하게 수행할 수 있도록 메모리에 캐시됩니다. 액세스 제어 정보가 WebSphere Commerce 관리 콘솔을 통하거나 XML 정책 데이터를 로드하여 데이터베이스에서 변경되면 액세스 제어 캐시를 갱신해야 합니다. 이것은 WebSphere Commerce 관리 콘솔에 있는 액세스 제어 레지스트리를 갱신하여 수행할 수 있습니다. WebSphere Commerce를 재시작하면 캐시도 갱신됩니다.

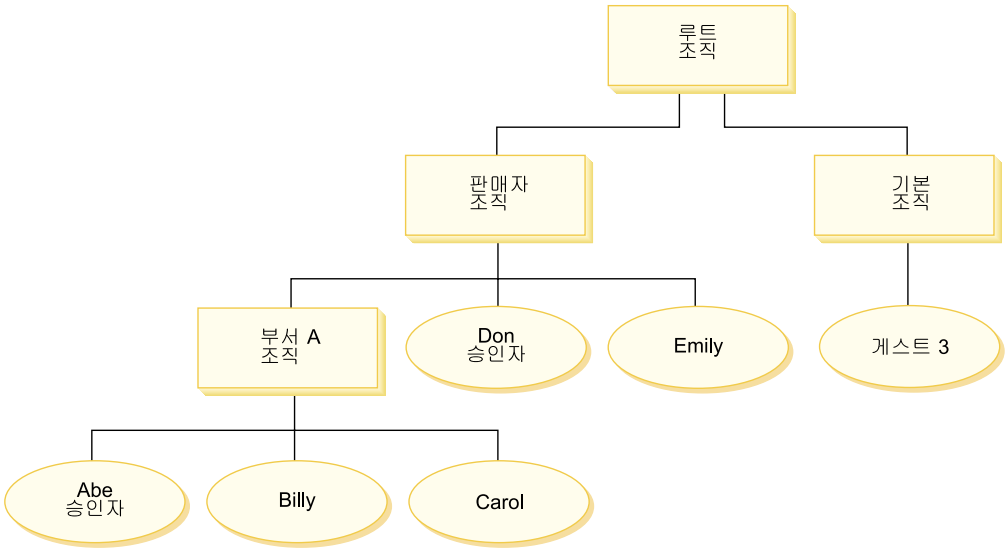
사용자가 액세스 제어 보호 조치를 수행하려고 할 때, 사용자가 권한을 가지고 있는지 확인하기 위해 액세스 제어 확인이 수행됩니다. 정책 관리자는 자원을 소유하는 조직에

적용되는 모든 액세스 제어 정책을 찾습니다. 그런 후 찾은 정책을 확인하여 사용자에게 대상 자원에서 조치를 수행할 수 있는 권한이 부여되었는지 확인합니다. 그러한 최소 하나의 정책이 있으면 정책 관리자는 액세스를 부여하고, 그렇지 않으면 액세스를 거부합니다.

액세스 제어 정책 확인

이 절은 액세스 제어 정책 확인에 대한 지침으로 사용할 수 있습니다. 이 절에서는 시나리오가 제시되어 표준 및 템플리트 액세스 제어 정책을 확인하는 방법에 대한 예를 자세히 안내합니다. 각 절은 관련 정책에 대한 설명 및 각 정책을 사용하는 시나리오로 시작합니다. 표준 및 템플리트 정책에 대한 자세한 정보는 25 페이지의 『액세스 제어 정책 유형』을 참조하십시오.

다음 도표는 시나리오를 그림으로 보여줍니다.



조직 계층

도표에서 다음 4개의 조직이 사이트에 있음을 볼 수 있습니다.

- 루트 조직
- 판매자 조직
- 기본 조직
- 부서 A 조직

그림에서 알 수 있듯이 루트 조직은 판매자 조직과 기본 조직의 상위입니다. 판매자 조직은 부서 A 조직의 상위입니다.

사용자

도표에서 Don과 Emily는 판매자 조직에 등록되어 있습니다. Abe, Billy, Carol은 부서 A 조직에 등록되어 있습니다. 게스트 3은 등록되어 있지 않지만 액세스 제어를 위해 암시적으로 기본 조직에 속해 있습니다.

역할

Don은 판매자 조직에 대한 승인자 역할이 있습니다. Abe는 부서 A 조직에 대한 승인자 역할이 있습니다.

액세스 그룹

다음과 같은 액세스 그룹을 이 시나리오에서 사용합니다.

- 등록된 사용자: 이 그룹은 등록된 모든 사용자를 암시적으로 포함합니다.
- 판매자에 대한 승인자: 이 그룹은 판매자 조직에 대한 승인자 역할이 있는 모든 사용자를 암시적으로 포함합니다.
- 부서 A에 대한 승인자: 이 그룹은 부서 A 조직에 대한 승인자 역할을 가진 모든 사용자를 암시적으로 포함합니다.

문서

문서 오브젝트는 보호되는 자원입니다. 문서의 소유자는 문서가 작성된 조직으로 정의됩니다.

문서 갱신에 대한 액세스 제어 요구사항

다음은 문서 갱신에 대한 액세스 제어 요구사항입니다.

1. 등록된 사용자는 작성한 문서를 갱신할 수 있습니다.
2. 부서 A에 대한 승인자는 판매자가 소유한 문서가 아닌 부서 A가 소유한 문서를 갱신할 수 있습니다. 판매자 조직에 대한 승인자는 부서 A와 판매자 조직이 모두 소유한 문서를 갱신할 수 있습니다.

표준 정책 확인

이 절에서는 표준 정책과 이를 확인하는 시나리오에 대해 자세히 안내합니다.

문서 갱신과 관련된 액세스 제어 정책

다음은 정책 형식과 문서 갱신과 관련된 액세스 제어 정책입니다.

정책 형식: [액세스 그룹, 조치 그룹, 자원 그룹, 관계]

정책 1:

[등록된 사용자, 실행 명령 조치 그룹, 문서 갱신
자원 그룹, -]

이것은 루트 조직이 소유하는 표준 역할 기반 정책입니다. 이 정책에서 등록된 사용자는 문서 갱신 명령을 실행할 수 있습니다.

정책 2:

[등록된 사용자, 문서 갱신 조치 그룹, 문서, 작성자]

이것은 루트 조직이 소유하는 표준 자원 레벨 정책입니다. 이 정책에서 등록된 사용자는 문서의 작성자인 경우 해당 문서를 갱신할 수 있습니다.

정책 3:

[판매자에 대한 승인자, 문서 갱신 조치 그룹, 문서, -]

이것은 판매자 조직이 소유하는 표준 자원 레벨 정책입니다. 이 정책에서 판매자에 대한 승인자는 판매자가 소유하는 문서를 갱신할 수 있습니다.

정책 4:

[부서 A에 대한 승인자, 문서 갱신 조치 그룹, 문서, -]

이것은 부서 A 조직이 소유하는 표준 자원 레벨 정책입니다. 이 정책에서 부서 A에 대한 승인자는 부서 A가 소유하는 문서를 갱신할 수 있습니다.

시나리오

시나리오 1: Billy가 자신의 문서를 갱신하려고 시도함: 다음은 이 시나리오에 대한 액세스 제어 확인입니다.

명령 - 레벨 확인:

1. 지정된 상점 ID가 없으므로 명령의 소유자가 루트 조직으로 설정됩니다. 따라서 루트 조직이 소유한 정책만 사용자가 명령 레벨 액세스를 가지고 있는지 여부를 확인하는데 사용됩니다. 정책 1과 2가 루트 조직에 의해 소유됩니다.
2. Billy가 등록된 사용자 액세스 그룹의 구성원이고 문서 갱신 명령 자원에서 실행 조치를 수행하므로 정책 1이 액세스를 부여합니다.

자원 - 레벨 확인:

1. 문서 갱신 명령은 문서 자원이 보호되어야 함을 지정합니다. Billy의 문서는 부서 A가 소유합니다. 따라서 부서 A와 해당 상위 조직이 소유한 정책(정책 1, 2, 3, 4)만 적용됩니다.
2. Billy가 등록된 사용자 액세스 그룹의 구성원이고 문서 자원에서 문서 갱신 명령 조치를 수행하며 문서와 작성자 관계를 충족하므로 정책 2가 액세스를 부여합니다.

Billy는 명령 레벨과 자원 레벨 액세스 제어 확인을 모두 통과했으므로 자신의 문서를 갱신할 수 있습니다.

시나리오 2: Don이 Carol의 문서를 갱신하려고 시도함: 다음은 이 시나리오에 대한 액세스 제어 확인입니다.

명령 - 레벨 확인:

1. 지정된 상점 ID가 없으므로 명령의 소유자가 루트 조직으로 설정됩니다. 따라서 루트 조직이 소유한 정책만 사용자가 명령 레벨 액세스를 가지고 있는지 여부를 확인하는데 사용됩니다. 정책 1과 2가 루트 조직에 의해 소유됩니다.
2. Don이 등록된 사용자 액세스 그룹의 구성원이고 문서 갱신 명령 자원에서 실행 조치를 수행하므로 정책 1이 액세스를 부여합니다.

자원 - 레벨 확인:

1. 문서 갱신 명령은 문서 자원이 보호되어야 함을 지정합니다. Carol의 문서는 부서 A가 소유합니다. 따라서 부서 A와 해당 상위 조직이 소유한 정책(정책 1, 2, 3, 4)만 적용됩니다.
2. Don이 판매자에 대한 승인자 액세스 그룹의 구성원이고 문서 자원에서 문서 갱신 명령 조치를 수행하므로 정책 4가 액세스를 부여합니다.

Don은 명령 레벨과 자원 레벨 액세스 제어 확인을 모두 통과했으므로 Carol의 문서를 갱신할 수 있습니다.

시나리오 3: Abe가 Emily의 문서를 갱신하려고 시도함: 다음은 이 시나리오에 대한 액세스 제어 확인입니다.

명령 - 레벨 확인:

1. 지정된 상점 ID가 없으므로 명령의 소유자가 루트 조직으로 설정됩니다. 따라서 루트 조직이 소유한 정책만 사용자가 명령 레벨 액세스를 가지고 있는지 여부를 확인하는데 사용됩니다. 정책 1과 2가 루트 조직에 의해 소유됩니다.
2. Abe가 등록된 사용자 액세스 그룹의 구성원이고 문서 갱신 명령 자원에서 실행 조치를 수행하므로 정책 1이 액세스를 부여합니다.

자원 - 레벨 확인:

1. 문서 갱신 명령은 문서 자원이 보호되어야 함을 지정합니다. Emily 문서는 판매자 조직이 소유합니다. 따라서 판매자 조직과 해당 상위 조직이 소유한 정책(정책 1, 2, 3)만 적용됩니다.
2. Abe는 판매자에 대한 승인자 액세스 그룹의 구성원이 아니므로 정책 3은 액세스를 부여하지 않습니다.

Abe는 명령 레벨 확인을 통과했지만 자원 레벨 액세스 제어 확인에 실패했으므로 Emily의 문서를 갱신할 수 없습니다.

시나리오 4: 게스트 3이 자신의 문서를 갱신하려고 시도함: 다음은 이 시나리오에 대한 액세스 제어 확인입니다.

명령 - 레벨 확인:

1. 지정된 상점 ID가 없으므로 명령의 소유자가 루트 조직으로 설정됩니다. 따라서 루트 조직이 소유한 정책만 사용자가 명령 레벨 액세스를 가지고 있는지 여부를 확인하는데 사용됩니다. 정책 1과 2가 루트 조직에 의해 소유됩니다.
2. 게스트 3은 등록된 사용자 액세스 그룹의 구성원이 아니므로 정책 1은 액세스를 부여하지 않습니다.

자원 - 레벨 확인:

1. 명령 레벨 확인에 실패했으므로 자원 레벨 확인은 수행되지 않습니다.

게스트 3이 명령 레벨 확인에 실패했으므로 자신의 문서를 갱신할 수 없습니다.

템플리트 정책 확인

이 예는 이전 시나리오를 기초로 합니다.

문서 갱신과 관련된 액세스 제어 정책

템플리트 정책을 확인할 때 표준 정책 확인에 사용된 액세스 제어 정책 1과 2는 여전히 적용되지만 표준 정책 3과 4는 템플리트 정책 5로 대체됩니다. 정책 1과 2에 대한 자세한 정보는 31 페이지의 『표준 정책 확인』을 참조하십시오.

정책 5:

[조직에 대한 승인자, 문서 갱신 조치 그룹, 문서, -]

이 정책은 템플리트 자원 레벨 정책입니다. 문서를 소유하는 조직에 대한 승인자는 문서를 갱신할 수 있습니다.

또한 이 템플리트 정책에서 사용할 매개변수화된 새 액세스 그룹이 필요합니다. 다음 액세스 그룹이 이 시나리오에 추가되었습니다.

- 조직에 대한 승인자: 이 그룹은 ? 조직에 대한 승인자 역할이 있는 모든 사용자를 암시적으로 포함합니다. (템플리트 정책은 런타임시 적용되므로 ? 매개변수는 정책 소유자로 동적 변경됩니다.)

시나리오

다음 시나리오는 정책 1, 2, 5만 사용합니다.

시나리오 1: Don이 Carol의 문서를 갱신하려고 시도함: 다음은 이 시나리오에 대한 액세스 제어 확인입니다.

명령 - 레벨 확인:

1. 지정된 상점 ID가 없으므로 명령의 소유자가 루트 조직으로 설정됩니다. 따라서 루트 조직이 소유한 정책만 사용자가 명령 레벨 액세스를 가지고 있는지 여부를 확인하는데 사용됩니다. 정책 1과 2가 루트 조직에 의해 소유됩니다. 정책 확인 중에 템

플리트 정책은 자원을 소유하는 조직으로, 이후에는 해당 조직의 상위로 소유권을 동적 변경합니다. 따라서 정책 5도 적용됩니다.

2. Don이 등록된 사용자 액세스 그룹의 구성원이고 문서 갱신 명령 자원에서 실행 조치를 수행하므로 정책 1이 액세스를 부여합니다.

자원 - 레벨 확인:

1. 문서 갱신 명령은 문서 자원이 보호되어야 함을 지정합니다. Carol의 문서는 부서 A가 소유합니다. 따라서 부서 A와 해당 상위 조직이 소유한 정책(정책 1)만 적용됩니다. 정책 확인 중에 템플리트 정책은 자원을 소유하는 조직으로, 이후에는 해당 조직의 상위로 소유권을 동적 변경합니다. 따라서 정책 5도 적용됩니다.
2. 템플리트 정책 5는 먼저 자원을 소유하는 조직(부서 A)에 적용됩니다. 이 때 정책 5는 기본적으로 다음 정책 5a와 같이 작동합니다.

   [부서 A에 대한 승인자, 문서 갱신 조치 그룹, 문서, -] 부서 A가 소유하는 표준 자원 레벨 정책.
3. Don은 부서 A에 대한 승인자 액세스 그룹의 구성원이 아니므로 정책 5a는 액세스를 부여하지 않습니다.
4. 다음으로 템플리트 정책 5는 부서 A의 상위 조직인 판매자 조직에 적용됩니다. 이 때 정책 5는 기본적으로 다음 정책 5b와 같이 작동합니다.

   [판매자에 대한 승인자, 문서 갱신 조치 그룹, 문서, -] 판매자가 소유하는 표준 자원 레벨 정책.
5. Don이 판매자에 대한 승인자 액세스 그룹의 구성원이고 문서 자원에서 문서 갱신 명령 조치를 수행하므로 정책 5b가 액세스를 부여합니다.

Don은 명령 레벨과 자원 레벨 액세스 제어 확인을 모두 통과했으므로 Carol의 문서를 갱신할 수 있습니다.

시나리오 2: Abe가 Emily의 문서를 갱신하려고 시도함: 다음은 이 시나리오에 대한 액세스 제어 확인입니다.

명령 - 레벨 확인:

1. 지정된 상점 ID가 없으므로 명령의 소유자가 루트 조직으로 설정됩니다. 따라서 루트 조직이 소유한 정책만 사용자가 명령 레벨 액세스를 가지고 있는지 여부를 확인하는데 사용됩니다. 정책 1과 2가 루트 조직에 의해 소유됩니다. 정책 확인 중에 템플리트 정책은 자원을 소유하는 조직으로, 이후에는 해당 조직의 상위로 소유권을 동적 변경합니다. 따라서 정책 5도 적용됩니다.
2. Abe가 등록된 사용자 액세스 그룹의 구성원이고 문서 갱신 명령 자원에서 실행 조치를 수행하므로 정책 1이 액세스를 부여합니다.

자원 - 레벨 확인:

1. 문서 갱신 명령은 문서 자원이 보호되어야 함을 지정합니다. Emily 문서는 판매자 조직이 소유합니다. 따라서 판매자와 해당 상위 조직이 소유한 정책(정책 1, 2)만 적용됩니다. 정책 확인 중에 템플리트 정책은 자원을 소유하는 조직으로, 이후에는 해당 조직의 상위로 소유권을 동적 변경합니다. 따라서 정책 5도 적용됩니다.
2. 템플리트 정책 5는 먼저 자원을 소유하는 조직(판매자 조직)에 적용됩니다. 이 때 정책 5는 기본적으로 다음 정책 5a와 같이 작동합니다.

   [판매자에 대한 승인자, 문서 갱신 조치 그룹, 문서, -] 판매자가 소유하는 표준 자원 레벨 정책.
3. Abe는 판매자에 대한 승인자 액세스 그룹의 구성원이 아니므로 정책 5a는 액세스를 부여하지 않습니다.
4. 다음으로 템플리트 정책 5는 판매자의 상위 조직인 루트 조직에 적용됩니다. 이 때 정책 5는 기본적으로 다음 정책 5b와 같이 작동합니다.

   [루트에 대한 승인자, 문서 갱신 조치 그룹, 문서, -] 루트가 소유하는 표준 자원 레벨 정책.
5. Abe는 루트에 대한 승인자 액세스 그룹의 구성원이 아니므로 정책 5b는 액세스를 부여하지 않습니다.
6. 루트 조직은 상위 조직을 갖지 않으므로 템플리트 정책 5는 완전히 확인되었습니다.

Abe는 명령 레벨 확인을 통과했지만 자원 레벨 액세스 제어 확인에 실패했으므로 Emily의 문서를 갱신할 수 없습니다.

정책 세부사항

이제 액세스 제어 정책의 기본 구조와 정책 유형을 이해하였으므로 여러 가지 예를 이용하여 기본 정책 중 하나를 자세히 살펴 보겠습니다. 살펴볼 정책은 다음과 같습니다.

`AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource`

주: 이 정책은 자원 레벨 정책입니다. 정책 유형은 템플리트입니다.

첫 번째 예에서는 WebSphere Commerce 관리 콘솔을 이용하여 정책을 읽고 각 부분을 식별하는 법과 정책의 의미를 이해하게 됩니다. 두 번째 예에서는 같은 정보가 코드에서는 어떻게 보이는 지에 대한 이해를 돕기 위해서 XML 내의 정책을 살펴봅니다.

세 번째 예에서는 한 걸음 더 나아가서 정책간의 관계를 이해하게 됩니다. 정책간의 종속성을 이해하는 것은 액세스 제어 정책을 변경하거나 새로 작성하는데 중요한 전제 조건입니다.

예제 1: 정책 읽기

이번 예에서는 WebSphere Commerce 관리 콘솔을 이용하여 정책을 찾고 이를 정의하는 부분들을 식별합니다. 또한 이 부분들을 이용하여 정책의 일반적 설명을 구성합니다.

관리 콘솔에서 정책 보기

1. WebSphere Commerce 관리 콘솔에 로그인합니다. 액세스 관리 메뉴에서 **정책**을 선택합니다.
2. 보기 드롭 다운 메뉴가 사용자의 조직으로 설정되어 있는지 확인합니다.
3. 정책 페이지에서 정책 목록들을 화면이동하여 다음 정책을 위치 지정합니다.

   AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource

   이동 막대뿐 아니라 **처음**, **이전**, **다음** 및 **마지막** 링크를 이용하여 정책 목록을 화면 이동할 수 있습니다.

정책 부분 보기

1. 옆에 있는 상자를 눌러 정책을 선택하고 **조치 그룹 표시**를 누릅니다.
2. 조치 그룹 페이지에는 조치 그룹, AuctionManage가 표시됩니다. 이것은 정책과 연관된 조치 그룹입니다. AuctionManage를 선택하고 **조치 표시**를 누릅니다.
3. 다음 페이지에는 AuctionManage 조치 그룹에 포함된 조치, 명령어 목록이 표시됩니다.
   - com.ibm.commerce.negotiation.commands.CloseBiddingCmd
   - com.ibm.commerce.negotiation.commands.DeleteAuctionCmd
   - com.ibm.commerce.negotiation.commands.ModifyAuctionCmd

   AuctionManage에는 경매 종료(CloseBiddingCmd), 경매 삭제,(DeleteAuctionCmd) 및 경매 수정(ModifyAuctionCmd)이 포함됩니다. 명령어에 대한 자세한 정보는 온라인 도움말 문서의 참조서 절을 참조하십시오.

   또한 정책 페이지의 **조치 표시**를 눌러 동일한 조치 목록을 볼 수 있음을 주목하십시오.
4. 정책 페이지로 돌아가려면, 아무 조치나 선택한 다음 **정책 표시**를 누릅니다.
5. 다시 정책을 선택하고, 이번에는 **구성원 그룹 표시**를 눌러 정책이 적용되는 구성원(액세스) 그룹을 봅니다.
6. 구성원(액세스) 그룹 이름을 기록합니다. 여기에서 구성원(액세스) 그룹은 AuctionAdministratorsForOrg입니다.
7. 액세스 관리 메뉴에서 **액세스 그룹**을 선택합니다.
8. AuctionAdministratorsForOrg를 찾습니다. 이를 선택하고 **변경**을 누릅니다.

9. **기준**을 누릅니다. 기준 페이지에서 선택된 역할 및 조직을 보십시오. 다음 역할들이 표시될 것입니다.
   - 판매자-조직용
   - 상품 관리자-조직용
   - 구매자(판매측)-조직용
   - 카테고리 관리자-조직용

   경매 자원을 소유하는 조직에 대해 이 역할들 중 하나에 지정된 사용자는 모두 AuctionAdministratorsForOrg 액세스 그룹의 일원입니다.
10. 기준 페이지는 변경하지 않은 채로 두십시오. 액세스 관리 메뉴에서 **정책**을 다시 선택합니다. 다음 정책을 찾으십시오.

    AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
11. 정책을 선택하고 **자원 표시**를 누릅니다. 자원 페이지에는 com.ibm.commerce.negotiation.objects.Auction 자원이 표시됩니다. 이는 조치 그룹 활동에 나열된 조치들에 대한 자원입니다. 이 경우 자원은 경매입니다. 정책 페이지에서 **자원 그룹 표시**를 누르고 개별 자원을 드릴 다운하여 이러한 동일한 목록에 액세스할 수 있습니다.
12. 이제 액세스 관리 메뉴에서 **정책**을 선택하고 다음 정책을 찾으십시오.

    AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
13. 정책을 선택하고 **변경**을 누릅니다. 정책 변경 페이지에서 **관계** 아래의 드롭 다운 메뉴를 봅니다. 관계가 없음으로 설정되어 있음을 주목하십시오. 이는 정책이 아무 관계도 가지고 있지 않음을 의미합니다.
14. 대화 상자에서 **취소** 및 **확인**을 누릅니다.

정책의 의미 이해

이제 정책의 개별 요소들을 식별하였으므로, 이를 종합하여 정책이 수행하는 작업을 이해할 수 있습니다. 먼저, 정책은 AuctionAdministratorsForOrg 그룹에 속한 모든 사용자에게 적용됨을 알고 있습니다. **구성원 그룹 표시**를 통해 학습하였습니다. 여기에서 액세스 관리 메뉴를 사용하여 액세스 그룹 페이지로 이동한 다음 액세스 그룹이 다음 역할을 포함하고 있는 것을 살펴보았습니다. 판매자, 상품 관리자, 구매자(판매측) 및 카테고리 관리자. 종합하면, 이 4가지 역할 중 하나를 가진 사용자는 경매 운영자라고 부를 수 있습니다.

또한 조치 그룹에는 수정, 유찰 및 경매 종료에 대한 명령이 포함되고 자원 그룹에는 관리 중인 경매 자원만 포함된다는 것을 알고 있습니다. 정책 페이지의 **조치 표시** 및 **자원 표시**를 눌러 세부 레벨로 들어가면 알 수 있습니다. 마지막으로 정책에는 액세스 그룹과 자원간의 관계가 포함되어 있지 않다는 것을 알 수 있습니다.

모든 것을 종합해 볼 때 이 정책은 운영자가 경매를 소유하는 조직의 역할을 수행하는 한 경매 운영자로 하여금 수정, 유찰, 경매 종료같이 경매 자원에서 경매를 관리하는 것과 연관된 모든 활동들을 수행할 수 있게 한다고 결론을 내릴 수 있습니다.

정책의 이름을 보면 그 의미를 알 수 있습니다. 이번 예제에서는, 정책의 이름이 AuctionAdministrator라는 지정된 사용자 그룹으로 시작됩니다. ForOrg는 조직에 적용되는 정책을 표시합니다. AuctionManageCommands는 조치 그룹을 설명하고, AuctionResource는 자원 그룹을 설명합니다.

예제 2: XML에서 정책 읽기

기본 액세스 제어 정책은 인스턴스 작성시 데이터베이스에 로드된 XML 파일에 저장되어 있습니다. WebSphere Commerce 관리 콘솔에서 정책을 볼 때는 데이터베이스에 저장된 정보를 보고 변경할 수 있는 인터페이스를 사용하고 있는 것입니다. 데이터베이스의 정보는 정책 관리자가 액세스 제어를 확인할 때 사용합니다. 데이터베이스 정보가 XML 파일보다 최신인 경우 추출기 도구를 사용하여 데이터베이스에서 XML 파일로 액세스 제어 정책 정보를 추출할 수 있습니다.

대부분의 경우 WebSphere Commerce 관리 콘솔 사용자 인터페이스를 사용하여 정책을 관리합니다. 하지만, XML에서 정책을 보고자 하거나 고급 수정을 하려는 경우, XML 파일의 정책은 다음과 같이 보입니다.

```
<!-- AuctionAdministrators
manage Auctions (Retract/delete auction,
Modify auction, Close Auction)
-->
<Policy
Name="AuctionAdministratorsForOrgExecuteAuctionManage
CommandsOnAuctionResource"
OwnerID="RootOrganization"
UserGroup="AuctionAdministratorsForOrg"
ActionGroupName="AuctionManage"
ResourceGroupName="AuctionDataResourceGroup"
PolicyType="template">
</Policy>
```

여기서, 정책은 다음과 같이 정의됩니다.

Name: 정책의 이름.

OwnerID: 정책이 적용되는 조직

UserGroup: 액세스 그룹

ActionGroupName: 조치 그룹

ResourceGroupName: 자원 그룹

PolicyType: 사이트 레벨, 템플리트 또는 조직과 같은 정책 유형

모든 기본 액세스 제어 정책은 defaultAccessControlPolicies.xml이라는 파일에 있으며 이 파일은 다음 디렉토리에 위치합니다.

X:*installation_directory*\xml\policies\xml.

주: 각 기본 액세스 제어 파일에 대한 설명은 defaultAccessControlPolicies_*locale*.xml 파일에 있으며, 이는 같은 디렉토리에서 찾을 수 있습니다. 기본 액세스 제어 파일에서 기본 액세스 제어 정책을 변경하면 이에 대응하는 defaultAccessControlPolicies_en_US.xml의 설명도 갱신해야 합니다. XML 파일에서의 변경은 고급 사용자들만 수행할 것을 강력히 권장합니다.

예제 3: 사용자의 정책과 연관된 기타 정책의 식별

마지막으로 이번 예제에서는, 액세스 제어 정책이 기타 정책에 어떻게 종속되어 있는지를 살펴 봅니다.

사용자 그룹(액세스 그룹)이 자원에서 수행할 수 있는 명령(조치)을 정의한 정책을 자원 레벨 정책이라고 합니다. 예를 들면, 지금까지 자세히 살펴본 정책은 아래와 같으며 자원 레벨 정책의 예입니다.

AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource

그러나, 자원 레벨 정책에서 허용되는 조치는 정책의 액세스 그룹에 속한 각 역할에 허용되는 조치에 종속적입니다. 특정 역할에게 허용되는 조치 항목을 설명하는 정책을 역할 기반 정책이라고 합니다.

자원 레벨 정책과 연관된 역할 기반 정책을 식별하려면 다음을 수행하십시오.

정책과 연관된 역할 찾기

1. WebSphere Commerce 관리 콘솔에 로그인하여 정책 페이지의 자원 레벨 정책을 찾으십시오. 같은 예를 사용하므로 다음이 원하는 정책임을 알 수 있습니다.

   AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
2. 정책과 연관된 액세스 그룹을 식별합니다. 이번 경우에는 액세스 그룹이 AuctionAdministratorsForOrg라는 것을 먼저 알 수 있습니다.
3. 액세스 그룹과 연관된 역할을 찾습니다. 앞선 예를 통해 AuctionAdministratorsForOrg에 대한 역할은 구매자(판매측), 카테고리 관리자, 상품 관리자 및 판매자임을 알 수 있습니다.

각 역할에 대한 역할 기반 정책 찾기

1. 이 책 끝의 부록으로 가서 역할 기반 정책이라는 절을 찾으십시오. 부록을 사용하여 역할과 연관된 각 역할 기반 정책을 찾습니다.
2. Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup 정책을 찾습니다. 이 정책은 구매자(판매측) 역할과 연관되어 있습니다. Buyers(sell-side) 접두어로 이를 알 수 있습니다.
3. 구매자(판매측), 카테고리 관리자, 상품 관리자 및 판매자 역할과 연관된 나머지 역할 기반 정책을 찾되, 접두어를 이용하여 올바른 정책을 식별합니다. 해당 목록은 다음과 같습니다.
   - Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup
   - Buyers(sell-side)ExecuteBuyers(sell-side)Views
   - CategoryManagersExecuteCategoryManagersCmdResourceGroup
   - CategoryManagersExecuteCategoryManagersViews
   - ProductManagersExecuteProductManagersCmdResourceGroup
   - ProductManagersExecuteProductManagersViews
   - SellersExecuteSellersCmdResourceGroup
   - SellersExecuteSellersViews
4. 각 역할 기반 정책은 해당 역할을 갖는 사용자가 특정 제어기 명령 또는 보기를 수행할 수 있게 허용합니다. 역할 기반 정책과 연관된 조치들을 보려면 예 1과 동일한 프로시저로 WebSphere Commerce 관리 콘솔의 정책 페이지에서 정책을 찾으십시오.

정책간 종속성 식별의 중요성

어떤 역할 기반 정책이 자원 레벨 정책과 연관되어 있는지를 이해하는 것은, 정책을 사용자 정의하고 새로 작성하는 데 있어서 필수조건입니다.

51 페이지의 제 5 장 『사용자 정의 시나리오』에서는 자원 레벨 정책과 역할 기반 정책을 구분하고 그 차이점을 이해하며 서로간의 관계를 보는 방법을 포함하여 자원 레벨 정책 및 역할 기반 정책에 대해 자세히 살펴봅니다.

제 4 장 기본 액세스 제어 정책 사용자 정의

WebSphere Commerce에서 제공하는 기본 액세스 제어 정책은 조직에서 사용자에 대해 사용 가능한 조치와 정보를 통제하고자 하는 기본적 요구 사항에 대처하기 위한 것입니다. 종종, 기본 정책으로도 사이트의 요구에 충분합니다. 동시에 기본 정책은, 많은 부분을 사용자 정의할 수 있는데, 이를 통해 사용자 고유의 요구 사항에 이를 맞출 수 있도록 합니다.

SiteAdministratorsCanDoEverything 정책은 사이트 운영자 역할을 가진 운영자에게 슈퍼유저 액세스를 부여하는 특별한 기본 정책입니다. 이 정책에서 사이트 운영자는 조치 또는 자원이 정의되어 있지 않아도 자원에서 조치를 수행할 수 있습니다. 이 역할을 사용자에게 지정할 때 이를 알고 있어야 합니다.

이번 장에서는 WebSphere Commerce에 포함된 기본 액세스 제어 정책에 대한 기본 변경 방법에 대한 정보를 제공합니다. 사용자가 이해할 필요가 있는 특정 개념과 관계를 소개하면서 시작합니다.

변경으로 영향받는 정책 식별

이전 장에서 정책이 종종 다른 정책들과 관련되어 있다는 것을 학습하였습니다. 또한 자원 레벨 정책에서 시작하는 방법과 이와 연관된 역할 기반 정책을 식별하는 법을 학습하였습니다. 이번 절에서는 정책들이 어떻게 서로 관련되어 있는지 자세히 설명하고 기존 정책을 수정하거나 새로 작성하기 전에 이들의 관계를 이해해야 하는 이유를 설명합니다. 많은 경우, 변경을 적절히 구현하려면 여러 정책을 수정해야 할 필요가 있습니다.

역할 기반 및 자원 레벨 정책 간의 관계 이해

WebSphere Commerce에서는, 다음과 같이 사용자가 취할 수 있는 각 조치가 하나 이상의 역할 기반 정책을 사용하여 지정됩니다.

- 각 기본 역할에는 해당 액세스 그룹이 있습니다. 예를 들어, 상점 운영자 역할의 액세스 그룹은 StoreAdministrators입니다.
- 각 "역할 기반" 액세스 그룹에는 일반적으로 두 개의 연관된 역할 기반 정책이 있습니다.
  - 역할이 실행 권한을 부여 받은 제어기 명령을 정의하는 정책.
  - 보기 조치 역할을 정의하는 정책은 실행 권한을 부여 받습니다. 보기 조치는 VIEWREG 테이블의 보기에 맵핑됩니다. 예를 들어, StoreListView는 시스템에 있는 상점 목록 웹 페이지를 표시합니다.

일부 제어기 명령은 자원 레벨 정책이 아닌 역할 기반 정책만 가집니다. 이것은 명령이 보호 가능한 자원에서 작동되지 않는 경우 발생합니다. 예를 들어, SetCurrencyPreferenceCmd 명령은 명령을 실행 중인 사용자의 통화 환경설정을 변경만 할 수 있으므로 자원 레벨 정책이 필요치 않습니다. 다른 사용자의 통화 환경설정을 변경할 수 있는 경우 사용자 오브젝트는 보호되어야 하고 자원 레벨 정책이 필요합니다.

제어기 명령의 자원 레벨 정책은 제어기 명령의 특정 역할 기반 정책과 직접 관련되어 있습니다. 자원 레벨 정책에서 제어기 명령은 조치 그룹의 일부이지만, 역할 기반 정책에서는 제어기 명령이 자원 그룹의 일부입니다. 아래 그림은 이러한 관계를 보여줍니다. 자원 레벨 정책에는 그 액세스 그룹 내에 역할 A와 역할 B가 포함되어 있고, 이것이 역할 A와 역할 B에 대한 역할 기반 정책이 실행에 옮겨지도록 합니다. 자원 레벨 정책은 역할 A 및 B의 사용자에게 특정 자원 세트에 대한 조치를 취할 수 있도록 권한을 부여하는 반면, 연관된 역할 기반 정책은 역할 A 및 B의 사용자에게 전반적인 권한부여를 합니다.

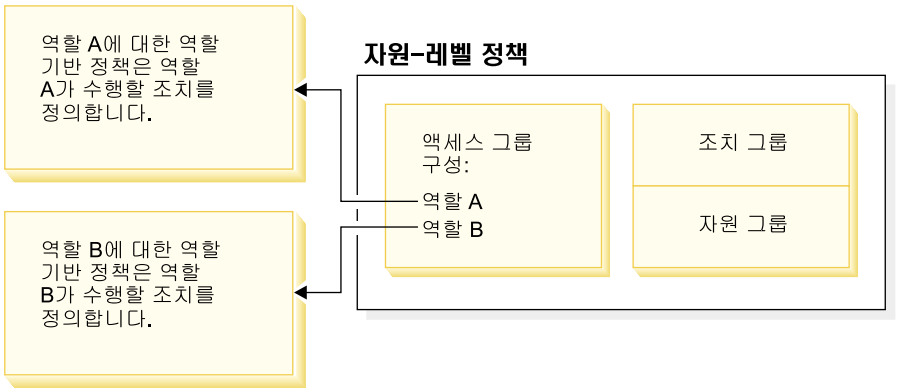
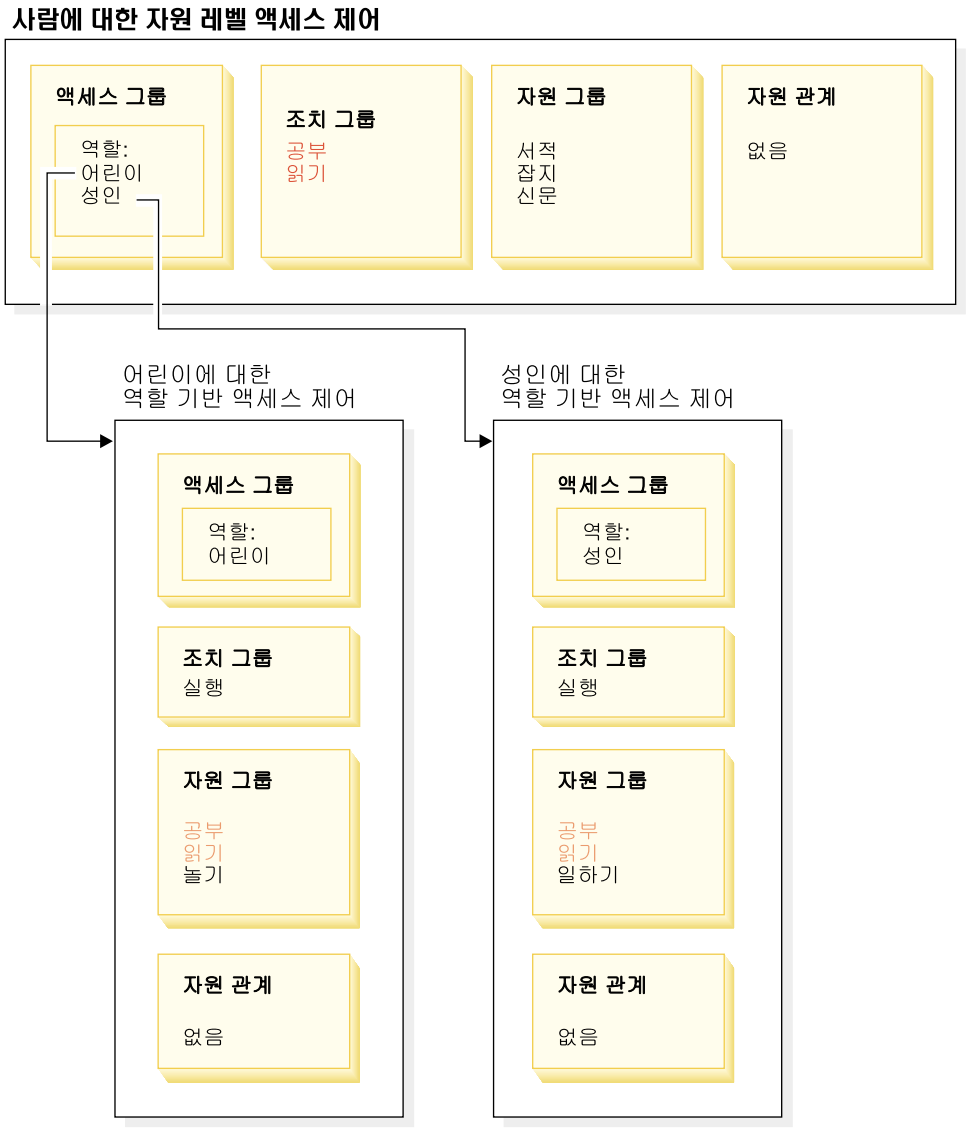


그림 3. 자원 레벨 정책과 연관된 역할 기반 정책의 관계

다음 그림은 사람들 액세스 그룹 내 사용자에게 도서, 잡지 및 신문같은 특정 자원을 읽거나 공부할 수 있도록 하는 권한을 부여하는 견본 자원 레벨 정책을 보여줍니다. 이 정책은 올바르게 고안되었는데 그 이유는 역할 어린이 및 성인에 대한 역할 기반 정책 또한 이들이 도서, 잡지 및 신문을 읽거나 공부할 수 있도록 권한을 부여하기 때문입니다.

그림 4. 자원 레벨 정책과 이에 영향을 주는 역할 기반 정책



제어기 명령의 역할 기반 정책에서는 다음에 유의하십시오.

- 조치 그룹에는 하나의 실행 조치만 있습니다.
- 자원 그룹에는 실행될 수 있는 제어기 명령이 있습니다.

마찬가지로 보기의 역할 기반 정책에서는 다음에 유의하십시오.

- 조치 그룹에는 실행될 수 있는 보기가 있습니다.
- 자원 그룹에는 하나의 `com.ibm.commerce.command.ViewCommand` 자원이 있습니다.

반면 자원 레벨 정책에서는 다음에 유의하십시오.

- 조치 그룹에는 자원 그룹내의 자원에게 수행 가능한 조치들의 세트가 있습니다.
- 자원 그룹에는 수행 가능한 실제 비즈니스 자원들의 목록이 있습니다.

자원 레벨 정책은 오직 특정 역할을 갖는 사용자에게 해당 역할 기반 정책에 의해 이미 조치를 취할 수 있도록 권한 부여된 역할을 수행하도록 권한을 부여합니다. 예를 들어, 위의 예에서 역할 어린이는 다음 조치들을 취할 수 있는 권한을 부여받습니다.

- 공부
- 읽기
- 놀기

자원 레벨 정책에 이제 일하기라는 새로운 조치를 포함하도록 변경했다고 가정합니다. 성인 역할을 가진 사용자는 일하기 조치를 수행할 수 있습니다. 하지만 어린이 역할을 가진 사용자는 할 수 없습니다. 그 이유는 두 역할에 대한 역할 기반 정책을 확인하면 명백합니다. 성인에 대한 정책은 자원 그룹의 일하기라는 조치가 나열됩니다. 어린이에 대한 정책은 그렇지 않습니다. 비록 어린이 및 성인 모두 자원 레벨 정책에 의해 적절하게 권한을 부여받았다고 하더라도, 어린이에 대한 역할 기반 정책은 일하기라는 조치 권한을 부여하지 않습니다.

자원 레벨 정책이 역할 기반 정책과 연결된 방식때문에, 특정 변경사항에 의해 영향을 받는 모든 정책을 추적하는 가장 좋은 방법은 자원 레벨 정책에서부터 거슬러 올라가서 작업하는 것입니다. 첫 번째 단계는 자원 레벨 정책의 액세스 그룹을 점검하고 여기에 역할들이 포함되어 있는지를 판별하는 것입니다. 관리 콘솔에서 액세스 관리 > 역할을 선택하여 기본 역할의 전체 목록을 표시할 수 있습니다.

만약, 자원 레벨 정책의 액세스 그룹이 역할을 포함하는 경우, 그들의 역할 기반 정책을 검토하여 변경할 필요가 여부가 있는지를 보십시오. 자원 레벨 정책의 조치 그룹에 조치를 추가하는 경우, 반드시 관련된 역할 기반 정책이 새 조치에 대한 권한을 부여하도록 해야 합니다. 자원 레벨 정책에서 조치를 삭제하고 있고 다른 자원 레벨 정책이 이 조치를 참조하지 않는 경우, 연관된 역할 기반 정책에서 해당 조치를 제거하는 것이 가장 좋습니다.

정책 모델 이해

권한을 부여하는 정책이 있어야만 사용자가 조치를 수행할 수 있습니다. 하지만, WebSphere Commerce에서는 **어느** 정책이든 필요한 권한을 제공하면 사용자가 조치를 취하도록 허용합니다. 그러므로, 기본값보다 더 제한적인 새 정책을 정의하는 경우, 더 폭넓은 기본 정책을 삭제하거나 수정하여 새 정책에 우선하는 것을 방지해야 합니다.

예를 들어, A라는 기본 정책이 등록된 모든 사용자에게 경매 입찰을 허용한다고 가정합니다. 이 정책을 변경하여 경매 입찰이 구매자 역할을 가진 사용자에게만으로 제한되도록 하고자 합니다. 단지 구매자가 새 경매 입찰을 할 수 있도록 권한을 부여하는 새 정책을 정의하는 경우, 이는 아무 효과가 없을 것입니다. 기본 정책 A는 여전히 등록된 모든 사용자가 입찰하는 것을 허용합니다. 새 정책이 영향을 미치려면, 더 폭넓은 기본 정책을 삭제해야만 합니다.

표 1은 자원 레벨 정책을 새로 작성하거나, 삭제 또는 변경할 때 필요한 추가 변경사항을 요약한 것입니다.

표 1. 역할을 사용하는 자원 레벨 정책을 변경할 때는 추가 변경이 요구됩니다.

자원 레벨 정책에서 다음을 변경할 경우:	**자원 레벨의 액세스 그룹이 역할을 사용하는 경우, 다음을 변경해야 합니다.**
정책의 조치 그룹에 조치를 추가합니다.	적용 가능한 역할 기반 정책이 자원 그룹 내의 조치를 반드시 포함하도록 하십시오.
정책의 조치 그룹에서 조치를 삭제합니다.	추가 변경이 필요하지 않습니다. 일관성을 위해 관련 역할 기반 정책에 있는 해당 자원 그룹에서 이 조치를 제거하는 것이 좋습니다. 이것은 다른 조치 그룹이 이 조치를 참조하지 않는 경우에만 수행되어야 합니다. 다른 조치 그룹이 이 조치를 참조하는 경우 자원 그룹에서 이 조치를 필요로 하는 역할 기반 정책이 있습니다.
다른 조치 그룹을 사용합니다.	적용 가능한 역할 기반 정책이 자원 그룹 내의 새 조치 그룹의 조치를 반드시 포함하도록 하십시오.
정책의 액세스 그룹에 역할을 추가합니다.	새 역할에 해당하는 역할 기반 정책이 자원 레벨 정책에 지정된 조치를 포함하는 자원 그룹을 참조하는지 확인하십시오.
정책의 액세스 그룹에서 역할을 삭제합니다.	추가 변경이 필요하지 않습니다. 일관성을 위해 자원 그룹의 이러한 조치를 더 이상 참조하지 않도록 해당 역할 기반 정책을 수정하는 것이 좋습니다.
다른 액세스 그룹을 사용합니다.	적용 가능한 역할 기반의 정책이 자원 그룹 내에 자원 레벨 정책의 조치 그룹 내의 조치를 반드시 포함하도록 하십시오.
새 정책을 작성합니다.	같은 조치에 권한을 부여하는 기존 정책이 있는지 확인하십시오. 필요할 경우 삭제합니다.
정책을 삭제하십시오.	사용자가 정책의 조치를 취하는 것을 방지하려면, 동일한 조치에 권한을 부여한 다른 정책을 삭제하십시오.

역할 기반 정책과 자원 레벨 정책 여부 결정

역할 기반 정책은 명령어 레벨 정책이라고도 알려져 있는데 그 이유는 특정 역할을 가진 사용자에게 명령어 세트를 실행하도록 권한을 부여하기 때문입니다. 자원 레벨 정책은 사용자 그룹에게 특정 자원 세트에 대해 명령어 세트를 실행할 수 있도록 권한을 부여합니다. 예를 들어, 역할 기반 정책은 어린이가 식사를 먹도록 승인할 수 있습니다. 반면, 자원 레벨 정책은 어린이가 쌀밥을 먹도록 승인할 수도 있습니다.

대체로 이름을 보면 역할 기반 정책과 자원 레벨 정책 여부를 판별할 수 있습니다.

역할 기반 정책

역할이 실행할 수 있는 제어기 명령어를 정의하는 정책은 다음 이름 지정 규칙을 따릅니다.

<AccessGroupforRoleXYZ> Execute <XYZCmdResourceGroup>

예제: `ProductManagersExecuteProductManagersCmdResourceGroup`.

제어기 명령어용 역할 기반 정책에는, 실행이라고 하는 단일 항목이 조치 그룹에 있으며, 자원 그룹에는 해당 역할을 가진 사용자가 실행할 수 있는 WebSphere Commerce 명령어 목록이 있습니다.

역할이 실행할 수 있는 보기를 정의하는 정책은 다음 이름 지정 규칙을 따릅니다.

<AccessGroupforRoleXYZ> Execute <XYZViews>

예제: SalesManagersExecuteSalesManagerViews.

보기용 역할 기반 정책에는 해당 역할을 가진 사용자가 실행할 수 있는 보기 목록이 있습니다.

자원 레벨 정책

데이터 자원(작성이 가능하거나 다룰 수 있는 비즈니스 오브젝트)에 대해 취할 수 있는 조치를 정의하는 정책은 다음 이름 지정 규칙을 따릅니다.

<AccessGroupXYZ> Execute <XYZCommands> On <XYZResource>

예제: AllUsersExecuteOrderProcessOnOrderResource.

자원 레벨 정책에서 조치 그룹에는 WebSphere Commerce 명령어가 있으며 자원 그룹은 작용 가능한 고유의 비즈니스 자원을 식별합니다.

한 가지 예외는 주문, 입찰, RFQ 같은 엔티티 작성에 대해 권한을 부여하는 정책입니다. 이러한 정책은 엔티티 그 자체에 대해 작용하지 않는데 그 이유는 엔티티가 작성 전이기 때문입니다. 대신, 이 정책들이 포함한 엔티티에 대해 작용합니다. 예를 들어, 경매는 상점이라는 배경하에서 작성되며, 사용자는 조직이라는 배경하에서 작성됩니다. 대부분의 자원은 상점이라는 배경하에서 작성됩니다. 그 결과, 이러한 정책의 이름은 다음과 같습니다.

<AccessGroupXYZs> Execute <XYZCommands> On <StoreEntityResource>

예 :
AuctionAdministorsForOrgExecuteAuctionCreateCommandsOnStoreEntityResource.

데이터 bean 자원(데이터 bean에는 대개 JSP에서 사용되는 입찰이나 주문같은 데이터 자원에 대한 정보가 있음)을 볼 수 있는 사용자를 정의하는 정책은 다음 이름 지정 규칙을 따릅니다.

<AccessGroupXYZs> Display <XYZDatabeanResourceGroup>

예: MembershipViewersForOrgDisplayMembershipDatabeanResourceGroup.

기본 정책 변경 추가정보

기본 정책을 변경할 때는 다음을 염두에 두십시오.

- 대부분의 액세스 그룹은 구매자나 상품 관리자같은 사용자 역할에 의해 정의됩니다. 이 역할들과 이들이 취할 수 있는 조치 항목에 대해 더 자세히 알려면 14 페이지의 『역할』을 참조하십시오.
- 다른 액세스 그룹을 사용하기 위해 정책을 변경하기 전에, 액세스 그룹의 정의를 검토하여 요구사항을 충족하는지를 확인하십시오. 그렇게 하려면, 관리 콘솔에서 **액세스 관리 > 액세스 그룹**을 선택하십시오.
- 보기에서 선택한 값에 따라, 정책 페이지는 사이트 레벨 정책이나 특정 조직에 고유한 정책을 표시합니다.
  - 보기 필드를 루트 조직으로 설정하면, 루트 조직이 소유하는 표준 정책과 템플리트 정책의 마스터 버전이 표시됩니다.
  - 보기 필드를 조직의 이름으로 설정하면, 해당 조직이 소유하는 표준 정책 및 조직에서 수정 가능한 템플리트 정책이 표시됩니다.
- 변경한 어떤 정책이든 이름을 바꾸어서 정책명이 정책이 하는 일을 반영하도록 하여 변경한 기본 정책을 식별할 수 있도록 하십시오. 사용자 정의한 정책에 대해 이름 이정 규칙을 구현하는 것을 고려하십시오. 적절하다면, 정책의 설명과 표시 이름도 수정하십시오.

주: WebSphere 관리 콘솔은 액세스 제어 정책 정의 및 액세스 그룹 정의에 대한 간단한 수정만 수행할 수 있습니다. 보다 견고한 해결책은 XML 파일을 사용하여 데이터를 갱신하는 것입니다. 다음 작업은 XML을 통해서만 수행할 수 있습니다.

1. 새 조치, 자원, 속성, 관계, 관계 그룹의 정의
2. 복잡한 암시적 자원 그룹 및 복잡한 암시적 액세스 그룹 정의

정책 변경 후

액세스 제어 정책을 작성하거나 수정할 때마다, 정책의 올바른 작동 여부를 검증하는 일정 테스트를 수행해야 합니다.

현재 데이터베이스에 있는 모든 새 정책 및 변경된 정책에 대한 테스트를 마치고 나면, 해당 정보를 XML 파일로 추출하는 것이 좋습니다. 이러한 파일은 초기 액세스 제어 정책 관련 파일 `defaultAccessControlPolices.xml`, `defaultAccessControlPolicies_locale.xml`, `ACUserGroup_locale.xml`과 동일한 형식을 갖습니다. 이 단계가 필요한 이유는 관리 콘솔을 이용하여 작성한 변경이 데이터베이스에 저장된 정책 정보에만 영향을 주기 때문입니다. 인스턴스 작성 중에 기본 액세스 제어 정책 및 그 구성요소를 로드하는데 사용된 XML 파일은 자동으로 갱신되지 않습니다.

XML 파일과 데이터베이스 내 액세스 제어 정보간의 일관성을 유지하는 데는 다음 몇 가지 이유가 있습니다.

- WebSphere Commerce의 인스턴스를 작성할 때, 정책 및 액세스 그룹 정의가 XML 파일에서 로드됩니다.
- XML 파일은 정책 및 구성 요소 부분을 직접 보거나 편집하는 편리한 방법을 제공하므로 파일을 최근으로 유지하는 것은 필수입니다.

정책 변경사항 테스트

각 정책에 대해 다음을 확인하십시오.

- 정책의 액세스 그룹에 속한 사용자는 지정된 자원에 대해 지정된 조치를 취할 수 있습니다. 조치를 수행하기 위해 권한을 제거하는 경우, 테스트를 통해 사용자가 더 이상 그 조치를 수행할 수 없는지 확실히 테스트하십시오.
- 액세스 그룹에 속하지 않은 사용자는 지정된 자원에 대해 지정된 조치를 취할 수 없습니다.

예를 들어, 제 5 장에서 경매 사용자 정의 시나리오 1을 구현하고, 여기에서는 경매 운영자가 경매 입찰을 종료할 수 없도록 했다고 가정합니다. 이 변경사항이 올바르게 작동하고 있는지를 테스트하려면, 경매 운영자 액세스 그룹에 속한 사용자로 로그인하여 다음 조치들을 수행하십시오.

- 경매 수정
- 경매 삭제

경매 운영자가 경매를 종료할 수 없는지를 반드시 검증하십시오.

그리고 나서, 경매 운영자 액세스 그룹에 속하지 않는 사용자로 로그인해서 다음 조치들을 수행해보십시오. 정책이 올바르게 작동하고 있는 경우, 이 시도가 실패해야 합니다.

정책 변경사항을 XML 파일로 추출

정책 변경을 완료하고 테스트를 하였으면, XML 파일을 데이터베이스의 정책 정보가 동기화되도록 갱신해야 합니다. 부록에서는 액세스 제어 정책 및 액세스 그룹과 관련된 여러 가지 XML 파일에 대해서 설명합니다. 또한 데이터베이스에서 XML 파일로 정책 변경사항을 추출하는 방법과 XML 파일에서 데이터베이스로 정책을 로드하는 방법을 설명합니다.

제 5 장 사용자 정의 시나리오

아래에 제공된 사용자 정의 시나리오는 지금까지 학습한 액세스 제어 정책을 다양한 기초적 변경을 통해 기본 정책에 적용해보도록 합니다. 이러한 모든 시나리오에서는 사이트 운영자가 루트 조직에 대한 정책을 수정하고 있다고 전제합니다. 몇몇 시나리오를 끝까지 마치고 나면, 같은 방법을 따라함으로써 여기서 구체적으로 다루지 않은 변경을 할 수 있습니다.

시나리오는 비즈니스 영역에 의해 구성되었습니다. 각 비즈니스 영역 내에서 시나리오는 복잡도의 증가순으로 제공됩니다.

표 2. 시나리오 목차

비즈니스 영역	시작 페이지
경매	52 페이지의『경매 시나리오 1: 경매 운영자의 경매 입찰 종료 권한 제거』
장기 구매 계약	57 페이지의『장기 구매 계약 시나리오 1: 장기 구매 계약 운영자의 장기 구매 계약 첨부 추가 또는 삭제 금지』
주문	60 페이지의『주문 시나리오 1: 구매자에게만 주문 작성 허용』
멤버쉽	67 페이지의『멤버쉽 시나리오 1: 사용자의 자체 등록 능력 제거』
쿠폰	72 페이지의『쿠폰 시나리오 1: 구매자만 쿠폰 회수 허용』
조달	77 페이지의『조달 시나리오 1: 조달 장바구니 관리자가 조직에서 작성된 주문에 대한 조달 장바구니를 관리할 수 있도록 허용』
재고	80 페이지의『재고 시나리오 1: 서비스 센터 관리자가 서비스 센터를 갱신하지만 삭제하지는 않도록 허용』
비즈니스 인텔리전스	82 페이지의『비즈니스 인텔리전스 시나리오 1: 감사자가 비즈니스 인텔리전스 보고서를 볼 수 있도록 허용』

특정 유형의 변경을 설명하는 시나리오를 찾으려면, 설명된 사용자 정의 유형에 의해 시나리오를 상호 참조해놓은 아래 테이블을 참조하십시오.

표 3. 사용자 정의 유형에 따라 구성된 사용자 정의 시나리오

사용자 정의	참조 페이지
정책의 액세스 그룹에 역할 추가	74
정책의 조치 그룹 변경	78,80
정책의 자원 관계 변경	62,77

표 3. 사용자 정의 유형에 따라 구성된 사용자 정의 시나리오 (계속)

정책을 변경하여 다른 액세스 그룹을 사용	55,60,62,68,72,74
새로운 액세스 그룹 작성 및 정책에서 사용	65,69
새 조치 그룹 작성 및 정책에서 사용	69,78
새 자원 레벨 정책 작성	58,78
새 역할 기반 정책 작성	69,82
새 역할 작성 및 자원 레벨 정책에서 사용	69,82
정책 삭제	53,54,67
정책의 조치 그룹에서 조치 제거	3,57

테이블 3: 사용자 정의 유형에 따라 구성된 사용자 정의 시나리오

경매 시나리오 1: 경매 운영자의 경매 입찰 종료 권한 제거

기본적으로 상점의 경매 운영자는 상점의 경매 수정이나 종료를 할 수 있으며 입찰 종료 또한 마찬가지입니다. 어떤 경우에는 경매 운영자에게 이 권한을 부여하는 것을 원치 않을 수도 있습니다. 그 이유는 경매를 다른 사람이 취급하거나 상점에서 이 조치가 필요하지 않기 때문입니다.

이번 시나리오에서는 경매 운영자에게서 입찰 종료 권한을 제거해 보겠습니다. 이 변경을 하려면, 다음을 수행하십시오.

1. 부록을 사용하여 경매 운영자가 취할 수 있는 조치를 정의하는 자원 레벨 정책을 찾으십시오.
2. 정책용 조치 그룹의 이름을 결정하십시오.
3. 정책의 조치 그룹에서 경매 입찰 종료 조치를 삭제하십시오.

수행 단계

조치 그룹이 반드시 변경되어야 하는 정책 식별

1. 부록에서 경매 아래의 내용을 보고 변경할 자원 레벨 정책을 식별하십시오. 정책은 다음과 같습니다.

   ```
   AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
   ```

2. 관리 콘솔에서 **액세스 관리 > 정책을 누르십시오.**
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 목록에서 정책을 찾으십시오.
5. 정책의 조치 그룹 이름 - `AuctionManage`를 유의하십시오. 이것이 입찰 종료 조치를 제거하기 위해 변경할 필요가 있는 조치 그룹입니다.

정책의 조치 그룹에서 입찰 종료 조치 제거

1. **액세스 관리 > 조치 그룹**을 누르십시오.
2. 조치 그룹 목록에서 **AuctionManage**를 선택하십시오.
3. **변경**을 눌러 자원 그룹 변경 페이지를 표시하십시오.
4. 선택된 조치 목록에서 **com.ibm.commerce.negotiation.commands.CloseBiddingCmd**를 선택하십시오.
5. **제거**를 누르십시오.
6. **확인**을 누르십시오.

변경사항으로 정책 레지스트리 갱신

1. **구성> 레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

경매 시나리오 2: 경매 운영자의 경매 유찰 권한 제거

기본적으로 상점의 경매 운영자는 경매에 제출된 입찰을 유찰시킬 수 있습니다. 어떤 경우에는 아무에게도 이 권한을 허용하려 하지 않을 수도 있습니다. 이렇게 변경하려면 입찰을 유찰시키고 삭제할 수 있는 사용자를 정의하는 자원 레벨 정책을 찾아야 합니다.

경매 시나리오 1에서 경매 종료 조치는 정책에 포함된 여러 조치 중 하나였습니다. 따라서 정책의 조치 그룹에서 이 조치를 삭제하기만 하면 됩니다. 하지만 이번 시나리오에서는 전체 정책이 경매 유찰을 제어합니다. 그러므로 조치만을 삭제하는 것이 아니라 정책을 삭제해야만 합니다.

정책을 삭제하려면 다음을 수행하십시오.

- 부록을 사용하여 경매 운영자의 경매 유찰을 다루는 자원 레벨 정책을 찾으십시오.
- 정책을 삭제하십시오.

주: 정책을 삭제하기 전에 정책 이름, 액세스 그룹 이름, 자원 그룹 이름 및 조치 그룹 이름을 기록하여 다음 시나리오를 위해 다시 작성할 수 있도록 하십시오.

수행 단계

1. 부록에서 경매 아래의 내용을 보고 변경할 자원 레벨 정책을 식별하십시오. 정책은 다음과 같습니다.

   ```
   AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource
   ```

2. 관리 콘솔에서 **액세스 관리 >정책을 누르십시오.**
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 정책 목록에서 다음을 선택하십시오.

AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource

5. **삭제**를 선택하십시오.

변경사항으로 정책 레지스트리 갱신

1. **구성 > 레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

경매 시나리오 3: 한 조직에서 경매 운영자의 경매 유찰 권한 제거

기본적으로 상점의 경매 운영자는 경매에 제출된 입찰을 유찰시킬 수 있습니다. 어떤 경우에는 사이트 운영자로서 특정 조직을 위해 이 정책을 변경하기를 원할 수도 있습니다. 이렇게 변경하려면 해당 조직에 대해 이 조치에 권한을 부여하는 템플리트 정책을 반드시 삭제해야 합니다.

주: WebSphere Commerce Professional Edition에서는, 루트 조직, 기본 조직 및 판매 조직, 3개의 조직만이 있습니다.

정책을 삭제한 후에는, 그 조직의 경매 운영자가 더 이상 입찰을 유찰시킬 수 없습니다. 다른 조직의 경매 운영자는 이 변경으로 영향을 받지 않습니다.

정책을 삭제하려면 다음을 수행하십시오.

- 부록을 사용하여 경매 유찰의 권한을 부여하는 자원 레벨 정책을 찾으십시오.
- 조직에 대한 정책 목록에서 정책을 위치 지정하십시오.
- 정책을 삭제하십시오.

수행 단계

정책 삭제

1. 부록에서 경매 아래의 내용을 보고 변경할 자원 레벨 정책을 식별하십시오. 정책은 다음과 같습니다.

   AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource

2. 관리 콘솔에서 **액세스 관리 > 정책을 누르십시오.**
3. 보기에 대해 삭제하고자 하는 정책의 조직을 선택하십시오. 루트 조직보다는 특정 조직을 선택할 때, 정책 변경은 사이트의 모든 조직에 적용되기보다는 해당 조직에만 적용됩니다.
4. 정책 목록에서 다음을 선택하십시오.

   AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource

5. **삭제**를 선택하십시오.

변경사항으로 액세스 제어 레지스트리 갱신

1. **구성 > 레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

경매 시나리오 4: 구매자로 경매 입찰 제한

기본적으로 모든 등록된 사용자는 그들의 조직내 지위에 관계없이 상점에서 경매 중인 상품에 대한 입찰이 허용되어 있습니다. 어떤 경우에는 WebSphere Commerce 내의 구매자 역할에 지정된 사용자처럼 제한된 사용자 그룹에게만 입찰을 제한하고자 할 수도 있습니다.

이번 시나리오에서는 자원 레벨 정책뿐만 아니라 그와 연관된 역할 기반 정책을 변경합니다. 구매자 조직에서 구매자 역할을 구성원에게만 입찰을 제한하려면, 다음을 수행하십시오.

- 부록을 사용하여 경매 입찰을 작성할 수 있는 사람을 지정하는 자원 레벨 정책을 찾으십시오.
- 정책의 액세스 그룹을 모든 등록된 사용자에서 구매자 역할을 가진 사용자로 변경하십시오.
- 정책 이름, 설명 및 표시 이름을 바꾸십시오.
- 입찰 작성용 명령어를 식별하십시오.
- 부록을 사용하여 구매자(구매측)용 역할 기반 정책을 찾으십시오. 이 정책은 구매자(구매측) 역할을 가진 사용자가 실행할 수 있는 명령을 정의합니다. 반드시 정책의 자원 그룹을 갱신하여 구매자가 입찰 작성용 명령어를 실행할 수 있도록 허용해야 합니다.
- 이 역할 기반 정책의 자원 그룹을 갱신하여 입찰 작성용 명령어를 포함하도록 하십시오.

수행 단계

자원 레벨 정책 식별

1. 부록에서 경매 아래의 내용을 보고 변경할 자원 레벨 정책을 식별하십시오. 정책은 다음과 같습니다.
   `RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource`
2. 관리 콘솔에서 **액세스 관리 > 정책을 누르십시오.**
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 정책 목록에서 다음을 선택하십시오.
   RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource

5. 정책의 조치 그룹 이름 - BidCreate를 유의하십시오. 이것이 입찰 작성용 명령어의 이름을 찾기 위해 볼 필요가 있는 조치 그룹입니다.

정책용 액세스 그룹 변경

1. **변경**을 눌러 정책 변경 페이지를 표시하십시오.
2. 사용자 그룹에 대해 **찾기**를 누르고 **구매자(구매측)**를 선택하십시오.
3. **확인**을 누르십시오.
4. 텍스트를 편집하여 정책 이름, 표시 이름 및 정책 설명을 바꾸십시오.
5. **확인**을 누르십시오.

입찰 작성용 명령어 식별

1. **액세스 관리 > 조치 그룹**을 누르십시오.
2. 조치 그룹 목록에서 **BidCreate**를 선택하십시오..
3. **변경**를 눌러 조치 그룹 변경 페이지를 표시하십시오. 입찰 작성용 명령어 이름 com.ibm.commerce.negotiation.commands.BidSubmitCmd를 유의하십시오. 반드시 이 명령어를 자원 그룹에 추가하여 구매자가 실행할 수 있는 명령어 목록에 포함되도록 해야 합니다.

역할 기반 정책과 구매자(구매측)용 자원 그룹 식별

1. 부록에서 역할 기반 정책 아래의 내용을 보고 구매자(구매측)용 역할 기반 정책을 찾으십시오. 정책은 다음과 같습니다.

   Buyers(buy-side)ExecuteBuyers(buyside)CommandsResourceGroup
2. **액세스 관리 > 정책**을 누르십시오.
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 자원 그룹 이름 Buyers(buy-side)CommandsResourceGroup에 유의하십시오. 이제 갱신할 자원 그룹의 이름을 알게 되었습니다.

역할 기반 정책에서 자원 그룹을 갱신하여 입찰 작성용 명령어가 포함되도록 하십시오.

1. **액세스 관리 > 자원 그룹**을 누르십시오.
2. **Buyers(buy-side)CommandsResourceGroup**을 선택하십시오.
3. **변경**을 눌러 자원 그룹 변경 페이지를 표시하십시오.
4. **다음**을 눌러 자세히 보기 페이지를 표시하십시오.
5. 사용 가능한 자원 목록에서 **com.ibm.commerce.negotiation.commands.BidSubmitCmd**를 선택하십시오. 이것은 입찰 작성용 명령어입니다.
6. **추가**를 눌러 자원 그룹에 명령어를 추가하십시오.
7. **완료**를 누르십시오.

변경사항으로 액세스 제어 레지스트리 갱신

1. **구성 > 레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

장기 구매 계약 시나리오 1: 장기 구매 계약 운영자의 장기 구매 계약 첨부 추가 또는 삭제 금지

기본적으로 상점에 대한 장기 구매 계약 운영자는 그들이 관리하는 장기 구매 계약의 첨부를 추가하거나 삭제할 수 있습니다. 어떤 경우에는 장기 구매 계약 운영자에게 이 권한을 허용하려 하지 않을 수도 있습니다.

이 시나리오에서는 장기 구매 계약 운영자가 취할 수 있는 조치를 정의하는 자원 레벨 정책을 변경합니다. 장기 구매 계약 운영자에게서 장기 구매 계약의 첨부를 추가하거나 삭제하는 권한을 제거하려면, 다음을 수행하십시오.

- 부록을 사용하여 장기 구매 계약 운영자가 취할 수 있는 조치를 정의하는 자원 레벨 정책을 찾으십시오.
- 정책용 조치 그룹의 이름을 결정하십시오.
- 정책의 조치 그룹에 있는 조치 목록에서 첨부 추가 및 삭제 조치를 삭제하십시오.

수행 단계

자원 레벨 정책 및 조치 그룹 식별

1. 부록에서 장기 구매 계약 아래의 내용을 보고 변경할 자원 레벨 정책을 식별하십시오. 정책은 다음과 같습니다.

   ```
   ContractAdministratorsForOrgExecuteContractManageCommandsOnContractResource
   ```

2. 관리 콘솔에서 **액세스 관리 > 정책을 누르십시오.**
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 목록에서 정책을 찾으십시오.
5. 정책의 조치 그룹 이름 - `ContractManage`를 유의하십시오. 이것이 첨부 추가 및 삭제용 조치를 제거하기 위해 변경할 필요가 있는 조치 그룹입니다.

정책의 조치 그룹에서 첨부 추가 및 삭제 조치 제거

1. **액세스 관리 > 조치 그룹**을 누르십시오.
2. 조치 그룹의 목록에서 **ContractManage**를 선택하십시오.
3. **변경**을 눌러 자원 그룹 변경 페이지를 표시하십시오.

4. 선택된 조치 목록에서 다음 조치들을 선택하십시오. **com.ibm.commerce.contract.commands.ContractAttachmentAddCmd com.ibm.commerce.contract.commands.ContractAttachmentDeleteCmd**.
5. **제거**를 누르십시오.
6. **확인**을 누르십시오.

변경사항으로 액세스 제어 레지스트리 갱신

1. **구성 > 레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

장기 구매 계약 시나리오 2: 장기 구매 계약 연산자 및 장기 구매 계약 운영자 모두 장기 구매 계약 전개 허용

기본적으로 상점의 장기 구매 계약 운영자는 장기 구매 계약을 전개할 수 있습니다. 어떤 경우에는 장기 구매 계약 운영자에게도 마찬가지로 이 권한을 부여하고자 할 수도 있습니다.

액세스 제어 정책의 탄력적인 설계는 이 변경을 구현하는 데 있어 몇 가지 방법을 제공합니다.

- 장기 구매 계약 연산자와 장기 구매 계약 운영자 모두를 포함하는 새 액세스 그룹을 작성하고 장기 구매 계약 전개가 가능한 사용자를 정의하는 정책을 새 액세스 그룹에 지정할 수 있습니다.
- 장기 구매 계약 운영자가 수행할 수 있는 조치를 지정하는 정책에 장기 구매 계약 전개 조치를 추가할 수 있습니다.
- 새 정책을 작성하여 장기 구매 계약 운영자가 장기 구매 계약을 전개할 수 있도록 허용할 수 있습니다.

이 시나리오는 세 번째 접근법을 설명합니다. 여기에서는 자원 레벨 정책을 새로 작성하여 장기 구매 계약 운영자에게 계약 전개 권한을 부여하는 방법을 보여줍니다.

새 정책을 작성하려면 다음을 수행하십시오.

- 부록을 사용하여 장기 구매 계약 운영자의 장기 구매 계약 전개 권한을 부여하는 자원 레벨 정책을 찾으십시오.
- 이 정책용 조치 그룹의 이름을 주목하십시오.
- 이 정책용 자원 그룹의 이름을 주목하십시오.
- 장기 구매 계약 운영자 액세스 그룹용 새 정책을 정의하여 장기 구매 계약 연산자에게 장기 구매 계약 전개 권한을 부여하는 정책의 조치 그룹과 자원 그룹을 지정하도록 하십시오.

수행 단계

새 정책에서 사용할 조치 그룹과 자원 그룹의 식별

1. 부록에서 장기 구매 계약 아래의 내용을 보고 장기 구매 계약 운영자의 장기 구매 계약 전개 권한을 부여하는 자원 레벨 정책을 찾으십시오. 이 정책은 다음과 같습니다.

   ContractOperatorsForOrgExecuteContractDeployCommandsOnContractResource

   입니다.
2. 관리 콘솔에서 **액세스 관리 > 정책을 누르십시오.**
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 목록에서 정책을 찾으십시오.
5. 정책의 조치 그룹 이름 - ContractDeploy를 주목하십시오. 이것이 새 정책을 정의하는 데 사용할 필요가 있는 조치 그룹입니다.
6. 자원 그룹의 이름 - ContractDataResourceGroup을 주목하십시오. 이것이 새 정책을 정의하는 데 사용할 필요가 있는 자원 그룹입니다.

새 정책 정의

1. **새로 만들기**를 눌러 새 정책 페이지를 표시하십시오.
2. 이름에서 다음을 지정하십시오.

   ContractAdministratorsForOrgExecuteContractDeployCommandsOnContractResource
3. 표시 이름에서 정책에 대한 간단한 설명을 자국어로 작성하십시오.
4. 설명에서 정책이 하는 일에 대한 좀 더 자세한 설명을 자국어로 작성하십시오.
5. 사용자 그룹에서 **찾기**를 눌러 **ContractAdministratorForOrg**를 선택하십시오.
6. **확인**을 누르십시오.
7. 자원 그룹에서 **ContractDataResourceGroup**을 선택하십시오.
8. 조치 그룹에서 **ContractDeploy**를 선택하십시오.
9. 정책 유형에서 **템플리트 정책**을 선택하여 정책을 템플리트 정책으로 지정하십시오.
10. **확인**을 누르십시오.

변경사항으로 액세스 제어 레지스트리 갱신

1. **구성 > 레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

주문 시나리오 1: 구매자에게만 주문 작성 허용

기본적으로 모든 사용자들은 그들의 조직 내 지위에 관계없이 상품에 대한 주문 작성이 허용되어 있습니다. 어떤 경우에는 구매 조직의 직원같은 제한된 사용자 그룹에게만 주문 작성을 할 수 있도록 제한하고자 할 수도 있습니다. 일반적으로 이 직원들은 구매 조직의 구매자(구매측) 역할에 지정되어 있습니다.

구매 조직에서 구매자 역할을 가진 구성원에게만 주문 작성을 제한하려면, 다음을 수행하십시오.

- 부록을 사용하여 주문을 작성할 수 있는 사람을 지정하는 자원 레벨 정책을 찾으십시오.
- 정책의 액세스 그룹을 모든 사용자에서 구매자 역할을 가진 사용자로 변경하십시오.
- 정책 이름, 표시 이름 및 설명을 갱신하십시오.
- 주문 작성용 명령어를 식별하십시오.
- 부록을 사용하여 구매자(구매측)용 역할 기반 정책을 찾으십시오. 이 정책은 구매자(구매측) 역할을 가진 사용자가 실행할 수 있는 명령을 정의합니다. 반드시 정책의 자원 그룹을 갱신하여 구매자가 주문 작성 명령어를 실행할 수 있도록 허용하십시오.
- 이 역할 기반 정책의 자원 그룹을 갱신하여 주문 작성용 명령어를 포함하도록 하십시오.

주: 이 자원 레벨 정책은 템플리트 정책입니다. 이 시나리오에서는 루트 조직 레벨에서 이 템플리트의 마스터 사본을 변경했습니다. 루트 조직이 아닌 특정 조직에 대해서만 변경한 경우 정책을 변경하기 전에 보기를 다른 조직으로 변경해야 합니다. 그러면 이 조직에 대해서만 템플리트 정책이 대체됩니다. 그런 후 이 조직에 대한 새 표준 정책이 작성되고 구매자(구매측) 사용자의 보다 제한된 액세스 그룹을 갖게 됩니다. 덜 제한적인 템플리트 정책이 여전히 루트 조직 레벨에서 적용되므로 역시 해당 레벨에서 대체해야 합니다. 현재 이를 수행할 수 있는 유일한 방법은 데이터베이스에서 수동으로 ACORGPOL 테이블을 갱신하고 다음 SQL을 실행하는 것입니다.

```
insert into ACORGPOL (acpolicy_id, member_id) values ( (select acpolicy_id
 from ACPOLICY where policyname = ' AllUsersExecuteOrderCreateCommands
OnStoreResource'), -2001)
```

수행 단계

자원 레벨 정책 식별

1. 부록에서 주문 아래의 내용을 보고 변경할 자원 레벨 정책을 식별하십시오. 이 정책은 AllUsersExecuteOrderCreateCommandsOnStoreResource입니다.
2. 관리 콘솔에서 **액세스 관리 > 정책을 누르십시오.**
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.

4. 정책 목록에서 **AllUsersExecuteOrderCreateCommandsOnStoreResource.**를 표시하십시오. 정책의 조치 그룹 이름을 주목하십시오. 이것이 주문 작성용 명령어의 이름을 찾기 위해 볼 필요가 있는 조치 그룹입니다.

액세스 그룹 변경

1. **변경**을 눌러 정책 변경 페이지를 표시하십시오.
2. 사용자 그룹에 대해 **찾기**를 누르고 **구매자(구매측)**를 선택하십시오.
3. **확인**을 누르십시오.
4. 정책의 이름, 표시 이름 및 설명을 갱신하여 액세스 그룹의 변경사항을 반영하십시오.
5. **확인**을 누르십시오.

주문 작성용 명령어 식별

1. **액세스 관리 > 조치 그룹**을 누르십시오.
2. 조치 그룹의 목록에서 **OrderCreateCommands**를 선택하십시오.
3. **변경**을 눌러 조치 그룹 변경 페이지를 표시하십시오. 주문 작성용 명령어의 이름에 유의하십시오.

```
com.ibm.commerce.order.commands.OrderCopyCmd
 com.ibm.commerce.order.commands.OrderScheduleCmd
 com.ibm.commerce.orderitems.commands.OrderItemMoveCmd
 com.ibm.commerce.orderitems.commands.OrderItemUpdateCmd
 com.ibm.commerce.requisitionlist.commands.RequisitionListSubmitCmd
```

   반드시 이 명령어를 자원 그룹에 추가하여 구매자가 실행할 수 있는 명령어 목록에 포함되도록 해야 합니다.

   주: 명령어 com.ibm.commerce.orderitems.commands.AdminOrderItemUpdateCmd는 필요하지 않습니다.

구매자(구매측)용 역할 기반 정책 식별

1. 부록에서 역할 기반 정책 아래의 내용을 보고 구매자(구매측)용 역할 기반 정책을 찾으십시오. 이 정책은 Buyers(buyside)ExecuteBuyers(buyside) CommandsResourceGroup입니다.
2. **액세스 관리 > 정책**을 누르십시오.
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 목록에서 정책을 찾으십시오.
5. 자원 그룹의 이름 - Buyers(buyside)CommandsResourceGroup을 주목하십시오. 이것이 갱신이 필요한 자원 그룹입니다.

역할 기반 정책의 자원 그룹을 갱신하여 주문 작성용 명령어 포함

1. **액세스 관리 > 자원 그룹**을 누르십시오.

2. 자원 그룹의 목록에서 **Buyers(buyside)CommandsResourceGroup**을 선택하십시오.
3. **변경**을 눌러 자원 그룹 변경 페이지를 표시하십시오.
4. **다음**을 눌러 자세히 보기 페이지를 표시하십시오.
5. 사용 가능한 자원 목록에서 다음 주문 작성용 명령어를 선택하십시오.

```
com.ibm.commerce.order.commands.OrderCopyCmd

com.ibm.commerce.order.commands.OrderScheduleCmd
 com.ibm.commerce.orderitems.commands.OrderItemMoveCmd
 com.ibm.commerce.orderitems.commands.OrderItemUpdateCmd
 com.ibm.commerce.requisitionlist.commands.RequisitionListSubmitCmd
```

6. **추가**를 누르십시오.
7. **완료**를 누르십시오.

변경사항으로 액세스 제어 레지스트리 갱신

1. **구성 > 레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

주문 시나리오 2: 구매자 관리자에게만 주문 수정 허용

주: 이 시나리오는 WebSphere Commerce Professional Edition에서는 적용되지 않습니다.

기본적으로 그들의 조직 내 지위에 관계없이 모든 사용자는 그들이 작성한 주문을 수정할 수 있습니다. 어떤 경우에는 조직의 구매자 관리자에게 주문 수정 권한을 부여하고자 할 수도 있습니다.

이번 시나리오에서는 자원 레벨 정책뿐만 아니라 역할 기반 정책도 변경합니다. 구매자 조직의 구성원에 속한 주문을 구매자 관리자만이 수정할 수 있도록 허용하려면, 다음을 수행하십시오.

- 부록을 사용하여 주문을 수정할 수 있는 사람을 지정하는 자원 레벨 정책을 찾으십시오.
- 정책의 액세스 그룹을 모든 사용자에서 구매자 관리자 역할을 가진 사용자로 변경하십시오.
- 자원 관계 지정을 제거하여 구매자 관리자가 다른 사용자에게 속한 주문을 수정할 수 있도록 허용하십시오.
- 정책 이름, 표시 이름 및 설명을 갱신하십시오.
- 주문 수정용 명령어를 식별하십시오.

- 부록을 사용하여 구매자 관리자용 역할 기반 정책을 찾으십시오. 이 정책이 구매자 역할을 가진 사용자가 실행할 수 있는 명령어를 정의합니다. 반드시 이 정책의 자원 그룹을 갱신하여 구매자 관리자가 주문 수정용 명령어를 실행할 수 있도록 허용하십시오.
- 역할 기반 정책의 자원 그룹을 갱신하여 주문 수정용 명령어를 포함하도록 하십시오.

수행 단계

자원 레벨 정책 식별

1. 부록에서 주문 아래의 내용을 보고 변경할 자원 레벨 정책을 식별하십시오. 이 정책은 AllUsersExecuteOrderWriteCommandsOnOrderResource입니다.
2. 관리 콘솔에서 **액세스 관리 > 정책을 누르십시오.**
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 정책의 목록에서 **AllUsersExecuteOrderWriteCommandsOnOrderResource**를 선택하십시오.
5. 정책의 조치 그룹 이름 - OrderWriteCommands를 주목하십시오. 주문 작성용 명령어를 이름을 찾기 위해서는 이 조치 그룹을 볼 필요가 있습니다.

액세스 그룹 변경

1. **변경**을 눌러 정책 변경 페이지를 표시하십시오.
2. 사용자 그룹에서 **찾기**를 누르고 **구매자 관리자**를 선택하십시오.
3. **확인**을 누르십시오.
4. 정책의 이름, 표시 이름 및 설명을 갱신하여 액세스 그룹의 변경사항을 반영하십시오.
5. **확인**을 누르십시오.

주문 수정용 명령어 식별

1. **액세스 관리 > 조치 그룹**을 누르십시오.
2. 조치 그룹의 목록에서 **OrderWriteCommands**를 선택하십시오.
3. **변경**을 눌러 조치 그룹 변경 페이지를 표시하십시오. 주문 수정용 명령어의 이름을 기록하십시오.

```
com.ibm.commerce.order.commands.OrderCancelCmd
 com.ibm.commerce.order.commands.OrderCopyCmd-Write
 com.ibm.commerce.order.commands.OrderUnlockCmd
 com.ibm.commerce.orderitems.commands.OrderItemAddCmd
 com.ibm.commerce.orderitems.commands.OrderItemDeleteCmd
 com.ibm.commerce.orderitems.commands.OrderItemMoveCmd
 com.ibm.commerce.orderitems.commands.OrderItemUpdate.Cmd
```

반드시 이 명령어를 자원 그룹에 추가하여 구매자가 실행할 수 있는 명령어 목록에 포함되도록 해야 합니다.

주:

a. 명령어 com.ibm.commerce.orderitems.commands.AdminOrderItemUpdateCmd는 필요하지 않습니다.

b. 명령어 com.ibm.commerce.order.commands.OrderCopyCmd-Write를 자원 그룹에 추가할 때, 사용 가능한 자원 밑에 com.ibm.commerce.order .commands.OrderCopyCmd로 나타납니다.

구매자 관리자 역할용 역할 기반 정책 식별

1. 부록에서 역할 기반 정책 아래의 내용을 보고 구매자 관리자용 역할 기반 정책을 찾으십시오. 이 정책은 BuyerAdministratorsExecuteBuyersAdministratorsCommands입니다.
2. **액세스 관리** > **정책**을 누르십시오.
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 목록에서 정책을 찾으십시오.
5. 자원 그룹의 이름(BuyersAdministratorsCommmandsResourceGroup)에 주목하십시오.

   이것은 갱신해야 할 자원 그룹의 이름입니다.

주문 수정 명령을 포함하도록 역할 기반 정책의 자원 그룹 갱신

1. **액세스 관리** > **자원 그룹**을 누르십시오.
2. **BuyersAdministratorsCommandsResourceGroup**을 선택하십시오.
3. **변경**을 눌러 자원 그룹 변경 페이지를 표시하십시오.
4. **다음**을 눌러 자세히 보기 페이지를 표시하십시오.
5. 사용 가능한 자원 목록에서 주문 수정 명령을 선택하십시오.

```
com.ibm.commerce.order.commands.OrderCancelCmd
 com.ibm.commerce.order.commands.OrderCopyCmd
 com.ibm.commerce.order.commands.OrderUnlockCmd
 com.ibm.commerce.orderitems.commands.OrderItemAddCmd
 com.ibm.commerce.orderitems.commands.OrderItemDeleteCmd
 com.ibm.commerce.orderitems.commands.OrderItemMoveCmd
 com.ibm.commerce.orderitems.commands.OrderItemUpdate.Cmd
```

6. **추가**를 눌러 자원 그룹에 명령을 추가하십시오.
7. **완료**를 누르십시오.

변경사항으로 액세스 제어 레지스트리 갱신

1. **구성** > **레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

주문 시나리오 3: RMA 승인자가 모든 RMA를 승인하도록 허용

기본적으로 상점에 대한 RMA(Return Merchandise Authorization) 승인자는 자신의 상점에 대한 RMA만 승인할 수 있습니다. 어떤 경우에는 RMA 승인자가 모든 상점에 대한 RMA를 승인할 수 있도록 할 수 있습니다. 같은 조직에서 몇 개의 상점을 소유하고 있거나 동일인이 여러 상점에 대한 RMA 승인을 처리할 경우가 그렇습니다.

이 시나리오에서는 새 액세스 그룹을 작성하고 새 자원 레벨 정책에서 이를 사용할 것입니다. RMA 승인자가 모든 상점에 대해 RMA를 승인할 수 있도록 하려면, 다음을 수행해야 합니다.

- 부록을 사용하여 조직의 RMA 승인자가 해당 조직의 RMA를 승인하도록 하는 자원 레벨 정책을 찾으십시오.
- 정책에 사용되는 조치 그룹 이름과 자원 그룹의 이름이 주목하십시오.
- 정책의 액세스 그룹인 RMAApproversForOrg를 보고 포함하고 있는 역할에 주목하십시오. 액세스 그룹은 선택 기준으로 조직과 역할 둘 다를 사용하여 정의됩니다. 사용자에게 여러 조직에서 조치를 수행할 수 있는 권한을 부여하려면, 액세스 그룹이 조직 기준 없이 정의되어야 합니다.
- 같은 역할을 사용하지만 조직 기준을 포함하지 않는 새 액세스 그룹 RMAApprovers를 작성하십시오.
- 다음을 사용하여 새 정책을 작성하십시오.
  - 새 액세스 그룹 RMAApprovers
  - 기존 정책으로부터 조치 그룹
  - 기존 정책으로부터 자원 그룹

수행 단계

새 정책을 정의할 때 사용할 조치 그룹 및 자원 그룹 식별

1. 부록에서 주문 아래의 내용을 보고 상점에 대한 RMA를 승인할 수 있는 RMAApproversForOrg 권한을 부여하는 자원 레벨 정책을 찾으십시오. 정책은 RMAApproversForOrgExecuteRMAApproveCommandsOnRMAResource입니다.
2. 관리 콘솔에서 **액세스 관리 > 정책을 누르십시오.**
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 목록에서 정책을 찾으십시오.
5. 정책의 조치 그룹 이름(RMAApproveCommands)에 유의하십시오. 이것이 새 정책을 정의하는데 사용할 조치 그룹입니다.
6. 자원 그룹의 이름(RMADataResourceGroup)에 유의하십시오. 이것이 새 정책을 정의하는데 사용할 자원 그룹입니다.

7. 액세스 그룹의 이름(RMAApproversForOrg)에 유의하십시오. 이 액세스 그룹을 보고 새 액세스 그룹에 포함할 역할을 살펴보십시오.

새 액세스 그룹에 사용할 역할 식별

1. **액세스 관리** > **액세스 그룹**을 누르십시오.
2. 액세스 그룹 목록에서 **RMAApproversForOrg**를 선택하십시오.
3. **변경**을 누르십시오.
4. **기준**을 선택하여 기준 페이지를 표시하십시오.
5. 선택한 역할 및 조직 아래에서 액세스 그룹에 사용된 역할을 주목하십시오.
   - 고객 서비스 영업대표
   - 판매자
   - 판매 관리자
   - 운영 관리자
6. **취소**를 눌러 액세스 그룹 목록으로 리턴하십시오.

새 액세스 그룹 정의

1. **새로 만들기**를 눌러 새 액세스 그룹에 대한 자세히 보기 페이지를 표시하십시오.
2. 이름에 대해 RMAApprovers를 지정하십시오.
3. 설명에 대해 액세스 그룹의 설명을 지정하십시오.
4. 상위 조직에 대해 루트 조직을 선택하십시오.
5. **다음**을 눌러 새 액세스 그룹에 대한 기준 페이지를 표시하십시오.
6. **조직 및 역할에 기초한 기준**을 누르십시오.
7. 역할 목록에서 다음 역할을 선택하십시오.
   - **고객 서비스 영업대표**
   - **판매자**
   - **판매 관리자**
   - **운영 관리자**
8. **완료**를 누르십시오.

새 정책 정의

1. **액세스 관리** > **정책**을 누르십시오.
2. **새로 만들기**를 눌러 새 정책 페이지를 표시하십시오.
3. 이름에 대해 RMAApproversExecuteRMAApproveCommandsOnRMAResource를 지정하십시오.
4. 표시 이름에 대해 로컬 언어로 된 간단한 정책 설명을 지정하십시오.

5. 설명에 대해 정책이 하는 일에 대한 좀 더 자세한 설명을 로컬 언어로 지정하십시오.
6. 사용자 그룹에 대해 **찾기**를 누르고 **RMAApprovers**를 선택하십시오.
7. **확인**을 누르십시오.
8. 자원 그룹에 대해 **RMADataResourceGroup**을 선택하십시오.
9. 조치 그룹에 대해 **RMAApproveCommands**를 선택하십시오.
10. **확인**을 누르십시오.

변경사항으로 액세스 제어 레지스트리 갱신

1. **구성 > 레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

멤버쉽 시나리오 1: 사용자의 자체 등록 능력 제거

기본적으로 사용자는 등록된 조직에 속할 경우 스스로 등록할 수 있습니다. 또한 멤버쉽 운영자에게는 해당 조직에 속하는 사용자들을 등록할 수 있는 권한이 있습니다. 강력하게 액세스를 제어해야 하는 사이트의 경우, 자체 등록 능력을 제거하고 멤버쉽 운영자에 의해 사용자가 등록되도록 해야 할 수도 있습니다.

주: WebSphere Commerce Professional Edition에서는, 루트 조직, 기본 조직 및 판매 조직, 3개의 조직만이 있습니다.

이 시나리오에서는 사용자가 자체 등록할 수 있도록 허용하는 자원 레벨 정책을 제거하지만 멤버쉽 운영자가 해당 조직에서 사용자를 등록할 수 있는 정책을 그대로 유지할 것입니다.

사용자가 자체 등록할 수 있는 자원 레벨 정책을 삭제하려면 다음을 수행하십시오.

- 부록을 사용하여 사용자가 자체 등록할 수 있도록 허용하는 자원 레벨 정책을 찾으십시오.
- 정책을 삭제하십시오.

수행 단계

정책 삭제

1. 부록에서 멤버쉽 아래의 내용을 보고 사용자가 자체 등록할 수 있도록 허용하는 자원 레벨 정책을 찾으십시오. 정책은 다음과 같습니다.

   ```
   GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource
   ```

2. 관리 콘솔에서 **액세스 관리 > 정책을 누르십시오.**
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.

4. 정책 목록에서 **GuestsExecuteUserSelfRegistrationCommandsOnOrganization Resource**를 선택하십시오.
5. **삭제**를 선택하십시오.

변경사항으로 액세스 제어 레지스트리 갱신

1. **구성 > 레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

멤버쉽 시나리오 2: 등록되고 승인된 사용자만 주소 정보를 변경할 수 있도록 허용

기본적으로 사용자는 등록이 승인되거나 승인이 보류 중인 경우에 주소 정보를 수정할 수 있습니다. 어떤 경우에는 등록되고 승인된 사용자만 주소를 관리하도록 할 수 있습니다.

이 시나리오에서는, 사용자에게 주소 정보를 관리할 수 있는 권한을 부여하는 자원 레벨 정책에 대해 액세스 그룹을 변경할 것입니다.

- 부록을 사용하여 사용자가 주소 정보를 관리할 수 있도록 허용하는 자원 레벨 정책을 찾으십시오.
- 정책에 대해 액세스 그룹을 변경하십시오.

  액세스 그룹 `RegisteredApprovedUsers`는 어떤 역할도 포함하고 있지 않으므로, 이러한 변경에 대해 역할 기반 정책을 갱신하지 않아도 됩니다.

수행 단계

자원 레벨 정책의 액세스 그룹 변경

1. 부록에서 멤버쉽 아래의 내용을 보고 사용자가 주소 정보를 관리할 수 있도록 허용하는 자원 레벨 정책을 찾으십시오. 정책은 `NonRejectedUsersExecuteAddressManageCommandsOnUserResource`입니다.

   주: 거부되지 않는 사용자는 등록이 거부되지 않은 사용자입니다. 그러한 사용자의 등록은 승인되었거나 승인 보류 중입니다.
2. 관리 콘솔에서 **액세스 관리 > 정책을 누르십시오.**
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 정책의 목록에서 **NonRejectedUsersExecuteAddressManageCommands OnUserResource**를 선택하십시오.
5. **변경**을 눌러 정책 변경 페이지를 표시하십시오.
6. 사용자 그룹에 대해 **찾기**를 누르고 **RegisteredApprovedUsers**를 선택하십시오.

7. **확인**을 누르십시오.
8. 정책의 이름, 표시 이름 및 설명을 갱신하여 액세스 그룹의 변경사항을 반영하십시오.
9. **확인**을 누르십시오.

변경사항으로 액세스 제어 레지스트리 갱신

1. **구성 > 레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

멤버쉽 시나리오 3: 구성원 등록 담당자가 사용자를 등록할 수 있도록 허용

기본적으로 조직의 멤버쉽 운영자는 해당 조직의 구성원을 등록할 수 있는 권한을 가지고 있습니다. 액세스 그룹인 MemberAdministratorsForOrg에는 다양한 관리 태스크를 수행할 수 있는 권한이 있는 구매자 관리자 및 판매자 관리자와 같은 몇 가지의 역할이 있습니다. 어떤 경우에는 조직 구성원만 등록할 수 있는 권한이 부여되는 별도의 역할을 작성할 수 있습니다.

다음은 관련된 단계에 대한 개요입니다.

- 새 역할을 작성하고, 새 역할에 대해 새 액세스 그룹, 새 자원 그룹 및 역할 기반 정책을 작성하십시오.
- 새 역할을 사용하도록 기존 자원 레벨 정책을 수정하십시오.

이 시나리오에서는 다음을 수행할 것입니다.

- 구성원 등록 담당자라고 하는 새 역할을 정의하십시오.
- MemberRegistrars라고 하는, 구성원 등록 담당자 역할을 포함하는 새 액세스 그룹을 정의하십시오.
- 부록을 사용하여 멤버쉽 운영자가 구성원을 등록할 수 있도록 허용하는 자원 레벨 정책을 찾으십시오.
- 조치 그룹에서 조치의 이름에 주목하십시오. 이 조치를 사용하여 새 자원 그룹을 작성하고 새 역할에 대해 역할 기반 정책에서 이를 사용하십시오. 조치에 대한 역할 기반 정책에서 조치 그룹에는 단일 조치 실행만 포함됩니다. 자원 그룹에는 실행될 수 있는 조치(명령)가 있습니다.
- MemberRegistrationCommands라고 하는, 구성원 등록 명령을 포함하는 새 자원 그룹을 정의하십시오. 구성원 등록 담당자 역할에 대해 역할 기반 정책에서 이 자원 그룹을 사용하게 됩니다.
- 구성원 등록 담당자에 대해 MemberRegistrars 액세스 그룹 및 MemberRegistrationCommands 자원 그룹을 사용하는 새 역할 기반 정책을 정의하십시오.

- 구성원을 등록하고 액세스 그룹을 MembershipAdministrators에서 MemberRegistrars로 변경할 수 있는 사람을 정의하는 자원 레벨 정책을 수정하십시오.

수행 단계

새 역할 정의

1. 관리 콘솔에서 **액세스 관리 > 역할**을 누르십시오.
2. 역할 페이지에서 **새로 만들기**를 누르십시오.
3. 이름에 대해 구성원 등록 담당자를 지정하십시오.
4. 설명에 대해 구성원 등록 담당자에 대한 설명을 자국어로 지정하십시오.
5. **확인**을 누르십시오.

구성원 등록 담당자를 포함하는 새 액세스 그룹 정의

1. **액세스 관리 > 액세스 그룹**을 누르십시오.
2. 액세스 그룹 페이지에서 **새로 만들기**를 눌러 새 액세스 그룹에 대한 자세히 보기 페이지를 표시하십시오.
3. 이름에 대해 MemberRegistrars를 지정하십시오.
4. 상위 조직에 대해 루트 조직을 선택하십시오.
5. 설명에 대해 액세스 그룹에 대한 설명을 자국어로 지정하십시오.
6. **다음**을 눌러 새 액세스 그룹에 대한 기준 페이지를 표시하십시오.
7. **조직 및 역할 기준**을 누르십시오.
8. 역할 목록에서 **구성원 등록 담당자**를 선택하십시오.
9. **조직**을 눌러 역할이 사용자 고유 조직 내에 있어야 함을 지정하십시오.
10. **완료**를 누르십시오.

구성원 등록 담당자 역할 기반 정책에 대한 자원 그룹에서 사용할 조치 식별

1. 부록에서 멤버쉽 아래의 내용을 보고 멤버쉽 운영자가 사용자를 등록할 수 있도록 허용하는 정책을 찾으십시오. 정책은 다음과 같습니다.

   ```
   MembershipAdministratorsForOrgExecuteUserAdminRegistration
   CommandsOnOrganizationResource
   ```

2. **액세스 관리 > 정책**을 누르십시오.
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 목록에서 정책을 찾으십시오.
5. 정책의 조치 그룹 이름(UserAdminRegistration)에 주목하십시오. 이것은 구성원 등록 조치를 식별하기 위해 보아야 하는 조치 그룹입니다.
6. **액세스 관리 > 조치 그룹**을 누르십시오.
7. 조치 그룹 목록에서 **UserAdminRegistration**을 선택하십시오.

8. **변경**을 눌러 조치 그룹 변경 페이지를 표시하십시오.
9. 구성원 등록 명령의 이름(com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd)에 주목하십시오.

구성원 등록 담당자에 대해 역할 기반 정책에 사용될 새 자원 그룹 정의

1. **액세스 관리** > **자원 그룹**을 눌러 자원 그룹 페이지를 표시하십시오.
2. **새로 만들기**를 눌러 새 자원 그룹에 대한 일반 페이지를 표시하십시오.
3. 이름에 대해 UserAdminRegistrationCommands를 지정하십시오.
4. 표시 이름에 대해 자원 그룹에 대한 설명을 로컬 언어로 지정하십시오.
5. 설명에 대해 자원 그룹에 대한 자세한 설명을 로컬 언어로 지정하십시오.
6. 유형에 대해 **명시적 자원 그룹**을 선택하십시오.
7. **다음**을 누르십시오.
8. **다음**을 눌러 새 자원 그룹에 대한 자세히 보기 페이지를 표시하십시오.
9. 사용 가능한 자원 목록에서 다음을 선택하십시오.

   com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd
10. **추가**를 누르십시오.
11. **완료**를 누르십시오.

구성원 등록 담당자 역할에 대한 역할 기반 정책 정의

1. **액세스 관리** > **정책**을 누르십시오.
2. 정책 페이지에서 **새로 만들기**를 누르십시오.
3. 이름에 대해 **MemberRegistrarsExecuteUserAdminRegistrationCommands**를 지정하십시오.
4. 표시 이름에 대해 정책에 대한 설명을 로컬 언어로 지정하십시오.
5. 설명에 대해 정책이 하는 일에 대한 좀 더 자세한 설명을 로컬 언어로 지정하십시오.
6. 사용자 그룹에 대해 **찾기**를 누르고 **MemberRegistrars**를 선택하십시오.
7. **확인**을 누르십시오.
8. 자원 그룹에 대해 **UserAdminRegistrationCommands**를 선택하십시오.
9. 조치 그룹에 대해 **ExecuteCommandActionGroup**을 선택하십시오.
10. **확인**을 누르십시오.

새 액세스 그룹을 사용하도록 자원 레벨 정책 수정

1. 정책 목록에서 다음을 선택하십시오.

   MembershipAdministratorsForOrgExecuteUserAdminRegistrationCommandsOnOrganizationResource

2. **변경**을 눌러 정책 변경 페이지를 표시하십시오.
3. 정책의 이름, 표시 이름 및 설명을 갱신하여 액세스 그룹의 변경사항을 반영하십시오.
4. 사용자 그룹에 대해 **찾기**를 누르고 **MemberRegistrars**를 선택하십시오.
5. **확인**을 누르십시오.

변경사항으로 액세스 제어 레지스트리 갱신

1. **구성 > 레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

쿠폰 시나리오 1: 구매자만 쿠폰 회수 허용

기본적으로 모든 등록된 사용자는 쿠폰을 회수할 수 있습니다. 어떤 경우에는 WebSphere Commerce 내에서 구매자 역할을 가지고 있는 사용자로 쿠폰 회수를 제한할 수 있습니다.

이번 시나리오에서는 자원 레벨 정책뿐만 아니라 그와 연관된 역할 기반 정책을 변경합니다. 구매자 역할을 가지고 있는 사용자로 쿠폰 회수를 제한하려면, 다음을 수행해야 합니다.

- 부록을 사용하여 쿠폰을 회수할 수 있는 사람을 지정하는 자원 레벨 정책을 찾으십시오.
- 정책의 액세스 그룹을 모든 등록된 사용자에서 구매자 역할을 가진 사용자로 변경하십시오.
- 쿠폰 회수 명령을 식별하십시오.
- 부록을 사용하여 구매자(구매측)용 역할 기반 정책을 찾으십시오. 이 정책은 구매자(구매측) 역할을 가진 사용자가 실행할 수 있는 명령어를 정의합니다. 이 정책의 자원 그룹을 갱신하여 구매자가 쿠폰 회수 명령을 실행할 수 있도록 허용해야 합니다.
- 이 역할 기반 정책의 자원 그룹을 갱신하여 쿠폰 회수 명령을 포함하도록 하십시오.

수행 단계

자원 레벨 정책 및 조치 그룹 식별

1. 부록에서 쿠폰 아래의 내용을 보고 변경할 자원 레벨 정책을 식별하십시오. 정책은 다음과 같습니다.

   ```
   RegisteredApprovedUsersExecuteCouponRedemptionCommandsOnCouponWalletResource
   ```

2. 관리 콘솔에서 **액세스 관리 > 정책을 누르십시오.**
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.

4. 정책 목록에서 다음을 선택하십시오.

   RegisteredApprovedUsersExecuteCouponRedemption CommandsOnCouponWalletResource

5. 정책의 조치 그룹 이름(CouponRedemption)에 유의하십시오. 이것은 쿠폰 회수 명령의 이름을 찾기 위해 보아야 하는 조치 그룹입니다.

액세스 그룹 변경

1. **변경**을 눌러 정책 변경 페이지를 표시하십시오.
2. 사용자 그룹에 대해 **찾기**를 누르고 **구매자(구매측)**를 선택하십시오.
3. **확인**을 누르십시오.
4. 정책의 이름, 표시 이름 및 설명을 갱신하여 액세스 그룹의 변경사항을 반영하십시오.
5. **확인**을 누르십시오.

쿠폰 회수 명령 식별

1. **액세스 관리 > 조치 그룹**을 누르십시오.
2. 조치 그룹 목록에서 **CouponRedemption**을 선택하십시오.
3. **변경**을 눌러 조치 그룹 변경 페이지를 표시하십시오. 입찰을 작성하기 위한 명령의 이름에 주목하십시오.

   ```
   com.ibm.commerce.couponredemption.commands.CouponDSSCmd
     com.ibm.commerce.couponredemption.commands.UseCouponIdCmd
   ```

   반드시 이 명령어를 자원 그룹에 추가하여 구매자가 실행할 수 있는 명령어 목록에 포함되도록 해야 합니다.

구매자(구매측)용 역할 기반 정책 식별

1. 부록에서 역할 기반 정책 아래의 내용을 보고 구매자(구매측)용 역할 기반 정책을 찾으십시오. 정책은

   Buyers(buy-side)ExecuteBuyers(buyside)CommandsResourceGroup입니다.

2. **액세스 관리 > 정책**을 누르십시오.
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 목록에서 정책을 찾으십시오.
5. 자원 그룹의 이름(Buyers(buyside)CommandsResourceGroup)을 주목하십시오. 이것은 갱신해야 할 자원 그룹의 이름입니다.

역할 기반 정책에서 자원 그룹을 갱신하여 입찰 작성용 명령어가 포함되도록 하십시오.

1. **액세스 관리 > 자원 그룹**을 누르십시오.
2. **Buyers(buy-side)CommandsResourceGroup**을 선택하십시오.

3. **변경**을 눌러 자원 그룹 변경 페이지를 표시하십시오.
4. **다음**을 눌러 자세히 보기 페이지를 표시하십시오.
5. 사용 가능한 자원 목록에서 **com.ibm.commerce.couponredemption.commands.CouponDSSCmd** 및 **com.ibm.commerce.couponredemption.commands.UseCouponIdCmd**를 **선택하십시오.** 이것은 쿠폰 회수 명령입니다.
6. **추가**를 눌러 자원 그룹에 명령어를 추가하십시오.
7. **완료**를 누르십시오.

변경사항으로 액세스 제어 레지스트리 갱신

1. **구성 > 레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

쿠폰 시나리오 2: 쿠폰 운영자 및 상점 운영자의 e-coupon 특별 판매 허용

기본적으로 상점의 쿠폰 운영자는 해당 상점들에 대해 e-coupon 특별 판매를 작성할 수 있습니다. 어떤 경우에는 상점 운영자에게도 이 권한을 부여하고자 할 수 있습니다.

액세스 제어 정책의 탄력적인 설계는 이 변경을 구현하는 데 있어 몇 가지 방법을 제공합니다.

- e-coupon 특별 판매를 작성할 수 있는 사람을 지정하는 정책에 대한 액세스 그룹에 상점 운영자 역할을 추가할 수 있습니다.
- 상점 운영자가 e-coupon 특별 판매를 작성할 수 있도록 허용하는 새 정책을 작성할 수 있습니다.

이 시나리오는 첫 번째 접근법을 설명합니다. 쿠폰 운영자에게 쿠폰을 작성할 수 있는 권한을 부여하는 상점 운영자 역할을 자원 레벨 정책에 추가하는 방법을 보여줍니다.

이러한 변경을 수행하려면, 다음을 수행해야 합니다.

- 부록을 사용하여 e-coupon 특별 판매를 작성할 수 있는 사람을 지정하는 자원 레벨 정책을 찾으십시오.
- 상점 운영자 역할을 가지고 있는 사용자를 포함하도록 정책의 액세스 그룹을 변경하십시오.
- 자원 레벨 정책의 조치 그룹을 보고 e-coupon 특별 판매 작성 명령을 식별하십시오.
- 부록을 사용하여 상점 운영자에 대한 역할 기반 정책을 찾으십시오. 이 정책은 상점 운영자 역할을 가지고 있는 사용자가 실행할 수 있는 명령을 정의합니다. 반드시 이 정책의 자원 그룹을 갱신하여 상점 운영자가 e-coupon 특별 판매를 작성하기 위한 명령을 실행할 수 있도록 허용해야 합니다.

- 이 역할 기반 정책의 자원 그룹을 갱신하여 e-coupon 특별 판매 명령을 포함하도록 하십시오.

수행 단계

자원 레벨 정책에 대한 조치 그룹 및 액세스 그룹 식별

1. 부록에서 경매 아래의 내용을 보고 변경할 자원 레벨 정책을 식별하십시오. 정책은 다음과 같습니다.

   CouponAdministratorsForOrgExecuteCouponPromotionCreateCommands OnStoreEntityResource

2. 관리 콘솔에서 **액세스 관리 > 정책을 누르십시오.**
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 목록에서 정책을 찾으십시오.
5. 정책의 조치 그룹 이름(CouponPromotionCreate)에 유의하십시오. 이는 e-coupon 특별 판매 작성 명령의 이름을 찾기 위해 보아야 하는 조치 그룹입니다.
6. 정책의 액세스 이름(CouponAdministratorsForOrg)에 유의하십시오. 이는 상점 운영자 역할을 포함하기 위해 갱신해야 하는 액세스 그룹입니다.

액세스 그룹 변경

1. **액세스 관리 > 액세스 그룹**을 누르십시오.
2. 액세스 그룹 목록에서 **CouponAdministratorsForOrg**를 선택하십시오.
3. **변경**을 눌러 자세히 보기 페이지를 표시하십시오.
4. **기준**을 눌러 기준 페이지를 표시하십시오.
5. 역할 목록에서 **상점 운영자**를 선택하십시오.
6. **조직**을 눌러 역할이 사용자 고유 조직 내에 있어야 함을 지정하십시오.
7. **추가**를 누르십시오.
8. **확인**을 누르십시오.

e-coupon 특별 판매 작성 명령 식별

1. **액세스 관리 > 조치 그룹**을 누르십시오.
2. 조치 그룹 목록에서 **CouponPromotionCreate**를 선택하십시오.
3. **변경**을 눌러 조치 그룹 변경 페이지를 표시하십시오. e-coupon 특별 판매 작성 명령의 이름(com.ibm.commerce.tools.ecoupon.ECouponPromotionSaveCmd)에 유의하십시오. 상점 운영자가 실행할 수 있는 명령 목록을 포함하는 자원 그룹에 이 명령을 추가해야 합니다.

상점 운영자에 대한 역할 기반 정책 식별

1. 부록에서 역할 기반 정책 아래의 내용을 보고 상점 운영자에 대한 역할 기반 정책을 찾으십시오. 정책은 StoreAdministratorsExecuteStoreAdministrators CmdResourceGroup입니다.
2. **액세스 관리** > **정책**을 누르십시오.
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 목록에서 정책을 찾으십시오.
5. 자원 그룹의 이름(StoreAdministratorsCmdResourceGroup)에 유의하십시오. 이것은 갱신해야 할 자원 그룹의 이름입니다.

e-coupon 특별 판매 작성 명령을 포함하도록 역할 기반 정책에서 자원 그룹 갱신

1. **액세스 관리** > **자원 그룹**을 누르십시오.
2. **StoreAdministratorsCmdResourceGroup**을 선택하십시오.
3. **변경**을 눌러 자원 그룹 변경 페이지를 표시하십시오.
4. **다음**을 눌러 자세히 보기 페이지를 표시하십시오.
5. 사용 가능한 자원 목록에서 com.ibm.commerce.tools.ecoupon.ECouponPromotionSaveCmd를 선택하십시오. 이것은 e-coupon 특별 판매 작성 명령입니다.
6. **추가**를 누르십시오.
7. **완료**를 누르십시오.

변경사항으로 액세스 제어 레지스트리 갱신

1. **구성** > **레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

조달 시나리오 1: 조달 장바구니 관리자가 조직에서 작성된 주문에 대한 조달 장바구니를 관리할 수 있도록 허용

주: 이 시나리오는 WebSphere Commerce Professional Edition에서는 적용되지 않습니다.

기본적으로 조달 장바구니 관리자에게는 주문을 작성할 때 조달 장바구니를 관리할 수 있는 권한이 부여됩니다. 어떤 경우에는 조달 장바구니 관리자가 해당 조직의 구성원이 작성한 조달 장바구니를 관리할 수 있도록 권한을 확장할 수 있습니다.

이러한 변경을 수행하려면, 다음을 수행해야 합니다.

- 부록을 사용하여 조달 장바구니 운영자가 조달 장바구니를 관리할 수 있는 권한을 부여하는 자원 레벨 정책을 찾으십시오.
- 이 정책에 대한 자원 관계를 작성자에서 작성자와 같은 조직 엔티티로 변경하십시오.

수행 단계

자원 레벨 정책에 대한 자원 관계 변경

1. 부록에서 조달 아래의 내용을 보고 조달 장바구니 관리자가 주문에 대한 조달 장바구니를 관리할 수 있는 권한을 부여하는 자원 레벨 정책을 찾으십시오. 정책은 다음과 같습니다.

   ```
   ProcurementShoppingCartManagersExecuteProcurementShopping
   CartManageOnOrderResource
   ```

2. 관리 콘솔에서 **액세스 관리 > 정책을 누르십시오.**
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 정책 목록에서 다음을 선택하십시오.

   ProcurementShoppingCartManagersExecuteProcurementShopping CartManageOnOrderResource

5. **변경**을 눌러 정책 변경 페이지를 표시하십시오.
6. 관계에 대해 **sameOrganizationalEntityAsCreator**를 선택하십시오.
7. **확인**을 누르십시오.

변경사항으로 액세스 제어 레지스트리 갱신

1. **구성 > 레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

조달 시나리오 2: 조달 구매자 관리자가 조직에서 작성된 주문에 대한 조달 장바구니를 제출할 수 있도록 허용

주: 이 시나리오는 WebSphere Commerce Professional Edition에서는 적용되지 않습니다.

기본적으로 조달 장바구니 관리자는 주문을 작성할 경우에 조달 장바구니를 저장 및 제출할 수 있습니다. 어떤 경우에는 이러한 태스크에 대한 책임을 구분할 수도 있습니다. 조달 장바구니 관리자는 자신이 작성한 주문을 포함하는 조달 장바구니를 저장할 수 있지만, 주문 작성자와 같은 조직 내의 조달 구매자 관리자에게 조달 장바구니를 제출할 수 있는 권한을 부여할 수 있습니다. 이는 조달 구매자 관리자가 계획된 구매를 제출하기 전에 이를 검토하도록 할 경우에 유용합니다.

이러한 변경을 수행하려면, 다음을 수행해야 합니다.

- 부록을 사용하여 조달 장바구니 관리자에게 서비스 센터를 관리할 수 있는 센터 관리자 권한을 부여하는 자원 레벨 정책을 찾으십시오.
- 정책의 조치 그룹에서 조달 장바구니를 제출하기 위한 조치를 제거하십시오.
- 조달 장바구니 제출 명령을 포함하는 새 조치 그룹을 정의하십시오. 이 조치 그룹을 사용하여, 조달 구매자 관리자가 주문 작성자와 같은 조직 내에 있는 경우 조달 장바구니를 제출할 수 있는 권한을 부여하는 새 자원 레벨 정책을 정의합니다.
- 조달 구매자 관리자가 주문 작성자와 같은 조직 내에 있는 경우 조달 장바구니를 제출할 수 있는 권한을 부여하는 새 자원 레벨 정책을 작성하십시오.

수행 단계

자원 레벨 정책의 조치 그룹 및 자원 그룹 식별

1. 부록에서 조달 아래의 내용을 보고 조달 장바구니 관리자가 주문에 대한 조달 장바구니를 관리할 수 있는 권한을 부여하는 자원 레벨 정책을 찾으십시오. 정책은 다음과 같습니다.

   ```
   ProcurementShoppingCartManagersExecuteProcurementShopping
   ShoppingCartManageOnOrderResource
   ```

2. 관리 콘솔에서 **액세스 관리 > 정책을 누르십시오.**
3. 정책 목록에서 정책을 찾으십시오.
4. 조치 그룹의 이름(ProcurementShoppingCartManage)에 유의하십시오. 이 조치 그룹을 갱신하여 조달 장바구니를 제출하기 위한 조치를 제거합니다.
5. 자원 그룹의 이름(OrderDataResourceGroup)에 유의하십시오. 이 자원 그룹을 사용하여 새 자원 레벨 정책을 정의합니다.

자원 레벨 정책의 조치 그룹 갱신

1. **액세스 관리 > 조치 그룹**을 누르십시오.
2. 조치 그룹 목록에서 **ProcurementShoppingCartManage**를 선택하십시오.
3. **변경**을 눌러 조치 그룹 변경 페이지를 표시하십시오.
4. 선택된 조치 목록에서 **com.ibm.commerce.me.commands.SubmitShoppingCartCmd**를 선택하십시오. 이 조치가 있는 새 조치 그룹을 작성하고 새 자원 레벨 정책에서 조치 그룹을 사용하십시오.
5. **제거**를 누르십시오.
6. **확인**을 누르십시오.

새 조치 그룹 정의

1. **액세스 관리 > 조치 그룹**을 누르십시오.
2. 새 조치 그룹 페이지를 표시하려면 **새로 만들기**를 누르십시오.
3. 이름에 대해 ProcurementShoppingCartSubmit를 지정하십시오.
4. 표시 이름에 대해 조치 그룹에 대한 간단한 설명을 자국어로 지정하십시오.
5. 설명에 대해 조치 그룹이 하는 일에 대한 좀 더 자세한 설명을 자국어로 지정하십시오.
6. 사용 가능한 조치 목록에서 **com.ibm.commerce.me.commands.SubmitShoppingCartCmd**를 선택하십시오.
7. **추가**를 누르십시오.
8. **확인**을 누르십시오.

새 정책 정의

1. **액세스 관리 > 정책**을 누르십시오.
2. 보기에 대해 **루트 조직**을 눌러 사이트 레벨 정책을 표시하십시오.
3. **새로 만들기**를 눌러 새 정책 페이지를 표시하십시오.
4. 이름에 대해 다음을 지정하십시오.

   ```
   ProcurementBuyerAdministratorsExecuteProcurementShoppingCartSubmitCommands
   OnOrderResource
   ```

5. 표시 이름에 대해 로컬 언어로 된 간단한 정책 설명을 지정하십시오.
6. 설명에 대해 정책이 하는 일에 대한 좀 더 자세한 설명을 로컬 언어로 지정하십시오.
7. 사용자 그룹에 대해 **찾기**를 누르고 **ProcurementBuyerAdministrators**를 선택하십시오.
8. **확인**을 누르십시오.

9. 자원 그룹에 대해 **OrderDataResourceGroup**을 선택하십시오.
10. 조치 그룹에 대해 **ProcurementShoppingCartSubmit**를 선택하십시오.
11. 관계에 대해 **sameOrganizationalEntityAsCreator**를 선택하십시오.
12. 정책 유형에서 **템플리트 정책**을 선택하여 정책을 템플리트 정책으로 지정하십시오.
13. **확인**을 누르십시오.

액세스 제어 정책 레지스트리를 변경사항으로 갱신

1. **구성 > 레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

재고 시나리오 1: 서비스 센터 관리자가 서비스 센터를 갱신하지만 삭제하지는 않도록 허용

기본적으로 서비스 센터 관리자에게는 해당 상점과 연관되는 서비스 센터를 갱신 또는 삭제할 수 있는 권한이 있습니다. 어떤 경우에는 서비스 센터 관리자가 서비스 센터를 갱신할 수는 있지만 삭제하지는 못하도록 할 수 있습니다.

이러한 변경을 수행하려면, 다음을 수행해야 합니다.

- 부록을 사용하여 서비스 센터 관리자가 서비스 센터를 관리할 수 있는 권한을 부여하는 자원 레벨 정책을 찾으십시오.
- 정책의 조치 그룹에서 서비스 센터를 삭제하기 위한 조치를 제거하십시오.

수행 단계

서비스 센터 삭제 조치 제거

1. 부록에서 조달 아래의 내용을 보고 조달 장바구니 관리자가 주문에 대한 조달 장바구니를 관리할 수 있는 권한을 부여하는 자원 레벨 정책을 찾으십시오. 정책은 다음과 같습니다.

   ```
   FulfillmentCenterManagersForOrgExecuteFulfillmentCenter
   ManageCommandsOnFulfillmentResource
   ```

2. 관리 콘솔에서 **액세스 관리 > 정책을 누르십시오.**
3. 정책 목록에서 정책을 찾으십시오.
4. 조치 그룹의 이름(`FulfillmentCenterManage`)에 유의하십시오. 이 조치 그룹을 갱신하여 서비스 센터를 삭제하기 위한 조치를 제거해야 합니다.
5. **액세스 관리 > 조치 그룹**을 누르십시오.
6. 조치 그룹 목록에서 **FulfillmentCenterManage**를 선택하십시오.
7. **변경**을 눌러 조치 그룹 변경 페이지를 표시하십시오.

8. 선택된 조치 목록에서 **com.ibm.commerce.inventory.commands.FulfillmentCenterDeleteCmd**를 선택하십시오.
9. **제거**를 누르십시오.
10. **확인**을 누르십시오.

변경사항으로 액세스 제어 레지스트리 갱신

1. **구성 > 레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

재고 시나리오 2: 물류 관리자 및 운영 관리자만 서비스 센터를 작성, 갱신 또는 삭제할 수 있도록 허용

기본적으로 서비스 센터 관리자에게는 해당 상점과 연관되는 서비스 센터를 작성, 갱신 또는 삭제할 수 있는 권한이 있습니다. 서비스 센터 액세스 그룹에는 판매자, 물류 관리자 및 운영 관리자 역할이 포함됩니다. 어떤 경우에는 판매자에게 서비스 센터 관리자로서의 권한이 부여되지 않도록 할 수 있습니다.

이러한 변경을 수행하려면, 다음을 수행해야 합니다.

- 부록을 사용하여 서비스 센터 관리자가 서비스 센터를 관리할 수 있는 권한을 부여하는 자원 레벨 정책을 찾으십시오.
- 서비스 센터 관리자 액세스 그룹 정의에서 판매자 역할을 제거하십시오.

수행 단계

액세스 그룹에서 판매자 역할 제거

1. 부록에서 조달 아래의 내용을 보고 조달 장바구니 관리자가 주문에 대한 조달 장바구니를 관리할 수 있는 권한을 부여하는 자원 레벨 정책을 찾으십시오. 정책은 다음과 같습니다.

   ```
   FulfillmentCenterManagersForOrgExecuteFulfillmentCenterManage
   CommandsOnFulfillmentResource
   ```

2. 관리 콘솔에서 **액세스 관리 > 액세스 그룹**을 누르십시오.
3. 액세스 그룹 목록에서 **FulfillmentCenterManagersForOrg**를 선택하십시오.
4. **변경**을 눌러 액세스 그룹 변경 페이지를 표시하십시오.
5. **액세스 관리 > 액세스 그룹**을 누르십시오.
6. **변경**을 눌러 자세히 보기 페이지를 표시하십시오.
7. **기준**을 눌러 기준 페이지를 표시하십시오.
8. 역할 목록에서 **판매자**를 선택하십시오.

9. **제거**를 누르십시오.
10. **확인**을 누르십시오.

변경사항으로 액세스 제어 레지스트리 갱신

1. **구성 > 레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

비즈니스 인텔리전스 시나리오 1: 감사자가 비즈니스 인텔리전스 보고서를 볼 수 있도록 허용

기본적으로 인텔리전스 보고서 열람자는 상점에 대한 비즈니스 인텔리전스 보고서를 볼 수 있습니다. 어떤 경우에는 감사자라고 하는 새 역할을 작성하고 이 역할을 가지고 있는 사용자가 상점의 비즈니스 인텔리전스 보고서를 볼 수 있는 권한을 부여할 수 있습니다.

다음은 관련된 단계에 대한 개요입니다.

- 새 역할을 작성하고, 새 역할에 대해 새 액세스 그룹, 새 자원 그룹 및 역할 기반 정책을 작성하십시오.
- 자원 레벨 정책의 액세스 그룹에 새 역할을 추가하십시오.
- 감사자라고 하는 새 역할을 정의하십시오.
- 감사자라고 하는 감사자 역할을 포함하는 새 액세스 그룹을 정의하십시오.
- 상점에 대한 비즈니스 인텔리전스 보고서를 볼 수 있는 사람을 정의하는 자원 레벨 정책의 액세스 그룹에 감사자 역할을 추가하십시오.

이 시나리오에서는 다음을 수행할 것입니다.

- 부록을 사용하여 비즈니스 인텔리전스 보고서 열람자가 비즈니스 인텔리전스 보고서를 볼 수 있도록 허용하는 자원 레벨 정책을 찾으십시오.
- 조치 그룹에서 조치의 이름에 유의하십시오. 이 조치를 사용하여 새 자원 그룹을 작성하고 새 역할에 대해 역할 기반 정책에서 이를 사용하십시오. 조치에 대한 역할 기반 정책에서 조치 그룹에는 단일 조치 실행만 포함됩니다. 자원 그룹에는 실행될 수 있는 조치(명령)가 있습니다.
- `AuditorCommands`라고 하는, 비즈니스 인텔리전스 보고서 보기 명령을 포함하는 새 자원 그룹을 정의하십시오. 감사자 역할에 대한 역할 기반 정책에서 이 자원 그룹을 사용하게 됩니다.
- 감사자에 대해 감사자 액세스 그룹 및 AuditorCommands 자원 그룹을 사용하는 새 역할 기반 정책을 정의하십시오.

- 상점에 대한 비즈니스 인텔리전스 보고서를 볼 수 있는 사람을 정의하는 자원 레벨 정책의 액세스 그룹에 감사자 역할을 추가하십시오.

수행 단계

새 감사자 역할 정의

1. 관리 콘솔에서 **액세스 관리 > 역할**을 누르십시오.
2. 역할 페이지에서 **새로 만들기**를 누르십시오.
3. 이름에 대해 감사자를 지정하십시오.
4. 설명에 대해 감사자 역할에 대한 설명을 자국어로 지정하십시오.
5. **확인**을 누르십시오.

감사자 역할에 대한 새 액세스 그룹 정의

1. **액세스 관리 > 액세스 그룹**을 누르십시오.
2. 액세스 그룹 페이지에서 **새로 만들기**를 눌러 새 액세스 그룹에 대한 자세히 보기 페이지를 표시하십시오.
3. 이름에 대해 감사자를 지정하십시오.
4. 설명에 대해 액세스 그룹에 대한 설명을 로컬 언어로 지정하십시오.
5. 상위 조직에 대해 루트 조직을 선택하십시오.
6. **다음**을 눌러 새 액세스 그룹에 대한 기준 페이지를 표시하십시오.
7. **조직 및 역할 기준**을 누르십시오.
8. 역할 목록에서 **감사자**를 선택하십시오.
9. **추가**를 누르십시오.
10. **완료**를 누르십시오.

감사자 역할의 역할 기반 정책에 대한 자원 그룹에서 사용할 조치 식별

1. 부록에서 비즈니스 인텔리전스 아래의 내용을 보고 인텔리전스 보고서 열람자가 비즈니스 인텔리전스 보고서를 볼 수 있는 권한을 부여하는 정책을 찾으십시오. 정책은 다음과 같습니다.

   ```
   IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReport
   CommandsOnStoreEntityResource
   ```

2. 관리 콘솔에서 **액세스 관리 > 정책을 누르십시오.**
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 목록에서 정책을 찾으십시오.
5. 정책의 조치 그룹 이름(`ViewBusinessIntelligenceReport`)에 유의하십시오. 이것은 구성원 등록 조치를 식별하기 위해 보아야 하는 조치 그룹입니다.
6. **액세스 관리 > 조치 그룹**을 누르십시오.

7. 조치 그룹 목록에서 **ViewBusinessIntelligenceReport**를 선택하십시오.
8. **변경**을 눌러 조치 그룹 변경 페이지를 표시하십시오.
9. 비즈니스 인텔리전스 보고서를 보기 위한 명령의 이름(com.ibm.commerce.bi.commands.BIShowReportCmd)에 유의하십시오.

감사자 역할에 대해 역할 기반 정책에 사용될 새 자원 그룹 정의

1. **액세스 관리 > 자원 그룹**을 눌러 자원 그룹 페이지를 표시하십시오.
2. **새로 만들기**를 눌러 새 자원 그룹에 대한 일반 페이지를 표시하십시오.
3. 이름에 대해 AuditorCommands를 지정하십시오.
4. 표시 이름에 대해 자원 그룹에 대한 설명을 자국어로 지정하십시오.
5. 설명에 대해 자원 그룹에 대한 자세한 설명을 자국어로 지정하십시오.
6. **다음**을 누르십시오.
7. 유형에 대해 **명시적 자원 그룹**을 선택하십시오.
8. **다음**을 눌러 새 자원 그룹에 대한 자세히 보기 페이지를 표시하십시오.
9. 사용 가능한 자원 목록에서 **com.ibm.commerce.bi.commands.BIShowReportCmd**를 선택하십시오.
10. **추가**를 누르십시오.
11. **완료**를 누르십시오.

감사자 역할에 대한 역할 기반 정책 정의

1. **액세스 관리 > 정책**을 누르십시오.
2. 정책 페이지에서 **새로 만들기**를 누르십시오.
3. 이름에 대해 **AuditorsExecuteAuditorCommands**를 지정하십시오.
4. 표시 이름에 대해 정책에 대한 설명을 자국어로 지정하십시오.
5. 설명에 대해 정책이 하는 일에 대한 좀 더 자세한 설명을 자국어로 지정하십시오.
6. 사용자 그룹에 대해 **찾기**를 누르고 **감사자**를 선택하십시오.
7. **확인**을 누르십시오.
8. 자원 그룹에 대해 **AuditorCommands**를 선택하십시오.
9. 조치 그룹에 대해 **ExecuteCommandActionGroup**을 선택하십시오.
10. **확인**을 누르십시오.

자원 레벨 정책의 액세스 그룹에 감사자 역할 추가

1. **액세스 관리 > 액세스 그룹**을 누르십시오.
2. 액세스 그룹 목록에서 **IntelligenceReportViewersForOrg**를 선택하십시오.
3. **변경**을 눌러 액세스 그룹 변경 페이지를 표시하십시오.
4. **기준**을 눌러 액세스 그룹에 대한 기준 페이지를 표시하십시오.

5. 역할 목록에서 **감사자**를 선택하십시오.
6. **조직**을 눌러 역할이 사용자 고유 조직 내에 있어야 함을 지정하십시오.
7. **추가**를 누르십시오.
8. **확인**을 누르십시오.

변경사항으로 정책 레지스트리 갱신

1. **구성 > 레지스트리**를 누르십시오.
2. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
3. **갱신**을 누르십시오.

제 6 장 XML 파일을 사용한 액세스 제어 정책 사용자 정의

WebSphere Commerce 관리 콘솔에서 액세스 제어 정책 및 해당 파트에 대한 간단한 변경을 수행할 수 있습니다. 더 세밀하게 변경하려면 XML 파일을 직접 편집해야 합니다.

액세스 제어를 위해 XML 파일 변경을 시작하기 전에 *IBM WebSphere Commerce 프로그래머 안내서*에 있는 액세스 제어 관련 장을 읽어야 합니다. 이 장은 액세스 제어에 대한 기술적 개요을 제공하고 액세스 제어 정책에 의해 보호할 수 있는 JSP 템플리트, 사용자 정의 명령 및 엔티티 bean을 작성하는 방법에 대해 설명합니다.

*IBM WebSphere Commerce 프로그래머 안내서*에 제공된 지침에 따라 코드 사용자 정의를 완료했으면, 액세스 제어에 대한 XML 파일을 편집하여 필요로 하는 보호를 설정할 수 있습니다.

XML 파일 편집 및 로드를 통해서만 수행될 수 있는 변경사항

다음 변경사항은 적절한 XML 파일을 편집하고 로드해야만 수행될 수 있습니다.

- 새 명령 또는 보기 보호
- 관계 작성 또는 수정
- 관계 그룹 작성 또는 수정
- 새 자원 보호
- 속성 작성 또는 수정
- 복잡한 기준을 사용한 액세스 그룹 작성 또는 수정
- 복잡한 기준을 사용한 자원 그룹 작성 또는 수정

액세스 제어에 대한 XML 파일에 관한 정보

XML 변환기에 대한 WebSphere Commerce의 XML 파일, DTD 파일 및 XSL 파일에 대한 이름 및 설명은 아래 테이블에 나와 있습니다.

표 4. 액세스 제어에 대한 WebSphere Commerce XML 파일

파일 이름	설명
ACUserGroups_de_DE.xmll ACUserGroups_en_US.xml ACUserGroups_es_ES.xml ACUserGroups_fr_FR.xml ACUserGroups_it_IT.xml ACUserGroups_ja_JP.xml ACUserGroups_ko_KR.xml ACUserGroups_pt_BR.xml ACUserGroups_zh_CN.xml ACUserGroups_zh_TW.xml	지원되는 각 언어로 된 액세스 그룹 정의 및 설명.
defaultAccessControlPolicies.xml	기본 액세스 제어 정책, 조치 그룹, 자원 그룹, 관계, 관계 그룹, 조치, 자원 카테고리 및 속성의 정의를 포함하는 기본 파일.
defaultAccessControlPolicies_de_DE.xml defaultAccessControlPolicies_en_US.xml defaultAccessControlPolicies_es_ES.xml defaultAccessControlPolicies_fr_FR.xml defaultAccessControlPolicies_it_IT.xml defaultAccessControlPolicies_ja_JP.xml defaultAccessControlPolicies_ko_KR.xml defaultAccessControlPolicies_pt_BR.xml defaultAccessControlPolicies_zh_CN.xml defaultAccessControlPolicies_zh_TW.xml	지원되는 각 언어로 된 기본 액세스 제어 정책, 조치 그룹, 조치, 자원 그룹, 자원 카테고리, 관계 및 속성의 표시 이름 및 설명을 포함하는 파일.
ACPoliciesfilter.xml	데이터베이스에서 변경된 액세스 제어 정보 추출에 사용된 필터 파일.
accesscontrolpolicies.dtd	액세스 제어 정책 XML 파일은 이 DTD를 따라야 합니다.
accesscontrolpoliciesnls.dtd	액세스 제어 정책 NLS(national language specific) XML 파일(표시 이름 및 설명만)은 이 DTD를 따라야 합니다.
ACUserGroups_en_US.dtd	액세스 제어 사용자 그룹 XML 파일은 이 DTD를 따라야 합니다.
accesscontrol.xsl	액세스 제어 정책 XML 파일의 XSL 변환 규칙 파일.

표 4. 액세스 제어에 대한 WebSphere Commerce XML 파일 (계속)

accesscontrolnls.xsl	액세스 제어 정책 NLS XML 파일(표시 이름 및 설명만)의 XSL 변환 규칙 파일.
ACUserGroup.xsl	액세스 그룹 XML 파일의 XSL 변환 규칙 파일.
wcstoacpolicies.xsl	추출 후 액세스 제어 정책 XML 파일을 작성하는 ExtractedACPolicies.xml 파일의 XSL 변환 규칙 파일.
wcstoacpoliciesnls.xsl	추출 후 액세스 제어 정책 NLS XML 파일을 작성하는 ExtractedACPolicies.xml의 XSL 변환 규칙 파일.
wcstoacusergroup.xsl	추출 후 액세스 그룹 XML 파일을 작성하는 ExtractedACPolicies.xml 파일의 XSL 변환 규칙 파일.

XML 파일 사용자 정의

보기 보호

URL에서 직접 호출하거나, 다른 명령에서의 경로 재지정으로 실행되는 보기를 표시하려면 역할 기반 액세스 제어 정책이 필요합니다. 다음 예는 보기에 대한 역할 기반 정책을 표시합니다.

```
<Policy Name="ProductManagersExecuteProductManagersViews"
OwnerID="RootOrganization"
UserGroup="ProductMangers"
ActionGroupName="ProductMangersViews"
ResourceGroupName="ViewCommandResourceGroup">
</Policy>
```

ResourceGroup 이름인 ViewCommandResourceGroup은 이것이 보기에 대한 역할 기반 정책임을 표시합니다. 정책은 ProductManagers 사용자 그룹의 사용자들이 ProductMangersViews 조치 그룹의 보기를 표시할 수 있음을 알려줍니다.

다음은 ProductMangersViews 조치 그룹의 예입니다.

```
<ActionGroup Name="ProductManagersViews"
OwnerID="RootOrganization">

<ActionGroupAction Name="ProductImageView"/>
<ActionGroupAction Name="ProductManufacturerView"/>
<ActionGroupAction Name="ProductSalesTaxView"/>

 </ActionGoup>
```

위의 예는 ProductManagerViews 조치 그룹에서 수행할 수 있는 세 가지의 조치인 ProductImageView, ProductManufacturerView, ProductSalesTaxView를 나열합니다.

다음은 ProductImageView 조치 정의의 예입니다.

```
<Action Name="ProductImageView"
CommandName="ProductImageView">
</Action>
```

Name 속성인 ProductImageView는 조치를 조치 그룹과 연관짓는 것과 같이 XML내의 어디에서나 조치를 참조하기 위한 태그로 사용됩니다.

주: VIEWREG 테이블의 VIEWNAME 열에 저장된 보기의 이름은 조치 정의에서 CommandName과 일치해야 합니다. CommandName의 값은 ACACTION 테이블의 ACTION 열에 저장됩니다. Name 와 CommandName 속성이 동일할 필요는 없습니다.

기존 정책을 사용하여 새 보기 추가

기존의 역할 기반 보기 정책을 사용하여 역할에 의해 액세스 가능한 새 보기를 추가하려면 다음을 수행하십시오.

1. XML 파일에서 보기 이름이 MyNewView인 새 조치 정의를 작성하십시오.

   ```
   <Action Name="MyNewView"
   CommandName="MyNewView">
   </Action>
   ```

2. 이 보기에 대한 액세스를 가지고 있어야 하는 역할을 판별하고, 새 조치를 XML 파일에서 해당되는 조치 그룹과 연관시키십시오.

   ```
   <ActionGroup Name="ProductManagersViews"
   OwnerID="RootOrganization">

   <ActionGroupAction Name="ProductImageView"/>
   <ActionGroupAction Name="ProductManufacturerView"/>
   <ActionGroupAction Name="ProductSalesTaxView"/>
   <ActionGroupAction Name="MyNewView"/>

   </ActionGroup>
   ```

3. XML 변경사항을 데이터베이스로 로드하십시오. XML 변경사항에 대한 자세한 정보는 114 페이지의 『변경사항을 데이터베이스에 로드』를 참조하십시오.
4. 관리 콘솔에서 액세스 제어 정책 레지스트리를 갱신하십시오.

이 조치 그룹을 포함하는 역발 기반 정책이 이미 있으므로, 이제 보기를 사용할 수 있습니다.

새 정책을 사용하여 새 보기 추가

기존의 역할 기반 정책을 가지고 있지 않은 새 역할에 의해 액세스 가능한 새 보기를 추가하려면, 다음을 수행하십시오.

1. XML 파일에서 보기 이름이 MyNewView인 새 조치 정의를 작성하십시오.

   ```
   <Action Name="MyNewView
   CommandName="MyNewView">
   </Action>
   ```

2. 새 역할과 연관될 새 조치 그룹을 작성하십시오.

```
<ActionGroupName="XYZViews"
OwnerID="RootOrganization">
</ActionGroup>
```

3. 새 조치를 새 조치 그룹과 연관시키십시오.

```
<ActionGroupName="XYZViews"
OwnerID="RootOrganization">

<ActionGroupAction Name="MyNewView"/>

</ActionGroup>
```

4. 새 조치 그룹을 참조하는 정책을 작성하십시오.

```
<Policy Name="XYZExecuteXYZViews"
OwnerID="RootOrganization"
UserGroup="XYZ"
ActionGroupName="XYZViews"
ResourceGroupName="ViewCommandResourceGroup">
</Policy>
```

5. XML 변경사항을 데이터베이스로 로드하십시오. XML 변경사항에 대한 자세한 정보는 114 페이지의 『변경사항을 데이터베이스에 로드』를 참조하십시오.
6. 관리 콘솔에서 액세스 제어 정책 레지스트리를 갱신하십시오.

이제 보기를 사용할 수 있습니다.

제어기 명령 보호

모든 제어기 명령은 역할 기반 액세스 제어 정책이 있어야 실행됩니다. 명령이 자원 레벨 확인을 수행하는 경우 제어기 또는 태스크 명령에도 자원 레벨 정책이 필요합니다. 자세한 정보는 94 페이지의 『자원 레벨 액세스 제어 구현』을 참조하십시오. 다음 예는 제어기 명령에 대한 역할 기반 정책을 표시합니다.

```
<Policy Name="SellersExecuteSellersCmdResourceGroup"
OwnerID="RootOrganization"
UserGroup="Sellers"
ActionGroupName="ExecuteCommandActionGroup"
ResourceGroupName="SellersCmdResourceGroup">
</Policy>
```

ActionGroupName인 ExecuteCommandActionGroup은 이것이 제어기 명령에 대한 역할 기반 정책임을 표시합니다. 정책은 판매자 액세스 그룹의 사용자가 SellersCmdResourceGroup 자원 그룹의 명령을 실행할 수 있음을 알려줍니다.

다음은 SellersCmdResourceGroup 자원 그룹 정의의 예입니다.

-
```
<ResourceGroup Name="SellersCmdResourceGroup" OwnerID="RootOrganization">
<ResourceGroupResource Name="com.ibm.contract.commands.Contract
CancelCmdResourceCategory"/>
<ResourceGroupResource Name="com.ibm.contract.commands.Contract
```

```
CloseCmdResourceCategory"/>
<ResourceGroupResource Name="com.ibm.contract.commands.Contract
CreateCmdResourceCategory"/>
</ResourceGroup>
```

위의 예는 제어기 명령에 응답하는 자원 그룹 내의 다음 세 자원을 보여줍니다.

- com.ibm.contract.commands.ContractCancelCmdResourceCategory
- com.ibm.contract.commands.ContractCloseCmdResourceCategory
- com.ibm.contract.commands.ContractCreateCmdResourceCategory

다음은 자원의 견본 정의입니다.

```
<ResourceCategory Name="com.ibm.commerce.contract.commands.Contract
CloseCmdResourceCategory"
ResourceBeanClass="com.ibm.commerce.contract.commands.ContractCloseCmd">

<ResourceAction Name="ExecuteCommand"/>

</ResourceCategory>
```

Name 속성인 com.ibm.commerce.contract.commands.
ContractCloseCmdResourceCategory는 XML 파일에서 자원을 참조하기 위한 태그로 사용됩니다. ResourceAction 이름인 ExecuteCommand는 자원에 대해 작동할 수 있는 조치를 지정하는 데 사용됩니다. 이 정보는 특정 자원에 해당되는 조치 선택 상자에 대량 자료 반입하기 위해 액세스 제어 정책을 사용할 때 관리 콘솔에서 사용됩니다. 이 경우, 조치 Execute이 지정됩니다. Execute 조치는 다음과 같이 정의됩니다.

```
<Action Name="ExcecuteCommand
CommandName="Execute">
</Action>
```

주: 제어기 명령의 인터페이스 이름은 자원 정의의 ResourceBeanClass와 일치해야 합니다. ResourceBeanClass의 값은 ACRESCGRY 테이블의 RESCLASSNAME 열에 저장됩니다. 이 명령은 AccCommand 인터페이스를 확장하는 ControllerCommand 인터페이스를 확장하므로 자원으로 사용됩니다. AccCommand 인터페이스는 다시 Protectable 인터페이스를 확장합니다. 이러한 인터페이스에 대한 자세한 정보는 *IBM WebSphere Commerce 프로그래머 안내서*를 참조하십시오.

기존 정책을 사용하여 새 제어기 명령 추가

기존의 역할 기반 제어기 명령 정책을 가지고 있는 역할에 의해 액세스할 수 있는 새 제어기 명령을 추가하려면, 다음을 수행하십시오.

1. 제어기 명령의 인터페이스 이름에 해당되는 새 자원 정의를 XML 파일에서 작성하십시오.

```
<ResourceCategory  Name="com.xyz.commands.MyNewControllerCmdResourceCategory"
ResourceBeanClass="com.xyz.commands.MyNewControllerCmd">
<ResourceAction Name="ExecuteCommand"/>
</ResourceCategory>
```

2. 명령에 대한 액세스를 가지고 있어야 하는 역할을 판별하고, 새 조치를 XML 파일에서 해당되는 자원 그룹과 연관시키십시오.

```
<ResourceGroup Name="SellersCmdResourceGroup" OwnerID="RootOrganization">
<ResourceGroupResource Name="com.ibm.commerce.contract.
commands.ContractCancelCmdResourceCategory"/>
<ResourceGroupResource Name="com.ibm.commerce.contract.
commands.ContractCloseCmdResourceCategory"/>
<ResourceGroupResource Name="com.ibm.commerce.contract.
commands.ContractCreateCmdResourceCategory"/>

<ResourceGroupResource Name="com.xyz.commands.
MyNewControllerCmdResourceCategory"/>

</ResourceGroup>
```

3. XML 변경사항을 데이터베이스로 로드하십시오. XML 변경사항에 대한 자세한 정보는 114 페이지의 『변경사항을 데이터베이스에 로드』를 참조하십시오.
4. 관리 콘솔에서 액세스 제어 정책 레지스트리를 갱신하십시오.

이 자원 그룹을 포함하는 역발 기반 정책이 이미 있으므로 자원 레벨 확인을 수행하지 않는 경우 이제 새 제어기 명령을 사용할 수 있습니다.

새 정책을 사용하여 새 제어기 명령 추가

기존의 역할 기반 정책을 가지고 있지 않은 새 역할에 의해 액세스될 새 제어기 명령을 추가하려면, 다음을 수행하십시오.

1. 제어기 명령의 인터페이스 이름에 해당되는 새 자원 정의를 XML 파일에서 작성하십시오. 예에 대해서는 92 페이지의 『기존 정책을 사용하여 새 제어기 명령 추가』의 1단계를 참조하십시오.
2. 다음과 같이 새 역할과 연관될 새 자원 그룹을 작성하십시오.

```
<ResourceGroup Name="XYZCmdResourceGroup" OwnerID="RootOrganization">
</ResourceGroup>
```

3. 다음과 같이 새 자원을 새 자원 그룹과 연관시키십시오.

```
<ResourceGroup Name="XYZCmdResourceGroup" OwnerID="RootOrganization">
<ResourceGroupResource Name="com.xyz.commands.MyNewControllerResourceCategory"/>
</ResourceGroup>
```

4. 다음과 같이 새 자원 그룹을 참조하는 정책을 작성하십시오.

```
<Policy Name="XYZExecuteXYZsCmdResourceGroup"
OwnerID="RootOrganization"
UserGroup="XYZ"
ActionGroupName="ExecuteCommandActionGroup"
ResourceGroupName="XYZCmdResourceGroup">
</Policy>
```

5. XML 변경사항을 데이터베이스로 로드하십시오. XML 변경사항에 대한 자세한 정보는 114 페이지의 『변경사항을 데이터베이스에 로드』를 참조하십시오.

6. 관리 콘솔에서 액세스 제어 정책 레지스트리를 갱신하십시오.

자원 레벨 확인을 수행하지 않는 경우 이제 제어기 명령을 사용할 수 있습니다.

자원 레벨 액세스 제어 구현

자원 레벨 액세스 제어를 제어기나 태스크 명령에 추가할 수 있습니다. 자원 레벨 확인은 명령의 getResources() 메소드에 의해 리턴되는 데이터를 기초로 WebSphere Commerce 런타임에서 수행됩니다. 또한 자원 레벨 확인은 void checkIsAllowed (Object resource, String action) throws ECException 메소드를 통해 직접 액세스 제어 정책 관리자를 호출하여 명령의 performExcecute() 부분 동안 수행할 수도 있습니다. 이 메소드는 현재 사용자가 지정된 자원에서 지정된 조치를 수행할 수 없는 경우 ECApplicationException을 일으킵니다.

주: 기본적으로 getResources() 메소드는 널(Null)값을 리턴하므로 자원 레벨 확인이 수행되지 않습니다.

다음 인스턴스에서 새 명령에 대한 자원 레벨 정책을 작성해야 합니다.

- 새 명령은 자원 레벨 확인을 수행하는 또 다른 명령으로부터 확장됩니다.
- 새 명령 자체가 자원 레벨 액세스 제어 확인을 수행합니다.

다음은 자원 레벨 정책의 예입니다.

```
<Policy Name="ContractMangersForOrgExecuteContractManageCommandsOnContractResource"
OwnerID="RootOrganization"
UserGroup="ContractManagersForOrg"
ActionGroupName="ContractManage"
ResourceGroupName="ContractDataResourceGroup"
PolicyType="template">
</Policy>
```

여기서

Name: 정책의 이름.

PolicyType: 정책 유형. 이것은 템플리트 정책으로 자원 및 해당 상위를 소유하는 조직 엔티티에 동적으로 적용됩니다.

OwnerID: 정책을 소유하는 구성원. 이것은 템플리트 정책으로, 조직 엔티티 및 해당되는 상위 요소를 소유하는 자원이 되도록 동적으로 변경됩니다. 정책이 액세스 제어 정책 관리자에 의해 적용되기 때문입니다.

UserGroup: 정책이 이 그룹의 사용자에게 적용됩니다. 역할이 자원 조직 엔티티 및 해당 상위로 동적 확장되는 액세스 그룹의 이름 지정 규칙은 그룹 이름에 ForOrg를 추가하는 것입니다.

ActionGroupName: 자원에서 수행할 조치를 포함하는 조치 그룹의 이름.

ResourceGroupName: 조치를 취할 자원을 포함하는 자원 그룹의 이름.

위 예에서 조치 그룹 ContractManage는 ContractDataResourceGroup에서 작동하는 명령 세트를 포함하는 조치 그룹입니다. 다음은 위 자원 레벨 정책에서 사용되는 조치 그룹의 예입니다.

```
<ActionGroupName="ContractManage" OwnerID="RootOrganization">
<ActionGroupActionName="com.ibm.commerce.contract.commands.ContractCancelCmd"/>
<ActionGroupActionName="com.ibm.commerce.contract.commands.ContractCloseCmd"/>
<ActionGroupActionName="com.ibm.commerce.contract.commands.ContractDeleteCmd"/>
</ActionGroup>
```

이전에 역할 기반 정책에 대한 자원으로 정의된 명령이 이제는 조치로 정의되었습니다. 다음은 위 ContractManage 그룹 일부인 조치의 견본 정의입니다.

```
<Action Name="com.ibm.commerce.contract.commands.ContractCloseCmd"
CommandName="com.ibm.commerce.contract.commands.ContractCloseCmd">
</Action>
```

주: CommandName 값은 자원 레벨 확인을 수행하는 명령의 인터페이스 이름과 일치해야 합니다.

대부분의 명령은 엔터프라이즈 bean과 함께 작동합니다. 이러한 bean은 대개 자원 레벨 정책이 보호하는 자원입니다. 다음은 위 자원 정책에 사용된 자원 그룹의 견본 정의입니다.

```
<ResourceGroup Name="ContractDataResourceGroup" OwnerId="RootOrganization">
<ResourceGroupResource Name="com.ibm.commerce.contract.
objects.ContractResourceCategory"/>
</ResourceGroup>
```

이 예에서 ContractDataResourceGroup이 정의되고 한 자원으로 구성됩니다. 자원은 다음과 같이 정의됩니다.

```
<ResourceCategory Name="com.ibm.commerce.contract.objects.ContractResourceCategory"
ResourceBeanClass="com.ibm.commerce.contract.objects.Contract"
<ResourceAction Name="com.ibm.commerce.contract.commands.ContractCancelCmd"/>
<ResourceAction Name="com.ibm.commerce.contract.commands.ContractCloseCmd"/>
<ResourceAction Name="com.ibm.commerce.contract.commands.ContractDeleteCmd"/>
 </ResourceCategory>
```

여기서

Name: XML 파일의 다른 위치에서 이 자원을 참조하는데 사용하는 태그.

ResourceBeanClass: 보호할 자원을 나타내는 클래스. 이 클래스는 Protectable 인터페이스를 구현해야 합니다. 자원이 엔터프라이즈 bean인 경우 원격 인터페이스는 Protectable 인터페이스를 확장해야 합니다.

ResourceAction: 이 자원에서 작동할 조치를 지정합니다. 이 정보는 특정 자원에 유효한 조치를 판별할 때 관리 콘솔에서 사용합니다.

주: Protectable 인터페이스에 대한 자세한 정보는 *WebSphere Commerce 프로그래머 안내서*를 참조하십시오.

데이터 bean 보호

데이터 bean은 비즈니스 오브젝트에 대한 정보를 포함하여 웹 페이지에 오브젝트 정보를 표시하기 위해 사용됩니다. 동적 웹 페이지는 보통 WebSphere Commerce 내의 보기에 맵핑되고 이러한 보기는 역할 기반 정책에 의해 보호받습니다. 일부의 경우 데이터 bean(존재하는 경우)을 보호하여 웹 페이지의 컨텐츠를 좀더 보호해야 할 필요가 있습니다.

데이터 bean이 `DataBeanManager.activate(..)` 메소드를 사용하여 대량 반입되면 데이터 bean 관리자는 데이터 bean에서의 액세스 제어를 실시합니다. 데이터 bean은 Delegator 인터페이스를 사용하여 직간접적으로 보호할 수 있습니다. 직접적으로 보호된 데이터 bean은 Protectable 인터페이스도 구현합니다. 간접적으로 보호된 데이터 bean이 Delegator 인터페이스를 구현하지 않거나 `getDelegate()` 메소드에 대한 널(Null)값을 리턴하는 경우 데이터 bean은 보호되지 않으며 아무에게나 표시될 수 있습니다.

주: Protectable 인터페이스에 대한 자세한 정보는 *WebSphere Commerce 프로그래머 안내서*를 참조하십시오.

다음은 데이터 bean에 대한 자원 레벨 정책의 예입니다.

```
<Policy Name="AllUsersDisplayOrderDataBeanResourceGroup"
OwnerID="RootOrganization"
UserGroup="AllUsers"
ActionGroupName="DisplayDataBeanActionGroup"
ResourceGroupName="OrderDataBeanResourceGroup"
RelationName="creator">
```

ActionGroupName인 `DisplayDataBeanActionGroup`은 이 정책이 데이터 bean에 대한 정책임을 나타냅니다. 이 조치 그룹은 하나의 `Display` 조치를 포함합니다.

여기서

`Name`: 이 정책의 이름.

`UserGroup`: 정책이 적용되는 사용자를 포함하는 액세스 그룹. 이 경우 모든 사용자를 포함합니다.

`ActionGroupName`: `DisplayDataBeanActionGroup` 값은 데이터 bean에 대한 자원 레벨 정책을 나타냅니다.

`ResourceGroupName`: 보호할 데이터 bean을 포함하는 자원 그룹의 이름.

RelationName: 사용자와 자원 간에 유지되어야 하는 관계. 이 경우 사용자는 비즈니스 Order 자원의 작성자여야 합니다.

OrderDataBeanResourceGroup은 다음과 같이 정의됩니다.

```
<ResourceGroup Name="OrderDataBeanResourceGroup" OwnerID="RootOrganization">
<ResourceGroupResource Name="com.ibm.commerce.order.beans.
OrderListDataBeanResourceCategory"/>
<ResourceGroupResource Name="com.ibm.commerce.order.beans
.OrderDataBeanResourceCategory"/>
</ResourceGroup>
```

OrderDataBeanResourceGroup은 두 자원으로 구성됩니다. 다음은 데이터 bean에 대한 견본 자원 정의입니다.

```
<ResourceCategory Name="com.ibm.commerce.order.beans.OrderDataBeanResourceCategory"
ResourceBeanClass="com.ibm.commerce.order.beans.OrderDataBean">
<ResourceAction Name="DisplayDataBean"/>
</ResourceCategory>
```

여기서

Name: XML 파일에서 이 자원을 참조하는데 사용되는 태그.

ResourceBeanClass: 직접적으로 보호되는 데이터 bean의 클래스 이름. 이 클래스는 Protectable 인터페이스를 구현해야 합니다.

ResourceAction: 관리 콘솔에서 편집 중인 정책에 필요한 요소. 이 경우 이 요소는 Display가 이 자원에서 수행하기에 올바른 조치임을 나타냅니다.

속성별로 자원 그룹화

자원 그룹은 ACRESGRP 테이블의 CONDITIONS 열을 사용하여 전체적으로 정의할 수 있습니다. CONDITIONS 열은 자원을 그룹화하는데 사용하는 제한자 및 속성값 쌍을 포함하는 XML 문서를 지정합니다. 이러한 유형의 자원 그룹을 암시적 자원 그룹이라고 하며 대개 자원의 클래스 이름이 충분하지 않을 때 사용됩니다. 예를 들어, 액세스 제어 정책이 P(보류 중) 또는 E(고객 서비스 영업대표가 편집 중) 상태인 Order 자원에 적용되는 경우 자원 그룹을 이에 대해 정의할 수 있습니다.

주: 클래스 이름이 아닌 속성별로 자원을 그룹화하려면 자원이 Groupable 인터페이스를 구현해야 합니다. Groupable 인터페이스에 대한 자세한 정보는 *IBM WebSphere Commerce 프로그래머 안내서*를 참조하십시오.

다음은 Order 자원 그룹에 대한 예입니다.

```
<ResourceGroup  Name="OrderResourceGroupwithPEStatus"
OwnerID="RootOrganization">
<ResourceCondition>
 <![CDATA[
  <profile>
   <andListCondition>
<orListCondition>
```

```
      <simpleCondition>
       <variable name="Status"/>
       <operator name="="/>
       <value data="P"/>
      </simpleCondition>
      <simpleCondition>
       <variable name="Status"/>
       <operator name="="/>
       <value data="E"/>
      </simpleCondition>
 </orListCondition>
      <simpleCondition>
       <variable name="classname"/>
       <operator name="="/>
       <value data="com.ibm.commerce.order.objects.Order"/>
      </simpleCondition>
    </andListCondition>
   </profile>
 ]]>
</ResourceCondition>
</ResourceGroup>
```

여기서

Name: ACRESGRP 테이블의 GRPNAME 열에 저장된 자원 그룹의 이름.

OwnerID: 자원 그룹의 소유자. 루트 조직이어야 합니다.

<ResourceCondition>: 자원 그룹을 정의하기 위해 ACRESGRP 테이블의 CONDITIONS 열로 로드할 데이터를 지정합니다.

<![CDATA[...]]>: 정확히 입력한 대로 사용되는 문자 데이터 절을 의미합니다.

<profile>: 모든 자원 조건에 필요한 매개변수.

자원 그룹 정의의 필수 구성요소는 name="classname"을 갖는 <simpleCondition> 요소입니다. 이 요소는 그룹이 적용되는 자원의 java 클래스를 식별합니다. Java 클래스인 com.ibm.commerce.order.objects.Order를 다음 예에서 볼 수 있습니다.

```
<simpleCondition>
   <variable name="classname"/>
   <operator name="="/>
   <value data="com.ibm.commerce.order.objects.Order"/>
   </simpleCondition>
```

다음 예는 상태가 P여야 하는 com.ibm.commerce.objects.order.objects.Order 자원에서의 조건을 지정합니다.

```
<simpleCondition>
<variable name="Status"/>
       <operator name="="/>
       <value data="P"/>
   </simpleCondition>
```

위 예에서 <variable name="*value*"/>는 자원에서 getGroupingAttributeValue (String attributeName, GroupContext context)() 메소드로 인식되는 속성 이름을 나타냅니다. 이 메소드는 Groupable 인터페이스의 일부입니다. WebSphere Commerce 관리 콘솔에서 암시적 자원 그룹의 목적에 맞게 속성은 ACATTR 테이블에도 정의되어야 하고 ACRESATREL 테이블의 자원과 연관되어야 합니다. 지정된 자원 및 조치에 적절한 정책을 찾아야 하는 시기가 오면 이 조건은 getGroupingAttributeValue(..) 메소드를 호출하여 확인됩니다. 이 경우에는 Status에서 attributeName 매개변수로 전달됩니다.

<orListCondition>은 이 블록 내의 조건이 부울 OR을 사용하여 적용되어야 함을 지정합니다. 이 경우 상태는 P 또는 E입니다. <andListConditon>은 이 블록 내의 조건이 부울 AND를 사용하여 적용되어야 함을 지정합니다. 이 경우에는 (Classname = com.ibm.commerce.order.objects.Order) AND (Status = P OR Status=E)입니다.

ACATTR 테이블의 대량 자료 반입을 위한 견본 속성 정의는 다음과 같습니다.

```
<Attribute Name="Status" Type="String">
</Attribute>
```

Name 요소는 속성을 식별하며 Type 요소는 속성의 데이터 유형을 식별합니다. 속성의 가능한 값은 다음과 같습니다.

- String
- Integer
- Double
- Currency
- Decimal
- URL
- Image
- Date

속성과 자원의 연관은 자원 정의 내에 지정됩니다. 예를 들어, Status 속성은 다음 예에서 OrderResourceCategory와 연관됩니다.

```
<ResourceCategory Name="com.ibm.commerce.order.objects.OrderResourceCategory"
ResourceBeanClass="com.ibm.commerce.order.objects.Order" >
<ResourceAttributes Name="Status"
AttributeTableName="ORDERS"
AttributeColumnName="STATUS"
ResourceKeyColumnName="ORDERS_ID"/>
</ResourceCategory>
```

여기서

<ResourceAttributes>: 속성과 자원을 연관시키는 코드 블록.

AttributeTableName: 자원의 데이터베이스 테이블 이름.

AttributeColumnName: 속성을 저장하는 자원 테이블의 열 이름.

ResourceKeyColumnName: 1차 키를 저장하는 자원 테이블의 열 이름.

관계 정의

액세스 제어 정책은 선택적 관계 요소를 갖습니다. 이 관계는 아래 표시된 관계 정의와 함께 XML 정책 파일을 로드하는 방식으로만 작성할 수 있습니다.

```
<Relation Name="value">
 </Relation>
```

Name 항목은 임의의 정책에 사용된 관계 이름이고 ACRELATION 테이블에 추가됩니다. Name은 보호 가능한 자원에서 fulfills() 메소드의 관계 매개변수와 일치합니다.

다음 예는 creator라는 관계 정의를 표시합니다.

```
<Relation Name="creator">
</Relation>
```

관계 그룹 정의

관계 그룹은 관계 그룹에 속하는 조건인 개방 조건을 포함합니다. 관계 그룹을 정의해야 하는 경우 XML 파일에 관계 그룹 정보를 정의하거나 아래와 같이 defaultAccessControlPolicies.xml 파일을 수정하여 정의해야 합니다.

```
<RelationGroup
Name="aValue"
OwnerID="aValue">
<RelationCondition><![CDATA[
<profile>
Relationship Chain Open Condition XML
</profile>
]]></RelationCondition>
</RelationGroup>
```

관계 체인

각 관계 그룹은 andListCondition 또는 orListCondition 요소별로 그룹화된 하나 이상의 RELATIONSHIP_CHAIN 개방 조건으로 구성됩니다. 관계 체인은 일련의 하나 이상의 관계입니다. 관계 체인의 길이는 구성되는 관계 수로 결정됩니다. 이것은 관계 체인의 XML 표현에서 <parmeter name= "X" value="Y"> 항목 수를 조사하여 판별할 수 있습니다. 다음은 길이가 1인 관계 체인의 예입니다.

```
<openCondition name="RELATIONSHIP_CHAIN">
<parameter name="RELATIONSHIP"
value="aValue"/>
</openCondition>
```

여기서

<parameter name="Relationshiop" value="something">: 사용자와 자원 간의 관계를 나타내는 문자열.

name: 보호 가능한 자원에서 fulfills() 메소드의 관계 매개변수.

관계 체인이 2 이상의 길이인 경우 이것은 일련의 두 관계입니다. 첫 번째 <parmeter name= "X" value="Y"> 항목은 사용자와 조직 엔티티 사이의 관계입니다. 마지막 <parmeter name= "X" value="Y"> 항목은 조직 엔티티와 자원 사이의 관계입니다. 체인의 중간 <parmeter name= "X" value="Y"> 항목은 조직 사이에 있습니다. 다음은 길이가 2인 관계 체인의 예입니다.

```
<openCondition name=RELATIONSHIP_CHAIN">
<parameter name="aValue1" value="aValue2"/>
<parameter name="RELATIONSHIP" value="aValue3"/>
</openCondition>
```

여기서

aValue1: 가능한 값은 HIERARCHY와 ROLE입니다. HIERARCHY는 멤버쉽 계층 구조에서 사용자와 조직 엔티티 간에 계층 구조 관계가 있음을 지정합니다. ROLE은 사용자가 조직 엔티티에서 역할을 수행함을 지정합니다. aValue1 값이 HIERARCHY인 경우 가능한 값은 child이며 이것은 사용자가 구성원 계층에서 직접 하위인 조직 엔티티를 리턴합니다. aValue1 값이 ROLE인 경우 가능한 값은 ROLE 테이블의 NAME 열에 있는 임의의 유효한 항목이며 이것은 현재 사용자가 이 역할을 수행하는 모든 조직 엔티티를 리턴합니다.

aValue3: 첫 번째 매개변수와 자원을 확인하여 검색된 하나 이상의 조직 엔티티 간의 관계를 나타내는 문자열. 이 값은 보호 가능한 자원에서 fulfills() 메소드의 관계 매개변수와 일치합니다. aValue1 매개변수를 확인하여 하나 이상의 조직 엔티티가 리턴된 경우 적어도 하나의 이러한 조직 엔티티가 aValue2 매개변수에 지정된 관계를 충족하는 경우 RELATIONSHIP_CHAIN의 이 부분이 충족됩니다.

주: 관계 그룹 정의에 대한 자세한 정보는 100 페이지의 『관계 그룹 정의』를 참조하십시오.

단일 체인 관계 그룹 정의

액세스 제어 정책의 일부로서 예를 들어 자원의 BuyingOrganizationalEntity인 조직 엔티티에 사용자가 속해야 하는 경우, 길이가 2인 하나의 관계 체인으로 구성된 관계 그룹을 작성해야 합니다. 다음은 이에 대한 예입니다.

```
<RelationGroup Name="MemberOf->BuyerOrganizationEntity"
OwnerID="RootOrganization
<RelationCondition><![CDATA[
<profile>
<openCondition name="RELATIONSHIP_CHAIN">
<parameter name="HIERARCHY" value="child"/>
<parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
```

```
</openCondition>
</profile>
]]><RelationCondition>
<RelationGroup>
```

관계 체인이 별개의 두 관계로 구성되므로 길이는 2입니다. 첫 번째 관계는 사용자와 해당 상위 조직 엔티티 사이에 있습니다. 사용자는 해당 관계에서 child입니다. 두 번째 관계의 경우 액세스 제어 정책 관리자는 상위 조직 엔티티가 자원과 BuyingOrganizationalEntity 관계를 충족하는지 확인합니다. 즉, 이것이 자원의 구매 조직 엔티티인 경우 true를 리턴합니다.

주: openCondition 태그에 대한 정보는 *WebSphere Commerce 액셀러레이터 사용자 정의 안내서*를 참조하십시오.

또 다른 예로는 사용자가 자원의 구매 조직 엔티티인 조직 엔티티의 회계 담당 역할을 갖도록 해야하는 경우가 있습니다. 다시 이것은 길이가 2인 단일 관계 체인으로 구성된 관계 그룹을 사용합니다. 체인의 첫 번째 부분은 사용자가 회계 담당 역할을 가진 모든 조직 엔티티를 찾습니다. 그런 후 액세스 제어 정책 관리자는 조직 엔티티 세트 중 적어도 하나가 자원과 BuyingOrganizationalEntity 관계를 충족하는지 확인합니다. 충족하는 경우 true 값이 리턴됩니다.

다음 예는 이러한 유형의 관계 그룹을 정의하는 방법을 보여줍니다.

```
<RelationGroup Name="AccountRep->BuyerOrganizationalEntity"
OwnerID="RootOrganization">
<RelationCondition><![CDATA[
<profile>
 <openCondition name="RELATIONSHIP_CHAIN">
 <parameter name="ROLE" value="Account Representative"/>
 <parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
</openCondition>
 </profile>
]]><RelationCondition>
<RelationGroup>
```

복수 체인 관계 그룹 정의

복수 체인 관계를 포함하는 관계 그룹을 작성해야 하는 경우, 사용자가 모든 관계 체인을 충족해야 하는지(AND 시나리오) 또는 사용자가 관계 체인 중 적어도 하나를 충족해야 하는지(OR 시나리오) 여부를 지정해야 합니다.

다음 예에서 사용자는 자원의 작성자이고 자원에 지정된 BuyingOrganizationalEntity에 속해야 합니다. 사용자가 자원의 작성자임을 지정하는 첫 번째 체인은 길이가 1입니다. 사용자가 자원에 지정된 BuyingOrganizationalEntity에 속해야 함을 지정하는 두 번째 체인의 길이는 3입니다.

```
<RelationshipGroup Name="Creator_And_MemberOf->BuyerOrganizationalEntity"
OwnerID="RootOrganization">
<RelationCondition><![CDATA[
<profile>
```

```
<andListCondition>
<openCondition name="RELATIONSHIP_CHAIN">
<parameter name="RELATIONSHIP" value="creator" />
</openCondition>
<openCondition name="RELATIONSHIP_CHAIN">
<parameter name="HIERARCHY" value="child"/>
<parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
</openCondition>
</andListCondition>
</profile>
]]></RelationCondition>
</RelationGroup>
```

주: 사용자가 두 관계 체인 중 하나를 충족해야 하는 경우 <andListConditon> 태그를 <orListConditon> 태그로 변경해야 합니다.

액세스 그룹

WebSphere Commerce의 일부인 기본 액세스 그룹은 언어 특정 XML 파일(예: *wc_install_directory*/xml/policies/xml/ACUserGroups_locale.xml)에 있습니다. 이 파일은 *wc_install_directory*/xml/policies/dtd/ACUserGroups_en_US.dtd에 지정된 DTD를 따릅니다.

다음은 액세스 그룹 요소의 형식입니다.

```
<UserGroup Name="value"
OwnerID="value"
Description="value"
<UserCondition>
<![CDATA[
<profile>
Condition XML
</profile>
]]>
</UserCondition>
</UserGroup>
```

여기서

Name: MBRGRP 테이블의 MBRGRPNAME 열에 저장된 액세스 그룹의 이름.

OwnerID: 이 액세스 그룹을 소유하는 Member ID. Name과 OwnerID의 조합은 고유해야 합니다. 사용할 수 있는 특수 값은 RootOrganization(-2001) 또는 DefaultOrganization(-2000)입니다.

Description(선택): 액세스 그룹을 설명하는데 사용하는 선택 속성.

UserCondition(선택): 이 액세스 그룹에 멤버쉽의 암시적 조건을 지정하는 선택 요소. 이 기준은 MBRGRPCOND 테이블의 CONDITIONS 열에 저장됩니다.

Condition XML: 조건 프레임워크를 사용하는 orListCondition, andListCondition, simpleCondition, trueConditionCondition 요소의 올바른 조합.

다음 SimpleCondition 이름은 UserCondition 요소에 대해 지원됩니다.

표 5. 지원되는 단순 조건 이름

변수 이름	설명	지원되는 연산자	지원되는 값	규정자	규정자 값
role	사용자가 MBRROLE 테이블에서 이 역할을 가져야 함을 지정합니다.	= !=	ROLE 테이블의 NAME 열 값.	org(지정하지 않는 경우 사용자는 MBRROLE 테이블에 조직의 역할을 가지고 있어야 함)	• OrgEntityID : 사용자가 역할을 가져야 하는 위치. • ?: 템플리트 정책에서 사용되는 시기.
registration status	사용자가 이 등록 상태를 가져야 함을 지정합니다.	= !=	USERS 테이블의 REGISTER-TYPE 열 값(예: 게스트의 경우 G, 등록된 경우 R)	없음	없음
status	사용자가 이 구성원 상태를 가져야 함을 지정합니다. 이것은 보통 등록 승인 상태에 사용됩니다.	= !=	MEMBER 테이블의 STATE 열 값(예: 보류 중인 등록 승인의 경우 0, 승인된 등록의 경우 1, 거부된 등록의 경우 2)	없음	없음
org	사용자가 이 상위 조직에 등록되어야 함을 지정합니다. 이것은 MBRREL 테이블에 저장됩니다.	= !=	• ORGENTITY 테이블의 ORGENTITY_ID 값. • ?- 템플리트 정책인 경우.	없음	없음

주: ?는 자원 소유 조직 엔티티로 동적 변경되고 그 후 런타임시 템플리트 정책이 적용되면 상위로 변경됩니다. ?로 정의된 액세스 그룹은 템플리트 정책에서만 작동합니다.

액세스 그룹에 대한 simpleConditions의 예

역할:

규정자 없는 역할: 다음 예는 보통 역할 기반 정책에서 사용되는 규정자 없는 역할 simpleCondition을 보여줍니다. 이 예에서 사용자는 조직 엔티티의 판매자 관리 역할을 가지고 있어야 합니다.

```
<UserConditon>
<![CDATA[
<profile>
<simpleCondition>
```

```
<variable name="role"/>
<operator name="="/>
<value data="Seller Administrator"/>
</simpleCondition>
</profile>
]]>
</UserCondition>
```

규정자가 있는 역할: 다음 예는 보통 조직 레벨 정책에서 사용되는 규정자 있는 역할 simpleCondition을 보여줍니다. 이 예에서 사용자는 조직 엔티티 100의 판매자 역할을 가지고 있어야 합니다.

```
<UserCondition>
<!CDATA[
<profile>
<simpleCondition>
<variable name="role"/>
<operator name="="/>
<value data="Seller"/>
<qualifier name="org" data="100"/>
<simpleCondition>
</profile>
]]>
</UserCondition>
```

규정자 및 매개변수가 있는 역할: 다음 예는 규정자와 매개변수가 있는 역할 simpleCondition을 보여줍니다. 이것은 템플리트 정책에서만 작동합니다. 이 예에서 사용자는 템플리트 정책에 지정된 자원을 소유하는 조직 엔티티에서 판매 관리자, 계정 관리자 또는 판매자 역할을 가지고 있어야 합니다.

```
<UserCondition><!CDATA[
<profile>
<orListCondition>
<simpleCondition>
<variable name="role"/>
<operator name="="/>
<value data="Sales Manager"/>
<qualifier name="org" data="?"/>
</simpleCondition>
<simpleCondition>
<variable name="role"/>
<operator name="="/>
<value data="Account Representative"/>
<qualifier name="org" data="?"/>
</simpleCondition>
<simpleCondition>
<variable name="role"/>
<operator name="="/>
<value data="Seller"/>
<qualifier name="org" data="?"/>
</simpleCondition>
</orListCondition>
</profile/>
]]></UserCondition>
```

registrationStatus: 다음 예는 registrationStatus simpleCondition을 보여줍니다. 이 예에서 사용자는 등록되어야 합니다(USERS.REGISTERTYPE = R).

```
<UserCondition><!CDATA[
<profile>
<simpleCondition>
<variable name="registrationStatus"/>
<operator name="="/>
<value data="R"/>
</simpleCondition>
</profile>
]]></UserCondition>
```

상태: 다음 예는 상태 simpleCondition을 보여줍니다. 이 예에서 사용자는 등록이 승인되었어야 합니다. (MEMBER.STATUS = 1)

```
<UserCondition><![CDATA[
<profile>
<simpleCondition>
<variable name="status"/>
<operator name="="/>
<value data="1"/>
</simpleCondition>
</profile>
]]></UserCondition>
```

org: 다음 예는 org simpleCondition을 보여줍니다. 이 예에서 사용자는 조직 엔티티 100에 등록되어야 합니다. MBRREL 테이블에서 사용자는 ANCESTOR_ID = 100 및 SEQUENCE = 1 값을 가지고 있어야 합니다.

```
<UserCondition><![CDATA[
<profile>
<simpleCondition>
<variable name="org"/>
<operator name="="/>
<value data="100"/>
</simpleCondition>
</profile>
]]>
</UserCondition>
```

정책

wc_install_directory/xml/policies/xml/defaultAccessControlPolicies.xml 파일은 상자 밖에서 제공하는 기본 액세스 제어 정책을 정의합니다. 이것은 *wc_install_directory* /xml/policies/dtd/accesscontrolpolicies.dtd에 지정된 DTD를 따릅니다.

다음은 정책 요소의 템플리트입니다.

```
<Policy Name="value"
OwnerId="value"
UserGroup="value"
UserGroupOwner="value"
ActionGroupName="value"
```

```
ResourceGroupName="value"
PolicyType="value"
RelationName="value"
RelationGroupName="value"
RelationGroupOwner="value"
</Policy>
```

여기서

Name: 정책의 이름. 이것은 ACPOLICY 테이블의 POLICYNAME 열로 로드됩니다. Name과 OwnerID의 조합은 고유해야 합니다.

OwnerID: 정책을 소유하는 조직 엔티티의 구성원 ID. 이것은 ACPOLICY 테이블의 member_id 열로 로드됩니다. OwnerID와 Name의 조합은 고유해야 합니다. 변환기 도구가 인식하는 두 가지 특수 값은 RootOrganization: -2001과 DefaultOrganization: -2000입니다.

UserGroup: MBRGRP 테이블의 MBRGRPNAME 열에 지정된 액세스 그룹의 이름. 이것은 ACPOLICY 테이블의 mbrgrp_id 열로 로드됩니다. 기본 액세스 그룹은 wc_install_directory/xml/policies/xml/ACUserGroups_language.xml 파일에 정의됩니다.

UserGroupOwner: 액세스 그룹을 소유하는 구성원의 구성원 ID. 이것은 액세스 그룹이 정책 소유자가 아닌 구성원에 의해 소유되는 경우 필요합니다. 이것을 지정하지 않으면 액세스 그룹이 OwnerID 속성에 지정된 구성원에 의해 소유된다고 간주합니다.

ActionGroupName: ACACTGRP 테이블의 GROUPNAME 열에 지정된 조치 그룹의 이름. ACPOLICY 테이블에 저장할 해당 조치 그룹 ID(ACACTGRP_ID)를 가져오는 데 사용합니다. 제어기 명령의 역할 기반 정책은 ActionGroupName을 ExecuteCommandActionGroup으로 설정합니다. 데이터 bean의 정책은 ActionGroupName을 DisplayDatabeanActionGroup으로 설정합니다.

ResourceGroupName: ACRESGRP 테이블의 GRPNAME 열에 지정된 자원 그룹의 이름. ACPOLICY 테이블에 저장된 해당 자원 그룹 ID(ACRESGRP_ID)를 가져오는 데 사용합니다. 보기의 역할 기반 정책은 ResoureGroupName을 ViewCommandResourceGroup으로 설정합니다.

PolicyType: 정책 유형. 유효한 값은 template입니다(POLICYTYPE은 ACPOLICY 테이블에서 1로 설정됨). 이 속성을 지정하지 않으면 정책 유형 값이 변경되지 않습니다. (기본적으로 이 열 값은 널(Null)값입니다. 1 이외의 다른 값은 템플리트가 아닌 정책 유형을 의미합니다.)

RelationName(선택): ACRELATION 테이블의 RELATIONNAME 열에 지정된 관계의 이름. 지정된 경우 ACPOLICY 테이블에 저장된 해당 자원 ID(ACRELATION_ID)를 가져오는데 사용합니다.

RelationGroupName(선택): ACRELGRP 테이블의 GRPNAME 열에 지정된 관계 그룹의 이름. 이 속성이 지정된 경우 관계 그룹이 우선순위를 가지므로 RelationName을 지정해서는 안됩니다.

RelationGroupOwner: 관계 그룹을 소유하는 구성원 ID. 이 속성은 RelationGroupName 속성이 지정되고 OwnerID 속성값이 RootOrganization이 아닌 경우에만 필요합니다. 이 경우 RelationGroupOwner는 RootOrganization(-2001)로 지정되어야 합니다.

정책 예

역할 기반 정책:

제어기 명령: 이 예에서 AllUsers 액세스 그룹에 속한 사용자는 AllUserCmdResourceGroup 자원 그룹의 일부인 제어기 명령을 실행할 수 있습니다.

```
<Policy Name="AllUsersExceuteAllUserCmdResourceGroup"
OwnerID="RootOrganization"
UserGroup="AllUsers"
ActionGroupName="ExecuteCommandActionGroup"
ResourceGroupName="AllUserCmdResourceGroup">
</Policy>
```

보기: 이 예에서 MarketingManagers 액세스 그룹에 속한 사용자는 MarketingManagersViews 조치 그룹에 속한 보기를 실행할 수 있습니다.

```
<Policy Name="MarketingManagersExecuteMarketingManagersViews"
OwnerID="RootOrganization"
UserGroup="MarketingManagers"
ActionGroupName="MarketingManagersViews"
ResourceGroupName="ViewCommandResourceGroup">
</Policy>
```

자원 레벨 정책:

명령: 이 예에서 사용자가 자원에 대해 creator 관계를 충족하는 한 RegisteredApprovedUsers 액세스 그룹에 속한 사용자는 CouponWalletResourceGroup에 지정된 자원에서 CouponRedemption 조치 그룹에 지정된 조치를 수행할 수 있습니다.

```
<Policy Name="RegisteredApprovedUsersExecuteCouponRedemptionCommandsOn
WalletResource"
OwnerID="RootOrganization"
UserGroup="RegisteredApprovedUsers"
ActionGroupName="CouponRedemption"
ResourceGroupName="CouponWalletResourceGroup"
RelationName="creator">
</Policy>
```

데이터 Bean: 이 예에서 사용자가 자원에 대해 owner 관계를 충족하는 한 AllUsers 액세스 그룹에 속한 사용자는 UserDatabeanResourceGroup 자원 그룹에 지정된 데이터 bean을 표시할 수 있습니다.

```
<Policy Name="AllUsersDisplayUserDatabeanResourceGroup"
OwnerID="RootOrganization"
UserGroup="AllUsers"
ActionGroupName="DisplayDatabeanActionGroup"
ResourceGroupName="UserDatabeanResourceGroup"
RelationName="owner">
</Policy>
```

템플리트 정책: 이 예에서 MembershipAdministratorsForOrg 액세스 그룹에 속한 사용자는 OrganizationDataResourceGroup에 지정된 자원에서 ApproveGroupUpdate 액세스 그룹에 지정된 조치를 수행할 수 있습니다.

```
<Policy Name=MembershipAdministratorsForOrgExecuteApproveGroupUpdateCommands
OnOrganizationResource"
OwnerID="RootOrganization"
UserGroup="MembershipAdministratorsForOrg"
ActionGroupName="ApproveGroupUpdate"
ResourceGroupName="OrganizationDataResourceGroup"
PolicyType="template">
</Policy>
```

이 템플리트 정책이 적용되면 정책 소유자는 RootOrganization에서 자원을 소유하는 조직 엔티티로, 그 이후에는 루트 조직을 포함하는 해당 상위 조직 엔티티로 동적 변경합니다. MembershipAdministratorsForOrg 액세스 그룹의 정의를 조사하여 멤버쉽에 대한 다음 조건을 표시합니다.

```
<UserCondition><![CDATA[
<profile>
<orListCondition>
<simple condition>
<variable name="role"/>
<operator name="="/>
<value data="Buyer Administrator"/>
<qualifier name="org" data="?"/>
</simpleCondition>
<simpleConditon>
<variable name="role"/>
<operator name="="/>
<value data="Seller Administrator"/>
<qualifier name="org" data="?"/>
</simpleConditon>
</orListCondtion>
</profile>
]]></UserCondition>
```

주: role의 simpleCondition은 org = **?**로 규정됩니다. 이 **?**는 위에서 설명한 대로 정책 소유자와 함께 동적으로 대체됩니다. 이 동적 동작은 템플리트 정책에서만 가

능합니다. 따라서 이 예에서 자원을 소유하는 조직 엔티티의 Buyer Administrator 또는 Seller Administrator 역할을 가진 사용자는 이 액세스 그룹에 있는 멤버쉽의 조건을 충족합니다.

번역 가능한 정책 데이터

다음은 최소한 defaultAccessControlPolicies_*locale*.xml 파일에 정의되어 있어야 하는 번역 가능한 액세스 제어 요소의 템플리트입니다.

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!--The following TRANSLATABLE access control elements should
 be defined in this file:
<Attribute_nls>
<Action_nls>
<Relation_nls>
<ResourceCategory_nls>
<ActionGroup_nls>
<ResourceGroup_nls>
<Policy_nls>-->
<!DOCTYPE PoliciesNLS SYSTEM "../dtd/accesscontrolpoliciesnls.dtd">

<PoliciesNLS LanguageID="value">


 <!--Insert access control element definitions here -->
 </PoliciesNLS>
```

LanguageID 속성은 로케일 특정 데이터 언어에 해당하는 문자열입니다. LanguageID의 유효한 값은 다음과 같습니다.

- en_US
- fr_FR
- de_DE
- it_IT
- es_ES
- pt_BR
- zh_CN
- zh_TW
- ko_KR
- ja_JP

번역 불가능한 정책 데이터

다음은 번역 불가능한 데이터를 포함하는 사용자 정의된 정책 파일의 템플리트입니다.

```
  <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>

<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">
```

```
<!--The following NON-TRANSLATABLE access control elements
 should be defined in this file:

<Attribute>
<Action>
<ResourceCategory>
<Relation>
<RelationGroup>
<ActionGroup>
<ResourceGroup>
<Policy-->
<Policies>

 <!--Insert access control element definitions here-->
 </Policies>
```

로케일 특정 데이터

다음의 선택적인 로케일 특정 데이터를 로드하여 번역 불가능한 XML 파일에 이미 정의된 액세스 제어 요소에 추가 설명을 지정할 수 있습니다. 기본 로케일 특정 데이터는 다음 주소에서 찾을 수 있습니다.

wc_install_directory\xml\policies\xml\
defaultAccessControlPolicies_*locale*.xml

예: defaultAccessControlPolicies_en_US.xml.

속성: 다음 예는 추가 속성 요소 정보를 정의합니다.

```
<Atrribute_nls AttributeName="Status"
DisplayName_nls="Status attribute"
Description_nls="Resource status attribute"
/>
```

여기서

AttributeName: 속성의 이름. 이 값은 ACATTR 테이블의 ATTRNAME 열에 저장됩니다.

DisplayName_nls: 속성의 표시 이름. 이 값은 ACATTRDESC 테이블의 DISPLAYNAME 열에 저장됩니다.

Description_nls: 속성의 선택적인 설명. 이 값은 ACATTRDESC 테이블의 DESCRIPTION 열에 저장됩니다.

조치: 다음 예는 추가 조치 요소 정보를 정의합니다.

```
<Action_nls ActionName="OrderAdjustmentButton"
DisplayName_nls="Order Adjustment Button View"
Description_nls="The view for loading buttons in the order adjustment page
 when placing an order from Commerce Acclerator"
/>
```

여기서

ActionName: 조치의 이름. 이 값은 ACACTION 테이블의 ACTION 열에 저장됩니다.

DisplayName_nls: 조치의 표시 이름. 이 값은 ACACTDESC 테이블의 DISPLAYNAME 열에 저장됩니다.

Description_nls: 조치의 선택적인 설명. 이 값은 ACACTDESC 테이블의 DESCRIPTION 열에 저장됩니다.

관계: 다음 예는 추가 관계 요소 정보를 정의합니다.

```
<Relation_nls RelationName="creator"
DisplayName_nls="creator"
Description_nls="creator"
/>
```

여기서

RelationName: 관계의 이름. 이 값은 ACRELATION 테이블의 RELATIONNAME 열에 저장됩니다.

DisplayName_nls: 관계의 표시 이름. 이 값은 ACRELDESC 테이블의 DISPLAYNAME 열에 저장됩니다.

Description_nls: 관계의 선택적인 설명. 이 값은 ACRELDESC 테이블의 DESCRIPTION 열에 저장됩니다.

자원 카테고리: 다음 예는 추가 자원 카테고리 정보를 정의합니다.

```
<ResourceCategory_nls ResourceCategoryName="com.ibm.commerce.
catalog.objects."InterestItemList"
DisplayName_nls="Interest Item List"
Description_nls="Interest Item List command"
/>
```

여기서

ResourceCategoryName: 자원 카테고리의 이름. 이 값은 ACRESCGRY 테이블의 RESCLASSNAME 열에 저장됩니다.

DisplayName_nls: 자원 카테고리의 표시 이름. 이 값은 ACRSCGDES 테이블의 DISPLAYNAME 열에 저장됩니다.

Description_nls: 자원 카테고리의 선택적인 설명. 이 값은 ACRSCGDES 테이블의 DESCRIPTION 열에 저장됩니다.

조치 그룹: 다음 예는 추가 조치 그룹 정보를 정의합니다.

```
<ActionGroup_nls ActionGroupName="DoEverything"
DisplayName_nls="Do Everything"
Description_nls="Permits access to all Actions"
/>
```

여기서

ActionGroupName: 조치 그룹의 이름. 이 값은 ACACTGRP 테이블의 GROUPNAME 열에 저장됩니다.

DisplayName_nls: 조치 그룹의 표시 이름. 이 값은 ACACGPDESC 테이블의 DISPLAYNAME 열에 저장됩니다.

Description_nls: 조치 그룹의 선택적인 설명. 이 값은 ACACGPDESC 테이블의 DESCRIPTION 열에 저장됩니다.

자원 그룹: 다음 예는 추가 자원 그룹 정보를 정의합니다.

```
<ResourceGroup_nls ResourceGroupName="AllResourceGroup"
DisplayName_nls="All Resources Group"
Description_nls="All Resources"
/>
```

여기서

ResourceGroupName: 자원 그룹의 이름. 이 값은 ACRESGRP 테이블의 GRPNAME 열을 저장합니다.

DisplayName_nls: 자원 그룹의 표시 이름. 이 값은 ACRESGPDES 테이블의 DISPLAYNAME 열에 저장됩니다.

Description_nls: 자원 그룹의 선택적인 설명. 이 값은 ACRESGPDES 테이블의 DESCRIPTION 열에 저장됩니다.

정책: 다음 예는 추가 정책 정보를 정의합니다.

```
<Policy_nls PolicyName="SiteAdministratorsCanDoEverything"
OnwerID="RootOrganization"
DisplayName_nls="Site Administrators Can Do Everything"
Description_nls="Policy that allows Site Administrators to do everything"
/>
```

여기서

PolicyName: 액세스 제어 정책의 이름. 이 값은 ACPOLICY 테이블의 POLICYNAME 열에 저장됩니다.

OwnerID: 이 정책을 소유하는 조직 엔티티의 구성원 ID.

DisplayName_nls: 정책의 표시 이름. 이 값은 ACPOLDESC 테이블의 DISPLAYNAME 열에 저장됩니다.

Description_nls: 정책의 선택적인 설명. 이 값은 ACPOLDESC 테이블의 DESCRIPTION 열에 저장됩니다.

XML 파일을 변경한 후

변경사항 테스트

변경사항 테스트에 대해서는 49 페이지의 『정책 변경 후』를 참조하십시오.

변경사항을 데이터베이스에 로드

XML 파일에 대해 직접 작업하여 정책을 변경한 경우, 변경된 XML 파일을 다시 데이터베이스에 로드해야 합니다. XML 파일과 데이터베이스 내의 액세스 제어 정보간의 일관성을 유지하는 것은 다음의 몇 가지 이유로 중요합니다.

- WebSphere Commerce의 인스턴스를 작성할 때, 정책 및 액세스 그룹 정의가 XML 파일에서 로드됩니다.
- WebSphere Commerce의 두 번째 인스턴스에서 액세스 제어 정책을 구현하려면, 두 번째 인스턴스를 작성하기 전에 적절한 디렉토리에 XML 파일을 복사함으로써 할 수 있습니다.
- XML 파일은 정책 및 구성 요소 부분을 직접 보거나 편집하는 편리한 방법을 제공하므로 파일을 최근으로 유지하는 것은 필수입니다.

XML 변경사항을 데이터베이스에 로드

로드 처리는 액세스 제어 정책 정보와 액세스 그룹 정의를 포함하는 XML 파일을 읽고 이를 적절한 데이터베이스로 로드합니다. XML 파일에 포함된 정책 및 액세스 그룹 정보는 설치 시 로드되지만, 변경한 경우에는 그 파일을 다시 로드해야 합니다.

주: 사용자 정의된 XML 파일을 작성할 경우, 이 파일을 *<c_install_directory>*/xml/policies/xml 디렉토리에 복사하여 데이터베이스에 로드해야 합니다.

400 의 경우, 사용자 정의된 XML 파일을 작성하려면 파일에서 DTD에 대한 전체 경로를 사용해야 합니다. 액세스 제어 정책 DTD는 /QIBM/ProdData/WebCommerce/xml/policies/dtd에 위치됩니다.

액세스 그룹과 액세스 제어 정책을 로드하려면, 다음 명령을 실행하십시오.

NT 2000

1. *<wc_install_directory>*\bin 디렉토리에서 여기에 나열된 순서대로 필요에 따라 다음 명령 파일을 실행하십시오.

- 사용자(액세스) 그룹 정의를 로드하려면, **acugload** 명령 파일을 실행하십시오. **구문**: acugload.cmd <*database name*> <*database user*> <*database user password*> <*UserGroups xml file*> **(예**: acugload mall dbuser dbusrpwd ACUserGroups_en_US.xml)
- 기본 액세스 제어 정책 파일을 로드하려면, **acpload** 명령 파일을 실행하십시오. **구문:** acpload.cmd <*database name*> <*database user*> <*database user password*> <*Policies xml file*> **(예**: acpload mall dbuser dbusrpwd defaultAccessControlPolicies.xml)
- 표시 이름 및 설명 파일을 로드하려면, **acpnlsload** 명령 파일을 실행하십시오. **구문:** acpnlsload.cmd <*database name*> <*database user*> <*database user password*> <*NLS Policies xml file*> **(예**: acpnlsload mall dbuser dbusrpwd defaultaccesscontrolpolicies_en_US.xml)

2. 오류를 보려면 <*wc_install_directory*>\logs에서 **acugload.log**, **acpload.log** 및 **acpnlsload.log** 로그 파일을 확인하십시오.

AIX Solaris Linux

데이터베이스 사용자 ID는 <*wc_install_directory*>/xml/policies, <*wc_install_directory*>/bin 및 <*wc_install_directory*>/properties/utilities 디렉토리와 그 서브디렉토리 및 파일에 대해 읽기/쓰기/실행 권한이 있어야 합니다.

1. 데이터베이스 사용자 ID로 로그인하십시오.
2. <*wc_install_directory*>/bin 디렉토리에서 여기에 나열된 순서대로 필요에 따라 다음 쉘 스크립트를 실행하십시오.

1. 사용자(액세스) 그룹 정의를 로드하려면, **acugload** 쉘 스크립트를 실행하십시오. **구문:** acugload.sh <*database name*> <*database user*> <*database* user *password*> <*UserGroups xml filename*> (**예**: acugload mall dbuser dbusrpwd ACUserGroups_en_US.xml)
2. 기본 액세스 제어 정책 파일을 로드하려면, **acpload** 쉘 스크립트를 실행하십시오. **구문:** acpload.sh <*database name*> <*database user*> <*database user password*> <*Policies xml filename*> (**예**: acpload mall dbuser dbusrpwd defaultAccessControlPolicies.xml)
3. 표시 이름 및 설명 파일을 로드하려면 acpnlsload 쉘 스크립트를 실행하십시오. **구문:** acpnlsload.sh <*database name*> <*database user*> <*database user password*> <*NLS Policies xml filename*> (**예**: acpnlsload mall dbuser dbusrpwd defaultaccesscontrolpolicies_en_US.xml)

오류를 보려면 <*wc_install_directory*>/logs에서 acugload.log, acpload.log 및 acpnlsload.log 로그 파일을 확인하십시오.

주: 이러한 스크립트를 실행하는 동안 발생할 수 있는 오류가 명령행에 표시되지 않으므로 이러한 스크립트를 수행한 후 로그 파일을 확인해야 합니다.

400

명령행에서 지정된 순서대로 필요에 따라 다음 명령을 실행하십시오.

- 사용자(액세스) 그룹 정의를 로드하려면 LODWCSUG 명령을 실행하십시오.
  구문: LODWCSUG DATABASE(<*데이터베이스 이름*>) SCHEMA (<*schema_name*>) PASSWD(<*instance_password*>) INSTROOT(<*instance_root*>) INFILE(<*XML 파일의 전체 경로*>)
- 기본 액세스 제어 정책 파일을 로드하려면 LODWCSAC 명령을 실행하십시오.
  구문: LODWCSAC DATABASE(<데이터베이스 이름>) SCHEMA (<schema_name>) PASSWD(<instance_password>) INSTROOT(<instance_root>) INFILE(<*XML 파일의 전체 경로*>)
- 표시 이름 및 설명 파일을 로드하려면, LODWCSACD 명령을 실행하십시오.
  구문: LODWCSACD DATABASE(<*데이터베이스 이름*>) SCHEMA (<*schema_name*>) PASSWD(<*instance_password*>) INSTROOT(<*instance_root*>) INFILE(<*XML 파일에 대한 전체 경로*>)

데이터베이스에서 XML 파일로 정책 및 액세스 그룹 정의 추출

추출 처리는 액세스 제어 데이터베이스에서 정책 및 액세스 그룹 정보를 읽고 XML 형식으로 정보를 캡처하는 파일을 생성합니다.

NT 2000

1. <*wc_install_directory*>\bin 디렉토리에서 다음 acpextract 명령을 실행하십시오.

   ```
   acpextract.cmd <database name> <database user> <database user password>
   ACPoliciesfilter.xml
   ```

   예:

   ```
   acpextract.cmd mall dbuser dbusrpwd ACPoliciesfilter.xml
   ```

   다음 파일이 작성됩니다.

   - ExtractedACPolicies.xml: 이 파일은 지정된 필터 기준에 대해 Extract 명령으로 추출된 데이터 포함
   - ExtractedACPolicies.dtd: ExtractedACPolicies.xml 파일의 DTD
   - AccessControlUserGroups.xml: 액세스 그룹 정의를 포함하는 파일
   - AccessControlPolicies.xml: 언어 독립적인 액세스 제어 정책 정보를 포함하는 파일

- AccessControlPolicies_LOCALE.xml: 표시 이름과 설명을 포함하는 언어 종속적인 액세스 제어 정책 파일

2. 발생했을 수 있는 처리 오류를 보려면 *<wc_install_directory>*\logs\acpextract.log 로그 파일을 확인하십시오.

AIX Solaris Linux

1. 데이터베이스 사용자 ID로 로그인하십시오.
2. *<wc_install_directory>*\bin 디렉토리에서 다음 acpextract 쉘 스크립트를 실행하십시오.

```
acpextract.sh <database name> <database user>
<database user password> ACPoliciesfilter.xml
```

예:

```
acpextract.sh mall dbuser dbusrpwd ACPoliciesfilter.xml
```

다음 파일이 작성됩니다.

- ExtractedACPolicies.xml: 이 파일은 지정된 필터 기준에 대해 Extract 명령으로 추출된 데이터를 포함합니다.
- ExtractedACPolicies.dtd: ExtractedACPolicies.xml 파일의 DTD.
- AccessControlUserGroups.xml: 액세스 그룹 정의를 포함하는 파일.
- AccessControlPolicies.xml: 언어 독립적인 액세스 제어 정책 정보를 포함하는 파일.
- AccessControlPolicies_LOCALE.xml: 표시 이름과 설명을 포함하는 언어 종속적인 액세스 제어 정책 파일.

3. 발생했을 수 있는 처리 오류를 보려면 *<wc_install_directory>*\logs\acpextract.log 로그 파일을 확인하십시오.

400

1. 명령행에서 다음 EXTWCSAC 명령을 실행하십시오.

```
EXTWCSAC DATABASE (<database name>)
 SCHEMA (<schema_name>) PASSWD (<database user>)
INSTROOT (<instance_root>) FILTER (<input filter XML file>) OUTDIR
 (<output directory
 for new files>)
```

다음 파일은 OUTDIR 매개변수를 사용하여 지정한 디렉토리에서 작성되었습니다.

- ExtractedACPolicies.xml: 이 파일은 지정된 필터 기준에 대해 Extract 명령으로 추출된 데이터 포함
- ExtractedACPolicies.dtd: ExtractedACPolicies.xml 파일의 DTD.
- AccessControlUserGroups.xml: 액세스 그룹 정의를 포함하는 파일

- AccessControlPolicies.xml: 언어 독립적인 액세스 제어 정책 정보를 포함하는 파일
- AccessControlPolicies_LOCALE.xml: 표시 이름과 설명을 포함하는 언어 종속적인 액세스 제어 정책 파일

부록. 기본 액세스 제어 정책

부록에는 WebSphere Commerce와 함께 제공되는 기본 정책이 나열되어 있습니다. 그 정책들은 다음 기준으로 구성되어 있습니다.

- **역할 기반 정책:** 각 기본 역할에 대한 역할 기반 정책. 이 정책은 각 명령을 실행할 수 있는 사람을 정의하므로, 명령 레벨 정책이라고도 합니다.
- **자원 레벨 정책:** 비즈니스 영역별로 그룹화된 자원 레벨 정책. 이 정책들은 사용자 그룹이 특정 자원에 대해 수행할 수 있는 조치를 정의합니다. 각 비즈니스 영역에서 정책은 규정하는 자원 유형별로 구성됩니다.
  - **데이터 자원** - 주문이나 입찰과 같이 조작될 수 있는 비즈니스 오브젝트.
  - **데이터 bean 자원** - 비즈니스 오브젝트에 대한 정보를 포함합니다. 데이터 bean은 웹 페이지에 오브젝트 정보를 표시하기 위해 사용됩니다.

표 6.

정책	**시작 페이지**
역할 기반 정책	120 페이지의 『역할 기반 정책』
비즈니스 영역별 자원 레벨 정책:	121 페이지의 『비즈니스 영역별 자원 레벨 정책』
주문	121 페이지의 『주문』
거래(장기 구매 계약)	122 페이지의 『거래(장기 구매 계약)』
승인	123 페이지의 『승인』
경매	123 페이지의 『Auctions』
비즈니스 인텔리전스	123 페이지의 『비즈니스 인텔리전스』
멤버쉽	124 페이지의 『멤버쉽』
구매자 관리 콘솔	124 페이지의 『구매자 관리 콘솔』
캠페인	125 페이지의 『캠페인』
카탈로그	125 페이지의 『카탈로그』
연결 및 알림	125 페이지의 『연결 및 알림』
조달	126 페이지의 『조달』
쿠폰	126 페이지의 『쿠폰』
고객 프로파일링	126 페이지의 『고객 프로파일링』
할인	127 페이지의 『할인』
재고	127 페이지의 『재고 관리』
계획된 재고	127 페이지의 『계획된 재고』
재고 관리	128 페이지의 『재고 관리』
주문 관리	128 페이지의 『주문 관리』
지불	129 페이지의 『지불』
정책, 액세스 그룹, 자원 그룹 및 조치 그룹을 편집하기 위한 관리 콘솔 페이지	129 페이지의 『정책, 액세스 그룹, 자원 그룹 및 조치 그룹을 편집하기 위한 관리 콘솔 페이지』
상품 어드바이저	129 페이지의 『상품 어드바이저』

표 6. *(계속)*

RFQ	130 페이지의 『RFQ』
규칙	130 페이지의 『규칙』
스케줄러	130 페이지의 『스케줄러』

역할 기반 정책

표 7.

AccountRepresentativesExecuteAccountRepresentativesCmdResourceGroup
AccountRepresentativesExecuteAccountRepresentativesViews
AllUsersExecuteAllUserCmdResourceGroup
AllUsersExecuteAllUsersViews
BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup
BuyerAdministratorsExecuteBuyerAdminstratorsViews
BuyerAdministratorsExecuteBuyerAdminstratorsCommands
BuyerApproversExecuteBuyerApproversCmdResourceGroup
BuyerApproversExecuteBuyerApproversViews
Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup
Buyers(buy-side)ExecuteBuyers(buy-side)Views
Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup
Buyers(sell-side)ExecuteBuyers(sell-side)Views
CategoryManagersExecuteCategoryManagersCmdResourceGroup
CategoryManagersExecuteCategoryManagersView
CustomerServiceRepresentativesExecuteCustomerServiceRepCmdResourceGroup
CustomerServiceRepresentativesExecuteCustomerServiceRepresentativeView
CustomerServiceSupervisorsExecuteCustomerServiceSupervisorCmdResourceGroup
CustomerServiceSupervisorsExecuteCustomerServiceSupervisorViews
CustomersExecuteCustomersViews
GuestsExecuteGuestUsersCmdResourceGroup
LogisticsManagersExecuteLogisticsManagersCmdResourceGroup
LogisticsManagersExecuteLogisticsManagersViews
MarketingManagersExecuteMarketingManagerCmdResourceGroup
MarketingManagersExecuteMarketingManagersViews
OperationsManagersExecuteOperationsManagersCmdResourceGroup
OperationsManagersExecuteOperationsManagersView
PickPackersExecutePickPackersCmdResourceGroup
PickPackersExecutePickPackersViews
ProcurementBuyersExecuteProcurementBuyersCmdResourceGroup
ProductManagersExecuteProductManagersCmdResourceGroup
ProductManagersExecuteProductManagersViews
ReceiversExecuteReceiversCmdResourceGroup

표 7. (계속)

ReceiversExecuteReceiversViews
ReturnsAdministratorsExecuteReturnsAdministratorsCmdResourceGroup
ReturnsAdministratorsExecuteReturnsAdministratorsViews
SalesManagersExecuteSalesManagersCmdResourceGroup
SalesManagersExecuteSalesManagersViews
SellerAdministratorsExecuteSellerAdministratorsCommands
SellerAdministratorsExecuteSellerAdministratorsViews
SellersExecuteSellersCmdResourceGroup
SellersExecuteSellersView
SiteAdministratorsCanDoEverything
StoreAdministratorsExecuteStoreAdministratorsCmdResourceGroup
StoreAdministratorsExecuteStoreAdministratorViews

비즈니스 영역별 자원 레벨 정책

주문

표 8.

Data Resources	
Order	AllUsersExecuteOrderCreateCommandsOnStoreResource
	AllUsersExecuteOrderPrepareCommandsOnOrderResource
	AllUsersExecuteOrderProcessOnOrderResource
	AllUsersExecuteOrderReadCommandsOnOrderResource
	AllUsersExecuteOrderWriteCommandsOnOrderResource
	AllUsersExecuteReturnAgainstOrderOnOrderResource
	AllUsersExecuteScheduledOrderCancelOnOrderResource
	OrderManagersForOrgExecuteOrderManageCommandsOnOrderResource
Requisition List	AllUsersExecuteRequisitionListCreateCommandsOnStoreEntityResource
	AllUsersExecuteRequisitionListExclusiveProcessCommands OnPrivateRequisitionListResource
	AllUsersExecuteRequisitionListExclusiveReadCommandsOn PrivateRequisitionListResource
	AllUsersExecuteRequisitionListSharedProcessCommandsOn SharedRequisitionListResource
	AllUsersExecuteRequisitionListSharedReadCommandsOn SharedRequisitionListResource
	AllUsersExecuteRequisitionListWriteCommandsOn RequisitionListResource
Interest Item	AllUsersExecuteInterestItemReadCommandsOnInterestItemListResource

표 8. (계속)

	AllUsersExecuteInterestItemWriteCommandsOnInterestItemListResource
RMA	AllUsersExecuteRMACreateCommandsOnStoreResource
	AllUsersExecuteRMAProcessCommandsOnRMAResource
	AllUsersExecuteRMAReadCommandsOnRMAResource
	AllUsersExecuteRMAWriteCommandsOnRMAResource
	RMAApproversForOrgExecuteRMAApproveCommandsOnRMAResource
	RMADisposersForOrgExecuteRMADisposeCommandsOnRMAResource
	RMAManagersForOrgExecuteRMAManageCommandsOnRMAResource
	RMAReceiversForOrgExecuteRMAReceiveCommandsOnRMAResource
	StoreAdministratorsForOrgExecuteRMACreditCommandsOnStoreEntityResource
DataBeans	
Order	AllUsersDisplayApprovalsOrderDataBeansResourceGroup
	AllUsersDisplayOrderDatabeanResourceGroup
Requisition List	AllUsersDisplaySharedRequisitionListDataBeansIfSame OrganizationalEntityAsCreator
Interest Item	AllUsersDisplayInterestItemDatabeanResourceGroup
RMA	AllUsersDisplayRMADatabeanResourceGroup

거래(장기 구매 계약)

표 9.

Data Resource	
Contract	ContractAdministratorsForOrgExecuteContractCreateCommandsOn MemberResource
	ContractAdministratorsForOrgExecuteContractManageCommandsOn ContractResource
	ContractOperatorsForOrgExecuteContractDeployCommandsOn ContractResource
	ContractOperatorsForOrgExecuteContractSubmitCommandsOn ContractResource
	ContractViewersExecuteContractDisplayCommandsOnContractResource
Business Policy	BusinessPolicyAdministratorsForOrgExecuteBusinessPolicy CreateCommandsOnStoreResoure
	BusinessPolicyAdministratorsForOrgExecuteBusinessPolicy ManageCommandsOnBusinessPolicyResourcee
DataBeans	AccountHandlersDisplayTradingDatabeanResourceGroup

승인

표 10.

Data Resources	
	AllUsersExecuteAllUsersActionGroupCommandsOnOrderResource
	AllUsersExecuteApproveCommandsOnApprovalResource
	AllUsersExecuteCancelApproveCommandsOnApprovalResource

Auctions

표 11.

Data Resources	
Auction	AuctionAdministratorsForOrgExecuteAdminRetractBidCommands OnAuctionResource
	AuctionAdministratorsForOrgExecuteAuctionCreateCommands OnStoreEntityResource
	AuctionAdministratorsForOrgExecuteAuctionManageCommands OnAuctionResource
Auction Style	AuctionAdministratorsForOrgExecuteAuctionStyleCreateCommands OnStoreEntityResource
	AuctionAdministratorsForOrgExecuteAuctionStyleManageCommands OnAuctionStyleResource
Bid Control Rule	AuctionAdministratorsForOrgExecuteBidControlRuleCreateCommands OnStoreEntityResource
	AuctionAdministratorsForOrgExecuteBidControlRuleManageCommands OnBidControlRuleResource
Bid	RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource
	RegisteredApprovedUsersExecuteBidManageCommands OnBidResourcesTheyOwn
AutoBid	RegisteredApprovedUsersExecuteAutoBidCreateCommands OnAuctionResource
	RegisteredApprovedUsersExecuteAutoBidManageCommands OnAutoBidResourcesTheyOwn
DataBeans	AuctionDatabeanOwnersDisplayAuctionDatabeans

비즈니스 인텔리전스

표 12.

데이터 자원	
	BusinessAnalystsForOrgExecuteViewContext ListCommandsOnStoreEntityResource
	IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReport CommandsOnStoreEntityResource

멤버쉽

표 13.

데이터 자원	
User	GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource
	MembershipAdministratorsForOrgExecuteUserAdminRegistration CommandsOnOrganizationResource
	MembershipAdministratorsForOrg ExecuteUserAdminUpdateCommandsOnUserResource
	NonRejectedUsersExecuteUserSelfRegistration ContinuationCommandsOnUserResource
Organization	MembershipAdministratorsForOrgExecute OrgEntityRegistrationCommandsOnOrganizationResource
	MembershipAdministratorsForOrgExecuteOrg EntityUpdateCommandsOnOrganizationResource
Address	MembershipAdministratorsForOrg ExecuteAddressManageCommandsOnMemberResource
	NonRejectedUsersExecuteAddressManageCommandsOn UserResource
Role	MembershipAdministratorsForOrgExecute RoleManageCommandsOnUserResource
	OrganizationRoleAdministratorsExecute RoleManageCommandsOnOrganizationResource
Member Group	MemberGroupAdministratorsForOrgExecute MemberGroupCreateCommandsOnMemberResource
	MemberGroupManagersForOrgExecute MemberGroupManageCommandsOnMemberGroupResource
DataBeans	MembershipAdministratorsForOrgDisplay OrganizationDatabeanResourceGroup
	MembershipViewersForOrgDisplayMembershipDatabeanResourceGroup

구매자 관리 콘솔

표 14.

데이터 자원	
Approval Group	MembershipAdministratorsForOrgExecute ApproveGroupUpdateCommandsOnOrganizationResource
Member Group	MembershipAdministratorsForOrgExecute MemberGroupMemberUpdateCommandsOnMemberGroupResource
	MembershipAdministratorsForOrgExecute MemberGroupMemberUpdateCommandsOnUserResource

캠페인

표 15.

데이터 자원	
	CampaignManagersForOrgExecute CampaignRelatedCreateCommandsOnStoreEntityResource
	CampaignManagersForOrgExecute CampaignUpdateCommandsOnCampaignResource
	CampaignManagersForOrgExecute CollateralUpdateCommandsOnCollateralResource
	CampaignManagersForOrgExecute EMarketingSpotUpdateCommandsOnEMarketingSpotResource
	CampaignManagersForOrgExecute InitiativeUpdateCommandsOnInitiativeResource
DataBeans	CampaignManagersForOrgDisplayCampaignDatabeanResourceGroup

카탈로그

표 16.

데이터 자원	
	CatalogEntryManagersForOrgExecute CatalogEntryManageCommandsOnCatalogEntryResource
	CatalogEntryManagersForOrgExecute CatalogEntryRelationManageCommandsOnCatalogResource
	CatalogEntryManagersForOrgExecute StoreCatalogEntryManageCommandsOnStoreEntityResource
	CatalogGroupManagersForOrgExecute CatalogGroupManageCommandsOnCatalogGroupResource
	CatalogGroupManagersForOrgExecute ProductSetAddCommandsOnCatalogResource
	CatalogGroupManagersForOrgExecute ProductSetManageCommandsOnProductSetResource
	CatalogManagersForOrgExecute CatalogManageCommandsOnCatalogResource
	CatalogManagersForOrgExecute StoreCategoryManageCommandsOnCatalogResource
DataBeans	CatalogGroupManagersForOrgDisplay CatalogGroupDataBeansResourceGroup
	ProductAdministratorsForOrgDisplayProductDataBeansResourceGroup

연결 및 알림

표 17.

데이터 자원	

표 17. (계속)

	BackendOrderAdministratorsForOrgExecute BackendOrderStatusCreateCommandsOnOrderDataResource
	BackendPickPackersForOrgExecute BackendPickPackListCommandsOnFulfillmentCenterDataResource
	StoreAdministratorsForOrgExecute MessagingAdminCommandsOnStoreEntityResource
DataBeans	StoreAdministratorsForOrgDisplayMessagingDataBeans

조달

표 18.

데이터 자원	
	ProcurementAdministratorsForOrgExecute ProcurementAuthenticationAndRegistrationOnOrderDataResource
	ProcurementShoppingCartManagersExecute ProcurementShoppingCartManageOnOrderResource

쿠폰

표 19.

데이터 자원	
	CouponAdministratorsForOrgExecute CouponPromotionCreateCommandsOnStoreEntityResource
	CouponAdministratorsForOrgExecuteCouponPromotionDeleteCommands OnCouponPromotionResource
	RegisteredApprovedUsersExecute CouponDeleteCommandsOnCouponWalletResource
	RegisteredApprovedUsersExecute CouponRedemptionCommandsOnCouponWalletResource
	StoreAdministratorsForOrgExecute ScheduledCouponCmdsOnStoreResource
DataBeans	CouponAdministratorsForOrgDisplayECouponPromotionListBeans

고객 프로파일링

표 20.

데이터 자원	
	CustomerProfileEditorsForOrgExecute SegmentManageCommandsOnStoreEntityResource
DataBeans	CustomerProfileEditorsForOrgDisplay SegmentationDatabeansResourceGroup

할인

표 21.

데이터 자원	
	DiscountAdministratorsForOrgExecute DiscountAssociateCommandsOnCalculationCodeResource
	DiscountAdministratorsForOrgExecute DiscountCreateCommandsOnStoreEntityResource
	DiscountAdministratorsForOrgExecute DiscountDeployCommandsOnCalculationCodeResource
DataBeans	DiscountViewersForOrgDisplayDiscountDatabeans

재고 관리

표 22.

데이터 자원	
	ExpectedInventoryManagersForOrgExecute InventoryManageCommandsOnStoreEntityResource
	FulfillmentCenterManagersForOrgExecute FulfillmentCenterCreateCommandsOnOrganizationResource
	FulfillmentCenterManagersForOrgExecute FulfillmentCenterManageCommandsOnFulfillmentResource
	InventoryAdjustersForOrgExecute InventoryAdjustCommandsOnStoreEntityResource
	PickBatchInventoryManagersForOrgExecuteReleaseReadyShipCommands OnFulfillmentCenterResource
	PickPackGeneratorsForOrgExecute PickPackGenerateCommandsOnFulfillmentCenterResource
	ReturnReasonsManagersForOrgExecute ReturnReasonsCommandsOnStoreEntityResource
	VendorInventoryManagersForOrgExecute VendorCreateCommandsOnStoreEntityResource
	VendorInventoryManagersForOrgExecute VendorManageCommandsOnVendorResource
DataBeans	StoreAdministratorsForOrgDisplay OrderFulfillmentStatusDataBeansResourceGroup

계획된 재고

표 23.

데이터 자원	
	StoreAdministratorsForOrgExecute InventoryScheduledCommandsOnStoreEntityResource

재고 관리

표 24.

DataBeans	
	ExpectedInventoryManagersForOrgDisplay ExpectedInventoryDataBeansResourceGroup
	FulfillmentCenterManagersForOrgDisplay FulfillmentCenterDataBeansResourceGroup
	PickBatchInventoryManagersForOrgDisplay PickBatchInventoryDataBeansResourceGroup
	ProductFindInventoryManagersForOrgDisplay ProductFindInventoryDataBeansResourceGroup
	ReceiverOrderManagersForOrgDisplay ReceiverOrderManagementDataBeansResourceGroup
	ReturnReasonsManagersForOrgDisplay ReturnReasonsOrderManagementDataBeansResourceGroup
	ReturnsAdminOrderManagersForOrgDisplay ReturnsAdminOrderManagementDataBeansResource
	SuperUserOrderManagersForOrgDisplay SuperUserOrderManagementDataBeansResourceGroup
	VendorInventoryManagersForOrgDisplay VendorInventoryDataBeansResourceGroup

주문 관리

표 25.

데이터 자원	
	CustomerOrderManagersExecute CustomerServiceCustomerWriteCommandsOnUserResource
	CustomerOrderManagersForDefaultOrgExecute CustomerServiceCustomerWriteCommandsOnUse
	CustomerOrderManagersForOrgExecute CustomerServiceOrderCreateCommandsOnStoreEntityResource
	CustomerOrderManagersForOrgExecute CustomerServiceOrderWriteCommandsOnOrderResource
	CustomerOrderManagersForOrgExecute CustomerServiceReturnCreateCommandsOnStoreEntity
	CustomerOrderManagersForOrgExecute CustomerServiceReturnWriteCommandsOnRMAResource
DataBeans	CustomerOrderManagersDisplay CustomerUserManagementDatabeans
	CustomerOrderManagersForDefaultOrgDisplay CustomerUserManagementDatabeans
	CustomerOrderManagersForOrgDisplay CustomerOrderManagementDatabeans

표 25. (계속)

	LogisticsManagersForOrgDisplay OrdersAndReturnsListsDatabeans
	ReturnsManagersForOrgDisplayReturnsListsDatabean
	UserOrderManagersDisplayUserDatabeans
	UserOrderManagersForDefaultOrgDisplayUserDatabeans

지불

표 26.

데이터 자원	
	AccountAdministratorsForOrgExecute AccountManageCommandsOnAccountResource
	AccountManagersForOrgExecute AccountCreateCommandsOnOrganizationResource
	AccountViewersForOrgExecute PaymentSummaryGenerateCommandsOnAccountResource
	AccountViewersForOrgExecute StorePaymentAdminCommandsOnStoreEntityResource
	AllUsersExecutePaymentOrderWrite CommandsOnOrderResource

정책, 액세스 그룹, 자원 그룹 및 조치 그룹을 편집하기 위한 관리 콘솔 페이지

표 27.

데이터 자원	
	DescendantStoreAdministratorsExecute ACViewPoliciesForOrgActionsOnOrganizationResource
	StoreAdministratorsForOrgExecute ACPolicyCreateCommandsOnOrganizationResource
	StoreAdministratorsForOrgExecute ACPolicyEditCommandsOnACPolicyResource
	StoreAdministratorsForOrgExecute ACViewApplicablePoliciesActionsOnOrganizationResource
	StoreAdministratorsForOrgExecute ACViewPoliciesForUpdateActionsOnOrganizationResource
데이터 bean	StoreAdministratorsForOrgExecute UserGroupSearchViews

상품 어드바이저

표 28.

DataBeans	

표 28. (계속)

	ProductAdvisorStatisticiansForOrgDisplay ProductAdvisorStatisticsDatabeans
	SalesAssistantStatisticiansForOrgDisplay SalesAssistantStatisticsDatabeans

RFQ

표 29.

데이터 자원	
	RFQAdministratorsAdministerRFQs
	RFQAdministratorsManageRFQResponses
	RFQBuyersEvaluateRFQResponsesForRFQsTheyOwn
	RFQBuyersForOrgExecuteRFQCreate CommandsOnStoreEntityDataResourceGroup
	RFQBuyersManageRFQResourcesTheyOwn
	RFQBuyersManageRFQResponsesForRFQsTheyOwn
	RFQSalesManagersExecuteRFQResponse ManageCommandsOnRFQResponseResource
	RFQSalesManagersForOrgCreateRFQResponse
DataBeans	RFQBuyersDisplayRFQDataBeanResourceGroupTheyOwn
	RFQBuyersDisplayRFQResponseDataBeans ViewabletoRFQOwnerResourceGroup
	RFQSalesViewersDisplayRFQDataBeanResourceGroup
	RFQSalesViewersDisplayRFQResponseDataBeanResourceGroup

규칙

표 30.

데이터 자원	
	StoreAdministratorsForOrgExecutePersonalization RuleServiceAdministrationCommandsOnStoreEntityResource
DataBeans	StoreAdministratorsForOrgDisplay PersonalizationRuleServiceAdministrationDataBeanResource

스케줄러

표 31.

데이터 자원	
	StoreAdministratorsForOrgExecute ScheduledJobManageCommandsOnStoreEntityResource
	StoreAdministratorsForOrgExecute ScheduledJobManageCommandsOnUserResource

표 31. (계속)

DataBeans	StoreAdministratorsForOrgDisplay SchedulerDataBeansResourceGroup

주의사항

이 정보는 미국에서 제공되는 제품 및 서비스용으로 작성된 것입니다.

IBM은 다른 국가에서 이 책에 기술된 제품, 서비스 또는 기능을 제공하지 않을 수도 있습니다. 현재 사용할 수 있는 제품 및 서비스에 대한 정보는 한국 IBM 담당자에게 문의하십시오. 이 책에서 IBM 제품, 프로그램 또는 서비스를 언급했다고 해서 해당 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM의 지적 재산권을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수도 있습니다. 그러나 비IBM 제품, 프로그램 또는 서비스의 운영에 대한 평가 및 검증은 사용자의 책임입니다.

IBM은 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 책을 제공한다고 해서 특허에 대한 사용권까지 부여하는 것은 아닙니다. 사용권에 대한 의문사항은 다음으로 문의하십시오.

135-270
서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
한국 아이.비.엠 주식회사
고객만족센터
전화번호: 080-023-8080

2바이트(DBCS) 정보에 관한 사용권 문의는 한국 IBM 고객만족센터에 문의하거나 다음 주소로 서면 문의하시기 바랍니다.

IBM World Trade Asia Corporation Licensing 2-31 Roppongi 3-chome, Minato-ku Tokyo 106, Japan

다음 단락은 현지법과 상충하는 영국이나 기타 국가에서는 적용되지 않습니다.

IBM은 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증없이 이 책을 현상태대로 제공합니다. 일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다.

이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다. 이 정보는 주기적으로 변경되며, 이 변경사항은 최신판에 통합됩니다. IBM은 이 책에서 설명한 제품 및/또는 프로그램을 사전 통고없이 언제든지 개선 및/또는 변경할 수 있습니다. 이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다. 일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다.

이 정보에서 비IBM의 웹 사이트는 단지 편의상 제공된 것으로, 어떤 방식으로든 이들 웹 사이트를 옹호하고자 하는 것은 아닙니다. 해당 웹 사이트의 자료는 본 IBM 제품 자료의 일부가 아니므로 해당 웹 사이트 사용으로 인한 위험은 사용자 본인이 감수해야 합니다.

IBM은 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다.

(i) 독립적으로 작성된 프로그램 및 기타 프로그램(이 프로그램 포함) 간의 정보 교환 및 (ii) 교환된 정보의 상호 이용을 목적으로 본 프로그램에 관한 정보를 얻고자 하는 사용권자는 다음 주소로 문의하십시오.

135-270
서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
한국 아이.비.엠 주식회사
고객만족센터

이러한 정보는 해당 조항 및 조건에 따라(예를 들면, 사용권 지불 포함) 사용할 수 있습니다.

이 정보에 기술된 사용권 프로그램 및 사용 가능한 모든 사용권 자료는 IBM이 IBM 기본 계약, IBM 프로그램 사용권 계약(IPLA) 또는 이와 동등한 계약에 따라 제공한 것입니다.

비IBM 제품에 관한 정보는 해당 제품의 공급업체, 공개 자료 또는 기타 범용 소스로부터 얻은 것입니다. IBM에서는 이러한 제품들을 테스트하지 않았으므로, 비IBM 제품과 관련된 성능의 정확성, 호환성 또는 배상 청구에 대해서는 확신할 수 없습니다. 비IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오.

이 정보에는 일상의 비즈니스 환경에서 사용되는 데이터와 보고서의 예가 들어 있습니다. 이들을 가능한 완벽하게 예시하기 위해 예에는 개인, 회사, 브랜드 및 제품의 이름이 들어 있습니다. 이들 이름은 모두 가공의 것이며 실제 기업의 이름 및 주소와 유사하더라도 이는 전적으로 우연입니다.

IBM의 향후 방향 또는 의도에 대한 모든 언급은 사전 통고 없이 변경되거나 취소될 수 있으며 단지 목표만을 나타내는 것입니다.

저작권

이 정보에는 여러 가지 운영 플랫폼에서 프로그래밍 기법을 보여주는 견본 응용프로그램이 소스 언어로 들어 있습니다. 견본 응용프로그램이 작성된 운영 플랫폼의 응용프로그램 프로그래밍 인터페이스에 부합하는 응용프로그램을 개발, 사용, 마케팅 또는 배포할 목적이라면 IBM에 비용을 지불하지 않고 이들 견본 프로그램을 복사, 수정 및 배포할 수 있습니다. 책에 들어 있는 예를 모든 조건에서 완벽하게 테스트하지는 않았습

니다. 그러므로 IBM은 이들 프로그램의 신뢰성, 서비스 가능성 또는 기능을 보증할 수 없습니다. IBM의 응용프로그램 프로그래밍 인터페이스에 부합하는 응용프로그램을 개발, 사용, 마케팅 또는 배포할 목적이라면 IBM에 비용을 지불하지 않고 이들 샘플 프로그램을 어떤 형태로든 복사, 수정 또는 배포할 수 있습니다.

상표

다음 용어는 미국 또는 기타 국가에서 사용되는 IBM Corporation의 상표입니다.

DB2 DB2 Universal Database

IBM WebSphere

Lotus®, Domino™ 및 Go Webserver는 미국 또는 기타 국가에서 사용되는 Lotus Development Corporation의 상표입니다.

Microsoft™®, Windows™ 및 Windows NT™는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 등록상표입니다.

Pentium™®은 미국 또는 기타 국가에서 사용되는 Intel Corporation의 상표입니다.

Solaris Operating Environment, JDBC, Java™ 및 모든 Java 기반 상표는 미국 또는 기타 국가에서 사용되는 Sun Microsystems, Inc.의 상표 또는 등록상표입니다.

Blaze Advisor, Blaze Expert, Blaze Presenter, Blaze Accessor, Blaze Enterprise, OOScript, 및 Smartlets는 미국 또는 기타 국가에서 사용되는 Blaze Software, Inc.의 상표입니다.

기타 회사, 제품 및 서비스 이름은 해당 회사의 상표 또는 서비스표입니다.

이 제품에 나오는 신용 카드 이미지, 상표 및 상호는 해당 신용 카드에 의한 지불을 승인하는 신용 카드 상표의 소유주에 의해 부여된 판매자만이 사용할 수 있습니다.

IBM 한글 지원에 관한 설문

FAX : (02) 3787-0123

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

책 제목: IBM® WebSphere Commerce®
액세스 제어 안내서
버전 5.4

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

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

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

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

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

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

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

☜ IBM 한글 지원 서비스에 대해 기타 제안사항이 있으시면 적어주십시오.

_____

_____

_____

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