IBM WebSphere Commerce

보안 안내서

버전 5.5

IBM WebSphere Commerce

보안 안내서

버전 5.5

주!

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, 반드시 247 페이지의 『주의사항』의 정보를 읽으십시오.

초판(2003년 6월)

이 개정판은 새 개정판에서 별도로 명시하지 않는 한, IBM WebSphere Commerce 버전 5.5(제품 번호 5724-A18) 및 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.

IBM은 여러분의 의견을 환영합니다. 다음 URL에서 사용할 수 있는 온라인 IBM WebSphere Commerce 문서 피드백 양식을 사용하여 사용자 의견을 보낼 수 있습니다.

http://www.ibm.com/software/commerce/rcf.html

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

목차

이 책에 대하여

이 책에서는 WebSphere Commerce의 보안 기능과 해당 기능의 구성 방법에 대해 설명합니다.

WebSphere Commerce와 관련된 인증, 권한 및 액세스 제어 정책과 같은 기능 및 보안 문제를 자세히 설명합니다. 이 책은 사이트의 보안을 담당하는 사람(시스템 관리자나 WebSphere Commerce 사이트 운영자를 포함)에게 WebSphere Commerce 프로덕션 사이트를 신뢰할 수 있도록 보안하는 방법에 대한 포괄적인 내용을 제공합니다.

이 책은 WebSphere Commerce 사이트의 보안 책임자 또는 보안 관리자용입니다.

중요

이 책에서는 전자상거래 사이트 전개와 관련된 WebSphere Commerce 보안 문제만을 다룹니다. 운영체제의 보안 취약점과 관련된 문제는 다루지 않습니다. 운영체제를 보안하기 위한 방법은 운영체제 공급업체에 문의하십시오.

변경사항 요약

이 책 및 이 책의 모든 갱신된 버전은 WebSphere® Commerce 기술 라이브러리 웹 페이지(http://www.ibm.com/software/commerce/library/)에서 사용 가능합니다. WebSphere Commerce 개정판에 대한 추가 정보는 다음 개요 페이지를 참조하십시오.

- Business Edition(http://www.ibm.com/software/webservers/commerce/wc_be/)
- Professional Edition(http://www.ibm.com/software/commerce/wscom/support/wc_pe/)

추가 지원 정보는 WebSphere Commerce 지원 페이지(http://www.ibm.com/software/commerce/support/)를 참조하십시오.

제품에 대한 최종 변경사항에 대해서는 위의 웹 사이트에서 갱신된 제품 README 파일을 참조하십시오.

이 책에 대한 모든 갱신이 이 절에 요약됩니다.

이 책의 내용

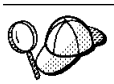
이 책은 다음과 같은 부분으로 구성됩니다.

- 1 페이지의 제 1 부 『WebSphere Commerce 보안 개념』에서는 WebSphere Commerce 보안 모델에 대해 설명하고 WebSphere Commerce 보안의 개념적인 개요에 대해 설명합니다. 이 부분은 WebSphere Commerce 보안에 대한 일반적인 개요를 알려는 사람이나 WebSphere Commerce 사이트에서 보안을 계획하는 사람에게 유용합니다.
- 53 페이지의 제 2 부 『보안 인증 관리』에서는 사이트 보안과 관련된 WebSphere Commerce 관리 태스크에 대해 설명합니다. 이 부분은 사이트 보안과 관련된 관리 태스크를 수행하는 사람에게 유용합니다.
- 99 페이지의 제 3 부 『보안 권한부여 관리』에서는 액세스 제어와 관련된 WebSphere Commerce 권한부여 태스크에 대해 설명합니다. 이 부분은 WebSphere Commerce에서의 액세스 관리와 관련된 시스템 권한부여 태스크를 수행하는 사람에게 유용합니다.
- 191 페이지의 제 4 부 『Payments 보안』에서는 WebSphere Commerce 지불 보안과 관련된 WebSphere Commerce 관리 태스크에 대해 설명합니다. 이 부분은 WebSphere Commerce Payments를 관리하는 사람에게 유용합니다.
- 197 페이지의 제 5 부 『기타 보안 관련 주제』에서는 WebSphere Application Server 보안 기능 향상과 같은 기타 WebSphere Commerce 시스템 관리 태스크에 대해 설명합니다. 이 부분은 보안을 책임지는 시스템 관리자에게 유용합니다.

이 책에서 사용된 규칙

이 책에서는 다음 강조표시 규칙을 사용합니다.

굵은체	필드, 아이콘 또는 메뉴 선택사항의 이름과 같은 GUI(Graphical User Interface) 제어 또는 명령을 표시합니다.
모노체	파일 이름, 디렉토리 경로 및 이름과 같이 정확하게 입력해야 하는 텍스트의 예를 표시합니다.
기울임꼴	단어를 강조하는 데 사용됩니다. 기울임꼴은 시스템의 적절한 값으로 대체해야 하는 이름을 표시합니다.
host_name	WebSphere Commerce 서버의 완전한 호스트 이름(예를 들어, `server.mydomain.ibm.com`이 완전한 이름입니다).
instance_name	사용자가 작업 중인 WebSphere Commerce 인스턴스의 이름.
Windows *드라이브*	논의되는 제품 또는 구성요소를 설치한 드라이브를 표시하는 문자(예: `C:`).



이 아이콘은 태스크를 완료하는 데 도움이 되는 추가정보를 표시합니다.

중요

특히 중요한 정보를 강조표시하는데 사용합니다.

주의

데이터를 보호하기 위한 정보를 강조표시하는데 사용합니다.

Business WebSphere Commerce Business Edition의 특정 정보를 표시합니다.

Professional WebSphere Commerce Professional Edition의 특정 정보를 표시합니다.

AIX AIX®용 WebSphere Commerce의 특정 정보를 표시합니다.

400 IBM® @server iSeries™ 400®(이전에는 AS/400®이라고 함)용 WebSphere Commerce의 특정 정보를 표시합니다.

Linux Linux용 WebSphere Commerce의 특정 정보를 표시합니다.

Solaris Solaris Operating Environment software용 WebSphere Commerce의 특정 정보를 표시합니다.

Windows Windows® 2000용 WebSphere Commerce의 특정 정보를 표시합니다.

경로 변수

다음 변수를 사용하여 디렉토리 경로를 나타냅니다.

DB2_installdir

사용자 시스템의 DB2 Universal Database에 대한 실제 설치 디렉토리를 표시합니다. 다음은 다양한 운영체제에서 DB2 Universal Database에 대한 기본 설치 디렉토리입니다.

AIX `/usr/lpp/db2_08_01`

400 적용되지 않음(운영체제의 일부로 설치됨)

Linux `/opt/IBM/db2/V8.1`

Solaris `/opt/IBM/db2/V8.1`

Windows `C:\Program Files\WebSphere\sqllib`

HTTPServer_installdir

사용자 시스템의 IBM HTTP Server에 대한 실제 설치 디렉토리를 표시합니다. 다음은 다양한 운영체제에서 IBM HTTP Server에 대한 기본 설치 디렉토리입니다.

AIX `/usr/IBMHttpServer`

400 적용되지 않음(운영체제의 일부로 설치됨)

Linux `/opt/IBMHttpServer`

Solaris `/opt/IBMHttpServer`

Windows `C:\Program Files\WebSphere\IBMHTTPServer`

Oracle_installdir

사용자 시스템의 Oracle에 대한 실제 설치 디렉토리를 표시합니다. 다음은 다양한 운영체제에서 Oracle에 대한 기본 설치 디렉토리입니다.

AIX `/oracle/u01/app/oracle/product/9.2.0`

400 OS/400®의 경우 적용되지 않음.

Linux Linux의 경우 적용되지 않음.

Solaris `/opt/oracle/u01/app/oracle/product/9.2.0`

Windows `C:\oracle\ora91`

WAS_installdir

사용자 시스템의 WebSphere Application Server에 대한 실제 설치 디렉토리를 표시합니다. 다음은 다양한 운영체제에서 WebSphere Application Server에 대한 기본 설치 디렉토리입니다.

AIX `/usr/WebSphere/AppServer`

400 `/QIBM/ProdData/WebAS5/Base`

Linux `/opt/WebSphere/AppServer`

Solaris `/opt/WebSphere/AppServer`

Windows `C:\Program Files\WebSphere\AppServer`

WAS_userdir

400 WebSphere Application Server가 사용하는 모든 데이터에 대한 디렉토리를 표시하며, iSeries 시스템에서 사용자가 수정할 수 있거나 구성해야 합니다. 이 디렉토리에 대한 기본값은 다음과 같습니다.

400 `/QIBM/UserData/WebAS5/Base/`*`WAS_instance_name`*

WC_installdir

사용자 시스템의 WebSphere Commerce에 대한 실제 설치 디렉토리를 표시합니다. 다음은 다양한 운영체제에서 WebSphere Commerce에 대한 기본 설치 디렉토리입니다.

AIX `/usr/WebSphere/CommerceServer55`

400 `/QIBM/ProdData/CommerceServer55`

Linux `/opt/WebSphere/CommerceServer55`

Solaris `/opt/WebSphere/CommerceServer55`

Windows `C:\Program Files\WebSphere\CommerceServer55`

WC_userdir

400 WebSphere Commerce가 사용하는 모든 데이터에 대한 디렉토리를 표시하며, iSeries 시스템에서 사용자가 수정할 수 있거나 구성해야 합니다. 이 디렉토리에 대한 기본값은 다음과 같습니다.

400 `/QIBM/UserData/CommerceServer55`

제 1 부 WebSphere Commerce 보안 개념

이 부분에서는 WebSphere Commerce 보안의 개념적인 개요를 제공합니다.

제 1 장 WebSphere Commerce 보안 모델에 대한 소개

이 장에서는 다양한 WebSphere Commerce 보안 개념뿐 아니라 WebSphere Commerce 보안 모델에 대해 설명합니다.

개요

이 절에서는 인증, 권한부여, 정책 및 기밀성의 일반 개념에 대해 설명합니다.

인증의 개념

인증은 사용자나 응용프로그램이 요청하는 신원을 확인하는 프로세스입니다. WebSphere Commerce 시스템에서 인증은 게스트 사용자를 제외하고 시스템에 액세스하는 모든 사용자 및 응용프로그램에 대해 필요합니다. 사용자 인증 프로세스는 항상 SSL에서 수행됩니다. 이것은 네트워크에 불법으로 접속하는 프로그램을 사용하는 제3자가 사용자가 암호를 입력할 때 네트워크에서 이를 *인식*하지 못하도록 합니다. 암호는 일반적인 보안 실례와 같이 인증 프로세스 중에 절대로 암호 해독되지 않습니다. 모든 사용자 암호는 *판매자 키*라고 알려진 128비트 키를 사용하여 단방향으로 해시되고 암호화됩니다. 판매자 키는 WebSphere Commerce 시스템의 설치 및 구성 중에 지정됩니다.

WebSphere Commerce 시스템은 관리 목적을 위해 자체 암호를 갖습니다. 이들 암호는 WebSphere Commerce 사이트측 보안 정책의 일부로서 주기적으로 변경되어야 합니다. WebSphere Commerce 시스템 암호 변경 방법에 대한 자세한 내용은 83 페이지의 제 6 장『암호 설정 및 변경』을 참조하십시오.

권한의 개념

권한부여는 사용자가 자원에 대해 특정 조작을 수행할 수 있는지 여부를 판별하는 프로세스입니다. 권한은 WebSphere Commerce 자원을 관리하는 액세스 제어 정책에서 결정됩니다. WebSphere Commerce 시스템의 다음 두 영역에서 액세스 제어가 필요합니다.

- 권한이 없는 액세스로부터 WebSphere Commerce Enterprise JavaBeans™(EJB beans) 보호. 이 프로세스는 199 페이지의 제 16 장『WebSphere Application Server 보안 사용』에서 설명됩니다.
- 권한 부여된 사용자만 WebSphere Commerce 명령의 서로 다른 그룹을 실행할 수 있도록 보장. 이 프로세스는 *WebSphere Commerce 프로그래밍 안내서 및 학습서*의 "액세스 제어" 절에서 설명합니다.

액세스 제어 정책의 개념

전자상거래 사이트에 참여할 조직과 사용자들의 정의를 완료했다고 가정할 때 일련의 정책을 통해 해당 활동을 관리할 수 있는데 이 프로세스를 *액세스 제어*라고 합니다.

액세스 제어 정책이란 사이트에서 특정 활동을 수행할 수 있도록 권한을 부여받은 사용자 그룹을 설명하는 규칙입니다. 이러한 활동에는 전자상거래 사이트를 운영하고 유지보수하는 데 필요한 수많은 다른 활동뿐 아니라 등록에서부터 경매 관리, 상품 카탈로그 갱신 및 주문 승인까지 포함됩니다.

정책은 사용자에게 사이트에 대한 액세스 권한을 부여하는 것입니다. 하나 이상의 액세스 제어 정책에서 권한이 부여되지 않은 사용자는 사이트의 어떤 기능에도 액세스할 수 없습니다.

WebSphere Commerce의 권한부여 모델은 액세스 제어 정책의 실행을 기반으로 합니다. 액세스 제어 정책은 액세스 제어 정책 관리자에 의해 강제 시행됩니다. 일반적으로 사용자가 보호 가능한 자원에 액세스하려 시도할 때 액세스 제어 정책 관리자는 먼저 해당 사용자에게 어떤 액세스 제어 정책이 적용될 수 있는지를 판별한 후 적용 가능한 액세스 제어 정책을 바탕으로 사용자가 주어진 자원에 대해 요청한 조작을 수행하도록 허용되는지 여부를 판별합니다.

감사 추적의 개념

컴퓨팅 환경에서 *감사 추적*은 컴퓨터 활동을 추적하는 데 사용되는 전자 또는 문서 로그를 의미합니다. 예를 들어 직원은 미수금 계정 같은 기업 네트워크의 한 부분에 액세스할 수 있지만 급여 같은 시스템의 다른 부분에 액세스하도록 권한 부여되지 않을 것입니다. 해당 직원이 암호를 입력하여 권한이 없는 섹션에 액세스하려 시도하는 경우, 이러한 부적절한 활동이 감사 추적에 기록됩니다.

전자상거래 시스템에서 감사 추적은 고객 활동을 기록하는 데 사용됩니다. 감사 추적은 고객과 시스템과의 초기 접속뿐 아니라 상품 또는 서비스의 지불 및 운송 같은 후속 조치를 기록합니다. 회사는 감사 추적을 사용하여 모든 조회나 불만사항에 응답할 수 있습니다. 또한 감사 추적을 사용하여 계정을 조정하고 앞으로의 사업계획과 예산수립을 위한 분석 및 이력 정보를 제공하고 세무 감사의 경우에 판매 기록을 제공할 수 있습니다.

감사 추적은 또한 사이버 공간과 인터넷을 통한 컴퓨터 범죄를 조사하는 데 사용할 수도 있습니다. 시스템에 대해 개별적으로 수행되는 악의적 공격을 밝히기 위해 조사자는 범인이 남긴 감사 추적을 따라갈 수 있습니다. 때로는 사이버 범죄의 범인이 모르고 인터넷 서비스 제공업체의 활동 로그나 대화방 로그에 감사 추적을 남길 수 있습니다.

기밀성의 개념

기밀성은 중요한 정보를 의도하지 않은 사람이 읽지 못하도록 보호하는 프로세스입니다. WebSphere Commerce 시스템에서 기밀성은 중요한 정보가 사용자의 브라우저에서 WebSphere Commerce 서버로, WebSphere Commerce 서버에서 사용자의 브라우저로 이동할 때 필요합니다. 211 페이지의 제 17 장 『IBM HTTP Server를 사용한 프로덕션을 위한 SSL 사용』에 설명된 대로, SSL을 사용하여 시나리오에 대한 기밀성을 제공합니다.

기밀성은 또한 세션 관리 영역에서 필요한 요구사항입니다. HTTP 프로토콜이 stateless이기 때문에 *쿠키*가 사용자를 WebSphere Commerce 서버에 지속적으로 식별하는 데 널리 사용됩니다. 이 쿠키가 도난되는 경우, 사용자 계정이 손상될 수 있습니다. 이것을 일반적으로 *세션 도난*이라고 합니다. WebSphere Commerce는 75 페이지의 제 5 장 『세션 관리』에 설명된 대로 쿠키 스펙의 고유한 특징을 사용하여 세션 도난을 방지합니다.

일반 보안 고려사항

진행 중인 보안 평가

WebSphere Commerce 제품군은 보통 IBM 보안 전문가의 독립된 그룹으로부터 보안 분석을 받습니다. 이 전문가들은 브라우저에서 WebSphere Commerce에 액세스 권한이 있는 사용자의 관점에서부터 WebSphere Commerce 서버가 실행 중인 동일한 시스템에 계정을 갖고 있는 권한이 더 많은 사용자에 이르기까지 보안 분석을 수행합니다. 보안 전문가 분석의 피드백이 WebSphere Commerce의 보안을 지속적으로 개선하는 데 사용됩니다.

WebSphere Commerce 5.5에서의 보안 개선

WebSphere Commerce 5.5에서는 액세스 제어 인프라에 정책 그룹 등록을 추가했습니다.

WebSphere Commerce 5.4에서 정책 소유자의 하위에서 소유한 자원에 정책을 적용했습니다. 동일한 조직 계층의 여러 조직이 다른 레벨의 액세스를 제어할 경우, 다른 레벨을 갖기가 어려울 수 있습니다. 그리고 조직 계층이 많은 경우, 계층의 맨 아래에 있는 조직에 적용되는 모든 정책을 이해하는 것이 혼란스러울 수 있습니다.

WebSphere Commerce 5.5에서 더 단순하고 명시적으로 하기 위해, 비즈니스 및 액세스 제어 요구사항에 근거하여 정책을 우선 정책 그룹으로 그룹화합니다. 예를 들어, 하나의 정책 그룹은 장기 구매 계약을 지원하는 데 필요한 정책을 가질 수 있는 반면, 다른 정책 그룹은 오직 등록된 사용자만이 구매하도록 허용할 수 있습니다. 그런 경우, 조직의 비즈니스 및 액세스 제어 요구사항에 따라 조직은 명시적으로 해당 정책 그룹에 등록합니다. 조직이 정책 그룹에 등록할 때, 그러한 정책 그룹의 정책만이 조직의 자원

에 적용됩니다. 상위 조직의 정책은 적용되지 않습니다. 그러나 조직이 명시적으로 정책 그룹에 등록하지 않는 경우, 등록 중인 가장 근접한 상위의 정책 등록을 상속합니다.

정책 그룹의 개요에 대해서는 19 페이지의 제 3 장 『권한부여 개념』의 "정책 그룹"에 관한 절을 참조하십시오.

WebSphere Commerce 5.4에서의 보안 개선

다음 절은 WebSphere Commerce Suite 5.1에서 WebSphere Commerce 5.4버전으로 향상된 보안 기능으로 WebSphere Commerce 5.5에서는 계속 지원되는 기능에 대해 설명합니다. 이들 개선사항의 대부분은 WebSphere Commerce Business Edition 5.1 릴리스에서 이루어졌습니다. 이들 개선사항은 일반적으로 다음에 적용할 수 있습니다.

- WebSphere Commerce 사이트 운영자
- 시스템 관리자
- WebSphere Commerce 개발자

때로는 이들 역할이 상호 작용할 수 있습니다.

사이트 운영자에 대한 개선사항

다음은 일반적으로 사이트 운영자를 대상으로 하는 WebSphere Commerce 보안 개선사항입니다.

액세스 제어

- **액세스 제어 프레임워크** -- 핵심 개선사항은 새 액세스 제어 프레임워크가 WebSphere Commerce 5.4에서 구현되고 WebSphere Commerce 5.5에서 계속 지원되는 것입니다.(WebSphere Commerce 5.5의 새 정책 그룹 개선에 따라). 이러한 새 프레임워크는 액세스 제어 정책을 사용하여 주어진 사용자가 주어진 자원에 대해 주어진 조치를 수행하도록 허용되는지를 결정합니다. 새 액세스 제어 프레임워크는 객체 단위 액세스 제어를 제공합니다. WebSphere Application Server가 제공하는 액세스 제어와 함께 작업하지만 이를 대체하지는 않습니다. 새 액세스 제어 프레임워크는 99 페이지의 제 3 부 『보안 권한부여 관리』에서 자세히 설명됩니다.

  새 액세스 제어 프레임워크는 다음 방법으로 이전 액세스 제어 기능을 개선합니다.

  빠릅니다.

  광범위한 액세스 정책의 의도를 캡쳐합니다. 프레임워크는 사용자 그룹, 자원 그룹, 조치 그룹 및 관계 그룹의 광범위한 배열을 처리할 수 있습니다.

계층적입니다.

액세스 제어 정책은 정책 그룹에 속합니다. 조직이 등록하는 정책 그룹은 또한 그의 하위 조직에 내재적으로 적용될 수 있습니다.

사용자 정의가 가능합니다.

액세스 제어 정책이 응용프로그램 코드와 분리되므로 코드를 다시 컴파일하지 않고 정책을 변경할 수 있습니다.

컴팩트합니다.

새 프레임워크는 확장성이 큽니다. 액세스 제어 정책의 수는 오브젝트 수가 아니라 비즈니스 프로세스의 수에 따라 확장합니다. 대부분의 그룹화 프레임워크가 암시적 조건을 바탕으로 하므로 조건이 충족되는 동안은 정책이 적용됩니다.

- **사이트간 스크립** -- WebSphere Commerce 구성 관리자의 사이트간 스크립트 보호 노드를 사용하여 허용되지 않는 것으로 지정되는 속성이나 문자를 포함하는 모든 사용자 요청을 거부합니다. 이것은 55 페이지의 제 4 장 『사이트 보안 개선』에서 자세히 설명됩니다.

인증

- **암호 저장** -- WebSphere Commerce는 암호 자체를 저장하는 대신 WebSphere Commerce 데이터베이스의 SHA-1 해싱 설계를 사용하여 암호의 단방향 해시를 암호화하고 저장합니다. 이것은 사이트 또는 시스템 관리자를 포함하여 누구도 사용자 암호를 해독할 수 없게 합니다.
- **암호 무효화** -- WebSphere Commerce 구성 관리자의 암호 무효화 노드를 사용하여 사용자가 처음으로 시스템에 로그인할 때 암호를 변경하도록 요구합니다. 이것은 55 페이지의 제 4 장 『사이트 보안 개선』에서 자세히 설명됩니다.
- **계정 정책** -- WebSphere Commerce 관리 콘솔의 계정 정책 페이지를 사용하여 사이트에 대한 계정 정책을 설정함으로써 사용 중인 계정 관련 정책을 정의합니다. 이것은 55 페이지의 제 4 장 『사이트 보안 개선』에서 자세히 설명됩니다.
- **암호 정책** -- WebSphere Commerce 관리 콘솔의 암호 정책 페이지를 사용하여 사이트에 대한 암호 정책을 설정함으로써 사용자의 암호 선택 특성을 제어합니다. 이것은 55 페이지의 제 4 장 『사이트 보안 개선』에서 자세히 설명됩니다.
- **계정 잠금 정책** -- WebSphere Commerce 관리 콘솔의 계정 잠금 정책 페이지를 사용하여 사이트에 대한 계정 잠금 정책을 설정함으로써 사용자 계정이 손상되는 기회를 줄입니다. 이것은 55 페이지의 제 4 장 『사이트 보안 개선』에서 자세히 설명됩니다.

권한부여

암호로 보호된 명령 -- WebSphere Commerce 구성 관리자의 암호로 보호된 명령 노드를 사용하여 사용자가 지정된 명령을 실행하는 요청을 하는 경우 암호를 입력하도록 설정합니다. 이것은 55 페이지의 제 4 장『사이트 보안 개선』에서 자세히 설명됩니다.

암호화된 데이터

데이터베이스 갱신 도구 -- WebSphere Commerce 구성 관리자의 데이터베이스 갱신 도구 노드를 사용하여 암호 및 신용 카드 정보뿐 아니라 WebSphere Commerce 데이터베이스의 판매자 키 같은 암호화된 데이터를 갱신합니다. 이것은 55 페이지의 제 4 장『사이트 보안 개선』에서 자세히 설명됩니다.

세션 관리

로그인 시간 종료 -- 로그인 시간 종료 노드를 사용하여 장시간 동안 사용하지 않는 사용자를 로그오프하고 시스템에 다시 로그온하도록 요청합니다. 이러한 개선 기능은 WebSphere Commerce 구성 관리자를 통해 호출되며 55 페이지의 제 4 장『사이트 보안 개선』에서 자세히 설명됩니다.

로그 작성

액세스 로그 작성 -- 액세스 로그 작성을 사용하여 WebSphere Commerce에 대한 모든 보안 위협을 빠르게 결정합니다. 이러한 개선 기능은 WebSphere Commerce 구성 관리자를 통해 호출되며 55 페이지의 제 4 장『사이트 보안 개선』에서 자세히 설명됩니다.

시스템 관리자에 대한 개선사항

다음은 일반적으로 사이트 운영자를 대상으로 하며 WebSphere Commerce 5.4에서 수행되고 WebSphere Commerce 5.5에서 계속 지원되는 보안 개선사항입니다.

- 중요한 보안 개선사항은 표준이 아닌 포트 번호(예: 포트 443과 반대인 포트 8000)에서 실행하도록 WebSphere Commerce 관리 도구를 구성하는 능력입니다. 이 포트에 대한 액세스를 제한하여 관리 도구에 대한 액세스를 로컬 네트워크나 인트라넷으로 제한할 수 있습니다.
- WebSphere Commerce 관리 콘솔에서 보안 확인 실행 페이지를 사용하여 가능한 보안 노출을 포함할 수 있는 임시 WebSphere Commerce 파일을 확인하고 삭제하는 보안 프로그램을 실행합니다.

WebSphere Commerce 프로그래머에 대한 개선사항

핵심 개선사항은 새 액세스 제어 프레임워크가 WebSphere Commerce 5.4에서 구현되고 WebSphere Commerce 5.5에서 계속 지원된다는 점입니다. 이 프레임워크는 액세스 제어 정책을 사용하여 주어진 사용자가 주어진 자원에 대해 주어진 조치를 수행하도록 허용되는지를 판별합니다. 새 액세스 제어 프레임워크는 객체 단위 액세스 제어를 제공합니다. WebSphere Application Server가 제공하는 액세스 제어에서 작업하

지만 이를 대체하지는 않습니다. 새 액세스 제어 프레임워크는 99 페이지의 제 3 부 『보안 권한부여 관리』에서 자세히 설명됩니다.

새 액세스 제어 프레임워크는 다음 방법으로 이전 액세스 제어 기능을 개선합니다.

빠릅니다.
광범위한 액세스 정책의 의도를 캡쳐합니다. 프레임워크는 사용자 그룹, 자원 그룹, 조치 그룹 및 관계 그룹의 광범위한 배열을 처리할 수 있습니다.

계층적입니다.
한 조직이 소유하는 액세스 제어 정책이 하위 조직에도 적용됩니다.

사용자 정의가 가능합니다.
액세스 제어 정책이 응용프로그램 코드와 분리되므로 코드를 다시 컴파일하지 않고 정책을 변경할 수 있습니다.

컴팩트합니다.
새 프레임워크는 확장성이 큽니다. 액세스 제어 정책의 수는 오브젝트 수가 아니라 비즈니스 프로세스의 수에 따라 확장합니다. 대부분의 그룹화 프레임워크가 암시적 조건을 바탕으로 하므로 조건이 충족되는 동안은 정책이 적용됩니다.

프로그래머를 위한 보안 고려사항에 대한 추가 정보는 *WebSphere Commerce 프로그래밍 안내서 및 학습서*를 참조하십시오.

WebSphere Commerce Suite 5.1 Pro Edition에서 보안 개선사항

Commerce Suite 5.1가 새 전자상거래 아키텍처를 보여주었고 C++ 기반의 Commerce Suite 4.1을 재작성하였지만 이전 WebSphere Commerce Suite 버전의 모든 보안 기능 뿐만 아니라 새 보안 개선사항을 추가했습니다. 이들 개선사항이 WebSphere Commerce 5.5에서 계승되었습니다.

Commerce Suite 5.1은 이전 릴리스에서 제공되었던 WebSphere Commerce Suite 운영자 및 구매자 자원에 액세스 권한이 없는 사용자로부터의 액세스 제한을 유지했습니다.

- WebSphere Commerce Suite 사용자가 중요한 정보에 대한 액세스를 하거나 제출하기 전에 인증되거나 SSL 모드에 있음을 보장하는 액세스 제어 기능에 대한 지원을 계속합니다.
- Commerce Suite 4.1과 동일한 모델에 따라서 WebSphere Commerce Suite 명령을 그룹에 지정하여 사이트 운영자나 상점 레벨 운영자만이 특정 명령을 실행할 수 있도록 합니다.

일반 보안 개선사항

Java™로 Commerce Suite 5.1을 재작성함하며 C++로 작성된 소프트웨어에 발생하는 많은 고유의 보안 문제점이 해결되었습니다. Java는 포인터를 사용하지 않으므로 대부분의 C++ 기반 소프트웨어의 보안 취약점인 버퍼 오버플로우 문제점을 해결했습니다.

업계 표준인 J2EE 스펙을 준수하여 WebSphere Commerce는 강력한 유형 확인 기능을 사용하여 서버가 크래커나 해커가 지정한 불법 명령문을 실행하지 않도록 합니다.

업계 표준인 Triple DES(데이터 암호화 표준) 알고리즘이 WebSphere Commerce 시스템의 중요한 정보를 보호하는 데 사용되었습니다. Triple DES 알고리즘을 포함하는 패키지는 디지털로 서명되어 패키지가 불법 변경된 경우, WebSphere Commerce 서버가 시작하지 않습니다. 이러한 개선사항이 WebSphere Commerce 5.5에 계속 지원됩니다.

세션 관리

쿠키가 도난되지 않았음을 보장하는 고유한 기술을 사용하여 WebSphere Commerce 세션 관리가 최대 보안을 위해 재작성되었습니다. SSL을 통해서만 이동하고 암호화된 시간소인으로 구성되는 인증 쿠키를 사용하여 재작성된 세션 관리 설계가 세션 도난에 대해 보호됩니다.

인증

실행 중에 WebSphere Commerce 서버에 필요한 시스템 및 응용프로그램 암호가 판매자 지정 128비트 키를 사용하여 안전하게 암호화되었고 WebSphere Commerce 구성 파일에 저장되었습니다. 사용자 URL 항목 상자에 나타나는 중요한 정보가 권한이 없는 노출로부터 구매자를 보호하기 위해 암호화됩니다.

로그 작성

WebSphere Commerce 로그 시스템은 보안을 핵심 고려사항으로 설계하여 구매자의 암호나 신용 카드 정보와 같은 중요한 정보가 기본적으로 WebSphere Commerce 로그 파일에 기록되지 않습니다.

제 2 장 인증

WebSphere Commerce에서 인증은 사용자 또는 응용프로그램이 요청하는 신원을 확인하는 프로세스입니다. 이 장에서는 WebSphere Commerce 인증의 여러 측면을 자세히 설명합니다.

WebSphere Commerce 인증 모델

WebSphere Commerce 인증 모델은 다음 개념을 기초로 합니다.

- 챌린지 메커니즘
- 인증 메커니즘
- 사용자 레지스트리

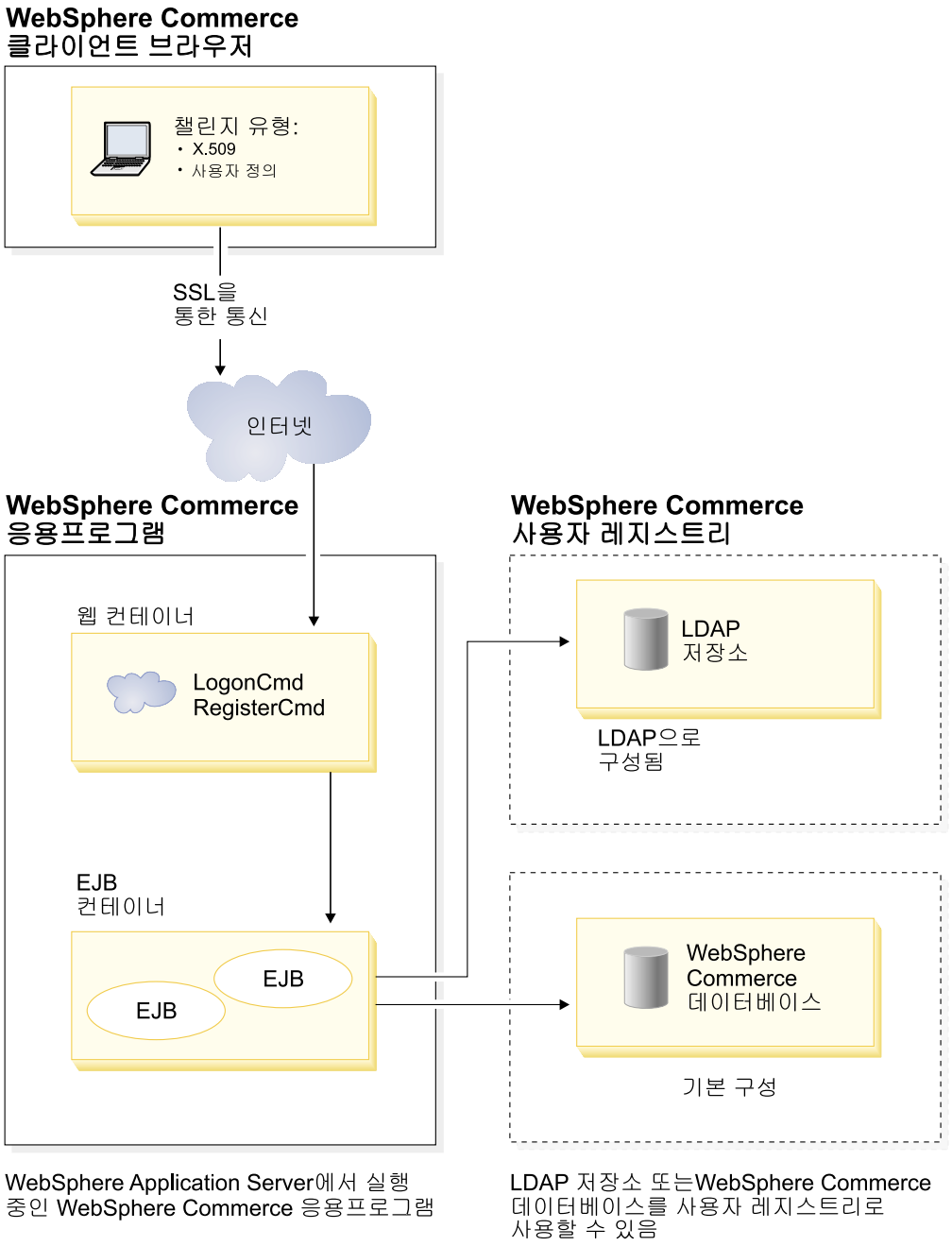


그림 1. WebSphere Commerce 보안 모델

챌린지 메커니즘

챌린지 메커니즘은 서버가 인증 데이터를 요구하고 사용자로부터 검색하는 방법을 지정합니다. WebSphere Commerce는 다음 인증 방법이나 챌린지 메커니즘을 지원합니다.

양식 기반 또는 사용자 정의 인증

이 인증 메커니즘은 HTML 페이지나 JSP 양식을 통한 사이트 또는 상점 고유의 로그인을 허용합니다.

인증서 기반 인증(X.509 인증)

인증 챌린지 메커니즘은 웹 서버가 SSL을 통해 상호 인증을 수행하도록 구성됨을 의미합니다. 클라이언트는 연결을 설정하기 위해 인증서를 제시해야 합니다. 그런 다음 이 인증서를 사용자 레지스트리에 신뢰가능하게 맵핑합니다.

인증 메커니즘

*인증 메커니즘*은 연관된 사용자 레지스트리에 대해 사용자의 인증 데이터를 검증하여 사용자를 인증합니다. WebSphere Commerce는 인증 프로세스 이후의 모든 후속 요청에 대해 사용자와 연관된 인증 토큰을 발행합니다. 이것은 사용자가 로그오프하거나 브라우저를 닫으면 종료됩니다.

인증 유효성 검증

X.509 클라이언트 인증이 웹 서버에서 신뢰되는지와 웹 서버의 인증 정책을 준수하는지를 검증하는 프로세스입니다. WebSphere Commerce는 WebSphere Commerce 데이터베이스에 대해서도 X.509 인증을 검증합니다. WebSphere Commerce가 인증에 대해 세부적인 액세스 제어를 수행하는 반면 웹 서버는 인증에서 정밀하지 않은 액세스 제어를 수행합니다.

LDAP 바인드

사용자를 인증하기 위해 LDAP 바인드 조작을 수행하여 제공된 챌린지 정보가 올바른지 검증하는 프로세스입니다.

데이터베이스 바인드

인증 프로세스 중에 제공되는 사용자 ID와 암호가 WebSphere Commerce 데이터베이스에 저장된 인증 정보와 비교할 때 올바른지 검증하는 프로세스입니다.

사용자 레지스트리

사용자 레지스트리는 사용자 정보 및 사용자의 인증 정보(예: 암호)가 있는 저장소입니다. 프린시펄(즉, 사용자 레지스트리에 있는 사람 사용자 또는 시스템 엔티티의 표현)에서 제공되는 인증 정보는 사용자 레지스트리에 대한 검증 또는 유효성 검증될 수 있습니다.

WebSphere Commerce는 LDAP 사용자 레지스트리와 WebSphere Commerce 데이터베이스의 사용자 도메인에 기반하여 사용자 레지스트리를 지원합니다.

WebSphere Commerce는 다음 LDAP 제공 프로그램을 지원합니다.

- AIX 400 Linux Solaris Windows IBM SecureWay® Directory
- AIX Solaris Windows Netscape Directory Server
- 2000 Windows 2000 Active Directory

신임장

WebSphere Commerce 서버는 인증서, 토큰 또는 사용자 ID와 암호 쌍 같은 신임장 확인에 기반한 인증 메커니즘을 지원합니다. 신임장은 이러한 스키마를 지원하는 사용자 레지스트리에 대해 검증됩니다.

WebSphere Commerce 토큰

WebSphere Commerce는 보안 인증 쿠키를 사용하여 인증 데이터를 관리합니다. 인증 쿠키는 SSL을 통해서만 이동하며 최대한의 보안을 위해 시간소인이 찍힙니다. 이 쿠키는 중요한 명령이 실행될 때마다(예: 사용자에게 신용 카드 번호를 묻는 DoPaymentCmd가 실행될 때) SSL 연결의 사용자를 인증하는데 사용됩니다. 이 쿠키가 도난되어 권한이 없는 사용자에 의해 사용될 수 있는 아주 작은 위험이 있습니다.

SSL 또는 비SSL 연결의 브라우저와 서버 간에 이동되는 제 2의 쿠키는 비SSL 연결의 사용자를 검증하는데 사용됩니다.

WebSphere Application Server LTPA 토큰

LTPA 토큰은 사용자가 요청하는 자원에 대한 액세스 권한을 판별하는 데 필요한 사용자 정보가 있는 데이터입니다. 여기에는 WebSphere Application Server LTPA 서버의 디지털 서명과 함께 인증 데이터가 들어 있습니다.

WebSphere Application Server LTPA(Lightweight Third Party Authentication) 스키마의 경우에는 사용자에 관한 정보가 있는 LDAP 디렉토리는 인증을 수행하는 사용자 레지스트리입니다. 자원 서버는 WebSphere Application Server 보안 서버에 접속하여 LTPA가 인증 메커니즘이 되도록 지정합니다. 또한 요청과 연관된 인증 데이터를 제공합니다. 그러면 WebSphere Application Server 보안 서버는 LTPA 서버에 대해 인증 데이터의 유효성을 검증하고 LTPA 토큰을 리턴합니다.

단일 사인온

HTTP 단일 사인온은 여러 웹 응용프로그램에 대한 사용자 인증을 보존하는 것입니다. 그 목적은 다음을 포함한 신뢰 도메인 안에서 보안 신임장에 대해 사용자가 여러 번 프롬프트되는 것을 막기 위한 것입니다.

- 같이 작동하지만 본질적으로 다른 WebSphere Application Server 서버
- 같이 작동하는 응용프로그램(IBM SecureWay Directory Server와 같은 LDAP 서버)

단일 사인온(SSO) 시나리오에서 HTTP 쿠키가 모든 새 클라이언트-서버 세션(기본 인증 전제)에 대해 사용자가 인증 정보를 입력하는 부담을 덜기 위해 사용자의 인증 정보를 분리하여 웹 서버에 전달하는 데 사용됩니다.

WebSphere Commerce에서의 단일 사인온을 구현하는 단계는 91 페이지의 제 7 장 『단일 사인온』을 참조하십시오.

인증 정책

인증 정책은 WebSphere Commerce에서 인증 프로세스와 인증 데이터 검증에 적용되는 규칙 세트입니다. WebSphere Commerce는 다음 절에서 설명한 대로 계정 정책, 기타 인증 관련 정책 및 세션 정책을 지원합니다.

계정 정책

이 절에서는 WebSphere Commerce에서 사용 가능한 계정 정책에 대해 설명합니다.

계정 정책

WebSphere Commerce 관리 콘솔의 계정 정책 페이지를 사용하여 계정 정책을 설정할 수 있습니다. 계정 정책은 암호 및 계정 잠금 정책 같은 계정 관련 정책을 정의합니다.

계정 정책을 작성한 후에는 사용자에게 해당 정책을 지정할 수 있습니다. 계정 정책이 사용 중인 경우(즉, 사용자에게 계정 정책이 지정된 경우) 계정 정책을 삭제할 수 없습니다.

계정 정책 작성에 대한 자세한 내용은 67 페이지의 『계정 정책 설정』을 참조하십시오.

WebSphere Commerce 온라인 도움말의 참조 주제 "기본 인증 정책"도 참조하십시오.

계정 잠금 정책

WebSphere Commerce 관리 콘솔의 계정 잠금 정책 페이지를 사용하여 WebSphere Commerce 내의 여러 사용자 역할에 대한 계정 잠금 정책을 설정할 수 있습니다. 계정 잠금 정책은 사용자 계정에 대해 잘못된 조치가 실행되는 경우 조치가 계정을 손상시키는 기회를 줄이기 위해 해당 계정을 사용 불가능하게 만듭니다.

계정 잠금 정책은 다음 항목을 강제 시행합니다.

- 계정 잠금 임계값. 이것은 계정이 사용되기 전의 올바르지 않은 로그온 시도 횟수입니다.
- 연속 실패 로그인 지연. 이것은 두 번의 로그인 시도 실패 후에 사용자가 로그인할 수 없는 기간입니다. 연속으로 로그인에 실패할 때마다 지연이 구성된 시간 지연 값(예: 10초)만큼 증가됩니다.

계정 잠금 정책 작성에 대한 자세한 내용은 69 페이지의 『계정 잠금 정책 설정』을 참조하십시오.

암호 정책

WebSphere Commerce 관리 콘솔의 암호 정책 페이지를 사용하면 암호의 특성을 정의하여 암호가 사이트의 보안 정책을 확실히 준수하도록 사용자의 암호 선택을 제어할 수 있습니다.

이 기능은 암호가 따라야 하는 속성을 정의합니다. 암호 정책은 다음 조건을 강제 시행합니다.

- 사용자 ID와 암호가 일치할 수 있는지 여부
- 연속 문자의 최대 발생
- 모든 문자의 최대 인스턴스 수
- 암호의 최대 기간
- 최소 영문자 수
- 최소 숫자 수
- 최대 암호 길이
- 사용자의 이전 암호의 재사용 가능 여부

암호 정책 작성에 대한 자세한 내용은 68 페이지의 『암호 정책 설정』을 참조하십시오.

WebSphere Commerce 온라인 도움말의 참조 주제 "기본 인증 정책"도 참조하십시오.

기타 인증 관련 정책

이 절에서는 WebSphere Commerce에서 사용 가능한 기타 인증 관련 정책을 설명합니다.

암호 무효화

암호 무효화 기능을 사용 또는 사용 불가능하게 하려면 구성 관리자의 암호 무효화 노드를 사용하십시오. WebSphere Commerce 사용자는 사용자의 암호가 만기되면 암호를 변경해야 합니다. 그 경우, 사용자에게 암호를 변경해야 하는 페이지가 경로 재지정됩니다. 사용자는 암호를 변경할 때까지 사이트의 어떤 보안 페이지에도 액세스할 수 없습니다.

암호 무효화 노드 사용에 대한 자세한 내용은 61 페이지의 『암호 무효화 활성』을 참조하십시오.

암호로 보호된 명령

암호로 보호된 명령 기능을 사용 또는 사용 불가능하게 하려면 구성 관리자의 암호로 보호된 명령 노드를 사용하십시오. WebSphere Commerce는 WebSphere Commerce에 로그온하는 등록 사용자가 지정된 WebSphere Commerce 명령을 실행하는 요청을 계속하기 전에 암호를 입력하도록 요구합니다.

주의: 암호로 보호된 명령을 구성할 때 명령 선택사항 목록에 표시된 명령의 일부는 일반 또는 게스트 사용자에 의해 실행될 수 있습니다. 이러한 명령을 암호로 보호된 명령으로 구성하면 일반 및 게스트 사용자가 해당 명령을 실행하는 데 제한을 받습니다. 그러므로 암호로 보호될 명령을 구성할 때 주의해야 합니다.

주: WebSphere Commerce는 `authenticated`로 지정되거나 사용 가능한 명령 목록의 `URLREG` 테이블에서 `https` 플래그가 설정된 명령만을 표시합니다.

암호로 보호된 명령 노드 사용에 대한 자세한 내용은 61 페이지의 『암호로 보호된 명령 사용』을 참조하십시오.

세션 정책

WebSphere Commerce에서 세션 정책은 로그인 시간 종료 정책에 포함됩니다.

로그인 시간 종료 정책을 사용할 때 WebSphere Commerce는 장시간 동안 사용하지 않는 사용자를 로그오프하고 해당 사용자에게 로그인 시간 종료 노드를 사용하여 시스템에 다시 로그온할 것을 요청합니다. 이러한 개선사항은 WebSphere Commerce 구성 관리자에서 호출되며 60 페이지의 『로그인 시간 종료 사용』에서 자세히 설명됩니다.

제 3 장 권한부여 개념

WebSphere Commerce에서 액세스 제어 또는 권한부여는 사용자나 응용프로그램이 자원에 액세스하기 위한 충분한 권한을 갖는지 검증하는 프로세스입니다. 이 장에서는 WebSphere Commerce 액세스 제어의 몇 가지 측면에 대해 자세히 설명합니다.

WebSphere Commerce에서 권한부여 또는 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 전자상거래 사이트에서 필요로 하는 많은 일반적인 액세스 제어 요구사항을 만족하도록 설계됩니다.

비즈니스 모델

WebSphere Commerce 5.4에서는 사용자가 인스턴스를 작성한 후 사이트 운영자가 다음 사항을 결정해야 합니다.

1. 사이트에 적합한 조직 구조
2. 특정 조직에 지정할 역할
3. 필요한 액세스 제어 정책

이러한 모든 사항을 결정한 후 해당 조직에 대해 상점을 공개할 수 있습니다.

WebSphere Commerce 5.5에서 이 프로세스는 비즈니스 모델 작성으로 단순화되었습니다. 비즈니스 모델은 특정 전자상거래 솔루션을 대상으로 하는 조직 구조, 역할, 액세스 제어 정책 및 사전 정의된 상점을 제공합니다. 컨텐츠를 추가, 삭제 또는 변경할 수 있는 기초로서의 개발 단계로 비즈니스 모델을 사용할 수 있습니다.

다음 비즈니스 모델은 WebSphere Commerce 5.5에서 사용할 수 있습니다.

- 직접형 B2C
- 직접형 B2B
- 수요 체인
- 호스트
- 공급 체인

WebSphere Commerce의 비즈니스 모델과 액세스 제어 구성요소를 이해하기 위해서는 먼저 전자상거래 사이트의 전형적인 조직 계층을 이해해야 합니다.

주: 비즈니스 모델에 대한 추가 정보는 *WebSphere Commerce 기본 정보*를 참조하십시오.

조직 계층

WebSphere Commerce 구성원 서브시스템 내의 사용자 및 조직 엔티티는 계층으로 구성됩니다. 이 계층은 조직 및 조직 단위에 대한 항목과 분기가 있는 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 하위 조직을 가질 수 있습니다. 구매자 또는 판매자 관리자는 조직의 최상위로서 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 전자상거래 사이트의 조직 계층을 보여줍니다.

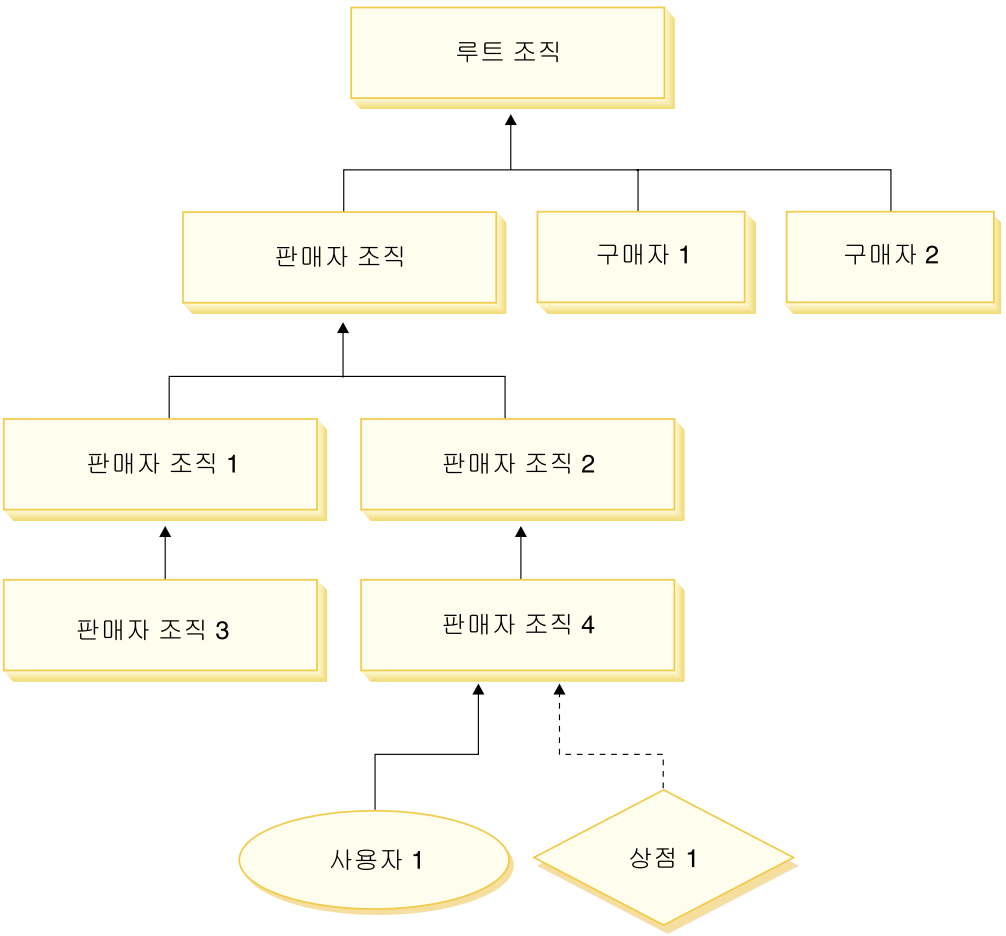


그림 2. B2B 사이트의 조직 계층

루트 조직

루트 조직은 조직 계층의 맨 위에 있습니다. 사이트 운영자에게는 WebSphere Commerce 내의 모든 작업을 수행할 수 있는 슈퍼 유저 액세스 권한이 있습니다. 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 역할에 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. 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 역할은 다음과 같습니다.

- 상점을 소유할 수 있는 부속 조직을 작성합니다. 선택적으로 조직 내에서 승인을 요구하는 프로세스를 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 등

록하고 해당 조직에 관련된 액세스 제어 정책에 따라 조직의 비즈니스 요구사항에 맞게 서로 다른 역할을 사용자에게 지정합니다.

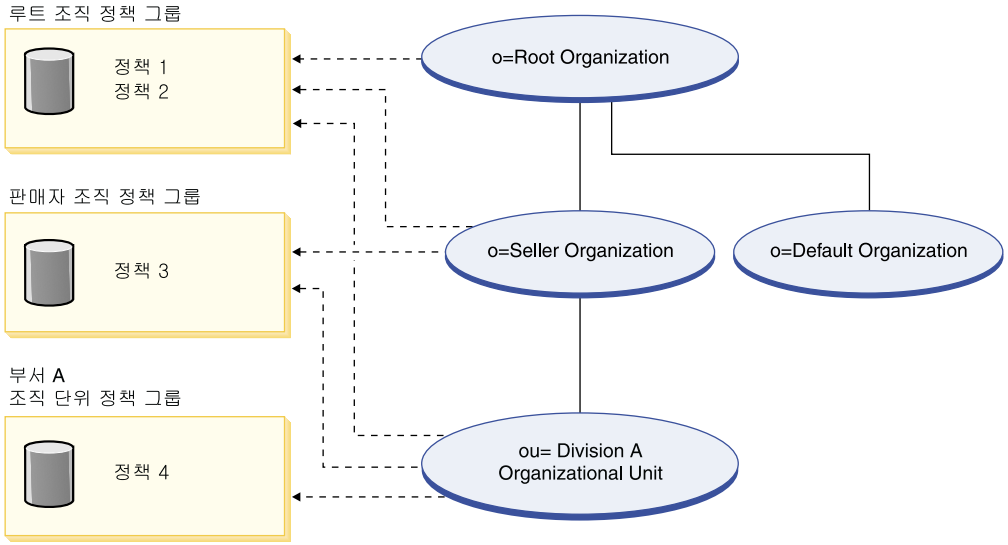
구매자 관리자의 역할은 다음과 같습니다.

- 구매자 조직 내에 부속 조직을 작성하고 관리합니다. 선택적으로, 조직 내에서 승인을 요구하는 프로세스를 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 WebSphere Commerce 온라인 도움말을 참조하십시오.

정책 그룹

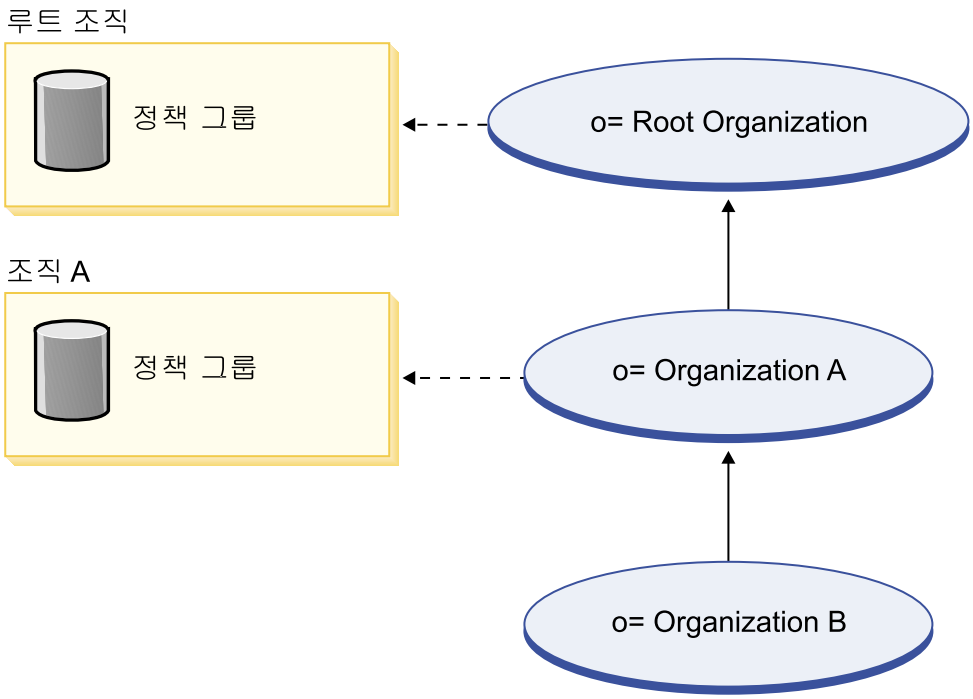
WebSphere Commerce 5.5에서는 다양한 비즈니스 모델을 지원하며 각 비즈니스 모델에는 고유한 액세스 제어 정책 세트가 있습니다. 모델 내에 있는 정책 세트를 그룹화하기 위해 정책 그룹이 작성되었습니다. 정책이 명시적으로 적당한 정책 그룹에 지정되고 나서 조직이 이들 정책 그룹 중 하나 이상에 등록할 수 있습니다. 예를 들면, 다음 도표에서 판매자 조직은 판매자 조직 정책 그룹과 루트 조직 정책 그룹에 등록합니다.



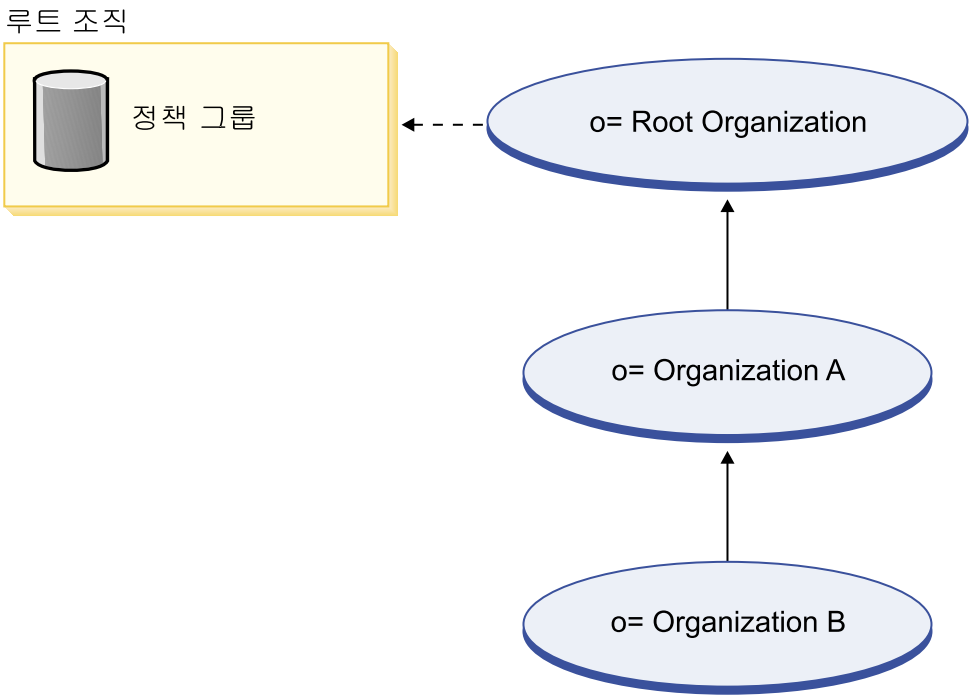
정책은 정책 그룹에 지정됩니다. 예를 들면, 이전 도표에서 정책 1 및 정책 2는 루트 조직 정책 그룹에 지정되고, 정책 3은 판매자 조직 정책 그룹에 지정되며, 정책 4는 부서 A 조직 단위 정책 그룹에 지정됩니다.

정책 그룹 등록

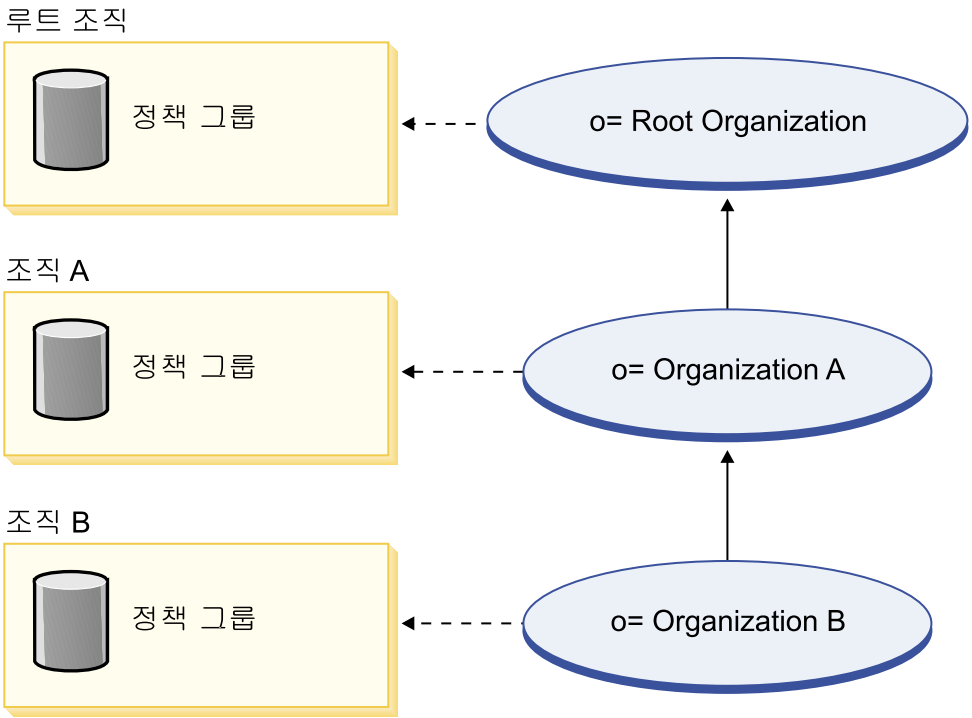
이전 버전의 WebSphere Commerce에서 정책은 해당 정책의 소유자 조직의 하위 조직에서 소유하는 모든 자원에 적용되었습니다. 예를 들어, 조직 A가 특정 정책을 소유하고 조직 B의 상위이면 조직 B는 해당 정책도 이미 포함합니다. WebSphere Commerce 5.5에서 조직은 이제 정책 그룹에 등록할 수 있습니다. WebSphere Commerce 5.5에서 조직 B가 어떤 정책 그룹에도 등록하지 않으면 액세스 제어 프레임워크는 최소한 하나의 정책 그룹에 등록하는 조직을 발견할 때까지 조직 계층을 위쪽으로 검색하기 시작합니다. 조직 B의 바로 위쪽 상위 조직인 조직 A가 정책 그룹에 등록된 경우, 검색은 중지되고 해당 정책이 조직 A 및 B에 적용됩니다. 이러한 내용은 다음 도표에서 볼 수 있습니다.



조직 A가 정책 그룹에 등록되어 있지 않으면 등록한 조직에 도달할 때까지 조직 계층의 위쪽으로 계속 검색합니다. 이러한 내용은 다음 도표에서 보여줍니다. 여기서 루트 조직은 정책 그룹에 등록합니다. 해당 그룹의 정책은 조직 B와 조직 A에 적용됩니다.



조직 B가 정책 그룹에 등록된 경우, 검색은 조직 B에서 중지됩니다. 따라서 조직 B 정책 그룹의 정책만이 조직 B에 적용됩니다.



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(선택적)

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 자신의 책임을 수행하도록 권한부여되지 않은 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 일반 사용 그룹인 반면 액세스 그룹(-2) 유형의 구성원 그룹은 액세스 제어 용도입니다. 구성원 그룹은 MBRGRPUSG 테이블의 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 요소입니다. 액세스 그룹에서 멤버쉽에 대한 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 관리자는 역할과 판매자 관리자라는 해당 액세스 그룹이 있습니다. 사이트 운영자는 WebSphere Commerce 관리 콘솔을 사용하여 사이트에 대한 액세스 그룹을 작성, 유지보수 및 삭제합니다. 사이트 운영자, 구매자 관리자, 판매자 관리자 또는 채널 관리자는 WebSphere Commerce 조직 관리 콘솔을 사용하여 사용자에게 역할을 지정하거나 명시적으로 액세스 그룹에 사용자를 지정합니다.

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 MBRGRPCOND 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. 그리고 복수 액세스 그룹은 동일한 사용자 속성을 나타낼 수 있으므로, 사용자에게 속성을 지정하면 해당 사용자를 묵시적으로 복수 액세스 그룹에 포함시킬 수 있습니다. 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 명시적으

로 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. 뷰에 대한 역할 기반 정책에서 조치는 뷰의 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, 컨트롤러 명령 com.ibm.commerce.order.commands.OrderCancelCmd는 com.ibm.commerce.order.objects.Order 자원에 대해 작동합니다. 마지막으로 데이터 bean 정책에서 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 포함하며 정책 그룹에 등록하는 동일 조직 엔티티가 소유하는 자원에만 적용됩니다. 자원을 소유하는 조직이 정책 그룹에 등록되지 않은 경우, 가장 근접한 상위 조직이 등록한 정책 그룹의 정책이 적용됩니다.

컨트롤러 명령 자원: 컨트롤러 명령에 대한 역할 기반 액세스 제어의 경우, 정책은 실행 조치가 컨트롤러 명령 자원에서 수행되는 것처럼 구조화됩니다. 이러한 정책은 컨트롤러 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 컨트롤러 명령 세트가 됩니다.

컨트롤러 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 뷰에 대한 역할 기반 액세스 제어에 의해 충분히 보호받지 못하는 경우 데이터 bean을 직간접적으로 보호해야 합니다. 이는 데이터 bean을 포함하는 JSP에 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 추가 정보는 *WebSphere Commerce 프로그래밍 안내서 및 학습서*에서 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 컨트롤러 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 표시하여 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 들면, 정책에서는 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="Relationship" value="something">` 요소는 사용자와 자원 사이의 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 평가하여 검색된 하나 이상의 조직 엔티티 간의 관계를 나타내는 문자열입니다. 이 값은 보호 가능한 자원에서 `fulfills()` 메소드의 관계 매개변수와 일치합니다. aValue1 매개변수를 평가하여 둘 이상의 조직 엔티티가 리턴되면, RELATIONSHIP_CHAIN의 이 부분은 이러한 조직 엔티티 중 최소한 하나가 aValue2 매개변수에서 지정한 관계에 만족하는 경우에 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 추가 정보는 171 페이지의 『관계 그룹 정의』를 참조하십시오.

액세스 제어 정책 유형

두 가지 유형의 액세스 제어 정책은 다음과 같습니다.

- 그룹화 가능 표준 정책(정책 유형 -2)
- 그룹화 가능 템플리트 정책(정책 유형 -3)

시스템에 적용하려면, 그룹화 가능 템플리트와 그룹화 가능 표준 정책은 모두 정책 그룹에 속해야 합니다. 정책을 포함하는 정책 그룹에 등록하는 조직에서 그룹화 가능 표준 정책은 한 번 적용됩니다.

시스템이 실행 중일 때 자원을 소유하는 조직으로 범위를 넓히는 액세스 그룹이 있는 그룹화 가능 템플리트 정책은 사실 동적입니다. 예를 들어, 이 정책 유형이 조직 XYZ에서 소유하는 자원에 적용되면, 이 정책 유형은 사용자가 조직 XYZ 또는 해당 상위 조직의 지정된 역할 중 하나를 실행하는지 확인합니다.

특별 기본 액세스 제어 정책

다음 정책은 몇 가지 기타 설명을 필요로 합니다.

- 사이트 운영자는 모든 것을 수행할 수 있습니다(SiteAdministratorsCanDoEverything).
- BecomeUser 고객 서비스 그룹은 고객을 위해 Become 사용자 명령을 실행합니다 (BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup).

SiteAdministratorsCanDoEverything 정책은 슈퍼유저에게 사이트 운영자 역할을 갖는 운용자에 대한 액세스를 부여하는 특별 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.

BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup 정책은 운영 사용자가 기타 사용자를 위해 지정된 명령을 실행하게 하는 특별 정책입니다. 고객이 서비스 담당자로 하여금 자신을 위해 주문을 작성하도록 요청할 때 이러한 정책이 필요합니다. 이 경우, 고객 서비스 담당자는 고객 자신이 명령을 실행하는 것과 같이 명령을 실행할 수 있습니다.

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.

WebSphere Commerce의 모든 역할의 범위는 조직입니다. 예를 들어, 사용자가 조직 X의 상품 관리자 역할을 수행합니다. 이 경우 조직 X는 상품 관리자 역할을 지원해야 합니다. 일반적으로 조직은 사용자에게 해당 조직의 역할을 지정하기 전에 해당 역할을 지원해야 합니다. 그러면 액세스 제어 정책은 이 사용자가 조직 X와 해당되는 부속 조직의 컨텍스트 내에서만 상품 관리 작업을 수행할 수 있도록 설정할 수 있습니다.

주: 사용자 및 조직에 역할을 지정하는 것은 MBRROLE 테이블에서 수행됩니다.

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

- 기술적 운영 역할
- 마케팅 역할
- 운영 역할
- 고객 서비스 역할
- 비즈니스 관계 역할
- 상품 관리 및 판매 계획 역할

WebSphere Commerce 5.5에서 각 역할은 하나 이상의 비즈니스 모델과 연관됩니다. 각 모델에서 역할은 Commerce 액셀러레이터, 관리 콘솔 및 조직 관리 콘솔 도구를 사용하여 선택한 수의 태스크를 수행할 수 있습니다. 비즈니스 모델에 대한 자세한 정보는 *WebSphere Commerce 기본 정보*를 참조하십시오.

다음 도표는 각 도구에 대해 각 역할이 갖는 액세스를 표시합니다. 사용자에게 역할을 지정하기 전에 해당 역할에 적용할 수 있는 액세스 제한에 대해 올바른 정보를 갖는지 확인하십시오.

모든 상점 견본의 WebSphere Commerce 도구에 맵핑되는 역할

표 1. WebSphere Commerce 도구에 맵핑되는 역할

역할	견본	도구
계정 담당	• 직접형 B2B : ToolTech	• 액셀러레이터
구매자 관리자	• 직접형 B2B : ToolTech	• 조직 관리 콘솔
구매자 승인자	• 직접형 B2B : ToolTech	• 조직 관리 콘솔
구매자(판매측)	• 직접형 B2C: Fashion Flow • 직접형 B2B : ToolTech	• 액셀러레이터
구매자(구매측)	• 직접형 B2B : ToolTech • 호스트: 호스팅된 상점 • 공급 체인: 공급자 호스팅된 상점	이 역할은 견본에서 사용할 수 있으나, 특정 도구에 대한 액세스 권한은 없습니다.
카테고리 관리자	• 직접형 B2C: FashionFlow • 직접형 B2B : ToolTech • 수요 체인: 호스팅된 상점, 카탈로그 자원 상점, • 호스트: 호스팅된 상점, 카탈로그 자원 상점 • 공급 체인: 카탈로그 자원 상점, 공급자 호스팅된 상점	• 액셀러레이터

표 1. WebSphere Commerce 도구에 맵핑되는 역할 (계속)

역할	견본	도구
채널 관리자	• 수요 체인: 채널 허브 • 호스트: 호스트 허브 • 공급 체인: 상점 디렉토리	• 액셀러레이터 • 조직 관리 콘솔
고객 서비스 영업대표	• 직접형 B2C: Fashion Flow • 직접형 B2B : ToolTech	• 액셀러레이터
고객 서비스 대표	• 직접형 B2C: Fashion Flow • 직접형 B2B : ToolTech	• 액셀러레이터
물류 관리자	• 직접형 B2B : ToolTech • 공급 체인: 공급자 호스팅된 상점	• 액셀러레이터
마케팅 관리자	• 직접형 B2C: Fashion Flow • 직접형 B2B : ToolTech • 수요 체인: 채널 허브, 호스팅된 상점, 재판매자 상점 첫화면 자원 상점 • 호스트: 호스팅된 상점, 호스팅된 상점 첫화면 자원 상점	• 액셀러레이터
운영 관리자	• 직접형 B2C: Fashion Flow • 수요 체인: 호스팅된 상점 • 호스트: 호스팅된 상점	• 액셀러레이터
포장업자	• 직접형 B2C: Fashion Flow • 직접형 B2B : ToolTech	• 액셀러레이터
조달 구매자	• 직접형 B2B : ToolTech • 공급 체인: 공급자 호스팅된 상점	이 역할은 견본에서 사용할 수 있으나, 특정 도구에 대한 액세스 권한은 없습니다.
조달 구매자 관리자	• 직접형 B2B : ToolTech • 공급 체인: 공급자 호스팅된 상점	이 역할은 견본에서 사용할 수 있으나, 특정 도구에 대한 액세스 권한은 없습니다.
상품 관리자	• 직접형 B2C: Fashion Flow • 직접형 B2B : ToolTech	• 액셀러레이터
수령인	• 직접형 B2C: Fashion Flow • 직접형 B2B : ToolTech	• 액셀러레이터

표 1. WebSphere Commerce 도구에 맵핑되는 역할 (계속)

역할	견본	도구
등록 고객	• 직접형 B2C: Fashion Flow • 직접형 B2B : ToolTech • 수요 체인: 채널 허브, 호스팅된 상점 • 호스트: 호스트 허브, 호스팅된 상점 • 공급 체인: 상점 디렉토리, 공급자 호스팅된 상점	이 역할은 견본에서 사용할 수 있으나, 특정 도구에 대한 액세스 권한은 없습니다.
반품 운영자	• 직접형 B2C: Fashion Flow • 직접형 B2B : ToolTech	• 액셀러레이터
판매 관리자	• 직접형 B2B : ToolTech • 공급 체인: 공급자 호스팅된 상점	• 액셀러레이터
판매자	• 직접형 B2C: Fashion Flow • 직접형 B2B : ToolTech • 수요 체인: 호스팅된 상점 • 호스트: 호스팅된 상점 • 공급 체인: 공급자 호스팅된 상점	• 액셀러레이터
판매자 관리자	• 직접형 B2C: Fashion Flow • 직접형 B2B : ToolTech • 수요 체인: 채널 허브, 호스팅된 상점 • 호스트: 호스트 허브, 호스팅된 상점 • 공급 체인: 상점 디렉토리, 공급자 호스팅된 상점	• 조직 관리 콘솔

표 1. WebSphere Commerce 도구에 맵핑되는 역할 (계속)

역할	견본	도구
사이트 운영자(루트 조직)	• 직접형 B2C: Fashion Flow • 직접형 B2B : ToolTech • 수요 체인: 채널 허브, 호스팅된 상점, 카탈로그 자원 상점, 재판매자 상점 첫화면 자원 상점. • 호스트: 호스트 허브, 호스팅된 상점, 카탈로그 자원 상점, 호스팅된 상점 첫화면 자원 상점 • 공급 체인: 상점 디렉토리, 공급자 호스팅된 상점, 카탈로그 자원 상점, 공급자 자원 상점	• 액셀러레이터 • 조직 관리 콘솔 • 관리 콘솔

주:

1. 사이트 운영자는 관리 콘솔에 대한 액세스를 갖는 유일한 역할입니다.
2. 특정 역할 및 역할이 액세스할 수 있는 각 도구의 메뉴에 대한 추가 정보는 WebSphere Commerce Production 온라인 도움말의 "역할" 파일을 참조하십시오.
3. 각 견본 상점에 대한 자세한 정보는 WebSphere Commerce Production 및 Development 온라인 도움말의 "상점"을 참조하십시오.

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

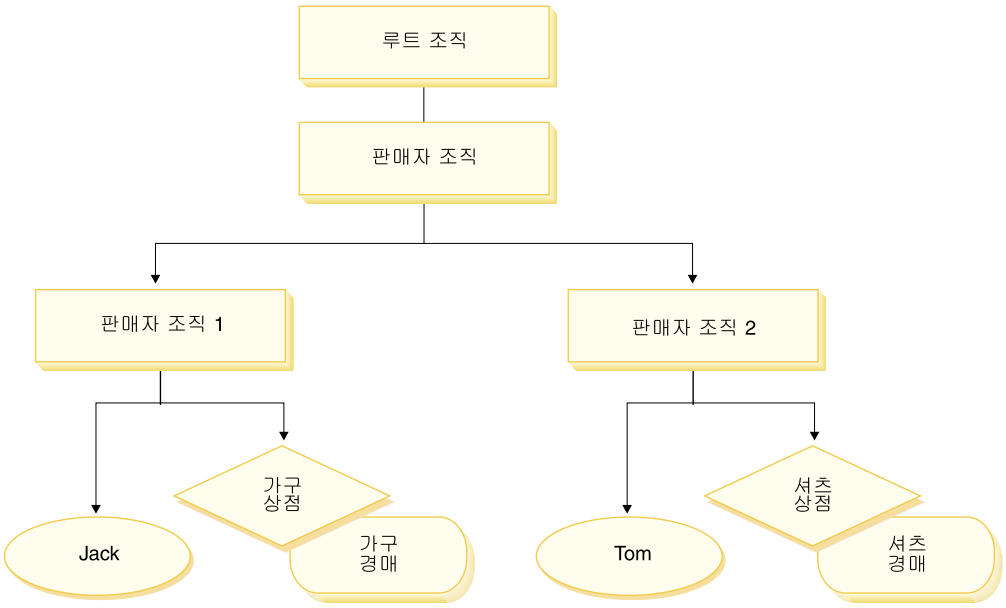
*정책 관리자*는 현재 사용자가 지정된 자원에 대해 지정된 조치를 실행할 수 있는지 여부를 판별하는 액세스 제어 구성요소입니다. 액세스 제어 정책은 XML 포맷으로 지정됩니다. 인스턴스 작성 중에 기본 정책 및 정책 그룹은 자동으로 해당되는 데이터베이스 테이블에 로드됩니다. WebSphere Commerce Application Server가 시작되면 액세스 제어 정보는 정책 관리자가 사용자 권한을 확인하도록 호출될 때 이를 신속하게 수행할 수 있도록 메모리에 캐시됩니다. 액세스 제어 정보가 WebSphere Commerce 관리 콘솔을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

정책 레지스트리를 갱신해야 합니다. 정책 그룹 데이터를 변경한 경우, 액세스 제어 정책 그룹 레지스트리를 갱신해야 합니다. WebSphere Commerce를 재시작하면 캐시도 갱신됩니다.

사용자가 보호 자원에 대한 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 평가하여 사용자에게 대상 자원에서 조치를 수행할 수 있는 권한이 부여되었는지 평가합니다. 그러한 최소 하나의 정책이 있으면 정책 관리자는 액세스를 부여하고, 그렇지 않으면 액세스를 거부합니다.

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 컨트롤러 명령과 뷰에 사용합니다. 이러한 유형의 액세스 제어는 명령이 작용하는 데이터 자원을 고려하지 않습니다. 단지 사용자가 특정 컨트롤러 명령 또는 뷰를 실행할 수 있는지를 판별합니다. 이러한 레벨의 액세스 제어는 필수이므로 런타임에 의해 수행됩니다.

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

뷰에 대한 명령 레벨 액세스 제어: URL에서 직접 뷰를 호출하거나 뷰가 명령을 통한 경로 재지정의 결과일 경우, 그 뷰는 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. 37페이지에서 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 자원에 대한 액세스를 갖도록 합니다. 기본적으로 getResources()는 널(Null)값을 리턴합니다. 즉, 어떤 자원 레벨 확인도 수행하지 않습니다.

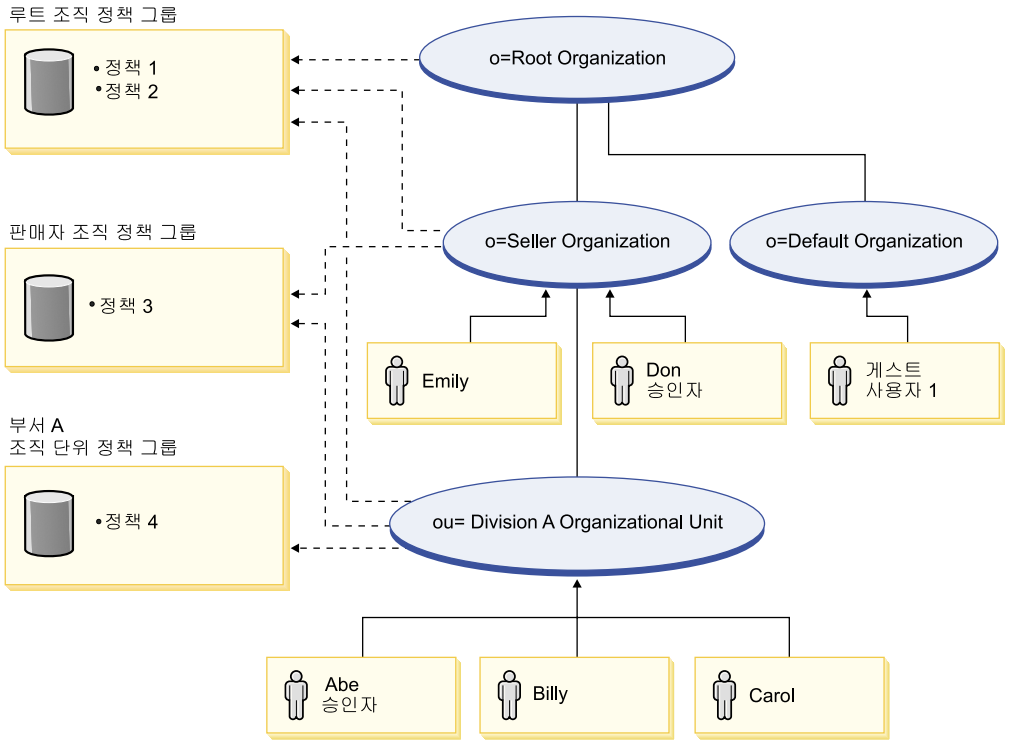
- 명령이 checkIsAllowed(Object Resource, String Action)를 호출합니다. 이 경우, 명령 작성자는 런타임에 의해 getResources()가 호출될 때 확인해야 하는 자원을 모르므로, 명령이 필요에 따라 이 checkIsAllowed() 메소드를 호출하여 현재 조치 및 자원 쌍에 대한 권한이 있는지 판별할 수 있습니다. 조치는 대개 현재 명령의 인터페이스 이름입니다. 이 메소드가 호출될 때, 액세스가 거부되면 ECApplicationException(ECMessage._ERR_USER_AUTHORITY,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

데이터 bean에 대한 자원 레벨 액세스 제어: 위에 설명된 대로 뷰는 보통 역할을 기반으로 하는 명령 레벨 정책에 의해 보호됩니다. 예를 들어, 명령 레벨 정책은 판매자 관리자가 특정 뷰에 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 제어 정책 평가

이 절은 액세스 제어 정책 평가에 대한 지침으로 사용할 수 있습니다. 이 절에서는 시나리오가 제시되어 그룹화 가능한 표준 및 그룹화 가능한 템플리트 액세스 제어 정책을 평가하는 방법에 대한 예를 자세히 안내합니다. 각 절은 관련 정책에 대한 설명 및 각 정책을 사용하는 시나리오로 시작합니다. 그룹화 가능 표준 및 그룹화 가능 템플리트 정책에 대한 자세한 정보는 31 페이지의 『액세스 제어 정책 유형』을 참조하십시오.

다음 도표는 각 시나리오를 그래픽으로 표시합니다.



조직 계층

도표에서 다음 조직이 사이트에 있음을 알 수 있습니다.

- 루트 조직
- 판매자 조직
- 기본 조직
- 부서 A 조직 단위

도표의 실선은 소유권을 표시하고 점선은 등록을 표시합니다. 보는 바와 같이 루트 조직이 판매자 조직 및 기본 조직의 상위입니다. 판매자 조직은 부서 A 조직 단위의 상위입니다.

사용자

도표에서 Don과 Emily는 판매자 조직에 등록되어 있습니다. Abe, Billy 및 Carol은 부서 A 조직 단위에 등록되어 있습니다. 게스트 사용자 1은 등록되어 있지 않지만 액세스 제어를 위해 암시적으로 기본 조직에 속해 있습니다.

역할

Don은 판매자 조직에 대한 승인자 역할이 있습니다. Abe는 부서 A 조직 단위의 승인자 역할을 갖습니다.

액세스 그룹

다음과 같은 액세스 그룹을 이 시나리오에서 사용합니다.

- 등록 사용자: 이 그룹은 암시적으로 사이트에 있는 최소한 한 조직에 등록된 모든 사용자를 포함합니다.
- 판매자에 대한 승인자: 이 그룹은 판매자 조직에 대한 승인자 역할이 있는 모든 사용자를 암시적으로 포함합니다.
- 부서 A에 대한 승인자: 이 그룹은 암시적으로 부서 A 조직 단위에 대한 승인자 역할을 갖는 모든 사용자를 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.

그룹화 가능한 표준 정책 평가

이 절에서는 그룹화 가능한 표준 정책과 이를 평가하는 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 조직, 판매자 조직 및 부서 A 조직 단위가 등록할 루트 조직 정책 그룹의 일부인 그룹화 가능한 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 조직, 판매자 조직 및 부서 A 조직 단위가 등록할 루트 조직 정책 그룹의 일부인 그룹화 가능한 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, -]

판매자 조직 및 부서 A 조직 단위가 등록할 판매자 조직 정책 그룹의 부분인 그룹화 가능 표준 자원 레벨 정책입니다. 이 정책에서 판매자의 승인자는 판매자가 소유하는 문서를 갱신할 수 있습니다.

정책 4:

[부서 A에 대한 승인자, 문서 갱신 조치 그룹, 문서, -]

이것은 부서 A가 등록할 부서 A 조직 단위 정책 그룹의 파트인 그룹화 가능한 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, 명령 소유자가 루트 조직으로 설정됩니다. 따라서 루트 조직에 의해 등록되는 정책 그룹에 속하는 정책만이 사용자가 명령 레벨 액세스를 갖는지 여부를 평가하는 데 사용됩니다. 정책 1과 2가 루트 조직이 등록하고 있는 정책 그룹의 파트입니다.
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. 부서 A가 정책 그룹에 등록하므로, 해당 정책 그룹에 속하는 모든 정책, 즉 정책 1, 2, 3 및 4가 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 조직에 의해 등록되는 정책 그룹에 속하는 정책만이 사용자가 명령 레벨 액세스를 갖는지 여부를 평가하는 데 사용됩니다. 루트 조직은 정책 1과 2를 소유합니다.
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. 부서 A가 정책 그룹에 등록하므로, 해당 정책 그룹에 속하는 모든 정책, 즉 정책 1, 2, 3 및 4가 적용됩니다.
2. Don이 판매자의 승인자 액세스 그룹의 구성원이고 문서 자원에서 문서 갱신 명령을 수행 중이므로 정책 3이 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 조직에 의해 등록되는 정책 그룹에 속하는 정책만이 사용자가 명령 레벨 액세스를 갖는지 여부를 평가하는 데 사용됩니다. 루트 조직은 정책 1과 2를 소유합니다.
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. 판매자 조직 정책 그룹에 등록하므로, 해당 정책 그룹에 속하는 모든 정책, 즉 정책 1, 2 및 3이 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 사용자 1이 자신의 문서를 갱신하려고 시도함: 다음은 이 시나리오에 대한 액세스 제어 확인입니다.

명령 - 레벨 확인:

1. 지정된 상점 ID가 없으므로, 명령 소유자가 루트 조직으로 설정됩니다. 따라서 루트 조직에 의해 등록되는 정책 그룹에 속하는 정책만이 사용자가 명령 레벨 액세스를 갖는지 여부를 평가하는 데 사용됩니다. 루트 조직은 정책 1과 2를 소유합니다.
2. 게스트 사용자 1은 등록된 사용자 액세스 그룹의 구성원이 아니므로 정책 1은 액세스를 부여하지 않습니다.

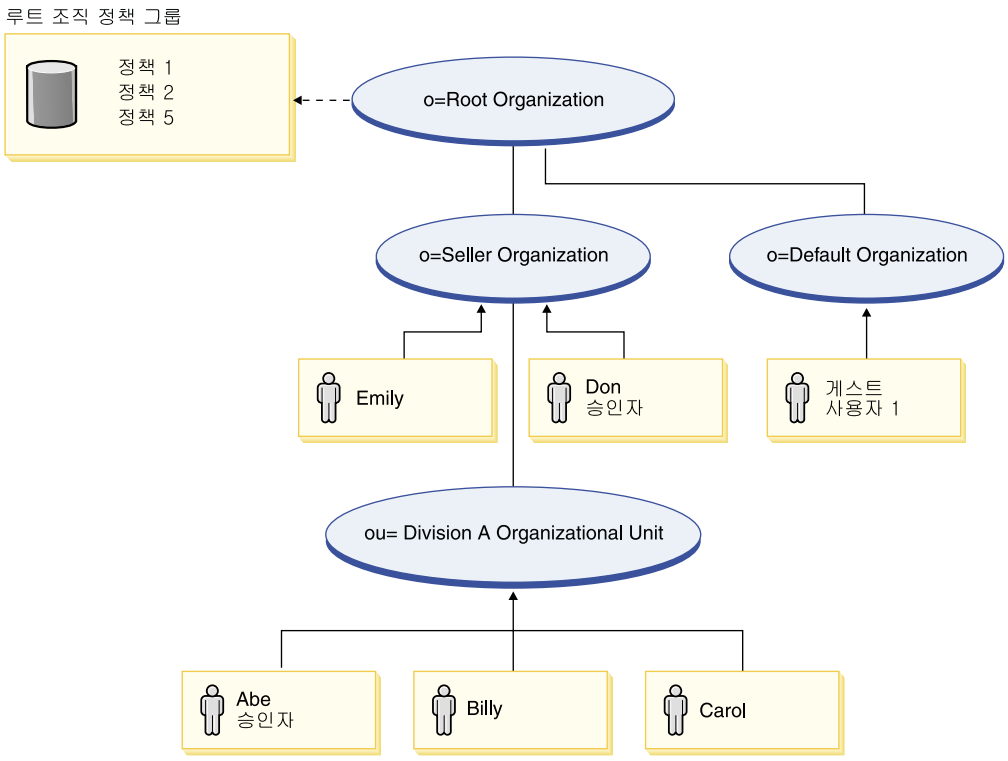
자원 - 레벨 확인:

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

게스트 사용자 1이 명령 레벨 확인에 실패했으므로 자신의 문서를 갱신할 수 없습니다.

그룹화 가능한 템플리트 정책 평가

이 절은 다음 도표에 표시된 구성을 바탕으로 합니다.



문서 갱신과 관련된 액세스 제어 정책

이 구성에서 액세스 제어 정책 1 및 2가 여전히 적용되지만 그룹화 가능한 표준 정책 3과 4가 이제 그룹화 가능 템플리트 정책 5로 대체됩니다. 정책 1과 2에 대한 추가 정보는 41 페이지의 『그룹화 가능한 표준 정책 평가』를 참조하십시오.

정책 5:

[조직에 대한 승인자, 문서 갱신 조치 그룹, 문서, -]

이 정책은 그룹화 가능 템플리트 자원 레벨 정책입니다. 이것은 루트 조직이 등록 중인 루트 조직 정책 그룹의 파트입니다. 그룹화 가능한 템플리트 정책은 런타임 중 자원을 소유하는 조직에 동적으로 적용합니다. 이 정책은 보통 매개변수화된 액세스 그룹을 사용합니다. 이 경우, 다음 매개변수화 액세스 그룹이 사용됩니다.

- 판매자의 승인자: 이 그룹은 문서 자원을 소유하는 조직이나 해당 상위 조직의 승인자 역할을 갖는 모든 사용자를 암시적으로 포함합니다.

시나리오

다음 시나리오는 정책 그룹만이 있는 이전 도표에 표시된 구성에 근거합니다. 루트 조직 정책 그룹은 정책 1, 2 및 5를 포함합니다.

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 조직에 의해 등록되는 정책 그룹에 속하는 정책, 즉 정책 1, 2 및 5만이 사용자가 명령 레벨 액세스를 갖는지 여부를 평가하는 데 사용됩니다.
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. 이 경우, 부서 A가 어떤 정책 그룹에도 등록하지 않으므로, 액세스 제어 프레임워크가 최소한 하나의 정책 그룹에 등록하는 그룹을 발견할 때까지 조직 계층을 위쪽으로 검색하기 시작합니다. 부서 A의 바로 상위 조직인 판매자 조직도 정책 그룹에 등록하지 않습니다. 조직 계층을 계속 위로 올라가면 루트 조직에 도달합니다. 이 조직은 정책 그룹에 등록하므로, 그의 정책, 즉 정책 1, 2 및 5가 적용될 수 있습니다.
2. 그룹화 가능한 템플리트 정책 5는 해당 자원을 소유하는 조직인 부서 A에 적용됩니다. 매개변수화 액세스 그룹인 조직에 대한 승인자가 사용자가 자원 또는 그의 상위를 소유하는 조직에 대한 액세스 그룹 조건에 만족하는지를 확인하도록 동적으로 현재 자원 컨텍스트로 범위를 확장합니다. 이 경우, Don은 판매자 조직(부서 A의 상위)에 대한 승인자이므로, 액세스 그룹의 조건에 만족합니다. Don이 문서 자원에 대해 문서 갱신 명령 조치를 수행 중이므로 정책 5의 다른 요소도 만족되며, 따라서 자원 레벨 정책 확인이 통과됩니다.

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 조직에 의해 등록되는 정책 그룹에 속하는 정책, 즉 정책 1, 2 및 5만이 사용자가 명령 레벨 액세스를 갖는지 여부를 평가하는 데 사용됩니다.
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. Emily의 문서는 판매자 조직이 소유합니다. 판매자 조직이 어떤 정책 그룹에도 등록하지 않으므로, 액세스 제어 프레임워크가 최소한 하나의 정책 그룹에 등록하는 그룹을 발견할 때까지 조직 계층을 위쪽으로 검색하기 시작합니다. 조직 계층을 계속 위로 올라가면 루트 조직에 도달합니다. 이 조직은 정책 그룹에 등록하므로, 그의 정책인 정책 1, 2 및 3이 적용될 수 있습니다.
2. 그룹화 가능한 템플리트 정책 5는 해당 자원을 소유하는 조직인 판매자 조직에 적용됩니다. 매개변수화 액세스 그룹인 조직에 대한 승인자가 사용자가 자원 또는 그의 상위를 소유하는 조직에 대한 액세스 그룹 조건에 만족하는지를 확인하도록 동적으로 현재 자원 컨텍스트로 범위를 확장합니다. 이 경우, Abe는 부서 A 조직 단위(판매자 조직의 하위)에 대한 승인자이므로 액세스 그룹의 조건에 만족하지 않습니다.

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.

```
AuctionAdministratorsForOrgExecuteAucti
onManageCommandsOnAuctionResource
```

주: 이 정책은 자원 레벨 정책입니다. 정책 유형은 그룹화 가능한 템플리트입니다.

첫 번째 예에서는 WebSphere Commerce 조직 관리 콘솔을 이용하여 정책을 읽고 파트를 구분하고 정책의 의미를 이해하는 방법을 학습합니다. 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

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

조직 관리 콘솔에서 정책 보기

1. WebSphere Commerce 조직 관리 콘솔에 로그인하십시오. 액세스 관리 메뉴에서 **정책**을 선택합니다.
2. 루트 조직은 대부분의 기본 액세스 제어 정책을 소유하므로 목록 상자에서 루트 조직을 선택하십시오.
3. 정책 페이지에서 정책 목록들을 화면이동하여 다음 정책을 위치 지정합니다. AuctionAdministratorsForOrgExecuteAuctionManageCommands OnAuctionResource

   이동 막대 도표 뿐만 아니라 **처음**, **이전**, **다음** 및 **마지막** 링크를 이용하여 정책 목록을 화면이동할 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 있음에 주의하십시오.
4. 정책 페이지로 돌아가려면, 아무 조치나 선택한 다음 **정책 표시**를 누르십시오.
5. 다시 정책을 선택하고, 이번에는 **구성원 그룹 표시**를 눌러 이 정책에서 사용되는 구성원(액세스 그룹)을 보십시오.

6. 구성원(액세스) 그룹 이름을 기록하십시오. 여기에서 구성원(액세스) 그룹은 AuctionAdministratorsForOrg입니다.
7. 액세스 관리 메뉴에서 **액세스 그룹**을 선택하십시오.
8. AuctionAdministratorsForOrg를 찾으십시오. 이를 선택하고 **변경**을 누르십시오.
9. **기준**을 누르십시오. 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.

    ```
    AuctionAdministratorsForOrgExecuteAuctionManageCommands
    OnAuctionResource
    ```
11. 정책을 선택하고 **자원 표시**를 누르십시오. 자원 페이지에는 com.ibm.commerce.negotiation.objects.Auction 자원이 표시됩니다. 이는 조치 그룹 활동에 표시된 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.

    ```
    AuctionAdministratorsForOrgExecuteAuctionManageCommands
    OnAuctionResource
    ```
13. 정책을 선택하고 **변경**을 누르십시오. 정책 변경 페이지에서 **관계** 아래의 드롭 다운 메뉴를 보십시오. 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. 이 예제에서는, 정책의 이름이 AuctionAdministratorForOrg라고 지정된 사용자 그룹으로 시작됩니다. ForOrg 표시는 이것이 그룹화 가능한 템플리트 정책임을 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 보려면 데이터베이스에 저장된 정보를 보거나 변경하는 인터페이스를 사용합니다. 데이터베이스의 정보는 정책 관리자가 액세스 제어를 평가할 때 사용합니다. 데이터베이스 정보가 XML 파일보다 최신인 경우 추출기 도구를 사용하여 데이터베이스에서 XML 파일로 액세스 제어 정책 정보를 추출할 수 있습니다.

이것은 XML 파일에서의 정책과 같습니다.

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

여기서, 정책은 다음과 같이 정의됩니다.

Name: 정책의 이름

OwnerID: 정책이 적용되는 조직

UserGroup: 액세스 그룹

ActionGroupName: 조치 그룹

ResourceGroupName: 자원 그룹

PolicyType: 그룹화 가능한 표준 또는 그룹화 가능한 템플리트와 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 같습니다.

AuctionAdministratorsForOrgExecuteAuctionManageCommands
OnAuctionResource

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.

   AuctionAdministratorsForOrgExecuteAuctionManageCommands
   OnAuctionResource
2. 정책과 연관된 액세스 그룹을 식별합니다. 이 경우에, 이미 액세스 그룹이 AuctionAdministratorsForOrg임을 알고 있습니다.
3. 액세스 그룹과 연관된 역할을 찾습니다. 앞의 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 정책 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 컨트롤러 명령 또는 뷰를 수행할 수 있게 허용합니다. 역할 기반 정책과 연관된 조치들을 보려면 예 1과 동일한 프로시저를 사용하여, 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.

99 페이지의 제 3 부『보안 권한부여 관리』에서는 자원 레벨 정책과 역할 기반 정책을 구분하고 그들의 차이점을 이해하며 서로 어떻게 연관되어 있는지를 알 수 있습니다.

제 2 부 보안 인증 관리

이 부분에서는 일반적으로 WebSphere Commerce 사이트 운영자가 수행할 수 있는 보안 인증 태스크에 대해 설명합니다.

제 4 장 사이트 보안 개선

WebSphere Commerce 사이트의 보안을 향상시키기 위해 WebSphere Commerce 구성 관리자에 있는 다음 기능을 사용할 수 있습니다.

- 로그인 시간 종료 노드를 사용하여 장시간 동안 사용하지 않는 사용자를 로그오프하고 시스템에 다시 로그온하도록 요청하십시오. 자세한 내용은 60 페이지의 『로그인 시간 종료 사용』을 참조하십시오.
- 암호 무효화 노드를 사용하여 사용자가 처음으로 시스템에 로그인할 때 암호를 변경하도록 요구하십시오. 자세한 내용은 61 페이지의 『암호 무효화 활성』을 참조하십시오.
- 암호로 보호된 명령 노드를 사용하여 사용자가 지정된 명령을 실행하는 요청을 실행 중인 경우 암호를 입력하도록 설정하십시오. 자세한 내용은 61 페이지의 『암호로 보호된 명령 사용』을 참조하십시오.
- 데이터베이스 갱신 도구 노드를 사용하여 암호 및 신용 카드 정보뿐 아니라 WebSphere Commerce 데이터베이스의 판매자 키 같은 암호화된 데이터를 갱신하십시오. 자세한 내용은 62 페이지의 『암호화 데이터 갱신』을 참조하십시오.
- 사이트간 스크립트 보호 노드를 사용하여 허용되지 않는 것으로 지정되는 속성이나 문자를 포함하는 모든 사용자 요청을 거부하십시오. 자세한 내용은 63 페이지의 『사이트간 스크립트 보호 사용』을 참조하십시오.
- 액세스 로그 작성을 사용하여 WebSphere Commerce에 대한 모든 보안 위협을 신속하게 식별하십시오. 자세한 내용은 66 페이지의 『액세스 로그 작성 사용』을 참조하십시오.

또한 WebSphere Commerce 관리 콘솔의 보안 드롭 다운에서 다음 기능을 사용할 수 있습니다.

- 계정 정책 페이지를 사용하여 사이트에 대한 계정 정책을 설정함으로써 사용 중인 계정 관련 정책을 정의하십시오. 자세한 내용은 67 페이지의 『계정 정책 설정』을 참조하십시오.
- 암호 정책 페이지를 사용하여 사이트에 대한 암호 정책을 설정함으로써 사용자의 암호 선택 특성을 제어하십시오(사용자가 WebSphere Commerce 데이터베이스에 대해 인증되는 경우에만). 자세한 내용은 68 페이지의 『암호 정책 설정』을 참조하십시오.
- 계정 잠금 정책 페이지를 사용하여 사이트에 대한 계정 잠금 정책을 설정함으로써 사용자 계정이 손상되는 기회를 줄이십시오(사용자가 WebSphere Commerce 데이터베이스에 대해 인증되는 경우에만). 자세한 내용은 69 페이지의 『계정 잠금 정책 설정』을 참조하십시오.

- 보안 확인 실행 페이지를 사용하여 가능한 보안 노출을 포함할 수 있는 임시 WebSphere Commerce 파일을 검사하고 삭제하는 보안 프로그램을 실행하십시오. 자세한 내용은 70 페이지의 『보안 확인 실행』을 참조하십시오.

관련 개념에 대한 정보는 WebSphere Commerce 온라인 도움말에서 다음 주제를 참조하십시오.

- 구성 관리자
- WebSphere Commerce 구성 파일
- 관리 콘솔
- 보안

관련 태스크에 대한 정보는 WebSphere Commerce 온라인 도움말에서 다음 주제를 참조하십시오.

- 구성 관리자 실행
- 관리 콘솔 열기

IIS(Internet Information Services) 웹 서버의 보안 고려사항

주의

WebSphere Commerce에서 IIS 웹 서버를 사용하려는 경우, 다음 보안 고려사항을 인식하고 WebSphere Commerce 데이터의 보안 노출을 최소화하는 권장 조치를 취해야 합니다.

문제점: IIS 웹 서버의 경우, 가상 디렉토리의 읽기 권한은 JSP 파일의 소스 코드에 대한 액세스를 제공합니다. JSP 소스 코드의 다운로드를 막으려면, IIS 웹 서버를 사용 중인 경우 웹 페이지의 동적 컨텐츠에서 실제로 정적 컨텐츠를 분리해야 합니다. 이것은 IIS 보안이 파일 유형보다는 디렉토리 위치에 근거하기 때문입니다. 기본 IIS 구성 아래에서 이미지 파일 및 JSP 파일은 단일 별명 아래에 위치 지정됩니다. 테스트 목적을 위해서만 기본값 구성을 사용해야 합니다.

해결 방법: 모든 웹 자원을 보안하려면, *정적 컨텐츠가 읽기 전용 권한을 갖는 다른 가상 디렉토리로 이동되어야 하는 반면 동적 컨텐츠는 실행 전용 권한(읽기가 아님)을 갖는 가상 디렉토리를 사용하여 액세스되어야 합니다.* 가상 디렉토리에 대한 권한을 설정하는 방법에 대한 자세한 정보는 IIS 도움말 정보의 지시사항을 참조하십시오. 또한 보안 패치 및 구성 정책에서 Microsoft® Corporations의 현재 문서를 참조할 것을 권장합니다.

보안에 대한 뷰

WebSphere Commerce의 특정 보안 기능을 사용하기 전에 해당 기능을 사용하려면 먼저 상점에 대한 관련된 뷰를 정의해야 합니다. 아래 정보는 다음에 대한 뷰를 정의하는 방법에 대해 설명합니다.

- 로그인 시간 종료(『로그인 시간 종료』 참조)
- 암호 무효화(58 페이지의 『암호 무효화』 참조)
- 암호로 보호된 명령(58 페이지의 『암호로 보호된 명령』 참조)
- 사이트간 스크립트 보호(59 페이지의 『사이트간 스크립트 보호』 참조)

뷰 작성 및 상점 첫화면 개발에 대한 일반 정보는 *WebSphere Commerce 상점 개발 안내서*를 참조하십시오.

로그인 시간 종료

로그인 시간 종료 기능을 사용하려면 상점에 대한 LoginTimeoutErrorView 및 ReLogonFormView 뷰를 정의해야 합니다.

LoginTimeoutErrorView

로그인 시간 종료 정보가 틀린 경우 WebSphere Commerce는 사용자 브라우저를 이 뷰로 경로 재지정합니다. 이것이 발생하는 경우 누군가가 쿠키를 무단 변경했기 때문일 수 있습니다.

표 2. LoginTimeoutErrorView 속성

ECConstants.EC_LOGIN_TIMEOUT_ERROR_MSGCODE	**1**	만기 시간이 잘못된 값으로 설정됨
	2	로그온 시간이 잘못된 값으로 설정됨
	3	만기 또는 로그온 시간이 잘못된 값으로 설정됨

ReLogonFormView

이 뷰는 사용자의 세션이 만기된 후 사용자에게 표시됩니다. 사용자에게 사용자의 로그온 ID와 암호를 입력하는 양식을 제공해야 합니다. 제출 버튼이 로그온 명령을 호출합니다. 또한 사용자를 다른 페이지, 대부분 상점 입구 페이지로 경로 재지정하는 취소 버튼도 있어야 합니다.

ReLogonFormView에 대한 속성은 없습니다.

표 3. ReLogonFormView 양식 속성

ECUserConstants.EC_UREG_LOGONID	사용자의 로그온 ID.
ECUserConstants.EC_UREG_LOGONPASSWORD	사용자의 로그온 암호.
ECUserConstants.EC_RELOGIN_URL	제공된 신임장이 올바르지 않은 경우에 표시되는 URL. 대부분의 경우, 이 뷰의 이름입니다.
ECConstants.EC_STORE_ID	상점 식별자.

표 3. ReLogonFormView 양식 속성 (계속)

ECConstants.EC_URL	입력되는 신임장이 다른 사용자에게 속할 때 표시되는 URL. 대부분의 경우, 이것은 상점 홈페이지 또는 상점 로그온 페이지에서 사용되는 것과 동일한 URL입니다.

암호 무효화

암호 무효화 보안 기능을 사용하려면 상점에 대한 ChangePassword 뷰를 정의해야 합니다.

ChangePassword

이 뷰는 사용자의 암호가 만기된 경우에 표시됩니다. 사용자에게 현재(만기된) 암호와 새 암호를 입력하는 양식을 제공해야 합니다. 제출 버튼은 ResetPassword 명령을 호출합니다. 또한 사용자를 다른 페이지, 대부분 상점 입구 페이지로 경로 재지정하는 취소 버튼도 있어야 합니다.

표 4. ChangePassword 속성

ECConstants.EC_PASSWORD_EXPIRED_FLAG	**1** 사용자의 암호가 만기되었습니다. 이 속성은 암호가 동일할 때 암호 변경 기능에 사용되는 뷰를 구별하기 위해 필요합니다. 사용자가 암호 변경에 대한 뷰를 호출할 수 있으며, 이 뷰에 지정된 JSP가 두 경우 모두에 동일해야 합니다. JSP는 표시할 것을 결정하기 위해 이 속성을 찾습니다. **널(Null)값** 속성이 URL에 없습니다. 이것은 정상적인 암호 변경 행위입니다.
ECUserConstants.EC_UREG_LOGONID	현재 사용자 로그온 ID.
ECConstants.EC_LOGIN_RETURN_URL	암호 변경이 완료된 후 브라우저가 경로 재지정되는 URL. 이 URL이 이름 ECConstants.EC_URL의 조치 명령으로 전달됩니다.

표 5. ChangePassword 양식 속성

ECUserConstants.EC_UREG_LOGONID	사용자의 로그온 ID id. 현재 로그온 ID가 뷰에 전달되었습니다.
ECUserConstants.EC_UREG_LOGONPASSWORDOLD	기존 암호.
ECUserConstants.EC_UREG_LOGONPASSWORD	새 암호.
ECUserConstants.EC_UREG_LOGONPASSWORDVERIFY	새 암호 확인.
ECConstants.EC_URL	암호 변경이 완료된 후 사용자가 경로 재지정되는 URL. 이 값이 뷰에 전달되었습니다.
ECUserConstants.EC_RELOGIN_URL	암호 변경에 실패하는 경우 브라우저가 경로 재지정되는 URL.

암호로 보호된 명령

암호로 보호된 명령 보안 기능을 사용하려면 상점에 대한 PasswordReEnterErrorView 및 PasswordReEnterFormView 뷰를 정의해야 합니다.

PasswordReEnterErrorView

이 뷰는 다음 시나리오에서 사용됩니다.

- 사용자가 올바른 암호를 제공하지 못하고 로그오프됩니다.
- 인증에 실패했습니다.

두 경우 모두 사용자에게는 현재 페이지의 링크를 통해 다른 페이지로 계속하는 방법이 있어야 합니다.

표 6. PasswordReEnterErrorView 속성

ECConstants.EC_PASSWORD_REREQUEST_MSGCODE	**0** 사용자를 인증하려 시도할 때 문제점이 발생했습니다. **널(Null)값** 속성이 URL에 없습니다. 암호를 제공하지 못한 사용자가 로그오프됩니다.

PasswordReEnterFormView

이 뷰는 사용자가 암호로 보호된 명령을 실행하려고 시도할 때 표시됩니다. 사용자에게 암호를 입력하는 양식을 제공해야 합니다. 암호에 대한 두 개의 입력 필드가 있어야 합니다.

표 7. PasswordReEnterFormView 속성

ECConstants.EC_PASSWORD_REREQUEST_URL	URL이 양식의 제출 버튼을 사용하여 실행됩니다.
ECConstants.EC_PASSWORD_REREQUEST_MSGCODE	사용자에게 표시되는 메시지를 지정하는 메시지 코드: **1** 입력된 암호가 일치하지 않습니다. **2** 암호를 입력하지 않았습니다. **3** 잘못된 암호를 입력했습니다.

조치: URL이 다음 매개변수로서 전달됩니다.

표 8. PasswordReEnterFormView 양식 속성

ECConstants.EC_PASSWORD_REREQUEST_PASSWORD1	첫 번째 암호.
ECConstants.EC_PASSWORD_REREQUEST_PASSWORD2	두 번째 암호.

사이트간 스크립트 보호

사이트간 스크립트 보호 보안 기능을 사용하려면 상점에 대한 ProhibitedAttrsErrorView, ProhibitedCharacterErrorView 및 ProhibCharEncodingErrorView 뷰를 정의해야 합니다.

ProhibitedAttrsErrorView

이 뷰는 사용할 수 없는 속성을 포함했기 때문에 요청이 처리되지 않을 때 사용자에게 표시됩니다.

ProhibitedCharacterErrorView

이 뷰는 사용할 수 없는 문자를 포함했기 때문에 요청이 처리되지 않을 때 사용자에게 표시됩니다.

ProhibCharEncodingErrorView

이 뷰는 위의 ProhibitedCharacterErrorView와 동일합니다.

로그인 시간 종료 사용

주: 상점에 대한 로그인 시간 종료 보안 기능을 사용하려면 57 페이지의 『로그인 시간 종료』에 설명된 대로 상점에 대한 LoginTimeoutErrorView 및 ReLogonFormView 뷰를 정의해야 합니다.

로그인 시간 종료 기능을 사용 또는 사용 불가능하게 하려면 구성 관리자의 로그인 시간 종료 노드를 사용하십시오. 이 기능이 사용될 때 장시간 동안 비활성된 WebSphere Commerce 사용자는 시스템에서 로그오프되고 다시 로그온하도록 요청됩니다. 사용자가 그 뒤에 로그온하는 경우, WebSphere Commerce는 사용자가 작성한 원래 요청을 실행합니다. 사용자가 로그온에 실패한 경우, 원래 요청이 무시되고 사용자는 시스템에서 로그오프 상태로 있게 됩니다.

WebSphere Commerce 도구(예: 관리 콘솔, WebSphere Commerce 액셀러레이터 등)의 경우 로그인 시간 종료가 사용자에게 다시 로그인 페이지를 표시하지 않음에 유의하십시오. 대신 브라우저 창을 닫고 도구에 다시 로그온하는 것은 사용자에게 달려 있습니다. 따라서 도구의 경우, 사용자가 제출한 원래 요청이 처리되지 않습니다.

이 기능을 사용하려면 다음을 수행하십시오.

1. 구성 관리자를 실행하고 다음과 같이 인스턴스에 대한 로그인 시간 종료 노드로 이동하십시오.
   WebSphere Commerce > *host_name* > **인스턴스 목록** > *instance_name* > **인스턴스 특성** > **로그인 시간 종료**
2. 로그인 시간 종료 기능을 활성화하려면 **사용** 선택란을 누르십시오.
3. 로그인 시간 종료 값 필드에 값을 초 단위로 입력하십시오.
4. 변경사항을 구성 관리자에 적용하려면 **적용**을 누르십시오.
5. 인스턴스에 대한 구성을 성공적으로 갱신할 때 갱신 성공을 표시하는 메시지가 수신됩니다.
6. WebSphere Application Server 관리 콘솔에서 WebSphere Commerce 서버 인스턴스를 중지한 후 다시 시작하십시오.

로그인 시간 종료 값이 *instance*.xml 파일에 밀리초 단위로 저장되는 반면 구성 관리자의 값은 초 단위로 입력됨에 유의하십시오.

암호 무효화 활성

주: 암호 무효화 보안 기능을 사용하려면 58 페이지의 『암호 무효화』에 설명된 대로 상점에 대한 ChangePassword 뷰를 정의하십시오.

암호 무효화 기능을 사용 또는 사용 불가능하게 하려면 구성 관리자의 암호 무효화 노드를 사용하십시오. 암호 무효화가 사용될 때 WebSphere Commerce 사용자는 사용자의 암호가 만기되면 암호를 변경해야 합니다. 이 경우, 사용자에게 암호를 변경해야 하는 페이지가 경로 재지정됩니다. 사용자는 암호를 변경할 때까지 사이트의 어떤 보안 페이지에도 액세스할 수 없습니다. 이 기능을 사용하려면 다음을 수행하십시오.

1. 구성 관리자를 실행하고 다음과 같이 인스턴스에 대한 암호 무효화 노드로 이동하십시오.
   WebSphere Commerce > *host_name* > **인스턴스 목록** > *instance_name* > **인스턴스 특성** > **암호 무효화**
2. 암호 무효화 기능을 활성화하려면 **사용** 선택란을 누르십시오.
3. 변경사항을 구성 관리자에 적용하려면 **적용**을 누르십시오.
4. 인스턴스에 대한 구성을 성공적으로 갱신할 때 갱신 성공을 표시하는 메시지가 수신됩니다.
5. WebSphere Application Server 관리 콘솔에서 WebSphere Commerce 서버 인스턴스를 중지한 후 다시 시작하십시오.

암호로 보호된 명령 사용

주: 암호로 보호된 명령 보안 기능을 사용하려면 58 페이지의 『암호로 보호된 명령』에 설명된 대로 상점에 대한 PasswordReEnterErrorView 및 PasswordReEnterFormView 뷰를 정의해야 합니다.

암호로 보호된 명령 기능을 사용 또는 사용 불가능하게 하려면 구성 관리자의 암호로 보호된 명령 노드를 사용하십시오. 이 기능이 사용될 때, WebSphere Commerce는 WebSphere Commerce에 로그온하는 등록 사용자가 지정된 WebSphere Commerce 명령을 실행하는 요청을 계속하기 전에 암호를 입력하도록 요구합니다.

주의: 암호로 보호된 명령을 구성할 때 명령 선택사항 목록에 표시된 명령의 일부는 일반 또는 게스트 사용자에 의해 실행될 수 있습니다. 이러한 명령을 암호로 보호된 명령으로 구성하면 일반 및 게스트 사용자가 해당 명령을 실행하는 데 제한을 받습니다. 그러므로 암호로 보호될 명령을 구성할 때 주의해야 합니다.

이 기능을 사용하려면 다음을 수행하십시오.

1. 구성 관리자를 실행하고 다음과 같이 인스턴스에 대한 암호로 보호된 명령 노드로 이동하십시오.

   WebSphere Commerce > *host_name* > **인스턴스 목록** > *instance_name* > **인스턴스 특성** > **암호로 보호된 명령**
2. 일반 탭에서
   a. 암호로 보호된 명령 기능을 활성화하려면 **사용**을 누르십시오.
   b. 재시도 필드에 재시도 횟수를 입력하십시오(기본 재시도 횟수는 3입니다).
3. 고급 탭에서
   a. 암호로 보호된 명령 목록 창의 목록에서 보호하려는 WebSphere Commerce 명령을 선택하고 **추가**를 누르십시오. 선택한 명령은 현재 암호로 보호된 목록 창에 나열되어 있습니다.
   b. 임의의 WebSphere Commerce 명령에 암호 보호를 사용하지 않으려면, 현재 암호로 보호된 명령 목록 창에서 명령을 선택한 후 **제거**를 누르십시오.
4. 변경사항을 구성 관리자에 적용하려면 **적용**을 누르십시오.
5. 인스턴스에 대한 구성을 성공적으로 갱신할 때 갱신 성공을 표시하는 메시지가 수신됩니다.
6. WebSphere Application Server 관리 콘솔에서 WebSphere Commerce 서버 인스턴스를 중지한 후 다시 시작하십시오.

주: WebSphere Commerce는 `authenticated`로 지정되거나 사용 가능한 명령 목록의 `URLREG` 테이블에서 `https` 플래그가 설정된 명령만을 표시합니다.

암호화 데이터 갱신

판매자 키를 변경하고 주어진 인스턴스에 대한 하나 이상의 WebSphere Commerce 데이터베이스에서 모든 암호화된 데이터(예: 암호 또는 신용카드 번호)를 갱신하려면 구성 관리자의 데이터베이스 노드에서 사용 가능한 데이터베이스 갱신 도구를 사용하십시오. 도구를 사용하려면 다음을 수행하십시오.

1. 구성 관리자를 실행하고 다음과 같이 특정 데이터베이스 항목으로 이동하십시오.

   WebSphere Commerce > *host_name* > **인스턴스 목록** > *instance_name* > **인스턴스 특성** > **데이터베이스** > *database_name*
2. *database_name*을 마우스 오른쪽 단추로 누르고 **데이터베이스 갱신 도구 실행**을 선택하십시오.
   - 선택한 인스턴스에 대한 모든 데이터베이스의 암호화된 데이터를 이주하려면 **이 인스턴스에 대한 모든 데이터베이스 갱신**을 선택하십시오.

     400 iSeries가 단일 데이터베이스 구성을 지원하므로, 이 옵션은 iSeries에 적용되지 않습니다.

- 드롭 다운 목록(기본값)에서 데이터베이스를 선택하여 특정 데이터베이스의 암호화된 데이터를 이주하려면 **선택한 데이터베이스 갱신**을 선택하십시오.

3. 조치 항목 상자에서 실행하려는 조치를 선택하고 매개변수 필드에 필수 정보를 기입하십시오.

조치	매개변수	필수 조치
판매자 키 변경	기존 판매자 키	현재 WebSphere Commerce 인스턴스를 작성할 때 사용한 기존 판매자 키를 입력하십시오.
	새 판매자 키	새 판매자 키를 입력하십시오. 이것은 구성 관리자가 현재 암호화된 데이터를 다시 암호화하기 위한 16자리 16진수입니다. 판매자 키에는 최소 하나의 영숫자(a - F)와 최소 하나의 숫자(0 - 9)가 포함되어야 합니다. 모든 영숫자는 소문자로 입력해야 하고 한 행에 같은 문자를 다섯 번 이상 입력할 수 없습니다.

4. 선택한 WebSphere Commerce 데이터베이스 또는 사용자의 모든 WebSphere Commerce 데이터베이스에 대해 데이터베이스 갱신 도구를 실행하려면 **확인**을 누르십시오.
5. 인스턴스에 대한 구성을 성공적으로 갱신할 때 갱신 성공을 표시하는 메시지가 수신됩니다.
6. WebSphere Application Server 관리 콘솔에서 WebSphere Commerce 서버 인스턴스를 중지한 후 다시 시작하십시오.

사이트간 스크립트 보호 사용

주: 상점에 대한 사이트간 스크립트 보호 기능을 사용하려면 59 페이지의 『사이트간 스크립트 보호』에 설명된 대로 상점에 대한 `ProhibitedAttrsErrorView`, `ProhibitedCharacterErrorView` 및 `ProhibCharEncodingErrorView` 뷰를 정의해야 합니다.

인스턴스에 대한 사이트간 스크립트 보호를 사용 또는 사용 불가능하게 하려면 구성 관리자의 사이트간 스크립트 보호 노드를 사용하십시오. 사이트간 스크립트 보호가 사용될 때 허용되지 않는 것으로 지정되는 속성이나 문자열을 포함하는 모든 사용자 요청을 거부합니다. 구성 관리자의 이 노드에 허용되지 않는 속성과 문자열을 지정할 수 있습니다. 또한 해당 특정 명령에 대한 지정된 속성의 값이 사용할 수 없는 문자열을 포함하도록 하여 사이트간 스크립트 보호로부터 명령을 제외할 수 있습니다. 사이트간 스크립트 보호는 기본적으로 사용하지 않는 것으로 되어 있습니다.

경고: 사이트간 스크립트 보호는 구성을 바탕으로 명령의 실행을 제한한다는 점에서 제한적 기능입니다. 이 기능은 어떤 속성이나 문자열이 사용할 수 없는 것으로 정의되었는지를 확인하지 않으므로, 이 기능을 구성할 때 사용할 수 없는 속성이 명령에 의해

사용되지 않는 것인지 확인하십시오. 또한 사용할 수 없는 문자열이 일반적으로 명령에 전달되는 값이 아닌지 확인하십시오. 이 기능을 구성할 때 매우 주의하십시오.

이 기능을 사용하려면 다음을 수행하십시오.

1. 구성 관리자를 실행하고 다음과 같이 인스턴스에 대한 사이트간 스크립트 보호 노드로 이동하십시오.

   WebSphere Commerce > *host_name* > **인스턴스 목록** > *instance_name* > **인스턴스 특성** > **사이트간 스크립트 보호**

2. 사이트간 스크립트 보호 기능을 활성화하려면 다음과 같이 일반 탭을 사용하십시오.
   a. **사용**을 누르십시오.
   b. WebSphere Commerce 명령에 대해 사용하지 않으려는 속성을 추가하려면 사용할 수 없는 속성 테이블을 마우스 오른쪽 단추로 누르고 **행 추가**를 선택하십시오. 허용하지 않으려는 속성을 입력하십시오. 행당 하나의 속성만을 지정할 수 있습니다.
   c. 사용할 수 없는 속성 테이블에서 속성을 제거하려면 테이블에서 해당 속성을 포함하는 행을 강조표시하고 오른쪽 마우스 단추로 누른 후 **행 삭제**를 선택하십시오.
   d. WebSphere Commerce 명령에 대해 허용하지 않으려는 문자열을 추가하려면 사용할 수 없는 문자 테이블을 오른쪽 마우스 단추로 누르고 **행 추가**를 선택하십시오. 허용하지 않으려는 문자열을 추가하십시오. 행당 하나의 문자열만을 지정할 수 있습니다.
   e. 사용할 수 없는 문자 테이블에서 문자를 제거하려면 사용할 수 없는 문자 테이블에서 해당 문자를 포함하는 행을 강조표시하고 오른쪽 마우스 단추로 누른 후 **행 삭제**를 선택하십시오.

   주: 다음 문자열은 사용할 수 없는 문자 필드에 기본적으로 지정됩니다. 이들 문자열은 대부분 잘못된 사이트간 스크립트 공격에서 스크립팅 태그로 공통적으로 사용됩니다.

   - `<SCRIPT`
   - `<SCRIPT`
   - `<%` 및 `<%`

   .

3. 다음과 같이 특정 명령에 대한 지정된 속성값이 사용할 수 없는 문자열을 포함할 수 있게 하여 사이트간 스크립트 보호에서 WebSphere Commerce 명령을 제외하려면 고급 탭을 사용하십시오.
   a. 명령 목록 상자에서 명령을 선택하십시오.
   b. 사용할 수 없는 문자가 예외 속성 목록 창에서 허용되는 속성 목록을 쉼표로 구분하여 입력하고 **추가**를 누르십시오.

c. 속성과 함께 명령을 제거하려면 예외 명령 목록 창에서 명령을 선택하고 **제거**를 누르십시오.

또한 속성을 선택하고 **제거**를 눌러 명령에서 특정 속성을 제거할 수도 있습니다.

4. 변경사항을 구성 관리자에 적용하려면 **적용**을 누르십시오.
5. 인스턴스에 대한 구성을 성공적으로 갱신할 때 갱신 성공을 표시하는 메시지가 수신됩니다.
6. WebSphere Application Server 관리 콘솔에서 WebSphere Commerce 서버 인스턴스를 중지한 후 다시 시작하십시오.

주:

1. 명령이 사이트간 스크립트 보호에서 제외될 때 지정된 속성의 값이 기호의 HTML 인코딩을 사용하여 인코딩됩니다. 예를 들어, 명령 `cmd1?user=<Thomas>`는 `ascmd1?user=&#60;Thomas&#62;`로 인코드됩니다.
2. 사용할 수 없는 문자 필드에 문자열을 지정할 때 다음에 주의하십시오.
   - 일련의 특정 문자는 문자열이 URL 인코딩 표준에 따라서 단일 문자로 변환될 수 있습니다. 예를 들어, 문자열 `<%bb`는 문자열 `<`*X*로 변환되는데 *X*는 HEX ’bb’(소수 187)의 16진 표시 값을 갖는 단일 문자입니다. 이 경우, 문자열 `<%bb`는 URL에서 전달되는 경우 사이트간 스크립트 보호에 의해 캡처되지 않습니다.
   - 일련의 특정 문자는 URL 인코딩 표준을 따르지 않는 경우 문자열 변환에 실패하게 만들 수 있습니다. 예를 들어, 문자열 `<%gg`는 HEX ‘gg’가 올바른 16진 값 표시가 아니므로 변환에 실패하게 만듭니다. 이 경우, 문자열 `<%gg`는 예외를 유발하여 사이트간 스크립트 보호가 사용되는지 여부와 상관없이 이러한 문자열을 포함하는 URL 요청에 대한 응답이 없게 됩니다.

예: 다음 예를 고려하십시오.

- 사용할 수 없는 문자열: `<SCRIPT`, `<%`

  사용할 수 없는 속성: `mycomment`, `description`

명령	상태
cmd1?description=Available...	거부됨
cmd2?userid=Thomas...	승인됨
cmd3?mycomment=<SCRIPT>...	거부됨
cmd4?password=<%...%>...	거부됨

- `cmd1` 명령의 `text` 속성이 사용할 수 없는 문자열(`<SCRIPT`, `<%`)을 포함하도록 허용하고 다른 속성은 허용하지 않으려는 경우. 예를 들어, `txt` 속성의 경우 `cmd1`을 제외하고 `text`를 예외됨 속성으로 지정할 수 있습니다.

명령	상태
cmd1?text=<SCRIPT>...	승인됨

명령	상태
cmd1?text=<%...%>...	승인됨
cmd1?txt=<SCRIPT>...	거부됨
cmd1?txt=<%..%>...	거부됨

액세스 로그 작성 사용

액세스 로그 작성 특징은 사용될 때 WebSphere Commerce 서버로 들어오는 모든 요청 또는 액세스 위반을 가져오는 요청만을 로그합니다. 액세스 위반 예로는 승인 실패, 충분하지 않은 명령 실행 권한 또는 암호 규칙을 위반하는 암호를 사이트에 재설정하는 것 등이 있습니다. 액세스 로그 작성이 사용될 때 WebSphere Commerce 운영자가 WebSphere Commerce 시스템에 대한 보안 위협을 빨리 식별할 수 있습니다.

승인 실패 또는 권한 부여 실패 이벤트가 발생할 때 다음 정보가 액세스 로그 파일 데이터베이스 테이블인 ACCLOGMAIN 및 ACCLOGSUB에 기록됩니다.

- 클라이언트의 호스트 이름
- 명령을 실행하는 스레드의 ID
- 클라이언트의 사용자 ID
- 이벤트가 발생한 시간
- 실행된 명령
- 명령이 실행된 상점
- 조작이 수행된 자원
- 액세스 제어 확인 결과

액세스 로그 작성을 사용하려면 다음을 수행하십시오.

1. 구성 관리자를 실행하십시오.
2. **호스트 이름** > **인스턴스** > **Instance_List**를 선택한 후 **구성요소** 폴더를 여십시오.
3. **AccessLoggingEventListener**를 선택하십시오.
4. 일반 패널에서 **구성요소 사용** 선택란을 활성화하십시오.
5. 고급 패널을 선택하고 **시작**을 사용하십시오.
6. **적용**을 누르십시오
7. 구성 관리자를 종료하십시오.
8. WebSphere Application Server를 다시 시작하십시오.

로그 파일의 크기를 변경하거나 모든 요청이 기록되는지 여부를 지정하려면 WebSphere Commerce 인스턴스 서브디렉토리에 있는 WebSphere Commerce 인스턴스에 대한 *instance*.xml 파일을 수동으로 편집해야 합니다.

1. 편집기에서 인스턴스에 대한 *instance*.xml 파일을 여십시오

2. <LogSystem>/<activitylog> 노드에 있는 다음 노드를 찾으십시오.

   ```
   <accessLogging cacheSize="aa" logAllRequests="bbbbb" />
   ```

   여기서

   - *aa*는 항목이 데이터베이스에 기록되기 전에 메모리에 기록되는 최대 항목 수를 지정하는 정수 값입니다. 일반적으로 숫자가 높을수록 액세스 로그 작성에 관한 성능이 향상됩니다. 기본값은 32입니다.
   - *bbbbb*는 true 또는 false입니다. true 값은 수신되는 모든 요청이 기록됨을 의미합니다. false 값은 액세스 위반만이 기록됨을 의미합니다. 과다하거나 불필요한 로그 작성을 방지하기 위해 false 값이 권장됩니다. 사이트에서의 인증 문제점이나 보안 위반을 의심할 때만 true를 사용하십시오. 기본값은 false입니다.

3. 갱신을 완료했을 때, WebSphere Commerce 인스턴스에 대한 *instance*.xml 파일을 저장하십시오.
4. WebSphere Application Server를 다시 시작하십시오.

다음 예에서 액세스 로그 작성은 데이터베이스 테이블에 항목을 로그 작성하기 전에 메모리에 3 항목을 보관합니다. 또한 WebSphere Commerce 서버에 대한 모든 수신되는 요청을 기록합니다.

```
<accessLogging cacheSize="3" logAllRequests="true" />
```

계정 정책 설정

WebSphere Commerce 관리 콘솔의 계정 정책 페이지를 사용하여 계정 정책을 설정할 수 있습니다. 이 페이지는 기본적으로 WebSphere Commerce에 제공되는 모든 사전 정의된 정책을 포함하여 모든 기존 계정 정책을 표시합니다. 계정 정책은 암호 및 계정 잠금 정책 같은 계정 관련 정책을 정의합니다. 이 페이지에서

- **새로 만들기**를 눌러 새 계정 정책을 작성할 수 있습니다.
- 목록에서 정책을 선택하고 **변경**을 눌러 기존 계정 정책의 특성을 변경할 수 있습니다.
- 목록에서 정책을 선택하고 **삭제**를 눌러 기존 계정 정책을 삭제할 수 있습니다.

새 계정 정책을 작성하려면 다음을 수행하십시오.

1. WebSphere Commerce 관리 콘솔을 여십시오.
2. 관리 콘솔의 보안 드롭 다운 메뉴에서 **계정 정책**을 누르십시오.
3. 계정 정책 페이지에서 **새로 만들기**를 눌러 새 계정 정책을 작성하십시오.
4. 이름 필드에 계정 정책에 대한 이름을 입력하십시오(예: my_account_policy).
5. 암호 정책 메뉴에서 이미 존재하는 암호 정책을 선택하십시오.
6. 계정 잠금 정책 메뉴에서 이미 존재하는 계정 잠금 정책을 선택하십시오.

7. **확인**을 누르십시오.

계정 정책을 작성한 후에는 사용자에게 해당 정책을 지정할 수 있습니다. 계정 정책을 사용 중인 경우(즉, 사용자에게 계정 정책이 지정된 경우)에는 해당 계정 정책을 삭제할 수 없음에 유의하십시오.

추가 정보에 대해 71 페이지의 『기본 인증 정책』도 참조하십시오.

암호 정책 설정

WebSphere Commerce 관리 콘솔의 암호 정책 페이지를 사용하면 암호가 사이트의 보안 정책을 준수하도록 암호의 특성을 정의하기 위해 사용자의 암호 선택을 제어할 수 있습니다. 이 페이지는 기본적으로 WebSphere Commerce와 함께 제공되는 모든 사전 정의된 정책을 포함하여 모든 기존 암호 정책을 표시합니다.

암호 정책은 암호가 따라야 하는 속성을 정의합니다. 암호 정책은 다음 조건을 강제 시행합니다.

- 사용자 ID와 암호가 일치할 수 있는지 여부
- 연속 문자의 최대 발생
- 모든 문자의 최대 인스턴스 수
- 암호의 최대 기간
- 최소 영문자 수
- 최소 숫자 수
- 최대 암호 길이
- 사용자의 이전 암호의 재사용 가능 여부
- **새로 만들기**를 눌러 새 암호 정책을 작성할 수 있습니다.
- 목록에서 정책을 선택하고 **변경**을 눌러 기존 암호 정책의 특성을 변경할 수 있습니다.
- 목록에서 정책을 선택하고 **삭제**를 눌러 기존 암호 정책을 삭제할 수 있습니다.

새 암호 정책을 작성하려면 다음을 수행하십시오.

1. WebSphere Commerce 관리 콘솔을 여십시오.
2. 관리 콘솔의 보안 드롭 다운 메뉴에서 **암호 정책**을 누르십시오.
3. 암호 정책 페이지에서 **새로 만들기**를 눌러 새 암호 정책을 작성하십시오.
4. 이름 필드에 암호 정책에 대한 이름을 입력하십시오(예: `my_password_policy`).
5. 필요한 대로 다음을 갱신하여 구매자에 대한 기본값에서 임의의 값을 수정하십시오.
   - **사용자 ID와 암호가 동일할 수 있습니까?** 사용자 ID와 암호가 동일할 수 있는지 여부를 정의합니다. 목록에서 예 또는 아니오를 선택하십시오.

- **최대 연속 문자 유형**. 암호에서 연속 문자의 최대 발생을 정의합니다. 최소값은 두 개의 연속 문자입니다. 예를 들어, 값 2를 사용할 때 aaabc 같은 암호를 입력할 수 없습니다.
- 모든 문자의 **최대 인스턴스 수**. 동일한 문자가 한 암호에 나타날 수 있는 최대 횟수를 정의합니다. 최소값은 한 문자의 1 인스턴스입니다. 예를 들어, 값 2를 사용하면 abcaabc 같은 암호를 입력할 수 없습니다.
- **암호의 최대 기간.** 암호가 존재할 수 있는 최대 시간을 일 단위로 정의합니다. 최소값은 1일입니다. 이 기간 후에는 사용자에게 암호를 변경하라는 프롬프트가 표시됩니다.
- **최소 영문자 수**. 암호에 사용되는 최소 영문자 수를 정의합니다. 최소값은 0개의 영문자입니다.
- **최소 숫자 수**. 암호에 사용되는 최소 숫자 수를 정의합니다. 최소값은 0개의 숫자입니다.
- **최소 암호 길이**. 암호의 가장 작은 길이를 문자 단위로 정의합니다. 최소값은 1개의 문자입니다.
- **암호를 재사용할 수 있습니까?** 사용자의 이전 암호를 재사용할 수 있는지 여부를 정의합니다. 목록에서 예 또는 아니오를 선택하십시오.

6. **확인**을 누르십시오.

주:

1. 암호 정책을 사용 중인 경우(즉, 사용자에게 해당 암호 정책이 지정된 경우)에는 암호 정책을 삭제할 수 없습니다.
2. 암호 정책은 사용자가 WebSphere Commerce 데이터베이스에 대해 인증되는 경우에만 강제 시행됩니다.

추가 정보에 대해 71 페이지의 『기본 인증 정책』도 참조하십시오.

계정 잠금 정책 설정

WebSphere Commerce 관리 콘솔의 계정 잠금 정책 페이지를 사용하여 WebSphere Commerce의 다른 사용자 역할에 대한 계정 잠금 정책을 설정할 수 있습니다. 이 페이지는 기본적으로 WebSphere Commerce에 제공되는 모든 사전 정의된 정책을 포함하여 모든 기존 계정 잠금 정책을 표시합니다. 계정 잠금 정책은 사용자 계정에 대해 잘못된 조치가 실행되는 경우, 조치가 계정을 손상시키는 기회를 줄이기 위해 해당 계정을 사용 불가능하게 만듭니다.

계정 잠금 정책은 다음 항목을 강제 시행합니다.

- 계정 잠금 임계값. 이것은 계정이 사용되기 전의 올바르지 않은 로그온 시도 횟수입니다.

- 이것은 두 번의 로그인 시도 실패 후에 사용자가 로그인할 수 없는 기간입니다. 연속으로 로그인에 실패할 때마다 지연이 구성된 시간 지연 값(예: 10초)만큼 증가됩니다.

계정 잠금 정책을 설정하려면 다음을 수행하십시오.

1. WebSphere Commerce 관리 콘솔을 여십시오.
2. 관리 콘솔의 보안 드롭 다운 메뉴에서 **계정 잠금 정책**을 누르십시오.
3. 계정 잠금 정책 페이지가 모든 기존 계정 잠금 정책을 표시합니다. 이 페이지에서
   - **새로 만들기**를 눌러 새 정책을 작성할 수 있습니다.
   - 목록에서 정책을 선택하고 **변경**을 눌러 기존 정책의 특성을 변경할 수 있습니다.
   - 목록에서 정책을 선택하고 **삭제**를 눌러 기존 정책을 삭제할 수 있습니다.

새 계정 잠금 정책의 경우, 계정 잠금 정책 페이지에서

1. 이름 필드에 계정 잠금 정책에 대한 이름을 입력하십시오(예: `my_policy`).
2. 계정 잠금 임계값 필드에 계정 잠금 임계값을 입력하십시오. 예를 들어, 6(여섯 번의 시도의 경우)을 입력하십시오.
3. 대기 시간 필드에 연속 실패 로그인 지연을 초 단위로 입력하십시오. 예를 들어, 10(10초의 경우)을 입력하십시오.
4. **확인**을 누르십시오.

주:

1. 계정 잠금 정책을 사용 중인 경우(즉, 사용자에게 계정 잠금 정책이 지정된 경우)에는 해당 계정 잠금 정책을 삭제할 수 없습니다.
2. 계정 잠금 정책은 사용자가 WebSphere Commerce 데이터베이스에 대해 인증되는 경우에만 강제 시행됩니다.

보안 확인 실행

400 이 기능은 iSeries용 WebSphere Commerce에는 적용되지 않습니다.

WebSphere Commerce 관리 콘솔의 보안 확인 실행 페이지를 사용하여 가능한 보안 노출을 포함할 수 있는 임시 WebSphere Commerce 파일을 확인하고 삭제하는 보안 프로그램을 수동으로 실행할 수 있습니다. 일반적으로 보안 확인 프로그램은 계획된 작업으로 실행하며 기본적으로 한 달에 한 번 실행하도록 설정됩니다.

보안 확인 프로그램을 호출하려면 다음을 수행하십시오.

1. WebSphere Commerce 관리 콘솔을 여십시오.
2. 관리 콘솔의 보안 드롭 다운 메뉴에서 **보안 확인 프로그램**을 누르십시오.
3. 보안 확인 실행 페이지에서 **실행**을 누르십시오.

프로그램에서 취한 모든 조치를 포함한 보안 확인의 결과는 보안 확인 로그 창과 logs 서브디렉토리의 sec_check.log 파일에 기록됩니다.

AIX Linux Solaris WC_installdir/instances/*instance_name*/logs

Windows WC_installdir\instances*instance_name*\logs

Windows Windows가 아닌 플랫폼에서는 권한이 없는 사용자가 중요한 파일에 액세스할 수 없도록 하기 위해 파일 권한이 WebSphere Commerce에 의해 자동으로 설정됩니다. Windows 플랫폼에서는 사용자가 다음과 같이 수동으로 권한을 설정해야 합니다. 이 프로시저는 관리자 그룹만이 중요한 파일에 대해 read/write/execute 권한을 갖도록 보장합니다.

1. Windows 탐색기에서 *drive*:\WebSphere 폴더를 마우스 오른쪽 단추로 누르십시오.
2. **등록 정보**를 누르고 **보안**을 누르십시오. 기본적으로 "Everyone" 그룹은 이 폴더에 대해 **모든** 권한을 갖습니다.
3. **추가**를 누르십시오
4. 창이 표시됩니다(사용자, 컴퓨터 선택...). 이 창에서 **관리자** 그룹을 선택하십시오.

   주: 관리자를 사용자로 볼 수 있으므로 여기에서는 애매모호할 수 있지만 관리자 사용자가 아닌 관리자 그룹을 추가해야 합니다.

   추가를 누른 후 **확인**을 누르십시오.
5. 보안 탭에 관리자 그룹이 추가되었습니다. "Everyone"을 제거해야 합니다. **Everyone**을 선택한 후 "부모로부터 상속 가능한...."이라는 상자의 선택을 취소하십시오.
6. 표시되는 보안 창에서 **제거**를 누르십시오.

구성 관리자 PDI 암호화 필드

WebSphere Commerce 인스턴스를 구성할 때 PDI 암호화 선택란을 선택하는 것이 좋습니다. PDI 암호화 필드를 사용하면 ORDPAYINFO 및 ORDPAYMTHD 테이블의 정보가 암호화됩니다. 선택란을 선택하면 지불 정보가 암호화된 형식으로 WebSphere Commerce 데이터베이스에 저장됩니다.

기본 인증 정책

WebSphere Commerce는 다음 두 가지 기본 인증 정책을 제공합니다.

- 72 페이지의 『구매자』
- 72 페이지의 『운영자』

구매자

구매자에 대한 기본 계정 정책은 구매자에 대한 기본 계정 잠금 정책과 기본 암호 정책을 포함합니다.

구매자에 대한 기본 계정 잠금 정책은 다음 기본 속성을 포함합니다.

속성	기본값
계정 잠금 임계값	6번 시도
연속 실패 로그인 지연	10초

구매자에 대한 기본 암호 정책은 다음 기본 속성을 포함합니다.

속성	기본값
사용자 ID와 암호가 일치할 수 있는지 여부	N(일치할 수 없음)
연속 문자의 최대 발생	3 문자
최대 인스턴스 수	4 인스턴스
암호의 최대 기간	180일
최소 영문자 수	1 영문자
최소 숫자 수	1 수치 문자
최소 암호 길이	6 문자
사용자 이전 암호의 재사용 가능 여부	N(재사용할 수 없음)

자체등록을 수행하는 구매자는 기본 구매자 인증 정책인 구매자가 지정됩니다.

운영자

운영자에 대한 기본 계정 정책은 운영자에 대한 기본 계정 잠금 정책과 기본 암호 정책을 포함합니다.

운영자에 대한 기본 계정 잠금 정책은 다음 기본 속성을 포함합니다.

속성	기본값
계정 잠금 임계값	3번 시도
연속 실패 로그인 지연	20초

구매자에 대한 기본 암호 정책은 다음 기본 속성을 포함합니다.

속성	기본값
사용자 ID와 암호가 일치할 수 있는지 여부	N(일치할 수 없음)
연속 문자의 최대 발생	3 문자
최대 인스턴스 수	4 인스턴스
암호의 최대 기간	90일
최소 영문자 수	1 영문자
최소 숫자 수	1 수치 문자

속성	기본값
최소 암호 길이	8 문자
사용자 이전 암호의 재사용 가능 여부	N(재사용할 수 없음)

WebSphere Commerce와 함께 제공되는 기본 wcsadmin 운영자 사용자에는 기본 인증 정책인 Administrators가 지정됩니다.

제 5 장 세션 관리

웹 브라우저와 전자상거래 사이트는 HTTP를 사용하여 통신합니다. HTTP가 stateless 프로토콜이기 때문에(각 명령이 이전의 명령에 대해 어떤 지식도 없이 독립적으로 실행됨을 의미) 브라우저측과 서버측 사이에 세션을 관리할 방법이 있어야 합니다.

WebSphere Commerce는 *쿠키 기반* 및 URL 재작성의 두 유형의 세션 관리를 지원합니다. 운영자는 *쿠키 기반* 세션 관리만을 지원하거나 *쿠키 기반* 및 URL 재작성 세션 관리를 모두 지원하도록 선택할 수 있습니다. WebSphere Commerce가 *쿠키 기반*만을 지원하는 경우, 구매자의 브라우저가 *쿠키*를 승인할 수 있어야 합니다. *쿠키 기반* 및 URL 재작성이 둘다 선택되는 경우, WebSphere Commerce는 먼저 *쿠키*를 사용하여 세션을 관리하려 시도합니다. 구매자의 브라우저가 *쿠키*를 승인하지 않도록 설정되는 경우 URL 재작성이 사용됩니다.

쿠키 기반 세션 관리

쿠키 기반 세션 관리가 사용될 때 사용자의 정보가 들어 있는 메시지(*쿠키*)가 웹 서버에 의해 브라우저로 보내집니다. 이 *쿠키*는 사용자가 특정 페이지에 액세스하려고 시도할 때 다시 서버로 보내집니다. *쿠키*를 다시 보내면 서버는 사용자를 식별하고 세션 데이터베이스에서 사용자의 세션을 검색할 수 있으므로 사용자의 세션을 관리합니다. *쿠키 기반* 세션은 사용자가 로그오프하거나 브라우저를 닫을 때 종료합니다. *쿠키 기반* 세션 관리는 안전하며 성능상의 이점을 갖습니다. *쿠키 기반* 세션 관리는 SSL를 통해서만 이동하는 식별 태그를 사용하므로 안전합니다. WebSphere Commerce 캐시 메커니즘이 *쿠키 기반* 세션만을 지원하고 URL 재작성을 지원하지 않기 때문에 *쿠키 기반* 세션 관리가 상당한 성능상의 이점을 제공합니다. *쿠키 기반* 세션 관리가 구매자 세션에 권장됩니다.

URL 재작성을 사용하지 않고 사용자가 자신의 브라우저에서 *쿠키*를 사용하게 하려는 경우, 구성 관리자의 세션 관리 페이지에서 **쿠키 수용 테스트**를 선택하십시오. 이것은 구매자에게 브라우저가 *쿠키*를 지원하지 않는 경우 또는 *쿠키*를 끈 경우 WebSphere Commerce 사이트를 보려면 *쿠키*를 지원하는 브라우저가 필요함을 알려줍니다.

보안상의 이유로 *쿠키 기반* 세션 관리는 다음 두 유형의 *쿠키*를 사용합니다.

- 비보안 세션 *쿠키*

  세션 데이터를 관리하는 데 사용됩니다. 세션 ID, 협상된 언어, 현재 상점 및 *쿠키*가 구성될 때의 구매자 선호 통화가 들어 있습니다. 이 *쿠키*는 SSL 또는 비SSL 연결을 통해 브라우저와 서버 사이에 이동할 수 있습니다. 비보안 세션 *쿠키*에는 다음 두 유형이 있습니다.

– WebSphere Application Server 세션 쿠키는 Servlet HTTP 세션 표준을 바탕으로 합니다. WebSphere Application Server 쿠키는 다중노드 전개에서 메모리 또는 데이터베이스에 지속됩니다. 추가 정보에 대해서는 WebSphere Application Server Information Center(http://www.ibm.com/software/webservers/appserv/infocenter.html)에서 "세션 관리"를 검색하십시오.

– WebSphere Commerce 세션 쿠키는 WebSphere Commerce에 대해 내부적이며 데이터베이스에 지속되지 않습니다.

사용할 쿠키 유형을 선택하려면 구성 관리자의 세션 관리 페이지에 있는 **쿠키 세션 관리자** 매개변수에 대해 WCS 또는 WAS를 선택하십시오.

- 보안 인증 쿠키

  인증 데이터를 관리하는 데 사용됩니다. 인증 쿠키는 SSL을 통해 이동하며 최대 보안을 위해 시간소인이 붙습니다. 이것은 사용자를 인증하는 데 사용되는 쿠키이지만, 중요한 명령, 예를 들어, 사용자에게 신용 카드 번호를 묻는 DoPaymentCmd가 실행됩니다. 이 쿠키가 도난되어 권한이 없는 사용자에 의해 사용될 수 있는 아주 작은 위험이 있습니다. 쿠키 기반 세션 관리가 사용될 때마다 항상 WebSphere Commerce에 의해 인증 코드 쿠키가 작성됩니다.

세션 및 인증 코드 쿠키가 모두 보안 페이지를 보기 위해 필요합니다.

쿠키 오류에 대해 CookieErrorView가 다음 경우에 호출됩니다.

- 사용자가 동일한 로그온 ID를 갖고 다른 위치에서 로그인했습니다.
- 쿠키가 손상되었거나 부당하게 변경되었습니다.
- 쿠키 승인이 『TRUE』로 설정되고 사용자의 브라우저가 쿠키를 지원하지 않습니다.

세션 관리를 위한 쿠키 사용

WebSphere Commerce에서 쿠키를 사용하려면, 다음을 수행하십시오.

1. 구성 관리자를 여십시오.
2. **인스턴스**를 선택한 후 **세션 관리** 폴더를 여십시오.
3. 적절한 세션 값을 선택하십시오.
   - 쿠키 수용 테스트

     쿠키만을 지원하는 사이트의 경우 고객의 브라우저가 쿠키를 수용하는지 확인하려면 이 선택란을 선택하십시오.
   - 쿠키 세션 관리자

     쿠키를 관리하기 위해 사용자가 WebSphere Commerce 또는 WebSphere Application Server를 원하는지 여부를 선택하십시오. 기본값은 WebSphere Commerce입니다.

     – WebSphere Application Server 세션 쿠키는 Servlet HTTP 세션 표준을 바탕으로 합니다. WebSphere Application Server 쿠키는 다중노드 전개에서 메

모리 또는 데이터베이스에 지속됩니다. 자세한 정보에 대해서는 WebSphere Application Server Information Center(http://www.ibm.com/software/webservers/appserv/infocenter.html)에서 "세션 관리"를 검색하십시오.

- WebSphere Commerce 세션 쿠키는 WebSphere Commerce에 대해 내부적이므로 데이터베이스로 지속되지 않습니다.

4. **고급** 탭을 누르십시오. 적절한 세션 값을 선택하십시오.
   - 쿠키 경로

     쿠키가 보내질 URL의 서브세트인 쿠키에 대한 경로를 지정합니다. 대개 이 필드는 수정하지 않아야 합니다.

     쿠키 경로에 대한 정보는 Netscape의 쿠키 스펙 및 RFC 2109를 참조하십시오.
   - 쿠키 도메인

     도메인 제한 패턴을 지정합니다. 대개 이 필드는 수정하지 않아야 합니다.

     도메인은 쿠키를 볼 서버를 지정합니다. 기본적으로 쿠키는 해당 쿠키를 발행한 WebSphere Commerce Server로만 다시 보내집니다. 기본적으로 쿠키는 쿠키를 저장한 호스트에만 리턴됩니다. 도메인 이름 패턴을 지정하면 이것이 대체됩니다. 패턴은 점으로 시작하고 최소한 두 개의 점을 포함해야 합니다. 패턴은 초기 점 이후의 한 항목만을 일치시킵니다. 예를 들어 『.ibm.com』은 올바르며 『a.ibm.com』 및 『b.ibm.com』과는 일치하지만 『www.a.ibm.com』과는 일치하지 않습니다. 도메인 패턴에 대한 자세한 내용은 Netscape의 쿠키 스펙 및 RFC 2109를 참조하십시오.
5. **적용**을 누르십시오.
6. 구성 관리자를 닫으십시오.
7. WebSphere Application Server 관리 콘솔에서 WebSphere Commerce 서버 인스턴스를 중지한 후 다시 시작하십시오.

URL 재작성

URL 재작성을 사용할 때 브라우저로 리턴되거나 경로 재지정된 모든 링크에 세션 ID가 추가됩니다. 사용자가 이들 링크를 누를 때 URL의 재작성된 양식이 클라이언트 요청의 일부로 서버에 보내집니다. Servlet 엔진이 URL에 있는 세션 ID를 인식하고 이 사용자에 대한 적합한 오브젝트를 얻기 위해 세션 ID를 저장합니다. URL 재작성을 사용하려면 링크에 HTML 파일(.html 또는 .htm 확장자를 가진 파일)을 사용할 수 없습니다. URL 재작성을 사용하려면 표시 목적을 위해 JSP 파일을 사용해야 합니다. URL 재작성을 갖는 세션은 구매자가 로그오프할 때 만기됩니다.

주: WebSphere Commerce 동적 캐시 및 URL 재작성은 함께 사용할 수 없습니다. URL 재작성이 켜져 있을 때는 WebSphere Commerce 동적 캐시를 사용하지 않아야 합니다. 자세한 정보는 *WebSphere Commerce 관리 안내서*의 동적 캐시에 관한 장을 참조하십시오.

URL 재작성 세션 관리 사용

세션이 관리되는 방법을 지정하려면 다음을 수행하십시오.

1. 구성 관리자를 여십시오.
2. **인스턴스**를 선택한 후 **세션 관리** 폴더를 여십시오.
3. 적절한 세션 값을 선택하십시오.

   URL 재작성 사용. 세션 관리에 URL 재작성을 사용하려면 이 선택란을 선택하십시오.

   쿠키 세션 관리자. WebSphere Application Server를 선택하십시오.
4. **적용**을 누르십시오.
5. 구성 관리자를 닫으십시오.
6. WebSphere Application Server 관리 콘솔에서 WebSphere Commerce 서버 인스턴스를 중지한 후 다시 시작하십시오.

URL 재작성을 위한 JSP 템플리트 작성

URL 재작성을 사용하여 세션 상태를 유지보수하려는 경우 일반 HTML 파일에 웹 응용프로그램의 일부에 대한 링크를 포함하지 마십시오. 이러한 제한은 URL 인코딩이 일반 HTML 파일에서 사용될 수 없기 때문에 필요합니다. URL 재작성을 사용하여 상태를 유지보수하려면 사용자가 세션 중에 요청하는 모든 페이지에는 Java 해석기가 이해할 수 있는 코드가 있어야 합니다. 사용자가 세션 중에 액세스할 수 있는 사이트 일부와 웹 응용프로그램에 일반 HTML 파일이 있는 경우 JSP 파일로 변환하십시오. 이것은 쿠키를 사용하여 세션을 유지보수하는 것과는 달리 URL 재작성을 사용한 세션 유지보수에서는 응용프로그램의 각 JSP 템플리트가 `<A>` 태그의 모든 `HREF` 속성에 대해 URL 인코딩을 사용해야 하기 때문에 응용프로그램 작성자에게 영향을 주게 됩니다. 응용프로그램에 있는 하나 이상의 JSP 템플리트가 `encodeURL(String url)`을 호출하지 않거나 `RedirectURL(String url)` 메소드를 인코드하지 않는 경우에는 세션이 유실됩니다.

링크 작성

URL 재작성을 사용할 때 사용자가 브라우저로 리턴하거나 경로 재지정하는 모든 링크에 세션 ID가 추가되어야 합니다. 예를 들어, 웹 페이지에 있는 다음 링크는

```
<a href="store/catalog">
```

아래와 같이 재작성됩니다.

```
<a href="store/catalog;$jsessionid$DA32242SSGE2">
```

사용자가 이 링크를 누를 때 재작성된 URL 양식이 클라이언트 요청의 일부로 서버에 보내집니다. Servlet 엔진은 ;$jsessionid$DA32242SSGE2를 세션 ID로 인식하고 이 사용자에 대한 적합한 HttpSession 오브젝트를 얻기 위해 저장합니다.

다음 예에서는 Java 코드가 JSP 파일 안에 임베드되는 방법을 보여줍니다.

```
<%
 response.encodeURL ("/store/catalog");
%>
```

브라우저로 리턴할 URL을 재작성하려면 출력 스트림에 URL을 보내기 전에 JSP 템플리트에서 encodeURL() 메소드를 호출하십시오. 예를 들어, URL 재작성을 사용하지 않는 JSP 템플리트가 다음을 갖는 경우,

```
out.println("<a href=\"/store/catalog\">catalog</a>")"
```

아래 코드로 바꾸십시오.

```
out.println("<a href=\"");
out.println(response.encodeURL ("/store/catalog"));
out.println("\">catalog</a>");
```

경로 재지정할 URL을 재작성하려면 encodeRedirctURL() 메소드를 호출하십시오. 예를 들어, JSP 템플리트가 다음과 같을 경우입니다.

```
response.sendRedirect(response.encodeRedirectURL
("http://myhost/store/catalog"));
```

encodeURL() 및 encodeRedirectURL() 메소드는 HttpServletResponse 오브젝트의 일부입니다. 두 경우 모두에서 이들 호출은 URL을 인코딩하기 전에 URL 재작성이 구성되었는지 확인합니다. 구성되지 않은 경우, 원래 URL을 리턴합니다.

양식 작성: 제출을 위한 양식을 작성하려면 양식 템플리트의 ACTION 태그에서 response.encodeURL("Logon");을 호출하십시오. 예를 들면, 다음과 같습니다.

```
String strLoginPost = response.encodeURL("Logon");
<FORM NAME="Logon" METHOD="post" ACTION= <%= strLoginPost %> >
...
</FORM>
```

첫 번째 페이지 작성: 대개 홈페이지의 시작 페이지는 프레임이 없습니다. 상점에서 프레임을 사용하려는 경우, 상점에 대한 링크를 갖는 비프레임 페이지가 상점의 시작 페이지로 작용하도록 할 수 있습니다. 그러나 상점이 프레임을 사용하고 고객이 먼저 시작 페이지를 통하지 않고 프레임을 갖는 페이지에 액세스하려는 경우, 고객의 세션이 유실될 수 있습니다. 고객들은 또한 **이전** 버튼을 사용하여(프레임을 갖는 경우에만) 시작 페이지로 리턴하고 시작 페이지를 최신 정보로 고치는 경우에는 세션을 유실할 수 있습니다. 시작 페이지를 최신 정보로 고치면 고객에게 새 세션 ID가 부여됩니다. **이전** 버튼의 대안으로 시작 페이지로 돌아가기 링크가 이런 유형의 세션 유실을 막기 위해 필요합니다.

상점 레벨 세션 관리

아래 도표는 WebSphere Commerce 상점 레벨 등록 인프라를 보여줍니다. 상점 레벨 등록은 액세스 제어 역할을 사용하여 구매자를 상점과 연관시킵니다.

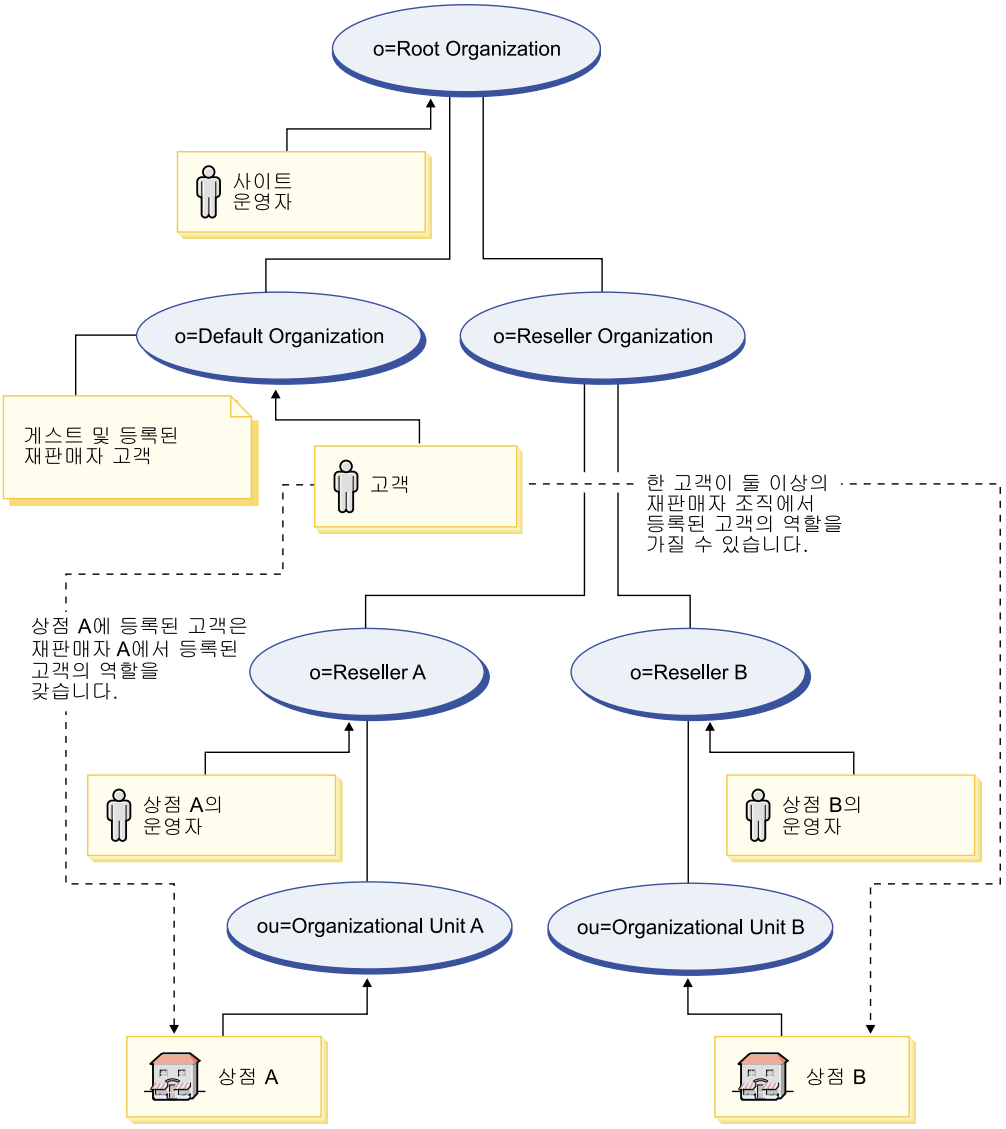


그림 3. 상점 레벨 등록

상점에서 구매하는 사용자가 반드시 상점 조직의 구성원일 필요는 없지만 해당 조직에서 구매 역할(즉, 등록 고객)을 수행할 필요가 있습니다. 조직에서 관리 역할을 수행하는 사용자는 대개 조직과의 상위 관계를 가짐으로써 조직과 연관됩니다.

예를 들어, 위의 도표에서 상점 A를 갖는다고 가정합시다. 또한, Sue는 상점 A에서 구매하며 Joe는 상점 A를 관리해야 할 상점 A의 직원이라고 가정합시다. 조직 측면에서 이 시나리오를 모델화하기 위해, Joe는 상점 A의 조직에 포함되어야 하나 Sue는 포함

되지 않아야 합니다. Sue는 상점 A의 직원이 아니므로, Sue는 상점 A의 조직에서 구매 역할을 수행하게 하여 상점 A와 연관됩니다.

상점은 상점의 조직에서 구매 역할을 수행하는 모든 사용자를 찾아서 모든 등록된 구매자를 판별합니다. 그러면 상점의 사용자 운영자가 상점의 모든 등록 사용자에 대한 캠페인 설정 같은 상점 전체의 활동이나 상점에 등록된 사용자의 암호 재설정 같은 특정 조치를 계속 수행할 수 있습니다.

80 페이지의 그림 3의 도표를 참조하여 다음 시나리오를 고려하십시오.

- 기본 조직의 구성원인 Sue는 재판매자 A의 조직에서 구매 역할을 수행합니다. 재판매자 A의 상위 조직은 재판매자 조직입니다.
- 재판매자 A는 상점 A를 소유합니다.
- Sue에게는 재판매자 B의 조직에서 조직 역할이 없습니다.
- 재판매자 B는 상점 B를 소유합니다.

Sue가 상점 A에 로그인하여 평소와 같이 구매합니다. Sue가 상점 B에 액세스할 때, Sue에게는 게스트 사용자로서 상점 B에 대한 새 세션 동일성이 지정됩니다. Sue가 다시 한 번 상점 A에 액세스하는 경우, WebSphere Commerce에서는 상점 A에 대한 이전 세션 동일성 정보를 사용하여 그녀의 세션을 관리합니다.

다음과 같은 경우 상점 A의 세션 동일성이 상점 B에 재사용됩니다.

- 상점 A와 상점 B가 동일한 조직에 속합니다.
- Sue에게 재판매자 A와 재판매자 B 조직 둘 모두에 정의된 역할이 있습니다.

제 6 장 암호 설정 및 변경

대부분의 WebSphere Commerce 구성요소는 운영체제에 의해 유효성이 검증된 사용자 ID 및 암호를 이용합니다. 암호 변경에 대한 자세한 내용은 운영체제 문서를 참조하십시오. 이 장에서는 운영체제를 통해 사용자 ID 및 암호의 유효성을 검증하지 않는 WebSphere Commerce 구성요소를 위해 암호를 설정 및 변경하는 방법을 다룹니다.

사용자 ID, 암호 및 웹 주소에 대한 빠른 참조

WebSphere Commerce 환경 관리에는 다양한 사용자 ID가 필요합니다. 이들 사용자 ID가 필수 권한과 함께 아래 목록에 설명되어 있습니다. WebSphere Commerce 사용자 ID인 경우에는 기본 암호가 식별됩니다.

400 **iSeries 사용자 프로파일**

두 개의 iSeries 사용자 프로파일이 WebSphere Commerce를 설치 및 구성할 때 자주 사용되고 참조됩니다.

- 사용자가 WebSphere Commerce를 설치하고 구성 관리자를 시작하기 위해 작성하여 사용하는 프로파일. WebSphere Commerce를 설치 및 구성하려면 USRCLS(*SECOFR)의 iSeries 사용자 프로파일을 사용하거나 QSECOFR 사용자 프로파일을 사용해야 합니다. 사용자 프로파일을 작성해야 하는 경우 iSeries용 *WebSphere Commerce 설치 안내서*를 참조하십시오.
- WebSphere Commerce 인스턴스를 작성할 때 구성 관리자가 작성하는 사용자 프로파일. 이 사용자 프로파일은 또한 *인스턴스 사용자 프로파일*이라고도 합니다. USRCLS(*USER)의 사용자 프로파일은 WebSphere Commerce 인스턴스를 작성할 때마다 구성 관리자에 의해 작성됩니다. 사용자 프로파일을 작성해야 하는 경우 iSeries용 *WebSphere Commerce 설치 안내서*를 참조하십시오.

구성 관리자 사용자 ID

구성 관리자 도구의 그래픽 인터페이스를 사용하여 WebSphere Commerce 구성 방법을 수정할 수 있습니다. 기본 구성 관리자 사용자 ID 및 암호는 webadmin과 webibm입니다.

AIX Linux Solaris Windows WebSphere Commerce 시스템 또는 WebSphere Commerce와 동일한 네트워크의 임의의 시스템에서 구성 관리자에 액세스할 수 있습니다.

400 iSeries의 경우 iSeries 서버와 동일한 네트워크에 있는 Windows 시스템에서 구성 관리자에 액세스할 수 있습니다.

IBM HTTP Server 사용자 ID

AIX Linux Solaris Windows IBM HTTP Server를 사용 중인 경우, 웹 브라우저를 열고 다음 웹 주소를 입력하여 웹 서버 홈 페이지에 액세스할 수 있습니다.

```
http://host_name
```

웹 서버를 사용자 정의한 경우, 호스트 이름 뒤에 웹 서버의 첫 페이지 이름을 입력할 수도 있습니다.

WebSphere Commerce 인스턴스 운영자

인스턴스 운영자 사용자 ID와 암호가 다음 WebSphere Commerce 도구에 적용됩니다.

- WebSphere Commerce 액셀러레이터. Windows 운영체제를 실행하는 원격 시스템으로부터 WebSphere Commerce 액셀러레이터에 액세스하려면 Internet Explorer 웹 브라우저를 열고 다음 웹 주소를 입력하십시오.

  ```
  https://host_name:8000/accelerator
  ```

- WebSphere Commerce 관리 콘솔. Windows 운영체제를 실행 중인 원격 시스템에서 WebSphere Commerce 관리 콘솔에 액세스하려면, Internet Explorer 웹 브라우저를 열고 다음 웹 주소를 입력하십시오.

  ```
  https://host_name:8002/adminconsole
  ```

- WebSphere Commerce 조직 관리 콘솔. Windows 운영체제를 실행 중인 원격 시스템에서 WebSphere Commerce 조직 관리 콘솔에 액세스하려면, Internet Explorer 웹 브라우저를 열고 다음 웹 주소를 입력하십시오.

  ```
  https://host_name:8004/orgadminconsole
  ```

위의 도구의 경우, WebSphere Commerce 인스턴스 작성 시 입력한 운영자 사용자 ID 및 암호를 입력하십시오.

주: 사이트 운영자 사용자 ID는 절대 제거해서는 안되며 항상 인스턴스 운영자 권한을 갖고 있어야 합니다.

WebSphere Commerce는 사용자 ID와 암호가 다음 규칙을 따를 것을 요구합니다.

- 암호의 길이가 최소한 8자여야 합니다.
- 암호는 최소한 하나의 숫자를 포함해야 합니다.
- 암호가 한 문자를 다섯 번 이상 포함하지 않습니다.
- 암호가 동일한 문자를 네 번 이상 연속해서 반복하지 않습니다.

WebSphere Commerce Payments 관리자

WebSphere Commerce Payments를 설치할 때 WebSphere Commerce 사이트 운영자 ID에 자동으로 지불 관리자 역할이 지정됩니다. 아직 수행하지 않은 경우 지불 범주 클래스를 WCSRealm으로 전환하려면 *WebSphere Commerce 설치 안내서*의 지시사항을 따르십시오.

지불 관리자 역할은 사용자 ID가 WebSphere Commerce Payments를 제어하고 관리할 수 있게 합니다.

400 **주:**

- WebSphere Commerce Payments 통합과 관련된 WebSphere Commerce 기능이 작동하지 않기 때문에 사용자 인스턴스에 대해 작성된 사이트 운영자 사용자 ID를 삭제하거나 이름을 바꾸지 말고 사전 지정된 WebSphere Commerce Payments 역할도 변경하지 마십시오.

Windows **Windows 사용자 ID**

Windows 사용자 ID는 관리자 권한을 갖고 *있어야* 합니다. DB2®를 사용 중인 경우, 사용자 ID와 암호가 다음 규칙을 따라야 합니다.

- 8자를 초과할 수 없습니다.
- A - Z, a - z, 0 - 9, @, #, $ 및 _ 문자만 포함할 수 있습니다.
- 밑줄(_)로 시작할 수 없습니다.
- 사용자 ID는 대문자, 소문자 또는 대소문자 혼합의 USERS, ADMINS, GUESTS, PUBLIC, LOCAL을 사용할 수 없습니다.
- 사용자 ID는 대문자, 소문자 또는 대소문자 혼합의 IBM, SQL, SYS로 시작할 수 없습니다.
- 사용자 ID는 Windows 서비스 이름과 같을 수 없습니다.
- 사용자 ID는 로컬 시스템에서 정의되어야 하며 로컬 운영자 그룹에 속해 있어야 합니다.
- 사용자 ID는 *운영체제의 일부로 활동*이라는 고급 사용자 권한을 갖고 있어야 합니다.

*운영체제의 일부로 활동*이라는 고급 사용자 권한이 없이 설치를 수행할 수 있지만 DB2 설치 프로그램이 사용자가 관리 서버에 대해 지정하는 계정의 유효성을 검증할 수 없습니다. DB2를 설치하는 데 사용되는 모든 사용자 계정에 이 고급 사용자 권한이 있는 것이 바람직합니다.

중요

Windows 사용자 ID가 관리자 권한을 갖지 *않거나* 8자를 초과하거나 로컬 시스템에 정의되지 않은 경우, 해당 문제점이 사용자에게 통지되며 사용자는 설치를 계속할 수 없습니다.

DB2를 사용 중인 경우, 이 사용자 ID를 DB2 데이터베이스 사용자 이름(데이터베이스 사용자 로그온 ID)으로 사용합니다.

위의 기준에 맞는 사용자 ID를 작성해야 하는 경우, Windows 온라인 도움말에서 Windows 사용자 ID 작성에 대한 정보를 찾을 수 있습니다.

구성 관리자 암호 변경

구성 관리자를 실행할 때 사용자 ID와 암호를 입력하는 창에서 **수정**을 눌러 구성 관리자 암호를 변경할 수 있습니다.

또는, 구성 관리자 사용자 ID 또는 암호를 변경하려면, WebSphere Commerce 설치 경로의 `bin` 서브디렉토리로 전환한 후 명령 창에 다음을 입력하십시오.

1. WebSphere Commerce `bin` 서브디렉토리로 변경하십시오.

   ```
   cd  WC55_installdir/bin
   ```

2. `wcs_encrypt` 스크립트를 실행하여 사용자 암호의 암호화 버전을 구하십시오.

   AIX 400 Linux Solaris

   ```
   ./wcs_encrypt.sh new_password
   ```

   Windows

   ```
   wcs_encrypt new_password
   ```

3. *WC55_installdir*`/instances` 디렉토리에서 `PwdMgr.xml` 파일을 열고 2단계에서 암호화한 암호로 LoginPassword를 수정하십시오.

IBM HTTP Server 운영자 암호 설정

AIX Linux Solaris Windows IBM HTTP Server 관리자 암호를 설정하려면, 다음을 수행하십시오.

1. 시스템에서 *HTTPServer_installdir*`/bin` 디렉토리로 변경하십시오.
2. 다음 명령을 입력하십시오.

AIX Linux Solaris `./htpasswd -b ../conf/admin.passwd user password`

Windows `htpasswd -b conf\admin.passwd user password` 여기서 *user* 및 *password*는 IBM HTTP Server에 대한 관리자 권한을 갖기 원하는 사용자 ID와 암호입니다.

이제 IBM HTTP Server 관리 암호가 설정되었습니다.

주: 운영자 암호가 없는 경우, 먼저 -c 옵션을 지정한 `htpassword` 명령을 실행하여 암호를 작성해야 합니다.

SSL 키 파일 암호 변경

AIX Linux Solaris Windows IBM HTTP Server를 사용 중인 경우, 아래 단계에 따라서 SSL 키 파일 암호를 변경하십시오.

1. Windows **시작 메뉴 → 프로그램 → IBM HTTP Server → 키 관리 유틸리티 시작**을 누르십시오.
2. **키 데이터베이스 파일** 메뉴에서 **열기**를 선택하십시오.
3. 시스템의 IBM HTTP Server 설치 경로에 있는 `ssl` 서브디렉토리로 전환하십시오. 키 파일(파일 확장자 `.kdb`)이 이 폴더에 있어야 합니다. 그렇지 않으면 211 페이지의 제 17 장 『IBM HTTP Server를 사용한 프로덕션을 위한 SSL 사용』에 설명된 지시사항에 따라서 새 키 파일을 작성하십시오.
4. **키 데이터베이스 파일** 메뉴에서 **암호 변경**을 선택하십시오. 암호 변경 창이 나타납니다.
5. 새 암호를 입력하고 **파일에 암호 저장**을 사용하십시오.
6. **확인**을 누르십시오. 암호가 변경되었습니다.

이제 SSL 키 파일 관리 암호가 성공적으로 변경되었습니다.

WebSphere Commerce 암호 작성

명령행에서 사용자의 암호를 수동으로 재설정하기 위해 암호를 작성할 수 있습니다. 동일한 태스크를 실행하는 다른 도구(예: ResetPassword 명령)가 있습니다. 암호를 수동으로 재설정하기 위해 운영자는 아래 유틸리티의 출력인 암호를 가져와 `USERREG` 테이블의 `LOGONPASSWORD` 필드를 갱신합니다. 운영자는 선택한 salt로 `USERREG`의 `SALT` 필드를 갱신하기도 합니다.

AIX Linux Solaris Windows WebSphere Commerce를 사용하면 암호를 작성할 수 있습니다. 암호를 작성하려면 다음을 수행하십시오.

1. WebSphere Commerce 설치 디렉토리의 bin 서브디렉토리로 이동하십시오.
2. 명령행에서 다음 스크립트를 실행하십시오.

   Windows `wcs_password.bat` *`password SALT merchant_key`*

   AIX Linux Solaris `./wcs_password.sh` *`password SALT merchant_key`*

   여기서,

   - *password*는 일반 텍스트 암호입니다.
   - *SALT*는 암호 작성에 사용되는 임의의 문자열입니다. 이것은 해당 암호가 갱신될 특정 사용자에 대한 USERREG 데이터베이스 테이블의 SALT 열에 있습니다.
   - *merchant_key*는 인스턴스 작성 중에 입력된 판매자 키입니다.

400 iSeries의 경우, 구매자의 암호를 변경하려면 chgwcspwd.sh 명령을 사용하십시오.

1. iSeries 시스템에서 QShell 세션을 시작하십시오.
2. *`WC_installdir`*/bin 디렉토리로 이동하십시오.
3. chgwcspwd.sh 명령행에서 다음 스크립트를 실행하십시오(사용 매개변수가 표시됩니다.)
4. 해당 매개변수를 사용하여 명령을 다시 실행하십시오.

이 명령을 실행하는 자세한 정보는 WebSphere Commerce Production 및 Development 온라인 도움말의 내용을 참조하십시오.

WebSphere Commerce Payments 암호 작성

WebSphere Commerce에서는 WebSphere Commerce Payments에 대한 암호를 작성할 수 있습니다. 암호를 작성하려면 다음을 수행하십시오.

1. WebSphere Commerce 설치 디렉토리의 bin 서브디렉토리로 이동하십시오.
2. 명령행에서 다음 스크립트를 실행하십시오.

   Windows `wcs_pmpassword.bat` *`password SALT`*

   AIX 400 Linux Solaris `./wcs_pmpassword.sh` *`password SALT`*

   여기서

   - *password*는 일반 텍스트 암호입니다.
   - *SALT*는 암호 작성에 사용되는 임의의 문자열입니다. 이것은 해당 암호가 갱신될 특정 사용자에 대한 USERREG 데이터베이스 테이블의 SALT 열에 있습니다.

운영자 계정 재설정

WebSphere Commerce 계정이 어떤 이유로 잠기거나 사용되지 않는 경우, 다음과 같이 잠금을 해제하거나 사용할 수 있습니다.

계정이 사이트 운영자의 계정이 *아닌* 경우, 다음을 수행하십시오.

1. 관리 콘솔을 여십시오.
2. **액세스 관리** > **사용자**를 누르십시오.
3. 사용자 계정을 두 번 누르거나 목록에서 사용자 계정을 선택하고 **변경**을 누르십시오.
4. 계정 상태 필드에서 **사용**을 선택하십시오.
5. **확인**을 누르십시오.

계정이 사이트 운영자의 계정 또는 임의의 다른 사용자 계정*인* 경우, DB2 명령 창이나 SQLPlus 프롬프트(Oracle 데이터베이스의 경우)에서 다음 SQL문을 실행하십시오.

```
CONNECT TO db_name [USER user_id USING password]
UPDATE USERREG SET STATUS=1, PASSWORDRETRIES=0 WHERE LOGONID='logonId'
```

여기서,

db_name
: WebSphere Commerce 데이터베이스 이름(예: MALL)입니다.

user_id
: 데이터베이스에 대한 데이터베이스 관리자 사용자 ID입니다.

password
: 데이터베이스 관리자 사용자 ID에 대응하는 암호입니다.

logonId
: 재설정하려는 계정의 사용자 ID입니다(예: wcsadmin).

예를 들어 wcsadmin 계정을 재설정하려면 데이터베이스 관리자 사용자 ID로서 시스템에 로그온된 경우 다음 SQL 문을 실행할 수 있습니다.

```
CONNECT TO mall
UPDATE USERREG SET STATUS=1, PASSWORDRETRIES=0 WHERE LOGONID='wcsadmin'
```

400 iSeries 플랫폼에서 SQL문을 입력하기 위해 DB2/400 Query Manager 및 SQL 개발 킷을 사용하거나 iSeries Navigator를 사용할 수 있습니다. IBM iSeries Access를 사용하여 데이터베이스 조회를 수행하려면, 다음을 수행하십시오.

1. iSeries Navigator가 설치된 PC에서 이를 시작하십시오.
2. iSeries 시스템을 펼치십시오. 데이터베이스를 펼치고, 관계형 데이터베이스를 마우스 오른쪽 단추로 누르고, **SQL 스크립트 실행**을 선택하십시오. SQL 스크립트 실행 창이 열립니다.

3. 연결 메뉴에서 **JDBC 설치**를 선택하십시오. **서버** 탭을 누르십시오.
4. 기본 라이브러리 필드에서 모든 기존 값을 지우고 사용자 인스턴스의 데이터베이스 스키마의 이름을 입력하십시오. 기본적으로 스키마 이름은 인스턴스의 이름입니다. **확인**을 눌러 변경사항을 저장하십시오.
5. 창에 위의 SQL 문을 입력하십시오.

제 7 장 단일 사인온

이 장에서는 WebSphere Commerce의 단일 사인온 설정 방법을 설명합니다.

전제 조건

단일 사인온을 사용하려면 다음 요구사항을 만족시켜야 합니다.

- 기존 LDAP 서버를 설치하고 구성해야 합니다. LDAP 서버를 구성하려면 *WebSphere Commerce 추가 소프트웨어 안내서*를 참조하십시오.
- LDAP을 사용하려면 WebSphere Commerce가 설치 및 구성되어야 합니다.
- WebSphere Application Server 보안이 사용되어야 합니다. WebSphere Application Server 보안을 사용하려면 199 페이지의 제 16 장 『WebSphere Application Server 보안 사용』을 참조하십시오.

단일 사인온 사용

주의

단일 사인온이 WebSphere Commerce에서 사용될 때 몇 가지 핵심 제한사항이 있습니다. 제한사항은 다음과 같습니다.

- LTPA 쿠키는 다른 웹 서버 포트를 통해 이동할 수 있습니다.
- `ldapentry.xml` 파일을 수정하고 오브젝트 클래스 `ePerson`을 추가할 필요가 있을 수 있습니다. 이것은 `ldapocs` 요소의 속성입니다.
- `instance.xml`을 수정하고 `MigrateUsersFromWCSdb` 플래그가 "켜짐" 상태인지 확인해야 합니다.
- 단일 사인온 구성에 참여하는 시스템은 동기화된 시스템 시계를 가져야 합니다.
- WebSphere Application Server LPTA(Light Weight Third Party Authentication) 토큰을 읽고 발행할 수 있는 응용프로그램간에만 단일 사인온이 지원됩니다.

단일 사인온을 사용하려면 다음을 수행하십시오.

1. WebSphere Application Server 내에서 단일 사인온을 사용하십시오. 추가 정보에 대해서는 WebSphere Application Server 정보 센터(`http://www.ibm.com/software/webservers/appserv/infocenter.html`)에서 "single sign-on"을 검색하십시오. **단일 사인온: WebSphere Application Server**를 선택하고 다음 절을 완료하십시오.

- **WebSphere Application Server에 대한 SSO 구성**
  - **WebSphere Application Server 보안 설정 수정**

    주: LDAP 필드에 값을 입력하는 방법을 설명하는 단계는 무시할 수 있습니다.
  - **LTPA 키를 파일로 반출**

2. WebSphere Commerce 시스템에서 WebSphere Commerce 구성 관리자를 시작하십시오.
3. **구성원 서브시스템** 노드를 구성하려면, 다음을 수행하십시오.
   a. **WebSphere Commerce** 아래에서 *host_name* → **인스턴스 목록** → *instance_name* → **인스턴스 특성** → **구성원 서브시스템**을 펼치십시오.
   b. **인증 모드** 드롭 다운 메뉴에서 **LDAP**을 선택하십시오.
   c. **단일 사인온** 선택란을 사용하십시오.
   d. **호스트** 필드에 LDAP 서버의 완전한 호스트 이름을 입력하십시오.
   e. **운영자 인식 이름** 필드에 운영자의 인식 이름을 입력하십시오. 이것은 LDAP 서버에서 사용된 것과 같은 이름이어야 합니다.
   f. **운영자 암호** 필드에 운영자 암호를 입력하십시오. 이것은 LDAP 서버에서 사용된 것과 같은 암호이어야 합니다. **암호 확인** 필드에서 암호를 확인하십시오.
   g. 나머지 각 필드를 완료하십시오.
   h. **적용**을 누른 다음 **확인**을 누르십시오.
4. 단일 사인온(SSO)에서 시스템에 들어 오는 사용자에게 지정된 역할을 구성하십시오. 사용자가 SSO에 의해 시스템에 연결할 때마다 WebSphere Commerce는 등록 유형 = ″SSO″인 `MemberRegistrationAttributes.xml` 파일에서 역할을 지정하려고 시도합니다. MRA.xml을 설명하는 새 절에 링크하십시오.
5. WebSphere Application Server를 다시 시작하십시오.

SSO 사용자의 역할 구성

WebSphere Commerce 5.5에서 보안 역할이 등록 프로세스의 일부로 지정됩니다. 단일 사인온을 사용하면 고객은 협업 시스템에 인증된 경우 사용자 사이트의 등록 단계를 생략할 수 있습니다. 예를 들어, 상점에서 구매 시 사용자가 사용하려는 기능에 대한 액세스가 거부될 경우 WebSphere Commerce 5.5 사이트에 묵시적으로 인증되는 능력은 매우 작은 값을 갖습니다.

그러므로 사용자 등록에서 발생하는 자동 역할 지정의 동일한 기능이 세션 관리 코드에도 발생합니다. 이 경우 'SSO' 등록 유형을 사용하여 SSO 구매자의 역할을 구성합니다. 고객이 시스템으로 인증할 때 이러한 방식으로 WebSphere Commerce 5.5에서는 자동으로 사이트에 대해 가져야 하는 모든 역할을 제공합니다. SSO 역할 지정은 상

점 레벨이 아닌 사이트 레벨에서 발생함을 기억하십시오(일반 사용자 등록에서와 같이). 그러므로 지정된 storeAncestor 속성은 실제로 사이트의 상위입니다(상점 0).

예:

```
<User registrationType="SSO" memberAncestor="o=Default Organization,o=Root Organization"
storeAncestor="o=Root Organization"><BR>
    <Role name="Registered Customer" roleContext="explicit"
    DN="o=Reseller Organization,o=Root Organization"/><BR>
    <Role name="Registered Customer" roleContext="explicit"
    DN="o=Seller Organization,o=Root Organization"/><BR>
    <Role name="Registered Customer" roleContext="explicit"
    DN="o=Supplier Organization,o=Root Organization"/><BR>
    <Role name="Registered Customer" roleContext="explicit"
    DN="ou=Supplier Hub Organization,o=Business Indirect Supplier Organization,
           o=Root Organization"/><BR>
  </User>
```

이 예는 SSO에서 시스템으로 오는 임의 구매자에게 네 가지 역할을 제공합니다.

제 8 장 X.509 인증 관리

WebSphere Commerce는 클라이언트 인증 로그온을 보안 메커니즘으로 지원하여 사이트와 고객 모두를 보호합니다. X.509 인증은 사이트에 들어오는 고객에 대한 기본 인증을 보완합니다. 이 인증을 보유하는 고객은 보안 WebSphere Commerce 사이트에 액세스할 수 있으며 이 사이트는 클라이언트 인증서 인증으로 사용 가능합니다.

WebSphere Commerce 인스턴스를 작성할 때 인증 모드를 선택합니다. 인증 모드는 기본 또는 X.509입니다. 기본값은 기본 인증으로 로그인 ID와 암호를 사용하는 로그온 인증입니다. X.509 인증을 사용하여 로그온 인증을 활성화하려면 X.509 인증을 선택하십시오.

X.509 인증 사용을 시작하기 전에 X.509 인증의 전자 인증을 처리하기 위한 외부 인증 기관과의 신뢰 관계를 준비해야 합니다. Netscape Enterprise를 웹 서버로 사용 중인 경우, 웹 서버에서 X.509 인증을 사용하기 위해 다음 추가 단계를 수행해야 합니다. 추가 정보와 전체 지시사항에 대해서는 Netscape Enterprise Server 문서를 참조하십시오.

X.509 사용자는 WebSphere Commerce 액셀러레이터를 사용하여 액세스할 수 있습니다. X.509 인증 인증이 사용되기 전에 운영자는 서버 인증에 의해 인식되고 브라우저에 설치되는 클라이언트 인증이 있음을 보장해야 합니다. 그렇지 않으면 운영자가 로그온할 수 없습니다. 운영자가 처음으로 WebSphere Commerce 관리 콘솔 로그인 창에 액세스할 때 정상 구매자가 보안 URL에 액세스할 때와 비슷하게 인증 구매자 레코드가 작성되고 구매자 쿠키가 발행됩니다. 운영자가 올바른 ID와 암호를 사용하여 WebSphere Commerce 관리 콘솔에 로그온한 후 운영자 쿠키가 발행되어 구매자 쿠키를 대체합니다. 그러면 운영자가 운영자 사용자와 이전 구매자 사용자의 두 사용자 레코드를 갖습니다.

다음 경우에 오류 메시지가 표시됩니다.

- 사용자의 X.509 인증이 사이트에 의해 취소되었습니다.
- 클라이언트 인증에 구매자가 WebSphere Commerce에서 고유함을 보증하기 위한 필요한 정보가 없습니다.

X.509 오류 보기 태스크는 `VIEWREG` 데이터베이스 테이블에 `X509 ErrorView`로 등록됩니다.

X.509 인증 사용

WebSphere Commerce 인스턴스를 작성할 때, 구성 관리자를 사용하여 기본 인증 또는 X.509 인증 중 하나를 선택합니다. 기본값은 기본 인증으로, 로그온 ID 및 암호를 사용하는 인증입니다.

X.509 인증을 사용한 인증을 사용하려면 다음을 수행하십시오.

1. IBM HTTP 웹 서버 SSL 인증을 설정하십시오. SSL 서버 인증은 신뢰 관계를 위한 클라이언트 권한의 목록을 포함합니다. 추가 클라이언트 인증 기관을 추가해야 할 수 있습니다.
2. WebSphere Commerce 구성 관리자를 시작하십시오.
3. **인스턴스 특성 -> WebServer**를 선택하십시오.
4. 인증 모드에 대해 **X.509** 상자를 선택하십시오. **적용**을 누르십시오. X.509 클라이언트 인증 사용자가 이제 승인됩니다. IBM HTTP 서버는 X.509 인증 모드를 선택하면 자동으로 사용됩니다.
5. WebSphere Commerce 서버를 시작하고 중지하십시오. WebSphere Commerce는 서버가 다시 시작될 때까지 `CERT_X509` 테이블에 X.509 사용자를 등록하지 않습니다.

주: IBM HTTP 서버를 구성하여 X.509 인증을 선택 또는 필수로 설정할 수 있습니다.

1. 구성 파일 `httpd.conf`를 열고 `SSLClientAuth` 지시문을 찾으십시오. 지시문을 1(선택) 또는 2(필수)로 설정하십시오. 권장 매개변수는 *필수*입니다.
2. WebSphere Commerce Payments 클라이언트가 SSL 클라이언트 인증을 지원하지 않으므로, WebSphere Commerce Payments 클라이언트와 웹 서버 사이에서 SSL을 사용하지 않아야 합니다.
   a. 텍스트 편집기로 `PaymentServlet.properties` 파일을 여십시오. 이 파일은 WebSphere Commerce Payments 설치 디렉토리에 있습니다.
      - `UseNonSSLWCSClient` 특성을 찾으십시오. 특성을 '1' 값으로 설정하십시오.
      - 파일에서 `UseNonSSLWCSClient` 특성을 찾을 수 없는 경우, 다음 행을 추가하십시오.

        ```
        UseNonSSLWCSClient=1
        ```

   b. 파일을 저장하고 편집기를 종료하십시오.
3. WebSphere Commerce Payments가 WebSphere Commerce와 동일한 시스템에 설치되는 경우,
   a. 구성 관리자를 시작하십시오.
   b. 인스턴스를 선택한 후 **Payments**를 선택하십시오.

c. **비SSL WebSphere Commerce Payments 클라이언트 사용**을 선택하십시오. 이렇게 하면 WebSphere Commerce 서버 클라이언트는 SSL을 사용하지 않고 WebSphere Commerce Payments와 통신할 수 있습니다.

d. **적용**을 누르십시오.

e. 구성 관리자를 닫으십시오.

4. WebSphere 관리 콘솔에서 WebSphere Commerce Payments 응용프로그램 서버를 다시 시작하십시오.

5. WebSphere 관리 콘솔에서 WebSphere Commerce 응용프로그램 서버를 다시 시작하십시오.

인증서의 제한사항 및 필터링 매개변수 설정에 대한 추가 옵션과 자세한 정보는 IBM HTTP 서버 문서를 참조하십시오.

X.509 인증 사용자의 상태 갱신

WebSphere Commerce 액셀러레이터를 사용하여 사이트 운영자는 X.509 인증 사용자 상태를 다음 상태 값 중 하나로 갱신할 수 있습니다.

올바름 사용자는 자신의 인증으로 보안 WebSphere Commerce 사이트에 액세스할 수 있습니다.

취소됨 사용자는 WebSphere Commerce 사이트에 액세스할 수 없습니다. 취소된 인증 사용자가 로그온하려 시도할 때 X.509 인증 오류 페이지가 표시됩니다.

만기 사용자는 WebSphere Commerce 사이트에 액세스할 수 없습니다. 만기된 인증 사용자가 로그온하려 시도할 때 X.509 인증 오류 페이지가 표시됩니다.

X.509 인증을 관리할 때 인증 보유자에 대한 제한 및 필터링 매개변수를 설정하기 원할 수도 있습니다. 예를 들어, `httpd.conf` 구성 파일을 수정하여 특정 유형의 인증 보유자가 사용자의 보안 사이트에 액세스하도록 허용하기 원할 수도 있습니다.

추가 정보와 지시사항에 대해서는 웹 서버 문서를 참조하십시오.

일반 인증 시나리오

다음 단계는 X.509 인증에 대한 일반 인증 시나리오를 보여줍니다.

1. 구매자가 액세스하는 사이트:
   - `http://`를 통해 비보안 URL

     인증이 수행되지 않습니다.
   - `https://`를 통한 보안 URL

     구매자에게 클라이언트 인증을 선택하도록 프롬프트합니다.
   - URL 명령의 액세스 모드 때문에 URL 명령은 `https://`로 경로 재지정됩니다.

구매자에게 클라이언트 인증을 선택하도록 프롬프트합니다.

2. WebSphere Commerce 서버는 클라이언트 인증의 정보를 사용하여 구매자가 이미 WebSphere Commerce SHOPPER 테이블에 존재하는지 확인합니다.
   - 구매자가 올바른 인증 상태를 갖고 존재하는 경우, 구매자는 인증되고 구매 플로우가 다시 시작됩니다.
   - 구매자가 존재하지 않는 경우:
     – 구매자가 자동으로 WebSphere Commerce 데이터베이스에 등록되고 구매 플로우가 다시 시작됩니다.

주: CERT_X509 테이블에 있는 정보만이 인증에 사용됩니다. 그러나, 사용 가능한 경우 X.509 클라이언트 인증에서 구매자 주소 정보를 사용할 수 있습니다.

제 3 부 보안 권한부여 관리

이 부분에서는 WebSphere Commerce 사이트 운영자가 수행할 수 있는 보안 권한부여 태스크에 대해 설명합니다.

제 9 장 액세스 제어 소개

전자상거래의 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 전자상거래 솔루션에 적합하도록 사용자 정의할 수 있습니다.

전자상거래 활동에 대한 액세스 관리는 사이트의 승인된 구성원간의 안전한 비즈니스 트랜잭션을 보장하고 온라인 조작의 적법성을 검증함으로써 회사의 재정적 자산 및 자원을 보호하는 데 있어서 필요한 부분입니다. 액세스 제어는 특히 전자상거래의 경우 매우 중요하며, 여기에서는 웹을 통한 고객 관계에 의한 비즈니스에 많은 영향을 끼칩니다.

액세스 제어의 의의

액세스 제어를 사용하면 비즈니스 워크플로우를 관리할 수 있으며 사용자가 해당 역할 및 책임에 맞는 활동만 수행해야 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 후에 사용자에게 허용되는 항목
고객은 스스로 등록할 수 있습니다.	판매자 관리자가 새 고객을 등록할 수 있습니다.

기본적으로 사용자에게 허용되는 항목	사용자 정의 후에 사용자에게 허용되는 항목
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(국가별 설정에 따라 다름) 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.
계정 담당은 모든 계정을 표시할 수 있습니다.	계정 담당은 활성된 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 설명합니다.

제 10 장 시작하기

이전 장에서는 전자상거래에서 액세스 제어 정책이 하는 중요한 역할과 웹상의 비즈니스 수행시 효율성과 신뢰성을 향상시키는 주요 이점들을 배웠습니다.

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

이 장은 다음 절로 구성됩니다.

- 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 전자상거래 사이트에 대한 액세스를 설정하고 관리하는 것입니다. 여기에는 사이트에 참가할 조직을 작성하고 그 조직들의 구성원을 정의하는 것이 포함됩니다. WebSphere Commerce 5.5, 비즈니스 모델이 도입되었습니다. 인스턴스가 작성되면, 조직 구조를 설정할 운영자가 공개할 수 있는 견본 비즈니스 모델이 존재하게 됩니다. 비즈니스 모델에 대한 자세한 정보는 19 페이지의 『비즈니스 모델』을 참조하십시오.

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. 제공된 견본 비즈니스 모델을 사용 중인 경우, 액세스 제어의 다음 장으로 건너뛰어도 됩니다. 고유의 조직 구조를 정의하려면, 다음 단계를 계속 진행하십시오.

조작, 사용자 및 역할 작성에 대한 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

*WebSphere Commerce 기본 정보*도 참조하십시오. 전체 비즈니스 모델을 보려면, 각각 *WebSphere Commerce 상점 개발 안내서* 및 *WebSphere Commerce 견본 상점 안내서*를 참조하십시오.

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 하위 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 프로세스나 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 사용 가능한 기본 역할 세트를 제공합니다. 판매자 조직을 작성하고 있으므로, 지정할 수 있는 일반 역할에는 판매자 관리자, 판매자 등이 포함됩니다. 기본 역할 목록은 32 페이지의 『역할』을 참조하십시오.
4. 사용자를 작성합니다. 조직과 마찬가지로, 각 사용자별로 사용자 이름, 연락처 정보 및 지정된 역할이 포함된 프로파일을 작성합니다. 역할을 지정할 때는, 이전 단계에서 조직에게 지정한 역할 목록에서 선택합니다.
5. 고객이 조직에서 관리하는 상점에서 구매할 수 있도록 새 조직에 정책 그룹을 지정하십시오. 필수 일반 정책 그룹으로는 관리 및 운영 정책 그룹, 공통 구매 정책 그룹, B2C 정책 그룹 또는 B2B 정책 그룹이 있습니다. 정책 그룹에 대한 자세한 정보는 229 페이지의 『기본 액세스 제어 정책 및 그룹』을 참조하십시오.

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

주: WebSphere Commerce Professional Edition에서는 어떠한 조직도 작성할 수 없습니다. 판매자 조직이 이미 작성되어 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 등록됩니다). 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.

주: 정상적인 환경에서 구매자 조직은 루트 조직이 등록한 정책 그룹을 상속하게 되므로, 어떠한 정책 그룹에도 등록할 필요가 없습니다.

위에서 요약한 모든 단계는 조직 관리 콘솔의 액세스 관리 메뉴에서 다시 수행됩니다.

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

액세스 제어 이해

전자상거래 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 전자상거래 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 부분, 즉 액세스 그룹, 조치 그룹, 자원 그룹 및 선택적 관계로 구성됩니다.

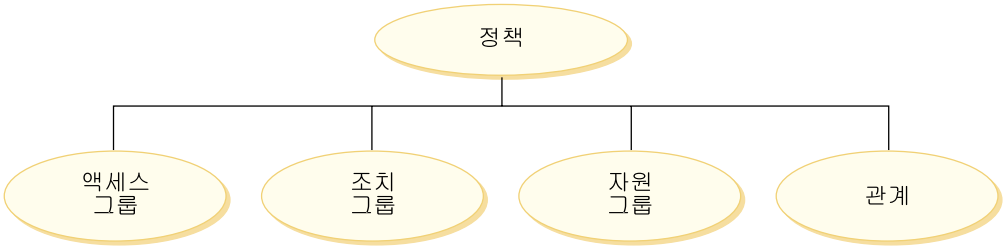
*액세스 그룹*은 사이트의 기능 세트에 대한 일반 액세스를 공유하는 사용자 그룹입니다. 액세스 그룹에는 일반적으로 같은 부서, 기량 또는 역할 같은 일반 속성을 공유하는 사용자들이 포함됩니다.

*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 4. 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 그룹, 조치 그룹, 자원 그룹 및 관계에 대한 자세한 정보에 대해서는 19 페이지의 제 3 장 『권한부여 개념』을 참조하십시오.

액세스 제어 사용 시작 방법

어떤 경우에는 아무 것도 수행할 필요가 없습니다. 비즈니스 모델을 도입하면 시스템의 기본 액세스 제어 구조를 제공하는 데에도 도움이 되며, WebSphere Commerce의 기본 정책은 시스템의 일반 사용자와 이러한 사용자가 조직에서 해당 역할과 연관하여 수행하는 활동에 기반을 둔 액세스 제어의 기본 구조를 제공하도록 설계되어 있습니다. 이 정책들은 광범위한 일반적 비즈니스 활동을 다루며 멤버쉽, 주문 작성 및 프로세스, 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 46 페이지의 『정책 세부사항』을 참조하십시오.

제 11 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.

주: 생소한 용어나 개념에 대한 자세한 정보는 19 페이지의 제 3 장『권한부여 개념』을 참조하십시오.

변경으로 영향받는 정책 구분

19 페이지의 제 3 장『권한부여 개념』에서 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 지정 대상 됩니다.

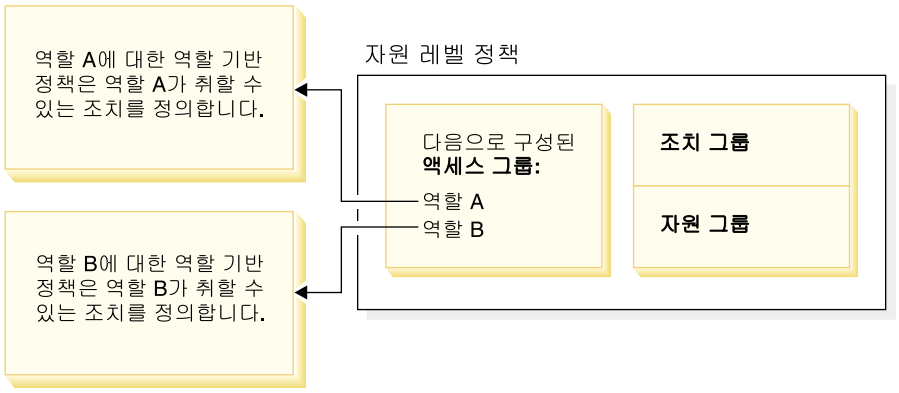
- 각 기본 역할에는 해당 액세스 그룹이 있습니다. 예를 들어, 판매자 역할의 액세스 그룹은 판매자입니다.
- 각 "역할 기반" 액세스 그룹에는 일반적으로 두 개의 연관된 역할 기반 정책이 있습니다.
  - 역할이 실행 권한을 부여 받은 컨트롤러 명령을 정의하는 정책

– 뷰 조치 역할을 정의하는 정책은 실행 권한을 부여 받습니다. 뷰 조치는 VIEWREG 테이블의 뷰에 맵핑됩니다. 예를 들어, OperationalReportsHomeRHSView는 판매자가 액세스할 수 있는 운영 보고서 목록이 있는 웹 페이지를 표시합니다.

일부 컨트롤러 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.

컨트롤러 명령의 자원 레벨 정책은 컨트롤러 명령의 특정 역할 기반 정책과 직접 관련되어 있습니다. 자원 레벨 정책에서 컨트롤러 명령은 조치 그룹의 일부이지만, 역할 기반 정책에서는 컨트롤러 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 5. 자원 레벨 정책과 연관된 역할 기반 정책의 관계



다음 그림은 사용자 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 정책이 이들에게 도서, 잡지 및 신문을 읽거나 공부할 수 있도록 권한을 부여하기 때문입니다.

그림 6. 자원 레벨 정책과 이에 영향을 주는 역할 기반 정책

컨트롤러 명령의 역할 기반 정책에서는 다음에 유의하십시오.

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

마찬가지로 뷰의 역할 기반 정책에서는 다음에 유의하십시오.

- 조치 그룹에는 실행될 수 있는 뷰가 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 권한부여된 역할을 수행하도록 권한을 부여합니다. 예를 들어, 위의 예에서 역할 어린이는 다음 조치들을 실행할 수 있는 권한을 부여받습니다.

- 공부
- 읽기
- 놀기

자원 레벨 정책에 이제 일하기라는 새로운 조치를 포함하도록 변경했다고 가정합니다. 성인 역할을 가진 사용자는 작업 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 표시됩니다. 어린이에 대한 정책은 그렇지 않습니다. 비록 어린이 및 성인 모두 자원 레벨 정책에 의해 적절하게 권한을 부여받았다고 하더라도 어린이에 대한 역할 기반 정책은 일하기 라는 조치 권한을 부여하지 않습니다.

자원 레벨 정책이 역할 기반 정책과 연결된 방식 때문에 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 역할이 포함되어 있는지를 판별하는 것입니다. 조직 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 실행하도록 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.

다음 테이블은 자원 레벨 정책을 새로 작성하거나, 삭제 또는 변경할 때 필요한 추가 변경사항을 요약한 것입니다.

표 9. 역할을 사용하는 자원 레벨 정책을 변경할 때는 추가 변경이 요구됩니다.

자원 레벨 정책으로 변경	**자원 레벨의 액세스 그룹이 역할을 사용하는 경우 다음과 같이 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 명령 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 하도록 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 컨트롤러 명령어를 정의하는 정책은 다음 이름 지정 규칙을 따릅니다.

<AccessGroupforRoleXYZ> Execute <XYZCmdResourceGroup>

예제: ProductManagersExecuteProductManagersCmdResourceGroup.

컨트롤러 명령용 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 뷰를 정의하는 정책은 다음 이름 지정 규칙을 따릅니다.

<AccessGroupforRoleXYZ> Execute <XYZViews>

예: SalesManagersExecuteSalesManagersViews.

자원 그룹에는 하나의 com.ibm.commerce.command.ViewCommand 자원이 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:

```
AuctionAdministratorsForOrgExecuteAuctionCreateCommands
OnStoreEntityResource
```

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 32 페이지의 『역할』을 참조하십시오.
- 다른 액세스 그룹을 사용하기 위해 정책을 변경하기 전에, 액세스 그룹의 정의를 검토하여 요구사항을 충족하는지를 확인하십시오. 이를 수행하려면, 조직 관리 콘솔에서 **액세스 관리 > 액세스 그룹**을 선택하십시오.
- 뷰에서 선택한 값에 따라 정책 페이지는 선택한 조직에서 소유한 정책 목록을 표시합니다. 특정 조직에 고유한 정책과 사이트 레벨 정책 간을 구별하지 않습니다.
- 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: 액세스 제어 정책 목록은 조직 관리 콘솔로 이동됩니다. 조직 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
3. 새 정책을 정책 그룹에 지정.

정책 변경 후

새 정책을 작성한 후에, 새 정책을 적용하려면 정책 그룹에 지정해야 합니다. 정책의 목적에 맞는 그룹에 새 정책을 지정해야 합니다. 정책 그룹 이름에 대한 추가 정보는 229 페이지의 『기본 액세스 제어 정책 및 그룹』의 내용을 참조하십시오.

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.xml과 동일한 형식을 갖습니다. 이 단계가 필요한 이유는 관리 콘솔을 이용하여 작성한 변경이 데

이터베이스에 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 테스트 하였으면 XML 파일을 데이터베이스의 정책 정보가 동기화되도록 갱신해야 합니다. 액세스 제어 정책 및 액세스 그룹과 관련된 여러가지 XML 파일의 설명에 대해서는 151 페이지의 제 13 장『XML을 사용한 액세스 제어 정책 사용자 정의』의 내용을 참조하십시오. 데이터베이스에서 XML 파일로 정책 변경사항을 추출하는 방법과 XML 파일에서 데이터베이스로 정책 정보를 로드하는 방법에 대한 설명도 포함됩니다.

제 12 장 GUI를 사용한 액세스 제어 정책 사용자 정의

아래에 제공된 시나리오에서는 GUI를 사용하여 기본 정책에 다양한 기초적 변경을 수행하기 위해 지금까지 학습한 액세스 제어 정책을 적용합니다. 복잡한 변경사항을 작성하려는 경우, XML을 사용해야 합니다. 151 페이지의 제 13 장『XML을 사용한 액세스 제어 정책 사용자 정의』의 내용을 참조하십시오.

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 10. 시나리오 목차

비즈니스 영역	시작 페이지
경매	118 페이지의『경매 시나리오 1: 경매 운영자의 경매 입찰 종료 권한 제거』
장기 구매 계약	122 페이지의『장기 구매 계약 시나리오 1: 장기 구매 계약 관리자의 장기 구매 계약 첨부 추가 또는 삭제 금지』
주문	125 페이지의『주문 시나리오 1: 구매자에게만 주문 작성 허용』
멤버쉽	132 페이지의『멤버쉽 시나리오 1: 사용자의 자체등록 능력 제거』
쿠폰	138 페이지의『쿠폰 시나리오 1: 구매자만 쿠폰 회수 허용』
조달	142 페이지의『조달 시나리오 1: 조달 장바구니 관리자가 조직에서 작성된 주문에 대한 조달 장바구니를 관리할 수 있도록 허용』
재고	146 페이지의『재고 시나리오 1: 서비스 센터 관리자가 서비스 센터를 갱신하지만 삭제하지는 않도록 허용』
비즈니스 인텔리전스	148 페이지의『비즈니스 인텔리전스 시나리오 1: 감사자가 비즈니스 인텔리전스 보고서를 볼 수 있도록 허용』

특정 유형의 변경을 보여주는 시나리오를 보려면 지정한 사용자 정의 유형에 따라 상호 참조되는 시나리오인 표 11을 참조하십시오.

표 11. 사용자 정의 유형에 따라 구성되는 사용자 정의 시나리오

사용자 정의	참조 페이지
정책의 액세스 그룹에 역할 추가	140

표 11. 사용자 정의 유형에 따라 구성되는 사용자 정의 시나리오 (계속)

사용자 정의	참조 페이지
정책의 조치 그룹 변경	143,146
정책의 자원 관계 변경	128,142
정책을 변경하여 다른 액세스 그룹을 사용	120,125,127,133,138,140
새로운 액세스 그룹 작성 및 정책에서 사용	130,134
새 조치 그룹 작성 및 정책에서 사용	135,144
새 자원 레벨 정책 작성	124,144
새 역할 기반 정책 작성	135,148
새 역할 작성 및 자원 레벨 정책에서 사용	135,148
정책 삭제	119,133
정책의 조치 그룹에서 조치 제거	3,122

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 경매에 대한 내용을 보고 변경할 자원 레벨 정책을 식별하십시오. 정책은 다음과 같습니다.

   ```
   AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
   ```

2. 조직 관리 콘솔에서 **액세스 관리 > 정책**을 누르십시오.
3. 보기에서 **루트 조직**을 선택하여 소유하고 있는 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 조치 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. 관리 콘솔에 로그온하십시오.
2. **구성 > 레지스트리**를 누르십시오.
3. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
4. **갱신**을 누르십시오.

경매 시나리오 2: 경매 관리자의 경매 유찰 권한 제거

기본적으로 상점의 경매 관리자는 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 관리자의 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 경매에 대한 내용을 보고 변경할 자원 레벨 정책을 식별하십시오. 정책은 다음과 같습니다.

   ```
   AuctionManagersForOrgExecuteAdminRetractBidCommandsOnAuctionResource
   ```

2. 조직 관리 콘솔에서 **액세스 관리 > 정책**을 누르십시오.
3. 보기에서 **루트 조직**을 선택하여 소유하고 있는 정책을 표시하십시오.

4. 정책 목록에서 다음을 선택하십시오.

   AuctionManagersForOrgExecuteAdminRetractBidCommandsOnAuctionResource

5. **삭제**를 선택하십시오.

변경사항으로 정책 레지스트리 갱신

1. 관리 콘솔에 로그온하십시오.
2. **구성 > 레지스트리**를 누르십시오.
3. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
4. **갱신**을 누르십시오.
5. **액세스 제어 정책 그룹 레지스트리**의 경우 3 - 4단계를 반복하여 실행하십시오.

경매 시나리오 3: 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 지정하십시오.
- 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 경매에 대한 내용을 보고 변경할 자원 레벨 정책을 식별하십시오.
   정책은 다음과 같습니다.
   RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource
2. 조직 관리 콘솔에서 **액세스 관리** > **정책**을 누르십시오.
3. 보기에서 **루트 조직**을 선택하여 소유하고 있는 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 정책에 대한 내용을 보고 구매자(구매측)용 역할 기반 정책을 찾으십시오.
   정책은 다음과 같습니다.
   Buyers(buy-side)ExecuteBuyers(buy-side)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. 관리 콘솔에 로그온하십시오.
2. **구성 > 레지스트리**를 누르십시오.
3. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
4. **갱신**을 누르십시오.

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

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

이 시나리오에서는 장기 구매 계약 관리자가 취할 수 있는 조치를 정의하는 자원 레벨 정책을 변경합니다. 장기 구매 계약 관리자에게서 장기 구매 계약의 첨부를 추가하거나 삭제할 권한을 제거하려면, 다음을 수행해야 합니다.

- 부록을 사용하여 장기 구매 계약 관리자가 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 계약에 대한 내용을 보고 변경할 자원 레벨 정책을 식별하십시오. 정책은 다음과 같습니다.

   ```
   ContractManagersForOrgExecuteContractManageCommandsOnContractResource
   ```

2. 조직 관리 콘솔에서 **액세스 관리 > 정책**을 누르십시오.
3. 보기에서 **루트 조직**을 선택하여 소유하고 있는 정책을 표시하십시오.
4. 목록에서 정책을 찾으십시오.
5. 정책의 조치 그룹 이름 - ContractManage를 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. 관리 콘솔에 로그온하십시오.
2. **구성 > 레지스트리**를 누르십시오.
3. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
4. **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 계약에 대한 내용을 보고 장기 구매 계약 운영자의 장기 구매 계약 전개 권한을 부여하는 자원 레벨 정책을 찾으십시오.
   이 정책은 다음과 같습니다.
   ```
   ContractOperatorsForOrgExecuteContractDeployCommands
   OnContractResource
   ```
2. 조직 관리 콘솔에서 **액세스 관리** > **정책**을 누르십시오.
3. 보기에서 **루트 조직**을 선택하여 소유하고 있는 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. 이름에 대해 다음을 지정하십시오.
   ```
   ContractAdministratorsForOrgExecuteContractDeployCommands
   OnContractResource
   ```
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 **그룹화 가능한 템플리트 정책**을 선택하여 정책을 템플리트 정책으로 지정하십시오.
10. **확인**을 누르십시오.

변경사항으로 액세스 제어 레지스트리 갱신

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

주: 이 새 정책을 적용하려면 정책 그룹에 지정해야 합니다. 정책 지정은 XML을 통해 수행되어야 합니다. 추가 정보를 참조하십시오.

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.

구매자 역할을 가지고 있는 사용자로 주문 작성을 제한하려면, 다음을 수행해야 합니다.

- 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.

수행 단계

자원 레벨 정책 식별

1. 부록에서 주문에 대한 내용을 보고 변경할 자원 레벨 정책을 식별하십시오. 이 정책은 `AllUsersExecuteOrderCreateCommandsOnStoreResource`입니다.

2. 조직 관리 콘솔에서 **액세스 관리 > 정책**을 누르십시오.
3. 보기에서 **루트 조직**을 선택하여 소유하고 있는 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
   com.ibm.commerce.orderitems.commands.OrderItemAddCmd
   com.ibm.commerce.orderquotation.commands.OrderQuotationCreateCmd
   ```

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

   주: 명령어 `com.ibm.commerce.orderitems.commands.AdminOrderItemUpdateCmd`는 필요하지 않습니다.

구매자(구매측)용 역할 기반 정책 식별

1. 부록에서 역할 기반 정책에 대한 내용을 보고 구매자(구매측)용 역할 기반 정책을 찾으십시오.
   이 정책은 다음과 같습니다.
   `Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup`
2. **액세스 관리 > 정책**을 누르십시오.
3. 보기에 대해 **루트 조직**을 선택하여 사이트 레벨 정책을 표시하십시오.
4. 목록에서 정책을 찾으십시오.

5. 자원 그룹 이름 Buyers(buy-side)CommandsResourceGroup에 유의하십시오. 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(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 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
com.ibm.commerce.orderitems.commands.OrderItemAddCmd
com.ibm.commerce.orderquotation.commands.OrderQuotationCreateCmd
```

6. **추가**를 누르십시오.
7. **완료**를 누르십시오.

변경사항으로 액세스 제어 레지스트리 갱신

1. 관리 콘솔에 로그온하십시오.
2. **구성 > 레지스트리**를 누르십시오.
3. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
4. **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 주문에 대한 내용을 보고 변경할 자원 레벨 정책을 식별하십시오. 이 정책은 `AllUsersExecuteOrderWriteCommandsOnOrderResource`입니다.
2. 조직 관리 콘솔에서 **액세스 관리 > 정책**을 누르십시오.
3. 보기에서 **루트 조직**을 선택하여 소유하고 있는 정책을 표시하십시오.
4. 정책의 목록에서 **AllUsersExecuteOrderWriteCommandsOnOrderResource**를 선택하십시오.
5. 정책의 조치 그룹 이름 - `OrderWriteCommands`를 주의하십시오. 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. 관계에 대해 **없음**을 선택하십시오.
5. 정책의 이름, 표시 이름 및 설명을 갱신하여 액세스 그룹의 변경사항을 반영하십시오.
6. **확인**을 누르십시오.

주문 수정용 명령어 식별

1. **액세스 관리 > 조치 그룹**을 누르십시오.
2. 조치 그룹의 목록에서 **OrderWriteCommands**를 선택하십시오.

3. **변경**를 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.
Cmdcom.ibm.commerce.orderquotation.commands.
OrderItemSelectCmd
```

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

주: 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 정책에 대한 내용을 보고 구매자 관리자용 역할 기반 정책을 찾으십시오.
   이 정책은 다음과 같습니다.
   BuyerAdministratorsExecuteBuyersAdministratorsCommands
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.
Cmdcom.ibm.commerce.orderquotation.commands.
OrderItemSelectCmd
```

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

변경사항으로 액세스 제어 레지스트리 갱신

1. 관리 콘솔에 로그온하십시오.
2. **구성 > 레지스트리**를 누르십시오.
3. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
4. **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 `RMAApproversForOrg`를 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 `RMAApprovers`를 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 주문에 대한 내용을 보고 상점에 대한 RMA를 승인할 수 있는 RMAApproversForOrg 권한을 부여하는 자원 레벨 정책을 찾으십시오. 정책은 RMAApproversForOrgExecuteRMAApproveCommandsOnRMAResource입니다.
2. 조직 관리 콘솔에서 **액세스 관리** > **정책**을 누르십시오.
3. 보기에서 **루트 조직**을 선택하여 소유하고 있는 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 자국어로 된 간단한 정책 설명을 지정하십시오.
5. 설명에 대해 정책이 하는 일에 대한 좀 더 자세한 설명을 자국어로 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. 관리 콘솔에 로그온하십시오.
2. **구성** > **레지스트리**를 누르십시오.
3. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
4. **갱신**을 누르십시오.

멤버쉽 시나리오 1: 사용자의 자체등록 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, 자체등록 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 자체등록할 수 있도록 허용하는 자원 레벨 정책을 제거하지만 멤버쉽 운영자가 해당 조직에서 사용자를 등록할 수 있는 정책을 그대로 유지할 것입니다.

사용자가 자체등록할 수 있는 자원 레벨 정책을 삭제하려면 다음을 수행하십시오.

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

수행 단계

정책 삭제

1. 부록에서 멤버쉽에 대한 내용을 보고 사용자가 자체등록할 수 있도록 허용하는 자원 레벨 정책을 찾으십시오.
   정책은 다음과 같습니다.
   `GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource`
2. 조직 관리 콘솔에서 **액세스 관리** > **정책**을 누르십시오.
3. 보기에서 **루트 조직**을 선택하여 소유하고 있는 정책을 표시하십시오.
4. 정책 목록에서 **GuestsExecuteUserSelfRegistrationCommands OnOrganizationResource**를 선택하십시오.
5. **삭제**를 선택하십시오.

변경사항으로 액세스 제어 레지스트리 갱신

1. 관리 콘솔에 로그온하십시오.
2. **구성** > **레지스트리**를 누르십시오.
3. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
4. **갱신**을 누르십시오.
5. **액세스 제어 정책 그룹 레지스트리**의 경우 3 - 4단계를 반복하여 실행하십시오.

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 RegisteredApprovedUsers는 어떤 역할도 포함하고 있지 않으므로, 이러한 변경에 대해 역할 기반 정책을 갱신하지 않아도 됩니다.

수행 단계

자원 레벨 정책의 액세스 그룹 변경

1. 부록에서 멤버쉽에 대한 내용을 보고 사용자가 주소 정보를 관리할 수 있도록 허용하는 자원 레벨 정책을 찾으십시오.
   정책은 다음과 같습니다.
   NonRejectedUsersExecuteAddressManageCommandsOnUserResource

   주: 거부되지 않는 사용자는 등록이 거부되지 않은 사용자입니다. 그러한 사용자의 등록은 승인되었거나 승인 보류 중입니다.
2. 조직 관리 콘솔에서 **액세스 관리 > 정책**을 누르십시오.
3. 보기에서 **루트 조직**을 선택하여 소유하고 있는 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. 관리 콘솔에 로그온하십시오.
2. **구성 > 레지스트리**를 누르십시오.
3. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
4. **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 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.
- UserAdminRegistrationCommands라고 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. 조직 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 조직에서 **루트 조직**을 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 또는 해당 상위 조직 내에 있도록 지정하십시오.
10. **완료**를 누르십시오.

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

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

   CSAMembershipAdministratorsForOrgExecuteUserAdminRegistrationCommandsOnOrganizationResource
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**를 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 자국어로 지정하십시오.
5. 설명에 대해 자원 그룹에 대한 자세한 설명을 자국어로 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 자국어로 지정하십시오.
5. 설명에 대해 정책이 하는 일에 대한 좀 더 자세한 설명을 자국어로 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.

주: 새 정책을 작성한 후에, 이 새 정책을 적용하려면 정책 그룹에 지정해야 합니다. 정책 지정은 XML을 통해 수행되어야 합니다. 151 페이지의 제 13 장 『XML을 사용한 액세스 제어 정책 사용자 정의』에서 추가 정보를 참조하십시오.

새 액세스 그룹을 사용하도록 자원 레벨 정책 수정

자원 레벨 정책을 수정한 후에, 자원과 동일한 조직에서 구성원 등록 역할을 수행하는 사용자만이 사용자를 등록할 수 있습니다. 기타 조직에서 역할을 수행하는 사용자는 이를 수행할 수 없습니다.

1. 정책 목록에서 다음을 선택하십시오.

   CSAMembershipAdministratorsForOrgExecuteUserAdmin RegistrationCommandsOnOrganizationResource

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. 관리 콘솔에 로그온하십시오.
2. **구성** > **레지스트리**를 누르십시오.
3. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
4. **갱신**을 누르십시오.

쿠폰 시나리오 1: 구매자만 쿠폰 회수 허용

기본적으로 모든 사용자는 쿠폰으로 상품을 구입할 수 있습니다. 어떤 경우에는 WebSphere Commerce 내에서 구매자 역할을 가지고 있는 사용자로 쿠폰 교환을 제한할 수 있습니다.

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

- 부록을 사용하여 쿠폰을 회수할 수 있는 사람을 지정하는 자원 레벨 정책을 찾으십시오.
- 정책의 액세스 그룹을 모든 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 명령을 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 쿠폰에 대한 내용을 보고 변경할 자원 레벨 정책을 식별하십시오. 정책은 다음과 같습니다.

   ```
   AllUsersExecuteCouponRedemptionCommandsOnCouponWalletResource
   ```

2. 조직 관리 콘솔에서 **액세스 관리 > 정책**을 누르십시오.
3. 보기에서 **루트 조직**을 선택하여 소유하고 있는 정책을 표시하십시오.
4. 정책 목록에서 다음을 선택하십시오.

   AllUsersExecuteCouponRedemptionCommandsOnCoupon WalletResource

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**를 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 정책에 대한 내용을 보고 구매자(구매측)용 역할 기반 정책을 찾으십시오.
   정책은 다음과 같습니다.

   `Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup`
2. **액세스 관리 > 정책**을 누르십시오.
3. 보기에서 **루트 조직**을 선택하여 소유하고 있는 정책을 표시하십시오.
4. 목록에서 정책을 찾으십시오.
5. 자원 그룹 이름 `Buyers(buy-side)CommandsResourceGroup`에 유의하십시오. 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. 관리 콘솔에 로그온하십시오.
2. **구성 > 레지스트리**를 누르십시오.
3. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.

4. **갱신**을 누르십시오.

쿠폰 시나리오 2: 쿠폰 운영자 및 운영 관리자의 e-coupon 특별 판매 허용

기본적으로 상점의 쿠폰 운영자는 해당 상점들에 대해 e-coupon 특별 판매를 작성할 수 있습니다. 어떤 경우에는 운영 관리자에게도 이 권한을 부여하고자 할 수도 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 운영 관리자 역할을 추가할 수 있습니다.
- 운영 관리자가 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 운영 관리자 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.
- 운영 관리자 역할이 있는 사용자를 포함하도록 정책의 액세스 그룹을 변경하십시오.
- 자원 레벨 정책의 조치 그룹을 보고 e-coupon 특별 판매 작성 명령을 식별하십시오.
- 부록을 사용하여 운영 관리자의 역할 기반 정책을 찾으십시오. 이 정책은 운영 관리자 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 경매에 대한 내용을 보고 변경할 자원 레벨 정책을 식별하십시오. 정책은 다음과 같습니다.

   ```
   CouponAdministratorsForOrgExecuteCouponPromotionCreateCommands
   OnStoreEntityResource
   ```

2. 조직 관리 콘솔에서 **액세스 관리** > **정책**을 누르십시오.
3. 보기에서 **루트 조직**을 선택하여 소유하고 있는 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 **운영 관리자**를 선택하십시오.
6. **조직**을 눌러 역할이 자원 고유 조직 또는 해당 상위 조직 내에 있도록 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**를 눌러 조치 그룹 변경 페이지를 표시하십시오. e-coupon 특별 판매 작성 명령의 이름(com.ibm.commerce.tools.ecoupon.ECouponPromotionSaveCmd)에 유의하십시오. 운영 관리자가 실행할 수 있는 명령 목록을 포함하는 자원 그룹에 이 명령을 추가해야 합니다.

운영 관리자의 역할 기반 정책 식별

1. 부록에서 역할 기반 정책에 대한 내용을 보고 운영 관리자의 역할 기반 정책을 찾으십시오.
   이 정책은 다음과 같습니다.
   OperationsManagersExecuteOperations ManagersCmdResourceGroup입니다.
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(OperationsManagersCmdResourceGroup)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. **OperationsManagersCmdResourceGroup**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. 관리 콘솔에 로그온하십시오.
2. **구성 > 레지스트리**를 누르십시오.
3. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
4. **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 조달에 대한 내용을 보고 조달 장바구니 관리자가 주문에 대한 조달 장바구니를 관리할 수 있는 권한을 부여하는 자원 레벨 정책을 찾으십시오. 정책은 다음과 같습니다.

   ```
   ProcurementShoppingCartManagersExecuteProcurementShopping
   CartManageOnOrderResource
   ```

2. 조직 관리 콘솔에서 **액세스 관리 > 정책**을 누르십시오.
3. 보기에서 **루트 조직**을 선택하여 소유하고 있는 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. 관리 콘솔에 로그온하십시오.
2. **구성 > 레지스트리**를 누르십시오.
3. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
4. **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 조달에 대한 내용을 보고 조달 장바구니 관리자가 주문에 대한 조달 장바구니를 관리할 수 있는 권한을 부여하는 자원 레벨 정책을 찾으십시오. 정책은 다음과 같습니다.

   ```
   ProcurementShoppingCartManagersExecuteProcurementShopping
   ShoppingCartManageOnOrderResource
   ```

2. 조직 관리 콘솔에서 **액세스 관리 > 정책**을 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**를 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. 보기에서 **루트 조직**을 선택하여 소유하고 있는 정책을 표시하십시오.
3. **새로 만들기**를 눌러 새 정책 페이지를 표시하십시오.
4. 이름에 대해 다음을 지정하십시오.

   ```
   ProcurementBuyerAdministratorsExecuteProcurementShoppingCartSubmit
   CommandsOnOrderResource
   ```

5. 표시 이름에 대해 자국어로 된 간단한 정책 설명을 지정하십시오.
6. 설명에 대해 정책이 하는 일에 대한 좀 더 자세한 설명을 자국어로 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 **그룹 가능한 템플리트 정책**을 선택하여 정책을 템플리트 정책으로 지정하십시오.
13. **확인**을 누르십시오.

액세스 제어 정책 레지스트리를 변경사항으로 갱신

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

주: 새 정책을 작성한 후에, 이 새 정책을 적용하려면 정책 그룹에 지정해야 합니다. 이 작업은 XML을 사용하여 수행됩니다. 151 페이지의 제 13 장 『XML을 사용한 액세스 제어 정책 사용자 정의』에서 추가 정보를 참조하십시오.

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

   ```
   FulfillmentCenterManagersForOrgExecuteFulfillmentCenter
   ManageCommandsOnFulfillmentResource
   ```

2. 조직 관리 콘솔에서 **액세스 관리** > **정책**을 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**를 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. 관리 콘솔에 로그온하십시오.
2. **구성** > **레지스트리**를 누르십시오.
3. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
4. **갱신**을 누르십시오.

재고 시나리오 2: 물류 관리자, 운영 관리자 및 계정 담당만 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 관리자 액세스 그룹은 판매자, 물류 관리자, 운영 관리자 및 계정 담당 역할이 포함됩니다. 어떤 경우에는 판매자에게 서비스 센터 관리자 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 조달에 대한 내용을 보고 조달 장바구니 관리자가 주문에 대한 조달 장바구니를 관리할 수 있는 권한을 부여하는 자원 레벨 정책을 찾으십시오. 정책은 다음과 같습니다.

   ```
   FulfillmentCenterManagersForOrgExecuteFulfillmentCenterManage
   CommandsOnFulfillmentResource
   ```

2. 조직 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. 관리 콘솔에 로그온하십시오.
2. **구성 > 레지스트리**를 누르십시오.
3. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
4. **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 역할(감사자)을 작성하고, 새 역할에 해당하는 새 액세스 그룹 감사자, 새 자원 그룹 및 새 역할 기반 정책을 작성하십시오.
- 자원 레벨 정책의 액세스 그룹에 새 역할을 추가하십시오.
- 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.
- AuditorCommands라고 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. 조직 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 자국어로 지정하십시오.
5. 상위 조직에서 **루트 조직**을 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 인텔리전스에 대한 내용을 보고 인텔리전스 보고서 열람자가 비즈니스 인텔리전스 보고서를 볼 수 있는 권한을 부여하는 정책을 찾으십시오. 정책은 다음과 같습니다.

   ```
   IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReport
   CommandsOnStoreEntityResource
   ```

2. 조직 관리 콘솔에서 **액세스 관리 > 정책**을 누르십시오.
3. 보기에서 **루트 조직**을 선택하여 소유하고 있는 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**를 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. **이름**에 AuditorCommands를 지정하십시오.
4. **표시 이름**에 자원 그룹에 대한 설명을 자국어로 지정하십시오.
5. **설명**에 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 자원 고유 조직 또는 해당 상위 조직 내에 있도록 지정하십시오.
7. **추가**를 누르십시오.
8. **확인**을 누르십시오.

변경사항으로 정책 레지스트리 갱신

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

제 13 장 XML을 사용한 액세스 제어 정책 사용자 정의

WebSphere Commerce 관리 콘솔에서 액세스 제어 정책 및 그 부분을 변경할 수 있습니다. 더 세밀하게 변경하려면 XML 파일을 직접 편집한 후 데이터베이스에 로드해야 합니다.

액세스 제어의 XML 파일을 변경하기 전에, *WebSphere Commerce 프로그래밍 안내서 및 학습서*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.

*WebSphere Commerce 프로그래밍 안내서 및 학습서*에 제공된 지침에 따라 코드 사용자 정의를 완료했으면 액세스 제어의 XML 파일을 편집하여 원하는 보호를 설정할 수 있습니다.

XML 파일 편집 및 로드를 통해서만 수행될 수 있는 변경사항

다음 변경사항은 해당 XML 파일을 편집하고 로드해야만 수행될 수 있습니다.

- 조치 작성 또는 수정
- 관계 작성 또는 수정
- 관계 그룹 작성 또는 수정
- 자원 작성 또는 수정
- 속성 작성 또는 수정
- 복잡한 기준을 사용한 액세스 그룹 작성 또는 수정
- 복잡한 기준을 사용한 자원 그룹 작성 또는 수정
- 뷰에 포함되는 역할 기반 정책 작성
- 뷰에 포함되는 역할 기반 정책에서 조치 그룹 변경
- 정책 그룹 작성 또는 수정
- 정책을 정책 그룹과 연관

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 12. 액세스 제어에 대한 WebSphere Commerce XML 파일

파일 이름	설명
ACUserGroups_de_DE.xml 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 모든 액세스 제어 정보 추출에 사용된 필터 파일.
OrganizationPoliciesFilter.xml	특정 조직이 소유하는 정책과 관련된 모든 액세스 제어 정보 추출에 사용된 필터 파일.
ACUserGroupsFilter.xml	모든 액세스 그룹 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.

표 12. 액세스 제어에 대한 WebSphere Commerce XML 파일 (계속)

파일 이름	설명
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.
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 변경

XML 파일을 조작하여 다음 권한부여 태스크를 수행할 수 있습니다.

- 뷰 보호
- 컨트롤러 명령 보호
- 자원 레벨 액세스 제어 구현
- 데이터 bean 보호
- 속성별로 자원 그룹화
- 관계 정의
- 관계 그룹 정의

뷰 보호

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

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

ResourceGroup 이름인 ViewCommandResourceGroup은 이것이 뷰에 대한 역할 기반 정책임을 표시합니다. 정책은 ProductManagers 사용자 그룹의 사용자들이 ProductMangersViews 조치 그룹의 뷰를 표시할 수 있음을 알려줍니다. 유사하게, 대부분의 역할의 경우 판매자 역할 -> 판매자 액세스 그룹 -> SellersViews 조치 그룹과 같이 역할이 액세스할 수 있는 뷰를 그룹화하는 해당 조치 그룹이 있습니다.

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 표시합니다.

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 뷰 이름은 조치 정의의 CommandName과 일치해야 합니다. CommandName 값은 ACACTION 테이블의 ACTION 열에 저장됩니다. Name과 CommandName 속성이 동일할 필요는 없습니다.

기존 정책을 사용하여 새 뷰 추가

기존의 역할 기반 뷰 정책을 사용하여 역할에 의해 액세스 가능한 새 뷰를 추가하려면 표시된 것과 유사한 XML 파일을 작성한 후 다음을 수행하십시오.

```
 <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">

<Policies>

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

  <ActionGroup Name="ProductManagersViews" OwnerID="RootOrganization">
              <ActionGroupAction Name="MyNewView"/>
 </ActionGroup>
 </Policies>
```

1. 뷰 이름 *MyNewView*를 갖는 XML 파일에 새 조치 정의를 작성하십시오. 이 이름은 사용자가 선택하는 어떤 이름도 가능합니다.

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

2. 어떤 역할이 이 뷰에 대한 액세스를 가질지를 판별하고 다음 예에서와 같이 새 조치를 XML 파일의 해당하는 조치 그룹과 연관시키십시오.

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

     <ActionGroupAction Name="MyNewView"/>

    </ActionGroup>
   ```

   이 조치 그룹을 포함하는 역할 기반 정책 (ProductManagersExecuteProductManagersViews)이 이미 있으므로, 새 정책을 작성할 필요가 없습니다. 또한 기본 역할 기반 정책은 사이트의 대부분 조직에 적용되는 ManagementAndAdministrationPolicyGroup 정책 그룹에 속하므로, 더 이상 정책 그룹 등록이 필요하지 않습니다.

3. XML 변경사항을 데이터베이스로 로드하십시오. XML 변경사항에 대한 자세한 정보는 187 페이지의 『변경사항을 데이터베이스에 로드』를 참조하십시오.

4. 다음을 수행하여 관리 콘솔에서 액세스 제어 정책 레지스트리를 갱신하십시오.

   a. 사이트 운영자로서 관리 콘솔에 로그온하십시오.

   b. **구성** > **레지스트리**를 누르십시오.

   c. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.

   d. **갱신**을 누르십시오.

새 정책을 사용하여 새 뷰 추가

기존의 역할 기반 정책을 가지고 있지 않은 새 역할에 의해 액세스 가능한 새 뷰를 추가하려면 표시된 것과 유사한 XML 파일을 작성한 후 다음을 수행하십시오.

```
 <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">

<Policies>

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

  <ActionGroup Name="XYZViews" OwnerID="RootOrganization">
             <ActionGroupAction Name="MyNewView"/>
 </ActionGroup>
 <Policy Name="XYZExecuteXYZViews"
   OwnerID="RootOrganization"
UserGroup="XYZ"
   ActionGroupName="XYZViews"
   ResourceGroupName="ViewCommandResourceGroup"
   PolicyType="groupableStandard">
 </Policy>
```

```
<PolicyGroup Name="ManagementAndAdministrationPolicyGroup" OwnerID="RootOrganization">
 <PolicyGroupPolicy Name="XYZExecuteXYZViews" PolicyOwnerId="RootOrganization" />
</PolicyGroup>

</Policies>
```

1. 뷰 이름 *MyNewView*를 갖는 XML 파일에 새 조치 정의를 작성하십시오. 이 이름은 사용자가 선택하는 어떤 이름도 가능합니다.

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

2. 새 역할과 연관될 새 조치 그룹을 작성하십시오.

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

   여기서 *XYZViews*는 사용자 조치 그룹의 이름입니다. 조치 그룹의 OwnerID는 항상 RootOrganization이어야 합니다.

3. 새 조치를 새 조치 그룹과 연관시키십시오.

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

    <ActionGroupAction Name="MyNewView"/>

     </ActionGroup>
   ```

   여기서 *XYZViews*는 사용자 조치 그룹이고 *MyNewView*는 사용자가 작성한 조치입니다.

4. 새 조치 그룹을 참조하는 정책을 작성하십시오.

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

   여기서 *XYZExecuteXYZViews*는 정책 이름이고 *XYZViews*는 조치 그룹입니다. WebSphere Commerce 5.5에서는 정책 등록 모델로 인해 그룹화할 수 있는 표준 정책 및 그룹화할 수 있는 템플리트 정책의 소유자 ID가 정책이 적용되는 자원을 결정하는 데 사용되지 않습니다. 조직(소유자)에서 정책을 볼 때 일반적으로 관리 콘솔에서만 소유자 ID 값을 사용합니다. 정책이 여러 개의 조직에 적용될 경우, 소유자 ID를 공통 상위 조직(예: 루트 조직)으로 설정할 것을 권장합니다. 정책이 특정 조직에만 적용되면, 소유자 ID를 해당 조직의 orgentity_id로 설정할 것을 권장합니다.

5. 적절한 정책 그룹에 새 정책을 포함시키십시오. 기본적으로 대부분의 역할 기반 정책은 모든 조직에 적용되어야 하는 ManagementAndAdministrationPolicyGroup에 저장됩니다.

```
<PolicyGroupName="ManagementAndAdministrationPolicyGroup"
OwnerID="RootOrganization">
<PolicyGroupPolicy Name="XYZExecuteXYZViews" PolicyOwnerId="RootOrganization"/>
</PolicyGroup>
```

   여기서 PolicyOwnerId 값은 정책 정의에서 사용되는 OwnerID 값과 같아야 합니다.

6. XML 변경사항을 데이터베이스로 로드하십시오. XML 변경사항에 대한 자세한 정보는 187 페이지의 『변경사항을 데이터베이스에 로드』를 참조하십시오.
7. 다음을 수행하여 관리 콘솔에서 액세스 제어 정책 레지스트리를 갱신하십시오.
   a. 사이트 운영자로서 관리 콘솔에 로그온하십시오.
   b. **구성** > **레지스트리**를 누르십시오.
   c. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
   d. **갱신**을 누르십시오.

이제 뷰를 사용할 수 있습니다.

컨트롤러 명령 보호

모든 컨트롤러 명령은 역할 기반 액세스 제어 정책이 있어야 실행됩니다. 명령이 자원 레벨 확인을 수행하는 경우 컨트롤러 또는 태스크 명령에도 자원 레벨 정책이 필요합니다. 자세한 정보는 164 페이지의 『자원 보호』를 참조하십시오. 다음 예는 컨트롤러 명령에 대한 역할 기반 정책을 표시합니다.

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

ActionGroupName인 ExecuteCommandActionGroup은 이것이 컨트롤러 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 컨트롤러 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 Execute가 지정됩니다. Execute 조치는 다음과 같이 정의됩니다.

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

주: 컨트롤러 명령의 인터페이스 이름은 자원 정의의 ResourceBeanClass와 일치해야 합니다. ResourceBeanClass 값은 ACRESCGRY 테이블의 RESCLASSNAME 열에 저장됩니다. 이러한 명령은 AccCommand 인터페이스를 확장하는 ControllerCommand 인터페이스를 확장하므로 자원으로 사용될 수 있습니다. AccCommand 인터페이스는 다시 Protectable 인터페이스를 확장합니다. 이러한 인터페이스에 대한 자세한 정보는 *WebSphere Commerce 프로그래밍 안내서 및 학습서*를 참조하십시오.

기존 정책을 사용하여 새 컨트롤러 명령 추가

기존 역할 기반 정책이 있는 새 역할에서 액세스할 새 컨트롤러 명령을 추가하려면, 표시된 파일과 유사한 XML 파일을 작성하십시오. 나중에 특정 단계가 나열됩니다.

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">

<Policies>

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

```
  <ResourceAction Name="ExecuteCommand"/>
 </ResourceCategory>

<ResourceGroup Name="SellersCmdResourceGroup" OwnerID="RootOrganization">
    ResourceGroupResource Name="com.xyz.commands.MyNewControllerCmdResource
    Category"/>
 </ResourceGroup>

 </Policies>
```

1. 컨트롤러 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. 어떤 역할이 명령에 대한 액세스를 가질지를 판별하고 다음 예에서와 같이 새 자원을 XML 파일의 해당하는 자원 그룹과 연관시키십시오.

   ```
   <ResourceGroup Name="SellersCmdResourceGroup" OwnerID="RootOrganization">
     <ResourceGroupResource Name="com.xyz.commands.
   MyNewControllerCmdResourceCategory"/>

    </ResourceGroup>
   ```

   사용하려는 역할에 따라서 자원 그룹을 변경할 수 있습니다. 역할 기반 정책에 대한 추가 정보는 230 페이지의 『역할 기반 정책』을 참조하십시오.

3. XML 변경사항을 데이터베이스로 로드하십시오. XML 변경사항에 대한 자세한 정보는 187 페이지의 『변경사항을 데이터베이스에 로드』를 참조하십시오.
4. 다음을 수행하여 관리 콘솔에서 액세스 제어 정책 레지스트리를 갱신하십시오.
   a. 사이트 운영자로서 관리 콘솔에 로그온하십시오.
   b. **구성** > **레지스트리**를 누르십시오.
   c. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
   d. **갱신**을 누르십시오.

이 자원 그룹을 포함하는 역발 기반 정책이 이미 있으므로 자원 레벨 확인을 수행하지 않는 경우 이제 새 컨트롤러 명령을 사용할 수 있습니다. 자원 레벨 확인 및 명령에 대한 정보는 162 페이지의 『기존 정책의 자원 레벨 액세스 제어 수정』을 참조하십시오.

새 정책을 사용하여 새 컨트롤러 명령 추가

기존 역할 기반 정책이 없는 새 역할에서 액세스할 새 컨트롤러 명령을 추가하려면, 표시된 파일과 유사한 XML 파일을 작성하십시오. 나중에 특정 단계가 나열됩니다.

```
 <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">
<Policies>

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

```
 <ResourceAction Name="ExecuteCommand"/>
</ResourceCategory>

      <ResourceGroup Name="XYZCmdResourceGroup"  OwnerID="RootOrganization"
   <ResourceGroupResource Name="com.xyz.commands.MyNewController
   CmdResourceCategory"/>
</ResourceGroup>

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

 <PolicyGroup Name="ManagementAndAdministrationPolicyGroup"
  OwnerID="RootOrganization">
 <PolicyGroupPolicy  Name="XYZExecuteXYZsCmdResourceGroup"
  PolicyOwnerId="RootOrganization" />
</PolicyGroup>

</Policies>
```

1. 컨트롤러 명령의 인터페이스 이름에 해당되는 새 자원 정의를 XML 파일에서 작성하십시오. 예에 대해서는 158 페이지의 『기존 정책을 사용하여 새 컨트롤러 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">
      PolicyType="groupableStandard">
   </Policy>
   ```

5. XML 변경사항을 데이터베이스로 로드하십시오. XML 변경사항에 대한 자세한 정보는 187 페이지의 『변경사항을 데이터베이스에 로드』를 참조하십시오.
6. 다음을 수행하여 관리 콘솔에서 액세스 제어 정책 레지스트리를 갱신하십시오.
   a. 사이트 운영자로서 관리 콘솔에 로그온하십시오.
   b. **구성** > **레지스트리**를 누르십시오.
   c. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
   d. **갱신**을 누르십시오.

자원 레벨 확인을 수행하지 않는 경우 이제 컨트롤러 명령을 사용할 수 있습니다. 자원 레벨 확인 및 명령에 대한 정보는 162 페이지의 『기존 정책의 자원 레벨 액세스 제어 수정』을 참조하십시오.

컨트롤러 명령의 명령 레벨 액세스 제어 수정

기본 액세스 제어 정책에 따라 UserRegistrationAdminAddCmd 명령은 마케팅 관리자 역할만 있는 사용자가 실행할 수 없습니다. 다음 시나리오는 이러한 사용자가 이 명령을 수행할 수 있도록 기존 정책을 수정하는 데 필요한 단계를 설명합니다. 이 시나리오의 단계를 사용해서 사용자 자신의 요구사항에 맞게 사용자 정의할 수 있습니다.

모든 컨트롤러 명령은 명령 레벨 액세스 제어 정책이 필요한데, 이것은 ActionGroupName = ExecuteCommandActionGroup을 갖습니다. 또한 컨트롤러 명령의 인터페이스 이름을 포함하는 자원 그룹도 있어야 합니다. 이러한 정책은 대개 특정 역할(예: MarketingManagersExecuteMarketingManagerCmdResourceGroup)을 참조합니다.

```
<Policy Name="MarketingManagersExecuteMarketingManagerCmdResourceGroup"
   OwnerID="RootOrganization"
   UserGroup="MarketingManagers"
   ActionGroupName="ExecuteCommandActionGroup"
   ResourceGroupName="MarketingManagerCmdResourceGroup"
   PolicyType="groupableStandard">

</Policy>
```

주: 위의 정책은 인스턴스 작성 중에 데이터베이스로 로드되는 기본 정책 중 하나입니다. 기본 정책에 대한 추가 정보는 229 페이지의 『기본 액세스 제어 정책 및 그룹』을 참조하십시오.

이 경우, 마케팅 관리자 역할을 갖는 사용자가 UserRegistrationAdminAddCmd를 실행할 수 있게 하려면, 사용자 고유 XML 파일을 작성하여 이 명령을 정책에 사용되는 기존 자원 그룹에 추가하고 다음을 수행해야 합니다.

1. ExecuteCommand 조치를 다시 정의하십시오.
2. com.ibm.commerce.usermanagement.commands.UserRegistrationAddCmd를 자원 카테고리로서 다시 정의하십시오.
3. 자원 카테고리를 필수 자원 그룹(이 경우에는 MarketingManagerCmdResourceGroup)에 연관시키십시오.
4. XML 파일을 *WC_installdir*/xml/policies/xml에 복사하십시오. 다음은 XML 파일의 예입니다.

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


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

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

```
 <ResourceCategory
      Name="com.ibm.commerce.usermanagement.commands.UserRegistrationAdmin
AddCmdResourceCategory"
   ResourceBeanClass="com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd">
  <ResourceAction Name="ExecuteCommand"/>
 </ResourceCategory>

 <ResourceGroup Name="MarketingManagerCmdResourceGroup"
OwnerID="RootOrganization"
  ResourceGroupResource
      Name="com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmdResourceCategory"/>
 </ResourceGroup>

 </Policies>
```

5. *WC_installdir*/bin/acpload 스크립트를 사용하여 XML 파일을 데이터베이스에 로드하십시오. XML 파일 로드에 대한 자세한 정보는 187 페이지의 『변경사항을 데이터베이스에 로드』를 참조하십시오.
6. 다음을 수행하여 WebSphere Commerce 관리 콘솔에서 액세스 제어 정책 레지스트리를 갱신하십시오.
   a. 사이트 운영자로서 관리 콘솔에 로그온하십시오.
   b. **구성** > **레지스트리**를 누르십시오.
   c. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
   d. **갱신**을 누르십시오.

자원 레벨 확인을 수행하지 않는 경우 이제 컨트롤러 명령을 사용할 수 있습니다. 자원 레벨 확인을 수행 중인 경우 『기존 정책의 자원 레벨 액세스 제어 수정』을 참조하십시오.

기존 정책의 자원 레벨 액세스 제어 수정: 자원 레벨 액세스 제어가 필요한 명령의 경우, 해당 명령은 명령의 getResources() 메소드에서 액세스할 보호된 자원을 리턴합니다. 이렇게 하여 WebSphere Commerce 액세스 제어 프레임워크에서 자원 레벨 액세스 제어 확인을 트리거합니다. WebSphere Commerce는 현재 명령과 동일한 조치를 포함하는 조치 그룹이 있는 시스템에서 액세스 제어 정책을 검색합니다(이 예에서는 com.ibm.commerce.usermanagement.commands.
UserRegistrationAdminAddCmd). 정책의 자원 그룹에는 getResources() 메소드에서 리턴된 자원도 포함되어야 합니다. 이 경우에 UserRegistrationAdminAddCmd 명령이 getResources() 메소드를 구현하고 새 사용자가 등록될 조직을 리턴합니다.

defaultAccessControlPolicies.xml에서 com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd가 조치로서 이미 정의됩니다.

```
<Action Name="com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd"
   CommandName="com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd">
 </Action>
```

defaultAccessControlPolicies.xml XML 파일에 정의된 조치 그룹에도 포함됩니다.

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

  <ActionGroupAction
        Name="com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd"/>
 </ActionGroup>
```

이 조치 그룹은 이미 기존 부트스트랩 정책에서 사용됩니다.

```
<Policy
   Name="MembershipAdministratorsForOrgExecuteUserAdminRegistrationCommandsOnOrganizationResource"
   OwnerID="RootOrganization"
   UserGroup="MembershipAdministratorsForOrg"
   ActionGroupName="UserAdminRegistration"
   ResourceGroupName="OrganizationDataResourceGroup"
   PolicyType="groupableTemplate">

</Policy>
```

주: 많은 정책이 기본 정책이며 인스턴스 작성 중에 데이터베이스에 로드됩니다. 기본 정책에 대한 추가 정보는 229 페이지의 『기본 액세스 제어 정책 및 그룹』을 참조하십시오.

UserRegistrationAdminAddCmd에 필수 역할을 추가하려면, 다음을 수행하십시오.

1. 정책이 사용하는 액세스 그룹에 필수 역할을 추가하십시오. 이 예에서는 MembershipAdministratorsForOrg입니다.

   이 액세스 그룹은 다음과 같이 *WC_installdir*/xml/policies/xml/ACUserGroup_en_US.xml에 정의됩니다.

   ```
   <UserGroup Name="MembershipAdministratorsForOrg" OwnerID="RootOrganization"
      Description="Administrators of membership for the organization" MemberGroupID="-97"

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

   위의 XML에서 getResources()에 의해 리턴되는 자원(조직)의 상위 소유자 조직에 대한 구매자 관리자 또는 판매자 관리자 역할 중 최소한 하나를 갖는 사용자가 포함됩니다. 마케팅 관리자 역할을 추가하기 원한 경우, 새 역할도 포함하도록 향상해야 할 수 있습니다.

2. XML 파일을 *WC_installdir*/xml/policies/xml에 복사하십시오. 다음은 XML 파일의 예입니다.

   ```
   ?xml version="1.0" encoding="UTF-8"?
   <!DOCTYPE UserGroups SYSTEM "../dtd/ACUserGroups_en_US.dtd">

   <UserGroups>
   ```

```
<UserGroup Name="MembershipAdministratorsForOrg" OwnerID="RootOrganization"
    Description="Administrators of membership for the organization" MemberGroupID="-97">

<UserCondition><![CDATA[
<profile>
    <orListConditio>
      <simpleCondition>
   <variable name="role"/>
     <operator name="="/>
   <value data="Buyer Administrator"/>
       <qualifier name="org" data="?"/>
      </simpleCondition>
      <simpleCondition>
   <variable name="role"/>
     <operator name="="/>
   <value data="Seller Administrator"/>
       <qualifier name="org" data="?"/>
      </simpleCondition>
      <simpleCondition>
        <variable name="role"/>
     <operator name="="/>
        <value data="Marketing Manager"/>
     <qualifier name="org" data="?"/>
      </simpleCondition>
   </orListCondition>
</profile>
]]></UserCondition>
</UserGroup>
</UserGroups>
```

3. *WC_installdir*/bin/acpload 스크립트를 사용하여 XML 파일을 데이터베이스에 로드하십시오. XML 파일 로드에 대한 자세한 정보는 187 페이지의 『변경사항을 데이터베이스에 로드』를 참조하십시오.
4. 다음을 수행하여 WebSphere Commerce 관리 콘솔에서 액세스 제어 정책 레지스트리를 갱신하십시오.
   a. 사이트 운영자로서 관리 콘솔에 로그온하십시오.
   b. **구성** > **레지스트리**를 누르십시오.
   c. 레지스트리 목록에서 **액세스 제어 정책**을 선택하십시오.
   d. **갱신**을 누르십시오.

자원 보호

컨트롤러 또는 태스크 명령에 자원 레벨 액세스 제어를 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 수행 중인 기본 WebSphere Commerce 명령에서 확장되므로 자원 레벨 정책을 가지며 새 명령은 기본 명령과 다른 인터페이스를 구현하게 됩니다.
- 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="groupableTemplate">
</Policy>
```

여기서

Name: 정책의 이름

PolicyType: 정책 유형. 그룹화 가능한 템플리트 정책으로 자원 및 해당 상위 자원을 소유하는 조직 엔티티에 동적으로 적용됩니다.

OwnerID: 정책을 소유하는 구성원.

UserGroup: 정책이 이 그룹의 사용자에게 적용됩니다. 역할이 자원을 소유하는 조직으로 동적으로 확장되는 액세스 그룹의 이름 지정 규칙은 그룹 이름에 ForOrg를 추가하는 것입니다.

ActionGroupName: 자원에서 수행할 조치를 포함하는 조치 그룹의 이름.

ResourceGroupName: 조치를 실행할 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 추가 정보는 *WebSphere Commerce 프로그래밍 안내서 및 학습서*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 뷰에 맵핑되고 이러한 뷰는 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 프로그래밍 안내서 및 학습서*를 참조하십시오.

다음은 데이터 bean에 대한 자원 레벨 정책의 예입니다.

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

ActionGroupName인 DisplayDataBeanActionGroup은 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. 그룹화 가능 인터페이스에 대한 자세한 정보는 *WebSphere Commerce 프로그래밍 안내서 및 학습서*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 그룹 관리 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 관계의 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="Root Organization">
  <RelationCondition><![CDATA[
   <profile>
    Relationship Chain Open Condition XML
   </profile>
  ]]></RelationCondition>
 </RelationGroup>
```

관계 체인

각 관계 이름은 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

aValue: 사용자와 자원의 관계를 나타내는 문자열입니다. 이 문자열은 자원의 이행 메소드를 체크인한 관계 중 하나여야 합니다.

관계 체인이 두 개 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, aValue2의 가능한 값은 child이며, 이 값은 사용자가 구성원 계층의 직접 하위 항목

인 조직 엔티티를 리턴합니다. aValue1 값이 ROLE이면, aValue2의 가능한 값은 ROLE 테이블의 NAME 열에 있는 유효한 항목이며, 이 값은 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 평가하여 둘 이상의 조직 엔티티가 리턴되면, 이러한 조직 엔티티 중 최소한 하나가 aValue2 매개변수에서 지정한 관계에 만족하는 경우 RELATIONSHIP_CHAIN의 이 부분이 충족됩니다.

주: 관계 그룹 정의에 대한 자세한 정보는 171 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 계정 담당 역할을 갖도록 해야하는 경우가 있습니다. 다시 이것은 길이가 2인 단일 관계 체인으로 구성된 관계 그룹을 사용합니다. 체인의 첫 번째 부분은 사용자가 계정 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_installdir*/xml/policies/xml/ACUserGroups_locale.xml)에 있습니다. 이 파일은 *WC_installdir*/xml/policies/dtd/ACUserGroups_ko_KR.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. 사용 가능한 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 13. 지원되는 단순 조건 이름

변수 이름	설명	지원되는 연산자	지원되는 값	규정자	규정자 값
역할	사용자가 MBRROLE 테이블에서 이 역할을 가져야 함을 지정합니다.	= !=	ROLE 테이블의 NAME 열 값.	org(지정하지 않는 경우 사용자 는 MBRROLE 테이블에 조직의 역할을 가지고 있어야 함)	• OrgEntityID : 사용자가 역할을 가져야 하는 위치. • OrgAndAncestorOrgs: 그룹화 가능 템플리트 정책에 사용되는 시기. 사용자에게 자원을 소유하는 조직 또는 해당 상위 조직에 지정된 역할이 있는지 확인합니다.
registration status	사용자가 이 등록 상태를 가져야 함을 지정합니다.	= !=	USERS 테이블의 REGISTER-TYPE 열 값(예: 게스트의 경우 G, 등록된 경우 R)	없음	없음

표 13. 지원되는 단순 조건 이름 (계속)

변수 이름	설명	지원되는 연산자	지원되는 값	규정자	규정자 값
상태	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 지정된 조직의 하위 조직이 되도록 지정합니다. 이 정보는 MBRREL 테이블에 저장된 데이터를 기초로 합니다.	= !=	• ORGENTITY 테이블 의 ORGENTITY_ID 값. • ?: 그룹화 가능 템플리트 정책인 경우. 사용자가 자원을 소유하는 조직의 하위 조직인지 확인합니다. 최대 정책 그룹에 등록 중인 가장 근접한 상위 조직까지(이 조직 포함) 사용자가 자원 소유자 상위 조직의 하위 조직인지 확인하기도 합니다.	없음	없음

액세스 그룹에 대한 simpleConditions의 예

역할:

규정자를 지정하지 않은 역할: 다음 예는 보통 역할 기반 정책에서 사용되는 규정자를 지정하지 않은 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 사용자에게는 조직 엔티티 ORGENTITY_ID = 100의 판매자 역할이 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 지정된 역할: 다음 예에서는 규정자와 특수 데이터 값 OrgAndAncestorOrgs가 지정된 역할 simpleCondition을 보여줍니다. 이 규정된 데이터 값인 OrgAndAncestorOrgs는 그룹화 가능 템플리트 정책에서만 작동합니다. 이 예에서, 사용자에게는 자원을 소유하는 조직 또는 조직의 상위 조직에서 판매 관리자, 계정 관리자 또는 판매자 역할이 지정되어 있어야 합니다.

```
<UserCondition><!CDATA[
  <profile>
   <orListCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
      <value data="Sales Manager"/>
       <qualifier name="org" data="OrgAndAncestorOrgs"/>
     </simpleCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
      <value data="Account Representative"/>
       <qualifier name="org" data="OrgAndAncestorOrgs"/>
     </simpleCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
      <value data="Seller"/>
       <qualifier name="org" data="OrgAndAncestorOrgs"/>
     </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 테이블에는 사용자가 ANCESTOR_ID = 100 및 SEQUENCE = 1인 조직에 종속되는 레코드가 있어야 합니다.

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

정책

WC_installdir/xml/policies/xml/defaultAccessControlPolicies.xml 파일은 기본적으로 제공하는 기본 액세스 제어 정책을 정의합니다. 이것은 *WC_installdir*/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. ACPOLICY 테이블의 POLICYNAME 열로 로드됩니다. Name과 OwnerID의 조합은 고유해야 합니다.

OwnerID: 정책을 소유하는 조직 엔티티의 구성원 ID. 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. ACPOLICY 테이블의 mbrgrp_id 열로 로드됩니다. 기본 액세스 그룹은 *WC_installdir*/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. 컨트롤러 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. 뷰의 역할 기반 정책은 ResoureGroupName을 ViewCommandResourceGroup으로 설정합니다.

PolicyType: 정책 유형. 올바른 값은 groupableStandard 및 groupableTemplate입니다. 역 호환성을 위해, standard 및 templete 값도 지원됩니다. 이러한 속성이 새 정책을 로드할 때 지정되지 않으면, 널(Null)값이 사용됩니다. 속성이 기존 정책을 갱신할 때 지정되지 않으면, 값은 변경되지 않은 상태로 남아 있습니다. 다음 테이블은 문자열 값과 ACPOLICY 테이블의 POLICYTYPE 열에 저장된 데이터베이스 값과의 맵핑을 표시합니다.

표 14. 문자열 값과 데이터베이스 값과의 맵핑

String	**ACPOLICY.POLICYTYPE**
groupableTemplate	3
groupableStandard	2
template	1
standard	0 또는 널(Null)값

정책 유형에 대한 추가 정보는 19 페이지의 제 3 장『권한부여 개념』을 참조하십시오.

RelationName(선택): ACRELATION 테이블의 RELATIONNAME 열에 지정된 관계의 이름. 이 이름이 지정되면, ACPOLICY 테이블에 저장된 해당 관계 ID(ACRELATION_ID)를 가져오는 데 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:

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

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

뷰: 이 예에서 MarketingManagers 액세스 그룹에 속한 사용자는 MarketingManagersViews 조치 그룹에 속한 뷰를 실행할 수 있습니다.

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

자원 레벨 정책:

명령: 이 예에서는 사용자가 자원에 대해 creator 관계를 이행하는 한, AllUsers 액세스 그룹에 속한 사용자는 CouponWalletResourceGroup이 지정한 자원에서 CouponRedemption 조치 그룹이 지정한 조치를 수행할 수 있습니다.

```
<Policy Name="AllUsersExecuteCouponRedemptionCommandsOnCouponWalletResource"
   OwnerID="RootOrganization"
   UserGroup="AllUsers"
   ActionGroupName="CouponRedemption"
```

```
   ResourceGroupName="CouponWalletResourceGroup"
   RelationName="creator"
   PolicyType="groupableStandard">
</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"
   PolicyType="groupableStandard">
</Policy>
```

그룹화 가능한 템플리트 정책: 이 예에서 OrgAdminConsoleMembershipAdministratorsForOrg 액세스 그룹에 속한 사용자는 OrganizationDataResourceGroup이 지정한 자원에서 ApproveGroupUpdate 조치 그룹이 지정한 조치를 수행할 수 있습니다.

```
<Policy Name="OrgAdminConsoleMembershipAdministratorsForOrgExecuteApprove
GroupUpdateCommandsOnOrganizationResource"
   OwnerID="RootOrganization"
   UserGroup="OrgAdminConsoleMembershipAdministratorsForOrg"
   ActionGroupName="ApproveGroupUpdate"
   ResourceGroupName="OrganizationDataResourceGroup"
   PolicyType="groupableTemplate">
</Policy>
```

OrgAdminConsoleMembershipAdministratorsForOrg 액세스 그룹의 정의를 조사하여 멤버쉽에 필요한 다음과 같은 조건을 표시합니다.

```
<UserCondition>

 <profile>
    <orListCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
      <value data="Buyer Administrator"/>
      <qualifier name="org" data="OrgAndAncestorOrgs"/>
     </simpleCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
      <value data="Seller Administrator"/>
      <qualifier name="org" data="OrgAndAncestorOrgs"/>
     </simpleCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
      <value data="Channel Manager"/>
      <qualifier name="org" data="OrgAndAncestorOrgs"/>
```

```
    </simpleCondition>
   </orListCondition>
  </profile>
 UserCondition>
```

주: role의 simpleCondition은 org = **OrgAndAncestorOrgs**로 규정됩니다. OrgAndAncestorOrgs는 그룹화 가능 템플리트 정책에만 사용 가능한 키워드입니다. 역할을 현재 자원의 소유자의 컨텍스트로 동적으로 범위를 넓힙니다. 이 예에서 사용자에게는 자원을 소유하는 조직 또는 조직의 상위 조직에 지정된 역할 중 하나가 있어야 합니다.

정책 그룹 정의

정책 그룹은 비즈니스 및 액세스 제어 요구사항에 따라 그룹 정책에 작성됩니다. 일부 기본 정책 그룹은 상자 외부에 작성됩니다. 자세한 정보는 229 페이지의 『기본 액세스 제어 정책 및 그룹』을 참조하십시오. 상점 또는 비즈니스 모델을 공개하는 동안 필요에 따라 다른 정책 그룹이 작성됩니다. 대부분의 경우, 작성한 새 정책을 기본 정책 그룹에 추가하기만 하면 됩니다. 새 정책 그룹을 작성해야 할 경우, defaultAccessControlPolicies.xml과 유사한 XML 파일에 새 정책 그룹을 정의한 후 데이터베이스로 로드해야 합니다. 견본 정의는 다음과 같습니다.

```
<PolicyGroup Name="aValue" OwnerID="aValue">
 </PolicyGroup>
```

여기서

Name: 정책 그룹의 이름.

OwnerID: 정책 그룹을 소유하는 조직 엔티티의 구성원 ID. ACPOLGRP 테이블의 member_id 열로 로드됩니다. OwnerID와 Name의 조합은 고유해야 합니다. 변환기 도구가 인식하는 두 가지 특수 값은 RootOrganization: -2001 및 DefaultOrganization: -2000입니다.

정책 그룹에 정책 연관

정책은 여러 개의 정책 그룹에 속할 수 있습니다. 그러나 정책을 용이하게 관리하기 위해서는 정책이 하나의 정책 그룹에만 속하는 것이 좋습니다. 이러한 연관은 defaultAccessControlPolicies.xml과 유사한 XML 파일에 정의된 후 데이터베이스로 로드되어야 합니다. 견본 정의는 다음과 같습니다.

```
<PolicyGroup Name="aValue" OwnerID="aValue">
  <PolicyGroupPolicy  Name="aValue" PolicyOwnerID="aValue" />
</PolicyGroup>
```

여기서

PolicyGroupPolicy Name: 지정된 정책 그룹과 연관될 이전에 정의한 정책의 이름. 이 정책은 groupableStandard 또는 groupableTemplate의 정책 유형 중 하나여야 합니다.

PolicyGroupPolicy PolicyOwnerID(선택): 지정된 정책을 소유하는 조직 엔티티의 구성원 ID. 이 매개변수가 지정되어 있지 않으면, 기본 값은 정책 그룹의 OwnerID입니다. 변환기 도구가 인식하는 두 가지 특수 값은 RootOrganization: -2001 및 DefaultOrganization: -2000입니다.

정책 그룹에 등록

조직의 자원은 해당 조직이 등록하는 정책 그룹의 정책으로 보호됩니다. 해당 조직이 정책 그룹에 등록하지 않았으면, 해당 조직의 가장 근접한 상위 조직이 등록한 정책 그룹이 적용됩니다. 조직에서 등록해야 하는 정책 그룹에 대한 자세한 정보는 229 페이지의 『기본 액세스 제어 정책 및 그룹』을 참조하십시오.

정책 그룹은 조직 관리 콘솔에서 등록될 수 있으나 defaultAccessControlPolicies.xml과 유사한 XML 파일에 정의되어 데이터베이스에 로드될 수도 있습니다. 견본 정의는 다음과 같습니다.

```
<PolicyGroup Name="aValue" OwnerID="aValue">
  <PolicyGroupSubscription OrganizationID="aValue"/>
 </PolicyGroup>
```

여기서

OrganizationID: 이 정책 그룹에 등록 중인 조직 엔티티의 구성원 ID. 변환기 도구가 인식하는 두 가지 특수 값은 RootOrganization: -2001 및 DefaultOrganization: -2000입니다.

번역 가능한 정책 데이터

다음은 번역 가능한 정책 데이터를 정의하는 데 사용할 수 있는 사용자 정의 정책 파일의 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>
 <PolicyGroup_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. LanguageID 의 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>
 <PolicyGroup>-->
<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_installdir\xml\policies\xml\
defaultAccessControlPolicies_*locale*.xml

예: defaultAccessControlPolicies_ko_KR.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 정의됩니다.

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 열에 저장됩니다.

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"
OwnerID="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.

정책 그룹: 다음 예는 추가 정책 그룹 정보를 정의합니다.

```
<PolicyGroup_nls PolicyGroupName="B2CPolicyGroup" OwnerID="RootOrganization"
DisplayName_nls="B2C Policy Group"
Description_nls="This policy group contains all the B2C specific policies."
/>
```

여기서

PolicyGroupName: 추가 정보가 추가되고 있는 액세스 제어 정책 그룹의 이름. 이 값은 ACPOLGRP 테이블의 NAME 열에 있습니다.

OwnerID: 이 정책 그룹을 소유하는 조직 엔티티의 구성원 ID.

DisplayName_nls: 정책 그룹의 표시 이름. 이 값은 ACPLGPDESC 테이블의 DISPLAYNAME 열에 저장됩니다.

Description_nls: 정책 그룹의 선택적인 설명. 이 값은 ACPLGPDESC 테이블의 DESCRIPTION 열에 저장됩니다.

XML 파일을 변경한 후

변경사항 테스트

변경사항 테스트에 대해서는 115 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 프로세스는 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:

1. 사용자 정의된 XML 파일을 작성할 경우, 이 파일을 *<WC_installdir>*/xml/policies/xml 디렉토리에 복사하여 데이터베이스에 로드해야 합니다.
2. ID를 분석하여 데이터베이스에 데이터를 로드하는 중에 다음 매개변수 설정을 지정하는 로드 중인 스크립트에 설정이 있습니다. "-maxerror 100000". 데이터를 로드하는 동안 최대 100000개의 위반이 있는 경우 중단하지 않고 무시한다는 의미입니다. 이 값은 필요에 따라 증가 또는 감소될 수 있습니다. 예를 들어, 이러한 오류가 발생한 후에 중지하려면, 값을 1로 변경하십시오.

400 의 경우, 사용자 정의된 XML 파일을 작성하려면 파일에서 DTD에 대한 전체 경로를 사용해야 합니다. 액세스 제어 정책 DTD는 *WC_installdir*/xml/policies/dtd에 위치 지정됩니다.

액세스 그룹과 액세스 제어 정책을 로드하려면, 다음 명령을 실행하십시오.

2000 의 경우

1. *<WC_installdir>*\bin 디렉토리에서 여기에 표시된 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>*[*schema name*]
     (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*>[*schema name*]
  (**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*>[*schema name*]
  (**예**: acpnlsload mall dbuser dbusrpwd defaultaccesscontrolpolicies_en_US.xml)

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

400 AIX Solaris Linux 의 경우

다음 단계로 진행하기 위해 데이터베이스 사용자 ID에는 다음과 같은 권한이 있어야 합니다.

- *WC_installdir*/xml/policies 및 *WC_installdir*/logs의 디렉토리, 서브디렉토리 및 파일에 대한 읽기/쓰기/실행 권한.
- *WC_installdir*/bin 디렉토리 및 해당 파일에 대한 읽기/실행 권한.

데이터베이스 사용자 ID에 위와 같은 필수 권한이 없는 경우, chmod 명령을 사용하여 이 권한을 부여해야 합니다.

1. 데이터베이스 사용자 ID로 로그인하십시오.
2. <*WC_installdir*>/bin 디렉토리에서 여기에 표시된 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*>[*schema name*]
   (**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*>[*schema name*]
   (**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*>[*schema name*]
   (**예**: acpnlsload mall dbuser dbusrpwd defaultaccesscontrolpolicies_en_US.xml)

오류를 보려면 <*WC_installdir*>/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 의 경우

주: 400 의 경우 로그 파일은 *WC_userdir*/instances에 위치 지정됩니다.

데이터베이스에서 XML 파일로 정책 및 액세스 그룹 정의 추출

추출 프로세스는 액세스 제어 데이터베이스에서 정책 및 액세스 그룹 정보를 읽고 XML 형식으로 정보를 캡처하는 파일을 작성합니다. 추출 유틸리티에서는 데이터베이스에서 추출할 데이터를 지정하기 위해 입력 필터 XML 파일을 사용합니다. 다음과 같은 필터 파일이 제공됩니다.

- ACPoliciesfilter.xml: 모든 액세스 그룹 및 정책 데이터를 추출하는 데 사용합니다.
- ACUserGroupsFilter.xml: 모든 액세스 그룹 데이터를 추출하는 데 사용합니다.
- OrganizationPoliciesFilter.xml: 특정 조직의 모든 액세스 그룹 및 정책 데이터를 추출하는 데 사용합니다. 이 파일을 사용하기 전에 필수 조직 ID를 지정하도록 편집해야 합니다. 이 조직 ID에서 소유하는 정책 데이터가 추출됩니다.

NT 2000 의 경우

1. <*WC_installdir*\bin 디렉토리에서 다음 acpextract 명령을 실행하십시오.

   ```
   acpextract.cmd <database name> <database user> <database user password>
   <input xml filter file> [schema name]
   ```

   (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 프로세스 오류를 보려면 <*WC_installdir*>\logs\acpextract.log 로그 파일을 확인하십시오.

400 AIX Solaris Linux 의 경우

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

   ```
   acpextract.sh <database name> <database user>
   <database user password> <input xml filter file> [schema name]
   ```

   예:

   ```
   acpextract.sh 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
3. 발생했을 수 있는 프로세스 오류를 보려면 *<WC_installdir>*\logs\acpextract.log 로그 파일을 확인하십시오.

▶ 400 의 경우

1. 다음 파일은 OUTDIR 매개변수를 사용하여 *WC_installdir*/xml/policies/xml 디렉토리에서 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

제 4 부 Payments 보안

이 부분에서는 Payments 보안 관리 태스크에 대해 설명합니다.

제 14 장 WebSphere Commerce Payments 액세스

WebSphere Commerce Payments는 범주(realm)를 지정하여 사용자를 인증합니다. 범주는 사용자 인증의 단일 메소드(예: 사용자 이름과 암호)를 갖는 사용자의 레지스트리입니다. 각 WebSphere Commerce Payments 설치는 한 번에 단 하나의 범주만을 사용할 수 있습니다. 범주 유형의 예에는 LDAP 범주와 운영체제 범주가 포함됩니다. 사용자는 범주에 정의되어야 자원에 대한 액세스가 부여될 수 있습니다. 사용자는 다음이 모두 해당하는 경우에만 올바른 WebSphere Commerce Payments 사용자입니다.

- 범주에 있습니다.
- WebSphere Commerce Payments에서 역할이 지정되었습니다.

WebSphere Commerce Payments은 다음 4가지 WebSphere Commerce Payments 역할을 정의하는 역할 기반 액세스 제어 설계를 채택합니다.

1. 지불 관리자
2. 판매자 관리자
3. 감독자
4. 점원

지불 관리자는 WebSphere Commerce Payments 사용자 인터페이스 사용자 창을 사용하여 범주에 정의된 사용자에게 액세스(역할 기준)를 지정할 수 있습니다. WCSRealm은 WebSphere Commerce Payments에서 제공됩니다. WCSRealm 클래스는 사용자 시스템에 대해 자동으로 구성됩니다. 이 범주에서 WebSphere Commerce Payments Servlet은 WebSphere Commerce 사용자 테이블에 이미 등록된 운영자 정보를 사용할 수 있습니다. 이 운영자 정보가 지불 관리자에 대해 사용되므로 WebSphere Commerce Payments 사용자 인터페이스를 사용하기 위해 운영자 ID의 다른 세트를 정의할 필요가 없습니다.

제 15 장 WebSphere Commerce Payments 보안 유지보수

WebSphere Commerce Payments 보안은 여러 키 보안 요소에 빌드됩니다. 이들 요소는 결합하여 서비스를 웹에서 안전하게 전개할 수 있는 환경을 작성합니다.

주: IBM WebSphere Commerce Payments(이하에서는 WebSphere Commerce Payments)를 이전에는 Payment Manager라고 했습니다. 버전 3.1.3에서 지불 응용프로그램이 WebSphere Commerce Payments로 이름이 변경되었으며 제품에 대한 참조가 이 책의 전체에서 변경되었습니다.

WebSphere Commerce Payments 보호

WebSphere Commerce Payments의 중심에 Payment Servlet이 있습니다. 여러 부수적인 제품, WebSphere Application Server로 구성되는 웹 서버, 데이터베이스 및 사용자 인터페이스가 WebSphere Commerce Payments을 완성합니다. 이 장에서는 다양한 WebSphere Commerce Payments 구성요소 보안을 위한 메소드에 대해 설명합니다.

중요한 데이터 보호

각 조회 명령에 대해 프레임워크는 최소 역할에 대한 사용자의 역할을 검증하고 역할에 따라 QueryRequest 오브젝트에 신용 카드 번호 또는 지불 청구 주소 같은 중요한 데이터가 전체 뷰로 리턴되는지 아니면 마스크로 가려져야 하는지 여부를 표시하는 지시자를 설정합니다. WebSphere Commerce Payments 프레임워크는 조회 명령을 통해 리턴할 수 있는 어떤 중요한 데이터도 유지보수하지 않습니다. 그러나 이 지시자의 값을 확인하고 중요한 데이터를 표준화된 방법으로 마스크하기 위해 카세트 작성자에게 새로운 방법이 제공됩니다. 각 카세트는 중요한 데이터를 나머지 저장된 데이터로부터 구별해야 합니다. 일반적으로, 중요한 데이터는 카세트가 WebSphere Commerce Payments 데이터베이스에 저장하기 전에 암호화하는 동일한 데이터 세트입니다.

JVM 시스템 매개변수 `wpm.MinSensitiveAccessRole={clerk|supervisor|madmin|psadmin|none}`이 중요한 데이터에 대한 액세스를 허용하기 위해 사용자가 가져야 하는 최소 역할을 지정합니다. 값은 대소문자를 구분합니다. 이 특성을 지정하지 않으면 clerk 값이 가정되어 모든 사용자가 중요한 데이터를 볼 수 있습니다. 올바르지 않은 값을 지정하는 경우 Payment Servlet이 초기화하는 데 실패합니다.

이 매개변수는 Payment 인스턴스 작성 중에 설정되므로 WebSphere Commerce 구성 관리자를 사용하여 언제든지 갱신할 수 있다는 점에 유의하십시오. 구성 관리자의 매개변수 이름은 Payment 인스턴스 패널의 최소 액세스 역할입니다. 구성 관리자 패널에

대한 자세한 정보는 해당 플랫폼의 *WebSphere Commerce 설치 안내서* 또는 구성 관리자에 있는 동안의 Payment 인스턴스 패널에 관한 온라인 도움말을 참조하십시오.

다음 테이블은 지원되는 값을 설명하는데, 값은 권한의 오름 차순으로 표시됩니다.

표 15. Payments 사용자 역할 권한

사용자	설명
점원	점원 이상의 역할을 갖는 사용자가 중요한 데이터를 볼 수 있습니다.
감독자	감독자 이상의 역할을 갖는 사용자가 중요한 데이터를 볼 수 있습니다.
madmin	판매자 관리자 이상의 역할을 갖는 사용자가 중요한 데이터를 볼 수 있습니다.
psadmin	지불 관리자만이 중요한 데이터를 볼 수 있습니다.
없음	누구도 중요한 데이터를 볼 수 없습니다.

WebSphere Commerce 구성 관리자를 통해 `wpm.MinSensitiveAccessRole` 매개변수를 지정할 수 있습니다.

데이터베이스 보호

WebSphere Commerce Payments 데이터베이스는 중요한 데이터를 저장하며 권한이 없는 소스의 읽기 및 쓰기에 대한 보호가 필요합니다. WebSphere Commerce Payments은 데이터베이스에 저장되는 중요한 데이터(예: 암호 및 카드 소유자 정보)의 암호화에 대한 지원을 제공합니다.

트랜잭션 데이터

다음은 트랜잭션 데이터 취급에 대한 지침입니다.

- 중요한 트랜잭션 정보는 인스턴스 라이브러리의 데이터베이스 테이블에 저장됩니다. 이 라이브러리가 Payments 인스턴스 작성 마법사에서 인스턴스 스키마 이름으로 지정됩니다.
- 모든 백업은 안전하게 보관되어야 합니다.
- 인스턴스 라이브러리의 데이터베이스 테이블에는 중요한 구성 및 트랜잭션 정보가 들어있으며 시스템 백업 전략의 일부로서 포함되어야 합니다. 또한 다음을 백업해야 합니다.
  - 인스턴스 이름이 WebSphere Commerce Payments인 `/QIBM/UserData/CommercePayments/V55/instance` 디렉토리의 파일.
  - WebSphere Commerce Payments에 대해 구성한 HTTP 서버 인스턴스. 이 HTTP 서버가 Payments 인스턴스 작성 마법사에서 웹 서버로 지정됩니다.
  - 로컬 시스템의 인스턴스 라이브러리의 오브젝트뿐 아니라, 원격 데이터베이스 기억장치가 사용되는 원격 시스템의 데이터베이스 콜렉션.

제 5 부 기타 보안 관련 주제

이 부분에서는 WebSphere Commerce 시스템 관리자가 수행할 수 있는 기타 보안 태스크에 대해 설명합니다.

제 16 장 WebSphere Application Server 보안 사용

이 장에서는 WebSphere Application Server에 대한 보안 기능을 사용하는 방법에 대해 설명합니다. WebSphere Application Server 보안을 사용하면 모든 Enterprise JavaBeans 구성요소가 다른 사람의 원격 호출에 노출되지 않습니다.

주:

1. Windows WebSphere Application Server 글로벌 보안을 이 장의 단계에서 설명한 대로 사용하면 Windows 2000 Services 패널에서 WebSphere Application Server 서버(예: server1)를 중지시킬 수 없습니다. 보안이 사용될 때 서비스를 중지하려면 다음과 같이 명령 프롬프트에서 WAS_*installdir*\bin 디렉토리의 stopserver 명령을 사용하십시오.

   ```
   stopserver server -username user_id -password password
   ```

   여기서 *server*는 중지하려는 서버(예: server1)의 WebSphere Application Server 구성 디렉토리의 이름이며, 보안이 서버에서 사용되는 경우 *user_id*는 인증용 사용자 이름이며, 보안이 서버에서 사용되는 경우 *password*는 인증용 암호입니다.

   서비스 패널에서 서버를 중지하려고 하면 특성에는 사용자 ID 및 암호가 포함되지 않습니다. 글로벌 보안이 사용되면, 서버를 중지할 때 사용자 ID 및 암호에는 모두 인증이 필요합니다. 서비스를 계속 실행합니다(서비스 패널에서 서비스가 중지되었음을 표시함에도 불구하고). 서비스 패널에서 서비스를 시작하는 데에는 사용자 ID 및 암호가 필요하지 않음에 유의하십시오.

2. WebSphere Application Server 보안을 사용할 때 응용프로그램 서버를 중지해야 할 경우, 다음과 같이 명령 프롬프트에서 WAS_*installdir*/bin 디렉토리의 stopserver 명령을 사용하십시오.

   AIX Linux Solaris

   ```
   stopserver server -username user_id -password password
   ```

   여기서 *server*는 중지하려는 WebSphere Application Server 응용프로그램 서버(예: server1)의 이름이고 *user_id*는 인증을 위한 사용자 이름이며 *password*는 인증을 위한 암호입니다.

   400

   ```
   stopserver -instance WAS_instancename server -username user_id
      -password password
   ```

여기서 *WAS_instancename*은 WebSphere Application Server 인스턴스의 이름이고, *server*는 중지하려는 WebSphere Application Server 응용프로그램 서버(예: server1)의 이름이며, *user_id*는 인증을 위한 사용자 이름, *password*는 인증을 위한 암호입니다.

3. AIX Linux Solaris Windows WebSphere Application Server 보안을 사용할 때, 사용자 시스템이 다음 요구사항을 만족시켜야 합니다.
   - 최소 1GB 시스템 메모리
   - WebSphere Commerce 응용프로그램을 위한 최소 384MB의 힙 크기

시작하기 전에

보안 사용을 시작하기 전에 보안을 사용하려는 WebSphere Application Server가 사용자 ID의 유효성을 검증하는 방법을 알아야 합니다. WebSphere Application Server는 LDAP 또는 운영체제의 사용자 레지스트리를 WebSphere Application Server 사용자 레지스트리로 사용할 수 있습니다.

LDAP 사용자 레지스트리를 사용한 보안 사용

AIX Solaris Linux LDAP을 WebSphere Application Server 사용자 레지스트리로 사용 중일 때 WebSphere Application Server 보안을 사용하려면, wasuser ID로서 시스템에 로그인하고 다음 단계를 수행하십시오.

400 LDAP을 WebSphere Application Server 사용자 레지스트리로 사용 중일 때 WebSphere Application Server 보안을 사용하려면 시스템에 로그인하고 다음 단계를 수행하십시오.

Windows LDAP을 WebSphere Application Server 사용자 레지스트리로 사용 중일 때 WebSphere Application Server 보안을 사용하려면 관리자 권한이 있는 사용자로서 시스템에 로그인하고 다음 단계를 수행하십시오.

1. WebSphere Application Server를 시작하고 WebSphere Application Server 관리 콘솔을 여십시오.
2. 관리 콘솔에서 글로벌 보안 설정을 다음과 같이 수정하십시오.
   a. **보안**에서 **사용자 레지스트리**를 펼치고 **LDAP**을 누르십시오. 사용 중인 디렉토리 서버의 유형에 따라서 다음과 같이 **구성** 탭의 필드를 채우십시오.

표 16. *IBM Directory Server 사용자.* AIX 400 Linux Solaris Windows

필드 이름	정의	견본 값	주
서버 사용자 ID	사용자 ID	*user_ID*	• 이것은 LDAP 운영자가 아니어야 합니다. • cn=xxx로 지정된 사용자를 사용하지 마십시오. • 이 사용자의 오브젝트 클래스가 LDAP 고급 특성 창의 사용자 필터 필드에 지정된 오브젝트 클래스와 호환되어야 합니다.
서버 사용자 암호	사용자 암호	*password*	
유형	LDAP 서버의 유형	SecureWay	
호스트	LDAP 서버의 호스트 이름	*hostname.domain.com*	
포트	LDAP 서버가 사용 중인 포트		이 필드는 필수가 아닙니다.
기본 인식 이름	검색이 발생하는 인식 이름	o=ibm,c=us	
바인드 인식 이름	검색할 때 디렉토리에 바인드하기 위한 인식 이름		이 필드는 필수가 아닙니다.
바인드 암호	바인드 인식 이름에 대한 암호		이 필드는 필수가 아닙니다.

표 17. *Netscape 사용자.* Windows

필드 이름	정의	견본 값	주
서버 사용자 ID	사용자 ID	*user_ID*	• 이것은 LDAP 운영자가 아니어야 합니다. • cn=xxx로 지정된 사용자를 사용하지 마십시오. • 이 사용자의 오브젝트 클래스가 LDAP 고급 특성 창의 사용자 필터 필드에 지정된 오브젝트 클래스와 호환되어야 합니다.
서버 사용자 암호	사용자 암호	*password*	
유형	LDAP 서버의 유형	Netscape	
호스트	LDAP 서버의 호스트 이름	*hostname.domain.com*	

표 17. *Netscape 사용자 (계속).* Windows

필드 이름	정의	견본 값	주
포트	LDAP 서버가 사용 중인 포트		이 필드는 필수가 아닙니다.
기본 인식 이름	검색이 발생하는 인식 이름	o=ibm	
바인드 인식 이름	검색할 때 디렉토리에 바인드하기 위한 인식 이름		이 필드는 필수가 아닙니다.
바인드 암호	바인드 인식 이름에 대한 암호		이 필드는 필수가 아닙니다.

표 18. *Domino™ 사용자.* Windows

필드 이름	정의	견본 값	주
서버 사용자 ID	짧은 이름/사용자 ID	*user_ID*	이 사용자의 오브젝트 클래스가 LDAP 고급 특성 창의 사용자 필터 필드에 지정된 오브젝트 클래스와 호환되어야 합니다.
서버 사용자 암호	사용자 암호	*password*	
유형	LDAP 서버의 유형	Domino 5.0	
호스트	LDAP 서버의 호스트 이름	*hostname.domain.com*	
포트	LDAP 서버가 사용 중인 포트		이 필드는 필수가 아닙니다.
기본 인식 이름	검색이 발생하는 인식 이름		이 필드는 필수가 아닙니다.
바인드 인식 이름	검색할 때 디렉토리에 바인드하기 위한 인식 이름		이 필드는 필수가 아닙니다.
바인드 암호	바인드 인식 이름에 대한 암호		이 필드는 필수가 아닙니다.

표 19. *활성 디렉토리 사용자.* Windows

필드 이름	정의	견본 값	주
서버 사용자 ID	sAMAccountName	*user_ID*	• 모든 일반 사용자의 사용자 로그온 이름. • cn=xxx로 지정된 사용자를 사용하지 마십시오. • 이 사용자의 오브젝트 클래스가 LDAP 고급 특성 창의 사용자 필터 필드에 지정된 오브젝트 클래스와 호환되어야 합니다.

표 19. 활성 디렉토리 사용자 (계속). Windows

필드 이름	정의	견본 값	주
서버 사용자 암호	사용자 암호	*password*	
유형	LDAP 서버의 유형	Active Directory	
호스트	LDAP 서버의 호스트 이름	*hostname.domain.com*	
포트	LDAP 서버가 사용 중인 포트		이 필드는 필수가 아닙니다.
기본 인식 이름	검색이 발생하는 인식 이름	CN=users, DC=domain1, DC=domain2, DC=com	
바인드 인식 이름	검색할 때 디렉토리에 바인드하기 위한 인식 이름	CN=*user_ID*, CN=users, DC=domain1, DC=domain2, DC=com	*user_ID* 값은 표시 이름입니다. 이것이 사용자 로그온 이름과 반드시 같지는 않습니다.
바인드 암호	바인드 인식 이름에 대한 암호	*bind_password*	이것은 보안 서버 암호와 동일해야 합니다.

적용을 누른 후 **저장**을 누르십시오.

b. 관리 콘솔에서 **보안**을 펼치고 **글로벌 보안**을 누르십시오.

1) 글로벌 보안 구성 탭에서 **사용**을 선택하고 **Java 2 보안 시행**을 선택하십시오.

주: WebSphere Commerce 5.5에서는 Java 2 보안을 지원하지 않습니다.

2) 활성 인증 메커니즘 필드에서 **LTPA(Lightweight Third Party Authentication)**를 선택하십시오.

3) 활성 사용자 레지스트리 필드에서 **LDAP**를 선택하십시오.

4) **적용**을 누른 후 **저장**을 누르십시오.

c. 관리 콘솔에서 **보안**을 펼치고, **인증 메커니즘**을 펼친 후 **LTPA**를 누르십시오.

1) LPTA 구성 탭에서 필요한 대로 LTPA 설정을 채우십시오.

2) 추가 특성에서 **단일 사인온(SSO)**을 누른 후 이 기능을 사용하지 않으려면 **사용** 선택란을 지우십시오.

3) **적용**을 누른 후 **저장**을 누르십시오.

d. 관리 콘솔에서 **응용프로그램**을 펼친 후 **엔터프라이즈 응용프로그램**을 누르십시오.

1) 엔터프라이즈 응용프로그램 창에서 Commerce 응용프로그램인 **WC_***instance_name*(예: WC_demo)을 누르십시오.

2) 추가 특성에서 **보안 역할을 사용자/그룹에 맵**을 누르십시오.

3) **사용자 찾아보기**를 누르고 그의 역할을 맵핑하려는 사용자를 찾으십시오.

4) 해당 사용자에 대해, **WCSecurityRole**을 선택하고 **확인**을 누르십시오.

3. 관리 콘솔을 닫고 WebSphere Application Server 관리 콘솔을 중지한 후 다시 시작하십시오. 이제부터 WebSphere Application Server 관리 콘솔을 열 때 보안 서버 ID와 암호를 입력하도록 프롬프트가 표시됩니다
4. WebSphere Commerce 구성 관리자를 열고 **인스턴스** > *instance_name* > **인스턴스 특성** > **보안**을 선택하고 **사용** 선택란을 누르십시오. 203 페이지의 2b단계에서 입력한 사용자 이름과 암호를 입력하도록 프롬프트가 표시됩니다. **적용**을 누른 후 구성 관리자를 종료하십시오.
5. WebSphere Application Server 관리 콘솔을 중지한 후 다시 시작하십시오.

운영체제 사용자 레지스트리를 사용한 보안 사용

AIX Linux Solaris 운영체제를 사용자 레지스트리로 사용하려면 WebSphere Application Server가 `root` ID로 실행되어야 합니다. `root`로 WebSphere Application Server를 실행하고 다음 단계를 수행하십시오.

400 Windows 운영체제 사용자 유효성 검증을 WebSphere Application Server 사용자 레지스트리로 사용 중일 때 WebSphere Application Server 보안을 사용하려면 관리자 권한을 갖는 사용자로 로그인하고 다음 단계를 수행하십시오.

1. AIX Linux Solaris root로 로그인하십시오.
2. AIX Linux Solaris `root`로 로그인하고 있는 동안 WebSphere Application Server를 시작하고 WebSphere Application Server 관리 콘솔을 실행하십시오. 서버를 시작하려면 다음을 수행하십시오.

   ```
   cd WAS_installdir/bin
   ./startServer server
   ```

   여기서 *server*는 WebSphere Application Server 응용프로그램 서버의 이름입니다 (예: `server1`).
3. WebSphere Application Server 관리 콘솔에서 다음과 같이 글로벌 보안 설정을 수정하십시오.
   a. 관리 콘솔에서 **보안**을 펼치고, **사용자 레지스트리**를 펼친 후 **로컬 OS**를 누르십시오. 보안 레지스트리 서버에 대해 다음과 같이 **구성** 탭의 필드를 채우십시오.

필드 이름	견본 값	주
서버 사용자 ID	*wcsuser*	400 iSeries의 사용자 ID에는 *SECOFR 권한이 있어야 합니다. AIX Solaris Linux root나 root 권한을 갖는 사용자 ID. Windows 사용자가 로그인한 운영체제 관리자 권한을 갖는 사용자 ID. 시스템이 도메인에 속하는 경우, 완전한 사용자 ID를 사용하십시오. 예를 들면, *DomainXYZ\user_id*. 이 계정이 도메인 서버에 존재하고 운영자 그룹의 구성원인지 확인하십시오.
보안 서버 암호	*password*	이것은 사용자가 로그인시 사용한 운영체제 관리자 권한을 갖는 사용자에 속하는 암호입니다.

적용을 누른 후 **저장**을 누르십시오.

b. 관리 콘솔에서 **보안**을 펼치고 **글로벌 보안**을 누르십시오.

1) 글로벌 보안 구성 탭에서 **사용**을 선택하고 **Java 2 보안 시행**을 선택하십시오.

2) 활성 인증 메커니즘 필드에서 **SWAM(Simple WebSphere Authentication Mechanism)**을 선택하십시오.

3) 활성 사용자 레지스트리 필드에서 **로컬 OS**를 선택하십시오.

4) **적용**을 누른 후 **저장**을 누르십시오.

4. 관리 콘솔에서 **응용프로그램**을 펼친 후 **엔터프라이즈 응용프로그램**을 누르십시오.

a. 엔터프라이즈 응용프로그램 창에서 Commerce 응용프로그램인 **WC_***instance_name*(예: WC_demo)을 누르십시오.

b. 추가 특성에서 **보안 역할을 사용자/그룹에 맵**을 누르십시오.

c. **사용자 찾아보기**를 누르고 그의 역할을 맵핑하려는 사용자를 찾으십시오.

d. 해당 사용자에 대해 **WCSecurityRole**을 선택하고 **확인**을 누르십시오.

5. WebSphere Commerce 구성 관리자를 열고 **인스턴스 목록** → *instance_name* → **인스턴스 특성** → **보안**을 선택하고 **보안 사용** 선택란을 선택하십시오. 인증 모드에 대한 **운영체제 사용자 레지스트리**를 선택하고 204 페이지의 3a단계에서 입력한 사용자 이름과 암호를 입력하십시오. **적용**을 누른 후 구성 관리자를 종료하십시오.

6. WebSphere Application Server 관리 서버를 중지한 후 다시 시작하십시오. 이제부터 WebSphere Application Server 관리 콘솔을 열 때 보안 서버 ID와 암호를 입력하도록 프롬프트가 표시됩니다

WebSphere Commerce EJB 보안 사용 안함

WebSphere Commerce Business Edition에서는 EJB 보안을 사용하지 않을 수 있습니다. WebSphere Commerce EJB 보안을 사용하지 않으려면, 다음을 수행하십시오.

1. WebSphere Application Server 관리 콘솔을 시작하십시오
2. 관리 콘솔에서 **보안**을 펼치고 **글로벌 보안**을 누르십시오. 글로벌 보안 구성 탭에서 **사용** 선택란을 지우십시오.
3. WebSphere Commerce 구성 관리자를 열고 **인스턴스 목록** → *instance_name* → **인스턴스 특성** → **보안**을 선택한 후 **보안 사용** 선택란을 지우십시오.
4. WebSphere Application Server 관리 콘솔을 종료하십시오.
5. WebSphere Application Server 관리 서버를 중지한 후 다시 시작하십시오.

WebSphere Commerce 보안 전개 옵션

WebSphere Commerce는 다양한 보안 전개 구성을 지원합니다. 다음 표에서는 사용자가 사용할 수 있는 보안 전개 옵션에 대해 설명합니다.

표 20. 단일 시스템 보안 시나리오

WebSphere Application Server 보안이 사용됩니다.	• 운영체제를 WebSphere Application Server 레지스트리로 사용하십시오. • 데이터베이스를 WebSphere Commerce 레지스트리로 사용하십시오.
	• LDAP을 WebSphere Application Server 레지스트리로 사용하십시오. • LDAP을 WebSphere Commerce 레지스트리로 사용하십시오
	• LDAP을 WebSphere Application Server 레지스트리로 사용하십시오.
WebSphere Application Server 보안이 사용되지 않고 WebSphere Commerce 사이트가 방화벽 밖에 있습니다.	• WebSphere Application Server 레지스트리가 필수가 아닙니다. • 데이터베이스를 WebSphere Commerce 레지스트리로 사용하십시오.
	• WebSphere Application Server 레지스트리가 필수가 아닙니다. • LDAP을 WebSphere Commerce 레지스트리로 사용하십시오.

표 21. 복수 시스템 보안 시나리오

WebSphere Application Server 보안이 사용됩니다. LDAP이 항상 전개됩니다.	• LDAP을 WebSphere Application Server 레지스트리로 사용하십시오. • LDAP을 WebSphere Commerce 레지스트리로 사용하십시오
	• LDAP을 WebSphere Application Server 레지스트리로 사용하십시오. • 데이터베이스를 WebSphere Commerce 레지스트리로 사용하십시오. • LDAP을 설정하고 LDAP 레지스트리에 하나의 관리 항목을 배치해야 합니다.
WebSphere Application Server 보안이 사용되지 않고 WebSphere Commerce 사이트가 방화벽 밖에 있습니다.	• 데이터베이스를 WebSphere Commerce 레지스트리로 사용하십시오. • WebSphere Application Server 레지스트리가 필수가 아닙니다. • 단일 사인온이 지원되지 않습니다.
	• LDAP을 WebSphere Application Server 레지스트리로 사용하십시오. • WebSphere Application Server 레지스트리가 필수가 아닙니다.

주: WebSphere Commerce 사이트를 방화벽 밖에서 운영하는 경우, WebSphere Application Server 보안을 사용하지 않을 수 있습니다. 방화벽 밖에서 악성 응용프로그램이 실행 중이 아니라고 확신하는 경우에만 WebSphere Application Server 보안을 사용하지 않아야 합니다.

동적 캐시 모니터의 보안 구성

모니터할 WebSphere Application Server 동적 캐시 모니터를 사용 중이고 모니터링 중인 응용프로그램에서 보안 역할이 해당 전개 설명자에 정의되어 있으면 다음을 수행해야 합니다.

WebSphere Application Server 관리 콘솔에서 ″단계: 사용자/그룹에 보안 역할 맵핑″ 패널을 탐색하려면, **응용프로그램 -> 새 응용프로그램 설치**를 누른 후 필수 단계(비보안 관련)를 완료하십시오. (자세한 정보는 WebSphere Application Server 정보 센터 (`http://www.ibm.com/software/webservers/appserv/infocenter.html`)에서 ″보안 응용프로그램 전개″ 및 ″역할에 사용자및 그룹 지정″을 참조하십시오. ″단계: 사용자/그룹에 보안 역할 맵핑″ 패널에서 다음을 수행하십시오.

1. 각 보안 역할에 맵핑되는 사용자 및 그룹을 지정하십시오.

2. 모든 역할을 선택하거나 개별 역할을 선택하는 데 필요한 **역할** 옆의 선택란을 선택하십시오. 역할마다 사전 정의된 사용자(예: Everyone 또는 모든 인증된 사용자)가 역할에 맵핑되는지 여부를 지정할 수 있습니다. 사용자 레지스트리에서 특정 사용자 또는 그룹을 선택하려면 다음을 수행하십시오.
   a. 역할을 선택한 후 **사용자 찾아보기** 또는 **그룹 찾아보기**를 누르십시오.
   b. 표시된 **사용자 찾아보기** 또는 **그룹 찾아보기** 패널에서 검색 기준을 입력하여 사용자 레지스트리로부터 사용자 또는 그룹 목록을 추출하십시오.
   c. 표시된 결과에서 개별 사용자 또는 그룹을 선택하십시오.
   d. 선택한 사용자 또는 그룹을 "단계: 사용자/그룹 패널에 보안 역할 맵핑"에서 선택한 역할에 맵핑하려면 **확인**을 누르십시오.

현재 모든 캐시 모니터 기능에 액세스할 수 있는 하나의 정의된 역할이 있습니다. 동적 캐시 모니터에 액세스할 수 있는 사용자를 지정하는 데 이 페이지를 사용할 수 있다는 의미입니다.

구성 관리자를 통해 WebSphere Commerce 인스턴스 관리

WebSphere Application Server 글로벌 보안을 사용했으면 구성 관리자를 사용하여 WebSphere Commerce 또는 WebSphere Commerce Payments 인스턴스를 적절하게 중지, 시작, 작성 또는 삭제할 수 있도록 다음 단계를 수행해야 합니다.

1. *WAS_installdir*/properties 디렉토리에서 다음 파일 및 특성을 다음 값으로 갱신하십시오.
   - sas.client.props

     com.ibm.CORBA.securityEnabled=true

     com.ibm.CORBA.loginSource=properties

     com.ibm.CORBA.LoginUserid=validUser

     com.ibm.CORBA.LoginPassword=validPassword
   - soap.client.props

     com.ibm.SOAP.loginUserid=validUser

     com.ibm.SOAP.loginPassword=validPassword

     com.ibm.SOAP.secrityEnabled=true
2. *WAS_installdir*/bin 디렉토리에서 PropFilePasswordEncoder 명령(한 행에 입력)을 실행하여 sas.client.props 및 soap.client.props 파일에서 암호를 인코드하십시오.

AIX Linux Solaris

```
PropFilePasswordEncoder.sh WAS_installdir/properties/
   sas.client.props com.ibm.CORBA.LoginPassword

PropFilePasswordEncoder.sh WAS_installdir/properties/
   soap.client.props com.ibm.SOAP.loginPassword
```

400

```
PropFilePasswordEncoder.sh WAS_userdir/WAS_instance/properties/
   sas.client.props com.ibm.CORBA.LoginPassword

PropFilePasswordEncoder.sh WAS_userdir/WAS_instance/properties/
   soap.client.props com.ibm.SOAP.loginPassword
```

Windows

```
PropFilePasswordEncoder.bat WAS_installdir\properties\
   sas.client.props com.ibm.CORBA.LoginPassword

PropFilePasswordEncoder.bat WAS_installdir\properties\
   soap.client.props com.ibm.SOAP.loginPassword
```

3. 다음과 같이 config_client 스크립트를 갱신하십시오.

   AIX 400 Linux Solaris $CLIENTSOAP $CLIENTSAS를 Java 인수 목록에 추가하십시오. 예를 들면 다음과 같습니다.

   ```
   ${JAVA_EXE?} -classpath $CLASSPATH -DIDIR="$WPMDIR"
   -Djava.security.policy="config.policy" -Djava.version="1.3"
   -Dwas.install.root="$WAS_HOME " -Dwas.repository.root="$CONFIG_ROOT"
   -Dcom.ibm.CORBA.BootstrapHost="$COMPUTERNAME" $CLIENTSOAP $CLIENTSAS
   $PM_ARGS -Xmx128m com.ibm.commerce.config.client.CMClient "$@"
   ```

   Windows %CLIENTSOAP% %CLIENTSAS%를 Java 인수 목록에 추가하십시오. 예를 들면 다음과 같습니다.

   ```
   "%JAVA_HOME%\bin\java" %CLIENTSOAP% %CLIENTSAS% %PM_ARGS% "
   -Dwas.install.root=%WAS_HOME%" "-Dwas.repository.root=%CONFIG_ROOT%"
   -Dcom.ibm.CORBA.BootstrapHost=%COMPUTERNAME%
   -Djava.security.policy="config.policy"
   com.ibm.commerce.config.client.CMClient %*
   ```

4. 다음과 같이 config_server 스크립트를 갱신하십시오.

   AIX 400 Linux Solaris $CLIENTSOAP $CLIENTSAS를 Java 인수 목록에 추가하십시오. 예를 들면 다음과 같습니다.

   ```
   ${JAVA_EXE?} -classpath $CLASSPATH -DIDIR="$WPMDIR"
   -Djava.security.policy="config.policy"
   -Dwas.install.root="$WAS_HOME " -Dwas.repository.root="$CONFIG_ROOT"
   -Dws.ext.dirs="$WAS_EXT_DIRS" -Dcom.ibm.CORBA.BootstrapHost="$COMPUTERNAME"
   $CLIENTSOAP $CLIENTSAS $PM_ARGS $MAX_HEAP
   com.ibm.commerce.config.server.CMServerImpl "$@"
   ```

   Windows %CLIENTSOAP% %CLIENTSAS%를 Java 인수 목록에 추가하십시오. 예를 들면 다음과 같습니다.

```
"%JAVA_HOME%\bin\java.exe" %CLIENTSOAP% %CLIENTSAS% %PM_ARGS%
"-Dwas.install.root=%WAS_HOME%" "-Dwas.repository.root=%CONFIG_ROOT%"
"-Dws.ext.dirs=%WAS_EXT_DIRS%" -Dcom.ibm.CORBA.BootstrapHost=%COMPUTERNAME%
-Djava.security.policy="config.policy"
com.ibm.commerce.config.server.CMServerImpl %*
```

제 17 장 IBM HTTP Server를 사용한 프로덕션을 위한 SSL 사용

400 이 장은 iSeries 플랫폼에 적용되지 않습니다. iSeries 정보에 대해서는 220 페이지의 『iSeries의 IBM HTTP Server에서 SSL 사용』을 참조하십시오.

IBM HTTP Server로 WebSphere Commerce 인스턴스를 작성하면 SSL(Secure Sockets Layer)이 테스트 용도로 사용됩니다. 사이트를 구매자에게 공개하기 전에 이 장의 단계를 수행하여 프로덕션에 SSL을 사용해야 합니다.

보안 정보

IBM HTTP Server는 암호화 기술을 사용하여 비즈니스 트랜잭션을 위한 보안 환경을 제공합니다. 암호화는 정보를 수령인이 암호화를 해제할 때까지 읽을 수 없도록 인터넷에서 정보 트랜잭션을 암호화하는 것입니다. 보낸 사람은 알고리즘 패턴이나 키를 사용하여 트랜잭션을 암호화하고 수령인은 암호 해독 키를 사용합니다. 이들 키는 SSL(Secure Sockets Layer) 프로토콜에 의해 사용됩니다.

웹 서버는 인증 프로세스를 사용하여 비즈니스를 수행하려는 사람의 동일성을 검증(즉, 그들이 자신이라고 주장하는 본인이 맞는지 확인)합니다. 여기에는 인증 기관(CA)이라는 신뢰되는 제3자가 서명한 인증 확보가 포함됩니다. IBM HTTP Server 사용자의 경우, CA는 Equifax® 또는 VeriSign® Inc.일 수 있습니다. 다른 CA도 사용할 수 있습니다.

프로덕션 키 파일을 작성하려면 다음 단계를 완료하십시오.

1. 프로덕션에 대한 보안 키 파일을 구성하십시오.
2. 인증 기관으로부터 보안 인증을 요청하십시오.
3. 프로덕션 키 파일을 현재 키 파일로 설정하십시오.
4. 인증을 받고 프로덕션 키 파일을 테스트하십시오.

이들 단계가 아래에 자세하게 설명됩니다.

주:

1. 이미 인증 기관이 서명한 프로덕션 키 파일을 사용 중인 경우, 이들 단계를 건너뛸 수 있습니다. 사용 여부를 판별하려면 이 장을 읽으십시오.
2. 이들 단계를 수행하면 브라우저가 보안 메시지를 표시할 수 있습니다. 각 메시지의 정보를 주의깊게 읽고 진행 방법을 결정하십시오.

프로덕션에 대한 보안 키 파일 구성

프로덕션에 대한 보안 키 파일을 구성하려면 웹 서버 시스템에서 다음을 수행하십시오.

1. IBM HTTP Server를 중지하십시오.
2. 디렉토리를 시스템의 IBM HTTP Server 설치 디렉토리의 conf 서브디렉토리로 변경하십시오.
3. httpd.conf의 백업 사본을 작성하고 파일의 백업 사본을 httpd.conf.backup으로 이름을 바꾸십시오.
4. 텍스트 편집기로 httpd.conf를 여십시오.
5. 포트 443에 대해 다음 행에서 주석 처리가 제거되었는지(행의 앞에 있는 『#』을 제거하여) 확인하십시오.
   - Windows
     a. LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
     b. Listen 443
     c. <VirtualHost *host.some_domain*.com:443> (또한 이 행에 완전한 호스트 이름을 삽입해야 합니다.)
     d. SSLEnable
     e. </VirtualHost>
     f. Keyfile "*HTTPServer_installdir*/ssl/keyfile.kdb"
   - AIX Linux Solaris
     a. LoadModule ibm_ssl_module libexec/mod_ibm_ssl_128.so
     b. AddModule mod_ibm_ssl.c
     c. Listen 443
     d. <VirtualHost *host.some_domain*.com:443> (또한 이 행에 완전한 호스트 이름을 삽입해야 합니다.)
     e. SSLEnable
     f. </VirtualHost>
     g. SSLDisable
     h. Keyfile "*HTTPServer_installdir*/ssl/keyfile.kdb"
     i. SSLV2Timeout 100
     j. SSLV3Timeout 1000
6. 다음 행에서 주석 처리가 제거되었는지(행의 앞에 있는 『#』을 제거하여) 확인하십시오.
   a. WebSphere Commerce 관리 도구의 경우 포트 8000, 8002 및 8004가 필요합니다.

```
Listen 8000
Listen 8002
Listen 8004
```

WebSphere Commerce Payments를 사용 중이면 포트 5432와 5433도 필요합니다.

```
Listen 5432
Listen 5433
```

b. 위의 포트에 대한 가상 호스트 섹션도 주석 처리가 제거(있는 경우 행의 앞에 있는 『#』을 제거하여)되었는지 확인하십시오. 이들 섹션에서 완전한 호스트 이름을 삽입해야 합니다. 다음 예에 있는 기본 경로 이름 변수의 목록에 대해서는 ix 페이지의 『경로 변수』를 참조하십시오.

다음 예는 Windows 시스템 `httpd.conf` 파일에서 주석 처리가 제거된 가상 호스트 섹션에서 파생되었습니다. 이러한 섹션은 다른 운영체제에서도 유사합니다.

```
########## IBM WebSphere Payments (Do not edit this section) #################
Listen 5432
Listen 5433
########## End of IBM WebSphere Payments (Do not edit this section) ##########

...

########## IBM WebSphere Commerce (Do not edit this section) #################
Listen 8000
Listen 8002
Listen 8004
########## End of IBM WebSphere Commerce (Do not edit this section) ##########
```

그림 7. httpd.conf 파일의 "Listen" 섹션 예

```
########## End of IBM WebSphere Commerce (Do not edit this section) ##########
## VirtualHost: Allows the daemon to respond to requests for more than one
## server address, if your server machine is configured to accept IP packets
## for multiple addresses. This can be accomplished with the ifconfig
## alias flag, or through kernel patches like VIF.
#
## Any httpd.conf or srm.conf directive may go into a VirtualHost command.
## See also the BindAddress entry.
#
#<VirtualHost host.some_domain.com:443>
```

그림 8. httpd.conf 파일의 가상 호스트 머리글 섹션 예

```
########## IBM WebSphere Payments (Do not edit this section) #################
<VirtualHost host.some_domain.com:5433>
SSLEnable
SSLClientAuth 0
ServerName wordsworth.torolab.ibm.com
DocumentRoot "HTTPServer_installdir\htdocs\en_US"
</VirtualHost>
########## End of IBM WebSphere Payments (Do not edit this section) ##########
```

그림 9. Payments에 대한 httpd.conf 파일의 가상 호스트 섹션 예

```
########## IBM WebSphere Commerce (Do not edit this section) #################
#Instance name : instance_name
<VirtualHost host.some_domain.com:80>
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc   "WC_installdir/web/doc"
Alias /wcsstore  "WAS_installdir\installedApps\host\WC_instance_name.ear/Stores.war"
Alias /wcs   "WAS_installdir\installedApps\host\WC_instance_name.ear/CommerceAccelerator.war"
</VirtualHost>
```

그림 10. WebSphere Commerce 포트 80에 대한 httpd.conf 파일의 가상 호스트 섹션 예. (보안되지 않는 포트)

```
<VirtualHost host.some_domain.com:443>
SSLEnable
SSLClientAuth 0
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc   "WC_installdir/web/doc"
Alias /wcsstore  "WAS_installdir\installedApps\
host\WC_instance_name
.ear/Stores.war"
Alias /wcs   "WAS_installdir
\installedApps\host\WC_
instance_name.ear/CommerceAccelerator.war"
</VirtualHost>
```

그림 11. WebSphere Commerce 포트 443에 대한 httpd.conf 파일의 가상 호스트 섹션 예. (보안 포트)

```
<VirtualHost host.some_domain.com:8000>
SSLEnable
SSLClientAuth 0
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc   "WC_installdir/web/doc"
Alias /wchelp   "WC_installdir/web/doc/en_US"
Alias /adminconsole  "WAS_installdir\installedApps\host
\WC_instance_name.ear/SiteAdministration
.war/tools/adminconsole/wcsadmincon.html"
Alias /wcsstore  "WAS_installdir\installedApps\host
\WC_instance_name.ear/Stores.war"
Alias /accelerator  "WAS_installdir\installedApps\host
\WC_instance_name.ear/CommerceAccelerator
.war/tools/common/accelerator.html"
Alias /wcs   "WAS_installdir\installedApps\host
\WC_instance_name.ear/CommerceAccelerator.war"
Alias /wcadmin  "WAS_installdir\installedApps\host
\WC_instance_name.ear/SiteAdministration.war"
Alias /wcorgadmin  "WAS_installdir\installedApps\host
\WC_instance_name.ear/OrganizationAdministration.war"
Alias /orgadminconsole "WAS_installdir\installedApps\host
\WC_instance_name.ear/OrganizationAdministration.war
/tools/buyerconsole/wcsbuyercon.html"
</VirtualHost>
```

그림 12. WebSphere Commerce 포트 8000에 대한 httpd.conf 파일의 가상 호스트 섹션 예. (WebSphere Commerce 액셀러레이터)

```
<VirtualHost host.some_domain.com:8002>
SSLEnable
SSLClientAuth 0
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc   "WC_installdir/web/doc"
Alias /wchelp   "WC_installdir/web/doc/en_US"
Alias /adminconsole  "WAS_installdir\installedApps\host
\WC_instance_name.ear/SiteAdministration
.war/tools/adminconsole/wcsadmincon.html"
Alias /wcsstore  "WAS_installdir\installedApps\host
\WC_instance_name.ear/Stores.war"
Alias /accelerator  "WAS_installdir\installedApps\host
\WC_instance_name.ear/CommerceAccelerator
.war/tools/common/accelerator.html"
Alias /wcs   "WAS_installdir\installedApps\host
\WC_instance_name.ear/CommerceAccelerator.war"
Alias /wcadmin  "WAS_installdir\installedApps\host
\WC_instance_name.ear/SiteAdministration.war"
Alias /wcorgadmin  "WAS_installdir\installedApps\host
\WC_instance_name.ear/OrganizationAdministration.war"
Alias /orgadminconsole "WAS_installdir\installedApps\host
\WC_instance_name.ear/OrganizationAdministration.war/tools
/buyerconsole/wcsbuyercon.html"
</VirtualHost>
```

그림 13. WebSphere Commerce 포트 8002에 대한 httpd.conf 파일의 가상 호스트 섹션 예. (WebSphere Commerce 관리 콘솔)

```
<VirtualHost host.some_domain.com:8004>
SSLEnable
SSLClientAuth 0
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc   "WC_installdir/web/doc"
Alias /wchelp   "WC_installdir/web/doc/en_US"
Alias /adminconsole  "WAS_installdir\installedApps\host
\WC_instance_name.ear/SiteAdministration.war
/tools/adminconsole/wcsadmincon.html"
Alias /wcsstore  "WAS_installdir\installedApps\host
\WC_instance_name.ear/Stores.war"
Alias /accelerator  "WAS_installdir\installedApps\host
\WC_instance_name.ear/CommerceAccelerator
.war/tools/common/accelerator.html"
Alias /wcs   "WAS_installdir\installedApps\host
\WC_instance_name.ear/CommerceAccelerator.war"
Alias /wcadmin  "WAS_installdir\installedApps\host
\WC_instance_name.ear/SiteAdministration.war"
Alias /wcorgadmin  "WAS_installdir\installedApps\host
\WC_instance_name.ear
/OrganizationAdministration.war"
Alias /orgadminconsole "WAS_installdir\installedApps\host
\WC_instance_name.ear/OrganizationAdministration.war
/tools/buyerconsole/wcsbuyercon.html"
</VirtualHost>
########## End of IBM WebSphere Commerce (Do not edit this section) ##########
```

그림 14. WebSphere Commerce 포트 8004에 대한 httpd.conf 파일의 가상 호스트 섹션 예. (WebSphere Commerce 조직 관리 콘솔)

주: 방화벽 소프트웨어가 WebSphere Commerce 도구에 대해 구성한 포트(기본적으로 포트 8000, 8002 및 8004)에 대한 외부 액세스를 차단하는 것이 바람직합니다. 작업 방법에 대한 자세한 내용은 사이트에서 사용 중인 방화벽 소프트웨어의 문서를 참조하십시오.

7. 변경사항을 저장하십시오.
8. `httpd.conf` 파일이 구문 오류를 포함하지 않는지 확인하십시오.

   AIX Linux Solaris 사용자 시스템의 IBM HTTP Server 설치 디렉토리의 `bin` 서브디렉토리로 변경하고 명령 `./httpd -t`를 실행하십시오.

   Windows 사용자 시스템의 IBM HTTP Server 설치 디렉토리로 변경하고 다음 명령을 실행하십시오.

   ```
   apache -t
   ```

9. IBM HTTP Server를 시작하십시오.

인증 기관으로부터 보안서 인증 요청

이전 단계에서 방금 작성한 보안 키 파일의 유효성을 검증하려면 Equifax 또는 VeriSign 같은 인증 기관(CA)의 인증서가 필요합니다. 인증서에는 서버의 공용 키, 서버의 인증과 연관된 인식 이름 및 인증의 일련 번호와 만기 날짜가 들어 있습니다.

다른 CA를 사용하려는 경우, 수행할 프로시저에 대한 정보를 직접 문의하십시오.

Equifax 사용자

Equifax로부터 보안 서버 인증서를 요청하려면 다음 웹 주소를 참조하여 제공되는 지시사항을 따르십시오.

```
http://www.equifax.com
```

2 - 4 영업일 안에 Equifax로부터 전자 우편을 통해 보안 서버 인증서를 받아야 합니다.

VeriSign 사용자

VeriSign으로부터 보안 서버 인증서를 요청하려면 다음 URL을 참조하여 제공되는 지시사항을 수행하십시오.

```
http://www.verisign.com
```

AIX IBM HTTP Server에 대한 프로시저를 사용 중인 경우에도 **인터넷 접속 보안 서버**(ICSS)에 대한 링크를 따르십시오. 제공되는 지시사항을 수행하십시오. 아직 수행하지 않은 경우, 인증서를 받을 때 이전 절에 설명된 대로 프로덕션 키 파일을 작성하십시오.

Solaris IBM HTTP Server에 대한 프로시저를 사용 중인 경우에도 **인터넷 접속 보안 서버**(ICSS)에 대한 링크를 따르십시오. 후속 페이지에 프로시저가 OS/2® 및 AIX 플랫폼에 적용된다고 표시됩니다. 이들 지시사항은 Solaris 소프트웨어에도 적용됩니다.

제공되는 지시사항을 수행하십시오. 요청을 제출한 후에 3 - 5 영업일 안에 인증서가 도착해야 합니다. 아직 수행하지 않은 경우, 인증서를 받을 때 이전 절에 설명된 대로 프로덕션 키 파일을 작성하십시오.

프로덕션 키 파일을 현재 키 파일로서 수신 및 설정

CA로부터 인증서가 도착한 후 웹 서버가 프로덕션 키 파일을 사용하도록 해야 합니다. 다음 단계를 수행하십시오.

1. 인증 기관에서 받은 *certificatename*.kdb, *certificatename*.rdb 및 *certificatename*.sth 파일을 시스템의 IBM HTTP Server 설치 경로 아래의 ssl 서브디렉토리에 복사하십시오. 여기서 *certificatename*은 인증 요청에서 제공된 인증서 이름입니다.
2. IBM HTTP Server를 중지하십시오.
3. AIX Solaris 다음 명령을 실행하여 JAVA_HOME을 반출하십시오.

   ```
   DISPLAY=host_name:0.0
   export DISPLAY
   JAVA_HOME=java_home
   export JAVA_HOME
   ```

   여기서 *host_name*은 현재 사용 중인 시스템의 완전한 호스트 이름이며 *java_home*은 다음과 같습니다.

   - AIX /usr/java130
   - Solaris /opt/WebSphere/AppServer/java131
4. 키 관리 유틸리티(ikeyman)를 여십시오.
5. *certificatename*.kdb 파일을 열고 프롬프트가 표시될 때 암호를 입력하십시오.
6. **개인 인증서**를 선택하고 **받기**를 누르십시오.
7. **찾아보기**를 누르십시오.
8. 인증 기관에서 받은 파일을 저장한 폴더를 선택하십시오. *certificatename*.txt 파일을 선택한 후 **확인**을 누르십시오.
9. **개인 인증서** 목록 상자에 이제 VeriSign *certificatename* 인증이나 Equifax *certificatename* 인증이 표시됩니다.
10. 키 관리 유틸리티를 종료하십시오.
11. 시스템의 IBM HTTP Server 설치 경로 아래의 conf 서브디렉토리로 디렉토리를 이동하십시오.
12. httpd.conf의 백업 사본을 작성하십시오.
13. 텍스트 편집기로 httpd.conf를 여십시오.
14. 212 페이지의 5단계에 표시된 행에서 주석 처리가 제거되었는지 확인하십시오.
15. Keyfile "*keyfile_path_name*/keyfile.kdb" 지시문을 검색하고, 위의 단계에서 작성된 파일을 가리키도록 경로 이름을 변경하십시오.
16. IBM HTTP Server를 다시 시작하십시오.

프로덕션 키 파일 테스트

프로덕션 키를 테스트하려면 다음을 수행하십시오.

1. 브라우저를 사용하여 다음 URL로 이동하십시오.

   `https://host_name`

   주:

   a. 웹 서버를 사용자 정의한 경우, 호스트 이름 뒤에 웹 서버의 앞 페이지 이름을 입력해야 할 수 있습니다.

   b. `http`가 *아닌* `https`를 입력하십시오.

   키가 올바르게 정의된 경우, 새 인증에 대한 여러 메시지가 표시됩니다.

2. **새 사이트 인증** 패널에서 이 인증을 승인하는 경우, **이 인증을 영원히(만기할 때까지) 승인** 라디오 버튼를 선택하십시오.
3. 웹 브라우저에서 캐시와 프록시(또는 소켓) 서버 설정을 원래 상태로 복원하십시오.

이제 서버에서 SSL이 사용되었습니다.

WebSphere Commerce Payments에 대한 SSL 고려사항

기본적으로 WebSphere Commerce와 WebSphere Commerce Payments간 통신은 SSL을 통합니다. 그러나 다음과 같이 WebSphere Commerce Payments 사용자 인터페이스를 직접 실행하는 경우, 비SSL 통신을 사용하여 WebSphere Commerce Payments를 호출할 수 있습니다.

http://*host_name*:*port_number*/webapp/PaymentManager

여기서 *host_name*은 Payments 서버 시스템 이름이며, *port_number*는 5432(기본값)입니다.

통신이 SSL을 통과하도록 하려면 다음 URL을 사용하십시오.

https://*host_name*:*port_number*/webapp/PaymentManager

여기서 *host_name*은 Payments 서버 시스템 이름이며, *port_number*는 5433(기본값)입니다.

기밀성 향상

WebSphere Commerce에서 URL 요청을 수신하면, 웹 컨트롤러가 요청된 컨트롤러 명령의 인터페이스 이름을 검색하고 이 이름을 사용하여 CMDREG 테이블에서 구현 클래스 이름을 찾습니다. 또한, HTTPS(보안) 프로토콜이 URLREG 테이블의 HTTPS 열을 확인하여 URL 요청에 필수인지 여부를 판별합니다.

중요한 정보를 표시하는 모든 명령은 HTTPS 값이 URLREG 테이블에서 『1』 값으로 설정되어야 합니다. 예를 들어, 고객 주문의 세부사항이 들어 있는 OrderProcessView 뷰 명령은 HTTPS 프로토콜을 통해서만 전송되어야 하므로 URLREG 테이블의 OrderProcessView 항목 값은 HTTPS 열의 『1』입니다.

iSeries의 IBM HTTP Server에서 SSL 사용

400 이 절은 iSeries 플랫폼에 작용됩니다.

SSL은 보안 프로토콜입니다. SSL은 클라이언트와 서버간에 전송된 데이터의 보안을 확실히 보장합니다. SSL을 사용하여 클라이언트는 서버의 동일성을 인증하고 서버는 클라이언트의 동일성을 인증합니다.

디지털 인증서는 인터넷를 통한 보안 트랜잭션에 포함된 서버와 클라이언트를 인증하는 전자 문서입니다. 디지털 인증서의 발행자를 인증 기관(CA)이라고 합니다. iSeries 시스템은 인트라넷 환경에서 서버와 클라이언트 인증서를 발행하는 CA 역할을 수행할 수 있고, iSeries CA 또는 VeriSign과 같은 인터넷 CA가 발행한 서버 인증서로 인증된 서버로서 실행될 수 있습니다. 웹 서버로서 iSeries용 IBM HTTP Server는 SSL 사용 클라이언트의 인증을 위해 클라이언트 인증서를 요청하도록 구성할 수도 있습니다.

iSeries용 IBM HTTP Server에서 SSL을 사용하는 방법에 대한 자세한 정보에 대해서는 iSeries 정보 센터(http://publib.boulder.ibm.com/html/as400/infocenter.html)를 참조하십시오. 해당 사이트에 있으면, 사용자의 운영체제 버전과 언어를 선택한 후 **이동**을 누르십시오. SSL 사용 방법에 대한 지침에 대해서는 『SSL을 사용한 응용프로그램 보안』 주제를 검색하십시오.

WebSphere Commerce Payments에서 SSL 사용

WebSphere Commerce 인스턴스를 작성한 후 시스템 인증 상점을 작성하는 경우, WebSphere Commerce Payments 인스턴스 및 WebSphere Commerce 인스턴스 모두에 시스템 인증 상점에 대한 액세스를 부여해야 합니다. 예를 들어 다음 명령은 WebSphere Commerce Payments 인스턴스에 V5R1 시스템에서의 필수 액세스를 부여합니다.

```
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server') USER(QPYMSVR) DTAAUT(*RX)
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server/DEFAULT.KDB') USER(QPYMSVR) DTAAUT(*R)
```

다음 명령은 V5R1 시스템에서 WebSphere Commerce에 필요한 액세스를 부여합니다.

```
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server') USER(QEJBSVR) DTAAUT(*RX)
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server/DEFAULT.KDB') USER(QEJBSVR) DTAAUT(*R)
```

원격 WebSphere Commerce Payments 인스턴스를 사용하려는 경우, 디지털 인증서를 발행하는 원격 인증 기관을 신뢰하도록 WebSphere Commerce 인스턴스와 WebSphere

Commerce Payments 인스턴스 모두를 구성해야 합니다. 두 원격 응용프로그램간 신뢰 관계를 구축하려면 다음 고급 프로시저를 참조하십시오.

1. WebSphere Commerce 시스템에서 디지털 인증서 관리자를 사용하여 서버의 인증 기관을 반출하십시오.
2. 인증서 파일을 WebSphere Commerce Payments 시스템으로 전송하십시오.
3. WebSphere Commerce Payments 시스템에서 디지털 인증 관리자를 사용하여 WebSphere Commerce 서버의 인증 기관을 반입하십시오.
4. 반입된 WebSphere Commerce 서버의 인증 기관을 신뢰하도록 WebSphere Commerce Payments 응용프로그램 서버를 구성하십시오.
5. WebSphere Commerce Payments 시스템에서 디지털 인증 관리자를 사용하여 서버의 인증 기관을 반출하십시오.
6. 인증서 파일을 WebSphere Commerce 시스템으로 전송하십시오.
7. WebSphere Commerce 시스템에서 디지털 인증 관리자를 사용하여 WebSphere Commerce Payments 서버의 인증 기관을 반입하십시오.
8. 반입된 WebSphere Commerce Payments 서버의 인증 기관을 신뢰하도록 WebSphere Commerce 응용프로그램 서버를 구성하십시오.

자세한 정보에 대해서는 다음 웹 주소에 있는 **힌트 및 추가정보**: WebSphere Commerce 기술 라이브러리 웹 페이지(`http://www.software.ibm.com/software/commerce/wscom/library/lit-tech.html`)를 참조하십시오.

제 18 장 IBM Directory Server(LDAP)의 SSL 사용

이 장에서는 IBM Directory Server 및 WebSphere Commerce의 SSL 보안을 구성하는 단계에 대해 설명합니다.

IBM Directory Server 설정

400 이 절은 iSeries 플랫폼에 적용되지 않습니다. iSeries 정보에 대해서는 224 페이지의 『iSeries 플랫폼에서 IBM OS/400 Directory Sevice 설정』을 참조하십시오.

IBM Directory Server를 설정하려면 다음을 수행하십시오.

1. IBM Directory Server 제품 설치 지시사항에 따라 IBM Directory Server를 설치하십시오. GSKit 구성요소를 설치되었는지 확인하십시오.
2. 설치 완료 이후에 gsk5ikm 실행 파일을 실행하여 IBM Key Manager를 호출하십시오.
3. 새 CMS 키 데이터베이스 파일을 작성하십시오. **파일에 암호 저장**이 선택되었는지 확인하십시오(예: `ldap_key.kdb`).
4. X509 V3 버전 및 1024 키 크기를 사용하여 자체 서명된 인증을 작성하십시오. (예를 들어, 사용자 이름과 같은 의미 있는 레이블을 인증에 지정할 수 있습니다.)
5. `Base64` 암호화 `ASCII` 데이터 데이터 유형을 사용하여 인증 파일(예를 들어, `cert.arm`)로 인증을 추출하십시오.
6. 브라우저로 `http://`*`host_name`*`/ldap` 주소를 여십시오. 여기서 *host_name*은 LDAP 서버 시스템 이름입니다.
7. **보안** > **SSL** > **설정**을 누르고 다음 변경을 수행하십시오.
   - SSL 상태: SSL 설정 또는 SSL만
   - 인증 방법: 서버 인증
   - 보안 포트: 636
   - 키 데이터베이스 경로 및 파일 이름:

     AIX Linux Solaris `/Keys/ldap_key.kdb`

     Windows *`drive`*`:\Keys\ldap_key.kdb`
   - 키 레이블: *your_label*(인증서의 레이블)
   - 키 암호: *xxxxx*(CMS 키 데이터베이스 파일의 암호. '**암호를 파일에 저장**'을 선택한 경우, 암호를 입력할 필요가 없습니다.
8. **갱신**을 누르고 SecureWay를 다시 시작하십시오.

iSeries 플랫폼에서 IBM OS/400 Directory Sevice 설정

400 iSeries에서 IBM OS/400 Directory Service를 설정하려면 다음을 수행하십시오.

1. Windows용 IBM iSeries Access를 설치하십시오.
2. **시작** -> **프로그램** -> **Windows용 IBM iSeries Access** -> **iSeries Navigator**를 선택하여 Windows에서 iSeries Navigator를 시작하십시오.
3. 시스템이 연결되어 있지 않은 경우 대상 iSeries 시스템에 대한 연결을 작성하십시오.
4. 왼쪽 패널에서 대상 시스템을 펼친 후, 왼쪽 패널에서 **네트워크** -> **서버**를 펼치십시오.
5. 왼쪽 패널에서 **TCP/IP**를 누르십시오.
6. 오른쪽 패널에서 **디렉토리**를 마우스 오른쪽 단추로 누르고 팝업 메뉴에서 **특성**을 선택하십시오.
7. 디렉토리 등록 정보 창에서 **네트워크** 탭을 누르십시오.
8. **디지털 인증 관리자**를 눌러 디지털 인증 관리자를 실행하고 응용프로그램 "Directory Service 서버"에 인증서를 지정하십시오.
9. Directory Service 서버에 인증서를 지정한 후에, **확인**을 눌러 디렉토리 등록 정보 창을 닫으십시오.
10. 디렉토리 등록 정보 창을 다시 열면 SSL(Secure Sockets Layer)이 사용됨을 볼 수 있습니다. 기본값 설정을 승인할 수 있습니다.
    - SSL 상태:
    - 인증 방법: 서버 인증
    - 보안 포트: 636
11. Directory Service 서버를 다시 시작하십시오.

자체 서명된 인증서를 WebSphere Application Server에 지정 및 반입

400 SSL 인증서가 인증 기관(CA)(예: VeriSign 또는 Thwate)에서 발행되지 않은 경우, iSeries 시스템에서 로컬 CA를 반출하고 WebSphere Commerce 시스템의 기본 신뢰 keystore로 반입해야 합니다. iSeries 로컬 인증으로 SSL을 사용하고 iSeries 시스템에서 로컬 CA를 반출하려면, 다음을 수행하십시오.

1. HTTP *Admin 서버가 가동되었는지 확인하십시오. 실행되지 않은 경우, 다음을 실행하십시오.

   ```
   STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
   ```

2. 브라우저를 실행하여 http://host name:2001/ 주소에서 iSeries 태스크 페이지를 여십시오.

3. **디지털 인증 관리자**를 선택하십시오.
4. **인증 상점 선택**을 누르십시오.
5. 인증 상점에서 ***시스템**을 선택하십시오.
6. **사용자 PC에 로컬 CA 인증서 설치** 링크를 볼 수 없는 경우, 로컬 CA를 작성하는 것이 필요합니다.
   a. 인증 기관(CA) 작성을 누르십시오.
   b. iSeries에서 `*Admin` HTTP 서버를 다시 시작하십시오.
   c. 클라이언트 또는 서버 유형으로 새 인증서를 작성하십시오.
   d. 새로 작성한 로컬 인증 기관을 선택하십시오.
   e. 이 인증서를 Directory Service 서버에 지정하십시오.
7. 사용자 PC에서 **로컬 CA 인증서 설치**를 누르십시오.
8. 인증서 설치를 누르십시오. 그런 후 임시 폴더에 인증서(`.cer` 파일)를 저장하십시오.
9. 인증 기관(`.cer` 파일)을 Microsoft Internet Explorer로 반입한 후 인증 기관을 다시 임시 디렉토리의 `.cer` 파일(바이너리 64 인코딩)로 반출하십시오.
10. 인증(바이너리 64 인코딩)을 WebSphere Application Server 신뢰 keystore로 반입하십시오. 예를 들면 다음과 같습니다.

```
keytool -import -alias nck -file /temp_dir/nck.cer
        -keystore /qibm/proddata/java400/jdk13/lib/security/cacerts
```

WebSphere Application Server

WebSphere Application Server에서 다음을 수행하십시오.

1. WebSphere Application Server에서 제공되는 IKeyMan(IBM Key Manager)을 실행하십시오. (WebSphere Application Server 메뉴에서 찾거나 명령 창에 직접 `ikeyman`을 입력할 수 있습니다.)

   주: 이 IBM Key Manager는 SecureWay에서 제공하는 것과는 다릅니다.
   기본 암호는 '`changeit`'입니다.

2. WebSphere Application Server carcerts keystore(예: Windows의 *`WAS_installdir`*`\AppServer\java\jre\lib\security\cacerts`)를 여십시오.
3. **서명자 인증서**를 수행하고 **추가**를 누르십시오. '**Base64 암호화 ASCII 데이터**' 데이터 유형을 사용하고 223 페이지의 5단계에서 작성한 인증서 파일을 선택하십시오.
4. 인증서 이름을 입력하십시오.
5. IKeyMan을 닫으십시오.

WebSphere Commerce

SecureWay Directory Server와 함께 작동하도록 WebSphere Commerce를 설정하려면 다음과 같이 *instance*.xml 파일을 수정해야 합니다.

1. 새 JNDI 환경 변수를 추가하십시오.

   ```
   java.naming.security.protocol = ssl
   ```

2. LdapPort를 '636'으로 변경하십시오.

   ```
   LdapPort = 636
   ```

3. WebSphere Commerce를 다시 시작하십시오.

다음은 예입니다.

```
<MemberSubSystem name="Member SubSystem"
          AuthenticationMode="LDAP"
                     ProfileDataStorage="LDAP"

  <Directory LdapAdminDN="cn=root"
                LdapAuthenticationMode="SIMPLE"
                LdapTimeOut="0"
                LdapVersion="3"
                EntryFileName="E:/WebSphere/WPS/xml/ldap/attributeMap.xml"
                LdapPort="636"
                LdapAdminPW="<adminpassword>"
                LdapHost="<hostname>"
                MigrateUsersFromWCSdb="OFF"
                JNDIEnvPropName1="java.naming.security.protocol"
                JNDIEnvPropValue1="ssl"
                display="false"
                LdapType="SECUREWAY"

   . . . .

  />


</MemberSubSystem>
```

제 6 부 부록

부록. 기본 액세스 제어 정책 및 그룹

부록에는 WebSphere Commerce와 함께 제공되는 기본 정책 및 그룹이 표시되어 있습니다.

기본 액세스 제어 정책

기본 액세스 제어 정책은 다음과 같은 카테고리로 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 22. 정책 정보가 있는 위치

정책	시작 페이지
역할 기반 정책	230 페이지의 『역할 기반 정책』
비즈니스 영역별 자원 레벨 정책	233 페이지의 『비즈니스 영역별 자원 레벨 정책』
주문	233 페이지의 『주문』
거래(장기 구매 계약)	235 페이지의 『거래(장기 구매 계약)』
승인	235 페이지의 『승인』
경매	236 페이지의 『경매』
비즈니스 인텔리전스	236 페이지의 『비즈니스 인텔리전스』
멤버쉽	236 페이지의 『멤버쉽』
마케팅	238 페이지의 『마케팅』
카탈로그	238 페이지의 『카탈로그』
연결 및 알림	239 페이지의 『연결 및 알림』
조달	239 페이지의 『조달』
쿠폰	239 페이지의 『쿠폰』
고객 프로파일링	239 페이지의 『고객 프로파일링』
할인	240 페이지의 『할인』
계획된 재고	
재고 관리	
주문 관리	241 페이지의 『주문 관리』
Payments	241 페이지의 『Payments』
정책 편집기	241 페이지의 『정책 편집기』
상품 어드바이저	242 페이지의 『상품 어드바이저』
RFQ	242 페이지의 『RFQ』

표 22. 정책 정보가 있는 위치 (계속)

정책	시작 페이지
규칙	242 페이지의 『규칙』
스케줄러	243 페이지의 『스케줄러』
Commerce 액셀러레이터	243 페이지의 『Commerce 액셀러레이터』
운송	243 페이지의 『운송』
과세	243 페이지의 『과세』
실시간 도움말/협업 작업 영역/고객 지원	244 페이지의 『실시간 도움말/협업 작업 영역/고객 지원』
상점 상태	244 페이지의 『상점 상태』
상점 관리	

역할 기반 정책

- SiteAdministratorsCanDoEverything
- BuyerAdministratorsExecuteBuyersAdministratorsCommands
- BuyerApproversExecuteBuyerApproversCmdResourceGroup
- GuestsExecuteGuestUsersCmdResourceGroup
- BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup
- CustomerServiceRepresentativesExecuteCustomerServiceRepCmdResourceGroup
- MarketingManagersExecuteMarketingManagerCmdResourceGroup
- CustomerServiceSupervisorsExecuteCustomerServiceSupervisorCmdResourceGroup
- AccountRepresentativesExecuteAccountRepresentativesCmdResourceGroup
- SalesManagersExecuteSalesManagersCmdResourceGroup
- ProductManagersExecuteProductManagersCmdResourceGroup
- SellerAdministratorsExecuteSellerAdministratorsCommands
- SellersExecuteSellersCmdResourceGroup
- CategoryManagersExecuteCategoryManagersCmdResourceGroup
- Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup
- Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup
- PickPackersExecutePickPackersCmdResourceGroup
- ReceiversExecuteReceiversCmdResourceGroup
- ReturnsAdministratorsExecuteReturnsAdministratorsCmdResourceGroup
- OperationsManagersExecuteOperationsManagersCmdResourceGroup
- LogisticsManagersExecuteLogisticsManagersCmdResourceGroup
- ProcurementBuyersExecuteProcurementBuyersCmdResourceGroup
- CustomerServiceRepresentativesExecuteCustomerServiceRepresentativeViews
- BuyerAdministratorsExecuteBuyerAdministratorsViews

- BuyerApproversExecuteBuyerApproversViews
- MarketingManagersExecuteMarketingManagersViews
- CustomerServiceSupervisorsExecuteCustomerServiceSupervisorViews
- SalesManagersExecuteSalesManagersViews
- AccountRepresentativesExecuteAccountRepresentativesViews
- Buyers(buy-side)ExecuteBuyers(buy-side)Views
- Buyers(sell-side)ExecuteBuyers(sell-side)Views
- CategoryManagersExecuteCategoryManagersViews
- CustomersExecuteCustomersViews
- ProductManagersExecuteProductManagersViews
- PickPackersExecutePickPackersViews
- ReceiversExecuteReceiversViews
- ReturnsAdministratorsExecuteReturnsAdministratorsViews
- OperationsManagersExecuteOperationsManagersViews
- LogisticsManagersExecuteLogisticsManagersViews
- SellerAdministratorsExecuteSellerAdministratorsViews
- SellersExecuteSellersViews
- RegisteredApprovedUsersExecuteRegisteredApprovedUsersViews
- NonRejectedUsersExecuteNonRejectedUsersViews
- GuestUsersExecuteGuestUsersViews
- RegisteredApprovedUsersExecuteRegisteredApprovedUsersCommandsResourceGroup
- ChannelManagersExecuteChannelManagersCommands
- AllUsersExecuteAllSiteUserCmdResourceGroup
- AllUsersExecuteAllSiteUsersViews
- RegisteredCustomersForOrgExecuteRegisteredUserCmdResourceGroup
- RegisteredCustomersForOrgExecuteRegisteredUserViews
- ChannelManagersExecuteChannelManagersViews
- AllUsersExecuteResellerUserCmdResourceGroup
- AllUsersExecuteResellerUserViews
- RegisteredCustomersForOrgExecuteRegisteredResellerUserCmdResourceGroup
- RegisteredCustomersForOrgExecuteRegisteredResellerUserViews

다음 테이블에서는 역할, 액세스 그룹, 자원 그룹 및 뷰별 역할 기반 정책을 표시합니다.

주:

1. **역할** 열을 제외한 테이블의 대부분의 항목은 길이가 길 경우 항목을 표시하기 위해 각 셀로 나뉘어집니다.
2. 아래의 모든 역할이 WebSphere Commerce에 정의되어 있는 것은 아닙니다. 정의된 WebSphere Commerce 역할에 대한 자세한 정보는 32 페이지의 『역할』을 참조하십시오.

표 23. 역할, 액세스 그룹, 자원 그룹 및 뷰별 역할 기반 정책

역할	역할 기반 정책에서 사용되는 액세스 그룹	컨트롤러 명령의 역할 기반 정책에서 사용되는 자원 그룹	뷰의 역할 기반 정책에서 사용되는 조치 그룹
사이트 운영자	SiteAdministrators	없음	없음
구매자 관리자	BuyerAdministrators	BuyerAdministrators CommandsResource Group	BuyerAdministrators Views
구매자 승인자	BuyerApprovers	BuyerApproversCmd ResourceGroup	BuyerApproversViews
게스트[1]	Guests	GuestUsersCmd ResourceGroup	GuestUsersViews
고객 서비스 영업대표	CustomerService Representatives	CustomerService RepCmdResourceGroup	CustomerService Representative Views
마케팅 관리자	MarketingManagers	MarketingManager CmdResourceGroup	MarketingManagersViews
고객 서비스 대표	CustomerService Supervisors	CustomerService Supervisor CmdResourceGroup	CustomerService SupervisorViews
계정 담당	Account Representatives	AccountRepresentativesCmd ResourceGroup	AccountRepresentatives Views
판매 관리자	SalesManagers	SalesManagersCmd ResourceGroup	SalesManagersViews
상품 관리자	ProductManagers	ProductManagers CmdResourceGroup	ProductManagersViews
판매자 관리자	Seller Administrators	SellerAdministrators CommandsResourceGroup	SellerAdministrators Views
판매자	Sellers	SellersCmdResourceGroup	SellersViews
카테고리 관리자	CategoryManagers	CategoryManagers CmdResourceGroup	CategoryManagersViews
구매자(구매측)	Buyers(buy-side)	Buyers(buy-side) CommandsResourceGroup	Buyers(buy-side)Views
구매자(판매측)	Buyers(sell-side)	Buyers(sell-side) CommandsResourceGroup	Buyers (sell-side)Views
포장업자	PickPackers	PickPackersCmd ResourceGroup	PickPackersViews
수령인	Receivers	ReceiversCmdResourceGroup	ReceiversViews
반품 운영자	ReturnsAdministrators	ReturnsAdministratorsCmd ResourceGroup	ReturnsAdministrators Views

표 23. 역할, 액세스 그룹, 자원 그룹 및 뷰별 역할 기반 정책 (계속)

역할	역할 기반 정책에서 사용되는 액세스 그룹	컨트롤러 명령의 역할 기반 정책에서 사용되는 자원 그룹	뷰의 역할 기반 정책에서 사용되는 조치 그룹
운영 관리자	OperationsManagers	OperationsManagersCmd ResourceGroup	OperationsManagersViews
물류 관리자	LogisticsManagers	LogisticsManagersCmd ResourceGroup	LogisticsManagersViews
조달 구매자	ProcurementBuyers	ProcurementBuyersCmd ResourceGroup	없음
등록 승인 사용자[2]	RegisteredApproved Users	RegisteredApprovedUsers CommandsResourceGroup	RegisteredApproved UsersViews
거부되지 않은 사용자[3]	NonRejectedUsers	NonRejectedUserCommands ResourceGroup	NonRejectedUsersViews
채널 관리자	ChannelManagers	ChannelManagersCmd ResourceGroup	ChannelManagersViews
모든 사용자[4]	AllUsers	ResellerUserCmd ResourceGroup[5]	ResellerUserViews[5]
		AllSiteUserCmd ResourceGroup[6]	AllSiteUsersViews[6]
등록 고객 (OrgandAncestorOrgs 역할 규정자 있음)	Registered CustomersForOrg	RegisteredUserCmd ResourceGroup	RegisteredUserViews
		RegisteredResellerUser CmdResourceGroup	RegisteredReseller UserViews

주:

1. 『게스트』는 실제 역할이 아닙니다. 등록 상태가 『G』로 설정된(USER.REGISTERTYPE 열이 『G』로 설정되어 있음) 사용자는 암시적으로 Guests 액세스 그룹에 속합니다.
2. 『등록 승인 사용자』는 실제 역할이 아닙니다. 등록 상태가 『R』로 설정되어 있고(USER.REGISTERTYPE 열이 『R』로 설정되어 있음) 상태가 승인된(MEMBER.STATE 열이 1로 설정되어 있음) 사용자는 암시적으로 RegisteredApprovedUsers 액세스 그룹에 속합니다.
3. 『거부되지 않은 사용자』는 실제 역할이 아닙니다. 등록 상태가 거부되지 않은(MEMBER.STATE 열이 2로 설정되어 있지 않음) 사용자는 암시적으로 NonRejectedUsers 액세스 그룹에 속합니다.
4. 『모든 사용자』는 실제 역할이 아닙니다. 시스템의 모든 사용자는 암시적으로 AllUsers 액세스 그룹에 속합니다.
5. 이러한 조치 및 자원 그룹은 B2CPolicyGroup의 부분인 정책에 속합니다. 이러한 정책 그룹은 B2C 비즈니스 모델을 따르는 조직에만 적용될 수 있습니다.
6. 이러한 조치 그룹 및 자원 그룹은 ManagementAndAdministrationPolicyGroup의 부분인 정책에 속합니다. 이러한 정책 그룹은 모든 조직에 적용될 수 있습니다.

비즈니스 영역별 자원 레벨 정책

주문

데이터 자원: 주문:

- AllUsersExecuteAllUsersActionGroupCommandsOnOrderResource

- AllUsersExecuteOrderCreateCommandsOnStoreResource
- AllUsersExecuteOrderReadCommandsOnOrderResource
- AllUsersExecuteOrderPrepareCommandsOnOrderResource
- AllUsersExecuteOrderWriteCommandsOnOrderResource
- AllUsersExecuteScheduledOrderCancelOnOrderResource
- AllUsersExecuteReturnAgainstOrderOnOrderResource
- AllUsersExecuteOrderProcessOnOrderResource
- OrderManagersForOrgExecuteOrderManageCommandsOnOrderResource
- CustomerOrderManagersForOrgExecuteOrderProcessOnOrderResource
- ResellerAdministratorsForOrgExecuteOrderReadCommandsOnOrderDataResourceGroup
- ResellerAdministratorsForOrgExecuteOrderPrepareCommandsOnOrderDataResourceGroup
- ResellerAdministratorsForOrgExecuteOrderWriteCommandsOnOrderDataResourceGroup
- ResellerAdministratorsForOrgExecuteScheduledOrderCancelOnOrderDataResourceGroup
- ResellerAdministratorsForOrgExecuteOrderProcessOnOrderDataResourceGroup
- EmailOrderNotificationManagersForOrgExecuteCustomerServiceEmailOrderOnOrderResource

데이터 자원: 요청 목록:

- AllUsersExecuteRequisitionListCreateCommandsOnStoreEntityResource
- AllUsersExecuteRequisitionListSharedReadCommandsOnSharedRequisitionListResource
- AllUsersExecuteRequisitionListExclusiveReadCommandsOnPrivateRequisitionListResource
- AllUsersExecuteRequisitionListWriteCommandsOnRequisitionListResource
- AllUsersExecuteRequisitionListSharedProcessCommandsOnSharedRequisitionListResource
- AllUsersExecuteRequisitionListExclusiveProcessCommandsOnPrivateRequisitionListResource

데이터 자원: 관심 항목:

- AllUsersExecuteInterestItemReadCommandsOnInterestItemListResource
- AllUsersExecuteInterestItemWriteCommandsOnInterestItemListResource

데이터 자원: RMA:

- AllUsersExecuteRMACreateCommandsOnStoreResource
- AllUsersExecuteRMAReadCommandsOnRMAResource
- AllUsersExecuteRMAPrepareOnRMAResource
- AllUsersExecuteRMAWriteCommandsOnRMAResource
- AllUsersExecuteRMAProcessCommandsOnRMAResource
- RMAApproversForOrgExecuteRMAApproveCommandsOnRMAResource
- RMADisposersForOrgExecuteRMADisposeCommandsOnRMAResource

- RMAReceiversForOrgExecuteRMAReceiveCommandsOnRMAResource
- RMAManagersForOrgExecuteRMAManageCommandsOnRMAResource
- StoreAdministratorsForOrgExecuteRMACreditCommandsOnStoreEntityResource

데이터 bean: 주문:

- AllUsersDisplayOrderDatabeanResourceGroup
- AllUsersDisplayApprovalsOrderDataBeansResourceGroup
- AccountRepresentativesForOrgDisplayOrderDatabeanOnlyResourceGroup

데이터 bean: 요청 목록:

AllUsersDisplaySharedRequisitionListDataBeansIfSameOrganizationalEntityAsCreator

데이터 bean: 관심 항목: AllUsersDisplayInterestItemDatabeanResourceGroup

데이터 bean: RMA: AllUsersDisplayRMADatabeanResourceGroup

거래(장기 구매 계약)

데이터 자원: 장기 구매 계약:

- ContractCreatorsForOrgExecuteContractCreateCommandsOnMemberResource
- ContractManagersForOrgExecuteContractManageCommandsOnContractResource
- ContractOperatorsForOrgExecuteContractDeployCommandsOnContractResource
- ContractViewersExecuteContractDisplayCommandsOnContractResource
- ContractOperatorsForOrgExecuteContractSubmitCommandsOnContractResource
- ContractManagersForOrgExecuteContractAccountManageCommandsOnAccountResource

데이터 자원: 비즈니스 정책:

- BusinessPolicyAdministratorsForOrgExecuteBusinessPolicyCreateCommandsOnStoreResource
- BusinessPolicyAdministratorsForOrgExecuteBusinessPolicyManageCommandsOnBusinessPolicyResource

데이터 자원: 상점 작성: StoreCreatorsForOrgExecuteStoreCreationCommandsOnOrganizationResource

데이터 bean: AccountHandlersForOrgDisplayTradingDatabeanResourceGroup

승인

데이터 자원:

- AllUsersExecuteApproveCommandsOnApprovalResource
- FlowAdministratorExecutesFlowAdminCreateCommandsOnStoreEntityResource
- FlowAdministratorExecutesFlowadminDeleteCommandsOnFlowadminResource

데이터 bean: FlowAdministratorsForOrgDisplayFlowadminDatabean

경매

데이터 자원:

- AuctionAdministratorsForOrgExecuteAuctionCreateCommandsOnStoreEntityResource
- AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
- AuctionManagersForOrgExecuteAdminRetractBidCommandsOnAuctionResource
- AuctionAdministratorsForOrgExecuteAuctionStyleCreateCommandsOnStoreEntityResource
- AuctionAdministratorsForOrgExecuteAuctionStyleManageCommandsOnAuctionStyleResource
- AuctionAdministratorsForOrgExecuteBidControlRuleCreateCommandsOnStoreEntityResource
- AuctionAdministratorsForOrgExecuteBidControlRuleManageCommandsOnBidControlRuleResource
- RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource
- RegisteredApprovedUsersExecuteBidManageCommandsOnBidResources
- RegisteredApprovedUsersExecuteAutoBidCreateCommandsOnAuctionResource
- RegisteredApprovedUsersExecuteAutoBidManageCommandsOnAutoBidResources

데이터 bean: AuctionDatabeanOwnersDisplayAuctionDatabeans

비즈니스 인텔리전스

데이터 자원:

- BusinessAnalystsForOrgExecuteViewContextListCommandsOnStoreEntityResource
- IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReportCommands OnStoreEntityResource

멤버쉽

데이터 자원: 사용자:

- MembershipAdministratorsForOrgExecuteUserAdminUpdateCommandsOnUserResource
- GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource
- NonRejectedUsersExecuteUserSelfRegistrationContinuationCommandsOnUserResource
- NonRejectedUsersExecuteNonRejectedUserCommands
- AllUsersDisplayUserDatabeanResourceGroup
- NonRejectedDisplayUserDatabeanResourceGroup

데이터 자원: 조직:

- OrgAdminConsoleMembershipAdministratorsForOrgExecuteOrgEntityPolicySubscription UpdateCommandsOnOrganizationResource
- OrgAdminConsoleMembershipAdministratorsForOrgExecuteOrganizationManageActions OnOrganiztionResource
- CSAMembershipAdministratorsForOrgExecuteUserAdminRegistrationCommands OnOrganizationResource

- CSAMembershipAdministratorsExecuteUserAdminRegistrationCommands OnOrganizationResource
- MembershipAdministratorsForOrgExecuteOrgEntityRegistrationCommands OnOrganizationResource
- MembershipAdministratorsForOrgExecuteOrgEntityUpdateCommandsOnOrganizationResource GuestsExecuteResellerSelfRegistrationCommandsOnOrganizationResource
- NonRejectedUsersExecuteResellerSelfRegistrationContinuationCommandsOnOrganizationResource
- ChannelManagersExecuteOrgEntityLockCommandsOnOrgResource
- OrgAdminConsoleMembershipAdministratorsForOrgExecuteApproveGroupUpdateCommands OnOrganizationResource

데이터 자원: 구성원 그룹:

- OrgAdminConsoleMembershipAdministratorsForOrgExecuteMemberGroupMemberUpdate CommandsOnUserResource
- OrgAdminConsoleMembershipAdministratorsForOrgExecuteMemberGroupMemberUpdate CommandsOnMemberGroupResource
- MemberGroupAdministratorsForOrgExecuteMemberGroupCreateCommandsOnMemberResource
- MemberGroupManagersForOrgExecuteMemberGroupManageCommandsOnMemberGroupResource

데이터 자원: 주소:

- NonRejectedUsersExecuteAddressManageCommandsOnUserResource
- MembershipAdministratorsForOrgExecuteAddressManageCommandsOnMemberResource

데이터 자원: 역할:

- MembershipAdministratorsForOrgExecuteRoleUnassignCommandsOnUserResource
- OrganizationRoleAdministratorsExecuteRoleManageCommandsOnOrganizationResource
- MembershipAdministratorsForOrgExecuteUserRoleAssignCommandsOnOrganizationResource

데이터 자원: 구성원 속성:

- OrgAdminConsoleMembershipAdministratorsForOrgExecuteMemberAttributeCommands OnOrgResource
- AllUsersExecuteMemberAttributeCommandsOnUserResource

데이터 bean:

- MembershipViewersForOrgDisplayMembershipDatabeanResourceGroup
- MembershipAdministratorsForOrgDisplayOrganizationDatabeanResourceGroup
- MembershipAdministratorsForOrgDisplayUserDatabeanResourceGroup
- EmployeesDisplayOrganizationSpecificDatabeanResourceGroup

마케팅

데이터 자원: 캠페인:

- CampaignManagersForOrgExecuteCampaignRelatedCreateCommandsOnStoreEntityResource
- CampaignManagersForOrgExecuteCampaignUpdateCommandsOnCampaignResource
- CampaignManagersForOrgExecuteInitiativeUpdateCommandsOnInitiativeResource
- CampaignManagersForOrgExecuteEMarketingSpotUpdateCommandsOnEMarketingSpotResource
- CampaignManagersForOrgExecuteCollateralUpdateCommandsOnCollateralResource

데이터 자원: 전자 우편 활동:

- EmailActivityEditorsForOrgExecuteEmailActivitySaveCommandsOnEmailActivity DataResourceGroup
- EmailActivityEditorsForOrgExecuteEmailActivitySaveCommandsOnStoreEntity DataResourceGroup
- EmailActivityEditorsForOrgExecuteEmailActivityDeleteCommandsOnEmailActivity DataResourceGroup
- EmailActivityConfigurationEditorsForOrgExecuteEmailActivityConfigurationSaveCommands OnEmailActivityDataResourceGroup
- EmailActivityConfigurationEditorsForOrgExecuteEmailActivitySaveCommandsOnStoreEntity DataResourceGroupAllUsersExecuteEmailOptOutDataResourceGroup

데이터 bean: 캠페인: CampaignManagersForOrgDisplayCampaignDatabeanResourceGroup

데이터 bean: 전자 우편 활동:

- EmailUserReceiveDataBeanPolicy
- EmailActivityDataBeanPolicy
- EmailConfigurationDataBeanPolicy

데이터 bean: e-promotion: EpromotionDisplayDataBeanPolicy

카탈로그

데이터 자원:

- CatalogManagersForOrgExecuteStoreCategoryManageCommandsOnCatalogResource
- CatalogManagersForOrgExecuteCatalogManageCommandsOnCatalogResource
- CatalogGroupManagersForOrgExecuteCatalogGroupManageCommandsOnCatalogGroupResource
- CatalogEntryManagersForOrgExecuteStoreCatalogEntryManageCommandsOnStoreEntityResource
- CatalogGroupManagersForOrgExecuteProductSetAddCommandsOnCatalogResource
- CatalogGroupManagersForOrgExecuteProductSetManageCommandsOnProductSetResource
- CatalogEntryManagersForOrgExecuteCatalogEntryManageCommandsOnCatalogEntryResource
- CatalogEntryManagersForOrgExecuteCatalogEntryRelationManageCommandsOnCatalogResource
- CatalogEntryManagersForOrgExecuteCatalogStoreManageCommandsOnStoreEntityResource

데이터 bean:

- ProductAdministratorsForOrgDisplayProductDataBeansResourceGroup
- CatalogGroupViewersForOrgDisplayCatalogGroupDataBeansResourceGroup
- CatalogListViewersForOrgDisplayCatalogListDataBeansResourceGroup

연결 및 알림

데이터 자원:

- BackendOrderAdministratorsForOrgExecuteBackendOrderStatusCreateCommandsOnOrderDataResource
- BackendPickPackersForOrgExecuteBackendPickPackListCommandsOnFulfillmentCenterDataResource
- MessagingUpdateAdministratorsForOrgExecuteMessagingUpdateCommandsOnStoreEntityResource

조달

데이터 자원:

- ProcurementAdministratorsForOrgExecuteProcurementAuthenticationAndRegistration OnOrganizationResource
- ProcurementShoppingCartManagersExecuteProcurementShoppingCartManageOnOrderResource

쿠폰

데이터 자원:

- CouponAdministratorsForOrgExecuteCouponPromotionCreateCommandsOnStoreEntityResource
- CouponAdministratorsForOrgExecuteCouponPromotionDeleteCommandsOnCouponPromotionResource
- AllUsersExecuteCouponRedemptionCommandsOnCouponWalletResource
- AllUsersExecuteCouponDeleteCommandsOnCouponWalletResource
- CouponAdministratorsForOrgExecuteCouponPromotionUpdateCommandsOnStoreEntityResource
- AllUsersExecuteCouponSaveCommandsOnCouponWalletResource

데이터 bean: CouponAdministratorsForOrgDisplayECouponPromotionBeans

고객 프로파일링

데이터 자원: CustomerProfileEditorsForOrgExecuteSegmentManageCommandsOnStoreEntityResource

데이터 bean: CustomerProfileEditorsForOrgDisplaySegmentationDatabeansResourceGroup

할인

데이터 자원:

- DiscountAdministratorsForOrgExecuteDiscountCreateCommandsOnStoreEntityResource
- DiscountAdministratorsForOrgExecuteDiscountDeployCommandsOnCalculationCodeResource
- DiscountAdministratorsForOrgExecuteDiscountAssociateCommandsOnCalculationCodeResource

데이터 bean: DiscountViewersForOrgDisplayDiscountDatabeans

재고 관리

데이터 자원:

- FulfillmentCenterManagersForOrgExecuteFulfillmentCenterCreateCommandsOn OrganizationResource
- FulfillmentCenterManagersForOrgExecuteFulfillmentCenterManageCommandsOn FulfillmentCenterResource
- PickBatchInventoryManagersForOrgExecuteReleaseReadyShipCommandsOn FulfillmentCenterResource
- VendorInventoryManagersForOrgExecuteVendorManageCommandsOnVendorResource
- VendorInventoryManagersForOrgExecuteVendorCreateCommandsOnStoreEntityResource
- ExpectedInventoryManagersForOrgExecuteInventoryManageCommandsOnStoreEntityResource
- PickPackGeneratorsForOrgExecutePickPackGenerateCommandsOnFulfillmentCenterResource
- InventoryAdjustersForOrgExecuteInventoryAdjustCommandsOnStoreEntityResource
- ReturnReasonsManagersForOrgExecuteReturnReasonsCommandsOnStoreEntityResource
- FulfillmentCenterManagersForOrgExecuteFulfillmentCenterReleaseOnFulfillmentCenter ReleaseDataResourceGroup
- SharedFulfillmentCenterPickBatchInventoryManagersExecuteReleaseReadyShipCommands OnFulfillmentCenterDataResource
- SharedFulfillmentCenterPickPackGeneratorsExecutePickPackGenerateCommands OnFulfillmentCenterResource
- SharedFulfillmentCenterManagersExecuteFulfillmentCenterReleaseCommandsOnFulfillment CenterReleaseDataResourceGroup

데이터 bean:

- ReturnReasonsManagersForOrgDisplayReturnReasonsOrderManagementDataBeansResourceGroup
- ExpectedInventoryManagersForOrgDisplayExpectedInventoryDataBeansResourceGroup
- VendorInventoryManagersForOrgDisplayVendorInventoryDataBeansResourceGroup
- ProductFindInventoryManagersForOrgDisplayProductFindInventoryDataBeansResourceGroup
- FulfillmentCenterManagersForOrgDisplayFulfillmentCenterDataBeansResourceGroup
- PickBatchInventoryManagersForOrgDisplayPickBatchInventoryDataBeansResourceGroup
- ReceiverOrderManagersForOrgDisplayReceiverOrderManagementDataBeansResourceGroup

- ReturnsAdminOrderManagersForOrgDisplayReturnsAdminOrderManagementDataBeans ResourceGroup
- SuperUserOrderManagersForOrgDisplaySuperUserOrderManagementDataBeans ResourceGroupFulfillmentManagersForOrgDisplayReleaseOrderItemsDatabeanResourceGroup

주문 관리

데이터 자원:

- CustomerOrderManagersForOrgExecuteCustomerServiceOrderWriteCommands OnOrderResource
- CustomerOrderManagersForOrgExecuteCustomerServiceOrderCreateCommands OnStoreEntityResource
- CustomerOrderManagersForOrgExecuteCustomerServiceReturnWriteCommands OnRMAResource
- CustomerOrderManagersForOrgExecuteCustomerServiceReturnCreateCommands OnStoreEntityResource
- CustomerOrderManagersExecuteCustomerWriteCommandsOnUserResource
- CustomerOrderManagersForDefaultOrgExecuteCustomerServiceCustomerWriteCommandsOn UserDataResourceGroupwithGuestRegisterType

데이터 bean:

- CustomerOrderManagersForOrgDisplayCustomerOrderManagementDatabeans
- MemberOrderManagersForDefaultOrgDisplayGuestMemberDatabeans
- MemberOrderManagersDisplayOrganizationSpecificDatabeans
- MemberOrderManagersDisplayUserDatabeanResourceGroup
- UserOrderManagersForDefaultOrgDisplayGuestMemberDatabeans
- UserOrderManagersDisplayOrganizationSpecificDatabeans
- UserOrderManagersDisplayUserDatabeanResourceGroup
- LogisticsManagersForOrgDisplayOrdersAndReturnsListsDatabeans
- ReturnsManagersForOrgDisplayReturnsListsDatabeans

Payments

데이터 자원:

- AccountManagersForOrgExecuteAccountCreateCommandsOnOrganizationResource
- AccountAdministratorsForOrgExecuteAccountManageCommandsOnAccountResource
- AccountViewersForOrgExecutePaymentSummaryGenerateCommandsOnAccountResource
- AccountViewersForOrgExecuteStorePaymentAdminCommandsOnStoreEntityResource
- AllUsersExecutePaymentOrderWriteCommandsOnOrderResource

정책 편집기

데이터 자원:

- StoreAdministratorsForOrgExecuteACPolicyCreateCommandsOnOrganizationResource

- StoreAdministratorsForOrgExecuteACPolicyEditCommandsOnACPolicyResource
- StoreAdministratorsForOrgExecuteACViewPoliciesForUpdateActionsOnOrganizationResource
- StoreAdministratorsForOrgExecuteACViewApplicablePoliciesActionsOnOrganizationResource
- DescendantStoreAdministratorsExecuteACViewPoliciesForOrgActionsOnOrganizationResource

데이터 bean: StoreAdministratorsForOrgExecuteUserGroupSearchViews

상품 어드바이저

데이터 bean:

- ProductAdvisorStatisticiansForOrgDisplayProductAdvisorStatisticsDatabeans
- SalesAssistantStatisticiansForOrgDisplaySalesAssistantStatisticsDatabeans
- ProductAdvisorManagersDisplayPAWCBEDatabeanResourceGroup
- GuidedSellManagersDisplayGSWCBEDatabeanResourceGroup

RFQ

데이터 자원:

- RFQBuyersExecuteRFQCreateCommandsOnStoreEntityDataResourceGroup
- RFQBuyersManageRFQResourcesTheyOwn
- RFQBuyersManageRFQResponsesForRFQsTheyOwn
- RFQAdministratorsAdministerRFQs
- RFQAdministratorsManageRFQResponses
- RFQSalesManagersForOrgCreateRFQResponse
- RFQSalesManagersExecuteRFQResponseManageCommandsOnRFQResponseResource
- RFQSalesManagersExecuteRFQResponseAdminCommandsOnRFQWithPublicAccess TypeResourceGroup
- RFQSalesManagersExecuteRFQResponseAdminCommandsOnRFQResourceGroup

데이터 bean:

- RFQBuyersDisplayRFQDataBeanResourceGroupTheyOwn
- RFQBuyersDisplayRFQResponseDataBeansViewabletoRFQOwnerResourceGroup
- RFQSalesViewersDisplayRFQResponseDataBeanResourceGroup
- RFQSalesViewersDisplayRFQDataBeanWithPublicAccessTypeResourceGroup
- RFQSalesViewersDisplayRFQDataBeanResourceGroup

규칙

데이터 자원: StoreAdministratorsForOrgExecutePersonalizationRuleServiceAdministrationCommands OnStoreEntityResource

데이터 bean:
StoreAdministratorsForOrgDisplayPersonalizationRuleServiceAdministrationDataBeanResourceGroup

스케줄러

데이터 자원:

- StoreAdministratorsForOrgExecuteScheduledJobManageCommandsOnStoreEntityResource
- StoreAdministratorsForOrgExecuteScheduledJobManageCommandsOnUserResource

데이터 bean: StoreAdministratorsForOrgDisplaySchedulerDataBeansResourceGroup

Commerce 액셀러레이터

데이터 자원:

- B2CCSAViewUsersForOrgExecuteB2CCSAViewActionsOnStoreEntityResource
- B2BCSAViewUsersForOrgExecuteB2BCSAViewActionsOnStoreEntityResource
- CHSCSAViewUsersForOrgExecuteCHSCSAViewActionsOnStoreEntityResource
- RHSCSAViewUsersForOrgExecuteRHSCSAViewActionsOnStoreEntityResource
- CPSCSAViewUsersForOrgExecuteCPSCSAViewActionsOnStoreEntityResource
- RPSCSAViewUsersForOrgExecuteRPSCSAViewActionsOnStoreEntityResource
- HCPCSAViewUsersForOrgExecuteHCPCSAViewActionsOnStoreEntityResource
- MHSCSAViewUsersForOrgExecuteMHSCSAViewActionsOnStoreEntityResource
- MPSCSAViewUsersForOrgExecuteMPSCSAViewActionsOnStoreEntityResource
- SCPCSAViewUsersForOrgExecuteSCPCSAViewActionsOnStoreEntityResource
- SHSCSAViewUsersForOrgExecuteSHSCSAViewActionsOnStoreEntityResource
- SPSCSAViewUsersForOrgExecuteSPSCSAViewActionsOnStoreEntityResource

운송

데이터 자원: ShippingMembershipAdministratorsForOrgExecuteShippingManageCommandsOnStore DataResourceGroup

데이터 bean: ShippingMembershipAdministratorsForOrgDisplayShippingDatabeanResourceGroup

과세

데이터 자원: TaxationAdministratorsForOrgExecuteTaxationManageCommandsOnStoreDataResourceGroup

데이터 bean: TaxationAdministratorsForOrgDisplayTaxationDatabeanResourceGroup

실시간 도움말/협업 작업 영역/고객 지원

데이터 자원: 실시간 도움말:

- LiveHelpAgentsForOrgExecuteLiveHelpRetrieveCommandsOnUserDataResources
- LiveHelpAgentsForOrgExecuteLiveHelpRetrieveCommandsOnOrderDataResources

데이터 자원: 고객 지원:
CustomerCareAdministratorsForOrgExecuteCustomerCareQueueManageCommandsOnStoreResource

데이터 bean: 실시간 도움말: LiveHelpAgentsForOrgDisplayCustomerCareDatabeanResourceGroup

데이터 bean: 협업 작업 영역:
CollaborativeWorkspaceAdministratorsForOrgDisplayCollaborativeWorkspaceDatabeanResourceGroup

상점 상태

데이터 자원:

- ChannelManagersExecuteStoreStateChangeCommandsOnStoreResource
- AdministrativeRolesForOrgExecuteStoreStateChangeCommandsOnStoreResource
- AdministratorsForOrgAccessStoreWithCloseOrSuspendStateResourceGroup
- AllUsersAccessStoreWithOpenStateResourceGroup

상점 관리

데이터 자원: 보고서 운송:
ReportDeliveryManagersForOrgExecuteSetupReportDeliveryCommandsOnStoreDataResourceGroup

데이터 자원: 상점:

- StoreFrontManagersForOrgExecuteStoreFrontRelatedUpdateOnStoreEntityResource
- StoreProfileManagersForOrgExecuteStoreProfileRelatedUpdateOnStoreEntityResource

---

기본 액세스 제어 정책 그룹

WebSphere Commerce와 함께 제공된 기본 액세스 제어 정책 그룹은 다음과 같습니다.

- 관리 및 운영 정책 그룹: 이 정책 그룹에는 모든 구성원 관리가 포함되며 운영 정책을 저장합니다.
- 게스트 구매자 관리 정책 그룹: 이 정책 그룹에는 게스트 구매자 관리와 관련된 모든 정책이 포함됩니다.
- 공통 구매 정책 그룹: 이 정책 그룹에는 직접형 B2C 및 B2B 시나리오 둘 모두에 공통인 모든 구매 관련 정책이 포함됩니다.
- B2C 정책 그룹: 이 정책 그룹에는 모든 직접형 B2C 특정 구매 정책이 포함됩니다.
- B2B 정책 그룹: 이 정책 그룹에는 모든 B2B 특정 구매 정책이 포함됩니다.

주: 관리 및 운영 정책 그룹은 일반적으로 모든 조직에 적용되어야 하는 핵심 정책 그룹입니다. 조직에서 임의의 정책 그룹에 등록할 때마다, 이 정책 그룹을 등록해야 합니다. 관리 및 운영 정책 그룹 외에도, 상점 유형에 따라 상점을 소유하는 조직의 경우, 공통 구매 정책 그룹, B2C 정책 그룹 및 B2B 정책 그룹에 등록해야 합니다. 게스트 구매자 관리 정책 그룹은 공통 시나리오의 기본 조직인 게스트 구매자를 소유하는 조직에서 등록해야만 합니다.

주의사항

이 정보는 미국에서 제공되는 제품 및 서비스용으로 작성된 것입니다.

IBM은 다른 국가에서 이 자료에 기술된 제품, 서비스 또는 기능을 제공하지 않을 수도 있습니다. 현재 사용 가능한 제품 및 서비스에 대한 정보는 한국 IBM 담당자에게 문의하십시오. 이 책에서 IBM 제품, 프로그램 또는 서비스를 언급하는 것이 해당 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM의 지적 재산권을 침해하지 않는 한, 기능상 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 라이센스까지 부여하는 것은 아닙니다. 라이센스에 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 라이센스 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) 묵시적으든 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 통지없이 언제든지 개선 및(또는) 변경할 수 있습니다.

이 정보에서 언급되는 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.

본 문서에 포함된 모든 성능 데이터는 제한된 환경에서 산출된 것입니다. 따라서 다른 운영 환경에서 얻어진 결과는 상당히 다를 수 있습니다. 일부 성능은 개발 레벨 상태의 시스템에서 측정되었을 수 있으므로 이러한 측정치가 일반적으로 사용되고 있는 시스템에서도 동일하게 나타날 것이라고는 보증할 수 없습니다. 또한, 일부 성능은 추정치일 수도 있으므로 실제 결과는 다를 수 있습니다. 이 문서의 사용자는 해당 데이터를 사용자의 특정 환경에서 검증해야 합니다.

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 비IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오.

IBM의 향후 방향 또는 의도에 대한 모든 언급은 사전 통고 없이 변경되거나 취소될 수 있으며 단지 목표만을 나타내는 것입니다.

이 정보에는 일상의 비즈니스 운영에서 사용되는 자료 및 보고서의 예제가 들어 있습니다. 이들 예제에는 개념을 가능한 완벽하게 설명하기 위해 개인, 회사, 브랜드 및 제품의 이름이 사용될 수 있습니다. 이들 이름은 모두 가공의 것이며 실제 기업의 이름 및 주소와 유사하더라도 이는 전적으로 우연입니다.

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.

저작권

상표

IBM 한글 지원에 관한 설문

IBM WebSphere Commerce
보안 안내서
버전 5.5

FAX : (02) 3787-0123

보내 주시는 의견은 더 나은 고객 지원 체제를 위한 귀중한 자료가 됩니다. 독자 여러분의 좋은 의견을 기다립니다.

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.