

버전 6.2.0



보안 응용프로그램 및 환경

버전 6.2.0



보안 응용프로그램 및 환경

주!

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, 이 문서의 맨 마지막의 주의사항 섹션의 일반 정보를 읽으십시오.

2008년 12월 12일

이 개정판은 새 개정판에 별도로 명시하지 않는 한, 멀티플랫폼용 WebSphere Process Server의 버전 6, 릴리스 2, 수정 2(제품 번호 5724-L01) 및 모든 후속 릴리스와 수정에 적용됩니다.

이 문서에 대한 사용자 의견을 보내시려면 ibmkspoe@kr.ibm.com으로 전자 우편 메시지를 보내십시오. 사용자의 의견을 기다리고 있습니다.

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

© Copyright International Business Machines Corporation 2005, 2008.

PDF 서적 및 Information Center

PDF 서적은 인쇄 및 오프라인 사용을 위한 목적으로 제공됩니다. 최신 정보는 온라인 Information Center를 참조하십시오.



PDF 서적은 Information Center와 동일한 내용을 제공합니다.

PDF 문서는 버전 6.0 또는 버전 6.1과 같이 주요 Information Center 릴리스 이후 분기 내에 사용 가능합니다.

PDF 문서는 Information Center보다 갱신되는 빈도는 적지만 Redbooks®보다 자주 갱신됩니다. 일반적으로 PDF 서적은 변경사항이 많을 경우에 갱신됩니다.

PDF 서적 외부에 있는 주제에 대한 링크는 Information Center 웹 사이트로 연결합니다. PDF 서적 외부의 대상에 대한 링크는 대상이 PDF 서적 또는 웹 페이지인지를 나타내는 아이콘으로 표시됩니다.

표 1. 이 서적 외부에 있는 주제에 대한 링크 접두부가 붙은 아이콘

아이콘	설명
	<p>Information Center의 페이지를 포함한 웹 페이지에 대한 링크</p> <p>Information Center에 대한 링크는 간접 라우팅 서비스를 통해 연결되기 때문에 대상 주제가 새 위치로 이동해도 지속적으로 작동합니다.</p> <p>로컬 Information Center에서 링크된 페이지를 찾으려는 경우 링크 제목을 검색할 수 있습니다. 또는 주제 ID를 검색할 수 있습니다. 다른 제품에 대해 여러 개의 검색 결과를 찾은 경우에는, 그룹별 제어를 사용하여 확인하려는 주제 인스턴스를 식별할 수 있습니다. 예를 들어 다음과 같습니다.</p> <ol style="list-style-type: none"> 1. 링크 URL 복사는 링크를 마우스 오른쪽 단추로 클릭한 후 링크 위치 복사를 선택하십시오. 예: <code>http://www14.software.ibm.com/webapp/wsbroker/redirect?version=wbpm620&product=wesb-dist&topic=tins_apply_service</code> 2. <code>&topic=</code> 뒤에 주제 ID를 복사하십시오. 예: <code>tins_apply_service</code> 3. 로컬 Information Center의 검색 필드에 주제 ID를 붙여넣으십시오. 로컬로 설치되어 있는 문서 기능이 있으면 검색 결과에 주제가 표시됩니다. 예를 들어 다음과 같습니다. <div style="border: 1px solid black; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p>1개의 결과를 찾음</p> <p>그룹 분류: 없음 플랫폼 버전 제품</p> <p>요약 표시</p> <p>설치 갱신 프로그램으로 픽스팩 및 갱신 팩 설치</p> </div> <ol style="list-style-type: none"> 4. 검색 결과에서 링크를 클릭하여 주제를 표시하십시오.
	PDF 서적의 링크

목차

PDF 서적 및 Information Center	iii	WebSphere Process Server의 전개 환경 보안	27
응용프로그램 및 환경 보안	1	보안 사용 가능	30
보안의 일반 개요	1	사용자 계정 저장소 구성	34
보안 시작	3	서버 시작 및 중지	41
WebSphere Process Server 설치: 보안 고려사항	5	관리 보안 역할	42
설치 시 제공되는 인증 정보	6	설치된 컴포넌트의 기본 보안	44
독립형 서버에 대해 WebSphere Process Server 보안 구성	7	WebSphere Process Server에서 응용프로그램 보안	47
독립형 WebSphere Process Server 설치 보안	7	응용프로그램 보안 요소	47
보안 사용 가능	10	보안 응용프로그램 전개(설치)	53
사용자 계정 저장소 구성	14	비즈니스 달력 관리자 보안	56
서버 시작 및 중지	21	어댑터 보안	60
관리 보안 역할	23	휴먼 태스크 및 비즈니스 프로세스 보안	61
설치된 컴포넌트의 기본 보안	24	Business Space에 대한 보안 설정	62
전개 환경 서버에 대해 WebSphere Process Server 보안 구성	27	종단간 보안 작성	65
		주의사항	69

응용프로그램 및 환경 보안

WebSphere® Process Server 환경 보안에는 관리 보안 사용, 응용프로그램 보안 사용, 보안을 사용한 프로파일 작성 및 선택한 사용자로 중요 기능의 액세스 제한이 포함됩니다.

WebSphere Process Server 보안은 WebSphere Application Server 버전 6.1 보안을 기반으로 합니다. 이러한 문서는 WebSphere Application Server Information Center 와 특히 WebSphere Application Server Security Documentation, 『응용프로그램 및 환경 보안』에 있는 핵심 보안 문서의 보충 정보입니다.

관련 정보

PDF 문서

WebSphere Process Server 문서(PDF 형식)

정보 길잡이

IBM developerWorks의 Business Process Management 정보 길잡이는 WebSphere Process Server, WebSphere ESB 및 기타 제품에 대한 정보를 포트폴리오로 구성합니다.

IBM Education Assistant

IBM Education Assistant에서 제공하는 WebSphere Process Server에 대한 멀티미디어 교육 모듈입니다.

기술 노트

WebSphere Process Server Support > 기술 노트는 6.2 보안 카테고리 문서를 검색합니다. 문서 유형, 제품 카테고리 및 검색 용어 필드를 사용하여 필요한 정보를 찾으십시오.

개요

제품 라이브러리 웹 페이지의 개요 탭입니다. 이 페이지를 사용하면 WebSphere ESB 와 관련된 발표 문서, 데이터 시트 및 기타 일반 라이브러리 문서에 액세스할 수 있습니다.

보안의 일반 개요

WebSphere Process Server 보안은 WebSphere Application Server 버전 6.1 보안을 기반으로 합니다.

보안에 대한 자세한 정보는 WebSphere Application Server Network Deployment Information Center를 참조하십시오.

보안 타스크는 WebSphere Process Server 환경에서 보안 관리에 관한 타스크와 WebSphere Process Server에서 실행 중인 응용프로그램 관련 타스크로 크게 나누어 질 수 있습니다. 서버 환경 보안이 응용프로그램 보안의 핵심이므로 두 측면을 따로 분리해서 생각하지 않아야 합니다.

환경 보안에는 관리 보안 및 응용프로그램 보안의 사용 가능 설정, 보안을 사용한 프로파일 작성 및 선택한 사용자로 중요 기능의 액세스 제한이 포함됩니다.

응용프로그램 보안에는 여러 측면이 있습니다. 여기에는 다음이 포함될 수 있습니다.

- 사용자 인증 - 응용프로그램을 호출하는 사용자 또는 프로세스를 인증해야 합니다. 단일 사인온으로 사용자는 인증 데이터를 한 번 제공한 후 이 인증 정보를 다운로드 컴포넌트로 전달할 수 있습니다.
- 액세스 제어 - 인증된 사용자가 조작을 수행할 수 있는 권한을 가지고 있는지 여부를 의미합니다.
- 데이터 무결성 및 프라이버시 - 응용프로그램이 액세스하는 데이터는 권한이 없는 관제자가 어떤 방법으로도 보거나 수정할 수 없도록 보안을 유지해야 합니다.

이 절의 나머지 부분에서는 WebSphere Process Server 조작의 다양한 단계에서 필요한 보안 고려사항에 대해 자세하게 설명합니다.

관련 개념

48 페이지의 『사용자 인증』

관리 보안이 작동되면 클라이언트를 인증해야 합니다.

50 페이지의 『액세스 제어』

액세스 제어는 인증된 사용자가 자원에 액세스하거나 특정 조작을 수행하는 데 필요한 권한을 가지고 있는지 확인하는 것입니다.

52 페이지의 『데이터 무결성 및 프라이버시』

WebSphere Process Server 프로세스의 호출 시에 액세스되는 데이터의 프라이버시 및 무결성은 보안에 중요합니다.

53 페이지의 『단일 사인온』

사용자 이름 및 암호 정보를 한 번만 제공하라는 질문이 클라이언트에 표시됩니다. 제공된 ID는 시스템 전반에 걸쳐 사용됩니다.

WebSphere Process Server에 특정한 보안 고려사항

WebSphere Process Server 보안은 WebSphere Application Server 6.1 보안에서 빌드됩니다. WebSphere Process Server에 특정한 고려사항이 표시됩니다.

- 관리 콘솔 패널 비즈니스 통합 보안은 WebSphere Process Server에 고유합니다. 보안을 펼치고 비즈니스 통합 보안을 클릭하여 이 패널을 표시합니다. 이 패널에서는

사용자가 자신의 사용자 레지스트리에서 중요한 비즈니스 통합 인증 별명으로 특정 ID를 지정할 수 있습니다. 또한 이 패널에서 Business Process Choreographer 보안 설정을 관리할 수 있습니다.

- 응용프로그램 보안은 기본적으로 WebSphere Process Server에서 작동됩니다. WebSphere Application Server에서는 그렇지 않습니다.
- WebSphere Process Server에는 컴포넌트 특정 보안 역할 세트가 있습니다.

보안 시작

보안은 WebSphere Process Server 설치를 계획할 때, 응용프로그램을 개발하고 전개할 때 및 사용자 프로세스 서버를 매일 실행할 때 중요한 고려사항입니다.

다음 목록은 WebSphere Process Server 보안을 설정할 때 수행하는 TASK의 개요를 제공합니다.

1. WebSphere Process Server를 설치할 때 보안을 고려하십시오.
2. 독립형 또는 전개 환경 설치에 대해 보안이 작동하는지 확인하십시오.
 - a. 관리 보안이 작동하는지 확인하십시오.
 - b. 응용프로그램 보안이 작동하는지 확인하십시오.
 - c. 필요한 경우 Java™ 2 보안을 작동시키십시오.
 - d. 관리 콘솔에서 보안 구성 마법사를 사용하여 보안 옵션을 구성하십시오.
 - e. 보안 인증 메커니즘과 사용자 계정 저장소를 설정하십시오.
 - f. 중요한 비즈니스 통합 인증 별명에 사용자 이름 및 암호를 지정하십시오.
 - g. 적절한 관리 보안 역할에 사용자를 지정하십시오.
3. 특정 WebSphere Process Server 컴포넌트에 대한 보안을 설정하십시오. 예를 들어, 보안 관리자를 사용하여 비즈니스 달력 관리자에 있는 시간표에 대한 역할 기반 액세스 제어를 설정하십시오.
4. 프로세스 서버 환경에 전개할 응용프로그램을 보호하십시오.
 - a. 해당되는 모든 보안 기능을 사용하여 WebSphere Integration Developer에서 응용프로그램을 전개하십시오.
 - b. WebSphere Process Server 환경에 응용프로그램을 전개하십시오.
 - c. 새로 전개된 응용프로그램에 대한 액세스를 제어할 적절한 보안 역할에 사용자 또는 그룹을 지정하십시오.
5. WebSphere Process Server 환경의 보안을 유지보수하십시오.

관련 TASK

5 페이지의 『WebSphere Process Server 설치: 보안 고려사항』

WebSphere Process Server 설치 전, 설치 중 및 설치 후 보안을 구현하는 방법을 고려하십시오.

10 페이지의 『보안 사용 가능』

WebSphere Process Server 환경 및 응용프로그램 보안 설정을 위한 첫 번째 단계는 관리 보안을 사용하도록 설정하는 것입니다.

14 페이지의 『사용자 계정 저장소 구성』

등록된 사용자의 사용자 이름 및 암호가 사용자 계정 레지스트리에 저장됩니다. 로컬 운영 체제(기본값), LDAP(Lightweight Directory Access Protocol), 연합 저장소 또는 사용자 정의 계정 저장소의 사용자 계정 저장소를 사용할 수 있습니다.

보안 컴포넌트 개발

개발한 컴포넌트에 대해 보안을 설정하십시오. 컴포넌트는 메소드가 있는 인터페이스를 구현합니다. SCA(Service Component Architecture) 규정자 SecurityPermission을 사용하여 인터페이스 또는 메소드에 보안을 설정하십시오.

53 페이지의 『보안 응용프로그램 전개(설치)』

보안 제한(보안 응용프로그램)이 있는 응용프로그램의 전개는 보안 제한이 없는 응용프로그램의 전개와 유사합니다. 활성 사용자 레지스트리가 올바른 보안 응용프로그램의 역할로 사용자 및 그룹을 지정해야 하는 것만 다릅니다. 보안 응용프로그램을 설치하는 경우 역할이 응용프로그램에 정의되어 있을 수 있습니다. 응용프로그램에서 위임이 필요했다면 RunAs 역할 또한 정의되며 유효한 사용자 이름 및 암호를 제공해야 합니다.

55 페이지의 『역할에 사용자 지정』

보안 응용프로그램은 securityPermission 및 securityIdentity인 두 개 규정자 중 하나 또는 둘 모두를 사용합니다. 이 규정자가 있으면 응용프로그램 및 보안 기능이 올바르게 작동하기 위해 전개 시에 추가 단계를 수행해야 합니다.

56 페이지의 『비즈니스 달력 관리자 보안』

보안 관리자는 비즈니스 달력 관리자의 개별 시간표에 액세스 보안을 설정할 수 있는 기능을 제공합니다. 보안 관리자를 사용하여 조직 구성원에게 역할을 지정합니다. 이러한 역할로 시간표에 대한 액세스 레벨을 판별합니다.

관련 정보

7 페이지의 『독립형 서버에 대해 WebSphere Process Server 보안 구성』

WebSphere Process Server의 독립형 설치 보안 구성에는 관리 보안 사용 및 사용자 계정 레지스트리 구성과 같은 타스크가 포함됩니다.

27 페이지의 『전개 환경 서버에 대해 WebSphere Process Server 보안 구성』

WebSphere Process Server의 전개 환경 설치 보안 구성에는 관리 보안 사용 및 사용자 계정 레지스트리 구성과 같은 타스크가 포함됩니다.

WebSphere Process Server 설치: 보안 고려사항

WebSphere Process Server 설치 전, 설치 중 및 설치 후 보안을 구현하는 방법을 고려하십시오.

프로시저

1. 설치 전에 환경의 보안을 설정하십시오.

적절한 보안을 사용하여 WebSphere Process Server를 설치하는 데 필요한 명령은 운영 체제에 따라 다릅니다. 설치 이전에 수행할 단계에 대한 자세한 정보는 WebSphere Application Server Information Center의 설치 이전 환경 보안 주제를 참조하십시오.

i5/OS 적절한 보안을 사용하여 WebSphere Process Server를 설치하는 데 필요한 명령은 운영 체제에 따라 다릅니다. 설치 이전에 수행할 단계에 대한 자세한 정보는 관련 타스크에서 설치를 위한 **i5/OS** 시스템 준비 주제를 참조하십시오.

2. WebSphere Process Server 설치를 위한 운영 체제를 준비하십시오.

이 단계에는 WebSphere Process Server의 설치를 위해 서로 다른 운영 체제를 준비하는 방법 관련 정보가 들어 있습니다. 설치를 위한 운영 체제 준비에 대한 자세한 정보는 WebSphere Application Server Information Center의 제품 설치를 위한 운영 체제 준비 주제를 참조하십시오.

3. 설치 후에 환경을 보안 설정하십시오.

이 타스크에서는 WebSphere Process Server를 설치한 후 암호 정보를 보호하는 방법에 관한 정보를 제공합니다. 설치 후 환경 보안에 대한 자세한 정보는 WebSphere Application Server Information Center의 설치 후 환경 보안 주제를 참조하십시오.

다음에 수행할 작업


설치를 완료했다면 관리 콘솔에서 보안을 관리할 수 있습니다.

관련 개념

3 페이지의 『보안 시작』


보안은 WebSphere Process Server 설치를 계획할 때, 응용프로그램을 개발하고 전개할 때 및 사용자 프로세스 서버를 매일 실행할 때 중요한 고려사항입니다.

관련 정보

 설치 전 환경 보안

 제품 설치를 위한 운영 체제 준비

 설치 후 환경 보안

 설치를 위해 i5/OS 시스템 준비

설치 시 제공되는 인증 정보

설치 중에 WebSphere Process Server 환경에 즉시 보안이 설정되도록 보안 정보에 대한 프롬프트가 표시됩니다.

WebSphere Process Server의 이전 릴리스에서는 설치 중 다양한 인증 정보에 대해 묻는 프롬프트가 표시되었습니다. 이제 모든 컴포넌트의 기본값은 사용자가 제공하는 1차 관리 신임으로 설정됩니다. 이 기본값은 기본 보안을 제공하지만 설치의 보안을 강화하기 위해서는 관리 콘솔을 사용하여 다양한 WebSphere Process Server 컴포넌트가 적절한 보안 ID를 갖도록 구성해야 합니다.

WebSphere Process Server 프로파일을 작성할 때 관리 보안 사용을 선택한 상태로 유지하는 경우 사용자 이름을 묻는 프롬프트가 표시됩니다. 이 ID는 모든 기본 컴포넌트의 기본값으로 사용됩니다. 보안을 더 강화하려면 프로파일 작성 후 이 ID를 구성해야 합니다.

WebSphere Process Server의 여러 컴포넌트에 인증 별명이 활용됩니다. 이 별명은 데이터베이스 및 메시징 엔진에 액세스하기 위해 런타임 컴포넌트를 인증하는 데 사용됩니다. 이 별명은 관리 콘솔의 비즈니스 통합 보안 패널에서 수정할 수 있습니다.

보안을 사용한 WebSphere Process Server 프로파일 작성

WebSphere Process Server 프로파일을 작성할 때 보안 신임으로 기본값이 사용됩니다. 프로파일을 작성한 후에 관리 콘솔에서 이 보안 설정을 구성해야 합니다.

이 태스크 정보

WebSphere Process Server 프로파일을 작성할 때, 관리자 ID를 기본값으로 사용하는 세 가지의 WebSphere Process Server 컴포넌트가 있습니다.

이 컴포넌트는 다음과 같습니다.

- SCA(Service Component Architecture)
- Business Process Choreographer
- CEI(Common Event Infrastructure)

이 컴포넌트와 연관되는 ID는 보안이 사용 가능할 때 필요한 인증 별명을 작성하는 데 사용됩니다. 이 ID를 계정 저장소의 적절한 사용자로 변경하는 것이 중요합니다.

프로시저

1. 관리 콘솔에서 비즈니스 통합 보안 패널을 표시하십시오. 보안을 펼치고 비즈니스 통합 보안을 클릭하십시오.
2. 서비스 컴포넌트 아키텍처, Business Process Choreographer 및 CEI(Common Event Infrastructure) 인증 별명 각각에 대해 인증 별명으로 사용할 적절한 사용자 이름 및 암호를 제공하십시오.

- a. 별명 열에서 해당 이름을 클릭하여 변경하려는 별명을 선택하십시오.

주: 경우에 따라서는 별명 열에 링크가 제공되지 않을 수도 있습니다. 이러한 경우 편집하려는 별명에 해당되는 선택 열에서 선택란을 선택란을 선택한 후 편집을 클릭합니다.

- b. 다음 패널에서 이 컴포넌트의 인증 별명으로 사용할 사용자 이름 및 암호를 제공하십시오.

주: 사용자가 제공하는 신임은 사용자가 사용하는 사용자 계정 저장소에 존재해야 합니다.

- c. 확인을 클릭하십시오.

관련 태스크

49 페이지의 『인증 별명 수정』

기존 인증 별명을 수정해야 할 수도 있습니다.

독립형 서버에 대해 WebSphere Process Server 보안 구성

WebSphere Process Server의 독립형 설치 보안 구성에는 관리 보안 사용 및 사용자 계정 레지스트리 구성과 같은 태스크가 포함됩니다.

관련 개념

3 페이지의 『보안 시작』

보안은 WebSphere Process Server 설치를 계획할 때, 응용프로그램을 개발하고 전개할 때 및 사용자 프로세스 서버를 매일 실행할 때 중요한 고려사항입니다.

독립형 WebSphere Process Server 설치 보안

WebSphere Process Server 환경의 보안은 관리 콘솔에서 제어됩니다. 특권이 충분한 사용자는 관리 콘솔에서 모든 응용프로그램 보안을 작동 또는 정지시킬 수 있습니다. 따라서 보안 응용프로그램을 전개하기 전에 환경 보안이 이루어져야 합니다.

시작하기 전에

이 태스크를 시작하기 전에 WebSphere Process Server를 설치하고 설치를 검증해야 합니다.

이 태스크 정보

WebSphere Process Server 환경이 프로파일 내에 정의되어 있습니다. 보안화할 프로파일에 대해 관리 콘솔을 여십시오. 임의 사용자 ID나 사용하여 콘솔에 로그인하십시오. 프로파일의 보안이 이루어질 때까지는 모든 사용자 이름이 허용됩니다.

다음 단계에서는 보안을 사용 가능하게 하기 위해 수행하는 태스크의 길잡이를 제공합니다. 이 태스크에 대한 특정 세부사항은 다음 주제에서 제공됩니다.

프로시저

1. 관리 보안이 작동되는지 확인하십시오. 10 페이지의 『보안 사용 가능』
2. 응용프로그램 보안이 작동하는지 확인하십시오. 47 페이지의 『WebSphere Process Server에서 응용프로그램 보안』
3. 관리 역할에 사용자나 그룹을 추가하십시오. 관리 사용자 역할 또는 관리 그룹 역할에 따라 개별 사용자나 사용자 그룹에 관리 권한을 부여할 수 있습니다.
4. 사용하려는 사용자 계정 저장소를 선택하십시오.

다음 표에는 사용자 레지스트리를 선택 및 구성하는 데 필요한 조치 및 사용자 레지스트리의 선택사항이 설명되어 있습니다.

사용자 레지스트리	조치
연합 저장소	<p>단일 범주 아래에 있는 여러 저장소에서 프로파일을 관리하려면 이 설정을 지정하십시오. 범주는 다음에서 ID로 구성될 수 있습니다.</p> <ul style="list-style-type: none"> • 시스템에 빌드된 파일 기반 저장소 • 하나 이상의 외부 저장소 • 내장된 파일 기반 저장소와 하나 이상의 외부 저장소 <p>주: 관리자 특권을 가지고 있는 사용자만 연합 저장소 구성을 볼 수 있습니다. 자세한 정보는 연합 저장소 구성에서 범주 관리를 참조하십시오.</p>
로컬 운영 체제	<p>기본 사용자 레지스트리. 사용자 계정 레지스트리를 구성하는 방법에 대한 세부사항은 15 페이지의 『로컬 운영 체제 또는 독립형 사용자 정의 사용자 계정 저장소 구성』을 참조하십시오.</p>
독립형 LDAP 레지스트리	<p>"사용자 레지스트리로 LDAP(Lightweight Directory Access Protocol) 구성"의 지시사항에 따라 사용자 계정 레지스트리로 LDAP을 구성하십시오.</p>
독립형 사용자 정의 레지스트리	<p>사용자 계정 레지스트리를 구성하는 방법에 대한 세부사항은 15 페이지의 『로컬 운영 체제 또는 독립형 사용자 정의 사용자 계정 저장소 구성』을 참조하십시오.</p>

5. 선택한 레지스트리를 현재 레지스트리로 설정했는지 확인하십시오.

아직 이를 수행하지 않은 경우 관리, 응용프로그램 및 하부 구조 보안 페이지의 맨 아래에 있는 현재로 설정을 클릭하십시오.

6. 사용자 레지스트리를 선택한 후 변경사항을 적용했는지 확인하십시오.

아직 이를 수행하지 않은 경우 관리, 응용프로그램 및 하부 구조 보안 페이지의 맨 아래에 있는 적용을 클릭하십시오.

7. 비즈니스 통합 보안 패널로 이동하십시오. 보안을 펼치고 비즈니스 통합 보안을 클릭하십시오.
8. 표시된 인증 별명에 대해 적절한 사용자 ID를 제공하십시오. 사용자가 제공하는 신임은 사용자가 사용하는 사용자 계정 저장소에 존재해야 합니다.
9. 동일한 패널에서 Business Process Choreographer에 대해 보안을 구성할 수 있습니다.

비즈니스 플로우 및 휴먼 타스크 관리자에 대해 Business Process Choreographer 사용자 역할 맵핑을 설정하십시오.

- 관리자: 비즈니스 플로우 및 휴먼 타스크 관리자 역할에 대한 사용자 이름, 그룹 이름 또는 둘 다. 이 역할로 지정된 사용자는 모든 특권을 가집니다.
- 모니터: 비즈니스 플로우 및 휴먼 타스크 모니터 역할에 대한 사용자 이름, 그룹 이름 또는 둘 다. 이 역할에 지정된 사용자는 모든 비즈니스 프로세스 및 타스크 오브젝트의 특성을 볼 수 있습니다.

Business Process Choreographer 인증 별명은 Business Process Choreographer가 설치된 전개 대상마다 구성할 수 있습니다. 다음 인증 별명이 표시됩니다.

- JMS API 인증: 비동기 API 호출을 처리하기 위한 비즈니스 플로우 관리자 메시지 구동 Bean에 대한 인증
- 에스컬레이션 사용자 인증: 비동기 API 호출을 처리하기 위한 휴먼 타스크 관리자 메시지 구동 Bean에 대한 인증

10. 변경사항을 적용하십시오.

패널의 맨 아래에서 적용 단추를 클릭하십시오.

11. 로컬 구성에 대한 변경사항을 저장하십시오.

메시지 분할창에서 저장을 클릭하십시오.

12. 필요하면 서버를 중지한 후 다시 시작하십시오.

서버를 다시 시작해야 하는 경우 관리 콘솔에 적용 메시지가 나타납니다.

결과

다음에 관리 콘솔에 로그인할 때는 유효한 사용자 이름 및 암호를 제공해야 합니다.

다음에 수행할 작업

사용자가 작성하는 각 프로파일은 이 방법으로 보안을 설정해야 합니다. 시스템 관리자 ID는 환경을 설치 및 구성하는 동안 여러 곳에서 사용되었을 수 있습니다. 핵심 보안 기능 외의 모든 보안 기능에 대해 사용자 계정 저장소의 적절한 사용자 신임으로 이 ID를 대체하는 것이 좋습니다. 관리 콘솔에서 비즈니스 통합 보안 패널을 사용하여 ID 및 별명을 관리하십시오.

관련 태스크

『보안 사용 가능』

WebSphere Process Server 환경 및 응용프로그램 보안 설정을 위한 첫 번째 단계는 관리 보안을 사용하도록 설정하는 것입니다.

47 페이지의 『WebSphere Process Server에서 응용프로그램 보안』

WebSphere Process Server 인스턴스로 전개하는 응용프로그램은 보안을 설정하여 런타임 시에 적용해야 합니다.

관련 정보



WebSphere Process Server에 설치 확인 도구 사용

보안 사용 가능

WebSphere Process Server 환경 및 응용프로그램 보안 설정을 위한 첫 번째 단계는 관리 보안을 사용하도록 설정하는 것입니다.

시작하기 전에

이 태스크를 시작하기 전에 WebSphere Process Server를 설치하고 설치를 확인하십시오.

보안화할 프로파일에 대해 관리 콘솔을 여십시오. 임의 사용자 ID나 사용하여 콘솔에 로그인하십시오. 프로파일의 보안이 이루어질 때까지는 모든 사용자 이름이 허용됩니다.

이 태스크 정보

관리 보안, 응용프로그램 보안 및 Java 2 보안에 대한 정보는 하위 주제 아래에 표시된 정보를 참조하십시오.

프로시저

1. 관리 콘솔에서 관리 보안 패널을 여십시오.

보안을 펼치고 관리, 응용프로그램 및 하부 구조 보안을 클릭하십시오.

2. 관리 보안을 사용 가능하게 하십시오.

관리 보안 사용을 선택하십시오.

3. 응용프로그램 보안을 사용 가능하게 하십시오.

응용프로그램 보안 사용을 선택하십시오.

4. 옵션: 필요한 경우, Java 2 보안을 강화하십시오.

Java 2 보안 권한 확인을 강화하려면 **Java 2** 보안을 사용하여 로컬 자원으로 응용프로그램 액세스 제한을 선택하십시오.

Java 2 보안을 사용 가능하도록 하는 경우, 응용프로그램의 app.policy 파일 또는 was.policy 파일에서 필요한 사용 권한이 부여될 때까지 기본 정책에서 부여된 것보다 많은 Java 2 보안 사용 권한이 필요한 응용프로그램은 올바르게 실행되지 않을 수 있습니다. 모든 필수 사용 권한이 없는 응용프로그램에서 액세스 제어 예외가 생성됩니다. Java 2 보안에 대한 자세한 정보는 WebSphere Application Server Information Center의 Java 2 보안 정책 파일 구성 주제를 참조하십시오.

주: app.policy 파일에 대한 갱신사항은 app.policy 파일이 속하는 노드의 엔터프라이즈 응용프로그램에만 적용됩니다.

- a. 옵션: 응용프로그램에 사용자 정의 사용 권한이 부여된 경우 경고를 선택하십시오. filter.policy 파일에는 응용프로그램이 J2EE 1.3 스펙에 따라 가지고 있어야 하는 사용 권한 목록이 있습니다. 응용프로그램이 이 정책 파일에 지정된 권한으로 설치되고 이 옵션이 사용 가능한 경우 경고가 발행됩니다. 기본값을 사용할 수 있습니다.
 - b. 옵션: 자원 인증 데이터로 액세스 제한을 선택하십시오. 응용프로그램 액세스를 민감한 JCA(Java Connector Architecture) 맵핑 인증 데이터로 제한해야 하는 경우 이 옵션이 사용 가능하도록 설정하십시오.
5. 변경사항을 적용하십시오.

패널의 맨 아래에서 적용 단추를 클릭하십시오.

6. 로컬 구성에 대한 변경사항을 저장하십시오.

메시지 분할창에서 저장을 클릭하십시오.

7. 필요하면 서버를 중지한 후 다시 시작하십시오.

서버를 다시 시작해야 하는 경우 관리 콘솔에 적용 메시지가 나타납니다.

다음에 수행할 작업

작성하는 프로파일마다 관리 보안을 작동시켜야 합니다.

관련 개념

3 페이지의 『보안 시작』


보안은 WebSphere Process Server 설치를 계획할 때, 응용프로그램을 개발하고 전개할 때 및 사용자 프로세스 서버를 매일 실행할 때 중요한 고려사항입니다.

관련 태스크

47 페이지의 『WebSphere Process Server에서 응용프로그램 보안』

WebSphere Process Server 인스턴스로 전개하는 응용프로그램은 보안을 설정하여 런타임 시에 적용해야 합니다.

관련 정보

 Java 2 보안 정책 파일 구성

관리 보안

관리 보안은 보안이 항상 사용되는지 여부, 인증이 발생하는 레지스트리의 유형, 기타 값(기본값으로 작동하는 많은 값)을 판별합니다. 관리 보안을 올바르게 사용하지 않게 사용 가능하도록 설정하면 사용자가 관리 콘솔을 잠그거나 서버가 이상 종료될 수 있으므로 적절한 계획이 필요합니다.

관리 보안은 WebSphere Process Server에 대한 다양한 보안 설정을 활성화하는 "큰 스위치"로 생각할 수 있습니다. 이 설정의 값은 지정할 수 있지만 관리 보안이 활성화 될 때까지는 적용되지 않습니다. 설정에는 사용자 인증, SSL(Secure Sockets Layer)의 사용, 사용자 계정 저장소 선택사항이 포함됩니다. 특히, 인증 및 역할 기반 권한을 포함한 응용프로그램 보안은 관리 보안이 활성화되지 않으면 시행되지 않습니다. 관리 보안은 기본적으로 사용 가능합니다.

관리 보안은 전체 보안 도메인에 적용되는 보안 구성을 표시합니다. 보안 도메인은 동일한 사용자 레지스트리 범주 이름으로 구성된 모든 서버로 구성됩니다. 어떤 경우에는, 범주가 로컬 운영 체제 레지스트리의 시스템 이름이 될 수 있습니다. 이 경우 모든 응용프로그램 서버는 동일한 물리적 시스템에 위치해야 합니다. 다른 경우에서, 범주가 독립형 LDAP(Lightweight Directory Access Protocol) 레지스트리의 시스템 이름이 될 수 있습니다.

LDAP 프로토콜을 지원하는 사용자 레지스트리에 원격으로 액세스할 수 있으므로 다중 노드 구성이 지원됩니다. 따라서, 어디에서나 인증을 사용할 수 있습니다.

보안 도메인에 대한 기본 요구사항은 보안 도메인 내의 한 서버에서 레지스트리 또는 저장소에 의해 리턴된 액세스 ID가 동일한 보안 도메인 내의 다른 서버에 있는 레지스트리 또는 저장소에서 리턴된 것과 같은 액세스 ID여야 한다는 것입니다. 액세스 ID는 사용자의 고유한 ID로 자원에 대한 액세스가 허용되는지 판별하기 위해 권한 부여 중에 사용됩니다.

관리 보안 구성은 보안 도메인 내의 모든 서버에 적용됩니다.

관리 보안 작동 이유

관리 보안을 작동하면 권한이 없는 사용자로부터 서버를 보호하는 설정이 활성화됩니다. 관리 보안은 기본적으로 프로파일 작성 중에 사용 가능합니다. 개발 시스템과 같이 보

안이 필요하지 않은 환경이 있을 수 있습니다. 이와 같은 시스템에서는 관리 보안을 사용하지 않도록 선택할 수 있습니다. 그러나 대부분의 환경에서는 권한이 없는 사용자가 관리 콘솔과 비즈니스 응용프로그램에 액세스하지 못하도록 해야 합니다. 액세스를 제한하려면 관리 보안이 사용 가능하도록 해야 합니다.

관리 보안 보호 대상

보안 도메인에 대한 관리 보안의 구성에는 다음 기술의 구성이 포함됩니다.

- HTTP 클라이언트 인증
- IIOP 클라이언트 인증
- 관리 콘솔 보안
- 네이밍 보안
- SSL 전송 사용
- Servlet, 엔터프라이즈 bean 및 MBean의 역할 기반 권한 확인
- ID 전파(RunAs)
- 공동 사용자 레지스트리
- 인증 메커니즘

보안 도메인의 작동을 정의하는 다른 보안 정보는 다음과 같습니다.

- 인증 프로토콜(RMI/IIOP(Remote Method Invocation over the Internet Inter-ORB Protocol) 보안)
- 기타 속성

응용프로그램 보안

응용프로그램 보안은 사용자 환경에서 응용프로그램에 대해 보안을 사용할 수 있도록 합니다. 이 유형의 보안은 응용프로그램 사용자를 인증하기 위한 요구사항과 응용프로그램 분리를 제공합니다.

WebSphere Process Server의 이전 릴리스에서는 사용자가 글로벌 보안을 사용 가능하도록 설정한 경우 관리 및 응용프로그램 보안 둘 다 사용 가능했습니다. 글로벌 보안의 개념은 이제 관리 보안 및 응용프로그램 보안으로 분할되며, 각각의 보안은 별도로 사용 가능하도록 설정할 수 있습니다.

WebSphere Process Server의 관리 보안은 기본적으로 사용 가능합니다. 응용프로그램 보안 역시 기본적으로 사용 가능합니다. 응용프로그램 보안은 관리 보안이 사용 가능한 경우에만 영향을 줍니다.

Java 2 보안

Java 2 보안은 특정 보호 대상 시스템 자원에 대한 액세스를 허용하기 전에 사용 권한을 확인하여 전체 시스템 통합 무결성을 증가시키는 정책 기반의 세밀한 액세스 제어

메커니즘을 제공합니다. Java 2 보안은 파일 I/O, 소켓 및 특성과 같은 시스템 자원에 대한 액세스를 보호합니다. J2EE(Java 2 Platform, Enterprise Edition) 보안은 Servlet, JSP(JavaServer Pages) 파일 및 EJB(Enterprise JavaBeans™) 메소드와 같은 웹 자원에 대한 액세스를 보호합니다.

WebSphere Process Server 보안에는 다음 기술이 포함됩니다.

- Java 2 Security Manager
- JAAS(Java Authentication and Authorization Service)
- Java 2 Connector 인증 데이터 항목
- J2EE 역할 기반 권한
- SSL(Secure Sockets Layer) 구성

Java 2 보안은 비교적 새 보안이므로 많은 기존 응용프로그램이나 새 응용프로그램조차도 Java 2 보안이 강화될 수 있는 아주 세밀한 액세스 제어 프로그래밍 모델에 대한 준비를 갖추지 못할 수 있습니다. 관리자는 응용프로그램이 Java 2 보안에 대해 준비되지 않은 경우에 Java 2 보안 사용 가능 설정의 가능한 결과를 이해해야 합니다. Java 2 보안을 사용하려면 응용프로그램 개발자와 관리자에 대한 일부 새 요구사항이 충족되어야 합니다.

Java 2 보안에 대한 세부사항은 관련 정보를 참조하십시오.

관련 정보







사용자 계정 저장소 구성

등록된 사용자의 사용자 이름 및 암호가 사용자 계정 레지스트리에 저장됩니다. 로컬 운영 체제(기본값), LDAP(Lightweight Directory Access Protocol), 연합 저장소 또는 사용자 정의 계정 저장소의 사용자 계정 저장소를 사용할 수 있습니다.

이 태스크 정보

사용자 계정 저장소는 인증을 수행할 때 인증 메커니즘이 참조하는 사용자 및 그룹 저장소입니다. 관리 콘솔에서 사용자 계정 저장소를 선택하십시오.

주:     Network Deployment 환경에서는 사용자 레지스트리로 LDAP을 사용해야 합니다.

프로시저

1. 관리 콘솔에서 관리, 응용프로그램 및 하부 구조 보안 패널을 탐색하십시오. 보안을 펼치고 관리, 응용프로그램 및 하부 구조 보안을 클릭하십시오.
2. 사용할 사용자 레지스트리를 선택하십시오.

다음 표에는 사용자 레지스트리를 선택 및 구성하는 데 필요한 조치 및 사용자 레지스트리의 선택사항이 설명되어 있습니다.

사용자 레지스트리	조치
연합 저장소	<p>단일 범주 아래에 있는 여러 저장소에서 프로파일을 관리하려면 이 설정을 지정하십시오. 범주는 다음에서 ID로 구성될 수 있습니다.</p> <ul style="list-style-type: none"> • 시스템에 빌드된 파일 기반 저장소 • 하나 이상의 외부 저장소 • 내장된 파일 기반 저장소와 하나 이상의 외부 저장소 <p>주: 관리자 특권을 가지고 있는 사용자만 연합 저장소 구성을 볼 수 있습니다. 자세한 정보는 연합 저장소 구성에서 범주 관리를 참조하십시오.</p>
로컬 운영 체제	<p>이는 기본 사용자 레지스트리입니다.</p> <p>『로컬 운영 체제 또는 독립형 사용자 정의 사용자 계정 저장소 구성』의 지시사항을 따르십시오.</p> <p>주: Network Deployment 환경에서 사용자 레지스트리로 로컬 운영 체제를 사용하지 마십시오.</p>
LDAP(Lightweight Directory Access Protocol)	<p>"사용자 레지스트리로 LDAP(Lightweight Directory Access Protocol) 구성"의 지시사항에 따라 사용자 레지스트리로 LDAP을 구성하십시오.</p>
사용자 정의 사용자 레지스트리	<p>『로컬 운영 체제 또는 독립형 사용자 정의 사용자 계정 저장소 구성』의 지시사항을 따라 사용자 정의 계정 저장소를 선택하고 사용자 필요에 맞게 구성하십시오.</p>
Tivoli® Access Manager	<p>주: 이 옵션은 관리 콘솔을 통해 사용할 수 없습니다. wsadmin 명령을 사용하여 구성해야 합니다.</p>

관련 개념

3 페이지의 『보안 시작』

보안은 WebSphere Process Server 설치를 계획할 때, 응용프로그램을 개발하고 전개할 때 및 사용자 프로세스 서버를 매일 실행할 때 중요한 고려사항입니다.

로컬 운영 체제 또는 독립형 사용자 정의 사용자 계정 저장소 구성

관리 콘솔을 사용하여 사용자 계정 저장소를 구성할 수 있습니다. 로컬 운영 체제(기본 값임)와 독립형 사용자 정의 사용자 계정 레지스트리 구성 단계는 비슷합니다.

이 태스크 정보

WebSphere Process Server가 자동으로 서버 사용자 ID를 생성하도록 허용할 것을 선택하거나 사용 중인 사용자 계정 저장소에서 지정할 수 있습니다. 후자를 사용하면 관리 조치의 감사 가능성이 개선됩니다.

프로시저

1. 관리 콘솔에서 사용자 레지스트리에 대한 구성 페이지를 여십시오.

보안을 펼치고 관리, 응용프로그램 및 하부 구조 보안을 클릭한 후 사용 가능한 범주 정의 메뉴에서 사용자가 사용하는 사용자 레지스트리를 선택하십시오. 구성을 클릭하십시오.

2. 옵션: 1차 관리 사용자 이름 필드에 유효한 사용자 이름을 입력하십시오.

이 값은 레지스트리에 정의된 관리 특권을 가지고 있는 사용자의 이름입니다. 이 사용자 이름은 관리 콘솔에 액세스하기 위해 사용됩니다. 이 이름은 wsadmin 명령에서도 사용됩니다.

3. 자동으로 생성된 서버 ID 또는 저장소에 저장된 서버 ID 옵션을 선택하십시오.

- 자동으로 생성된 서버 ID를 선택하면 응용프로그램 서버에서는 내부 프로세스 통신에 사용되는 서버 ID를 생성합니다.

인증 메커니즘 및 만기 페이지에서 이 서버 ID를 변경할 수 있습니다. 인증 메커니즘 및 만기 페이지에 액세스하려면 보안 → 관리, 응용프로그램 및 하부 구조 보안 → 인증 메커니즘 및 만기를 클릭하십시오. 내부 서버 ID 필드의 값을 변경하십시오.

- 저장소에 저장된 서버 ID 옵션을 선택한 경우 다음 정보를 입력하십시오.
 - 버전 6.0.x 노드의 관리 사용자 또는 서버 사용자 ID에 대해 보안을 위해 응용프로그램 서버를 실행하는 데 사용되는 사용자 ID를 지정하십시오.
 - 암호에 대해 이 사용자와 연관된 암호를 지정하십시오.

4. 옵션: 독립형 사용자 정의 레지스트리의 경우에만 다음 단계를 수행하십시오.

- a. 사용자 정의 레지스트리 클래스 이름에 있는 값이 올바른지 확인하여 필요한 경우 변경하십시오.
- b. 인증 시 대소문자 구분 안 함에서 체크를 선택하거나 제거하십시오.

이 옵션을 선택하면 권한 검사 시 대소문자를 구분하지 않습니다.

5. 적용을 클릭하십시오.
6. 관리, 응용프로그램 및 하부 구조 보안 페이지에서 현재로 설정을 클릭하십시오.
7. 확인을 클릭한 후 적용 또는 저장을 클릭하십시오.

사용자 계정 저장소로 Tivoli Access Manager를 사용하도록 WebSphere Process Server 구성

Tivoli Access Manager를 사용자 계정 저장소로 사용하려면 관리 콘솔 외부에서 wsadmin 명령을 사용하여 구성해야 합니다.

이 태스크 정보

Tivoli Access Manager는 사용자 계정 저장소로 사용할 수 있습니다. 관리 콘솔에서는 이와 같이 구성할 수 없으므로 wsadmin 명령을 사용해야 합니다. WebSphere Application Server Information Center 주제인 wsadmin 스크립트를 사용하여 설치된 응용프로그램의 보안 정책을 JACC 프로바이더에 전파를 참조하십시오.

사용자 레지스트리로 LDAP(Lightweight Directory Access Protocol) 구성

기본적으로 사용자 레지스트리는 로컬 운영 체제 레지스트리입니다. 원할 경우 사용자 레지스트리로 외부 LDAP(Lightweight Directory Access Protocol)을 사용할 수 있습니다.

시작하기 전에

이 태스크는 관리 보안이 설정되어 있다고 가정합니다.

LDAP을 사용하여 사용자 레지스트리에 액세스하려면 유효한 사용자 이름(ID) 및 암호, 레지스트리 서버의 서버 호스트 및 포트, 기본 식별 이름(DN)과 필요한 경우 바인드 DN 및 바인드 암호를 알아야 합니다.

Network Deployment 환경 환경에서는 LDAP을 사용해야 합니다.

검색 가능한 사용자 레지스트리에서 유효한 사용자를 선택할 수 있습니다. 관리 역할을 가진 모든 사용자 ID를 사용하여 로그인할 수 있습니다.

프로시저

1. 관리 콘솔을 시작하십시오.
 - 보안이 현재 사용 불가능으로 설정된 경우 사용자 ID에 대한 프롬프트가 표시됩니다. 임의의 사용자 ID로 로그인하십시오.
 - 보안이 현재 사용 가능으로 설정된 경우에는 사용자 ID와 암호 둘 다에 대한 프롬프트가 표시됩니다. 사전 정의된 관리 사용자 ID 및 암호로 로그인하십시오.
2. 보안을 펼치고 관리, 응용프로그램 및 하부 구조 보안을 클릭하십시오.
3. 관리, 응용프로그램 및 하부 구조 보안 페이지에서 다음 단계를 수행하십시오.
 - a. 관리 보안 사용이 선택되어 있는지 확인하십시오.
 - b. 사용 가능한 범주 정의 목록에서 독립형 LDAP 레지스트리를 선택하십시오.
 - c. 구성을 클릭하십시오.
4. 독립형 LDAP 레지스트리 페이지의 구성 탭에서 다음 단계를 수행하십시오.
 - a. 1차 관리 사용자 이름 필드에 유효한 사용자 이름을 입력하십시오.

이 값은 레지스트리에 정의된 관리 특권을 가지고 있는 사용자의 이름입니다. 이 사용자 이름은 관리 콘솔에 액세스하기 위해 사용됩니다. 이 이름은 wsadmin 명령에서도 사용됩니다.

고급 LDAP 설정 페이지에서 사용자 필터에 의해 정의된 대로 사용자의 완전한 식별 이름(DN) 또는 축약 이름을 입력할 수 있습니다.

b. 옵션: 자동으로 생성된 서버 ID 또는 저장소에 저장된 서버 ID 옵션을 선택하십시오.

- 자동으로 생성된 서버 ID를 선택하면 응용프로그램 서버에서는 내부 프로세스 통신에 사용되는 서버 ID를 생성합니다.

인증 메커니즘 및 만기 페이지에서 이 서버 ID를 변경할 수 있습니다. 인증 메커니즘 및 만기 페이지에 액세스하려면 보안 → 관리, 응용프로그램 및 하부 구조 보안 → 인증 메커니즘 및 만기를 클릭하십시오. 내부 서버 ID 필드의 값을 변경하십시오.

- 저장소에 저장된 서버 ID 옵션을 선택한 경우 다음 정보를 입력하십시오.
 - 버전 6.0.x 노드의 관리 사용자 또는 서버 사용자 ID에 대해 보안을 위해 응용프로그램 서버를 실행하는 데 사용되는 사용자 ID를 지정하십시오.
 - 암호에 대해 이 사용자와 연관된 암호를 지정하십시오.

이 ID가 LDAP 관리자 ID가 아니더라도 LDAP에 항목이 있어야 합니다.

c. 옵션: LDAP 서버 유형 목록에서 사용할 LDAP 서버를 선택하십시오.

LDAP 서버 유형에 따라 WebSphere Process Server가 사용하는 기본 필터가 결정됩니다. 이러한 기본 필터는 LDAP 서버 유형 필드를 사용자 정의로 변경하며 이는 사용자 정의 필터가 사용됨을 표시합니다. 이 조치는 고급 LDAP 설정 페이지에서 확인 또는 적용을 클릭한 후 발생합니다. 목록에서 사용자 정의 유형을 선택한 후 필요한 경우 다른 LDAP 서버를 사용하도록 사용자 및 그룹 필터를 수정하십시오.

IBM Tivoli Directory Server 사용자는 IBM Tivoli Directory Server를 디렉토리 유형으로 선택할 수 있습니다. 최상의 성능을 위해 IBM Tivoli Directory Server 디렉토리 유형을 사용하십시오.

d. 호스트 필드에 LDAP이 있는 컴퓨터의 완전한 이름을 입력하십시오.

IP 주소 또는 도메인 이름 시스템(DNS) 이름을 입력할 수 있습니다.

e. 옵션: 포트 필드에 LDAP 서버가 청취하는 포트 번호를 입력하십시오.

호스트 이름 및 포트 번호는 WebSphere Process Server 셸에서 이 LDAP 서버의 범주를 표시합니다. 따라서 서로 다른 셸에 있는 서버가 LTPA(Lightweight

Third Party Authentication) 토큰을 사용하여 서로 통신하는 경우 이러한 범주는 모든 셀에서 정확하게 일치해야 합니다.

기본값은 389입니다.

동일한 단일 사인은 도메인에 복수의 WebSphere Process Server가 설치되어 있거나 실행되도록 구성된 경우 또는 WebSphere Process Server가 WebSphere Process Server의 이전 버전과 상호 운영되는 경우 포트 번호가 모든 구성과 일치하는지 확인하십시오.

- f. 옵션: 기본 식별 이름(DN) 필드에 기본 식별 이름을 입력하십시오.

기본 식별 이름은 이 LDAP 디렉토리 서버에서 LDAP 검색의 시작점을 표시합니다. 예를 들어, DN이 cn=John Doe, ou=Rochester, o=IBM, c=US인 사용자의 경우 기본 DN을 다음 옵션 중 하나로 지정하십시오(점미부가 c=us라고 가정). ou=Rochester, o=IBM, c=us, o=IBM c=us 또는 c=us.

권한 부여 목적인 경우 이 필드는 대소문자를 구분합니다. 이 스펙은 토큰을 수신하는 경우(예: 다른 셀 또는 Lotus Domino® Server에서) 서버의 기본 식별 이름(DN)이 다른 셀 또는 Domino Server의 기본 DN과 정확히 일치해야 함을 의미합니다. 권한 부여 시 대소문자를 구분하지 않아도 되는 경우 권한 부여 시 대소문자 구분 안 함을 사용 가능으로 설정하십시오.

WebSphere Process Server에서 식별 이름은 LDAP(Lightweight Directory Access Protocol) 스펙에 따라 정규화됩니다. 정규화는 기본 식별 이름에서 쉼표 및 등호 앞뒤의 공백을 제거하여 수행됩니다. 비정규 기본 식별 이름의 예로는 o = ibm, c = us 또는 o=ibm, c=us가 있습니다. 정규화된 기본 식별 이름의 예로는 o=ibm,c=us가 있습니다.

이 필드는 Domino 디렉토리를 제외한 모든 LDAP 디렉토리에 필요하며 여기서 이 필드는 선택적입니다.

- g. 선택사항: 바인드 식별 이름 필드에 바인드 DN 이름을 입력하십시오.

바인드 DN은 사용자 및 그룹 정보를 가져오는 LDAP 서버에서 익명 바인드를 사용할 수 없는 경우 필요합니다.

LDAP 서버가 익명 바인드를 사용하도록 설정된 경우에는 이 필드를 공백으로 두십시오. 이름이 지정되지 않은 경우 응용프로그램 서버는 익명으로 바인드됩니다. 식별 이름의 예제는 기본 식별 이름 필드 설명을 참조하십시오.

- h. 옵션: 바인드 암호 필드에 바인드 DN에 해당하는 암호를 입력하십시오.
- i. 옵션: 검색 제한시간 값을 수정하십시오.

이 제한시간 값은 LDAP 서버가 요청을 중지하기 전에 응답을 제품 클라이언트에 전송하기 위해 대기하는 최대 시간입니다. 기본값은 120초입니다.

j. 연결 재사용이 선택되어 있는지 확인하십시오.

이 옵션은 서버가 LDAP 연결을 재사용하도록 지정합니다. 복수의 LDAP 서버에 요청을 전송하기 위해 라우터가 사용되는 드문 경우와 라우터가 유사성을 지원하지 않는 경우에만 이 옵션을 선택 해제하십시오. 기타 모든 상황에 대해서는 이 옵션을 선택된 상태로 두십시오.

k. 옵션: 권한 부여 시 대소문자 구분 안 함이 사용 가능한지 확인하십시오.

이 옵션을 사용 가능으로 설정하면 권한 검사 시 대소문자를 구분하지 않습니다.

일반적으로 권한 검사에는 LDAP 서버에서 고유하며 대소문자를 구분하는 사용자의 완전한 DN에 대한 검사가 포함됩니다. 그러나 IBM Directory Server 또는 Sun ONE(이전에는 iPlanet이었음) Directory Server LDAP 서버를 사용하는 경우에는 LDAP 서버에서 가져오는 그룹 정보의 대소문자가 일치하지 않으므로 이 옵션을 사용 가능으로 설정해야 합니다. 이러한 불일치는 권한 검사에만 영향을 미칩니다. 그렇지 않은 경우 이 필드는 선택사항이며 대소문자 구분 권한 검사가 필요한 경우 사용 가능으로 설정할 수 있습니다.

예를 들어, 인증 사용 시 인증 콘텐츠가 LDAP 서버에 있는 항목의 대소문자와 일치하지 않는 경우 이 옵션을 선택할 수 있습니다. 제품과 Lotus Domino 사이에 단일 사인온(SSO)을 사용하는 경우에도 권한 부여 시 대소문자 구분 안 함을 사용 가능으로 설정할 수 있습니다.

기본값을 사용할 수 있습니다.

1. 옵션: LDAP 서버와의 SSL(Secure Socket Layer) 통신을 사용하려면 SSL 사용 기능을 선택하십시오.

SSL 사용 가능 옵션을 선택하면 중앙에서 관리 또는 특정 SSL 별명 사용을 선택할 수 있습니다.

• 중앙에서 관리

이 옵션을 사용하면 한 위치에서 셀, 노드, 서버 또는 클러스터와 같은 특정 범위에 대한 SSL 구성을 지정할 수 있습니다. 중앙에서 관리 옵션을 사용하려면 특정 엔드포인트 세트에 대한 SSL 구성을 지정해야 합니다.

엔드포인트 보안 구성 관리 페이지에는 SSL 프로토콜을 사용하는 모든 인바운드 및 아웃바운드 엔드포인트가 표시됩니다.

엔드포인트 보안 구성 관리 페이지의 인바운드 또는 아웃바운드 섹션을 펼친 후 노드 이름을 클릭하여 해당 노드의 모든 엔드포인트에 사용되는 SSL 구성을 지정하십시오. LDAP 레지스트리의 경우 LDAP에 대한 SSL 구성을 지정하여 상속된 SSL 구성을 대체할 수 있습니다.

- 특정 SSL 별명 사용

이 옵션은 옵션 아래의 목록에서 SSL 구성 중 하나를 선택하는 데 사용됩니다.

이 구성은 LDAP에 대해 SSL이 사용 가능으로 설정된 경우에만 사용됩니다. 기본값은 **NodeDefaultSSLSettings**입니다.

- m. 확인을 클릭한 후 관리, 응용프로그램 및 하부 구조 페이지로 돌아갈 때까지 적용 또는 저장을 클릭하십시오.
- 5. 관리, 응용프로그램 및 하부 구조 보안 페이지에서 현재로 설정을 클릭하십시오.
- 6. 확인을 클릭한 후 적용 또는 저장을 클릭하십시오.

다음에 수행할 작업

갱신사항이 적용되도록 모든 서버를 저장하고 중지한 후 다시 시작하십시오.

아무 문제 없이 서버가 시작되면 올바르게 설정된 것입니다.

서버 시작 및 중지

관리 보안이 사용되는 경우 서버를 종료하려면 해당 사용자 이름과 암호를 제공해야 합니다. 서버가 인증없이 시작되지만 관리 콘솔에 액세스하는 데는 인증이 필요합니다.





시작하기 전에

관리 보안이 사용 가능해야 합니다.

프로시저

1. 서버를 시작하십시오.

다음 표에는 서버 시작 옵션이 설명되어 있습니다.

서버 시작	세부사항
첫 번째 단계 사용자 인터페이스에서	서버 시작을 클릭하십시오.
명령행에서	<p>다음을 입력하십시오.</p> <ul style="list-style-type: none"> •  Windows® 플랫폼: <code>startserver servername</code> •   Linux® 및 UNIX® 플랫폼: <code>startserver.sh servername</code> •  System i®(QShell 명령행에서): <code>startserver servernameinstall_dir/bin</code> 디렉토리의 명령 프롬프트에서 입력하십시오.

주: 서버를 시작하는 데에는 사용자 이름과 암호를 제공하지 않아도 됩니다. 하지만 관리 콘솔을 실행하거나 기타 관리 작업을 수행하고자 할 경우에는 인증이 필요합니다.

서버가 시작되거나 오류 메시지가 리턴됩니다.

2. 서버를 중지하십시오.

다음 표에는 서버 중지 옵션이 설명되어 있습니다.

서버 중지	세부사항
첫 번째 단계 사용자 인터페이스에서	서버 중지를 클릭하고 프롬프트가 표시되면 유효한 사용자 이름과 암호를 제공하십시오. 제공하는 사용자 이름에 운영자 또는 관리자 역할이 있어야 합니다.
명령행에서	<p>다음을 입력하십시오.</p> <ul style="list-style-type: none"> Windows Windows 플랫폼: <code>stopservice servername -profileName ProfileName -username username -password password</code> Linux UNIX Linux 및 UNIX 플랫폼: <code>stopservice.sh servername -profileName ProfileName -username username -password password</code> i5/OS System i(QShell 명령행에서): <code>stopservice servername -profileName ProfileName -username username -password password</code> <code>install_dir/bin</code> 디렉토리의 명령 프롬프트에서 입력하십시오. 제공되는 사용자 이름은 운영자 또는 관리자 역할의 구성원이어야 합니다.

주: 서버를 중지하는 데에는 사용자 이름과 암호를 제공해야 합니다.

제공하는 사용자 이름과 암호가 운영자 또는 관리자 역할의 구성원인 경우에는 서버가 중지됩니다.

3. 서버가 중지되었는지 확인하십시오.

다음 표에는 서버가 올바르게 중지되었는지 확인하는 옵션이 설명되어 있습니다.

서버 중지	세부사항
사용자 인터페이스에서	첫 번째 단계 출력 창에 요청 결과가 자세히 설명됩니다.
명령행에서	요청 결과가 요청이 시작된 명령창에 표시됩니다.

관리 보안 역할

몇 가지의 관리 보안 역할은 WebSphere Process Server 설치의 일부로 제공됩니다.

관리 콘솔의 파트로 7개의 역할이 제공됩니다. 이 역할은 관리 콘솔의 기능 범위에 권한을 부여합니다. 관리 보안이 사용 가능한 경우 관리 콘솔에 액세스하려면 이 7개의 역할 중 하나에 사용자가 맵핑되어야 합니다.

설치 후 서버에 로그인하는 첫 번째 사용자가 관리 콘솔에 추가됩니다.

표 2. 관리 보안 역할

관리 보안 역할	설명
모니터	모니터 역할의 구성원은 서버의 WebSphere Process Server 구성 및 현재 상태를 볼 수 있습니다.
구성자	구성자 역할의 구성원은 WebSphere Process Server 구성을 편집할 수 있습니다.
운영자	운영자 역할의 구성원은 모니터 특권을 가지며 런타임 상태를 수정(즉, 서버 시작 및 중지)할 수 있습니다.
관리자	관리자 역할은 구성자 역할과 운영자 역할이 조합된 것이며 관리자 역할에만 추가 특권이 부여됩니다. 예는 다음과 같습니다. <ul style="list-style-type: none"> 서버 사용자 ID 및 암호 수정 관리자 역할에 사용자 및 그룹 맵핑 또한 관리자는 다음과 같이 민감한 정보에 액세스하는 데 필요한 권한을 갖습니다. <ul style="list-style-type: none"> LTPA 암호 키
Adminsecuritymanager	이 역할이 부여된 사용자만 사용자를 관리 역할에 맵핑할 수 있습니다. 또한, 세밀한 관리 보안이 사용되는 경우에는 이 역할이 부여된 사용자만 권한 그룹을 관리할 수 있습니다. 자세한 정보는 관리 역할을 참조하십시오.
전개자	이 역할이 부여된 사용자만 응용프로그램에 대해 구성 조치 및 런타임 조작 둘 다를 수행할 수 있습니다.
iscadmins	이 역할은 관리 콘솔 사용자에게 대해서만 사용 가능하고 wsadmin 사용자에게 대해서는 사용할 수 없습니다. 이 역할이 부여된 사용자는 연합 저장소에서 사용자와 그룹을 관리하기 위한 관리자 특권을 가지고 있습니다. 예를 들어, iscadmins 역할의 사용자는 다음 작업을 완료할 수 있습니다. <ul style="list-style-type: none"> 연합 저장소 구성에서 사용자 작성, 갱신 또는 삭제 연합 저장소 구성에서 그룹 작성, 갱신 또는 삭제

관리 보안을 사용할 때 지정된 서버 ID는 자동으로 관리자 역할에 맵핑됩니다. WebSphere Process Server 관리 콘솔을 사용하여 언제든지 관리 역할에 사용자 또는 그룹을 추가하고 반대로 제거할 수도 있습니다. 하지만 변경사항을 적용하려면 서버를 다시 시작해야 합니다. 우수 사례는, 특정 사용자보다는 그룹을 관리 역할에 맵핑하는 것입니다. 왜냐하면 그것이 보다 유연하고 관리가 쉽기 때문입니다. 그룹을 관리 콘솔에 맵핑하면 그룹에 사용자 추가 또는 반대인 제거가 WebSphere Process Server 외부에서 이루어지며 변경사항을 적용하는 데 서버를 다시 시작할 필요가 없습니다.

실패한 이벤트 관리자는 관리자 또는 운영자 역할 권한을 부여한 사용자가 사용할 수 있습니다.

선택기는 관리자 또는 구성자 역할 권한을 부여한 사용자가 구성할 수 있습니다.

사용자 또는 그룹 맵핑 외에 특별 주제 또한 관리 역할에 맵핑될 수 있습니다. 특별 주제는 특정 클래스의 사용자를 일반화한 것입니다.

- **AllAuthenticated** 특별 주제는 관리 역할의 액세스 확인에서 적어도 요청 중인 사용자는 인증됨을 의미합니다.
- 모든 사용자 특별 주제는 보안이 사용 가능으로 설정되지 않은 것처럼 인증과 무관하게 모든 사용자가 조치를 수행할 수 있음을 의미합니다.

설치된 컴포넌트의 기본 보안

WebSphere Process Server의 여러 중요 컴포넌트에 기본 보안 정보가 있습니다. 이 정보에는 기본 사용자가 맵핑되는 별명과 이 컴포넌트를 호출하도록 사용자에게 액세스 권한을 부여해야 하는 보안 역할이 포함됩니다.

WebSphere Process Server의 Business Process Choreographer, CEI(Common Event Infrastructure) 및 서비스 컴포넌트 아키텍처 컴포넌트는 메시징 엔진 및 데이터베이스에서의 인증을 위해 사전 정의된 별명을 사용합니다. 프로파일 작성 중 이 인증 별명에는 기본 관리자 ID 및 암호의 기본값이 제공됩니다. 사용자 계정 저장소에 있는 다른 사용자에게 해당되도록 이 별명을 구성해야 합니다.

Business Process Choreographer 인증 별명

비즈니스 프로세스에는 사전 정의된 인증 별명이 있습니다. 이러한 별명은 관리 콘솔에서 수정하십시오.

호출 사용자의 ID와 관계없이 25 페이지의 표 3의 별명을 사용하여 컴포넌트를 호출합니다.

표 3. 비즈니스 프로세스와 연관된 인증 별명

별명	설명	정보
BPEAuthDataAliasJMS_node_server	메시징 엔진을 사용한 인증에 사용됩니다.	프로파일 관리 도구의 Business Process Choreographer 구성 패널에서 사용자 이름 및 암호 값을 입력하십시오.
BPEAuthDataAliasDbType_node_server	데이터베이스를 사용한 인증에 사용됩니다.	제공된 스크립트를 사용하여 데이터베이스를 구성하십시오.

표 4에는 비즈니스 프로세스에 대해 작성된 RunAs 역할이 설명되어 있습니다.

표 4. 비즈니스 프로세스와 연관된 RunAs 역할

RunAs 역할	설명	정보
JMSAPIUser	bpecontainer.ear에서 BFM JMS API MDB에서 사용합니다.	프로파일 관리 도구의 Business Process Choreographer 구성 패널에서 사용자 이름 및 암호 값을 입력하십시오.
EscalationUser	task.ear MDB에서 사용합니다.	프로파일 관리 도구의 Business Process Choreographer 구성 패널에서 사용자 이름 및 암호 값을 입력하십시오.

제공하는 사용자 이름이 RunAs 역할에 추가됩니다.

CEI(Common Event Infrastructure) 인증 별명

CEI(Common Event Infrastructure)에는 사전 정의된 인증 별명이 있습니다. 이러한 별명은 관리 콘솔에서 수정하십시오.

호출 사용자의 ID와 관계없이 표 5의 별명을 사용하여 컴포넌트를 호출합니다.

표 5. CEI(Common Event Infrastructure)와 연관된 인증 별명

별명	설명	정보
CommonEventInfrastructureJMSAuthAlias 주: 실제 별명에는 문자 공간이 포함되어 있지 않습니다.	메시징 엔진을 사용한 인증에 사용됩니다.	프로파일 관리 도구의 CEI(Common Event Infrastructure) 구성 패널에 사용자 이름 및 암호 값을 입력하십시오.
EventAuthAliasDbType	데이터베이스를 사용한 인증에 사용됩니다.	프로파일 관리 도구의 CEI(Common Event Infrastructure) 구성 패널에 사용자 이름 및 암호 값을 입력하십시오.

서비스 컴포넌트 아키텍처 인증 별명

SCA(Service Component Architecture)는 사전 정의된 인증 별명을 가지고 있습니다. 관리 콘솔을 사용하여 별명을 수정하십시오.

호출 사용자의 ID와 관계없이 표 6의 별명을 사용하여 컴포넌트를 호출합니다.

표 6. SCA 컴포넌트와 연관된 인증 별명

별명	설명	정보
SCA_Auth_Alias	메시징 엔진을 사용한 인증에 사용됩니다.	프로파일 관리 도구의 SCA 구성 패널에서 사용자 이름 및 암호 값을 입력하십시오.

비즈니스 프로세스 및 휴먼 태스크 응용프로그램에서의 액세스 제어

Business Process Choreographer는 WebSphere Process Server 설치의 일부로 설치됩니다. 설치 중에 액세스 제어에 대한 역할이 연관되어 있는 엔터프라이즈 아카이브 (EAR) 파일이 설치됩니다. 휴먼 태스크 관리자는 이러한 역할을 사용하여 프로덕션 시스템에서 사용자의 역할을 판별합니다.

EAR 파일 및 연관된 역할은 표 7에 표시되어 있습니다.

표 7. EAR 파일에 대한 역할 및 기본 사용 권한

EAR 파일	역할	기본 권한	참고
bpecontainer.ear	BPESystemAdministrator	설치 중에 입력된 그룹 이름	모든 비즈니스 프로세스 및 모든 조작에 액세스할 수 있습니다.
bpecontainer.ear	BPESystemMonitor	인증된 모든 사용자	읽기 조작에 액세스할 수 있습니다.
task.ear	TaskSystemAdministrator	설치 중에 입력된 그룹 이름	모든 휴먼 태스크에 액세스할 수 있습니다.
task.ear	TaskSystemMonitor	인증된 모든 사용자	읽기 조작에 액세스할 수 있습니다.
Bpcexplorer.ear	WebClientUser	인증된 모든 사용자	Business Process Choreographer 탐색기에 액세스할 수 있습니다.

CEI(Common Event Infrastructure) 응용프로그램에서의 액세스 제어

CEI(Common Event Infrastructure)는 WebSphere Process Server 설치의 일부로 설치됩니다. 설치 중에 액세스 제어에 대한 역할이 연관되어 있는 EventServer.ear 파일이 설치됩니다.

다음 역할이 EventServer.ear 파일과 연관되어 있습니다.

역할	기본 권한
eventAdministrator	인증된 모든 사용자
eventConsumer	인증된 모든 사용자
eventUpdater	인증된 모든 사용자
eventCreator	인증된 모든 사용자
catalogAdministrator	인증된 모든 사용자

역할	기본 권한
catalogReader	인증된 모든 사용자

전개 환경 서버에 대해 WebSphere Process Server 보안 구성

WebSphere Process Server의 전개 환경 설치 보안 구성에는 관리 보안 사용 및 사용자 계정 레지스트리 구성과 같은 타스크가 포함됩니다.

관련 개념

3 페이지의 『보안 시작』

보안은 WebSphere Process Server 설치를 계획할 때, 응용프로그램을 개발하고 전개할 때 및 사용자 프로세스 서버를 매일 실행할 때 중요한 고려사항입니다.

WebSphere Process Server의 전개 환경 보안

WebSphere Process Server 환경의 보안은 관리 콘솔에서 제어됩니다. 특권이 충분한 사용자는 관리 콘솔에서 모든 응용프로그램 보안을 작동 또는 정지시킬 수 있습니다. 따라서 보안 응용프로그램을 전개하기 전에 환경 보안이 이루어져야 합니다.

시작하기 전에

이 타스크를 시작하기 전에 WebSphere Process Server를 설치하고 설치를 검증해야 합니다.

이 태스크 정보

WebSphere Process Server 환경이 프로파일 내에 정의되어 있습니다. 보안화할 프로파일에 대해 관리 콘솔을 여십시오. 임의 사용자 ID나 사용하여 콘솔에 로그인하십시오. 프로파일의 보안이 이루어질 때까지는 모든 사용자 이름이 허용됩니다.

다음 단계에서는 보안을 사용 가능하게 하기 위해 수행하는 타스크의 길잡이를 제공합니다. 이 타스크에 대한 특정 세부사항은 다음 주제에서 제공합니다.

프로시저

1. 관리 보안이 작동되는지 확인하십시오. 10 페이지의 『보안 사용 가능』
2. 응용프로그램 보안이 작동하는지 확인하십시오. 47 페이지의 『WebSphere Process Server에서 응용프로그램 보안』
3. 관리 역할에 사용자나 그룹을 추가하십시오. 관리 사용자 역할 또는 관리 그룹 역할에 따라 개별 사용자나 사용자 그룹에 관리 권한을 부여할 수 있습니다.
4. 사용하려는 사용자 계정 저장소를 선택하십시오.

다음 표에는 사용자 레지스트리를 선택 및 구성하는 데 필요한 조치 및 사용자 레지스트리의 선택사항이 설명되어 있습니다.

사용자 레지스트리	조치
연합 저장소	<p>단일 범주 아래에 있는 여러 저장소에서 프로파일을 관리하려면 이 설정을 지정하십시오. 범주는 다음에서 ID로 구성될 수 있습니다.</p> <ul style="list-style-type: none"> • 시스템에 빌드된 파일 기반 저장소 • 하나 이상의 외부 저장소 • 내장된 파일 기반 저장소와 하나 이상의 외부 저장소 <p>주: 관리자 특권을 가지고 있는 사용자만 연합 저장소 구성을 볼 수 있습니다. 자세한 정보는 연합 저장소 구성에서 범주 관리를 참조하십시오.</p>
로컬 운영 체제	<p>기본 사용자 레지스트리. 사용자 계정 레지스트리를 구성하는 방법에 대한 세부사항은 15 페이지의 『로컬 운영 체제 또는 독립형 사용자 정의 사용자 계정 저장소 구성』을 참조하십시오.</p>
독립형 LDAP 레지스트리	<p>"사용자 레지스트리로 LDAP(Lightweight Directory Access Protocol) 구성"의 지시사항에 따라 사용자 레지스트리로 LDAP을 구성하십시오.</p>
독립형 사용자 정의 레지스트리	<p>사용자 계정 레지스트리를 구성하는 방법에 대한 세부사항은 15 페이지의 『로컬 운영 체제 또는 독립형 사용자 정의 사용자 계정 저장소 구성』을 참조하십시오.</p>

5. 선택한 레지스트리를 현재 레지스트리로 설정했는지 확인하십시오.

아직 이를 수행하지 않은 경우 관리, 응용프로그램 및 하부 구조 보안 페이지의 맨 아래에 있는 **현재로 설정**을 클릭하십시오.

6. 사용자 레지스트리를 선택한 후 변경사항을 적용했는지 확인하십시오.

아직 이를 수행하지 않은 경우 관리, 응용프로그램 및 하부 구조 보안 페이지의 맨 아래에 있는 **적용**을 클릭하십시오.

7. 비즈니스 통합 보안 패널로 이동하십시오. 보안을 펼치고 **비즈니스 통합 보안**을 클릭하십시오.

8. 표시된 인증 별명에 대해 적절한 사용자 ID를 제공하십시오. 사용자가 제공하는 신임은 사용자가 사용하는 사용자 계정 저장소에 존재해야 합니다. 인증 별명으로 작동하기에 적절한 사용자 ID를 선택하는 것은 사용자 시스템의 보안에 중요합니다.

9. 동일한 패널에서 Business Process Choreographer에 대해 보안을 구성할 수 있습니다.

비즈니스 플로우 및 휴먼 태스크 관리자에 대해 Business Process Choreographer 사용자 역할 맵핑을 설정하십시오.

- **관리자:** 비즈니스 플로우 및 휴먼 태스크 관리자 역할에 대한 사용자 이름, 그룹 이름 또는 둘 다. 이 역할로 지정된 사용자는 모든 특권을 가집니다.
- **모니터:** 비즈니스 플로우 및 휴먼 태스크 모니터 역할에 대한 사용자 이름, 그룹 이름 또는 둘 다. 이 역할에 지정된 사용자는 모든 비즈니스 프로세스 및 태스크 오브젝트의 특성을 볼 수 있습니다.

Business Process Choreographer 인증 별명은 Business Process Choreographer가 설치된 전개 대상마다 구성할 수 있습니다. 다음 인증 별명이 표시됩니다.

- **JMS API 인증:** 비동기 API 호출을 처리하기 위한 비즈니스 플로우 관리자 메시지 구동 Bean에 대한 인증
- **에스컬레이션 사용자 인증:** 비동기 API 호출을 처리하기 위한 휴먼 태스크 관리자 메시지 구동 Bean에 대한 인증

10. 변경사항을 적용하십시오.

패널의 맨 아래에서 **적용** 단추를 클릭하십시오.

11. 로컬 구성에 대한 변경사항을 저장하십시오.

메시지 분할창에서 **저장**을 클릭하십시오.

12. 보안 정보가 셀의 노드에 사용되었는지 확인하십시오.

관리 콘솔에서 시스템 관리를 펼치고 노드를 클릭하십시오. **전체 재동기화**를 클릭하십시오.

13. 필요하다면 서버를 중지한 후 다시 시작하십시오.

서버를 다시 시작해야 하는 경우 관리 콘솔에 적용 메시지가 나타납니다.

결과

다음에 관리 콘솔에 로그인할 때는 유효한 사용자 이름 및 암호를 제공해야 합니다.

다음에 수행할 작업

사용자가 작성하는 각 프로파일은 이 방법으로 보안을 설정해야 합니다. 시스템 관리자 ID는 환경을 설치 및 구성하는 동안 여러 곳에서 사용되었을 수 있습니다. 핵심 보안 기능 외의 모든 보안 기능에 대해 사용자 계정 저장소의 적절한 사용자 신임으로 이 ID를 대체하는 것이 좋습니다. 관리 콘솔에서 **비즈니스 통합 보안** 패널을 사용하여 ID 및 별명을 관리하십시오.

관련 태스크

10 페이지의 『보안 사용 가능』

WebSphere Process Server 환경 및 응용프로그램 보안 설정을 위한 첫 번째 단계는 관리 보안을 사용하도록 설정하는 것입니다.

47 페이지의 『WebSphere Process Server에서 응용프로그램 보안』

WebSphere Process Server 인스턴스로 전개하는 응용프로그램은 보안을 설정하여 런타임 시에 적용해야 합니다.

관련 정보



WebSphere Process Server에 설치 확인 도구 사용

보안 사용 가능

WebSphere Process Server 환경 및 응용프로그램 보안 설정을 위한 첫 번째 단계는 관리 보안을 사용하도록 설정하는 것입니다.

시작하기 전에

이 작업을 시작하기 전에 WebSphere Process Server를 설치하고 설치를 확인하십시오.

보안화할 프로파일에 대해 관리 콘솔을 여십시오. 임의 사용자 ID나 사용하여 콘솔에 로그인하십시오. 프로파일의 보안이 이루어질 때까지는 모든 사용자 이름이 허용됩니다.

이 태스크 정보

관리 보안, 응용프로그램 보안 및 Java 2 보안에 대한 정보는 하위 주제 아래에 표시된 정보를 참조하십시오.

프로시저

1. 관리 콘솔에서 관리 보안 패널을 여십시오.

보안을 펼치고 관리, 응용프로그램 및 하부 구조 보안을 클릭하십시오.

2. 관리 보안을 사용 가능하게 하십시오.

관리 보안 사용을 선택하십시오.

3. 응용프로그램 보안을 사용 가능하게 하십시오.

응용프로그램 보안 사용을 선택하십시오.

4. 옵션: 필요한 경우, Java 2 보안을 강화하십시오.

Java 2 보안 권한 확인을 강화하려면 **Java 2 보안을 사용하여 로컬 자원으로 응용프로그램 액세스 제한**을 선택하십시오.

Java 2 보안을 사용 가능하도록 하는 경우, 응용프로그램의 app.policy 파일 또는 was.policy 파일에서 필요한 사용 권한이 부여될 때까지 기본 정책에서 부여된 것보다 많은 Java 2 보안 사용 권한이 필요한 응용프로그램은 올바르게 실행되지 않을 수 있습니다. 모든 필수 사용 권한이 없는 응용프로그램에서 액세스 제어 예외

가 생성됩니다. Java 2 보안에 대한 자세한 정보는 WebSphere Application Server Information Center의 Java 2 보안 정책 파일 구성 주제를 참조하십시오.

주: app.policy 파일에 대한 갱신사항은 app.policy 파일이 속하는 노드의 엔터프라이즈 응용프로그램에만 적용됩니다.

- a. 옵션: 응용프로그램에 사용자 정의 사용 권한이 부여된 경우 경고를 선택하십시오. filter.policy 파일에는 응용프로그램이 J2EE 1.3 스펙에 따라 가지고 있어야 하는 사용 권한 목록이 있습니다. 응용프로그램이 이 정책 파일에 지정된 권한으로 설치되고 이 옵션이 사용 가능한 경우 경고가 발행됩니다. 기본값을 사용할 수 있습니다.
 - b. 옵션: 자원 인증 데이터로 액세스 제한을 선택하십시오. 응용프로그램 액세스를 민감한 JCA(Java Connector Architecture) 맵핑 인증 데이터로 제한해야 하는 경우 이 옵션이 사용 가능하도록 설정하십시오.
5. 변경사항을 적용하십시오.

패널의 맨 아래에서 적용 단추를 클릭하십시오.

6. 로컬 구성에 대한 변경사항을 저장하십시오.

메시지 분할창에서 저장을 클릭하십시오.

7. 필요하면 서버를 중지한 후 다시 시작하십시오.

서버를 다시 시작해야 하는 경우 관리 콘솔에 적용 메시지가 나타납니다.

다음에 수행할 작업

작성하는 프로파일마다 관리 보안을 작동시켜야 합니다.

관련 개념

3 페이지의 『보안 시작』

보안은 WebSphere Process Server 설치를 계획할 때, 응용프로그램을 개발하고 전개할 때 및 사용자 프로세스 서버를 매일 실행할 때 중요한 고려사항입니다.

관련 태스크

47 페이지의 『WebSphere Process Server에서 응용프로그램 보안』

WebSphere Process Server 인스턴스로 전개하는 응용프로그램은 보안을 설정하여 런타임 시에 적용해야 합니다.

관련 정보



Java 2 보안 정책 파일 구성

관리 보안

관리 보안은 보안이 항상 사용되는지 여부, 인증이 발생하는 레지스트리의 유형, 기타 값(기본값으로 작동하는 많은 값)을 판별합니다. 관리 보안을 올바르게 사용하지 않게 사용 가능하도록 설정하면 사용자가 관리 콘솔을 잠그거나 서버가 이상 종료될 수 있으므로 적절한 계획이 필요합니다.

관리 보안은 WebSphere Process Server에 대한 다양한 보안 설정을 활성화하는 "큰 스위치"로 생각할 수 있습니다. 이 설정의 값은 지정할 수 있지만 관리 보안이 활성화될 때까지는 적용되지 않습니다. 설정에는 사용자 인증, SSL(Secure Sockets Layer)의 사용, 사용자 계정 저장소 선택사항이 포함됩니다. 특히, 인증 및 역할 기반 권한을 포함한 응용프로그램 보안은 관리 보안이 활성화되지 않으면 시행되지 않습니다. 관리 보안은 기본적으로 사용 가능합니다.

관리 보안은 전체 보안 도메인에 적용되는 보안 구성을 표시합니다. 보안 도메인은 동일한 사용자 레지스트리 범주 이름으로 구성된 모든 서버로 구성됩니다. 어떤 경우에는, 범주가 로컬 운영 체제 레지스트리의 시스템 이름이 될 수 있습니다. 이 경우 모든 응용프로그램 서버는 동일한 물리적 시스템에 위치해야 합니다. 다른 경우에서, 범주가 독립형 LDAP(Lightweight Directory Access Protocol) 레지스트리의 시스템 이름이 될 수 있습니다.

LDAP 프로토콜을 지원하는 사용자 레지스트리에 원격으로 액세스할 수 있으므로 다중 노드 구성이 지원됩니다. 따라서, 어디에서나 인증을 사용할 수 있습니다.

보안 도메인에 대한 기본 요구사항은 보안 도메인 내의 한 서버에서 레지스트리 또는 저장소에 의해 리턴된 액세스 ID가 동일한 보안 도메인 내의 다른 서버에 있는 레지스트리 또는 저장소에서 리턴된 것과 같은 액세스 ID여야 한다는 것입니다. 액세스 ID는 사용자의 고유한 ID로 자원에 대한 액세스가 허용되는지 판별하기 위해 권한 부여 중에 사용됩니다.

관리 보안 구성은 보안 도메인 내의 모든 서버에 적용됩니다.

관리 보안 작동 이유

관리 보안을 작동하면 권한이 없는 사용자로부터 서버를 보호하는 설정이 활성화됩니다. 관리 보안은 기본적으로 프로파일 작성 중에 사용 가능합니다. 개발 시스템과 같이 보안이 필요하지 않은 환경이 있을 수 있습니다. 이와 같은 시스템에서는 관리 보안을 사용하지 않도록 선택할 수 있습니다. 그러나 대부분의 환경에서는 권한이 없는 사용자가 관리 콘솔과 비즈니스 응용프로그램에 액세스하지 못하도록 해야 합니다. 액세스를 제한하려면 관리 보안이 사용 가능하도록 해야 합니다.

관리 보안 보호 대상

보안 도메인에 대한 관리 보안의 구성에는 다음 기술의 구성이 포함됩니다.

- HTTP 클라이언트 인증
- IIOP 클라이언트 인증
- 관리 콘솔 보안
- 네이밍 보안
- SSL 전송 사용
- Servlet, 엔터프라이즈 bean 및 MBean의 역할 기반 권한 확인
- ID 전파(RunAs)
- 공동 사용자 레지스트리
- 인증 메커니즘

보안 도메인의 작동을 정의하는 다른 보안 정보는 다음과 같습니다.

- 인증 프로토콜(RMI/IIOP(Remote Method Invocation over the Internet Inter-ORB Protocol) 보안)
- 기타 속성

응용프로그램 보안

응용프로그램 보안은 사용자 환경에서 응용프로그램에 대해 보안을 사용할 수 있도록 합니다. 이 유형의 보안은 응용프로그램 사용자를 인증하기 위한 요구사항과 응용프로그램 분리를 제공합니다.

WebSphere Process Server의 이전 릴리스에서는 사용자가 글로벌 보안을 사용 가능하도록 설정한 경우 관리 및 응용프로그램 보안 둘 다 사용 가능했습니다. 글로벌 보안의 개념은 이제 관리 보안 및 응용프로그램 보안으로 분할되며, 각각의 보안은 별도로 사용 가능하도록 설정할 수 있습니다.

WebSphere Process Server의 관리 보안은 기본적으로 사용 가능합니다. 응용프로그램 보안 역시 기본적으로 사용 가능합니다. 응용프로그램 보안은 관리 보안이 사용 가능한 경우에만 영향을 줍니다.

Java 2 보안

Java 2 보안은 특정 보호 대상 시스템 자원에 대한 액세스를 허용하기 전에 사용 권한을 확인하여 전체 시스템 통합 무결성을 증가시키는 정책 기반의 세밀한 액세스 제어 메커니즘을 제공합니다. Java 2 보안은 파일 I/O, 소켓 및 특성과 같은 시스템 자원에 대한 액세스를 보호합니다. J2EE(Java 2 Platform, Enterprise Edition) 보안은 Servlet, JSP(JavaServer Pages) 파일 및 EJB(Enterprise JavaBeans) 메소드와 같은 웹 자원에 대한 액세스를 보호합니다.

WebSphere Process Server 보안에는 다음 기술이 포함됩니다.

- Java 2 Security Manager
- JAAS(Java Authentication and Authorization Service)
- Java 2 Connector 인증 데이터 항목
- J2EE 역할 기반 권한
- SSL(Secure Sockets Layer) 구성

Java 2 보안은 비교적 새 보안이므로 많은 기존 응용프로그램이나 새 응용프로그램조차도 Java 2 보안이 강화될 수 있는 아주 세밀한 액세스 제어 프로그래밍 모델에 대한 준비를 갖추지 못할 수 있습니다. 관리자는 응용프로그램이 Java 2 보안에 대해 준비되지 않은 경우에 Java 2 보안 사용 가능 설정의 가능한 결과를 이해해야 합니다. Java 2 보안을 사용하려면 응용프로그램 개발자와 관리자에 대한 일부 새 요구사항이 충족되어야 합니다.

Java 2 보안에 대한 세부사항은 관련 정보를 참조하십시오.

관련 정보



사용자 계정 저장소 구성

등록된 사용자의 사용자 이름 및 암호가 사용자 계정 레지스트리에 저장됩니다. 로컬 운영 체제(기본값), LDAP(Lightweight Directory Access Protocol), 연합 저장소 또는 사용자 정의 계정 저장소의 사용자 계정 저장소를 사용할 수 있습니다.

이 태스크 정보

사용자 계정 저장소는 인증을 수행할 때 인증 메커니즘이 참조하는 사용자 및 그룹 저장소입니다. 관리 콘솔에서 사용자 계정 저장소를 선택하십시오.

주: **Windows** **Linux** **UNIX** **i5/OS** Network Deployment 환경에서는 사용자 레지스트리로 LDAP을 사용해야 합니다.

프로시저

1. 관리 콘솔에서 관리, 응용프로그램 및 하부 구조 보안 패널을 탐색하십시오. 보안을 펼치고 관리, 응용프로그램 및 하부 구조 보안을 클릭하십시오.
2. 사용할 사용자 레지스트리를 선택하십시오.

다음 표에는 사용자 레지스트리를 선택 및 구성하는 데 필요한 조치 및 사용자 레지스트리의 선택사항이 설명되어 있습니다.

사용자 레지스트리	조치
연합 저장소	<p>단일 범주 아래에 있는 여러 저장소에서 프로파일을 관리하려면 이 설정을 지정하십시오. 범주는 다음에서 ID로 구성될 수 있습니다.</p> <ul style="list-style-type: none"> • 시스템에 빌드된 파일 기반 저장소 • 하나 이상의 외부 저장소 • 내장된 파일 기반 저장소와 하나 이상의 외부 저장소 <p>주: 관리자 특권을 가지고 있는 사용자만 연합 저장소 구성을 볼 수 있습니다. 자세한 정보는 연합 저장소 구성에서 범주 관리를 참조하십시오.</p>
로컬 운영 체제	<p>이는 기본 사용자 레지스트리입니다.</p> <p>15 페이지의 『로컬 운영 체제 또는 독립형 사용자 정의 사용자 계정 저장소 구성』의 지시사항을 따르십시오.</p> <p>주: Network Deployment 환경에서 사용자 레지스트리로 로컬 운영 체제를 사용하지 마십시오.</p>
LDAP(Lightweight Directory Access Protocol)	<p>"사용자 레지스트리로 LDAP(Lightweight Directory Access Protocol) 구성"의 지시사항에 따라 사용자 레지스트리로 LDAP을 구성하십시오.</p>
사용자 정의 사용자 레지스트리	<p>15 페이지의 『로컬 운영 체제 또는 독립형 사용자 정의 사용자 계정 저장소 구성』의 지시사항을 따라 사용자 정의 계정 저장소를 선택하고 사용자 필요에 맞게 구성하십시오.</p>
Tivoli Access Manager	<p>주: 이 옵션은 관리 콘솔을 통해 사용할 수 없습니다. wsadmin 명령을 사용하여 구성해야 합니다.</p>

관련 개념

3 페이지의 『보안 시작』

보안은 WebSphere Process Server 설치를 계획할 때, 응용프로그램을 개발하고 전개할 때 및 사용자 프로세스 서버를 매일 실행할 때 중요한 고려사항입니다.

로컬 운영 체제 또는 독립형 사용자 정의 사용자 계정 저장소 구성

관리 콘솔을 사용하여 사용자 계정 저장소를 구성할 수 있습니다. 로컬 운영 체제(기본 값임)와 독립형 사용자 정의 사용자 계정 레지스트리 구성 단계는 비슷합니다.

이 태스크 정보

WebSphere Process Server가 자동으로 서버 사용자 ID를 생성하도록 허용할 것을 선택하거나 사용 중인 사용자 계정 저장소에서 지정할 수 있습니다. 후자를 사용하면 관리 조치의 감사 가능성이 개선됩니다.

프로시저

1. 관리 콘솔에서 사용자 레지스트리에 대한 구성 페이지를 여십시오.

보안을 펼치고 관리, 응용프로그램 및 하부 구조 보안을 클릭한 후 사용 가능한 범주 정의 메뉴에서 사용자가 사용하는 사용자 레지스트리를 선택하십시오. 구성을 클릭하십시오.

2. 옵션: 1차 관리 사용자 이름 필드에 유효한 사용자 이름을 입력하십시오.

이 값은 레지스트리에 정의된 관리 특권을 가지고 있는 사용자의 이름입니다. 이 사용자 이름은 관리 콘솔에 액세스하기 위해 사용됩니다. 이 이름은 wsadmin 명령에서도 사용됩니다.

3. 자동으로 생성된 서버 ID 또는 저장소에 저장된 서버 ID 옵션을 선택하십시오.

- 자동으로 생성된 서버 ID를 선택하면 응용프로그램 서버에서는 내부 프로세스 통신에 사용되는 서버 ID를 생성합니다.

인증 메커니즘 및 만기 페이지에서 이 서버 ID를 변경할 수 있습니다. 인증 메커니즘 및 만기 페이지에 액세스하려면 보안 → 관리, 응용프로그램 및 하부 구조 보안 → 인증 메커니즘 및 만기를 클릭하십시오. 내부 서버 ID 필드의 값을 변경하십시오.

- 저장소에 저장된 서버 ID 옵션을 선택한 경우 다음 정보를 입력하십시오.
 - 버전 6.0.x 노드의 관리 사용자 또는 서버 사용자 ID에 대해 보안을 위해 응용프로그램 서버를 실행하는 데 사용되는 사용자 ID를 지정하십시오.
 - 암호에 대해 이 사용자와 연관된 암호를 지정하십시오.

4. 옵션: 독립형 사용자 정의 레지스트리의 경우에만 다음 단계를 수행하십시오.

- a. 사용자 정의 레지스트리 클래스 이름에 있는 값이 올바른지 확인하여 필요한 경우 변경하십시오.
- b. 인증 시 대소문자 구분 안 함에서 체크를 선택하거나 제거하십시오.

이 옵션을 선택하면 권한 검사 시 대소문자를 구분하지 않습니다.

5. 적용을 클릭하십시오.

6. 관리, 응용프로그램 및 하부 구조 보안 페이지에서 현재로 설정을 클릭하십시오.

7. 확인을 클릭한 후 적용 또는 저장을 클릭하십시오.

사용자 계정 저장소로 Tivoli Access Manager를 사용하도록 WebSphere Process Server 구성

Tivoli Access Manager를 사용자 계정 저장소로 사용하려면 관리 콘솔 외부에서 wsadmin 명령을 사용하여 구성해야 합니다.

이 태스크 정보

Tivoli Access Manager는 사용자 계정 저장소로 사용할 수 있습니다. 관리 콘솔에서는 이와 같이 구성할 수 없으므로 wsadmin 명령을 사용해야 합니다. WebSphere Application Server Information Center 주제인 wsadmin 스크립트를 사용하여 설치

된 응용프로그램의 보안 정책을 JACC 프로바이더에 전파를 참조하십시오.

사용자 레지스트리로 LDAP(Lightweight Directory Access Protocol) 구성

기본적으로 사용자 레지스트리는 로컬 운영 체제 레지스트리입니다. 원할 경우 사용자 레지스트리로 외부 LDAP(Lightweight Directory Access Protocol)을 사용할 수 있습니다.

시작하기 전에

이 타스크는 관리 보안이 설정되어 있다고 가정합니다.

LDAP을 사용하여 사용자 레지스트리에 액세스하려면 유효한 사용자 이름(ID) 및 암호, 레지스트리 서버의 서버 호스트 및 포트, 기본 식별 이름(DN)과 필요한 경우 바인드 DN 및 바인드 암호를 알아야 합니다.

Network Deployment 환경 환경에서는 LDAP을 사용해야 합니다.

검색 가능한 사용자 레지스트리에서 유효한 사용자를 선택할 수 있습니다. 관리 역할을 가진 모든 사용자 ID를 사용하여 로그인할 수 있습니다.

프로시저

1. 관리 콘솔을 시작하십시오.
 - 보안이 현재 사용 불가능으로 설정된 경우 사용자 ID에 대한 프롬프트가 표시됩니다. 임의의 사용자 ID로 로그인하십시오.
 - 보안이 현재 사용 가능으로 설정된 경우에는 사용자 ID와 암호 둘 다에 대한 프롬프트가 표시됩니다. 사전 정의된 관리 사용자 ID 및 암호로 로그인하십시오.
2. 보안을 펼치고 관리, 응용프로그램 및 하부 구조 보안을 클릭하십시오.
3. 관리, 응용프로그램 및 하부 구조 보안 페이지에서 다음 단계를 수행하십시오.
 - a. 관리 보안 사용이 선택되어 있는지 확인하십시오.
 - b. 사용 가능한 범주 정의 목록에서 독립형 LDAP 레지스트리를 선택하십시오.
 - c. 구성을 클릭하십시오.
4. 독립형 LDAP 레지스트리 페이지의 구성 탭에서 다음 단계를 수행하십시오.
 - a. 1차 관리 사용자 이름 필드에 유효한 사용자 이름을 입력하십시오.

이 값은 레지스트리에 정의된 관리 특권을 가지고 있는 사용자의 이름입니다. 이 사용자 이름은 관리 콘솔에 액세스하기 위해 사용됩니다. 이 이름은 wsadmin 명령에서도 사용됩니다.

고급 LDAP 설정 페이지에서 사용자 필터에 의해 정의된 대로 사용자의 완전한 식별 이름(DN) 또는 축약 이름을 입력할 수 있습니다.

b. 옵션: 자동으로 생성된 서버 ID 또는 저장소에 저장된 서버 ID 옵션을 선택하십시오.

- 자동으로 생성된 서버 ID를 선택하면 응용프로그램 서버에서는 내부 프로세스 통신에 사용되는 서버 ID를 생성합니다.

인증 메커니즘 및 만기 페이지에서 이 서버 ID를 변경할 수 있습니다. 인증 메커니즘 및 만기 페이지에 액세스하려면 보안 → 관리, 응용프로그램 및 하부 구조 보안 → 인증 메커니즘 및 만기를 클릭하십시오. 내부 서버 ID 필드의 값을 변경하십시오.

- 저장소에 저장된 서버 ID 옵션을 선택한 경우 다음 정보를 입력하십시오.
 - 버전 6.0.x 노드의 관리 사용자 또는 서버 사용자 ID에 대해 보안을 위해 응용프로그램 서버를 실행하는 데 사용되는 사용자 ID를 지정하십시오.
 - 암호에 대해 이 사용자와 연관된 암호를 지정하십시오.

이 ID가 LDAP 관리자 ID가 아니더라도 LDAP에 항목이 있어야 합니다.

c. 옵션: LDAP 서버 유형 목록에서 사용할 LDAP 서버를 선택하십시오.

LDAP 서버 유형에 따라 WebSphere Process Server가 사용하는 기본 필터가 결정됩니다. 이러한 기본 필터는 LDAP 서버 유형 필드를 사용자 정의로 변경하며 이는 사용자 정의 필터가 사용됨을 표시합니다. 이 조치는 고급 LDAP 설정 페이지에서 확인 또는 적용을 클릭한 후 발생합니다. 목록에서 사용자 정의 유형을 선택한 후 필요한 경우 다른 LDAP 서버를 사용하도록 사용자 및 그룹 필터를 수정하십시오.

IBM Tivoli Directory Server 사용자는 IBM Tivoli Directory Server를 디렉토리 유형으로 선택할 수 있습니다. 최상의 성능을 위해 IBM Tivoli Directory Server 디렉토리 유형을 사용하십시오.

d. 호스트 필드에 LDAP이 있는 컴퓨터의 완전한 이름을 입력하십시오.

IP 주소 또는 도메인 이름 시스템(DNS) 이름을 입력할 수 있습니다.

e. 옵션: 포트 필드에 LDAP 서버가 청취하는 포트 번호를 입력하십시오.

호스트 이름 및 포트 번호는 WebSphere Process Server 셀에서 이 LDAP 서버의 범주를 표시합니다. 따라서 서로 다른 셀에 있는 서버가 LTPA(Lightweight Third Party Authentication) 토큰을 사용하여 서로 통신하는 경우 이러한 범주는 모든 셀에서 정확하게 일치해야 합니다.

기본값은 389입니다.

동일한 단일 사인은 도메인에 복수의 WebSphere Process Server가 설치되어 있거나 실행되도록 구성된 경우 또는 WebSphere Process Server가 WebSphere Process Server의 이전 버전과 상호 운영되는 경우 포트 번호가 모든 구성과 일치하는지 확인하십시오.

- f. 옵션: 기본 식별 이름(DN) 필드에 기본 식별 이름을 입력하십시오.

기본 식별 이름은 이 LDAP 디렉토리 서버에서 LDAP 검색의 시작점을 표시합니다. 예를 들어, DN이 cn=John Doe, ou=Rochester, o=IBM, c=US인 사용자의 경우 기본 DN을 다음 옵션 중 하나로 지정하십시오(점미부가 c=us라고 가정). ou=Rochester, o=IBM, c=us, o=IBM c=us 또는 c=us.

권한 부여 목적인 경우 이 필드는 대소문자를 구분합니다. 이 스펙은 토큰을 수신하는 경우(예: 다른 셸 또는 Lotus Domino Server에서) 서버의 기본 식별 이름(DN)이 다른 셸 또는 Domino Server의 기본 DN과 정확히 일치해야 함을 의미합니다. 권한 부여 시 대소문자를 구분하지 않아도 되는 경우 권한 부여 시 대소문자 구분 안 함을 사용 가능으로 설정하십시오.

WebSphere Process Server에서 식별 이름은 LDAP(Lightweight Directory Access Protocol) 스펙에 따라 정규화됩니다. 정규화는 기본 식별 이름에서 쉼표 및 등호 앞뒤의 공백을 제거하여 수행됩니다. 비정규 기본 식별 이름의 예로는 o = ibm, c = us 또는 o=ibm, c=us가 있습니다. 정규화된 기본 식별 이름의 예로는 o=ibm,c=us가 있습니다.

이 필드는 Domino 디렉토리를 제외한 모든 LDAP 디렉토리에 필요하며 여기서 이 필드는 선택적입니다.

- g. 선택사항: 바인드 식별 이름 필드에 바인드 DN 이름을 입력하십시오.

바인드 DN은 사용자 및 그룹 정보를 가져오는 LDAP 서버에서 익명 바인드를 사용할 수 없는 경우 필요합니다.

LDAP 서버가 익명 바인드를 사용하도록 설정된 경우에는 이 필드를 공백으로 두십시오. 이름이 지정되지 않은 경우 응용프로그램 서버는 익명으로 바인드됩니다. 식별 이름의 예제는 기본 식별 이름 필드 설명을 참조하십시오.

- h. 옵션: 바인드 암호 필드에 바인드 DN에 해당하는 암호를 입력하십시오.
- i. 옵션: 검색 제한시간 값을 수정하십시오.

이 제한시간 값은 LDAP 서버가 요청을 중지하기 전에 응답을 제품 클라이언트에 전송하기 위해 대기하는 최대 시간입니다. 기본값은 120초입니다.

- j. 연결 재사용이 선택되어 있는지 확인하십시오.

이 옵션은 서버가 LDAP 연결을 재사용하도록 지정합니다. 복수의 LDAP 서버에 요청을 전송하기 위해 라우터가 사용되는 드문 경우와 라우터가 유사성을 지원하지 않는 경우에만 이 옵션을 선택 해제하십시오. 기타 모든 상황에 대해서는 이 옵션을 선택된 상태로 두십시오.

k. 옵션: 권한 부여 시 대소문자 구분 안 함이 사용 가능한지 확인하십시오.

이 옵션을 사용 가능으로 설정하면 권한 검사 시 대소문자를 구분하지 않습니다.

일반적으로 권한 검사에는 LDAP 서버에서 고유하며 대소문자를 구분하는 사용자의 완전한 DN에 대한 검사가 포함됩니다. 그러나 IBM Directory Server 또는 Sun ONE(이전에는 iPlanet이었음) Directory Server LDAP 서버를 사용하는 경우에는 LDAP 서버에서 가져오는 그룹 정보의 대소문자가 일치하지 않으므로 이 옵션을 사용 가능으로 설정해야 합니다. 이러한 불일치는 권한 검사에만 영향을 미칩니다. 그렇지 않은 경우 이 필드는 선택사항이며 대소문자 구분 권한 검사가 필요한 경우 사용 가능으로 설정할 수 있습니다.

예를 들어, 인증 사용 시 인증 콘텐츠가 LDAP 서버에 있는 항목의 대소문자와 일치하지 않는 경우 이 옵션을 선택할 수 있습니다. 제품과 Lotus Domino 사이에 단일 사인온(SSO)을 사용하는 경우에도 권한 부여 시 대소문자 구분 안 함을 사용 가능으로 설정할 수 있습니다.

기본값을 사용할 수 있습니다.

l. 옵션: LDAP 서버와의 SSL(Secure Socket Layer) 통신을 사용하려면 SSL 사용 기능을 선택하십시오.

SSL 사용 가능 옵션을 선택하면 중앙에서 관리 또는 특정 SSL 별명 사용을 선택할 수 있습니다.

• 중앙에서 관리

이 옵션을 사용하면 한 위치에서 셀, 노드, 서버 또는 클러스터와 같은 특정 범위에 대한 SSL 구성을 지정할 수 있습니다. 중앙에서 관리 옵션을 사용하려면 특정 엔드포인트 세트에 대한 SSL 구성을 지정해야 합니다.

엔드포인트 보안 구성 관리 페이지에는 SSL 프로토콜을 사용하는 모든 인바운드 및 아웃바운드 엔드포인트가 표시됩니다.

엔드포인트 보안 구성 관리 페이지의 인바운드 또는 아웃바운드 섹션을 펼친 후 노드 이름을 클릭하여 해당 노드의 모든 엔드포인트에 사용되는 SSL 구성을 지정하십시오. LDAP 레지스트리의 경우 LDAP에 대한 SSL 구성을 지정하여 상속된 SSL 구성을 대체할 수 있습니다.

• 특정 SSL 별명 사용

이 옵션은 옵션 아래의 목록에서 SSL 구성 중 하나를 선택하는 데 사용됩니다.

이 구성은 LDAP에 대해 SSL이 사용 가능으로 설정된 경우에만 사용됩니다. 기본값은 `NodeDefaultSSLSettings`입니다.

- m. 확인을 클릭한 후 관리, 응용프로그램 및 하부 구조 페이지로 돌아갈 때까지 적용 또는 저장을 클릭하십시오.
- 5. 관리, 응용프로그램 및 하부 구조 보안 페이지에서 현재로 설정을 클릭하십시오.
- 6. 확인을 클릭한 후 적용 또는 저장을 클릭하십시오.

다음에 수행할 작업

갱신사항이 적용되도록 모든 서버를 저장하고 중지한 후 다시 시작하십시오.

아무 문제 없이 서버가 시작되면 올바르게 설정된 것입니다.

서버 시작 및 중지

관리 보안이 사용되는 경우 서버를 종료하려면 해당 사용자 이름과 암호를 제공해야 합니다. 서버가 인증없이 시작되지만 관리 콘솔에 액세스하는 데는 인증이 필요합니다.

시작하기 전에

관리 보안이 사용 가능해야 합니다.

프로시저

1. 서버를 시작하십시오.

다음 표에는 서버 시작 옵션이 설명되어 있습니다.

서버 시작	세부사항
첫 번째 단계 사용자 인터페이스에서	서버 시작을 클릭하십시오.
명령행에서	<p>다음을 입력하십시오.</p> <ul style="list-style-type: none"> • Windows Windows 플랫폼: <code>startserver servername</code> • Linux UNIX Linux 및 UNIX 플랫폼: <code>startserver.sh servername</code> • i5/OS System i(QShell 명령행에서): <code>startserver servernameinstall_dir/bin</code> 디렉토리의 명령 프롬프트에서 입력하십시오.

주: 서버를 시작하는 데에는 사용자 이름과 암호를 제공하지 않아도 됩니다. 하지만 관리 콘솔을 실행하거나 기타 관리 작업을 수행하고자 할 경우에는 인증이 필

요합니다.

서버가 시작되거나 오류 메시지가 리턴됩니다.

2. 서버를 중지하십시오.

다음 표에는 서버 중지 옵션이 설명되어 있습니다.

서버 중지	세부사항
첫 번째 단계 사용자 인터페이스에서	서버 중지를 클릭하고 프롬프트가 표시되면 유효한 사용자 이름과 암호를 제공하십시오. 제공하는 사용자 이름에 운영자 또는 관리자 역할이 있어야 합니다.
명령행에서	<p>다음을 입력하십시오.</p> <ul style="list-style-type: none"> Windows Windows 플랫폼: <code>stopserver servername -profileName ProfileName -username username -password password</code> Linux UNIX Linux 및 UNIX 플랫폼: <code>stopserver.sh servername -profileName ProfileName -username username -password password</code> i5/OS System i(QShell 명령행에서): <code>stopserver servername -profileName ProfileName -username username -password password</code> <code>install_dir/bin</code> 디렉토리의 명령 프롬프트에서 입력하십시오. 제공되는 사용자 이름은 운영자 또는 관리자 역할의 구성원이어야 합니다.

주: 서버를 중지하는 데에는 사용자 이름과 암호를 제공해야 합니다.

제공하는 사용자 이름과 암호가 운영자 또는 관리자 역할의 구성원인 경우에는 서버가 중지됩니다.

3. 서버가 중지되었는지 확인하십시오.

다음 표에는 서버가 올바르게 중지되었는지 확인하는 옵션이 설명되어 있습니다.

서버 중지	세부사항
사용자 인터페이스에서	첫 번째 단계 출력 창에 요청 결과가 자세히 설명됩니다.
명령행에서	요청 결과가 요청이 시작된 명령창에 표시됩니다.

관리 보안 역할

몇 가지의 관리 보안 역할은 WebSphere Process Server 설치의 일부로 제공됩니다.

관리 콘솔의 파트로 7개의 역할이 제공됩니다. 이 역할은 관리 콘솔의 기능 범위에 권한을 부여합니다. 관리 보안이 사용 가능한 경우 관리 콘솔에 액세스하려면 이 7개의 역할 중 하나에 사용자가 맵핑되어야 합니다.

설치 후 서버에 로그인하는 첫 번째 사용자가 관리 콘솔에 추가됩니다.

표 8. 관리 보안 역할

관리 보안 역할	설명
모니터	모니터 역할의 구성원은 서버의 WebSphere Process Server 구성 및 현재 상태를 볼 수 있습니다.
구성자	구성자 역할의 구성원은 WebSphere Process Server 구성을 편집할 수 있습니다.
운영자	운영자 역할의 구성원은 모니터 특권을 가지며 런타임 상태를 수정(즉, 서버 시작 및 중지)할 수 있습니다.
관리자	관리자 역할은 구성자 역할과 운영자 역할이 조합된 것이며 관리자 역할에만 추가 특권이 부여됩니다. 예는 다음과 같습니다. <ul style="list-style-type: none"> 서버 사용자 ID 및 암호 수정 관리자 역할에 사용자 및 그룹 맵핑 또한 관리자는 다음과 같이 민감한 정보에 액세스하는 데 필요한 권한을 갖습니다. <ul style="list-style-type: none"> LTPA 암호 키
Adminsecuritymanager	이 역할이 부여된 사용자만 사용자를 관리 역할에 맵핑할 수 있습니다. 또한, 세밀한 관리 보안이 사용되는 경우에는 이 역할이 부여된 사용자만 권한 그룹을 관리할 수 있습니다. 자세한 정보는 관리 역할을 참조하십시오.
전개자	이 역할이 부여된 사용자만 응용프로그램에 대해 구성 조치 및 런타임 조작 둘 다를 수행할 수 있습니다.
iscadmins	이 역할은 관리 콘솔 사용자에게 대해서만 사용 가능하고 wsadmin 사용자에게 대해서는 사용할 수 없습니다. 이 역할이 부여된 사용자는 연합 저장소에서 사용자와 그룹을 관리하기 위한 관리자 특권을 가지고 있습니다. 예를 들어, iscadmins 역할의 사용자는 다음 작업을 완료할 수 있습니다. <ul style="list-style-type: none"> 연합 저장소 구성에서 사용자 작성, 갱신 또는 삭제 연합 저장소 구성에서 그룹 작성, 갱신 또는 삭제

관리 보안을 사용할 때 지정된 서버 ID는 자동으로 관리자 역할에 맵핑됩니다. WebSphere Process Server 관리 콘솔을 사용하여 언제든지 관리 역할에 사용자 또는 그룹을 추가하고 반대로 제거할 수도 있습니다. 하지만 변경사항을 적용하려면 서버를

다시 시작해야 합니다. 우수 사례는, 특정 사용자보다는 그룹을 관리 역할에 맵핑하는 것입니다. 왜냐하면 그것이 보다 유연하고 관리가 쉽기 때문입니다. 그룹을 관리 콘솔에 맵핑하면 그룹에 사용자 추가 또는 반대인 제거가 WebSphere Process Server 외부에서 이루어지며 변경사항을 적용하는 데 서버를 다시 시작할 필요가 없습니다.

실패한 이벤트 관리자는 관리자 또는 운영자 역할 권한을 부여한 사용자가 사용할 수 있습니다.

선택기는 관리자 또는 구성자 역할 권한을 부여한 사용자가 구성할 수 있습니다.

사용자 또는 그룹 맵핑 외에 특별 주제 또한 관리 역할에 맵핑될 수 있습니다. 특별 주제는 특정 클래스의 사용자를 일반화한 것입니다.

- **AllAuthenticated** 특별 주제는 관리 역할의 액세스 확인에서 적어도 요청 중인 사용자는 인증됨을 의미합니다.
- 모든 사용자 특별 주제는 보안이 사용 기능으로 설정되지 않은 것처럼 인증과 무관하게 모든 사용자가 조치를 수행할 수 있음을 의미합니다.

설치된 컴포넌트의 기본 보안

WebSphere Process Server의 여러 중요 컴포넌트에 기본 보안 정보가 있습니다. 이 정보에는 기본 사용자가 맵핑되는 별명과 이 컴포넌트를 호출하도록 사용자에게 액세스 권한을 부여해야 하는 보안 역할이 포함됩니다.

WebSphere Process Server의 Business Process Choreographer, CEI(Common Event Infrastructure) 및 서비스 컴포넌트 아키텍처 컴포넌트는 메시징 엔진 및 데이터베이스에서의 인증을 위해 사전 정의된 별명을 사용합니다. 프로파일 작성 중 이 인증 별명에는 기본 관리자 ID 및 암호의 기본값이 제공됩니다. 사용자 계정 저장소에 있는 다른 사용자에게 해당되도록 이 별명을 구성해야 합니다.

Business Process Choreographer 인증 별명

비즈니스 프로세스에는 사전 정의된 인증 별명이 있습니다. 이러한 별명은 관리 콘솔에서 수정하십시오.

호출 사용자의 ID와 관계없이 25 페이지의 표 3의 별명을 사용하여 컴포넌트를 호출합니다.

표 9. 비즈니스 프로세스와 연관된 인증 별명

별명	설명	정보
BPEAuthDataAliasJMS_node_server	메시징 엔진을 사용한 인증에 사용됩니다.	프로파일 관리 도구의 Business Process Choreographer 구성 패널에서 사용자 이름 및 암호 값을 입력하십시오.

표 9. 비즈니스 프로세스와 연관된 인증 별명 (계속)

별명	설명	정보
BPEAuthDataAliasDbType_node_server	데이터베이스를 사용한 인증에 사용됩니다.	제공된 스크립트를 사용하여 데이터베이스를 구성하십시오.

25 페이지의 표 4에는 비즈니스 프로세스에 대해 작성된 RunAs 역할이 설명되어 있습니다.

표 10. 비즈니스 프로세스와 연관된 RunAs 역할

RunAs 역할	설명	정보
JMSAPIUser	bpecontainer.ear에서 BFM JMS API MDB에서 사용합니다.	프로파일 관리 도구의 Business Process Choreographer 구성 패널에서 사용자 이름 및 암호 값을 입력하십시오.
EscalationUser	task.ear MDB에서 사용합니다.	프로파일 관리 도구의 Business Process Choreographer 구성 패널에서 사용자 이름 및 암호 값을 입력하십시오.

제공하는 사용자 이름이 RunAs 역할에 추가됩니다.

CEI(Common Event Infrastructure) 인증 별명

CEI(Common Event Infrastructure)에는 사전 정의된 인증 별명이 있습니다. 이러한 별명은 관리 콘솔에서 수정하십시오.

호출 사용자의 ID와 관계없이 25 페이지의 표 5의 별명을 사용하여 컴포넌트를 호출합니다.

표 11. CEI(Common Event Infrastructure)와 연관된 인증 별명

별명	설명	정보
CommonEventInfrastructureJMSAuthAlias 주: 실제 별명에는 문자 공간이 포함되어 있지 않습니다.	메시징 엔진을 사용한 인증에 사용됩니다.	프로파일 관리 도구의 CEI(Common Event Infrastructure) 구성 패널에 사용자 이름 및 암호 값을 입력하십시오.
EventAuthAliasDbType	데이터베이스를 사용한 인증에 사용됩니다.	프로파일 관리 도구의 CEI(Common Event Infrastructure) 구성 패널에 사용자 이름 및 암호 값을 입력하십시오.

서비스 컴포넌트 아키텍처 인증 별명

SCA(Service Component Architecture)는 사전 정의된 인증 별명을 가지고 있습니다. 관리 콘솔을 사용하여 별명을 수정하십시오.

호출 사용자의 ID와 관계없이 26 페이지의 표 6의 별명을 사용하여 컴포넌트를 호출합니다.

표 12. SCA 컴포넌트와 연관된 인증 별명

별명	설명	정보
SCA_Auth_Alias	메시징 엔진을 사용한 인증에 사용됩니다.	프로파일 관리 도구의 SCA 구성 패널에서 사용자 이름 및 암호 값을 입력하십시오.

비즈니스 프로세스 및 휴먼 태스크 응용프로그램에서의 액세스 제어

Business Process Choreographer는 WebSphere Process Server 설치의 일부로 설치됩니다. 설치 중에 액세스 제어에 대한 역할이 연관되어 있는 엔터프라이즈 아카이브 (EAR) 파일이 설치됩니다. 휴먼 태스크 관리자는 이러한 역할을 사용하여 프로덕션 시스템에서 사용자의 역량을 판별합니다.

EAR 파일 및 연관된 역할은 26 페이지의 표 7에 표시되어 있습니다.

표 13. EAR 파일에 대한 역할 및 기본 사용 권한

EAR 파일	역할	기본 권한	참고
bpecontainer.ear	BPESystemAdministrator	설치 중에 입력된 그룹 이름	모든 비즈니스 프로세스 및 모든 조작에 액세스할 수 있습니다.
bpecontainer.ear	BPESystemMonitor	인증된 모든 사용자	읽기 조작에 액세스할 수 있습니다.
task.ear	TaskSystemAdministrator	설치 중에 입력된 그룹 이름	모든 휴먼 태스크에 액세스할 수 있습니다.
task.ear	TaskSystemMonitor	인증된 모든 사용자	읽기 조작에 액세스할 수 있습니다.
Bpcexplorer.ear	WebClientUser	인증된 모든 사용자	Business Process Choreographer 탐색기에 액세스할 수 있습니다.

CEI(Common Event Infrastructure) 응용프로그램에서의 액세스 제어

CEI(Common Event Infrastructure)는 WebSphere Process Server 설치의 일부로 설치됩니다. 설치 중에 액세스 제어에 대한 역할이 연관되어 있는 EventServer.ear 파일이 설치됩니다.

다음 역할이 EventServer.ear 파일과 연관되어 있습니다.

역할	기본 권한
eventAdministrator	인증된 모든 사용자
eventConsumer	인증된 모든 사용자
eventUpdater	인증된 모든 사용자
eventCreator	인증된 모든 사용자

역할	기본 권한
catalogAdministrator	인증된 모든 사용자
catalogReader	인증된 모든 사용자

WebSphere Process Server에서 응용프로그램 보안

WebSphere Process Server 인스턴스로 전개하는 응용프로그램은 보안을 설정하여 런타임 시에 적용해야 합니다.

이 태스크 정보

WebSphere Process Server 환경에서 호스팅하는 응용프로그램은 보안을 필요한 여러 비즈니스 중요 기능을 수행합니다. 일부 응용프로그램은 민감한 정보(예: 임금 정보 또는 신용 카드 세부사항)를 액세스, 전송 또는 변경합니다. 기타 응용프로그램은 빌딩 또는 인벤토리 관리를 수행합니다. 이 응용프로그램의 보안은 매우 중요합니다.

다음 태스크를 수행하여 응용프로그램을 보안 설정하십시오.

프로시저

1. 관리 보안이 사용 가능한지 확인하십시오.
2. 응용프로그램 보안이 사용 가능한지 확인하십시오.
 - a. 관리 콘솔에서 보안을 펼치고 관리, 응용프로그램 및 하부 구조 보안을 클릭하십시오.
 - b. 보안 응용프로그램에 액세스하려고 하는 사용자로부터 WebSphere Process Server가 인증을 요구할 수 있도록 응용프로그램 보안 사용을 선택하십시오.
3. 해당되는 모든 보안 기능을 사용하여 WebSphere Integration Developer에서 응용프로그램을 전개하십시오.
4. WebSphere Process Server 환경에 응용프로그램을 전개하여 사용자 또는 그룹을 해당 보안 역할에 지정하십시오.
5. WebSphere Process Server 환경의 보안을 유지보수하십시오.

관련 태스크

10 페이지의 『보안 사용 가능』

WebSphere Process Server 환경 및 응용프로그램 보안 설정을 위한 첫 번째 단계는 관리 보안을 사용하도록 설정하는 것입니다.

응용프로그램 보안 요소

WebSphere Process Server에서 실행되는 응용프로그램은 인증 및 액세스 제어에 의해 보안이 이루어집니다. 또한 응용프로그램 호출 중에 전송되는 데이터가 다양한 메커니즘에 의해 보안이 유지되며 이 메커니즘으로 인해 중간에 데이터를 읽거나 변경할 수

없게 됩니다. 최종 보안 요소는 사용자가 사용자 이름 및 암호를 반복 입력할 필요가 없도록 다양한 시스템을 통해 보안 정보를 전파하는 것입니다.

WebSphere Process Server의 보안은 세 개의 일반 그룹으로 나눌 수 있습니다.

- 응용프로그램 보안
- 데이터 무결성 및 프라이버시
- ID 사용

응용프로그램 보안

WebSphere Process Server 응용프로그램의 보안은 두 가지 방법으로 유지됩니다.

- 인증

응용프로그램을 사용하려는 사용자는 사용자 레지스트리에서 사용자 이름 및 암호를 제공해야 합니다.

- 액세스 제어

사용자는 응용프로그램 호출 권한을 갖고 있어야 합니다. 역할은 응용프로그램의 호출과 연관됩니다. 인증된 사용자가 해당 역할의 일부가 아닌 경우 응용프로그램이 실행되지 않습니다.

데이터 무결성 및 프라이버시

응용프로그램에서 액세스하는 데이터는 기점, 대상 및 중간에 보안이 이루어집니다.

- 무결성

네트워크상에서 전송된 데이터는 중간에 변경할 수 없습니다.

- 프라이버시/기밀성

네트워크 상에서 전송된 데이터는 중간에 수집하여 읽을 수 없습니다.

ID 사용

최종 보안 요소는 ID 전파 중 하나이며 단일 사인온을 통해 얻을 수 있습니다.

클라이언트 요청을 엔터프라이즈 내의 여러 시스템을 통해 전달해야 하는 경우 클라이언트가 인증 데이터를 여러 번 제공하지 않아도 됩니다. 단일 사인온 메소드는 인증 정보를 다운스트림 시스템으로 전파하여 액세스 제어를 차례로 적용할 수 있도록 하는 데 사용됩니다.

사용자 인증

관리 보안이 작동되면 클라이언트를 인증해야 합니다.

클라이언트가 인증을 받지 않고 보안 응용프로그램에 액세스하려고 하면 예외가 생성됩니다.

표 14에는 WebSphere Process Server 컴포넌트를 호출하는 전형적인 클라이언트와 각 유형의 클라이언트에 사용 가능한 인증 옵션이 표시되어 있습니다.

표 14. 다양한 클라이언트용 인증 옵션

클라이언트	인증 옵션	참고
웹 서비스 클라이언트	WS-Security/SOAP 인증	
웹 또는 HTTP 클라이언트	HTTP 기본 인증(브라우저에서 클라이언트에 사용자 이름 및 암호를 묻는 프롬프트가 표시됨)	이 클라이언트는 JSP, Servlet 및 HTML 문서를 참조합니다.
Java 클라이언트	JAAS	
모든 클라이언트	SSL 클라이언트 인증	

WebSphere Process Server 하부 구조의 일부 컴포넌트에는 데이터베이스 및 메시징 엔진에 액세스하기 위해 런타임 코드를 인증하는 데 사용되는 인증 별명이 있습니다. 이러한 Business Process Choreographer 및 CEI(Common Event Infrastructure) 인증 별명은 계속되는 주제에 요약되어 있습니다. WebSphere Process Server 설치 프로그램은 이러한 별명을 작성하기 위해 사용자 이름 및 암호를 수집합니다.

일부 런타임 컴포넌트에는 runAs 역할을 사용하여 구성된 메시지 구동 Bean(MDB)이 있습니다. WebSphere Process Server 설치 프로그램은 runAs 역할에 맞는 사용자 이름과 암호를 수집합니다.

인증 별명 수정:

기존 인증 별명을 수정해야 할 수도 있습니다.

이 태스크 정보

관리 콘솔에서 인증 별명을 수정하십시오.

프로시저

1. 비즈니스 통합 인증 별명 패널에 액세스하십시오.

관리 콘솔에서 보안을 펼치고 비즈니스 통합 보안을 클릭하십시오.

주: 또한 인증 별명 정보가 필요한 다양한 관리 콘솔 패널에서 이 패널에 액세스할 수 있습니다.

인증 별명 구성 패널이 표시됩니다.

이 패널에는 인증 별명 목록, 연관된 컴포넌트, 이 별명과 연관된 사용자 ID 및 선택적으로 별명에 대한 설명이 포함되어 있습니다.

2. 별명 열에서 해당 이름을 클릭하여 수정하려는 인증 별명을 선택하십시오.

주: 경우에 따라서는 별명 옆에 링크가 제공되지 않을 수도 있습니다. 이러한 경우 편집하려는 별명에 해당되는 선택 옆에서 선택란을 선택란을 선택한 후 편집을 클릭합니다.

3. 별명의 등록 정보를 변경하십시오.

선택한 별명의 인증 별명 구성 패널에서 별명 이름이나 연관된 사용자 ID 및 암호를 수정할 수 있습니다. 인증 데이터 항목의 설명을 수정할 수도 있습니다.

4. 변경사항을 확인하십시오.

확인 또는 적용을 클릭하십시오. 비즈니스 통합 인증 별명 패널로 돌아가서 적용을 클릭하여 마스터 구성에 변경사항을 적용하십시오.

주: Network Deployment 설치의 경우 파일 동기화 조작을 수행하여 변경사항을 다른 노드로 전파해야 합니다.

관련 정보는 보안을 사용한 *WebSphere Process Server* 프로파일 기능 보장을 참조하십시오.

관련 태스크

6 페이지의 『보안을 사용한 *WebSphere Process Server* 프로파일 작성』

WebSphere Process Server 프로파일을 작성할 때 보안 신임으로 기본적으로 사용됩니다. 프로파일을 작성한 후에 관리 콘솔에서 이 보안 설정을 구성해야 합니다.

액세스 제어

액세스 제어는 인증된 사용자가 자원에 액세스하거나 특정 조작을 수행하는 데 필요한 권한을 가지고 있는지 확인하는 것입니다.

일반 사용자가 *WebSphere Process Server*에 대해 인증된 경우 해당 사용자에게 일부 조작을 허용하지 않는 것이 보안상 중요합니다. 다른 사용자에게는 일부 특정 태스크를 거부하면서 일부 사용자에게는 이러한 태스크를 수행하도록 허용하는 것을 액세스 제어라고 합니다.

액세스 제어는 개발하는 컴포넌트에 맞게 배열하여 보안을 설정할 수 있습니다. 개발 시 서비스 컴포넌트 아키텍처 규정자를 사용하여 이를 수행합니다. 자세한 정보는 *WebSphere Integration Developer Information Center*를 참조하십시오.

엔터프라이즈 아카이브(EAR) 파일로 패키징된 일부 *WebSphere Process Server* 컴포넌트는 J2EE 역할 기반 보안을 사용하여 조작을 보안합니다. 이러한 컴포넌트의 세부 사항이 제공됩니다.

컴포넌트의 조작에 대해 보안을 설정하는 J2EE 역할 기반 보안과는 대조적으로 역할 기반 액세스 제어에서는 자원에 대해 보안을 설정합니다. 예를 들어, 비즈니스 달력 관리자 내에서는 사용자가 개별 시간표에 대해 가지는 액세스의 유형을 지정할 수 있습

니다. Business Space의 Security Manager를 사용하여 각 시간표에 대해 시간표의 소유자와 시간표에 대한 작성자 및 독자 액세스 권한을 가지는 사용자를 지정합니다.

Business Process Choreographer 및 CEI(Common Event Infrastructure)는 WebSphere Process Server의 일부로 설치됩니다. 이러한 컴포넌트와 연관된 역할 기반 보안은 계속되는 주제에서 자세하게 설명합니다.

이러한 컴포넌트의 세부사항이 아래에 제공됩니다.

표 15. .ear 파일 및 연관된 J2EE 역할

EAR 파일	J2EE 역할	사용자 지정
BPCExplorer_<node>_<server>	CleanupUser	모두 인증됨
BPCObserver_<node>_<server>	ObserverUser	모두 인증됨
BPEContainer_<node>_<server>	BPEAPIUser	모두 인증됨
	BPESystemAdministrator	wsadmin
	BPESystemMonitor	wsadmin
	CleanupUser	모두 인증됨
	JMSAPIUser	모두 인증됨
REST 서비스 게이트웨이	RestServicesUser	모두 인증됨
TaskContainer_<node>_<server>	TaskAPIUser	모두 인증됨
	TaskSystemAdministrator	wsadmin
	TaskSystemMonitor	wsadmin
	EscalationUser	모두 인증됨
	CleanupUser	모두 인증됨
wpsFEMgr_6.2.0	WBIOperator	모두
EventService(*)	eventAdministrator	모두 인증됨
	eventConsumer	모두 인증됨
	eventUpdater	모두 인증됨
	eventCreator	모두 인증됨
	catalogAdministrator	모두 인증됨
	catalogReader	모두 인증됨

(*) EventService는 시스템 응용프로그램이며 관리 콘솔의 엔터프라이즈 응용프로그램 아래에 표시되지 않습니다.

관련 태스크

56 페이지의 『비즈니스 달력 관리자 보안』

보안 관리자는 비즈니스 달력 관리자의 개별 시간표에 액세스 보안을 설정할 수 있는 기능을 제공합니다. 보안 관리자를 사용하여 조직 구성원에게 역할을 지정합니다. 이러한 역할로 시간표에 대한 액세스 레벨을 판별합니다.

관련 정보

 WebSphere Integration Developer Information Center

데이터 무결성 및 프라이버시

WebSphere Process Server 프로세스의 호출 시에 액세스되는 데이터의 프라이버시 및 무결성은 보안에 중요합니다.

데이터 프라이버시 및 데이터 무결성은 밀접한 관련 개념입니다. 자세한 의미에 대해서는 관련 정보를 참조하십시오.

프라이버시

프라이버시는 권한이 없는 사용자가 데이터를 수집하여 읽을 수 없어야 함을 의미합니다.

무결성

무결성은 권한이 없는 사용자가 데이터를 변경할 수 없어야 함을 의미합니다.

WebSphere Process Server에서 제공되는 솔루션

WebSphere Process Server는 데이터 프라이버시 및 무결성에 대해 널리 사용되는 두 개의 솔루션을 지원합니다.

- SSL(Secure Sockets Layer) 프로토콜. SSL은 핸드셰이크를 사용하여 엔드포인트를 인증하고 암호화 및 해독을 위해 엔드포인트에 사용되는 세션 키를 작성하는 데 사용되는 정보를 교환합니다. SSL은 동기 프로토콜이며 지점간 통신에 적합합니다. SSL의 경우 SSL 지속 기간 동안 두 개의 엔드포인트가 서로 계속 연결되어야 합니다.
- WS-Security. 이 표준은 보안 SOAP 메시지의 SOAP(Simple Object Access Control) 확장자를 정의합니다. WS-Security는 단일 SOAP 메시지의 인증, 무결성 및 프라이버시 지원을 추가합니다. SSL과 달리 세션 키를 설정하기 위한 핸드셰이크가 없습니다. 이에 따라 JMS(Java Message Service) 상의 SOAP 또는 SIB(Service Integration Bus) 상의 SOAP와 같이 비동기 환경의 메시지 보안에 WS-Security가 적합하게 됩니다. WS-Security 전개 설명자는 전개 이전에 응용프로그램에 설정할 수 있습니다. 자세한 정보는 관련 정보를 참조하십시오.

여러 시스템이 상호작용하는 비즈니스 통합 환경에서는 일부 통신이 비동기 방식으로 이루어집니다. 따라서 대부분의 경우에 WS-Security가 탁월한 솔루션이 됩니다.

관련 정보

 보안 계획 개요

 모듈 전개 특성 편집

SSL을 사용하도록 웹 서비스 웹 클라이언트 구성:

SSL(Secure Sockets Layer)을 사용하여 웹 서비스를 호출하도록 웹 서비스 클라이언트를 구성할 수 있습니다.

이 태스크 정보

SSL을 사용하도록 웹 서비스 웹 클라이언트를 구성하는 방법에 대한 세부사항은 이 WebSphere Application Server 기술 노트에 제공되어 있습니다. 웹 서비스 보안에 대한 일반적인 설명은 WebSphere Application Server 주제 전송 레벨에서 웹 서비스 응용프로그램 보안에 있습니다.

단일 사인은

사용자 이름 및 암호 정보를 한 번만 제공하라는 질문이 클라이언트에 표시됩니다. 제공된 ID는 시스템 전반에 걸쳐 사용됩니다.

클라이언트 요청을 엔터프라이즈 내의 여러 시스템을 통해 전달하는 경우 클라이언트가 한 번만 인증하면 됩니다. 이 ID 사용 개념은 단일 사인온 메소드를 사용하여 해결됩니다.

인증된 컨텍스트가 다운스트림 시스템에 사용되어 액세스 제어를 적용할 수 있습니다.

웹 서버용 Tivoli Access Manager WebSEAL 또는 Tivoli Access Manager 플러그인을 역방향 프록시 서버로 사용하여 액세스 관리 및 단일 사인온 기능을 WebSphere Process Server 자원에 제공할 수 있습니다. 이 도구의 구성 방법과 관련한 세부사항은 WebSphere Application Server 문서에서 찾을 수 있습니다.

관련 정보



Tivoli Access Manager 또는 WebSEAL에서 단일 사인온 기능 구성

보안 응용프로그램 전개(설치)

보안 제한(보안 응용프로그램)이 있는 응용프로그램의 전개는 보안 제한이 없는 응용프로그램의 전개와 유사합니다. 활성 사용자 레지스트리가 올바른 보안 응용프로그램의 역할로 사용자 및 그룹을 지정해야 하는 것만 다릅니다. 보안 응용프로그램을 설치하는 경우 역할이 응용프로그램에 정의되어 있을 수 있습니다. 응용프로그램에서 위임이 필요했다면 RunAs 역할 또한 정의되며 유효한 사용자 이름 및 암호를 제공해야 합니다.

시작하기 전에

이 태스크를 수행하기 전에 관련된 모든 보안 구성으로 응용프로그램을 설계, 개발 및 어셈블했는지 확인하십시오. 이러한 태스크에 대한 자세한 정보는 WebSphere Integration Developer Information Center를 참조하십시오. 이 컨텍스트에서 응용프로그램의 전개와 설치의 동일한 태스크로 간주합니다.

이 태스크 정보

보안 응용프로그램 전개의 필수 단계 중 하나로 응용프로그램 구성 시에 정의된 역할로 사용자 및 그룹을 지정합니다. 이 태스크는 "사용자 및 그룹에 보안 역할 맵핑"이란

제목의 단계 중 일부로 완료됩니다. 어셈블리 도구를 사용한 경우 이 지정이 사전에 완료되었을 수도 있습니다. 이 경우 이 단계를 완료하여 맵핑을 확인할 수 있습니다. 이 단계 동안 새 사용자 및 그룹을 추가하고 기존 정보를 수정할 수 있습니다.

응용프로그램에서 RunAs 역할이 정의된 경우 전개 동안 응용프로그램이 ID 설정을 사용하여 메소드를 호출합니다. RunAs 역할을 사용하여 다운스트림 호출이 이루어지는 ID를 지정하십시오. 예를 들어, RunAs 역할이 지정된 사용자가 『bob』일 때 클라이언트(『alice』)가 위임이 설정된 상태에서 엔터프라이즈 Bean을 호출하는 Servlet을 호출할 경우 엔터프라이즈 Bean의 메소드가 『bob』이라는 ID로 호출됩니다.

전개 프로세스의 일부인 하나의 단계에서는 사용자를 RunAs 역할에 지정하거나 수정합니다. 이 단계의 제목은 "사용자를 RunAs 역할에 맵핑"입니다. 이 단계를 사용하여 위임 정책이 SpecifiedIdentity에 설정될 때 새 사용자를 RunAs 역할로 지정하거나 기존 사용자를 이 역할로 수정하십시오.

아래 설명된 단계는 응용프로그램 설치 및 기존 응용프로그램 수정에 공통입니다. 응용프로그램에 역할이 들어 있는 경우 응용프로그램 설치 중 및 관리 중에도 사용자 및 그룹에 보안 역할 맵핑 링크가 추가 특성 섹션에 하나의 링크로 표시됩니다.

프로시저

1. 관리 콘솔에서 응용프로그램을 펼치고 새 응용프로그램 설치를 클릭하십시오.

"사용자 및 그룹에 보안 역할 맵핑"이란 제목의 단계에 앞서 응용프로그램 설치에 필요한 단계를 완료하십시오.

2. 사용자 및 그룹을 역할에 지정하십시오.
3. RunAs 역할이 응용프로그램에 있는 경우 사용자를 RunAs 역할에 맵핑하십시오.
4. 필요한 경우 시스템 ID의 올바른 사용을 클릭하여 RunAs 역할을 지정하십시오.

Enterprise Bean에만 적용 가능한 시스템 ID를 사용하도록 응용프로그램에서 위임이 설정된 경우에는 이 조치를 완료하십시오. 시스템 ID가 WebSphere Process Server 보안 서버 ID를 사용하여 다운스트림 메소드를 호출합니다. WebSphere Process Server 내부 메소드에 액세스하는 경우 이 ID는 다른 ID에 비해 많은 특권을 가지므로 이 ID는 주의하여 사용하십시오. 패널에 표시된 메소드의 시스템 ID가 위임을 위해 설정되었음을 전개자가 인식하고 필요한 경우 이를 정정할 수 있도록 이 타스크가 제공됩니다. 변경사항이 불필요하면 이 타스크를 건너뛰십시오.

5. 남은 비보안 관련 단계를 완료하여 응용프로그램 설치 및 전개를 마치십시오.

다음에 수행할 작업


보안 응용프로그램이 전개되면 올바른 신임으로 응용프로그램의 자원에 액세스할 수 있는지 확인하십시오. 예를 들어, 응용프로그램에 보호 설정된 웹 모듈이 있는 경우 역할에 지정된 사용자만이 응용프로그램을 사용하도록 하십시오.


관련 개념

3 페이지의 『보안 시작』

보안은 WebSphere Process Server 설치를 계획할 때, 응용프로그램을 개발하고 전개할 때 및 사용자 프로세스 서버를 매일 실행할 때 중요한 고려사항입니다.

관련 정보

 역할에 사용자 및 그룹 지정

 RunAs 역할에 사용자 지정

역할에 사용자 지정

보안 응용프로그램은 securityPermission 및 securityIdentity인 두 개 규정자 중 하나 또는 둘 모두를 사용합니다. 이 규정자가 있으면 응용프로그램 및 보안 기능이 올바르게 작동하기 위해 전개 시에 추가 단계를 수행해야 합니다.

시작하기 전에

이 태스크에서는 EAR 파일로써 보안 응용프로그램을 WebSphere Process Server로 전개할 준비가 된 것으로 가정합니다.

이 태스크 정보

응용프로그램은 메소드가 있는 인터페이스를 구현합니다. SCA(Service Component Architecture) 규정자 securityPermission을 사용하여 인터페이스 또는 메소드에 보안을 설정할 수 있습니다. 이 규정자를 호출할 경우 보안 메소드의 호출 권한이 있는 역할(예: 『감독자』)을 지정합니다. 응용프로그램을 전개할 경우 사용자를 지정된 역할에 지정할 수 있습니다.

securityIdentity 규정자는 WebSphere Application Server에서 위임에 사용하는 RunAs 역할과 동등합니다. 이 규정자와 연관된 값이 역할입니다. 전개 수행 중에 역할이 ID에 매핑됩니다. securityIdentity로 보안 설정된 컴포넌트의 호출에서는 응용프로그램을 호출하는 사용자의 ID와 무관하게 지정된 ID를 사용합니다.

프로시저

1. 응용프로그램을 WebSphere Process Server로 전개하는 지침을 따르십시오. 자세한 내용은 프로덕션 서버에 모듈 설치를 참조하십시오.

2. 올바른 사용자를 역할과 연관시키십시오.

보안 규정자	수행 조치
보안 권한	<p>사용자를 지정된 역할에 지정하십시오. 다음과 같은 네 가지 선택사항이 있습니다.</p> <ul style="list-style-type: none"> • 모든 사용자 - 보안이 없는 것과 같습니다. • 모두 인증 - 인증된 모든 사용자가 역할의 구성원입니다. • 맵핑된 사용자 - 개별 사용자가 역할에 추가됩니다. • 맵핑된 그룹 - 사용자 그룹이 역할에 추가됩니다. <p>사용자가 그룹에 추가되어 서버 다시 시작 없이도 응용프로그램에 액세스할 수 있기 때문에 가장 유연한 선택은 맵핑된 그룹입니다.</p>
보안 ID	<p>역할이 맵핑되는 ID에 유효한 사용자 이름 및 암호를 제공하십시오.</p>

관련 개념

3 페이지의 『보안 시작』

보안은 WebSphere Process Server 설치를 계획할 때, 응용프로그램을 개발하고 전개할 때 및 사용자 프로세스 서버를 매일 실행할 때 중요한 고려사항입니다.

관련 정보



위임

비즈니스 달력 관리자 보안

보안 관리자는 비즈니스 달력 관리자의 개별 시간표에 액세스 보안을 설정할 수 있는 기능을 제공합니다. 보안 관리자를 사용하여 조직 구성원에게 역할을 지정합니다. 이러한 역할로 시간표에 대한 액세스 레벨을 판별합니다.

비즈니스 달력 관리자 내의 각 시간표에 대해 구성원을 세 가지 역할(소유자, 작성자 또는 독자) 중 하나에 지정할 수 있습니다.

비즈니스 달력 관리자의 역할 기반 액세스 제어를 관리하는 데 사용하는 보안 관리자는 WebSphere에서 제공하는 Business Space에 있습니다.

비즈니스 달력 관리자에 대한 이 역할 기반 액세스는 개방형 표준인 XACML(eXtensible Access Control Markup Language)을 기반으로 합니다.

보안 관리자 사용의 이점

비즈니스 달력 관리자에서 역할 기반 액세스 제어용 보안 관리자 사용 시 장점은 다음과 같습니다.

- 시간표의 특정 인스턴스에 대한 액세스를 제어할 수 있습니다.

예를 들어, 사용자가 사용자 소유 시간표에만 액세스할 수 있도록 지정하고 사용자가 다른 사용자의 시간표를 보거나 변경할 수 없도록 지정할 수 있습니다.

- 개별 사용자 레벨 대신 역할 레벨에서 액세스 제어가 수행됩니다.

구성원을 역할에 매핑합니다. 역할은 자원의 특정 인스턴스에 대해 구성원이 가지는 권한을 정의합니다.

시간표와 연관된 역할

시간표가 설치되면 해당 시간표에 대해 세 가지 역할(소유자, 작성자 및 독자)이 작성됩니다.

이러한 역할의 사용 방법 조직에서 사용되는 휴일 시간표의 경우를 고려해보십시오. 모든 직원이 시간표에 액세스할 수 있게 하려고 하지만 시간표를 실제로 갱신할 수 있는 직원 수는 제한하려고 합니다.

휴일 시간표가 설치되면 다음과 같은 역할이 작성됩니다.

- **HolidayOwner**

이 역할에 지정된 구성원은 휴일 시간표를 읽을 수 있고 휴일 시간표에 쓸 수도 있습니다. 예를 들어, 회사에서 휴일을 추가하도록 결정하면 HolidayOwner 역할을 가진 구성원이 변경사항을 작성할 수 있습니다.

이 역할을 가진 구성원은 구성원을 HolidayWriter 및 HolidayReader 역할에 지정할 수도 있습니다. 예를 들어, HolidayOwner는 선임 관리자를 HolidayWriter 역할에 추가하도록 결정할 수 있습니다.

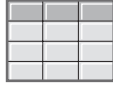
- **HolidayWriter**

이 역할에 지정된 구성원은 휴일 시간표를 읽을 수 있고 휴일 시간표에 쓸 수도 있습니다. HolidayOwner의 경우와 마찬가지로 HolidayWriter 역할을 가진 구성원은 휴일을 추가할 수 있습니다.

- **HolidayReader**

이 역할에 지정된 구성원은 휴일 시간표를 읽을 수는 있지만 휴일 시간표에 쓸 수는 없습니다.

다음 그림과 같이 HolidayOwner 역할을 인적 자원 관리자에, HolidayWriter 역할을 인적 자원 전문가 그룹에, HolidayReader 역할을 직원 그룹에 지정할 수 있습니다.



휴일 시간표



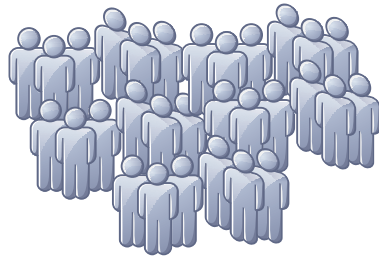
휴일을 보고 갱신할 수 있습니다.
휴일에 대한 작성자 및 독자 역할을 지정할 수 있습니다.

Holiday.Owner=인적 자원 관리자



휴일을 보고 갱신할 수 있습니다.

Holiday.Writer=인적 자원 전문가 그룹



휴일을 볼 수 있습니다.

Holiday.Reader=직원 그룹

그림 1. 시간표에 지정된 역할의 예제

시간표를 전개하면 세 가지 역할(소유자, 작성자 및 독자)이 작성됩니다. 모든 역할의 권한은 초기에는 인증된 모든 사용자로 설정됩니다. 이 대상을 변경하여 조직의 구성원을 올바른 역할에 지정하는지 확인하십시오.

주: 역할의 멤버십을 변경(예: 독자 역할에서 구성원 제거)할 수 있지만 역할 이름을 변경하거나 역할을 추가 또는 삭제하거나 역할과 연관된 권한을 변경할 수는 없습니다. 권한은 다음과 같이 설정됩니다.

- 소유자 역할을 가진 구성원은 시간표를 읽고 쓸 수 있으며 작성자 및 독자 역할에 다른 구성원을 지정할 수 있습니다.
- 작성자 역할을 가진 구성원은 시간표를 읽고 쓸 수 있습니다.
- 독자 역할을 가진 구성원은 시간표를 읽을 수 있습니다.

보안 관리자에서 이 시간표 관련 역할은 모듈 역할로도 알려져 있습니다.

보안 관리자 관리 역할

WebSphere Process Server 설치(또는 WebSphere Process Server 6.2로 업그레이드) 후 서버를 다시 시작하면 다음과 같은 역할이 작성됩니다.

- BPMAdmin

BPMAdmin은 BPMRoleManager 역할에서 구성원을 추가 또는 제거하는 권한을 가집니다.

예를 들어, BPMRoleManager 역할을 수행하는 사용자가 조직을 떠나면 BPMAdmin 만 다른 구성원을 해당 역할에 지정할 수 있습니다.

BPMAdmin은 초기에는 한 명의 구성원(1차 관리자)에게 지정됩니다. 설치 또는 업그레이드 후 서버를 다시 시작하는 즉시 이 지정을 다른 구성원으로 변경하십시오.

- BPMRoleManager

BPMRoleManager는 세 가지 시간표 관련 역할(소유자, 작성자 및 독자)에서 구성원을 추가 또는 제거하는 권한을 가집니다.

예를 들어, 휴일 시간표가 작성되면 BPMRoleManager는 구성원을 HolidayOwner, HolidayWriter 및 HolidayReader 역할에 지정합니다.

BPMRoleManager는 초기에는 한 명의 구성원(1차 관리자)에게 지정됩니다. 설치 또는 업그레이드 후 서버를 다시 시작하는 즉시 이 지정을 다른 구성원으로 변경하십시오.

주: 보안 관리자에서 이 역할은 시스템 역할로도 알려져 있습니다.

역할 설정

WebSphere Process Server가 설치되면 Security Manager에서 다음과 같은 작업을 수행해야 합니다.

1. BPMAdmin이 BPMRoleManager 역할을 재지정합니다.
2. BPMRoleManager가 시간표와 연관된 세 가지 역할 중 하나에 구성원을 지정합니다.

이러한 작업의 수행 방법에 대한 정보는 Security Manager의 도움말 항목을 참조하십시오.

관련 개념

3 페이지의 『보안 시작』

보안은 WebSphere Process Server 설치를 계획할 때, 응용프로그램을 개발하고 전개할 때 및 사용자 프로세스 서버를 매일 실행할 때 중요한 고려사항입니다.

50 페이지의 『액세스 제어』

액세스 제어는 인증된 사용자가 자원에 액세스하거나 특정 작업을 수행하는 데 필요한 권한을 가지고 있는지 확인하는 것입니다.

WebSphere에서 지원하는 Business Space

WebSphere Process Server는 응용프로그램 사용자가 IBM® WebSphere Business Process Management 포트폴리오 사이에 웹 인터페이스를 작성, 관리 및 통합하기 위한 공통 인터페이스를 제공하는 WebSphere에서 지원하는 Business Space를 포함합니다.

어댑터 보안

두 가지 유형의 어댑터 WebSphere Business Integration Adapter 및 WebSphere Adapter가 WebSphere Process Server에서 지원됩니다. 두 가지 유형의 어댑터 보안에 대해 설명합니다.

이 태스크 정보

어댑터는 응용프로그램이 엔터프라이즈 정보 시스템(EIS)과 통신하는 메커니즘입니다. 응용프로그램과 EIS 사이에 교환되는 정보는 매우 민감한 정보일 수 있습니다. 이 정보 트랜잭션의 보안을 설정하는 것이 중요합니다.

WebSphere Business Integration Adapter는 응용프로그램이 통합 브로커를 통해 비즈니스 데이터를 교환하는 소프트웨어, API(Application Program Interface) 및 도구의 콜렉션으로 구성됩니다. WebSphere Business Integration Adapter는 JMS 메시징에 의존하며 JMS는 보안 컨텍스트 전파를 지원하지 않습니다.

WebSphere Adapter는 엔터프라이즈 정보 시스템(EIS)과 WebSphere Process Server가 지원하는 J2EE 컴포넌트 사이의 관리된 양방향 연결을 가능하게 합니다.

어댑터 유형 모두에서 WebSphere Process Server에 대한 인바운드 통신의 경우 인증 메커니즘이 없습니다. WebSphere Business Integration Adapter의 경우 JMS 메시징에 대한 의존으로 인해 보안 컨텍스트 전파가 불가능합니다. J2C에도 인바운드 보안 지원이 없으므로 WebSphere Adapter에도 인바운드 통신을 위한 인증 메커니즘이 없습니다.

어댑터에서 WebSphere Process Server에 입력 시에는 항상 SCA(Service Component Architecture) 내보내기를 사용합니다. SCA 내보내기는 중개, 비즈니스 프로세스, SCA Java 컴포넌트 또는 선택기와 같은 SCA 컴포넌트에 연결해야 합니다.

보안 솔루션은 WebSphere Adapter 내보내기의 대상인 컴포넌트에서 runAs 역할을 정의하는 것입니다. 이러한 작업은 개발 중 SCA 규정자 SecurityIdentity를 사용하여 수행됩니다(자세한 정보는 WebSphere Integration Developer Information Center 참조). 컴포넌트가 실행될 때에는 runAs 역할에 정의된 ID에서 실행됩니다.

SecurityIdentity에 대한 값은 사용자가 아니라 역할입니다. 그럼에도 EAR 파일이 WebSphere Process Server로 전개되면 사용할 ID에 대한 사용자 이름 및 암호를 제

공해야 합니다. 다운스트림 컴포넌트가 보안이 이루어지고 클라이언트가 인증된 ID를 갖고 있어야 하는 경우 SecurityIdentity를 사용하면 예외가 처리되지 않습니다.

주: SecurityIdentity를 사용하는 경우에는 어댑터와 EIS 간의 통신 보안이 이루어지지 않습니다.

WebSphere Business Integration Adapter가 서비스 통합 버스 상에서 JMS 메시지로 써 데이터를 WebSphere Process Server로 전송합니다.

WebSphere Adapter가 WebSphere Process Server의 JVM에 위치하기 때문에 어댑터와 대상 EIS 간의 통신 보안만이 필요합니다. 어댑터와 EIS 간의 프로토콜은 EIS에 특정합니다. EIS 문서에서는 이 링크의 보안 방법에 대한 정보를 제공합니다.

관련 개념

 서비스 통합 버스에 대한 보안 고려사항

휴먼 태스크 및 비즈니스 프로세스 보안

휴먼 태스크 및 비즈니스 프로세스에는 여러 가지 역할이 관련되어 있습니다. 이 주제는 사용 가능한 역할에 대해 설명합니다.

휴먼 태스크는 완료하는 데 사람의 개입이 필요합니다. 일부 비즈니스 프로세스에도 사람의 개입이 필요할 수 있습니다. 이러한 휴먼 태스크 및 비즈니스 프로세스는 WebSphere Integration Developer를 사용하여 개발되며 Business Process Choreographer를 사용하여 호출됩니다. 태스크 또는 프로세스를 개발할 때 휴먼 태스크 및 비즈니스 프로세스와 관련된 사용자나 그룹에 역할을 지정해야 합니다. 역할 지정 또는 특정 역할과 연관된 역할 조회에 대한 자세한 정보는 WebSphere Integration Developer Information Center를 참조하십시오.

휴먼 태스크 관리자는 이러한 역할을 사용하여 프로덕션 시스템에서 사용자의 역량을 판별합니다.

휴먼 태스크 및 비즈니스 프로세스와 연관된 역할

중요사항: 이러한 역할은 Business Process Choreographer 비즈니스 컨테이너 및 휴먼 태스크 컨테이너에서 실행 중인 태스크 및 프로세스에만 해당됩니다.

WebSphere Process Server는 태스크 및 프로세스에 대해 다음의 역할을 지원합니다.

관리자 이 역할에 속한 사용자는 태스크 및 프로세스를 모니터, 종료 또는 삭제할 수 있으며 태스크 및 프로세스에 대한 정보를 표시할 수도 있습니다.

독자 이 역할에 속한 사용자는 태스크 및 프로세스를 표시할 수만 있습니다.

시작자 이 역할에 속한 사용자는 태스크 및 프로세스를 시작하거나 표시할 수 있습니다.


타스크에는 다음과 같은 추가 역할도 있습니다.

소유자 이 역할에 속한 사용자는 이미 청구한 타스크를 저장, 취소, 완료 또는 표시할 수 있습니다.


잠재적 소유자

이 역할에 속한 사용자는 타스크를 청구 및 표시할 수 있습니다.

관련 개념

 프로세스에 대한 권한 및 개인 지정

관련 정보

 권한 및 개인 지정

Business Space에 대한 보안 설정

제품에 대해 WebSphere에서 지원하는 Business Space를 설치 및 구성한 후 팀에서 Business Space의 아티팩트에 대해 작업할 방법의 보안 옵션을 고려해야 합니다. 응용 프로그램 보안을 설정할 수 있으며, 이 경우 응용프로그램의 관리 보안도 필요합니다. 또한 Jython 스크립트를 실행하여 Business Space에 대한 슈퍼유저 역할을 지정해야 합니다.

Business Space에 대한 응용프로그램 보안 설정

Business Space에 대한 보안을 설정하려면 응용프로그램 보안 및 관리 보안을 모두 사용 가능하게 해야 합니다.

시작하기 전에

이 타스크를 완료하기 전에 다음 타스크를 완료해야 합니다.

- 프로파일을 구성하고 해당 프로파일에 Business Space를 구성합니다.
- 데이터베이스 테이블을 구성합니다(원격 데이터베이스 또는 전개 환경을 사용 중인 경우).
- Business Space에 사용할 위지트(widget)에 대한 REST 서비스 엔드포인트를 구성합니다.
- 사용자 ID가 제품에 대한 사용자 레지스트리에 등록되어 있는지 확인합니다.

이 태스크 정보

Business Space 엔터프라이즈 아카이브(EAR) 파일은 액세스의 인증 및 권한을 확인 하도록 사전 구성됩니다. Business Space는 하나의 기본 J2EE 역할을 사용하고, 인증 된 모든 사용자에게 맵핑되며, Business Space URL에 액세스할 때 인증하도록 사용자에게 프롬프트합니다. 인증되지 않은 사용자의 경로는 로그인 페이지로 재지정됩니다.

Business Space의 영역 및 페이지 콘텐츠에 대한 권한은 Business Space의 내부에서 관리 영역의 일부로 처리됩니다.

Business Space에 대해 인증된 액세스(J2EE 역할 기반 권한)를 사용 가능하게 하려면 사용자 레지스트리가 구성되어 있어야 하고 응용프로그램 보안이 사용 가능해야 합니다.

프로시저

1. 보안에 대한 전체 지시사항은 제품의 보안 문서를 참조하십시오.
2. Business Space 응용프로그램에 대해 보안 관리, 응용프로그램 및 하부 구조 관리 콘솔에서 관리 보안 사용 가능 및 응용프로그램 보안 사용 가능을 모두 선택하십시오.
3. 동일한 관리 콘솔 페이지의 사용자 계정 저장소 아래에서 연합 저장소, 로컬 운영 체제, **LDAP(Lightweight Directory Access Protocol)** 또는 사용자 정의 사용자 레지스트리를 지정할 수 있습니다. 그러나 Business Space에 대한 연합 저장소를 선택하는 경우, 위지트(widget) 및 프레임워크에 추가 기능(예: 확장 검색 기능)이 포함됩니다. 영역 및 페이지를 공유할 사용자를 검색할 때 검색 범위에는 전자우편, 사용자의 전체 및 사용자 ID가 포함됩니다.

다음에 수행할 작업

- 관리 및 응용프로그램 보안이 설정된 후 Business Space에 로그인하면 사용자 ID 및 암호에 대한 프롬프트를 수신합니다. 로그인하기 위해서는 선택한 사용자 레지스트리에서 올바른 사용자 ID 및 암호를 사용해야 합니다. 관리 보안을 설정한 후 관리 콘솔로 리턴할 때마다 관리 권한이 있는 사용자 ID로 로그인해야 합니다.
- Business Space에 대한 로그인을 사용자 및 그룹의 서브세트로 제한하려는 경우, Business Space J2EE 역할의 맵핑을 변경할 수 있습니다. **응용프로그램** → **엔터프라이즈 응용프로그램** → **응용프로그램 이름**을 클릭하십시오. 오른쪽 패널의 "세부 특성" 아래에서 보안 역할 대 사용자/그룹 맵핑을 선택하십시오.
- Business Space의 페이지 및 영역에 대한 권한을 설정하기 위해 페이지 및 영역을 작성할 때 Business Space에서 이 권한을 관리할 수 있습니다.
- 사용자 및 그룹에 따라 위지트(widget)의 데이터에 대한 보안을 설정하려면 사용자 대 REST 서비스 게이트웨이 응용프로그램의 맵핑을 수정해야 합니다. REST 서비스 게이트웨이 응용프로그램을 선택하고 오른쪽 패널의 세부 특성 아래에서 보안 역할 대 사용자/그룹 맵핑을 선택하십시오. RestServicesUser 역할의 사용자 및 그룹을 해당 역할에 추가하여 모든 REST 서비스 위지트(widget)의 데이터에 대한 액세스를 제어할 수 있습니다.
- 사용자 그룹 역할에 따라 위지트(widget)의 데이터에 대한 액세스를 제한하려는 경우, 관리 그룹 역할에 지정된 사용자를 변경해 보십시오. 관리 콘솔을 열고 **보안** →

보안 관리, 응용프로그램 및 하부 구조 → 관리 그룹 역할을 클릭한 후 그룹을 선택 하여 이 역할에 누가 지정되어 있는지 확인하기 위해 역할 목록을 볼 수 있습니다.

비즈니스 규칙 및 비즈니스 변수와 같은 위지트(widget)의 관리 그룹 역할에 지정된 사용자 변경을 고려할 수 있습니다.

예를 들어, 성능 상태 모니터 위지트(widget)에 대해 다음 관리 역할은 모두 모니터링 권한이 있으며, 모두 관리 콘솔에 대한 액세스를 허용하므로 해당 역할에 지정된 사용자가 성능 상태 모니터의 데이터에 액세스하도록 허용합니다.

- 모니터
- 구성자
- 운영자
- 관리자
- Adminsecuritymanager
- 전개자
- iscadmins

해당 관리 그룹 역할로 맵핑되는 사용자는 성능 상태 모니터의 데이터에 액세스할 수 있습니다. 해당 역할에 맵핑되지 않은 사용자는 성능 상태 모니터의 데이터에 액세스할 수 없습니다.

- 마지막으로, 일부 위지트(widget)에는 비즈니스 사용자가 작성한 아티팩트에 대한 역할 기반 액세스의 추가 레이어가 있습니다. 솔루션 관리용 보안 관리자 위지트(widget)를 사용하면 사용자 및 그룹, 비즈니스 달력 관리자 위지트(widget)의 시간표에 대한 구성원의 액세스 레벨을 판별하는 시스템 역할 또는 모듈 역할을 지정할 수 있습니다. 검토용 공개 서버 액세스 제어 위지트(widget)는 검토하고 검토사항에 대해 설명할 수 있는 사용자의 사용 권한을 관리합니다. 자세한 정보는 위지트(widget)에 대한 온라인 도움말을 참조하십시오.

Business Space 슈퍼유저 역할 지정

Business Space에서 사용자를 슈퍼유저로 지정할 수 있습니다. 슈퍼유저는 모든 영역 및 페이지를 보고 편집하고 삭제할 수 있으며, Business Space의 영역이 템플릿이 될 수 있는지를 지정할 수 있습니다. 사용자 ID에 대해 Business Space 슈퍼유저 역할을 지정하는 스크립트를 실행하거나 wsadmin 스크립팅 클라이언트를 사용하여 Business Space 슈퍼유저를 사용 가능하게 할 스크립트를 작성할 수 있습니다.

시작하기 전에

사용자 ID가 제품에 대한 사용자 레지스트리에 등록되어 있어야 합니다.

프로시저

1. 사용자에게 슈퍼유저 역할을 지정하기 위한 스크립트 `install_root/BusinessSpace/scripts/createSuperUser.py`를 찾으십시오.
2. 명령 프롬프트를 열고 디렉토리를 `profile_root/bin` 디렉토리로 변경하십시오. 여기서 `profile_root`는 Business Space가 설치되어 있는 프로파일의 디렉토리를 나타냅니다.
3. 다음 명령을 입력하십시오. `wsadmin -lang jython -wsadmin_classpath install_root#plugins#com.ibm.bspace.plugin_6.2.0.jar -f createSuperUser.py user_short_name_in_VMM`

다음에 수행할 작업

사용자 이름이 슈퍼유저 역할을 가지고 있는지 조회하려는 경우 또는 슈퍼유저 역할을 제거하려는 경우 또 다른 두 개의 스크립트가 제공됩니다. 둘 다 `install_root/BusinessSpace/scripts/` 디렉토리에서 사용 가능합니다.

- 사용자 이름이 슈퍼유저 역할을 가지고 있는지 조회하는 `isSuperUser.py`.
- 사용자에게서 슈퍼유저 역할을 제거하는 `removeSuperUserAccess.py`.

제공된 세 개의 스크립트에 기초하여 추가 스크립트를 작성할 수 있습니다. 스크립트의 MBean 호출을 슈퍼유저 역할에 대해 작업할 다음 메소드 중 하나로 바꿀 수 있습니다.

```
public boolean assignSuperUserRole(String userId);
public boolean removeSuperUserRole(String userId);
public List getAllSuperUsers();
public boolean isSuperUser(String userId);
public boolean removeAllSuperUsers();
```

MBean 설명자 파일 `BSpaceSecurityAdminMBean.xml`을 참조하십시오(이 파일은 `install_root/BusinessSpace/scripts`에서 제공함).

Business Space를 열려면 다음 URL을 사용하십시오. `http://host:port/BusinessSpace`. 여기서 `host`는 서버가 실행되고 있는 호스트의 이름이고, `port`는 서버의 포트 번호입니다.

종단간 보안 작성

내재된 여러 종단간 보안 시나리오가 있습니다. 이들 각각에 대한 보안 단계가 서로 다를 수 있습니다. 필요한 보안 옵션이 있는 전형적인 여러 가지 시나리오가 제공됩니다.

시작하기 전에

이 시나리오에는 모두 관리 보안이 강화된 것으로 가정합니다.

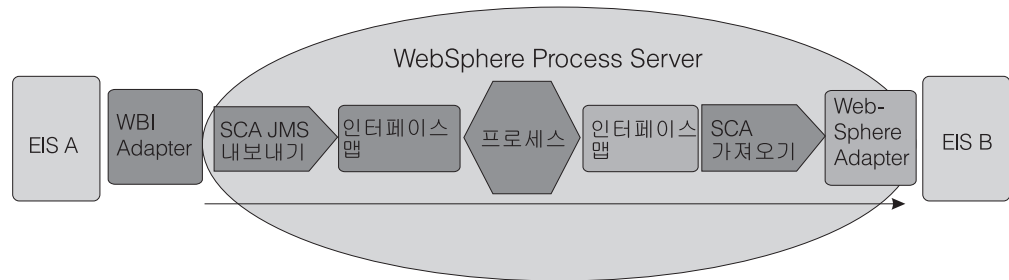
프로시저

1. 이 섹션에 제공된 예제 중 보안 필요성에 가장 가까운 예제를 판별하십시오. 일부 경우 둘 이상의 예제에서 정보를 조합하여 사용해야 할 수도 있습니다.
2. 관련 시나리오의 보안 정보를 읽고 보안 필요성에 적용하십시오.

예

종래의 통합 시나리오 - 인바운드 및 아웃바운드 어댑터

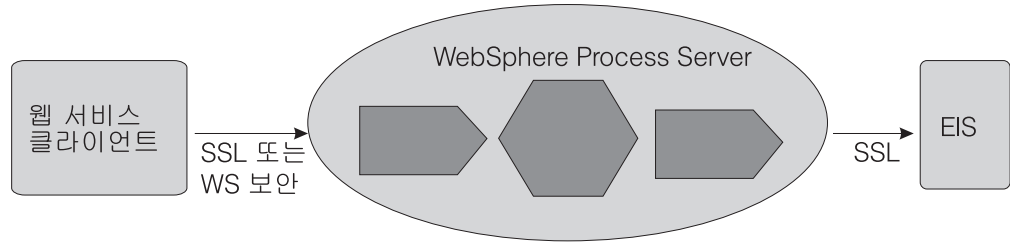
인바운드 요청이 WebSphere Business Integration Adapter에서 나옵니다. SCA(Service Component Architecture)는 SCA 내보내기를 기반으로 하는 인터페이스 맵을 호출합니다. 요청이 프로세스 컴포넌트 및 두 번째 인터페이스 맵을 거친 후 WebSphere Adapter를 통해 두 번째 EIS(B)로 전달됩니다. 이는 하나의 컴포넌트가 다음 컴포넌트의 메소드를 호출하는 SCA 호출입니다.



인바운드 어댑터의 인증 메커니즘은 없습니다. 첫 번째 컴포넌트(이 경우 첫 번째 인터페이스 맵 컴포넌트)의 SecurityIdentity 규정자를 정의하여 보안 컨텍스트를 설정할 수 있습니다. 이 지점에서 SCA가 한 컴포넌트에서 다음 컴포넌트로 보안 컨텍스트를 전달합니다. 각 컴포넌트의 액세스 제어는 SecurityPermission 규정자를 사용하여 정의합니다.

인바운드 웹 서비스 요청

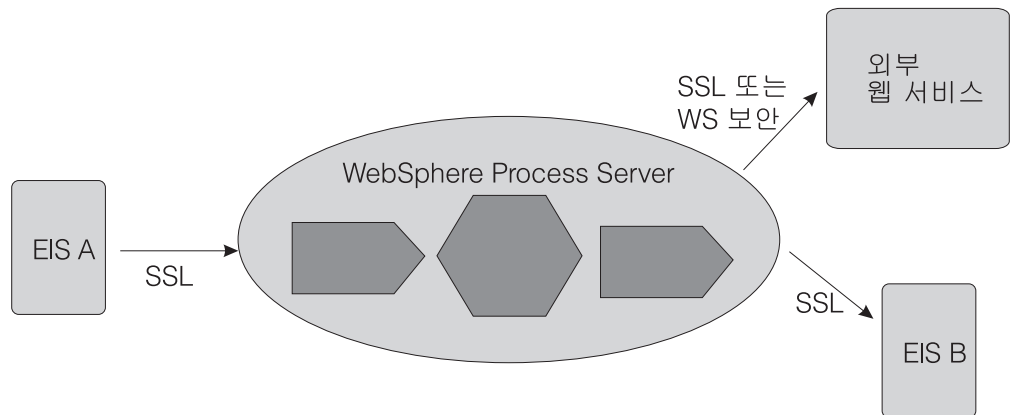
이 시나리오에서 웹 서비스 클라이언트가 WebSphere Process Server 컴포넌트를 호출합니다. 요청이 어댑터에 의해 EIS로 전달되기 전에 WebSphere Process Server 환경의 여러 컴포넌트를 거칩니다.



HTTP 기본 인증 또는 WS-Security 인증을 사용하여 웹 서비스 클라이언트를 SSL 클라이언트로 인증할 수 있습니다. 클라이언트가 인증되면 SecurityPermission 규정자에 따라 액세스 제어가 적용됩니다. 클라이언트와 WebSphere Process Server 인스턴스 사이에서 SSL 또는 WS-Security를 사용하여 데이터 무결성 및 프라이버시를 보호할 수 있습니다. SSL이 파이프 전체를 암호화하는 반면 WS-Security에서는 SOAP 메시지의 일부를 암호화하거나 디지털로 부호화할 수 있습니다. 웹 서비스의 경우 WS-Security가 우선된 표준입니다.

아웃바운드 웹 서비스 요청

이 시나리오의 경우 인바운드 요청이 어댑터, 웹 서비스 클라이언트 또는 HTTP 클라이언트에서 나올 수 있습니다. WebSphere Process Server의 컴포넌트(예: BPEL 컴포넌트)는 외부 웹 서비스를 호출합니다.



인바운드 웹 서비스 요청의 경우 HTTP 기본 인증 또는 WS-Security 인증을 사용하여 외부 웹 서비스를 SSL 클라이언트로 인증할 수 있습니다. LTPACallbackHandler를 콜백 메커니즘으로 사용하여 현재 RunAs주제에서 usernameToken을 추출하십시오. WebSphere Process Server와 대상 웹 서비스 사이에서 WS-Security를 사용하여 데이터 프라이버시 및 무결성을 보장할 수 있습니다.

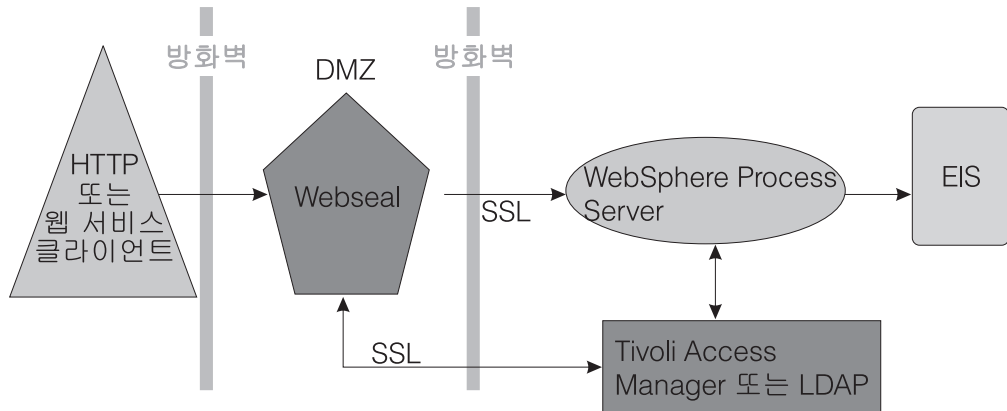
웹 응용프로그램 - WebSphere Process Server로의 HTTP 인바운드 요청

WebSphere Process Server는 HTTP에 대해 세 가지 유형의 인증을 지원합니다.

- HTTP 기본 인증

- HTTP 양식 기반 인증
- HTTPS SSL 기반 클라이언트 인증

또한 침입자로부터 인트라넷을 보호하도록 웹 서버를 DMZ(Demilitarized Zone)에 위치시키고 WebSphere Process Server를 내부 방화벽 안에 위치시킬 수 있습니다. 이 예에서는 인증을 수행하는 역 프록시로 WebSEAL을 사용합니다. 이는 방화벽 뒤의 WebSphere Process Server와 신뢰 연관이 있으며 인증된 요청을 전달할 수 있습니다.



관련 개념

➡ 서비스 통합 버스에 대한 보안 고려사항

주의사항

이 정보는 미국에서 제공되는 제품 및 서비스용으로 작성된 것입니다.

IBM은 다른 국가에서 이 책에 기술된 제품, 서비스 또는 기능을 제공하지 않을 수도 있습니다. 현재 사용할 수 있는 제품 및 서비스에 대한 정보는 한국 IBM 담당자에게 문의하십시오. 이 책에서 IBM 제품, 프로그램 또는 서비스를 언급했다고 해서 해당 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM의 지적 재산을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수도 있습니다. 그러나 비IBM 제품, 프로그램 또는 서비스의 운영에 대한 평가 및 검증은 사용자의 책임입니다.

IBM은 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 책을 제공한다고 해서 특허에 대한 라이선스까지 부여하는 것은 아닙니다. 라이선스에 대한 의문사항은 다음으로 문의하십시오.

135-700

서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩

한국 아이.비.엠 주식회사

고객만족센터

전화번호: 080-023-8080

2바이트 문자 세트(DBCS) 정보에 관한 라이선스 조치는 한국 IBM 지적재산권에 문의하거나 다음 주소로 서면 문의하시기 바랍니다.

IBM World Trade Asia Corporation

Licensing

2-31 Roppongi 3-chome, Minato-ku

Tokyo 106-0032, Japan

다음 단락은 현지법과 상충하는 영국이나 기타 국가에서는 적용되지 않습니다. IBM은 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여 (단, 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증 없이 이 책을 "현 상태대로" 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, 변경된 사항은 최신판에 통합됩니다. IBM은 이 책에서 설명한 제품 및/또는 프로그램을 사전 통지 없이 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 프로그램과 기타 프로그램(본 프로그램 포함)간의 정보 교환 및
(ii) 교환된 정보의 상호 이용을 목적으로 본 프로그램에 관한 정보를 원하는 프로그램 라이선스 사용자는 다음 주소로 문의하십시오.

135-700

서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩

한국 아이.비.엠 주식회사

고객만족센터

이러한 정보는 해당 조건(예를 들면, 사용료 지불 등)하에서 사용될 수 있습니다.

이 문서에 기술된 라이선스가 있는 프로그램 및 이 프로그램에 대해 사용 가능한 라이선스가 있는 모든 자료는 IBM이 IBM 기본 계약, IBM 프로그램 라이선스 계약 또는 모든 동등한 계약 하에서 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 단계의 시스템에서 측정되었을 수 있으므로 이러한 측정치가 일반적으로 사용되고 있는 시스템에서도 동일하게 나타날 것이라고는 보증할 수 없습니다. 또한 일부 성능은 추정을 통해 추측되었을 수도 있으므로 실제 결과는 다를 수 있습니다. 이 책의 사용자는 해당 데이터를 본인의 특정 환경에서 검증해야 합니다.

비IBM 제품에 관한 정보는 해당 제품의 공급업체, 공개 자료 또는 기타 범용 소스로부터 얻은 것입니다. IBM에서는 이러한 비IBM 제품을 반드시 테스트하지 않았으므로, 이들 제품과 관련된 성능의 정확성, 호환성 또는 기타 주장에 대해서는 확인할 수 없습니다. 비IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오.

IBM이 제시하는 방향 또는 의도에 관한 모든 언급은 특별한 통지 없이 변경될 수 있습니다.

이 정보에는 일상의 비즈니스 운영에서 사용되는 자료 및 보고서에 대한 예제가 들어 있습니다. 이들 예제에는 개념을 가능한 완벽하게 설명하기 위하여 개인, 회사, 상표 및 제품의 이름이 사용될 수 있습니다. 이들 이름은 모두 가공의 것이며 실제 기업의 이름 및 주소와 유사하더라도 이는 전적으로 우연입니다.

저작권 라이선스:

이 정보에는 여러 운영 플랫폼에서의 프로그래밍 기법을 보여주는 원어로 된 샘플 응용프로그램이 들어 있습니다. 귀하는 이러한 샘플 프로그램의 작성 기준이 된 운영 플랫폼의 응용프로그램 프로그래밍 인터페이스(API)에 부합하는 응용프로그램을 개발, 사용, 판매 또는 배포할 목적으로 IBM에 비용을 지불하지 않고 이들 샘플 프로그램을 어떠한 형태로든 복사, 수정 및 배포할 수 있습니다. 이러한 샘플 프로그램은 모든 조건 하에서 완전히 테스트된 것은 아닙니다. 따라서 IBM은 이러한 프로그램의 신뢰성, 서비스 가능성 또는 기능을 보증하거나 진술하지 않습니다.

이러한 샘플 프로그램 또는 파생 제품의 각 사본이나 그 일부에는 반드시 다음과 같은 저작권 표시가 포함되어야 합니다. © (귀하의 회사명) (연도). 이 코드의 일부는 IBM Corp.의 샘플 프로그램에서 파생됩니다. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

이 정보를 소프트카피로 확인하는 경우에는 사진과 컬러 삽화가 제대로 나타나지 않을 수도 있습니다.

프로그래밍 인터페이스 정보

프로그래밍 인터페이스 정보는 본 프로그램을 사용하는 응용프로그램 소프트웨어 작성을 돕기 위해 제공됩니다.

귀하는 범용 프로그래밍 인터페이스를 통해 본 프로그램 툴의 서비스를 제공하는 응용프로그램 소프트웨어를 작성할 수 있습니다.

그러나 본 정보에는 진단, 수정 및 성능 조정 정보도 포함되어 있습니다. 진단, 수정 및 성능 조정 정보는 응용프로그램 소프트웨어의 디버그를 돕기 위해 제공된 것입니다.

경고: 본 진단, 수정 및 조정 정보는 변경될 수 있으므로 프로그램 인터페이스로서 사용될 수 없습니다.

상표 및 서비스표

IBM, IBM 로고 및 ibm.com은 미국 또는 기타 국가에서 사용되는 International Business Machines Corporation의 상표 또는 등록상표입니다. 이들 및 기타 IBM 상표 용어가 이 정보에서 처음 나타날 때 상표 기호(^R 또는 TM)와 함께 표시되는 경우, 이들 기호는 이 정보가 출판된 당시 IBM이 소유한 미국 등록 또는 관습법 상표를 표시합니다. 또한 이러한 상표는 기타 국가에서 등록상표 또는 일반 법적 상표입니다. IBM 상표의 현재 목록은 www.ibm.com/legal/copytrade.shtml 웹 페이지의 "저작권 및 상표 정보"에 있습니다.

Windows는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 등록상표입니다.

Linux는 미국 또는 기타 국가에서 사용되는 Linus Torvalds의 등록상표입니다.

Java 및 JavaBeans는 미국 또는 기타 국가에서 사용되는 Sun Microsystems, Inc.의 상표입니다.

UNIX는 미국 또는 기타 국가에서 사용되는 The Open Group의 등록상표입니다.

기타 회사, 제품 및 서비스 이름은 해당 회사의 상표 또는 서비스표입니다.

이 제품은 Eclipse 프로젝트에서 개발한 소프트웨어를 포함합니다.
(<http://www.eclipse.org> 웹 사이트 참조)



멀티플랫폼용 IBM WebSphere Process Server, 버전 6.2

IBM