WebSphere® 멀티플랫폼용 Process Server

버전 6.1.0

보안 응용프로그램 및 환경

WebSphere 멀티플랫폼용 Process Server

버전 6.1.0

보안 응용프로그램 및 환경

주!

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

2008년 2월 1일

이 개정판은 새 개정판에서 별도로 명시하지 않는 한 멀티플랫폼용 WebSphere Process Server의 버전 6, 릴리스 1, 수정판 0(제품 번호: 5724-L01) 및 모든 후속 릴리스와 수정판에 적용됩니다.

이 문서에 대한 의견을 보내려면 doc-comments@us.ibm.com으로 전자 우편 메시지를 전송하십시오. 여러분의 의견을 기대하고 있습니다.

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

목차

응용프로그램 및 환경 보안

WebSphere® Process Server 환경 및 응용프로그램 보안은 매우 중요합니다.

1. 이 설명서에 제공되는 정보는 다음 링크에서 Adobe® PDF 형식으로 사용할 수 있습니다. WebSphere Process Server documentation(PDF 형식).
2. IBM® developerWorks®의 비즈니스 프로세스 관리 정보 로드맵은 포트폴리오에서 WebSphere Process Server 및 다른 제품에 대한 정보를 구성합니다.

이러한 문서는 WebSphere Application Server Network Deployment, 버전 6 Information Center와 특히 WebSphere Application Server Network Deployment, 버전 6 Security Documentation에 있는 핵심 보안 문서의 보충 정보입니다.

데이터 및 프로세스의 보안은 매우 중요합니다. WebSphere Process Server 보안은 WebSphere Application Server 버전 6.1 보안을 기반으로 합니다. 보안에 대한 자세한 정보는 WebSphere Application Server Network Deployment, 버전 6 Information Center를 참조하십시오.

일반 개요

데이터 및 프로세스의 보안은 매우 중요합니다.

WebSphere Process Server 보안은 WebSphere Application Server 버전 6.1 보안을 기본으로 합니다. 보안에 대한 자세한 정보는 WebSphere Application Server Network Deployment, 버전 6 Information Center를 참조하십시오.

보안 타스크는 크게 WebSphere Process Server 환경의 보안 관리와 관련된 타스크 및 WebSphere Process Server에서 실행되는 응용프로그램과 관련된 타스크로 구분할 수 있습니다. 서버 환경 보안이 응용프로그램 보안의 핵심이므로 두 보안을 따로 분리해서 생각하지 않아야 합니다.

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

응용프로그램 보안에는 여러 측면이 있습니다. 여기에는 다음이 포함됩니다.

- **38 페이지의 『인증』**. 응용프로그램을 호출하는 사용자 또는 프로세스를 인증해야 합니다.
- **40 페이지의 『액세스 제어』**. 인증된 사용자는 조작을 수행할 수 있는 권한을 가지고 있어야 합니다.

- **40 페이지의 『데이터 무결성 및 프라이버시』**. 응용프로그램이 액세스하는 데이터는 권한이 없는 관계자가 어떤 방법으로도 보거나 수정할 수 없도록 보안을 유지해야 합니다.
- **41 페이지의 『단일 사인온』**. 단일 사인온으로, 사용자가 인증 데이터를 한 번 제공하도록 한 후 이 인증 정보를 다운스트림 컴포넌트로 전달합니다.

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

WebSphere Process Server에 특정한 보안 고려사항

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

WebSphere Process Server 보안 기능

- 관리 콘솔 패널 비즈니스 통합 보안은 WebSphere Process Server에 고유합니다. **보안**을 펼치고 **비즈니스 통합 보안**을 클릭하면 이 패널에 도달할 수 있습니다. 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.
- 컴포넌트 특정 보안 역할 세트가 있습니다.

보안 시작하기

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

타스크 정보

민감한 데이터의 보안을 유지보수하려면 프로세스 서버 환경과 해당 환경에 전개하는 응용프로그램을 보호해야 합니다.

프로시저

1. WebSphere Process Server를 설치할 때 보안을 고려하십시오. 3 페이지의 『WebSphere Process Server 설치: 보안 고려사항』의 내용을 참조하십시오.
2. 독립형 또는 전개 환경 설치에 대해 보안이 작동하는지 확인하십시오.
   a. 9 페이지의 『관리 보안』이 작동하는지 확인하십시오. 관리 보안은 기본적으로 작동됩니다.
   b. 11 페이지의 『응용프로그램 보안』이 작동하는지 확인하십시오. 응용프로그램 보안은 기본적으로 작동됩니다.

c. 필요한 경우 11 페이지의 『Java 2 보안』을 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. 프로세스 서버 환경에 전개하는 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.

   d. WebSphere Process Server 환경의 보안을 유지보수하십시오.

WebSphere Process Server 설치: 보안 고려사항

다음 타스크를 수행하여 WebSphere Process Server 설치 전, 설치 중 및 설치 후 보안을 구현하십시오.

타스크 정보

이 타스크는 WebSphere Process Server 설치 시에 수행해야 합니다.

프로시저

1. 설치 전에 환경의 보안을 설정하십시오.

   적절한 보안을 사용하여 WebSphere Process Server를 설치하는 데 필요한 명령은 운영 체제에 따라 다릅니다. 설치 이전에 취할 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 취할 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 완료했으면 관리 콘솔에서 보안을 관리할 수 있습니다.

관련 태스크

설치를 위한 i5/OS® 시스템 준비
WebSphere Process Server 설치에 대해 i5/OS 시스템을 준비하는 방법을 학습합니다.

관련 정보

설치 전 환경 보안

제품 설치를 위한 운영 체제 준비

설치 후 환경 보안

설치 시 제공되는 인증 정보

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 사용**을 선택한 상태로 유지하는 경우 사용자 이름 및 암호를 묻는 프롬프트가 표시됩니다. 이 ID는 모든 기본 컴포넌트의 기본값으로 사용됩니다. 보안을 더 강화하려면 프로파일 작성 후 이 ID를 구성해야 합니다.

WebSphere Process Server의 여러 구성요소에 인증 별명이 활용됩니다. 이 별명은 데이터베이스 및 메시징 엔진에 액세스하기 위해 런타임 구성요소를 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.

타스크 정보

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

이 컴포넌트는 다음과 같습니다.

- 서비스 컴포넌트 아키텍처(SCA)
- 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 패널로 이동하십시오. 보안을 펼치고 비즈니스 통합 보안을 클릭하십시오.
2. 서비스 컴포넌트 아키텍처(SCA), Business Process Choreographer 및 CEI(Common Event Infrastructure) 인증 별명 각각에 대해, 인증 별명으로 사용할 적절한 사용자 이름과 암호를 제공하십시오. 선택 열에서 선택란을 선택하여 변경하려는 별명을 선택하고 편집을 클릭하십시오. 후속 패널에서 컴포넌트에 대한 인증 별명으로 사용할 사용자 이름과 암호를 제공하십시오. 사용자가 제공하는 신임은 사용자가 사용하는 사용자 계정 저장소에 존재해야 합니다.

다음에 수행할 작업

인증 별명 관리에 대한 자세한 정보는 계속되는 주제에서 제공됩니다.

관련 태스크

39 페이지의『인증 별명 수정』
기존 인증 별명을 수정해야 할 수도 있습니다.

독립형 서버에 대해 WebSphere Process Server 보안 구성

WebSphere Process Server의 독립형 설치에 대한 보안 구성 방법에 대해서는 아래에 있는 링크를 따르십시오.

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 타스크를 시작하기 전에 WebSphere Process Server를 설치하고 설치를 검증해야 합니다.

타스크 정보

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

프로시저

1. 관리 보안이 작동되는지 확인하십시오. 8 페이지의 『관리 보안 사용 가능』을 참조하십시오.
2. 응용프로그램 보안이 작동하는지 확인하십시오. 37 페이지의 『WebSphere Process Server에서 응용프로그램 보안』을 참조하십시오.
3. 관리 역할에 사용자나 그룹을 추가하십시오. **관리 사용자 역할** 또는 **관리 그룹 역할**에 따라 개별 사용자나 사용자 그룹에 관리 권한을 부여할 수 있습니다.
4. 사용하려는 사용자 계정 저장소를 선택하십시오.

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

사용자 레지스트리	조치
연합 저장소	단일 범주 아래에 있는 여러 저장소에서 프로파일을 관리하려면 이 설정을 지정하십시오. 범주는 다음에서 ID로 구성될 수 있습니다. • 시스템에 빌드된 파일 기반 저장소 • 하나 이상의 외부 저장소 • 내장된 파일 기반 저장소와 하나 이상의 외부 저장소 **주:** 관리자 특권을 가지고 있는 사용자만 연합 저장소 구성을 볼 수 있습니다. 자세한 정보는 연합 저장소 구성에서 범주 관리를 참조하십시오.
로컬 운영 체제	기본 사용자 레지스트리. 사용자 계정 레지스트리를 구성하는 방법에 대한 세부사항은 13 페이지의 『사용자 계정 저장소 구성』을 참조하십시오.
독립형 LDAP 레지스트리	사용자 레지스트리로 LDAP를 구성하려면 사용자 레지스트리로 LDAP(Lightweight Directory Access Protocol) 구성의 지시사항에 따르십시오.
독립형 사용자 정의 레지스트리	사용자 계정 레지스트리를 구성하는 방법에 대한 세부사항은 13 페이지의 『사용자 계정 저장소 구성』을 참조하십시오.

5. 변경사항을 적용하십시오.

   패널의 맨 아래에서 **적용** 단추를 클릭하십시오.

6. 비즈니스 통합 보안 패널로 이동하십시오. **보안**을 펼치고 **비즈니스 통합 보안**을 클릭하십시오.
7. 나열된 인증 별명에 대해 적절한 사용자 ID를 제공하십시오. 사용자가 제공하는 신임은 사용자가 사용하는 사용자 계정 저장소에 존재해야 합니다.
8. 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 및/또는 그룹 이름. 이 역할로 지정된 사용자는 모든 특권을 가집니다.
   - **모니터**: 비즈니스 플로우 및 휴먼 타스크 모니터 역할에 대한 사용자 이름 및/또는 그룹 이름. 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 나열됩니다.

   - **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.
9. 변경사항을 적용하십시오.

   패널의 맨 아래에서 **적용** 단추를 클릭하십시오.
10. 로컬 구성에 대한 변경사항을 저장하십시오.

    메시지 분할창에서 **저장**을 클릭하십시오.
11. 필요하면, 서버를 중지한 후 재시작하십시오.

    서버를 재시작해야 하는 경우 관리 콘솔에 적용 메시지가 나타납니다.

결과

그런 다음 유효한 사용자 이름 및 암호를 제공해야 하는 관리 콘솔에 로그인합니다.

사용자가 작성하는 각 프로파일은 이 방법으로 보안을 설정해야 합니다. 시스템 관리자 사용자 ID는 설치 및 환경 구성 중 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

제품 설치 확인
설치 확인 도구를 사용하여 WebSphere Process Server 설치와 독립형 서버 또는 Deployment Manager 프로파일 작성이 성공했는지 확인하십시오. *프로파일*은 Deployment Manager 또는 서버에 대한 런타임 환경을 정의하는 파일로 구성됩니다. installver_wbi 체크섬 도구로 코어 제품 파일을 확인하십시오. IVT(Installation Verification Test) 도구를 사용하여 각각의 프로파일을 확인하십시오.

관리 보안 사용 가능

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

시작하기 전에

이 타스크를 시작하기 전에 WebSphere Process Server를 설치하고 설치를 확인하십시오.

타스크 정보

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

프로시저

1. 관리 콘솔에서 관리 보안 패널을 여십시오.

   보안을 펼치고 **보안 관리, 응용프로그램 및 하부 구조**를 클릭하십시오.
2. 관리 보안을 사용 가능하게 하십시오.

   관리 보안 사용을 선택하십시오.
3. 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. 필요한 모든 사용 권한이 없는 응용프로그램에서 AccessControl 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 경고**를 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 제한**을 선택하십시오. 응용프로그램 액세스를 민감한 JCA(Java Connector Architecture) 맵핑 인증 데이터로 제한해야 하는 경우 이 옵션이 사용 가능하도록 설정하십시오.

4. 변경사항을 적용하십시오.

   패널의 맨 아래에서 **적용** 단추를 클릭하십시오.

5. 로컬 구성에 대한 변경사항을 저장하십시오.

   메시지 분할창에서 **저장**을 클릭하십시오.

6. 필요하면, 서버를 중지한 후 재시작하십시오.

   서버를 재시작해야 하는 경우 관리 콘솔에 적용 메시지가 나타납니다.

다음에 수행할 작업

작성하는 프로파일마다 관리 보안을 작동시켜야 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 올바르지 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 응

용프로그램 서버는 동일한 물리적 시스템에 상주해야 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 않을 것을 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)
- 공통 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 모두 사용 가능했습니다. 글로벌 보안의 개념은 이제 관리 보안 및 응용프로그램 보안으로 분할되며, 각각의 보안은 별도로 사용 가능하도록 설정할 수 있습니다.

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 특정의 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 대해 준비하지 못할 수도 있습니다. 관리자는 응용프로그램이 Java 2 보안에 대해 준비되지 않은 경우에 Java 2 보안 사용 가능화에 대해 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

Java 2 보안

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.

타스크 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 환경에서 사용자 레지스트리로 LDAP를 사용해야 합니다.

프로시저

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

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

사용자 레지스트리	조치
연합 저장소	단일 범주 아래에 있는 여러 저장소에서 프로파일을 관리하려면 이 설정을 지정하십시오. 범주는 다음에서 ID로 구성될 수 있습니다. • 시스템에 빌드된 파일 기반 저장소 • 하나 이상의 외부 저장소 • 내장된 파일 기반 저장소와 하나 이상의 외부 저장소 **주:** 관리자 특권을 가지고 있는 사용자만 연합 저장소 구성을 볼 수 있습니다. 자세한 정보는 연합 저장소 구성에서 범주 관리를 참조하십시오.
로컬 운영 체제	기본 사용자 레지스트리. **사용 가능한 범주 정의**에서 **로컬 운영 체제**를 선택하고 **구성**을 클릭하십시오. 로컬 OS 사용자 레지스트리 페이지에 사용자 이름과 암호를 제공하십시오. 이 사용자 이름은 서버의 ID로 사용됩니다. 사용자가 자동으로 **관리자** 역할에 추가됩니다. **주:** Network Deployment 환경에서 사용자 레지스트리로 로컬 운영 체제를 사용하지 마십시오.
LDAP(Lightweight Directory Access Protocol)	사용자 레지스트리로 LDAP(Lightweight Directory Access Protocol) 구성의 지시사항에 따라 사용자 레지스트리로 LDAP를 구성하십시오.

사용자 레지스트리	조치
사용자 정의 사용자 레지스트리	사용자 정의 계정 저장소를 선택하고 사용자 필요에 맞게 구성하십시오.
Tivoli® Access Manager	**주:** 이 옵션은 관리 콘솔을 통해 사용할 수 없으므로, wsadmin 명령을 사용하여 구성해야 합니다.

사용자 계정 저장소 구성

관리 콘솔을 사용하여 사용자 계정 저장소를 구성할 수 있습니다. 서버 사용자 ID를 선택하거나 자동으로 서버 ID를 생성할 수 있습니다.

타스크 정보

관리 콘솔을 사용하여 사용자 계정 저장소를 구성할 수 있습니다. WebSphere Process Server가 자동으로 서버 사용자 ID를 생성하도록 허용할 것을 선택하거나 사용 중인 사용자 계정 저장소에서 지정할 수 있습니다. 후자의 선택을 사용하면 관리 조치의 감사 가능성이 개선됩니다.

프로시저

1. 관리 콘솔에서 사용자 레지스트리에 대한 **사용자 계정 저장소** 구성 페이지를 여십시오.

   보안을 펼치고 **보안 관리, 응용프로그램 및 하부 구조**를 클릭한 후 **사용 가능한 범주 정의** 메뉴에서 사용자가 사용하는 사용자 레지스트리를 선택하십시오. **구성**을 클릭하십시오.
2. 옵션: **1차 관리 사용자 이름**을 입력하십시오. 로컬 운영 체제에 정의된 관리 특권을 가지고 있는 사용자의 이름을 지정합니다. 사용자 이름은 관리 보안이 사용 가능한 경우 관리 콘솔에 로그온하는 데 사용됩니다.
3. **자동으로 생성된 서버 ID** 또는 **저장소에 저장된 서버 ID** 옵션을 선택하십시오.

   저장소에 저장된 서버 ID 옵션을 선택한 경우 다음 정보를 입력하십시오.
   - 서버 사용자 ID 또는 관리 사용자
   - 이 사용자에 대해 연관된 암호

   이 ID는 사용자 계정 저장소에 존재해야 합니다.

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.

타스크 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 JACC 프로바이더에 설치된 응용프로그램의 보안 정책 전파를 참조하십시오.

사용자 레지스트리로 LDAP(Lightweight Directory Access Protocol) 구성

기본적으로 사용자 레지스트리는 로컬 운영 체제 레지스트리입니다. 가능하면 사용자 레지스트리로 외부 LDAP(Lightweight Directory Access Protocol)를 사용하십시오. Network Deployment 환경에서 LDAP를 사용해야 합니다.

타스크 정보

이 타스크는 글로벌 보안이 켜져 있다고 가정합니다.

프로시저

1. WebSphere Process Server를 시작하십시오.
2. 관리 콘솔을 실행하십시오.
3. LDAP 사용자 레지스트리 구성 페이지를 여십시오.

   보안을 펼치고 **보안 관리, 응용프로그램 및 하부 구조**를 클릭한 후 **사용 가능한 범주 정의** 메뉴에서 **LDAP**를 선택하십시오. **구성**을 클릭하십시오.
4. **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 사용하거나 wsadmin 명령에서 사용됩니다.
5. **적용**을 클릭하십시오.
6. **자동으로 생성된 서버 ID** 또는 **저장소에 저장된 서버 ID** 옵션을 선택하십시오.

   저장소에 저장된 서버 ID 옵션을 선택한 경우 다음 정보를 입력하십시오.
   - 서버 사용자 ID 또는 관리 사용자
   - 이 사용자에 대해 연관된 암호

   이 ID가 LDAP 관리자의 사용자 ID는 아니지만 LDAP에 입력이 있어야 합니다.
7. 사용 중인 LDAP 유형을 선택하십시오.

   유형 목록에서 사용자 레지스트리로 사용할 특정 LDAP을 선택하십시오.
8. LDAP가 상주하는 컴퓨터의 이름을 입력하십시오.

   호스트 필드에 LDAP가 상주하는 서버의 이름을 입력하십시오.
9. LDAP이 청취하는 포트 번호를 입력하십시오.

   포트 필드에 LDAP 서버가 청취하는 포트 번호를 입력하십시오.

10. **기본 식별 이름**을 입력하십시오.

    이 값은 디렉토리 서비스의 기본 식별 이름을 지정하며 이는 디렉토리 서비스의 LDAP 검색에 대한 시작점을 표시합니다.

    권한 목적의 경우, 이 필드는 대소문자를 구분합니다. 이 스펙은 토큰을 수신하는 경우(예: 다른 셀 또는 Domino® Server에서) 서버의 기본 식별 이름(DN)이 다른 셀 또는 Domino Server의 기본 DN과 정확히 일치해야 함을 의미합니다. 권한에 대해 대소문자를 구분하지 않아도 될 경우 **대소문자 구분 안함** 필드를 사용 가능하게 하십시오. 이 필드는 Domino 디렉토리를 제외한 모든 LDAP 디렉토리에 필요하며 여기서 이 필드는 선택적입니다.
11. 나머지 매개변수는 기본값으로 두고 변경을 확인하십시오.

    확인을 클릭하십시오.

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 테이블에는 서버 시작 옵션이 설명되어 있습니다.

서버 시작	세부사항
첫 번째 단계 사용자 인터페이스에서	서버 시작을 클릭하십시오.
명령행에서	다음을 입력하십시오. • Windows **Windows® 플랫폼:** startserver *servername* • Linux UNIX **Linux® 및 UNIX® 플랫폼:** startserver.sh *servername* • i5/OS **System i(QShell 명령행에서):** startserver *servername* *install_dir*/bin 디렉토리의 명령 프롬프트에서 입력하십시오.

주: 서버를 시작하는 데에는 사용자 이름과 암호를 제공하지 않아도 됩니다. 하지만 관리 콘솔을 실행하거나 기타 관리 타스크를 수행하려 시도할 경우에는 인증이 필요합니다.
서버가 시작되거나 오류 메시지가 리턴됩니다.

2. 서버를 중지하십시오.

   다음 테이블에는 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 이름은 운영자 또는 관리자 역할에 있어야 합니다.
명령행에서	다음을 입력하십시오. • Windows **Windows 플랫폼:** stopserver *servername* -profileName *ProfileName* -username *username* -password *password* • Linux UNIX **Linux 및 UNIX 플랫폼:** stopserver.sh *servername* -profileName *ProfileName* -username *username* -password *password* • i5/OS **System i(QShell 명령행에서):** stopserver *servername* -profileName *ProfileName* -username *username* -password *password* *install_dir*/bin 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 테이블에는 서버가 올바로 중지되었는지 확인하는 옵션이 설명되어 있습니다.

서버 중지 확인	세부사항
사용자 인터페이스에서	첫 번째 단계 출력 창에 요청 결과가 자세히 설명됩니다.
명령행에서	요청 결과가 요청이 시작된 명령 창에 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 액세스하도록 이 네 개 역할 중 하나로 사용자가 맵핑되어야 합니다.

설치 후 서버에 로그인하는 첫 번째 사용자가 관리 콘솔에 추가됩니다.

표 1. 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 수정할 수 있습니다(즉, 서버 시작 및 중지).
관리자	관리자 역할은 구성자 역할과 운영자 역할이 조합된 것이며 관리자 역할에만 추가 특권이 부여됩니다. 예는 다음과 같습니다. • 서버 사용자 ID 및 암호 수정 • 관리자 역할에 사용자 및 그룹 맵핑 또한 다음과 같이 민감한 정보에 액세스하는 데 필요한 권한을 갖습니다. • 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 사용자에 대해서만 사용 가능하고 wsadmin 사용자에 대해서는 사용할 수 없습니다. 이 역할이 부여된 사용자는 연합 저장소에서 사용자와 그룹을 관리하기 위한 관리자 특권을 가지고 있습니다. 예를 들어, iscadmins 역할의 사용자는 다음 타스크를 완료할 수 있습니다. • 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 언제라도 관리 역할에 사용자 또는 그룹을 추가하고 반대로 제거할 수도 있습니다. 하지만 변경사항을 적용하는 데 서버 재시작이 필요합니다. 우수 사례는, 보다 유연하고 관리가 쉽기 때문에 특정 사용자보다는 그룹을 관리 역할에 맵핑하는 것입니다. 그룹을 관리 콘솔에 맵핑하면 그룹에 사용자 추가 또는 반대인 제거가 WebSphere Process Server 외부에서 이루어지며 변경사항을 적용하는 데 서버를 재시작할 필요가 없습니다.

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. Everyone 특별 주제는 보안이 사용 가능화되지는 않은 것처럼 인증과 무관하게 아무나 조치 수행이 가능함을 의미합니다.

설치된 구성요소의 기본 보안

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

용도

WebSphere Process Server의 여러 중요 컴포넌트는 메시징 엔진 및 데이터베이스에서의 인증을 위해 사전 정의된 별명을 사용합니다. 프로파일 작성 중 이 인증 별명에는 기본 관리자 사용자 ID 및 암호의 기본값이 제공됩니다. 사용자 계정 저장소에 있는 다른 사용자에 해당되도록 이 별명을 구성해야 합니다.

Business Process Choreographer 인증 별명

비즈니스 프로세스에는 다음과 같은 인증 별명이 있습니다. 이러한 별명은 관리 콘솔에서 수정하십시오.

호출 사용자의 ID와 관계없이 표 2의 별명을 사용하여 구성요소를 호출합니다.

표 2. 비즈니스 프로세스와 연관된 인증 별명

별명	설명	정보
BPEAuthDataAliasJMS_*node_server*	메시징 엔진을 사용한 인증에 사용됩니다.	프로파일 마법사의 Business Process Choreographer 구성 패널에 사용자 이름 및 암호를 입력하십시오.
BPEAuthDataAlias*DbType_node_server*	데이터베이스를 사용한 인증에 사용됩니다.	제공된 스크립트를 사용하여 데이터베이스를 구성하십시오.

표 3에는 비즈니스 프로세스에 대해 작성된 RunAs 역할이 설명되어 있습니다.

표 3. 비즈니스 프로세스와 연관된 RunAs 역할

RunAs 역할	설명	정보
JMSAPIUser	bpecontainer.ear에서 BFM JMS API MDB에 의해 사용됩니다.	프로파일 마법사의 Business Process Choreographer 구성 패널에 사용자 이름 및 암호를 입력하십시오.
EscalationUser	task.ear MDB에 의해 사용됩니다.	프로파일 마법사의 Business Process Choreographer 구성 패널에 사용자 이름 및 암호를 입력하십시오.

제공하는 사용자 이름이 RunAs 역할에 추가됩니다.

CEI(Common Event Infrastructure) 인증 별명

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

호출 사용자의 ID와 관계없이 표 4의 별명을 사용하여 구성요소를 호출합니다.

표 4. CEI(Common Event Infrastructure)와 연관된 인증 별명

별명	설명	정보
CommonEventInfrastructure JMSAuthAlias 테이블 셀에 맞춰 사용할 수 있도록 이 항목에 문자 공간이 추가되었습니다. 실제 별명에는 문자 공간이 포함되어 있지 않습니다.	메시징 엔진을 사용한 인증에 사용됩니다.	프로파일 마법사의 CEI(Common Event Infrastructure) 구성 패널에 사용자 이름 및 암호를 입력하십시오.
EventAuthAlias*DBType*	데이터베이스를 사용한 인증에 사용됩니다.	프로파일 마법사의 CEI(Common Event Infrastructure) 구성 패널에 사용자 이름 및 암호를 입력하십시오.

서비스 구성요소 아키텍처 인증 별명

서비스 구성요소 아키텍처(SCA)에 다음의 인증 별명이 있습니다. 이러한 별명은 관리 콘솔에서 수정하십시오.

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

표 5. SCA 구성요소와 연관된 인증 별명

별명	설명	정보
SCA_Auth_Alias	메시징 엔진을 사용한 인증에 사용됩니다.	프로파일 마법사의 SCA 구성 패널에 사용자 이름 및 암호를 입력하십시오.

비즈니스 프로세스 및 휴먼 타스크 응용프로그램에서의 액세스 제어

다음의 엔터프라이즈 아카이브(EAR) 파일은 액세스 제어를 통해 Business Process Choreographer 설치의 일부분으로 설치됩니다. Business Process Choreographer는 WebSphere Process Server 설치의 일부로 설치됩니다. 휴먼 타스크 관리자는 이러한 역할을 사용하여 프로덕션 시스템에서 사용자의 역량을 판별합니다.

EAR 파일	역할	기본 권한	Notes®
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 타스크에 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

다음의 엔터프라이즈 아카이브(EAR) 파일은 액세스 제어를 통해 CEI(Common Event Infrastructure) 설치의 일부로 설치됩니다. CEI(Common Event Infrastructure)는 WebSphere Process Server 설치의 일부로 설치됩니다.

EventServer.ear 파일은 CEI(Common Event Infrastructure) 설치의 일부분으로 설치된 EAR 파일만 가능합니다.

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

전개 환경 서버에 대해 WebSphere Process Server 보안 구성

WebSphere Process Server의 전개 환경 설치에 대한 보안 구성 방법에 대해서는 아래에 있는 링크를 따르십시오.

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.

타스크 정보

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

프로시저

1. 관리 보안이 작동되는지 확인하십시오. 8 페이지의 『관리 보안 사용 가능』을 참조하십시오.
2. 응용프로그램 보안이 작동하는지 확인하십시오. 37 페이지의 『WebSphere Process Server에서 응용프로그램 보안』을 참조하십시오.
3. 관리 역할에 사용자나 그룹을 추가하십시오. **관리 사용자 역할** 또는 **관리 그룹 역할**에 따라 개별 사용자나 사용자 그룹에 관리 권한을 부여할 수 있습니다.
4. 사용하려는 사용자 계정 저장소를 선택하십시오.

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

사용자 레지스트리	조치
연합 저장소	단일 범주 아래에 있는 여러 저장소에서 프로파일을 관리하려면 이 설정을 지정하십시오. 범주는 다음에서 ID로 구성될 수 있습니다. • 시스템에 빌드된 파일 기반 저장소 • 하나 이상의 외부 저장소 • 내장된 파일 기반 저장소와 하나 이상의 외부 저장소 **주:** 관리자 특권을 가지고 있는 사용자만 연합 저장소 구성을 볼 수 있습니다. 자세한 정보는 연합 저장소 구성에서 범주 관리를 참조하십시오.
로컬 운영 체제	기본 사용자 레지스트리. 사용자 계정 레지스트리를 구성하는 방법에 대한 세부사항은 13 페이지의 『사용자 계정 저장소 구성』을 참조하십시오.

사용자 레지스트리	조치
독립형 LDAP 레지스트리	사용자 레지스트리로 LDAP(Lightweight Directory Access Protocol) 구성의 지시사항에 따라 사용자 레지스트리로 LDAP를 구성하십시오.
독립형 사용자 정의 레지스트리	사용자 계정 레지스트리를 구성하는 방법에 대한 세부사항은 13 페이지의 『사용자 계정 저장소 구성』을 참조하십시오.

5. 변경사항을 적용하십시오.

   패널의 맨 아래에서 **적용** 단추를 클릭하십시오.
6. 비즈니스 통합 보안 패널로 이동하십시오. **보안**을 펼치고 **비즈니스 통합 보안**을 클릭하십시오.
7. 나열된 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.
8. 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 및/또는 그룹 이름. 이 역할로 지정된 사용자는 모든 특권을 가집니다.
   - **모니터**: 비즈니스 플로우 및 휴먼 타스크 모니터 역할에 대한 사용자 이름 및/또는 그룹 이름. 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 나열됩니다.

   - **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.
9. 변경사항을 적용하십시오.

   패널의 맨 아래에서 **적용** 단추를 클릭하십시오.
10. 로컬 구성에 대한 변경사항을 저장하십시오.

    메시지 분할창에서 **저장**을 클릭하십시오.
11. 보안 정보가 셀의 노드에 사용되었는지 확인하십시오.

관리 콘솔에서 **시스템 관리**를 펼치고 **노드**를 클릭하십시오. **전체 재동기화**를 클릭하십시오.

12. 필요하면, 서버를 중지한 후 재시작하십시오.

    서버를 재시작해야 하는 경우 관리 콘솔에 적용 메시지가 나타납니다.

결과

그런 다음 유효한 사용자 이름 및 암호를 제공해야 하는 관리 콘솔에 로그인합니다.

사용자가 작성하는 각 프로파일은 이 방법으로 보안을 설정해야 합니다. 시스템 관리자 사용자 ID는 설치 및 환경 구성 중 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

제품 설치 확인
설치 확인 도구를 사용하여 WebSphere Process Server 설치와 독립형 서버 또는 Deployment Manager 프로파일 작성이 성공했는지 확인하십시오. *프로파일*은 Deployment Manager 또는 서버에 대한 런타임 환경을 정의하는 파일로 구성됩니다. installver_wbi 체크섬 도구로 코어 제품 파일을 확인하십시오. IVT(Installation Verification Test) 도구를 사용하여 각각의 프로파일을 확인하십시오.

관리 보안 사용 가능

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

시작하기 전에

이 타스크를 시작하기 전에 WebSphere Process Server를 설치하고 설치를 확인하십시오.

타스크 정보

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

프로시저

1. 관리 콘솔에서 관리 보안 패널을 여십시오.

   보안을 펼치고 **보안 관리, 응용프로그램 및 하부 구조**를 클릭하십시오.

2. 관리 보안을 사용 가능하게 하십시오.

관리 보안 사용을 선택하십시오.

3. 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. 필요한 모든 사용 권한이 없는 응용프로그램에서 AccessControl 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 경고**를 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 제한**을 선택하십시오. 응용프로그램 액세스를 민감한 JCA(Java Connector Architecture) 맵핑 인증 데이터로 제한해야 하는 경우 이 옵션이 사용 가능하도록 설정하십시오.

4. 변경사항을 적용하십시오.

   패널의 맨 아래에서 **적용** 단추를 클릭하십시오.

5. 로컬 구성에 대한 변경사항을 저장하십시오.

   메시지 분할창에서 **저장**을 클릭하십시오.

6. 필요하면, 서버를 중지한 후 재시작하십시오.

   서버를 재시작해야 하는 경우 관리 콘솔에 적용 메시지가 나타납니다.

다음에 수행할 작업

작성하는 프로파일마다 관리 보안을 작동시켜야 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 올바르지 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 상주해야 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 않을 것을 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)
- 공통 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 모두 사용 가능했습니다. 글로벌 보안의 개념은 이제 관리 보안 및 응용프로그램 보안으로 분할되며, 각각의 보안은 별도로 사용 가능하도록 설정할 수 있습니다.

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 특정의 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 대해 준비하지 못할 수도 있습니다. 관리자는 응용프로그램이 Java 2 보안에 대해 준비되지 않은 경우에 Java 2 보안 사용 가능화에 대해 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

Java 2 보안

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.

타스크 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 환경에서 사용자 레지스트리로 LDAP를 사용해야 합니다.

프로시저

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

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

사용자 레지스트리	조치
연합 저장소	단일 범주 아래에 있는 여러 저장소에서 프로파일을 관리하려면 이 설정을 지정하십시오. 범주는 다음에서 ID로 구성될 수 있습니다. • 시스템에 빌드된 파일 기반 저장소 • 하나 이상의 외부 저장소 • 내장된 파일 기반 저장소와 하나 이상의 외부 저장소 **주:** 관리자 특권을 가지고 있는 사용자만 연합 저장소 구성을 볼 수 있습니다. 자세한 정보는 연합 저장소 구성에서 범주 관리를 참조하십시오.
로컬 운영 체제	기본 사용자 레지스트리. **사용 가능한 범주 정의**에서 **로컬 운영 체제**를 선택하고 **구성**을 클릭하십시오. 로컬 OS 사용자 레지스트리 페이지에 사용자 이름과 암호를 제공하십시오. 이 사용자 이름은 서버의 ID로 사용됩니다. 사용자가 자동으로 **관리자** 역할에 추가됩니다. **주:** Network Deployment 환경에서 사용자 레지스트리로 로컬 운영 체제를 사용하지 마십시오.
LDAP(Lightweight Directory Access Protocol)	사용자 레지스트리로 LDAP(Lightweight Directory Access Protocol) 구성의 지시사항에 따라 사용자 레지스트리로 LDAP를 구성하십시오.
사용자 정의 사용자 레지스트리	사용자 정의 계정 저장소를 선택하고 사용자 필요에 맞게 구성하십시오.
Tivoli Access Manager	**주:** 이 옵션은 관리 콘솔을 통해 사용할 수 없으므로, wsadmin 명령을 사용하여 구성해야 합니다.

사용자 계정 저장소 구성

관리 콘솔을 사용하여 사용자 계정 저장소를 구성할 수 있습니다. 서버 사용자 ID를 선택하거나 자동으로 서버 ID를 생성할 수 있습니다.

타스크 정보

관리 콘솔을 사용하여 사용자 계정 저장소를 구성할 수 있습니다. WebSphere Process Server가 자동으로 서버 사용자 ID를 생성하도록 허용할 것을 선택하거나 사용 중인 사용자 계정 저장소에서 지정할 수 있습니다. 후자의 선택을 사용하면 관리 조치의 감사 가능성이 개선됩니다.

프로시저

1. 관리 콘솔에서 사용자 레지스트리에 대한 **사용자 계정 저장소** 구성 페이지를 여십시오.

보안을 펼치고 **보안 관리, 응용프로그램 및 하부 구조**를 클릭한 후 **사용 가능한 범주 정의** 메뉴에서 사용자가 사용하는 사용자 레지스트리를 선택하십시오. **구성**을 클릭하십시오.

2. 옵션: **1차 관리 사용자 이름**을 입력하십시오. 로컬 운영 체제에 정의된 관리 특권을 가지고 있는 사용자의 이름을 지정합니다. 사용자 이름은 관리 보안이 사용 가능한 경우 관리 콘솔에 로그온하는 데 사용됩니다.
3. **자동으로 생성된 서버 ID** 또는 **저장소에 저장된 서버 ID** 옵션을 선택하십시오.

   저장소에 저장된 서버 ID 옵션을 선택한 경우 다음 정보를 입력하십시오.

   - 서버 사용자 ID 또는 관리 사용자
   - 이 사용자에 대해 연관된 암호

   이 ID는 사용자 계정 저장소에 존재해야 합니다.

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.

타스크 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 JACC 프로바이더에 설치된 응용프로그램의 보안 정책 전파를 참조하십시오.

사용자 레지스트리로 LDAP(Lightweight Directory Access Protocol) 구성

기본적으로 사용자 레지스트리는 로컬 운영 체제 레지스트리입니다. 가능하면 사용자 레지스트리로 외부 LDAP(Lightweight Directory Access Protocol)를 사용하십시오. Network Deployment 환경에서 LDAP를 사용해야 합니다.

타스크 정보

이 타스크는 글로벌 보안이 켜져 있다고 가정합니다.

프로시저

1. WebSphere Process Server를 시작하십시오.
2. 관리 콘솔을 실행하십시오.
3. LDAP 사용자 레지스트리 구성 페이지를 여십시오.

보안을 펼치고 **보안 관리, 응용프로그램 및 하부 구조**를 클릭한 후 **사용 가능한 범주 정의** 메뉴에서 **LDAP**를 선택하십시오. **구성**을 클릭하십시오.

4. **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 사용하거나 wsadmin 명령에서 사용됩니다.
5. **적용**을 클릭하십시오.
6. **자동으로 생성된 서버 ID** 또는 **저장소에 저장된 서버 ID** 옵션을 선택하십시오.

   저장소에 저장된 서버 ID 옵션을 선택한 경우 다음 정보를 입력하십시오.
   - 서버 사용자 ID 또는 관리 사용자
   - 이 사용자에 대해 연관된 암호

   이 ID가 LDAP 관리자의 사용자 ID는 아니지만 LDAP에 입력이 있어야 합니다.
7. 사용 중인 LDAP 유형을 선택하십시오.

   유형 목록에서 사용자 레지스트리로 사용할 특정 LDAP을 선택하십시오.
8. LDAP가 상주하는 컴퓨터의 이름을 입력하십시오.

   호스트 필드에 LDAP가 상주하는 서버의 이름을 입력하십시오.
9. LDAP이 청취하는 포트 번호를 입력하십시오.

   포트 필드에 LDAP 서버가 청취하는 포트 번호를 입력하십시오.
10. **기본 식별 이름**을 입력하십시오.

    이 값은 디렉토리 서비스의 기본 식별 이름을 지정하며 이는 디렉토리 서비스의 LDAP 검색에 대한 시작점을 표시합니다.

    권한 목적의 경우, 이 필드는 대소문자를 구분합니다. 이 스펙은 토큰을 수신하는 경우(예: 다른 셀 또는 Domino Server에서) 서버의 기본 식별 이름(DN)이 다른 셀 또는 Domino Server의 기본 DN과 정확히 일치해야 함을 의미합니다. 권한에 대해 대소문자를 구분하지 않아도 될 경우 **대소문자 구분 안함** 필드를 사용 가능하게 하십시오. 이 필드는 Domino 디렉토리를 제외한 모든 LDAP 디렉토리에 필요하며 여기서 이 필드는 선택적입니다.
11. 나머지 매개변수는 기본값으로 두고 변경을 확인하십시오.

    확인을 클릭하십시오.

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 테이블에는 서버 시작 옵션이 설명되어 있습니다.

서버 시작	세부사항
첫 번째 단계 사용자 인터페이스에서	서버 시작을 클릭하십시오.
명령행에서	다음을 입력하십시오. • Windows **Windows 플랫폼:** startserver *servername* • Linux UNIX **Linux 및 UNIX 플랫폼:** startserver.sh *servername* • i5/OS **System i(QShell 명령행에서):** startserver *servername* *install_dir*/bin 디렉토리의 명령 프롬프트에서 입력하십시오.

   주: 서버를 시작하는 데에는 사용자 이름과 암호를 제공하지 않아도 됩니다. 하지만 관리 콘솔을 실행하거나 기타 관리 타스크를 수행하려 시도할 경우에는 인증이 필요합니다.
   서버가 시작되거나 오류 메시지가 리턴됩니다.

2. 서버를 중지하십시오.

   다음 테이블에는 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 이름은 운영자 또는 관리자 역할에 있어야 합니다.

서버 중지	세부사항
명령행에서	다음을 입력하십시오. • Windows **Windows 플랫폼:** stopserver *servername* -profileName *ProfileName* -username *username* -password *password* • Linux UNIX **Linux 및 UNIX 플랫폼:** stopserver.sh *servername* -profileName *ProfileName* -username *username* -password *password* • i5/OS **System i(QShell 명령행에서):** stopserver *servername* -profileName *ProfileName* -username *username* -password *password* *install_dir*/bin 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 테이블에는 서버가 올바로 중지되었는지 확인하는 옵션이 설명되어 있습니다.

서버 중지 확인	세부사항
사용자 인터페이스에서	첫 번째 단계 출력 창에 요청 결과가 자세히 설명됩니다.
명령행에서	요청 결과가 요청이 시작된 명령 창에 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 액세스하도록 이 네 개 역할 중 하나로 사용자가 맵핑되어야 합니다.

설치 후 서버에 로그인하는 첫 번째 사용자가 관리 콘솔에 추가됩니다.

표 6. 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 수정할 수 있습니다(즉, 서버 시작 및 중지).
관리자	관리자 역할은 구성자 역할과 운영자 역할이 조합된 것이며 관리자 역할에만 추가 특권이 부여됩니다. 예는 다음과 같습니다. • 서버 사용자 ID 및 암호 수정 • 관리자 역할에 사용자 및 그룹 맵핑 또한 다음과 같이 민감한 정보에 액세스하는 데 필요한 권한을 갖습니다. • 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 사용자에 대해서만 사용 가능하고 wsadmin 사용자에 대해서는 사용할 수 없습니다. 이 역할이 부여된 사용자는 연합 저장소에서 사용자와 그룹을 관리하기 위한 관리자 특권을 가지고 있습니다. 예를 들어, iscadmins 역할의 사용자는 다음 타스크를 완료할 수 있습니다. • 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 언제라도 관리 역할에 사용자 또는 그룹을 추가하고 반대로 제거할 수도 있습니다. 하지만 변경사항을 적용하는 데 서버 재시작이 필요합니다. 우수 사례는, 보다 유연하고 관리가 쉽기 때문에 특정 사용자보다는 그룹을 관리 역할에 맵핑하는 것입니다. 그룹을 관리 콘솔에 맵핑하면 그룹에 사용자 추가 또는 반대인 제거가 WebSphere Process Server 외부에서 이루어지며 변경사항을 적용하는 데 서버를 재시작할 필요가 없습니다.

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. Everyone 특별 주제는 보안이 사용 가능화되지는 않은 것처럼 인증과 무관하게 아무나 조치 수행이 가능함을 의미합니다.

설치된 구성요소의 기본 보안

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

용도

WebSphere Process Server의 여러 중요 컴포넌트는 메시징 엔진 및 데이터베이스에서의 인증을 위해 사전 정의된 별명을 사용합니다. 프로파일 작성 중 이 인증 별명에는 기본 관리자 사용자 ID 및 암호의 기본값이 제공됩니다. 사용자 계정 저장소에 있는 다른 사용자에 해당되도록 이 별명을 구성해야 합니다.

Business Process Choreographer 인증 별명

비즈니스 프로세스에는 다음과 같은 인증 별명이 있습니다. 이러한 별명은 관리 콘솔에서 수정하십시오.

호출 사용자의 ID와 관계없이 18 페이지의 표 2의 별명을 사용하여 구성요소를 호출합니다.

표 7. 비즈니스 프로세스와 연관된 인증 별명

별명	설명	정보
BPEAuthDataAliasJMS_*node_server*	메시징 엔진을 사용한 인증에 사용됩니다.	프로파일 마법사의 Business Process Choreographer 구성 패널에 사용자 이름 및 암호를 입력하십시오.
BPEAuthDataAlias*DbType_node_server*	데이터베이스를 사용한 인증에 사용됩니다.	제공된 스크립트를 사용하여 데이터베이스를 구성하십시오.

19 페이지의 표 3에는 비즈니스 프로세스에 대해 작성된 RunAs 역할이 설명되어 있습니다.

표 8. 비즈니스 프로세스와 연관된 RunAs 역할

RunAs 역할	**설명**	**정보**
JMSAPIUser	bpecontainer.ear에서 BFM JMS API MDB에 의해 사용됩니다.	프로파일 마법사의 Business Process Choreographer 구성 패널에 사용자 이름 및 암호를 입력하십시오.
EscalationUser	task.ear MDB에 의해 사용됩니다.	프로파일 마법사의 Business Process Choreographer 구성 패널에 사용자 이름 및 암호를 입력하십시오.

제공하는 사용자 이름이 RunAs 역할에 추가됩니다.

CEI(Common Event Infrastructure) 인증 별명

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

호출 사용자의 ID와 관계없이 19 페이지의 표 4의 별명을 사용하여 구성요소를 호출합니다.

표 9. CEI(Common Event Infrastructure)와 연관된 인증 별명

별명	**설명**	**정보**
CommonEventInfrastructure JMSAuthAlias 테이블 셀에 맞춰 사용할 수 있도록 이 항목에 문자 공간이 추가되었습니다. 실제 별명에는 문자 공간이 포함되어 있지 않습니다.	메시징 엔진을 사용한 인증에 사용됩니다.	프로파일 마법사의 CEI(Common Event Infrastructure) 구성 패널에 사용자 이름 및 암호를 입력하십시오.
EventAuthAlias*DBType*	데이터베이스를 사용한 인증에 사용됩니다.	프로파일 마법사의 CEI(Common Event Infrastructure) 구성 패널에 사용자 이름 및 암호를 입력하십시오.

서비스 구성요소 아키텍처 인증 별명

서비스 구성요소 아키텍처(SCA)에 다음의 인증 별명이 있습니다. 이러한 별명은 관리 콘솔에서 수정하십시오.

호출 사용자의 ID와 관계없이 19 페이지의 표 5의 별명을 사용하여 구성요소를 호출합니다.

표 10. SCA 구성요소와 연관된 인증 별명

별명	**설명**	**정보**
SCA_Auth_Alias	메시징 엔진을 사용한 인증에 사용됩니다.	프로파일 마법사의 SCA 구성 패널에 사용자 이름 및 암호를 입력하십시오.

비즈니스 프로세스 및 휴먼 타스크 응용프로그램에서의 액세스 제어

다음의 엔터프라이즈 아카이브(EAR) 파일은 액세스 제어를 통해 Business Process Choreographer 설치의 일부분으로 설치됩니다. Business Process Choreographer는 WebSphere Process Server 설치의 일부로 설치됩니다. 휴먼 타스크 관리자는 이러한 역할을 사용하여 프로덕션 시스템에서 사용자의 역량을 판별합니다.

EAR 파일	역할	기본 권한	Notes
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 타스크에 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

다음의 엔터프라이즈 아카이브(EAR) 파일은 액세스 제어를 통해 CEI(Common Event Infrastructure) 설치의 일부로 설치됩니다. CEI(Common Event Infrastructure)는 WebSphere Process Server 설치의 일부로 설치됩니다.

EventServer.ear 파일은 CEI(Common Event Infrastructure) 설치의 일부분으로 설치된 EAR 파일만 가능합니다.

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

시작하기 전에

응용프로그램 보안에서는 관리 보안이 사용 가능하다고 가정합니다.

타스크 정보

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

다음 타스크를 수행하여 응용프로그램을 보안 설정하십시오.

프로시저

1. 관리 보안이 사용 가능한지 확인하십시오. 세부사항은 8 페이지의 『관리 보안 사용 가능』을 참조하십시오.
2. 응용프로그램 보안이 사용 가능한지 확인하십시오. 관리 콘솔에서 **보안**을 펼치고 **보안 관리, 응용프로그램 및 하부 구조**를 클릭하십시오. 보안 응용프로그램에 액세스하려고 하는 사용자로부터 WebSphere Process Server가 인증을 요구할 수 있도록 **응용프로그램 보안 사용**을 선택하십시오.
3. 해당되는 모든 보안 기능을 사용하여 WebSphere Process Server에서 응용프로그램을 전개하십시오.
4. 사용자 또는 그룹을 해당 보안 역할에 지정하는 WebSphere Process Server 환경으로 응용프로그램을 전개하십시오.
5. WebSphere Process Server 환경의 보안을 유지보수하십시오.

응용프로그램 보안 요소

WebSphere Process Server에서 실행되는 응용프로그램은 인증 및 액세스 제어에 의해 보안이 이루어집니다. 또한 응용프로그램의 호출 동안 전송되는 데이터가 다양한 메커니즘에 의해 보안이 유지되며 이 메커니즘에 따라 데이터를 중간에 읽거나 변경할 수 없습니다. 최종 보안 요소는 사용자가 사용자 이름 및 암호를 반복 입력할 필요가 없도록 다양한 시스템을 통해 보안 정보를 사용하는 것입니다.

WebSphere Process Server의 보안을 세 개의 광역 그룹으로 구분할 수 있습니다.

- 응용프로그램 보안
- 데이터 무결성 및 프라이버시

- ID 사용

응용프로그램 보안

WebSphere Process Server 응용프로그램의 보안은 두 가지 방법으로 유지됩니다.

- **인증** 응용프로그램 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 일부분이 아닌 경우, 응용프로그램이 실행되지 않습니다.

데이터 무결성 및 프라이버시

응용프로그램에서 액세스하는 데이터는 기점, 목적지 및 중간에 보안이 이루어집니다.

- **무결성** 네트워크 상에서 전송된 데이터는 중간에 변경할 수 없습니다.
- **프라이버시/기밀성** 네트워크 상에서 전송된 데이터는 중간에 수집하여 읽을 수 없습니다.

ID 사용

최종 보안 요소는 ID 사용 중 하나입니다.

- **단일 사인온** 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 적용할 수 있도록 하는 데 사용합니다.

인증

관리 보안이 작동되면 클라이언트를 인증해야 합니다.

클라이언트가 인증을 받지 않고 보안 응용프로그램에 액세스하려고 하면 예외가 생성됩니다.

표 11에는 WebSphere Process Server 컴포넌트를 호출하는 전형적인 클라이언트와 각 유형의 클라이언트에 사용 가능한 인증 옵션이 나열되어 있습니다.

표 11. 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 구성요소에는 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 구성요소에는 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.

타스크 정보

관리 콘솔에서 인증 별명을 수정하십시오.

프로시저

1. 비즈니스 통합 인증 별명 패널에 액세스하십시오.

   관리 콘솔에서 **보안**을 펼치고 **비즈니스 통합 인증 별명**을 클릭하십시오.

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

   비즈니스 통합 인증 별명 패널에는 인증 별명 목록, 연관된 컴포넌트, 별명과 연관된 사용자 ID, 선택적으로 별명에 대한 설명이 있습니다. 수정할 별명을 클릭하십시오.또는 편집하려는 인증 별명에 해당되는 **선택** 열에서 선택란을 선택한 후 **편집** 단추를 클릭할 수 있습니다. 인증 별명 구성 패널이 표시됩니다.
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 **적용**을 클릭하십시오. 비즈니스 통합 인증 별명 패널로 돌아가서 **적용**을 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 보강*을 참조하십시오.

관련 태스크

4 페이지의『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.

액세스 제어

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

일반 사용자가 WebSphere Process Server에 대해 인증된 경우 해당 사용자에게 모든 조작을 허용하지 않는 것이 보안 상의 이유로 중요합니다. 일부 사용자가 특정 타스크를 수행하도록 허용하고 이러한 타스크를 다른 사용자에게는 금지하는 것이 액세스 제어입니다.

액세스 제어는 개발하는 구성요소에 맞게 배열하여 보안을 설정할 수 있습니다. 개발 시 서비스 구성요소 아키텍처 규정자를 사용하여 이를 수행합니다. 자세한 정보는 WebSphere Integration Developer Information Center를 참조하십시오.

엔터프라이즈 아카이브(EAR) 파일로 패키지된 일부 WebSphere Process Server 구성요소는 J2EE 역할 기반 보안을 사용하여 조작을 보안합니다. 이러한 구성요소의 세부사항이 제공됩니다. Business Process Choreographer 및 CEI(Common Event Infrastructure)는 WebSphere Process Server의 일부로 설치됩니다. 이러한 구성요소와 연관된 역할 기반 보안은 계속되는 주제에서 자세하게 설명합니다.

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 논의에 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 핸드쉐이크를 사용하여 엔드포인트를 인증하고 암호화 및 해독을 위해 엔드포인트에 사용되는 세션 키를 작성하는 데 사용되는 정보를 교환합니다. SSL은 동기 프로토콜이며 포인트 간 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 핸드쉐이크가 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 상호 작용하는 비즈니스 통합 환경에서는 일부 통신이 비동기 방식으로 이루어집니다. 따라서 대부분의 경우에 WS-Security가 탁월한 솔루션이 됩니다.

관련 정보

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/csec_plan.html

http://publib.boulder.ibm.com/infocenter/dmndhelp/v6r1mx/topic/com.ibm.wbit.610.help.runtime.doc/topics/tusergoal.html

SSL을 사용하도록 웹 서비스 웹 클라이언트 구성:

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

타스크 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 보안에서 찾을 수 있습니다.

단일 사인온

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

클라이언트 요청을 엔터프라이즈 내의 여러 시스템을 통해 전달해야 하는 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 구성요소 개발

개발한 구성요소에 대해 보안을 설정하십시오. 구성요소는 메소드가 있는 인터페이스를 구현합니다. 서비스 구성요소 아키텍처(SCA) 규정자 SecurityPermission을 사용하여 인터페이스 또는 메소드에 보안을 설정하십시오.

시작하기 전에

WebSphere Integration Developer에서 보안 응용프로그램을 개발하십시오. WebSphere Process Server에서 전개할 엔터프라이즈 아카이브(EAR) 파일로 응용프로그램을 내보내십시오.

타스크 정보

다음 단계를 사용하여 WebSphere Process Server에 보안 응용프로그램을 가져오십시오.

프로시저

1. 응용프로그램 EAR 파일을 설치하십시오.

   관리 콘솔에서 **응용프로그램**을 펼치고 **엔터프라이즈 응용프로그램**을 클릭하십시오. **설치**를 클릭하고 새 응용프로그램의 세부사항을 입력하십시오.
2. 새 응용프로그램에 보안 역할을 지정하십시오.

   사용자/그룹에 보안 역할 맵핑을 클릭하십시오. 응용프로그램의 역할에는 네 가지 선택사항이 있습니다.

옵션	설명
모두	이 역할은 보안 없음과 동일합니다.
모두 인증됨	이 역할의 구성원은 유효한 사용자 이름과 암호로 인증된 모든 사용자입니다.

옵션	설명
맵핑된 사용자	개별 사용자는 이 역할의 구성원으로 나열됩니다.
맵핑된 그룹	그룹은 사용자를 추가하는 가장 편리한 방법입니다. 식별된 그룹의 모든 구성원은 이 역할의 구성원이 됩니다.

역할에 맵핑할 수 있는 사용자 및 그룹을 표시하려면 **사용자 찾기** 및 **그룹 찾기**를 사용하십시오.

아래의 샘플 SCDL에서 메소드 **onewayinvoke**에 대한 액세스는 **manager** 역할의 구성원인 사용자로 제한됩니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<scdl:component xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:java="http://www.ibm.com/xmlns/prod/websphere/scdl/java/6.0.0"
xmlns:ns1="http://sample.recovery.security/Itarget"
xmlns:scdl="http://www.ibm.com/xmlns/prod/websphere/scdl/6.0.0"
xmlns:wsdl="http://www.ibm.com/xmlns/prod/websphere/scdl/wsdl/6.0.0"
displayName="secure" name="Component1">
  <interfaces>
    <interface xsi:type="wsdl:WSDLPortType" portType="ns1:Itarget">
      <method name="onewayinvoke">
       <scdl:interfaceQualifier xsi:type="scdl:SecurityPermission"
role="manager"/>
      </method>
      </interface>
  </interfaces>
  <references/>
  <implementation xsi:type="java:JavaImplementation"
class="sca.component.java.impl.Component1Impl1">
 </implementation>
</scdl:component>
```

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 타스크를 수행하기 전에 관련된 모든 보안 구성으로 응용프로그램을 설계, 개발 및 어셈블했는지 확인하십시오. 이러한 타스크에 대한 자세한 정보는 WebSphere Integration Developer Information Center를 참조하십시오. 이 컨텍스트에서 응용프로그램의 전개와 설치는 동일한 타스크로 간주합니다.

타스크 정보

보안 응용프로그램 전개의 필수 단계 중 하나로 응용프로그램 구성 시에 정의된 역할로 사용자 및 그룹을 지정합니다. 이 타스크는 ″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 사용자인 『bob』이고 클라이언트인 『alice』가 위임이 설정된 상태에서 Enterprise Bean을 호출하는 Servlet을 호출할 경우 Enterprise Bean이 『bob』이라는 ID로 호출됩니다. 전개 프로세스의 일부인 한 단계로 사용자를 RunAs 역할에 지정하거나 수정합니다. 이 단계의 제목은 ″사용자로 RunAs 역할 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 동안과 응용프로그램 관리 동안에도 ″사용자 및 그룹에 보안 역할 맵핑″ 링크가 추가 등록 정보 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 데 이 ID 가 다른 ID에 비해 많은 특권을 가지므로 이 ID를 주의하여 사용하십시오. 패널에 나열된 메소드의 시스템 ID 가 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 정보


역할에 사용자 및 그룹 지정


RunAs 역할에 사용자 지정

역할에 사용자 지정

보안 응용프로그램은 securityPermission 및 securityIdenitity인 두 개 규정자 중 하나 또는 둘 모두를 사용합니다. 이 규정자가 있으면 응용프로그램 및 보안 기능이 올바로 작동하도록 전개 시에 추가 단계를 수행해야 합니다.

시작하기 전에

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

타스크 정보

응용프로그램은 메소드가 있는 인터페이스를 구현합니다. 서비스 구성요소 아키텍처(SCA) 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 동안 역할이 ID로 맵핑됩니다. securityIdentity로 보안된 구성요소의 호출에는 응용프로그램을 호출하는 사용자의 ID와 무관하게 지정된 ID가 필요합니다.

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	사용자를 지정된 역할에 지정하십시오. 다음과 같은 네 가지 선택사항이 있습니다. • 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. 사용자가 그룹에 추가되어 서버 재시작 없이도 응용프로그램에 액세스할 수 있기 때문에 가장 유연한 선택은 맵핑된 그룹입니다.
보안 ID	역할이 맵핑되는 ID에 유효한 사용자 이름 및 암호를 제공하십시오.

관련 정보

위임

어댑터 보안

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

타스크 정보

어댑터는 응용프로그램이 엔터프라이즈 정보 시스템(EIS)과 통신하는 데 사용하는 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 교환할 수 있게 하는 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 가능케 합니다.

어댑터 유형 모두에서 WebSphere Process Server에 대한 인바운드 통신의 경우 인증 메커니즘이 없습니다. WebSphere Business Integration Adapter의 경우 JMS 메시징

에 대한 의존으로 보안 컨텍스트 전파가 불가능합니다. J2C에도 인바운드 보안 지원이 없으므로 WebSphere Adapter에도 인바운드 통신을 위한 인증 메커니즘이 없습니다.

어댑터에서 WebSphere Process Server에 입력 시에는 항상 서비스 구성요소 아키텍처(SCA) 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). 구성요소가 실행될 때에는 runAs 역할에 정의된 ID에서 실행됩니다.

SecurityIdentity에 대한 값은 사용자가 아닌, 역할입니다. 그럼에도 불구하고 EAR 파일이 WebSphere Process Server로 전개되면 사용할 ID에 대한 사용자 이름 및 암호를 제공해야 합니다. 다운스트림 구성요소가 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 메시지로써 데이터를 WebSphere Process Server로 전송합니다.

WebSphere Adapter가 WebSphere Process Server의 JVM에 상주하기 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 타스크 및 비즈니스 프로세스 보안

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

휴먼 타스크는 완료하는 데 사람의 개입이 필요합니다. 일부 비즈니스 프로세스에도 사람의 개입이 필요할 수 있습니다. 이러한 휴먼 타스크 및 비즈니스 프로세스는 WebSphere Integration Developer를 사용하여 개발되며 Business Process Choreographer를 사용하여 호출됩니다. 타스크 또는 프로세스를 개발할 때 휴먼 타스크 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 타스크 관리자는 이러한 역할을 사용하여 프로덕션 시스템에서 사용자의 역량을 판별합니다.

휴먼 타스크 및 비즈니스 프로세스와 연관된 역할

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

WebSphere Process Server는 타스크 및 프로세스에 대해 다음의 역할을 지원합니다.

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

독서자 이 역할에 속한 사용자는 타스크 및 프로세스를 표시할 수만 있습니다.

시작자 이 역할에 속한 사용자는 타스크 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

학습서

학습서는 중요한 일부 보안 시나리오를 안내하기 위해 제공됩니다.

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 시나리오 모두는 글로벌 보안이 강화된 것으로 가정합니다.

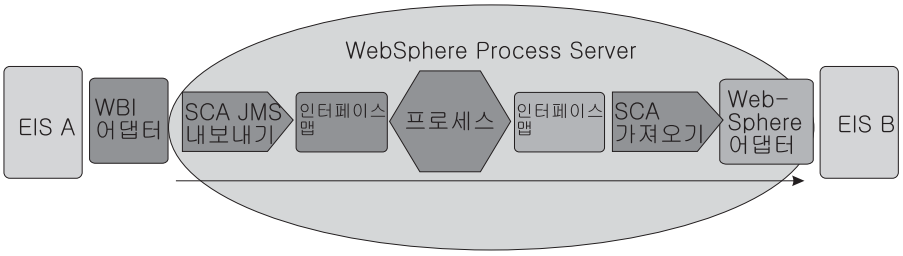
타스크 정보

프로시저

1. 이 섹션에 제공된 예제 중 보안 필요성에 가장 가까운 예제를 판별하십시오. 특정한 경우에는 둘 이상의 예제가 조합된 정보가 시나리오에 포함됩니다.
2. 관련 시나리오의 보안 정보를 읽고 보안 필요성에 적용하십시오.

종래의 통합 시나리오 - 인바운드 및 아웃바운드 어댑터

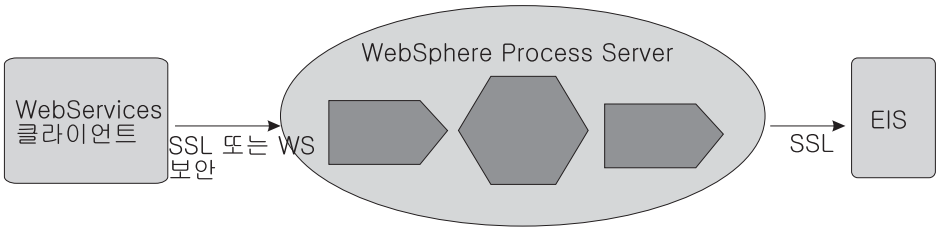
인바운드 요청이 WebSphere Business Integration Adapter에서 나옵니다. 서비스 구성요소 아키텍처(SCA)는 SCA 내보내기를 기반으로 하는 인터페이스 맵을 호출합니다. 요청이 두 번째 인터페이스 맵인 프로세스 컴포넌트를 거친 후 WebSphere Adapter를 통해 두 번째 EIS(B)로 전달됩니다. 이는 하나의 구성요소가 다음 구성요소의 메소드를 호출하는 SCA 호출입니다.



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

WebSphere Process Server로의 인바운드 웹 서비스 요청

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

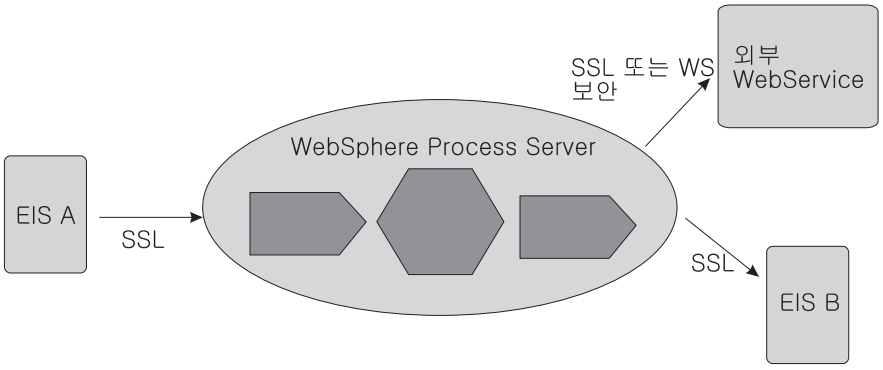


HTTP 기본 인증 또는 WS-Security 인증을 사용하여 웹 서비스 클라이언트를 SSL 클라이언트로 인증할 수 있습니다. 클라이언트가 인증되면 SecurityPermission 규정자에 따라 액세스 제어가 적용됩니다. 클라이언트와 WebSphere Process Server 인스턴스 사이에서 SSL 또는 WS-Security를 사용하여 데이터 무결성 및 프라이버시를 보안시킬

수 있습니다. SSL이 파이프 전체를 보안시키는 반면 WS-Security에서는 SOAP 메시지의 일부를 암호화하거나 디지털로 부호화할 수 있습니다. 웹 서비스의 경우 WS-Security가 우선된 표준입니다.

WebSphere Process Server의 아웃바운드 웹 서비스 요청

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



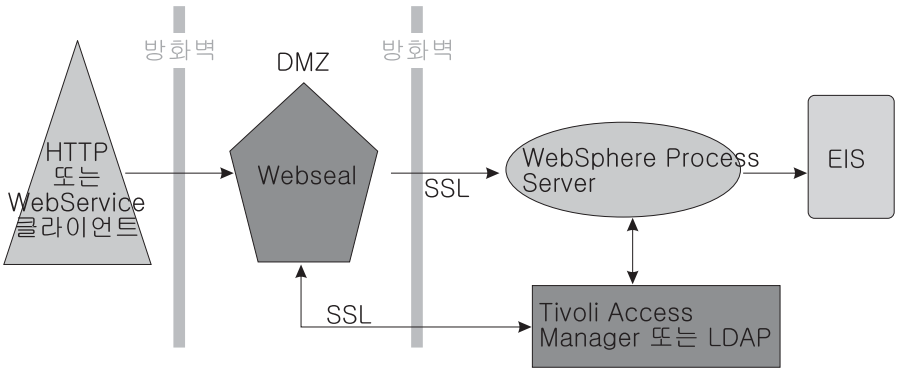
인바운드 웹 서비스 요청의 경우 HTTP 기본 인증 또는 WS-Security 인증을 사용하여 외부 웹 서비스를 SSL 클라이언트로 인증할 수 있습니다. LTPACallBackHandler를 콜백 메커니즘으로 사용하여 현재 RunAs주제에서 usernameToken을 추출하십시오. WebSphere Process Server와 대상 웹 서비스 사이에서 WS-Security를 사용하여 데이터 프라이버시 및 무결성을 보장할 수 있습니다.

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

학습: 보안 역할을 표시하는 Jacl 스크립트 작성

이 학습에서는 JMX MBean에 액세스하여 관리할 수 있는 간단한 Jacl 스크립트를 작성하고 실행하는 방법에 대해 설명합니다. 이 특정 스크립트는 글로벌 보안이 사용 가능할 때 역할 호출과 관련이 있습니다. 이 스크립트를 사용하여 관계에서 각 역할에 대한 역할 이름을 인쇄할 수 있습니다.

이 학습의 목표

이 학습을 완료한 후에는 다음이 가능합니다.

- 모든 관계 목록을 요청하는 JMX MBean을 호출하는 Jacl 스크립트를 작성하십시오.

스크립트 작성에 대한 자세한 정보는 WebSphere Application Server Network Deployment, 버전 6 Information Center에서 "스크립팅 사용(wsadmin)"을 참조하십시오.

이 학습을 완료하는 데 필요한 시간

이 학습은 완료하는 데 약 15 - 30분이 필요합니다.

전제조건

이 학습에서는 JMX 보안 샘플에 포함된 스크립트를 사용합니다. 이 샘플은 역할 관계 목록을 인쇄하는 MBean 기능을 보여 줍니다.

주: 이 스크립트를 사용하려면 WebSphere Process Server 설치 중 코드 샘플을 설치하는 옵션을 선택해야 합니다.

샘플 Jacl 스크립트는 *install_root*/samples/JMXSample/scripts 및 *install_root*₩samples₩JMXSample₩scripts에 있습니다. 스크립트의 이름은 `RelServicesAdmin.jacl`입니다.

스크립트를 실행하려면 다음을 입력하십시오. UNIX Linux

```
wsadmin -f install_root/samples/JMXSample/scripts/RelServicesAdmin.jacl
 -server servername -node nodename
```

스크립트를 실행하려면 다음을 입력하십시오. Windows

```
wsadmin -f install_root¥samples¥JMXSample¥scripts¥RelServicesAdmin.jacl
 -server servername -node nodename
```

이 스크립트는 환경에서 최대 10개의 관계를 호출하며 각 관계에 대해 최대 10개의 역할이 콘솔에 인쇄됩니다.

연습: Jacl 스크립트 작성

타스크 정보

이 스크립트의 기본 개념은 시스템에서 MBean과 통신하는 데 사용할 수 있습니다. 필요한 것은 MBean의 이름 및 유형과 MBean에서 사용 가능한 메소드 및 속성 뿐입니다. getAttribute 및 setAttribute 명령이 속성으로 사용됩니다. invoke 명령은 메소드로 사용됩니다. 다음 단계를 수행하여 JMX 보안 MBean을 관리하는 .jacl 스크립트를 작성하십시오.

주: 각 단계의 코드는 코드의 수행 내용을 설명하는 지시문으로 시작됩니다.

프로시저

1. **nodename**을 판별하십시오.

   아래에 표시된 스크립트의 첫 번째 부분에서 nodename을 판별할 수 있습니다. nodeName이 올바로 지정되지 않은 경우 올바른 구문이 인쇄되고 스크립트가 종료됩니다.

   ```
   # read and validate arguments

       if {{$argc == 1 } && { [lindex $argv $i] == "-nodeName" } {
              set nodeName [lindex $argv $i]
   ```

2. **MBean**을 식별하십시오.

   MBean은 유형 및 이름으로 식별됩니다.

   주: 사용할 특정 MBean을 알고 있으므로 이 경우 이름과 유형은 하드 코드화됩니다.

   스크립트의 두 번째 부분은 MBean을 나타냅니다.

   ```
   # these two variables, mbeanName and mbeanType are used
     to uniquely identify the mbean.
         # for this sample, the mbean that access relationship
           services will be used.

         set mbeanName"RelService"
         set mbeanType"WBIRelServices"
   ```

3. **reference**를 찾아서 MBean으로 설정하십시오.

   여기에 표시된 코드를 사용하여 MBean의 참조를 설정하십시오.

   ```
   # locate the mbean and set a reference to it in "relSvcsMBean" variable

         set relSvcsMBean [$AdminControl queryNames
             name=$mbeanName,node=$nodeName,type=$mbeanType,*]
   ```

4. getAttribute 명령을 사용하여 **relationship**을 호출하십시오.

   이 특정 MBean의 문서는 `allRelationshipNames`라고 하는 속성을 정의합니다. getAttribute 명령을 사용하여 MBean에 이 속성을 요청하십시오. 속성 값은 명령을 호출하는 다음 단계에서 통과하는 목록입니다.

   ```
   # request the list of relationships from the mbean

         set relationships
          [$AdminControl getAttribute $relSvcsMBean allRelationshipNames]
   ```

5. 각 관계 이름의 **command**를 호출하고 이름을 인쇄한 후에 추가 정보를 얻으려면 MBean으로 돌아가십시오.

   이 예에서 MBean은 특정 관계 이름에 대해 단일 매개변수를 사용하여 getAllRoleNames 메소드를 정의합니다. invoke 명령을 사용하여 이 메소드를 호출하며 현재 관계 이름을 전달합니다. 관계의 각 역할에 대한 역할 이름이 인쇄됩니다.

   ```
   # loop through the list of role names and print name

         foreach roleName $roles {
           puts "    Role: $roleName"
         }
       }
           } else {
         # arguments were not correct, print correct syntax
            puts "Usage: wsadmin -f RelServicesAdmin.jacl -nodeName nodeName"
    }
   ```

결과

이제 관계를 호출하는 스크립트를 작성했습니다.

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. IBM 제품, 프로그램 또는 서비스에 대한 모든 언급은 IBM 제품, 프로그램 또는 서비스를 사용할 수 있음을 의미하거나 암시하지 않습니다. IBM의 지적 재산권을 침해하지 않는 한, 기능상으로 동등한 모든 제품, 프로그램 또는 서비스를 대신 사용할 수도 있습니다. 그러나 비IBM 제품, 프로그램 또는 서비스의 작동을 평가 및 검증은 사용자의 책임입니다.

IBM이 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 106-0032, 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 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, 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 얻고자 하는 라이센스 사용자는 다음 주소로 문의해야 합니다.

135-270
서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
한국 아이.비.엠 주식회사
고객만족센터

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

이 정보에 기술된 라이센스가 부여된 프로그램 및 이 프로그램에 대해 사용 가능한 모든 라이센스가 부여된 자료는 IBM이 IBM 기본 계약, IBM 프로그램 라이센스 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 라이센스:

이 정보에는 여러 가지 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 추가 비용 없이 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. (c) (회사명) (연도). 이 코드의 일부는 IBM Corp. 의 샘플 프로그램에서 파생됩니다. (c) Copyright IBM Corp. 연도_. 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 프로그래밍 인터페이스로서 사용될 수 없습니다.

상표 및 서비스표

IBM, IBM 로고, Domino, Tivoli, WebSphere 및 z/OS는 미국 또는 기타 국가에서 사용되는 IBM Corporation의 등록상표입니다.

Java 및 모든 Java 기반 상표는 미국 또는 기타 국가에서 사용되는 Sun Microsystems, Inc.의 상표입니다.

Windows는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 등록상표입니다.

UNIX는 미국 또는 기타 국가에서 사용되는 The Open Group의 등록상표입니다.

Linux는 미국 또는 기타 국가에서 사용되는 Linus Torvalds의 등록상표입니다.

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

본 제품에는 Eclipse 프로젝트에서 개발한 소프트웨어가 포함되어 있습니다. (http://www.eclipse.org 웹 사이트 참조)

IBM WebSphere Process Server for Multiplatforms, 버전 6.1.0