WebSphere® 멀티플랫폼용

IBM WebSphere Process Server

버전 7.0.0

응용프로그램 및 해당 환경 보안

IBM®

WebSphere® 멀티플랫폼용

IBM WebSphere Process Server

버전 7.0.0

응용프로그램 및 해당 환경 보안

IBM®

2010년 4월

이 개정판은 새 개정판에 별도로 명시하지 않는 한, 멀티플랫폼용 WebSphere Process Server의 버전 7, 릴리스 0, 수정 0(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.

목차

WebSphere Process Server 및 응용프로그램 보안

WebSphere® Process Server 및 응용프로그램 보안은 런타임 환경 보안 및 응용프로그램 보안에 따라 다릅니다.

WebSphere Process Server 런타임 환경 보안에는 관리 보안 사용, 응용프로그램 보안 사용, 보안을 사용한 프로파일 작성 및 선택한 사용자에 대해 중요 기능으로의 액세스 제한이 포함됩니다.

응용프로그램 보안에는 사용자 인증, 조작 및 자원에 대한 액세스 제어 구현, 데이터 무결성 및 개인 정보 보호 제공이 포함됩니다.

WebSphere Process Server 보안은 WebSphere Application Server 버전 7.0 보안을 기반으로 합니다. 이러한 문서는 WebSphere Application Server Information Center에 있는 핵심 보안 문서의 보충 정보입니다(특히 『응용프로그램 및 환경 보안』의 주제).

보안의 일반 개요

WebSphere Process Server 보안은 WebSphere Application Server 버전 7.0 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 나누어질 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 다운스트림 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 관계자가 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.

WebSphere Process Server에 특정한 보안 고려사항

WebSphere Process Server 보안이 WebSphere Application Server 7.0 보안에 빌드됩니다. WebSphere Process Server에 특정한 고려사항이 표시됩니다.

- 관리 콘솔 페이지 비즈니스 통합 보안은 WebSphere Process Server에 고유합니다. **보안**을 펼치고 **비즈니스 통합 보안**을 클릭하여 이 페이지를 표시합니다.

  이 페이지를 사용하면 사용자는 사용자 레지스트리의 특정 ID를 중요한 비즈니스 통합 인증에 지정할 수 있습니다. 또한 이 페이지에서 Business Process Choreographer Security 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 타스크의 개요를 제공합니다.

1. WebSphere Process Server를 설치할 때 보안을 고려하십시오.
   a. 설치 전에 환경의 보안을 설정하십시오.
   b. WebSphere Process Server 설치를 위한 운영 체제를 준비하십시오.
   c. 설치 후 환경을 준비하십시오.
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 역할 위젯을 사용하여 비즈니스 달력 위젯에 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.

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 시 보안 준비** 주제를 참조하십시오.

2. WebSphere Process Server 설치를 위한 운영 체제를 준비하십시오.

   Windows Linux UNIX 이 단계에는 WebSphere Process Server의 설치를 위해 서로 다른 운영 체제를 준비하는 방법 관련 정보가 포함되어 있습니다. 설치를 위한 운영 체제 준비에 대한 자세한 정보는 WebSphere Application Server Information Center의 **제품 설치에 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.

설치 시 제공되는 인증 정보

설치 동안 모든 컴포넌트의 기본값은 사용자가 제공하는 1차 관리 신임입니다. 이러한 기본값은 기본 보안을 제공하지만 설치의 보안을 더 확고하게 하려면 다양한 WebSphere Process Server 컴포넌트를 구성해서 적절한 보안 ID를 가져야 합니다.

WebSphere Process Server 프로파일을 작성하고 **관리 보안 사용**을 선택한 경우 사용자 이름에 대해 프롬프트됩니다. 이 ID는 모든 기본 컴포넌트의 기본값으로 사용됩니다. 보안을 더 강화하려면 프로파일 작성 후 이 ID를 구성해야 합니다.

WebSphere Process Server의 여러 컴포넌트는 인증 별명을 사용합니다. 이 별명은 데이터베이스 및 메시징 엔진에 액세스하기 위해 런타임 컴포넌트를 인증하는 데 사용됩니다. 이러한 별명은 관리 콘솔의 BIS(Business Integration Security) 페이지에서 수정될 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
- 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 페이지를 표시하십시오. **보안**을 펼치고 **비즈니스 통합 보안**을 클릭하십시오.
2. Service Component Architecture, Business Process Choreographer 및 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 **편집**을 클릭합니다.
   b. 다음 페이지에서 이 컴포넌트의 인증 별명으로 사용할 사용자 이름 및 암호를 제공하십시오.

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

c. **확인**을 클릭하십시오.

독립형 서버에 대한 WebSphere Process Server 보안 구성

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

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.

이 태스크 정보

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. 『보안 사용 가능』.
2. 응용프로그램 보안이 작동하는지 확인하십시오. 『보안 사용 가능』.
3. 사용하려는 사용자 계정 저장소를 선택하십시오. 8 페이지의 『사용자 계정 저장소 구성』

   선택한 레지스트리를 **현재로 설정**을 사용하여 현재 레지스트리로 설정했는지 확인하십시오.
4. 관리 역할에 사용자나 그룹을 추가하십시오.
5. 필요하면 서버를 중지한 후 다시 시작하십시오. 14 페이지의 『서버 시작 및 중지』
6. 설치된 컴포넌트에 대한 기타 보안 메커니즘, 액세스 제어 및 인증 별명을 설정하십시오. 31 페이지의 『WebSphere Process Server에서 응용프로그램 보안』

보안 사용 가능

WebSphere Process Server 환경 및 응용프로그램 보안의 첫 번째 단계는 관리 보안이 사용 가능한지 확인하는 것입니다.

시작하기 전에

이 타스크를 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 콘솔을 사용하여 관리 보안, 응용프로그램 보안 및 Java 2 보안을 사용할 수 있습니다.

- *관리 보안*은 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 보안 구성은 보안 도메인 내의 모든 서버에 적용됩니다.
- *응용프로그램 보안*은 환경에서 응용프로그램에 대해 보안을 사용할 수 있도록 합니다. 이 유형의 보안은 응용프로그램 사용자를 인증하기 위한 요구사항과 응용프로그램 분리를 제공합니다.

  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*은 보호 설정된 특정 시스템 자원에 액세스를 허용하기 전에 사용 권한을 확인해서 전반적인 시스템 무결성을 증가시키는 정책 기반의 세밀한 액세스 제어 메커니즘을 제공합니다. Java 2 보안은 파일 I/O, 소켓 및 특성과 같은 시스템 자원에 대한 액세스를 보호합니다. 보안은 서블릿, JSP(JavaServer Page) 파일 및 EJB(Enterprise JavaBeans™) 메소드와 같은 웹 자원에 대한 액세스를 보호합니다.

  Java 2 보안이 상대적으로 새로운 보안이기 때문에 많은 기존 응용프로그램이나 새 응용프로그램 조차도 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.

  경고: SDK(Software Development Kit)에 대한 갱신사항이 포함된 픽스팩은 제한되지 않은 정책 파일을 겹쳐씁니다. 픽스팩을 적용하기 전에 제한되지 않은 정책 파일을 백업하고 픽스팩을 적용한 후 이 파일을 다시 적용하십시오.

프로시저

1. 관리 콘솔에서 관리 보안 페이지를 여십시오.

   보안을 펼치고 **글로벌 보안**을 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 예외가 생성됩니다. Java 2 보안에 대한 자세한 정보는 WebSphere Application Server Information Center에서 Java 2 보안 정책 파일 구성에 대한 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 1.4 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.

5. 변경사항을 적용하십시오.

   페이지의 맨 아래에서 **적용** 단추를 클릭하십시오.

6. 로컬 구성에 대한 변경사항을 저장하십시오.

   메시지 분할창에서 **저장**을 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.

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 Network Deployment 환경에서는 사용자 레지스트리로 LDAP을 사용해야 합니다.

프로시저

1. 관리 콘솔에서 관리, 응용프로그램 및 인프라 보안 패널을 탐색하십시오. **보안**을 펼치고 **글로벌 보안**을 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	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	이는 기본 사용자 레지스트리입니다. **주:** Windows Linux UNIX Network Deployment 환경에서 사용자 레지스트리로 로컬 운영 체제를 사용하지 마십시오. 9 페이지의 『로컬 운영 체제 또는 독립형 사용자 정의 사용자 계정 저장소 구성』의 지시사항을 따르십시오.

사용자 레지스트리	조치
LDAP(Lightweight Directory Access Protocol)	10 페이지의 『사용자 레지스트리로 LDAP(Lightweight Directory Access Protocol) 구성』의 지시사항을 준수해서 LDAP를 사용자 레지스트리로 구성하십시오.
사용자 정의 사용자 레지스트리	『로컬 운영 체제 또는 독립형 사용자 정의 사용자 계정 저장소 구성』의 지시사항을 따라 사용자 정의 계정 저장소를 선택하고 사용자 필요에 맞게 구성하십시오.
Tivoli® Access Manager	**주:** 이 옵션은 관리 콘솔을 통해 사용할 수 없습니다. wsadmin 명령을 사용하여 구성해야 합니다.

로컬 운영 체제 또는 독립형 사용자 정의 사용자 계정 저장소 구성

관리 콘솔을 사용하여 사용자 계정 저장소를 구성할 수 있습니다. 로컬 운영 체제(기본값임) 또는 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 **글로벌 보안**을 클릭한 후 **사용 가능한 범주 정의** 메뉴 아래에서 사용자가 사용하는 사용자 레지스트리를 선택하십시오. **구성**을 클릭하십시오.
2. 옵션: **1차 관리 사용자 이름** 필드에 유효한 사용자 이름을 입력하십시오.

   이 값은 레지스트리에 정의된 관리 권한을 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 ID**를 선택하면 Application Server에서는 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 → 글로벌 보안 → 인증 메커니즘 및 만기**를 클릭하십시오. **내부 서버 ID** 필드의 값을 변경하십시오.
   - **저장소에 저장된 서버 ID** 옵션을 선택한 경우 다음 정보를 입력하십시오.
     - **버전 7.0 노드의 관리 사용자 또는 서버 사용자 ID**의 경우 보안을 위해 Application Server를 실행하는 데 사용되는 사용자 ID를 지정하십시오.

– **암호**에 대해 이 사용자와 연관된 암호를 지정하십시오.

4. 옵션: 독립형 사용자 정의 레지스트리의 경우에만 다음 단계를 수행하십시오.
   a. **사용자 정의 레지스트리 클래스 이름**에 있는 값이 올바른지 확인하여 필요한 경우 변경하십시오.
   b. **인증 시 대소문자 구분 안 함**에서 체크를 선택하거나 제거하십시오.

      이 옵션을 선택하면 권한 검사 시 대소문자를 구분하지 않습니다.
5. **적용**을 클릭하십시오.
6. 페이지 맨 아래에서 **현재로 설정**을 클릭하십시오.
7. **확인**을 클릭한 후 **적용** 또는 **저장**을 클릭하십시오.

다음에 수행할 작업

갱신사항이 적용되도록 모든 서버를 저장하고 중지한 후 다시 시작하십시오.

아무 문제 없이 서버가 시작되면 올바르게 설정된 것입니다.

사용자 계정 저장소로 Tivoli Access Manager를 사용하도록 WebSphere Process Server 구성

Tivoli Access Manager를 사용자 계정 저장소로 사용할 수 있습니다. 그러나 관리 콘솔 외부에서 wsadmin 명령을 사용하여 이를 구성해야 합니다.

이 태스크 정보

Tivoli Access Manager는 사용자 계정 저장소로 사용할 수 있습니다. 관리 콘솔에서는 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 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. **보안**을 펼치고 **글로벌 보안**을 클릭하십시오.
3. 관리, 응용프로그램 및 인프라 보안 페이지에서 다음 단계를 수행하십시오.
   a. **관리 보안 사용**이 선택되어 있는지 확인하십시오.
   b. **사용 가능한 범주 정의** 목록에서 **독립형 LDAP 레지스트리**를 선택하십시오.
   c. **구성**을 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 권한을 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 ID**를 선택하면 Application Server에서는 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 → 글로벌 보안 → 인증 메커니즘 및 만기**를 클릭하십시오. **내부 서버 ID** 필드의 값을 변경하십시오.
      - **저장소에 저장된 서버 ID** 옵션을 선택한 경우 다음 정보를 입력하십시오.
        – **버전 7.0 노드의 관리 사용자 또는 서버 사용자 ID**의 경우 보안을 위해 Application Server를 실행하는 데 사용되는 사용자 ID를 지정하십시오.
        – **암호**에 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 정의**로 변경하며 이는 사용자 정의 필터가 사용됨을 표시합니다. 이 조치는 고급 LDAP 설정 페이지에서 **확인** 또는 **적용**을 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 Server**를 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 사인온 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=US`인 사용자의 경우 기본 DN을 다음 옵션 중 하나로 지정하십시오(접미부가 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 함**을 사용 가능으로 설정하십시오.

WebSphere Process Server에서 식별 이름은 LDAP(Lightweight Directory Access Protocol) 스펙에 따라 정규화됩니다. 정규화는 기본 식별 이름에서 쉼

표 및 등호 앞뒤의 공백을 제거하여 수행됩니다. 비정규 기본 식별 이름의 예로는 `o = ibm, c = us` 또는 `o=ibm, c=us`가 있습니다. 정규화된 기본 식별 이름의 예로는 `o=ibm,c=us`가 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 Application Server는 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 재사용**이 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 함**이 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 컨텐츠가 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 함**을 사용 가능으로 설정할 수 있습니다.

기본값을 사용할 수 있습니다.

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

SSL 사용 가능 옵션을 선택하면 **중앙에서 관리** 또는 **특정 SSL 별명 사용**을 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. **확인**을 클릭한 후 관리, 응용프로그램 및 인프라 페이지로 돌아갈 때까지 **적용** 또는 **저장**을 클릭하십시오.

5. 관리, 응용프로그램 및 인프라 보안 페이지에서 **현재로 설정**을 클릭하십시오.
6. **확인**을 클릭한 후 **적용** 또는 **저장**을 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.

문제점 피하기: Vista Windows 7 일부 레벨에서 사용자 계정 제어(UAC)가 사용되는 경우, 명령 프롬프트를 사용하려면 관리자 특권으로 Application Server를 시작해야 합니다. 다음 조치를 수행하여 실행되는 명령 프롬프트 창에서 Application Server를 시작하십시오.

- 명령 프롬프트 바로 가기를 마우스 오른쪽 단추로 클릭하십시오.
- **관리자로 실행**을 클릭하십시오.
- 명령 프롬프트 창을 관리자로 여는 경우, 계속할 것인지 묻는 운영 체제 대화 상자가 나타납니다. **계속**을 클릭하여 계속하십시오.

프로시저

1. 서버를 시작하십시오.

   다음 표에는 서버 시작 옵션이 설명되어 있습니다.

서버 시작	세부사항
첫 번째 단계 사용자 인터페이스에서	**서버 시작**을 클릭하십시오.
명령행에서	다음을 입력하십시오. • Windows **Windows® 플랫폼:** `startserver servername` • Linux UNIX **Linux® 및 UNIX® 플랫폼:** `startserver.sh servername`

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

   서버가 시작되거나 하나의 오류 메시지가 리턴됩니다.

2. 서버를 중지하십시오.

   다음 표에는 서버 중지 옵션이 설명되어 있습니다.

서버 중지	세부사항
첫 번째 단계 사용자 인터페이스에서	**서버 중지**를 클릭하고 프롬프트가 표시되면 유효한 사용자 이름과 암호를 제공하십시오. 제공하는 사용자 이름에 운영자 또는 관리자 역할이 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`

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 올바로 중지되었는지 확인하는 옵션이 설명되어 있습니다.

서버가 중지되었는지 확인하십시오.	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 제공된 8개의 역할이 있습니다. 이 역할은 관리 콘솔의 기능 범위에 권한을 부여합니다. 관리 보안이 사용 가능한 경우 사용자는 관리 콘솔에 액세스하기 위해 이러한 역할 중 하나에 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 수정(즉, 서버 시작 및 중지)할 수 있습니다.

표 1. 관리 보안 역할 (계속)

관리 보안 역할	설명
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 관리자는 다음과 같이 민감한 정보에 액세스하는 데 필요한 권한을 갖습니다. • LTPA(Lightweight Third Party Authentication) 암호 • 키
ISC Admins	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, ISC Admins 역할의 사용자는 다음 타스크를 완료할 수 있습니다. • 연합 저장소 구성에서 사용자 작성, 갱신 또는 삭제 • 연합 저장소 구성에서 그룹 작성, 갱신 또는 삭제
전개자	이 역할이 부여된 사용자만 응용프로그램에 대해 구성 조치 및 런타임 조작 둘 다를 수행할 수 있습니다.
관리 보안 관리자	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.
감사	이 역할이 부여된 사용자는 보안 감사 서브시스템에 대한 구성 설정값을 보고 수정할 수 있습니다. **주:** 감사 역할에는 모니터 역할이 포함됩니다. 이는 감사가 볼 수 있지만 나머지 보안 구성을 변경할 수 없도록 합니다.

자세한 정보는 WebSphere Application Server Information Center의 관리 역할을 참조하십시오.

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 적용하려면 서버를 다시 시작해야 합니다.

팁: 더 유연하고 관리가 쉽기 때문에 특정 사용자보다 그룹을 관리 역할로 맵핑하십시오. 그룹을 관리 콘솔에 맵핑하면 그룹에 사용자 추가 또는 반대인 제거가 WebSphere Process Server 외부에서 이루어지며 변경사항을 적용하는 데 서버를 다시 시작할 필요가 없습니다.

실패 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.

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 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.

이 태스크 정보

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. 5 페이지의 『보안 사용 가능』.
2. 응용프로그램 보안이 작동하는지 확인하십시오. 5 페이지의 『보안 사용 가능』.
3. 사용하려는 사용자 계정 저장소를 선택하십시오. 8 페이지의 『사용자 계정 저장소 구성』

   선택한 레지스트리를 **현재로 설정**을 사용하여 현재 레지스트리로 설정했는지 확인하십시오.
4. 관리 역할에 사용자나 그룹을 추가하십시오.
5. 필요하면 서버를 중지한 후 다시 시작하십시오. 14 페이지의 『서버 시작 및 중지』

6. 설치된 컴포넌트에 대한 기타 보안 메커니즘, 액세스 제어 및 인증 별명을 설정하십시오. 31 페이지의『WebSphere Process Server에서 응용프로그램 보안』

보안 사용 가능

WebSphere Process Server 환경 및 응용프로그램 보안의 첫 번째 단계는 관리 보안이 사용 가능한지 확인하는 것입니다.

시작하기 전에

이 타스크를 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 콘솔을 사용하여 관리 보안, 응용프로그램 보안 및 Java 2 보안을 사용할 수 있습니다.

- *관리 보안*은 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 보안 구성은 보안 도메인 내의 모든 서버에 적용됩니다.
- *응용프로그램 보안*은 환경에서 응용프로그램에 대해 보안을 사용할 수 있도록 합니다. 이 유형의 보안은 응용프로그램 사용자를 인증하기 위한 요구사항과 응용프로그램 분리를 제공합니다.

  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*은 보호 설정된 특정 시스템 자원에 액세스를 허용하기 전에 사용 권한을 확인해서 전반적인 시스템 무결성을 증가시키는 정책 기반의 세밀한 액세스 제어 메커니즘을 제공합니다. Java 2 보안은 파일 I/O, 소켓 및 특성과 같은 시스템 자원

에 대한 액세스를 보호합니다. 보안은 서블릿, JSP(JavaServer Page) 파일 및 EJB(Enterprise JavaBeans) 메소드와 같은 웹 자원에 대한 액세스를 보호합니다.

Java 2 보안이 상대적으로 새로운 보안이기 때문에 많은 기존 응용프로그램이나 새 응용프로그램 조차도 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.

경고: SDK(Software Development Kit)에 대한 갱신사항이 포함된 픽스팩은 제한되지 않은 정책 파일을 겹쳐씁니다. 픽스팩을 적용하기 전에 제한되지 않은 정책 파일을 백업하고 픽스팩을 적용한 후 이 파일을 다시 적용하십시오.

프로시저

1. 관리 콘솔에서 관리 보안 페이지를 여십시오.

   보안을 펼치고 **글로벌 보안**을 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 예외가 생성됩니다. Java 2 보안에 대한 자세한 정보는 WebSphere Application Server Information Center에서 Java 2 보안 정책 파일 구성에 대한 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 1.4 스펙에 따라 가지고 있

어야 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.

5. 변경사항을 적용하십시오.

   페이지의 맨 아래에서 **적용** 단추를 클릭하십시오.

6. 로컬 구성에 대한 변경사항을 저장하십시오.

   메시지 분할창에서 **저장**을 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.

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 Network Deployment 환경에서는 사용자 레지스트리로 LDAP을 사용해야 합니다.

프로시저

1. 관리 콘솔에서 관리, 응용프로그램 및 인프라 보안 패널을 탐색하십시오. **보안**을 펼치고 **글로벌 보안**을 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	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	이는 기본 사용자 레지스트리입니다. **주:** Windows Linux UNIX Network Deployment 환경에서 사용자 레지스트리로 로컬 운영 체제를 사용하지 마십시오. 9 페이지의 『로컬 운영 체제 또는 독립형 사용자 정의 사용자 계정 저장소 구성』의 지시사항을 따르십시오.
LDAP(Lightweight Directory Access Protocol)	10 페이지의 『사용자 레지스트리로 LDAP(Lightweight Directory Access Protocol) 구성』의 지시사항을 준수해서 LDAP를 사용자 레지스트리로 구성하십시오.
사용자 정의 사용자 레지스트리	9 페이지의 『로컬 운영 체제 또는 독립형 사용자 정의 사용자 계정 저장소 구성』의 지시사항을 따라 사용자 정의 계정 저장소를 선택하고 사용자 필요에 맞게 구성하십시오.
Tivoli Access Manager	**주:** 이 옵션은 관리 콘솔을 통해 사용할 수 없습니다. wsadmin 명령을 사용하여 구성해야 합니다.

로컬 운영 체제 또는 독립형 사용자 정의 사용자 계정 저장소 구성

관리 콘솔을 사용하여 사용자 계정 저장소를 구성할 수 있습니다. 로컬 운영 체제(기본값임) 또는 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 **글로벌 보안**을 클릭한 후 **사용 가능한 범주 정의** 메뉴 아래에서 사용자가 사용하는 사용자 레지스트리를 선택하십시오. **구성**을 클릭하십시오.

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

   이 값은 레지스트리에 정의된 관리 권한을 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 ID**를 선택하면 Application Server에서는 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 → 글로벌 보안 → 인증 메커니즘 및 만기**를 클릭하십시오. **내부 서버 ID** 필드의 값을 변경하십시오.
   - **저장소에 저장된 서버 ID** 옵션을 선택한 경우 다음 정보를 입력하십시오.
     - **버전 7.0 노드의 관리 사용자 또는 서버 사용자 ID**의 경우 보안을 위해 Application Server를 실행하는 데 사용되는 사용자 ID를 지정하십시오.
     - **암호**에 대해 이 사용자와 연관된 암호를 지정하십시오.
4. 옵션: 독립형 사용자 정의 레지스트리의 경우에만 다음 단계를 수행하십시오.
   a. **사용자 정의 레지스트리 클래스 이름**에 있는 값이 올바른지 확인하여 필요한 경우 변경하십시오.
   b. **인증 시 대소문자 구분 안 함**에서 체크를 선택하거나 제거하십시오.

      이 옵션을 선택하면 권한 검사 시 대소문자를 구분하지 않습니다.
5. **적용**을 클릭하십시오.
6. 페이지 맨 아래에서 **현재로 설정**을 클릭하십시오.
7. **확인**을 클릭한 후 **적용** 또는 **저장**을 클릭하십시오.

다음에 수행할 작업

갱신사항이 적용되도록 모든 서버를 저장하고 중지한 후 다시 시작하십시오.

아무 문제 없이 서버가 시작되면 올바르게 설정된 것입니다.

사용자 계정 저장소로 Tivoli Access Manager를 사용하도록 WebSphere Process Server 구성

Tivoli Access Manager를 사용자 계정 저장소로 사용할 수 있습니다. 그러나 관리 콘솔 외부에서 wsadmin 명령을 사용하여 이를 구성해야 합니다.

이 태스크 정보

Tivoli Access Manager는 사용자 계정 저장소로 사용할 수 있습니다. 관리 콘솔에서는 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 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. **보안**을 펼치고 **글로벌 보안**을 클릭하십시오.
3. 관리, 응용프로그램 및 인프라 보안 페이지에서 다음 단계를 수행하십시오.
   a. **관리 보안 사용**이 선택되어 있는지 확인하십시오.
   b. **사용 가능한 범주 정의** 목록에서 **독립형 LDAP 레지스트리**를 선택하십시오.
   c. **구성**을 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 권한을 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 ID**를 선택하면 Application Server에서는 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 → 글로벌 보안 → 인증 메커니즘 및 만기**를 클릭하십시오. **내부 서버 ID** 필드의 값을 변경하십시오.

   - **저장소에 저장된 서버 ID** 옵션을 선택한 경우 다음 정보를 입력하십시오.
     - **버전 7.0 노드의 관리 사용자 또는 서버 사용자 ID**의 경우 보안을 위해 Application Server를 실행하는 데 사용되는 사용자 ID를 지정하십시오.
     - **암호**에 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 정의**로 변경하며 이는 사용자 정의 필터가 사용됨을 표시합니다. 이 조치는 고급 LDAP 설정 페이지에서 **확인** 또는 **적용**을 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 Server**를 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 사인온 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=US`인 사용자의 경우 기본 DN을 다음 옵션 중 하나로 지정하십시오(접미부가 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 함**을 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=us`가 있습니다. 정규화된 기본 식별 이름의 예로는 `o=ibm,c=us`가 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 Application Server는 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 재사용**이 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 함**이 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 컨텐츠가 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 함**을 사용 가능으로 설정할 수 있습니다.

   기본값을 사용할 수 있습니다.

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

   SSL 사용 가능 옵션을 선택하면 **중앙에서 관리** 또는 **특정 SSL 별명 사용**을 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. **확인**을 클릭한 후 관리, 응용프로그램 및 인프라 페이지로 돌아갈 때까지 **적용** 또는 **저장**을 클릭하십시오.

5. 관리, 응용프로그램 및 인프라 보안 페이지에서 **현재로 설정**을 클릭하십시오.
6. **확인**을 클릭한 후 **적용** 또는 **저장**을 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.

문제점 피하기: Vista Windows 7 일부 레벨에서 사용자 계정 제어(UAC)가 사용되는 경우, 명령 프롬프트를 사용하려면 관리자 특권으로 Application Server를 시작해야 합니다. 다음 조치를 수행하여 실행되는 명령 프롬프트 창에서 Application Server를 시작하십시오.

- 명령 프롬프트 바로 가기를 마우스 오른쪽 단추로 클릭하십시오.
- **관리자로 실행**을 클릭하십시오.
- 명령 프롬프트 창을 관리자로 여는 경우, 계속할 것인지 묻는 운영 체제 대화 상자가 나타납니다. **계속**을 클릭하여 계속하십시오.

프로시저

1. 서버를 시작하십시오.

   다음 표에는 서버 시작 옵션이 설명되어 있습니다.

서버 시작	세부사항
첫 번째 단계 사용자 인터페이스에서	**서버 시작**을 클릭하십시오.

서버 시작	세부사항
명령행에서	다음을 입력하십시오. • Windows **Windows 플랫폼:** `startserver` *servername* • Linux UNIX **Linux 및 UNIX 플랫폼:** `startserver.sh` *servername*

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

2. 서버를 중지하십시오.

   다음 표에는 서버 중지 옵션이 설명되어 있습니다.

서버 중지	세부사항
첫 번째 단계 사용자 인터페이스에서	**서버 중지**를 클릭하고 프롬프트가 표시되면 유효한 사용자 이름과 암호를 제공하십시오. 제공하는 사용자 이름에 운영자 또는 관리자 역할이 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*

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 올바로 중지되었는지 확인하는 옵션이 설명되어 있습니다.

서버가 중지되었는지 확인하십시오.	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 제공된 8개의 역할이 있습니다. 이 역할은 관리 콘솔의 기능 범위에 권한을 부여합니다. 관리 보안이 사용 가능한 경우 사용자는 관리 콘솔에 액세스하기 위해 이러한 역할 중 하나에 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. • 서버 사용자 ID 및 암호 수정 • 관리자 역할에 사용자 및 그룹 맵핑 또한 관리자는 다음과 같이 민감한 정보에 액세스하는 데 필요한 권한을 갖습니다. • LTPA(Lightweight Third Party Authentication) 암호 • 키
ISC Admins	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, ISC Admins 역할의 사용자는 다음 타스크를 완료할 수 있습니다. • 연합 저장소 구성에서 사용자 작성, 갱신 또는 삭제 • 연합 저장소 구성에서 그룹 작성, 갱신 또는 삭제
전개자	이 역할이 부여된 사용자만 응용프로그램에 대해 구성 조치 및 런타임 조작 둘 다를 수행할 수 있습니다.
관리 보안 관리자	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.

표 2. 관리 보안 역할 (계속)

관리 보안 역할	설명
감사	이 역할이 부여된 사용자는 보안 감사 서브시스템에 대한 구성 설정값을 보고 수정할 수 있습니다. **주:** 감사 역할에는 모니터 역할이 포함됩니다. 이는 감사가 볼 수 있지만 나머지 보안 구성을 변경할 수 없도록 합니다.

자세한 정보는 WebSphere Application Server Information Center의 관리 역할을 참조하십시오.

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 적용하려면 서버를 다시 시작해야 합니다.

팁: 더 유연하고 관리가 쉽기 때문에 특정 사용자보다 그룹을 관리 역할로 맵핑하십시오. 그룹을 관리 콘솔에 맵핑하면 그룹에 사용자 추가 또는 반대인 제거가 WebSphere Process Server 외부에서 이루어지며 변경사항을 적용하는 데 서버를 다시 시작할 필요가 없습니다.

실패 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.

WebSphere Process Server에서 응용프로그램 보안

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

이 태스크 정보

WebSphere Process Server 환경에서 호스트하는 응용프로그램은 보안이 필요한 여러 비즈니스 중요 기능을 수행합니다. 일부 응용프로그램은 민감한 정보(예: 임금 정보 또

는 신용 카드 세부사항)를 액세스, 전송 또는 변경합니다. 기타 응용프로그램은 빌링 또는 인벤토리 관리를 수행합니다. 이 응용프로그램의 보안은 매우 중요합니다.

다음을 수행하여 응용프로그램을 보안하십시오.

프로시저

1. 관리 보안이 사용 가능한지 확인하십시오.
2. 응용프로그램 보안이 사용 가능한지 확인하십시오.
   a. 관리 콘솔에서 **보안**을 펼치고 **글로벌 보안**을 클릭하십시오.
   b. 보안 응용프로그램에 액세스하려고 하는 사용자로부터 WebSphere Process Server가 인증을 요구할 수 있도록 **응용프로그램 보안 사용**을 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.

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 일부분이 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 단일 사인온을 통해 성취된 전파 ID 중 하나입니다.

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

사용자 인증

관리 보안이 작동되면 클라이언트를 인증해야 합니다.

클라이언트가 인증을 받지 않고 보안 응용프로그램에 액세스하려고 하면 예외가 생성됩니다.

표 3에는 WebSphere Process Server 컴포넌트를 호출하는 전형적인 클라이언트와 각 유형의 클라이언트에 사용 가능한 인증 옵션이 표시되어 있습니다.

표 3. 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, 서블릿 및 HTML 문서를 참조합니다.
Java 클라이언트	JAAS	
모든 클라이언트	SSL 클라이언트 인증	

WebSphere Process Server 인프라의 일부 컴포넌트에는 데이터베이스 및 메시징 엔진에 액세스하기 위해 런타임 코드를 인증하는 데 사용되는 인증 별명이 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.

기본 인증 별명:

WebSphere Process Server의 여러 컴포넌트는 메시징 엔진 및 데이터베이스를 사용해서 인증을 위한 사전 정의된 별명을 사용합니다. 프로파일 작성 중 이 인증 별명에는 기본 관리자 ID 및 암호의 기본값이 제공됩니다. 사용자 계정 저장소에 있는 다른 사용자에 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 표 4의 별명을 사용하여 컴포넌트를 호출합니다.

표 4. 비즈니스 프로세스와 연관된 인증 별명

별명	설명	정보
BPEAuthDataAliasJMS_*node_server*	메시징 엔진을 사용한 인증에 사용됩니다.	프로파일 관리 도구의 Business Process Choreographer 구성 페이지에 사용자 이름 및 암호 값을 입력하십시오.
BPEAuthDataAlias*DbType_node_server*	데이터베이스를 사용한 인증에 사용됩니다.	제공된 스크립트를 사용하여 데이터베이스를 구성하십시오.

표 5에는 비즈니스 프로세스에 대해 작성된 RunAs 역할이 설명되어 있습니다.

표 5. 비즈니스 프로세스와 연관된 RunAs 역할

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

제공하는 사용자 이름이 RunAs 역할에 추가됩니다.

Common Event Infrastructure 인증 별명:

Common Event Infrastructure에는 사전 정의된 인증 별명이 있습니다. 이러한 별명은 관리 콘솔에서 수정하십시오.

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

표 6. Common Event Infrastructure와 연관된 인증 별명

별명	설명	정보
CommonEventInfrastructure JMSAuthAlias **주:** 실제 별명에는 문자 공간이 포함되어 있지 않습니다.	메시징 엔진을 사용한 인증에 사용됩니다.	프로파일 관리 도구의 Common Event Infrastructure 구성 페이지에 사용자 이름 및 암호 값을 입력하십시오.
EventAuthAlias*DBType*	데이터베이스를 사용한 인증에 사용됩니다.	프로파일 관리 도구의 Common Event Infrastructure 구성 페이지에 사용자 이름 및 암호 값을 입력하십시오.

Service Component Architecture 인증 별명:

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

호출 사용자의 ID와 관계없이 표 7의 별명을 사용하여 컴포넌트를 호출합니다.

표 7. SCA 컴포넌트와 연관된 인증 별명

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

인증 별명 수정:

기존 인증 별명을 수정해야 할 수도 있습니다.

이 태스크 정보

관리 콘솔에서 인증 별명을 수정하십시오.

프로시저

1. 비즈니스 통합 인증 별명 페이지에 액세스하십시오.

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

   주: 또한 인증 별명 정보가 필요한 다양한 관리 콘솔 페이지에서 이 페이지에 액세스할 수 있습니다.
   인증 별명 구성 페이지가 표시됩니다.

이 페이지에는 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** 열에 링크가 제공되지 않을 수도 있습니다. 이러한 경우 편집하려는 별명에 해당되는 **선택** 열에서 선택란을 선택란을 선택한 후 **편집**을 클릭합니다.

3. 별명의 특성을 변경하십시오.

   선택한 별명의 인증 별명 구성 페이지에서 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 페이지로 리턴해서 **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.

액세스 제어

일반 사용자가 WebSphere Process Server에 대해 인증된 경우 해당 사용자에게 일부 조작을 허용하지 않는 것이 보안상 중요합니다. 다른 사용자에게는 일부 특정 타스크를 거부하면서 일부 사용자에게는 이러한 타스크를 수행하도록 허용하는 것을 *액세스 제어*라고 합니다.

액세스 제어는 개발하는 컴포넌트에 맞게 배열하여 보안을 설정할 수 있습니다. 개발 시 Service Component Architecture 규정자를 사용하여 컴포넌트에 대한 액세스 제어를 제공합니다. 자세한 정보는 WebSphere Integration Developer Information Center를 참조하십시오.

EAR(Enterprise Archive) 파일로 패키지된 일부 WebSphere Process Server 컴포넌트는 Java EE 역할 기반 보안을 사용하여 해당 조작을 보안합니다. 컴포넌트의 조작에 대해 보안을 설정하는 코드 기반 보안과는 대조적으로 역할 기반 액세스 제어는 *자원*에 대한 보안을 설정합니다. 예를 들어, 비즈니스 달력 위젯에서 사용자가 개별 시간표에 대해 가지는 액세스 유형을 지정할 수 있습니다.

보안 역할 위젯

Business Space의 보안 역할 위젯을 사용하여 각 시간표에 대해 시간표의 소유자와 시간표에 대한 작성자 및 독자 액세스 권한이 있는 사용자를 지정합니다.

다음 테이블에는 관리 역할 및 기본 권한이 표시됩니다.

역할	기본 권한
BPMAdmin	1차 관리 사용자
BPMRoleManager	인증된 모든 사용자

EAR 파일 및 연관된 역할

Business Process Choreographer 및 Common Event Infrastructure는 WebSphere Process Server의 파트로 설치됩니다.

표 8. WebSphere Process Server의 연관 역할 및 EAR 파일

.ear 파일의 이름	역할	기본값
BPEContainer_*nodeName_serverName*.ear 또는 BPEContainer_*clusterName*	APIUser	모두 인증됨
	SystemAdministrator	없음
	SystemMonitor	없음
	JMSAPIUser	모두 인증됨
	AdminJobUser	모두 인증됨
	JAXWSAPIUser	모두
BPCExplorer_*nodeName_serverName*.ear 또는 BPCExplorer_*clusterName*	WebClientUser	모두 인증됨
BSpaceEAR_*nodeName_server*.ear	businessspaceusers	모두 인증됨
BSpaceWebformsEnabler_*nodeName_server*.ear	WebFormUsers	모두 인증됨
BusinessRulesManager.ear	BusinessRuleUsers	모두 인증됨
	NoOne	없음
	AnyOne	모두
BusinessRules_*nodeName_server*.ear	관리자	모두 인증됨
EventService.ear	eventAdministrator	모두 인증됨
	eventConsumer	모두 인증됨
	eventUpdater	모두 인증됨
	eventCreator	모두 인증됨
	catalogAdministrator	모두 인증됨
	catalogReader	모두 인증됨
mm.was_*nodeName_server*.ear	모두 인증됨	모두 인증됨
	everyone	모두
REST 서비스 게이트웨이.ear	RestServicesUser	모두 인증됨
REST Services Gateway Dmgr .ear	RestServicesUser	모두 인증됨

표 8. WebSphere Process Server의 연관 역할 및 EAR 파일 (계속)

.ear 파일의 이름	**역할**	**기본값**
TaskContainer_*nodeNameserverName*.ear 또는 TaskContainer_*clusterName*	APIUser	모두 인증됨
	SystemAdministrator	없음
	SystemMonitor	없음
	EscalationUser	모두 인증됨
	AdminJobUser	모두 인증됨
	JAXWSAPIUser	모두
wpsFEMgr_7.0.0 Security	WBIOperator	모두

Business Process Choreographer Java EE 역할

다음 테이블에는 Business Process Choreographer Java EE 역할이 나열됩니다.

표 9. Business Process Choreographer 역할

컴포넌트	**역할**	**값**
BPEContainer	APIUser	인증된 모든 사용자
	SystemAdministrator	구성 시 입력되는 사용자 이름, 그룹 이름 또는 둘 다
	SystemMonitor	인증된 모든 사용자
	JMSAPIUser	구성 시 입력된 사용자 이름
	AdminJobUser	구성 시 입력된 사용자 이름
	JAXWSAPIUser	모두
TaskContainer	APIUser	인증된 모든 사용자
	SystemAdministrator	SystemAdministrator
	SystemMonitor	SystemMonitor
	EscalationUser	EscalationUser
	AdminJobUser	AdminJobUser
	JAXWSAPIUser	모두

비즈니스 프로세스 및 휴먼 타스크 응용프로그램에서의 액세스 제어:

WebSphere Process Server 설치의 파트로 설치된 Business Process Choreographer는 역할을 사용하여 프로덕션 시스템의 사용자 기능을 판별합니다.

Business Process Choreographer 역할이 표 10에 표시됩니다.

표 10. 역할 및 기본 사용 권한

역할	**기본 권한**	**참고**
시스템 관리자	구성 시 입력되는 사용자 이름, 그룹 이름 또는 둘 다	모든 비즈니스 프로세스 및 모든 조작에 액세스할 수 있습니다.
시스템 모니터	인증된 모든 사용자	읽기 조작에 액세스할 수 있습니다.

표 10. 역할 및 기본 사용 권한 (계속)

역할	기본 권한	참고
JMSAPIUser	구성 시 입력된 사용자 이름	모든 Business Process Choreographer JMS API가 이 단일 사용자 ID를 대신해서 실행됩니다.
EscalationUser	구성 시 입력된 사용자 이름	비동기 API 호출을 처리하기 위해 휴먼 타스크 관리자가 사용합니다.
AdminJobUser	구성 시 입력된 사용자 이름 **주:** 제공된 사용자는 Business Process Choreographer 시스템 관리자 역할의 구성원이어야 합니다.	관리 작업(예: 정리 서비스 또는 비즈니스 프로세스 인스턴스 이주)이 이 단일 사용자 ID 대신 실행됩니다.

주: Bpcexlorer.ear 파일과 연관된 WebClientUser 역할은 Business Process Choreographer Explorer에 액세스할 수 있습니다. 이 역할에 대한 기본 권한은 모두 인증됩니다.

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 설명은 WebSphere Application Server Network Deployment Information Center를 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 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 프라이

버시 지원을 추가합니다. SSL과 달리 세션 키를 설정하기 위한 핸드쉐이크가 없습니다. 이에 따라 JMS(Java Message Service) 상의 SOAP 또는 SIB(서비스 통합 버스) 상의 SOAP와 같이 비동기 환경의 메시지 보안에 WS-Security가 적합하게 됩니다. WS-Security 전개 설명자는 전개 이전에 응용프로그램에 설정할 수 있습니다.

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

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 더 일반적인 설명은 WebSphere Application Server 주제 전송 레벨에서 웹 서비스에 대한 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 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.

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.

이 태스크 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 사용자가 『bob』일 때 클라이언트(『alice』)가 위임이 설정된 상태에서 엔터프라이즈 Bean을 호출하는 서블릿을 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 **응용프로그램**을 펼치고 **새 응용프로그램 설치**를 클릭하십시오.

   "보안 역할을 사용자 및 그룹에 맵핑"이란 제목의 단계에 앞서 응용프로그램 설치를 위해 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 사용**을 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 특

권을 가지므로 이 ID는 주의하여 사용하십시오. 페이지에 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.

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 작동하기 위해 전개 시에 추가 단계를 수행해야 합니다.

시작하기 전에

이 타스크에서는 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 맵핑됩니다. securityIdentity로 보안 설정된 컴포넌트의 호출에서는 응용프로그램을 호출하는 사용자의 ID와 무관하게 지정된 ID를 사용합니다.

프로시저

1. 응용프로그램을 WebSphere Process Server로 전개하는 지침을 따르십시오. 자세한 사항은 모듈 전개을 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 다시 시작 없이도 응용프로그램에 액세스할 수 있기 때문에 가장 유연한 선택은 맵핑된 그룹입니다.
보안 ID	역할이 맵핑되는 ID에 유효한 사용자 이름 및 암호를 제공하십시오.

비즈니스 달력 위젯에 대한 보안

보안 역할 위젯은 비즈니스 달력 위젯의 개별 시간표에 대한 액세스 보안을 설정할 수 있는 기능을 제공합니다. 보안 역할 위젯을 사용해서 조직 구성원에게 역할을 지정합니다. 이러한 역할로 시간표에 대한 액세스 레벨을 판별합니다.

비즈니스 달력 위젯에 대한 역할 기반 액세스 제어를 관리하는 데 사용하는 보안 역할 위젯은 WebSphere로 구현되는 Business Space에 있습니다.

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

비즈니스 달력 위젯의 보안 역할 위젯 역할 기반 액세스 제어를 사용하는 장점은 무엇입니까?

- 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 맵핑합니다. 역할은 자원의 특정 인스턴스에 대해 구성원이 가지는 권한을 정의합니다.

시간표와 연관된 역할

시간표가 설치될 때 세 가지 역할(시간표 소유자, 작성자 및 독자)이 작성됩니다. 이러한 역할은 컴포넌트 특정 역할로 알려져 있습니다.

이러한 역할의 사용 방법 조직에서 사용되는 휴일 시간표의 경우를 고려해보십시오. 모든 직원이 시간표에 액세스할 수는 있지만 시간표를 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.

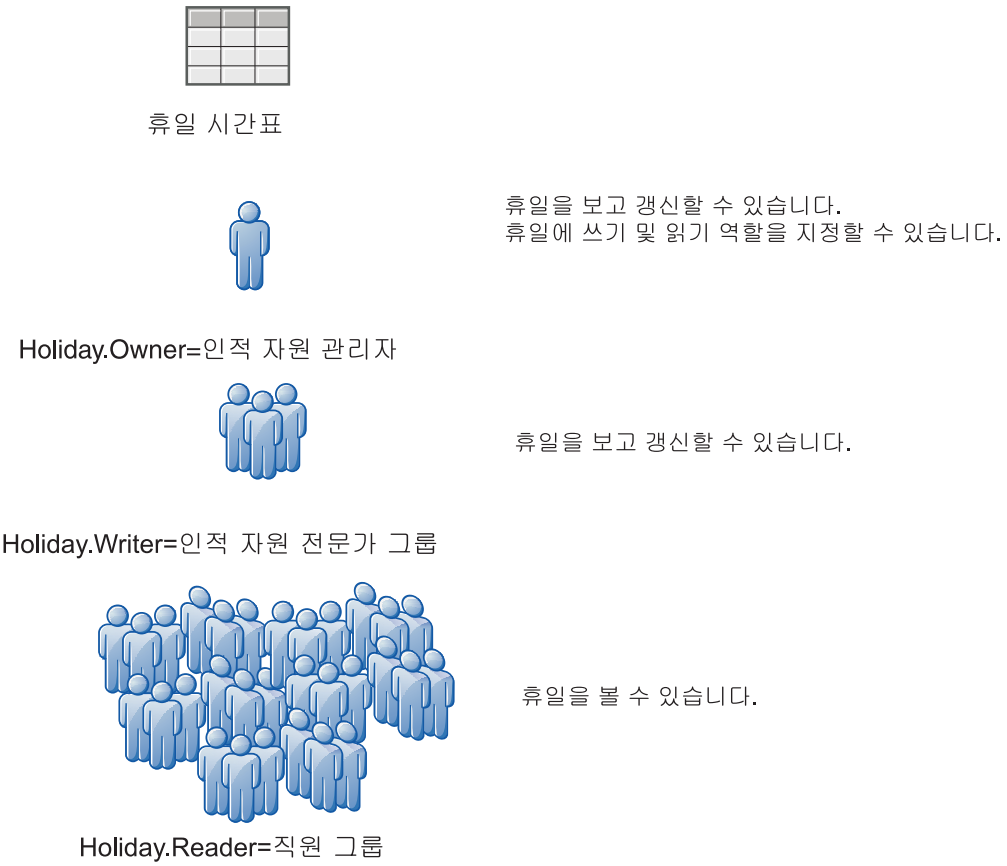


그림 1. 시간표에 지정된 역할의 예제

시간표를 전개하면 세 가지 역할(소유자, 작성자 및 독자)이 작성됩니다. 모든 역할의 권한은 *초기에는* **인증된 모든 사용자**로 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 역할 위젯에서 이러한 시간표 관련 역할은 모듈 역할로도 알려져 있습니다.

보안 역할 위젯의 시스템 역할

BPMAdmin 및 BPMRoleManager 역할은 WebSphere Process Server를 설치한 후에 보안을 사용할 수 있을 때 자동으로 작성됩니다(또는 WebSphere Process Server 7.0으로 업그레이드).

- BPMAdmin

  BPMAdmin은 BPMRoleManager 역할에서 구성원을 추가 또는 제거하는 권한을 가집니다. 예를 들어, BPMRoleManager 역할을 수행하는 사용자가 조직을 떠나면 BPMAdmin만 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

  BPMRoleManager에는 세 가지 시간표 관련 역할(소유자, 작성자 및 독자)에서 구성원을 추가 또는 제거하는 권한이 있습니다. 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.

보안 역할 위젯에서 역할 관리

보안 역할 위젯을 사용하여 사용자 또는 그룹을 시스템 역할에 지정할 수 있습니다. 시간 테이블과 연관되는 컴포넌트 역할에 사용자 또는 그룹을 지정할 수도 있습니다.

컴포넌트 역할 지정

비즈니스 달력 위젯의 모든 시간표에는 연관된 세 개의 컴포넌트 역할(소유자, 작성자 및 독자)이 있습니다. 보안 역할 위젯을 사용하여 이러한 역할에 사용자 또는 그룹을 지정합니다.

시작하기 전에

보안 역할 위젯이 표시되는지 확인하십시오.

이 태스크 정보

BPMRoleManager는 사용자 또는 그룹을 컴포넌트 역할에 지정할 수 있습니다.

시간표의 소유자는 사용자 또는 그룹을 해당 시간표에 대한 소유자, 작성자 및 독자 역할에 지정할 수도 있습니다.

프로시저

1. 개별 구성원을 모듈 역할에 지정하려면 다음 단계를 완료하십시오.
   a. **모듈** 목록에서 시간표를 선택하십시오.
   b. 역할(예: 시간표에 대한 작성자 역할)의 경우 역할 이름을 클릭하십시오.

c. 페이지의 오른쪽에서 **추가**를 클릭하십시오.

d. **검색할 사용자 또는 그룹** 필드에 이름(또는 이름 파트)을 입력하십시오.

e. 검색 기준을 기반으로 리턴된 사용자 또는 그룹의 구성원을 제한하려면 **최대 결과** 필드의 값을 변경하십시오. 이 값을 0으로 설정해서 전체 결과 세트를 리턴하십시오.

f. **검색**을 클릭하십시오.

g. 표시된 목록에서 하나 이상의 사용자 또는 그룹을 선택하고 **확인**을 클릭하십시오.

h. 모든 구성원을 지정한 경우 **저장**을 클릭하십시오.

2. 모든 구성원을 모듈 역할에 지정하려면 다음 단계를 완료하십시오.

a. **모듈** 목록에서 시간표를 선택하십시오.

b. 역할(예: 시간표에 대한 독자 역할)의 경우 역할 이름을 클릭하십시오.

c. **모두 인증**을 선택하십시오.

d. **저장**을 클릭하십시오.

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 EIS와 WebSphere Process Server가 지원하는 Java EE 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. JCA에도 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. 이는 전개 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. 그러나 EAR 파일이 WebSphere Process Server로 전개되면 사용할 ID에 대한 사용자 이름 및 암호를 제공해야 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 메시지로써 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.

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. 특정 역할과 연관된 역할 조회 또는 역할 지정에 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.

독자 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.

Business Space에 대한 보안 설정

사용자 환경에서 WebSphere로 구현되는 Business Space를 사용하는 경우, Business Space의 아티팩트에 대해 팀이 작업할 방법의 보안 옵션을 고려해야 합니다. Business Space에 대한 보안을 켜려면 응용프로그램 보안을 설정하고 사용자 저장소를 지정하십시오. Business Space 관리자를 정의하려면 슈퍼유저 역할을 지정하십시오.

이 태스크 정보

최선의 결과를 위해 Business Space를 구성하기 전에 보안을 사용 가능으로 설정하십시오. 관리 콘솔의 글로벌 보안 관리 페이지에서 관리 보안과 응용프로그램 보안을 둘 다 사용 가능하게 하십시오. 또한 사용자 계정 저장소를 지정하십시오.

Business Space에 대한 사용자 계정 레지스트리 사용 고려사항:

- 사용하는 LDAP 구성 유형에 따라 설정은 Business Space에 올바르게 액세스하는 기능에 영향을 미칠 수 있습니다. 사용자 필터, 그룹 필터 및 맵핑 설정이 올바르게 구성되었는지 확인하십시오. 자세한 정보는 WebSphere Application Server 문서의 LDAP(Lightweight Directory Access Protocol) 검색 필터 구성을 참조하십시오.
- 사용하는 연합 저장소 구성 유형에 따라 설정은 Business Space에 올바르게 액세스하는 기능에 영향을 미칠 수 있습니다. 범주가 올바르게 구성되었는지 확인하십시오. 자세한 정보는 WebSphere Application Server 문서에서 연합 저장소 구성의 범주 관리를 참조하십시오.
- LDAP 보안은 Business Space에서 검색할 때 기본적으로 로그인 특성 `uid`(사용자 ID)를 사용하도록 설정됩니다. LDAP 보안이 로그인 특성의 `mail`(전자 우편 주소)과 같은 다른 고유 LDAP 필드를 사용하도록 변경된 경우, Business Space에서 검색이 작동하도록 하려면 `ConfigServices.properties` 파일의 userIdKey 특성을 수정해야 합니다. `ConfigServices.properties` 파일은 독립형 서버의 경우

profile_root₩BusinessSpace₩*node_name*₩*server_name*₩mm.runtime.prof₩config₩ConfigService.properties에 있으며 클러스터의 경우 *deployment_manager_profile_root*₩BusinessSpace₩*cluster_name*₩mm.runtime.prof₩config₩ConfigService.properties에 있습니다. userIdKey 속성을 uid에서 LDAP 보안의 로그인 특성에 일치하도록 변경하십시오(예: mail). 그런 다음 wsadmin 스크립트 클라이언트를 사용하고 매개변수 **-serverName**과 **-nodeName**(독립형 서버의 경우) 또는 **-clusterName**(클러스터의 경우), **-propertyFileName**과 ConfigServices.properties 파일의 경로 값 및 **-prefix**와 값 Mashups_를 지정하여 updatePropertyConfig 명령을 실행하십시오.

- Microsoft® SQL Server 데이터베이스 및 **독립형 LDAP** 레지스트리를 사용 중인 경우, 사용자 식별 이름(사용자 DN)이 131자를 초과하지 않는지 확인하십시오. 사용자 DN 항목 중 131자를 초과하는 것이 있는 경우에는 사용자 계정 저장소에 대해 **연합 저장소** 옵션을 지정해야 합니다. 연합 저장소와 다른 저장소 간에 전환하는 경우 모든 기존 영역과 페이지는 Business Space에서 더 이상 액세스할 수 없으며 다시 작성해야 합니다.
- **연합 저장소**를 사용하는 경우, 위젯 및 프레임워크에 확장 검색 기능과 같은 추가 기능이 있습니다. 영역 및 페이지를 공유할 사용자를 검색하는 경우, 검색 범위에는 전자 우편, 전체 사용자 이름 및 사용자 ID가 포함됩니다.

IBM® Tivoli Access Manager WebSEAL을 사용하는 경우 Business Space 환경에 대해 사용하려면 추가 구성 단계를 완료해야 합니다. 외부 JACC(Java Authorization Contract for Containers) 프로바이더에 대해 Tivoli Access Manager 보안을 구성하고 Tivoli Access Manager에 대해 WebSEAL을 구성하고 제품 Application Server에 대해 WebSEAL을 구성하고 사용자 환경에 대한 호스트 응용프로그램 서버에 대해 호스트 연결을 구성하십시오.

Business Space 환경에서 관리자가 될 사용자를 설정하려면 스크립트를 실행하여 Business Space 슈퍼유저 역할을 지정하십시오.

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.

- 사용자 ID가 제품에 대한 사용자 레지스트리에 등록되어 있는지 확인합니다.

보안 환경을 사용할 것으로 예상하는 경우에는 Business Space를 구성하기 전에 보안을 사용 가능으로 설정하십시오. Business Space를 구성한 후에 보안을 사용하거나 제

거하려면 ConfigServices.properties 파일에서 MashupAdminForOOBSpace 특성과 noSecurityAdminInternalUserOnly 특성을 모두 수정하여 올바른 사용자 ID를 올바른 관리자 ID로 설정해야 합니다. ConfigServices.properties 파일은 독립형 서버의 경우 *profile_root*₩BusinessSpace₩*node_name*₩*server_name*₩mm.runtime.prof₩config₩ConfigService.properties에 있으며 클러스터의 경우 *deployment_manager_profile_root*₩BusinessSpace₩*cluster_name*₩mm.runtime.prof₩config₩ConfigService.properties에 있습니다. 수정한 파일을 시스템의 빈 폴더에 복사하십시오. 그런 다음 wsadmin 스크립트 클라이언트를 사용하고 다음 매개변수를 지정하여 updatePropertyConfig 명령을 실행하십시오.

- 독립형 서버의 경우 **-serverName** 및 **-nodeName**, 클러스터의 경우 **-clusterName**
- **-propertyFileName**과 ConfigServices.properties 파일의 경로 값
- **-prefix**와 값 Mashups_

이 태스크 정보

Business Space는 액세스의 인증 및 권한을 확인하도록 사전 구성됩니다. 사용자는 Business Space URL에 액세스할 때 인증하도록 프롬프트됩니다. 인증되지 않은 사용자의 경로는 로그인 페이지로 재지정됩니다. Business Space는 HTTP 또는 HTTPS로 액세스할 수 있습니다. 다만 로그인 페이지는 항상 HTTPS로 경로 재지정됩니다. 그러므로 IBM HTTP Server와 같은 웹 서버를 사용하는 경우에는 HTTPS를 지원하도록 구성해야 합니다.

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

Business Space에 대해 인증된 액세스를 사용하려면 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 글로벌 보안 관리 콘솔 페이지에서 **관리 보안 사용** 및 **응용프로그램 보안 사용**을 모두 선택하십시오.
3. 동일한 관리 콘솔 페이지의 **사용자 계정 저장소** 아래에서 **연합 저장소**, **로컬 운영체제**, **독립형 LDAP 레지스트리** 또는 **독립형 사용자 정의 레지스트리**를 지정하십시오. Business Space의 보안 설정에서 사용자 레지스트리 선택에 대한 고려사항을 검토하십시오.
4. Business Space가 제품이 실행 중인 위치와 떨어져 있으며 Business Space가 실행 중인 노드와 제품이 실행 중인 노드가 동일한 셀에 있지 않은 경우 수동 단계를 완료하여 단일 사인온(SSO)을 사용 가능하도록 설정해야 합니다. 예를 들어, 둘 이

상의 제품(WebSphere Business Compass, WebSphere Business Monitor, WebSphere Enterprise Service Bus 또는 WebSphere Process Server)을 사용 중이고 서버가 서로 다른 노드에 있는 경우 모든 서버가 Business Space 서버에 대해 작업할 수 있도록 하려면 수동으로 SSO를 구성해야 합니다. SSO를 사용 가능으로 설정하려면 다음 단계를 완료하십시오.

a. 각 서버에 대한 관리 콘솔에서 **보안 → 글로벌 보안**을 클릭하여 글로벌 보안 페이지를 여십시오. **웹 및 SIP 보안**을 펼치고 **단일 사인온(SSO)**을 클릭하여 **사용 가능** 선택란이 체크되었는지 확인하십시오.

b. 모든 노드가 동일한 **사용자 계정 저장소** 정보를 사용하는지 확인하십시오(3단계 참조).

c. 첫 번째 노드에 대한 관리 콘솔에서 글로벌 보안 페이지를 여십시오. 인증에서 **LTPA**를 클릭하십시오.

d. **교차 셀 단일 사인온**에서 키 파일의 암호 및 완전한 키 파일 이름(키 파일을 내보낼 위치와 파일 이름)을 입력하십시오. 완전한 키 파일 이름은 서버를 실행 중인 시스템의 절대 경로입니다.

e. **키 내보내기**를 클릭하십시오. 키 파일이 서버가 실행 중인 시스템에 저장됩니다.

f. 두 노드가 동일한 시스템에 있지 않은 경우 키 파일을 물리적으로 다른 시스템에 복사하십시오.

g. 동일한 키 파일을 사용하여 다른 모든 노드의 키 파일 가져오기: 다른 노드의 관리 콘솔에 로그인하여 글로벌 보안 > LTPA 페이지로 이동하십시오. **교차 셀 단일 사인온**에서 키 파일의 암호 및 완전한 키 파일 이름(복사하여 내보낸 키 파일과 동일한 암호 사용)을 입력하고 **키 가져오기**를 클릭하십시오.

h. 각 시스템의 키를 가져온 후 서버를 다시 시작하십시오.

5. 엔드포인트 파일에서 HTTPS를 사용 중이며 엔드포인트 위치가 Business Space와 다른 노드에 있고 SSL(Secure Sockets Layer) 인증이 자체 서명된 SSL 인증인 경우 SSL 인증을 가져와야 합니다.

   a. Business Space가 포함된 서버의 관리 콘솔에 로그온하여 제품이 실행 중인 원격 노드에서 사용하는 SSL 인증을 가져오십시오.

      1) 보안 아래에서 **SSL 인증 및 키 관리**를 클릭하십시오.

      2) SSL 인증 및 키 관리 페이지의 관련 항목에서 **키 저장소 및 인증**을 클릭하십시오.

      3) 키 저장소 및 인증 페이지에서 **NodeDefaultTrustStore**를 클릭하여 신뢰 저장소 유형을 수정하십시오.

      4) NodeDefaultTrustStore 페이지의 추가 특성에서 **서명자 인증**을 클릭하십시오.

      5) **NodeDefaultTrustStore**의 서명자 인증 페이지에서 **포트에서 검색** 단추를 클릭하십시오.

6) 포트에서 검색 페이지의 일반 특성에서 제품을 실행하는 위치의 호스트, 포트 및 별명을 입력하십시오. **서명자 정보 검색** 단추를 클릭한 후 **확인**을 클릭하십시오.

7) 두 서버를 모두 다시 시작하십시오.

b. 제품 노드의 관리 콘솔에 로그온하여 Business Space가 실행 중인 노드에서 사용하는 SSL 인증을 가져오십시오.

1) a. i. - v. 단계를 반복하십시오.

2) 포트에서 검색 페이지의 일반 특성 아래에 Business Space가 실행 중인 위치의 호스트 및 포트를 입력하십시오. **서명자 정보 검색** 단추를 클릭한 후 **확인**을 클릭하십시오.

3) 두 서버를 모두 다시 시작하십시오.

SSO 및 SSL에 대한 자세한 정보는 WebSphere Application Server Information Center를 참조하십시오.

다음에 수행할 작업

- 관리 보안 및 응용프로그램 보안이 설정된 후 Business Space에 로그온하면 사용자 ID 및 암호에 대한 프롬프트가 표시됩니다. 로그온하기 위해서는 선택한 사용자 레지스트리에서 올바른 사용자 ID 및 암호를 사용해야 합니다. 관리 보안을 설정한 후 관리 콘솔로 리턴할 때마다 관리 권한이 있는 사용자 ID로 로그온해야 합니다.
- Business Space의 페이지 및 영역에 대한 권한을 설정하려면 Business Space 페이지 및 영역을 작성할 때 권한을 관리할 수 있습니다.
- 사용자 및 그룹에 따라 위젯의 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 맵핑**을 선택하십시오. RestServicesUser 역할의 사용자 및 그룹을 해당 역할에 추가하여 모든 REST 서비스 위젯의 데이터에 대한 액세스를 제어할 수 있습니다.
- 사용자 그룹 역할을 기반으로 한 위젯의 데이터에 대한 액세스를 제한하려면 관리 그룹 역할에 지정된 사용자를 변경하십시오. 관리 콘솔을 열고 **보안 → 관리, 응용프로그램 및 인프라 보안 → 관리 그룹 역할**을 클릭한 후 그룹을 선택하여 이 역할에 지정된 사용자를 표시하는 역할 목록을 볼 수 있습니다.

  비즈니스 규칙 및 비즈니스 변수와 같은 위젯의 관리 그룹 역할에 지정된 사용자 변경을 고려할 수 있습니다.

  예를 들어, 시스템 성능 상태 위젯의 경우 다음 관리 역할에는 모두 모니터링 사용권한이 있으며 모두 관리 콘솔에 액세스할 수 있으므로 이 역할에 지정된 사용자는 시스템 성능 상태 위젯의 데이터에 액세스할 수 있습니다.

  – **모니터**

- 구성자
- 운영자
- 관리자
- **Adminsecuritymanager**
- 전개자
- **iscadmins**

관리 그룹 역할에 맵핑된 사용자는 시스템 성능 상태 위젯의 데이터에 액세스할 수 있습니다. 이 역할에 맵핑되지 않은 사용자는 시스템 성능 상태 위젯의 데이터에 액세스할 수 없습니다.

- 마지막으로, 일부 위젯에는 비즈니스 사용자가 작성한 아티팩트에 대한 역할 기반 액세스의 추가 레이어가 있습니다. 솔루션 관리의 경우 보안 역할 위젯을 사용하여 비즈니스 달력 위젯의 시간표에 대해 구성원이 가진 액세스 레벨을 판별하는 사용자 및 그룹 시스템 역할을 지정할 수 있습니다. 검토를 위해 검토 액세스 제어 위젯은 검토할 수 있고 검토에 주석을 추가할 수 있는 사용자의 사용 권한을 관리합니다. 자세한 정보는 위젯에 대한 온라인 도움말을 참조하십시오.

주:

SystemOut.log 파일에 다음 오류가 있는 경우, 사용자 레지스트리에 처리할 수 없는 여분의 속성이 있을 수 있습니다.

```
00000046 SystemErr R Caused by: com.ibm.websphere.wim.exception.WIMSystemException: CWWIM1013E
    The value of the property secretary is not valid for entity uid=xxx,c=us,ou=yyy,o=ibm.com.
00000046 SystemErr R at com.ibm.ws.wim.adapter.ldap.LdapAdapter
.setPropertyValue(LdapAdapter.java:3338)
```

ConfigServices.properties 파일에 다음 속성을 설정하여 이러한 속성을 생략하십시오.

```
com.ibm.mashups.user.userProfile = LIMITED
com.ibm.mashups.user.groupProfile = LIMITED
```

ConfigServices.properties 파일은 독립형 서버의 경우 *profile_root*₩BusinessSpace₩*node_name*₩*server_name*₩mm.runtime.prof₩config₩ConfigService.properties에 있으며 클러스터의 경우 *deployment_manager_profile_root*₩BusinessSpace₩*cluster_name*₩mm.runtime.prof₩config₩ConfigService.properties에 있습니다. ConfigServices.properties 파일을 수정한 후 wsadmin 스크립트 클라이언트를 사용하고 매개변수 **-serverName**과 **-nodeName**(독립형 서버의 경우) 또는 **-clusterName**(클러스터의 경우), **-propertyFileName**과 ConfigServices.properties 파일의 경로 값 및 **-prefix**와 값 Mashups_를 지정하여 updatePropertyConfig 명령을 실행하십시오.

주:

클러스터에서 Java 2 보안이 사용되는 경우, Business Space 도움말 위치에 적용되는 서버 정책의 항목을 엄격하게 할 것을 고려하십시오.

Business Space 도움말 위치 정책은 다음과 같습니다.

```
grant codeBase     "file:${was.install.root}/profiles/profile_name/
temp/node_name/-" {

    permission java.security.AllPermission;

};
```

다음과 같이 변경하여 정책을 엄격하게 하십시오.

```
grant codeBase     "file:${was.install.root}/profiles/profile_name/
temp/node_name/server_name/BusinessSpaceHelpEAR_node_name_server_name/
BusinessSpaceHelp.war/-" {

    permission java.security.AllPermission;

 };
```

Business Space에 대해 작동하도록 Tivoli Access Manager WebSEAL 구성

Tivoli Access Manager WebSEAL이 있고 Business Space에 대해 이를 사용하려는 경우, 몇 가지 추가 구성 단계를 완료해야 합니다.

이 태스크 정보

Business Space에 대해 Tivoli Access Manager WebSEAL을 사용하려는 경우, 외부 JACC(Java Authorization Contract for Containers) 프로바이더에 대해 Tivoli Access Manager 보안을 구성하고 Tivoli Access Manager에 대해 WebSEAL을 구성하고 제품 Application Server에 대해 WebSEAL을 구성하고 사용자 환경에 대한 호스트 응용프로그램 서버에 대해 호스트 연결을 구성해야 합니다.

프로시저

1. JACC에 대해 Tivoli Access Manager 구성
   a. 관리 콘솔을 사용할 것인지 wsadmin 명령을 사용할 것인지에 따라 다음 단계 중 하나를 완료하십시오.
      - 관리 콘솔을 사용하여 JACC에 대해 Tivoli Access Manager를 구성하려는 경우에는 다음 단계를 완료하십시오.
        1) 글로벌 보안을 사용 가능으로 설정하십시오.
           a) **보안 → 글로벌 보안**을 선택하십시오.

b) Tivoli Access Manager가 구성된 LDAP 서버에 대해 **관리 보안**, **응용프로그램 보안** 및 **Java 2 보안**을 사용 가능으로 설정하십시오.

c) **글로벌 보안** → **LDAP**을 선택하고 다음 정보를 입력한 후 **확인**을 클릭하십시오.

이름	**Description**
서버 사용자 ID	Tivoli Access Manager 설정의 관리자 DN에 대해 입력한 것과 동일한 사용자 ID를 입력하십시오. 예: user1
서버 사용자 암호	puser1
호스트	Tivoli Access Manager에 대해 구성된 LDAP
포트	예: 389
기본 DN	예: o=ibm, c=us
바인드 DN	예: cn=SecurityMaster,secAuthority=Default
바인드 pwd	SecurityMaster 사용자의 암호

d) 구성을 저장하고 서버를 다시 시작하십시오.

2) Tivoli Access Manager 및 JACC에 대해 외부 권한을 사용 가능으로 설정하십시오.

a) **보안** → **글로벌 보안** → **외부 권한 프로바이더**를 선택하십시오.

b) **권한 프로바이더** 목록에서 **외부 JACC 프로바이더**를 선택한 후 **구성**을 클릭하십시오. Tivoli Access Manager의 기본 특성이 올바릅니다. 기본값을 변경하지 마십시오.

c) **추가 특성**에서 **Tivoli Access Manager 특성**을 선택하십시오. **임베디드 Tivoli Access Manager 사용 가능**을 선택하고 다음 정보를 입력한 후 **확인**을 클릭하십시오.

이름	값
클라이언트 청취 포트 설정	기본 설정은 8900 - 8999입니다. 다른 포트를 사용할 경우에만 변경하십시오.
Policy Server(이름:포트)	*policyserver*:*port*를 지정하십시오. 예: windomain3.rtp.raleigh.ibm.com:7135
권한 서버 및 우선순위(이름:포트:우선순위)	*authorizationserver*:*port*:*priority*를 지정하십시오. 예: windomain3.rtp.raleigh.ibm.com:7136:1
관리자 사용자 이름	Tivoli Access Manager 서버에서 다른 관리자 이름을 사용하지 않으려면 사용자 이름을 **sec_master**(기본값)로 두십시오.
관리자 사용자 암호	domino123
사용자 레지스트리 식별 이름 확장자	Application Server에 사용할 이름을 입력하십시오. 예: o=ibm, c=us

이름	값
보안 도메인	보안 도메인은 **기본값**으로 설정된 채로 두십시오. Tivoli Access Manager 서버에서 기본 도메인을 사용하지 않는 경우 이 설정을 변경하십시오. Tivoli Access Manager 서버에서 여러 도메인을 작성했고 **기본값**이 아닌 도메인을 연결하거나 사용하려는 경우 이 설정을 변경하십시오.
관리자 사용자 식별 이름	사용자의 완전한 이름을 입력하십시오. 예: `cn=user1,o=ibm,c=us` **주:** 이 사용자는 LDAP 사용자 레지스트리 패널에 구성된 **서버 사용자 ID**와 동일합니다.

서버는 Tivoli Access Manager 서버에 접속하여 Application Server에 여러 특성 파일을 작성합니다. 이 프로세스에는 몇 분이 걸릴 수 있습니다. 오류가 발생하는 경우 시스템 출력을 찾아보고 문제점을 정정하십시오.

- wsadmin 유틸리티를 사용하여 JACC에 대해 Tivoli Access Manager를 구성하려는 경우에는 다음 단계를 완료하십시오. Deployment Manager 서버에 대해 다음 프로시저를 한 번 수행하십시오. 동기화가 수행될 때 구성 매개변수가 관리 서버(Node Agent 포함)로 전달됩니다. 구성 변경사항을 적용하려면 관리 서버를 다시 시작해야 합니다.
  1) 모든 관리 서버(Node Agent 포함)가 시작되는지 확인하십시오.
  2) 서버를 시작하십시오.
  3) *install_root*/bin 디렉토리에서 wsadmin 명령을 실행하여 명령행 유틸리티를 시작하십시오.
  4) wsadmin 프롬프트에서 다음 표의 적절한 정보를 포함하여 configureTAM 명령을 실행하십시오.

     Jacl 예제:

     ```
     $AdminTask configureTAM -interactive
     ```

     Jython 예제:

     ```
     AdminTask.configureTAM('-interactive')
     ```

     이제 다음 정보를 입력하십시오.

이름	값
제품 서버의 노드 이름	단일 노드를 지정하거나 별표(*)를 입력하여 모든 노드를 선택하십시오.

이름	값
Tivoli Access Manager Policy Server	Tivoli Access Manager Policy Server의 이름 및 연결 포트를 입력하십시오. *policy_server:port* 형식을 사용하십시오. Policy Server 통신 포트는 Tivoli Access Manager를 구성할 때 설정됩니다. 기본 포트는 7135입니다.
Tivoli Access Manager 권한 서버	Tivoli Access Manager 권한 서버의 이름을 입력하십시오. *auth_server:port:priority* 형식을 사용하십시오. 권한 서버 통신 포트는 Tivoli Access Manager를 구성할 때 설정됩니다. 기본 포트는 7136입니다. 쉼표로 항목을 구분하여 둘 이상의 권한 서버를 지정할 수 있습니다. 둘 이상의 권한 서버를 구성하면 장애 복구 및 성능 향상에 유용합니다. 우선순위 값은 권한 서버의 사용 순서입니다. 예: `auth_server1:7136:1,auth_server2:7137:2`. 단일 권한 서버에 대해 구성하는 경우에도 우선순위 1은 필요합니다.
제품 서버의 관리자 식별 이름	제품 서버에 대한 보안 관리자 ID의 전체 식별 이름을 입력하십시오. 예: `cn=wasadmin,o=organization,c=country`. 자세한 정보는 관련 링크를 참조하십시오.
Tivoli Access Manager 사용자 레지스트리 식별 이름 확장자	예: o=organization, c=country
Tivoli Access Manager 관리자 사용자 이름	Tivoli Access Manager를 구성할 때 작성한 대로 Tivoli Access Manager 관리 사용자 ID를 입력하십시오. 이 ID는 일반적으로 sec_master입니다.
Tivoli Access Manager 관리자 사용자 암호	Tivoli Access Manager 관리자의 암호를 입력하십시오.
Tivoli Access Manager 보안 도메인	사용자 및 그룹을 저장하는 데 사용되는 Tivoli Access Manager 보안 도메인의 이름을 입력하십시오. Tivoli Access Manager를 구성할 때 보안 도메인을 아직 설정하지 않은 경우에는 **리턴**을 클릭하여 기본값을 승인하십시오.
임베디드 Tivoli Access Manager 청취 포트 설정	제품 서버는 TCP/IP 포트에서 Policy Server의 권한 데이터베이스 갱신사항을 청취합니다. 특정 노드 및 시스템에서 둘 이상의 프로세스가 실행될 수 있으므로 프로세스에 대한 포트 목록이 필요합니다. Tivoli Access Manager 클라이언트에서 청취 포트로 사용할 포트를 쉼표로 구분하여 지정하십시오. 포트 범위를 지정하는 경우에는 하한 값과 상한 값을 콜론으로 구분하십시오. 예: 7999, 9990:9999.
지연	`yes`로 설정: 이 옵션은 다음에 다시 시작될 때까지 관리 서버의 구성을 지연합니다. `no`로 설정: 관리 서버의 구성이 즉시 발생합니다. 관리 서버는 다음 번에 다시 시작할 때 구성됩니다.

5) 필요한 정보를 모두 입력한 후 구성 특성을 저장하려면 **F**를 선택하고, 구성 프로세스를 취소하고 입력한 정보를 버리려면 **C**를 선택하십시오.

SVTM TAM60 서버에 대한 예:

```
wsadmin>$AdminTask configureTAM -interactive
Configure embedded Tivoli Access Manager

This command configures embedded Tivoli Access Manager
on the WebSphere
Application Server node or nodes specified.

WebSphere Application Server Node Name (nodeName): *
*Tivoli Access Manager Policy Server (policySvr):
 windomain3.rtp.raleigh.ibm.com:7135
*Tivoli Access Manager Authorization Servers (authSvrs):
 windomain3.rtp.raleigh.ibm.com:7136:1
*WebSphere Application Server administrator's
distinguished name (wasAdminDN):
 cn=was61admin,o=ibm,c=us
*Tivoli Access Manager user registry distinguished
name suffix (dnSuffix):
o=ibm,c=us
Tivoli Access Manager administrator's
user name (adminUid):
 [sec_master]
*Tivoli Access Manager administrator's
user password (adminPasswd):
 domino123
Tivoli Access Manager security domain
(secDomain): [Default]
Embedded Tivoli Access Manager
listening port set (portSet): [9900:9999]
Defer (defer): [no]

Configure embedded Tivoli Access Manager

F (Finish)
C (Cancel)

Select [F, C]: [F] F
WASX7278I: Generated command line:
$AdminTask configureTAM {-policySvr
 windomain3.rtp.raleigh.ibm.com:

 7135 -authSvrs
 windomain3.rtp.raleigh.ibm.com:

 7136:1 -wasAdminDN cn=wa
Embedded Tivoli Access Manager
configuration action parameters saved successfully.
 Restart all WebSphere Application

 Server instances running on the target node or
 nodes to
wsadmin>
```

6) 관리 콘솔에서 **보안 → 글로벌 보안 → 외부 권한 프로바이더**를 선택하십시오. 그런 다음 **JACC 프로바이더**를 **사용하는 외부 권한**을 선택하고 **확인**을 클릭하십시오.

7) 기본 보안 화면으로 이동하여 **확인**을 클릭하십시오. 변경사항을 저장하고 동기화하십시오.

8) 셀 내의 모든 프로세스를 다시 시작하십시오.

b. Tivoli Access Manager를 사용 가능으로 설정하기 전에 응용프로그램을 설치한 경우(예를 들어, LDAP 보안을 사용 가능으로 설정하고 일부 보안 응용프로그램을 설치하고 사용자 및 그룹을 보안 역할에 맵핑한 경우), 보안 역할 맵핑 정보를 전개 설명자에서 Tivoli Access Manager Policy Server로 전파하십시오. 관리 콘솔을 사용할 것인지 wsadmin 명령을 사용할 것인지에 따라 다음 단계 중 하나를 수행하십시오.

- propagatePolicyToJACCProvider wsadmin 명령을 사용하려면 wsadmin 스크립트를 사용하여 JACC 프로바이더로 설치된 응용프로그램의 보안 정책 전파를 참조하십시오.
- 관리 콘솔을 사용하려면 이전에 전개된 응용프로그램에 대해 보안 정책 및 역할 전파를 참조하십시오.

2. Tivoli Access Manager에 대해 WebSEAL을 구성하십시오.

a. WebSEAL이 설치되었으며 올바르게 구성되었는지 확인하십시오.

b. TAI++의 경우 **-c iv_creds** 옵션 및 TAI의 경우 **-c iv_user** 옵션을 사용하여 WebSEAL과 제품 Application Server 사이의 연결을 작성하십시오. 환경에 알맞은 변수를 사용하여 다음 명령 중 하나를 한 행으로 입력하십시오.

TAI++의 경우

```
server task webseald-server create -t tcp -b supply -c iv_creds

-h host_name -p websphere_app_port_number junction_name
```

c. Tivoli Access Manager에서 TAI 구성에 사용할 수 있는 신뢰되는 사용자 계정을 작성하려면 다음 명령을 실행하십시오.

```
pdadmin -a sec_master -p domino123

pdadmin sec_master> user create -gsouser -no-password-policy
taiuser "cn=taiuser,ou=websphere,o=ibm,c=us" taiuser taiuser
ptaiuser

pdadmin sec_master> user modify taiuser password-valid yes

pdadmin sec_master> user modify taiuser account-valid yes
```

d. WebSEAL 구성 파일 *webseal_install_directory*/etc/webseald-default.conf에서 다음 매개변수를 설정하십시오.

```
basicauth-dummy-passwd=webseal_userid_passwd
```

예를 들어, Tivoli Access Manager에 taiuser/ptaiuser를 설정하는 경우 다음 매개변수를 설정하십시오. `basicauth-dummy-passwd = ptaiuser`

형식 기반 인증을 사용하는 경우에는 다음 매개변수를 설정하십시오.

`forms-auth=both`

`ba-auth=none`

3. 서버에서 TAI++ 인터셉터를 사용 가능하게 하여 제품 Application Server에 대해 WebSEAL을 구성하십시오.
   a. 관리 콘솔에서 **글로벌 보안 → 인증 메커니즘 및 만기**를 선택하십시오.
   b. **웹 및 SIP 보안**을 펼친 다음 **신뢰 연관**을 선택하십시오. 선택란에 체크하고 **적용**을 클릭하십시오.
   c. **인터셉터 → TAMTrustAssociationInterceptorPlus → 사용자 정의 특성**을 선택하고 다음 특성을 추가하십시오.

이름	값
com.ibm.websphere.security.webseal.configURL	${WAS_INSTALL_ROOT}/java/jre/PdPerm.properties
com.ibm.websphere.security.webseal.id	iv-creds
com.ibm.websphere.security.webseal.loginId	taiuser(taiuser/ptaiuser 사용자가 Tivoli Access Manager에서 작성된 경우)

   d. 셀을 다시 시작하십시오.
   e. 클라이언트에 액세스하려면 https://*webseal_server_name*:*webseal_port*/*junction name*/*web_uri_for_client*로 이동하십시오.
4. 사용자 환경에 대해 호스트 연결을 구성하여 Business Space 위젯을 표시하십시오. 가상 호스트 연결과 투명 호스트 연결 중 어느 것을 사용하는지에 따라 다음 단계 중 하나를 완료하십시오.
   - 가상 호스트 연결을 사용하는 경우에는 가상 호스트 연결을 작성하십시오. 가상 호스트 연결을 작성하면 별도의 연결을 작성할 필요가 없습니다.
     a. 가상 호스트가 구성되었는지 확인하십시오. 가상 호스트 연결은 호스트, 포트 번호 및 전달 주소가 대상 호스트와 일치합니다. URL 필터링이 발생하지 않으며, 일치하는 모든 요청이 대상 호스트로 전달됩니다.
     b. 동일한 가상 호스트에 대해 다음 응용프로그램이 사용 가능한지 확인하십시오. Business Space와 함께 사용 중인 제품에 따라 응용프로그램의 전부 또는 일부가 있을 수 있습니다.
        - BPMAdministrationWidgets_*nodename_servername*(WebSphere Enterprise Service Bus 및 WebSphere Process Server의 경우)
        - BusinessSpaceHelpEAR_*nodename_servername*(모든 제품의 경우)
        - BSpaceEAR_*nodename_servername*(모든 제품의 경우)

- BSpaceWebformsEnabler_*nodename_servername*(모든 제품의 경우)
- HumanTaskManagementWidgets_*nodename_servername*(WebSphere Process Server 및 WebSphere Business Monitor의 경우)
- REST Services Gateway(모든 제품의 경우)
- REST Services Gateway Dmgr(WebSphere Enterprise Service Bus 및 WebSphere Process Server의 경우)
- mm.was_*nodename_servername*(모든 제품의 경우)
- WBMDashboardWeb_*nodename_servername*(WebSphere Business Monitor의 경우)
- wesbWidgets_*nodename_servername*(WebSphere Enterprise Service Bus의 경우)
- widgets_busleader_*nodename_servername*(WebSphere Business Compass의 경우)
- widgets_pubserver_*nodename_servername*(WebSphere Business Compass의 경우)
- widgets_fabric_*nodename_servername*(WebSphere Business Services Fabric의 경우)

주: 이 응용프로그램은 Business Space에 필요한 응용프로그램만 다룹니다. Tivoli Access Manager WebSEAL을 사용하는 Business Space가 아닌 시나리오에 대해서는 목록에 다른 응용프로그램을 추가해야 합니다.

c. pdadmin을 사용하여 다음 명령을 실행하십시오. `server task` *`webseal server`* `virtualhost create -t` *`transport`* `-h` *`target_host`* `[-p` *`port`*`]` `[-v` *`virtual_host_name`*`]` *`virtual_host_label`*

다음 정보를 사용하십시오.

- *webseal server*는 가상 호스트 항목을 작성할 WebSEAL 서버의 이름입니다.
- *transport*는 전송 유형입니다. 유효한 입력은 `tcp`, `ssl`, `tcpproxy` 및 `sslproxy`입니다.
- *target_host*는 필수 응용프로그램의 호스트입니다.
- *virtual_host_name*는 HTTP 요청을 가상 호스트 연결에 일치시키는 데 사용됩니다. 값이 입력되지 않은 경우 기본적으로 대상 호스트 및 포트가 작성됩니다. 예를 들어, *virtual_host_name*을 `myvirthost.ibm.com:80`으로 설정하는 경우, WebSEAL은 `myvirthost.ibm.com:80`을 포함하는 URL을 일치시키고 pdadmin 명령에서 제공된 호스트로 라우트합니다.
- *virtual_host_label*은 WebSEAL의 항목을 식별하는 데 사용되는 레이블입니다. 이 레이블은 고유해야 합니다.

Business Space를 예상대로 실행하려면 전송 유형에 대해 ssl 및 tcp 항목을 작성해야 합니다. 동일한 가상 호스트 연결에서 SSL(Secure Sockets Layer)과 TCP(Transmission Control Protocol)를 둘 다 지원해야 하는 경우, -g *vhost_label* 옵션을 사용해야 합니다. 여기서 *vhost_label*은 구성을 공유할 원래 가상 호스트 레이블입니다. 이 옵션은 이전에 작성한 가상 호스트 연결(이전에 작성한 것. 여기서 *virtual_host_label*은 -g 옵션에 제공한 레이블과 일치함)을 찾아서 구성을 공유합니다. 두 번째 입력은 여전히 자체 *virtual_host_label*이 필요하지만 대상 호스트, 포트 및 기타 값을 공유할 수 있습니다. 이 -g 옵션을 제공하지 않으면 WebSEAL은 대상 호스트와 포트를 이전에 작성한 연결과 동일하게 보므로(이는 허용되지 않음) 두 번째 가상 호스트를 작성할 수 없습니다.

- 투명 호스트 연결을 사용하는 경우에는 각 제품의 위젯에 대해 일련의 투명 경로 연결을 작성하십시오.
  a. pdadmin을 사용하여 다음 명령을 실행하십시오. `server task *webseal server* create -t *transport type (ssl) or (tcp)* -x -h hostname *path*`

     예를 들어, `server task webseald-default create -t tcp -x -h monServer.ibm.com /BusinessSpace`를 입력하십시오.
  b. 사용자 제품에 대해 다음 컨텍스트 루트를 작성하십시오. 역방향 프록시 서버의 Business Space URL 맵핑.

5. 추가 구성 단계를 완료하여 브라우저 쿠키 및 가상 호스트에 대한 문제를 해결하십시오.
   a. Business Space 쿠키의 이름 바꾸기를 해결하려면 WebSEAL 구성 파일에 다음 컨텐츠를 추가하십시오.

      ```
      [preserve-cookie-names]

      name = com.ibm.bspace.UserName

      name = com.ibm.wbimonitor.UserName
      ```

   b. 옵션: 비기본 가상 호스트와 컨텍스트를 사용 중인 경우에는 Business Space 페이지에 대한 문제가 발생할 수 있습니다. 컨텍스트 루트에 -j 연결을 추가하여 Business Space의 JavaScript™ 다시 쓰기에서 연결을 중지해야 할 수도 있습니다. 다음 명령을 실행하십시오. `server task default-webseald create -f -h *hostname* -p *portnumber* -t tcp -b supply -c iv-user,iv-creds,iv-groups -x -s -j -J trailer/*root context*`

Business Space 슈퍼유저 역할 지정

Business Space에서 사용자를 슈퍼유저(또는 Business Space 관리자)로 지정할 수 있습니다. 슈퍼유저는 모든 영역 및 페이지를 보고 편집하고 삭제할 수 있으며 템플리트를 관리하고 작성할 수 있고 소유자 ID를 변경하여 영역의 소유권을 변경할 수 있습니다.

시작하기 전에

Business Space를 구성할 때 관리 보안이 사용되는 경우 그룹 및 슈퍼유저에 대해 다음 정보를 고려하십시오.

- 특수 사용자 그룹인 **관리자**에 속하는 사용자는 기본적으로 슈퍼유저 역할이 있습니다. 따라서 슈퍼유저 역할 지정은 사용자 그룹 멤버십에 의해 처리됩니다.
- 단일 서버 환경에서 Business Space 서버는 기본 사용자 레지스트리에 **관리자** 사용자 그룹을 작성합니다. 구성하는 동안 제공되는 관리자 ID는 이 그룹의 구성원으로 자동 추가됩니다.
- Network Deployment 환경에서 **관리자** 사용자 그룹은 자동으로 작성되지 않습니다. `createSuperUser.py` 스크립트를 사용하여 사용자 그룹을 작성하고 기본 사용자 레지스트리에서 그룹에 구성원을 추가하십시오.
- 기본 사용자 레지스트리 대신 다른 사용자 레지스트리(예: LDAP)가 사용되거나, 기본 사용자 레지스트리가 사용되지만 **관리자** 사용자 그룹을 사용하고 싶지 않은 경우에는 Business Space 슈퍼유저로 사용할 사용자 그룹을 식별해야 합니다. 제공하는 값은 사용자 레지스트리에서 이해할 수 있습니다. 예를 들어, LDAP의 경우에는 `cn=administrators,dc=company,dc=com`과 같은 이름을 제공할 수 있습니다. 이 사용자 그룹 식별에 대한 자세한 정보는 다음에 수행할 사항 절에서 관리자 그룹 변경에 대한 지시사항을 참조하십시오.
- WebSphere Portal의 Business Space에서 기본 그룹 **wpsadmins**는 슈퍼유저 역할에도 사용됩니다. 이 그룹의 구성원은 Business Space의 슈퍼유저 역할이 부여됩니다.

  주: WebSphere Portal에서 Business Space를 사용하려는 경우, 보안이 사용 가능해야 합니다.

Business Space를 구성할 때 관리 보안이 사용되지 않는 경우에는 특수 사용자 ID **BPMAdministrator**에만 Business Space 슈퍼유저 역할이 있습니다.

Network Deployment 환경이 있는 경우 `createSuperUser.py` 스크립트를 실행하여 슈퍼유저 역할을 작성(사용자 그룹을 작성하고 구성원을 추가)해야 합니다. 스크립트를 실행하기 전에 다음 단계를 완료하십시오.

- 기본 **관리자** 그룹 이름이 변경되지 않았는지 확인하십시오.
- 사용자 레지스트리에 대해 기본 저장소를 사용하십시오.

- Business Space가 설치된 프로파일의 Business Space 환경에 대해 서버 또는 Deployment Manager를 시작하십시오.

프로시저

1. 사용자에게 슈퍼유저 역할을 지정하는 *install_root*₩BusinessSpace₩scripts₩createSuperUser.py 스크립트를 찾으십시오.
2. 명령 프롬프트를 열고 디렉토리를 *profile_root*₩bin으로 변경하십시오. 여기서 *profile_root*는 Business Space가 설치된 프로파일의 디렉토리를 나타냅니다.
3. 다음 명령을 입력하십시오. wsadmin -lang jython -f *install_root*₩BusinessSpace₩scripts₩createSuperUser.py *user_short_name password* 여기서 *user_short_name*은 가상 구성원 관리자(VMM)에서 사용자의 고유 ID이고 *password*는 사용자의 VMM 암호입니다. VMM에 해당 사용자가 있는 경우, 사용자가 관리자 그룹에 추가됩니다.

   주: 경로에 공백이 있는 경우(예: *install_root*가 My install dir인 경우), 경로 이름을 따옴표 안에 넣어야 합니다. 예를 들어, 다음 명령을 입력하십시오. wsadmin -lang jython -f "₩My install dir₩BusinessSpace₩scripts₩createSuperUser.py" *user_short_name_in_VMM*.

다음에 수행할 작업

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

이름이 **관리자**인 기본 특수 사용자 그룹을 변경할 수 있습니다. 다음 단계를 수행하여 현재 그룹 이름을 확인하거나 다른 이름으로 변경하십시오.

구성 파일에서 com.ibm.mashups.adminGroupName 메트릭의 값을 검사하십시오.

- 독립형 서버에서 *profile_root*₩BusinessSpace₩*node_name*₩*server_name*₩mm.runtime.prof₩config₩ConfigService.properties 또는
- 클러스터에서 *deployment_manager_profile_root*₩BusinessSpace₩*cluster_name*₩mm.runtime.prof₩config₩ConfigService.properties.

관리 그룹을 변경하려면 독립형 서버에서 다음 단계를 수행하십시오.

1. 구성 파일 *profile_root*₩BusinessSpace₩*node_name*₩*server_name*₩mm.runtime.prof₩config₩ConfigService.properties에서 com.ibm.mashups.adminGroupName 메트릭을 수정하십시오.

2. 프로파일의 wsadmin 환경에서 updatePropertyConfig 명령 $AdminTask updatePropertyConfig {-serverName *server_name* -nodeName *node_name* -propertyFileName "*profile_root*₩BusinessSpace₩*node_name*₩*server_name*₩mm.runtime.prof₩config₩ConfigService.properties" -prefix "Mashups_"} 를 실행하고 $AdminConfig save를 실행하십시오.
3. 서버를 다시 시작하십시오.

관리 그룹을 변경하려면 클러스터에서 다음 단계를 수행하십시오.

1. 구성 파일 *deployment_manager_profile_root*₩BusinessSpace₩*cluster_name*₩mm.runtime.prof₩config₩ConfigService.properties에서 com.ibm.mashups.adminGroupName 메트릭을 수정하십시오.
2. 전개 환경 프로파일의 wsadmin 환경에서 updatePropertyConfig 명령 $AdminTask updatePropertyConfig {-clusterName *cluster_name* -propertyFileName "*deployment_manager_profile_root*₩BusinessSpace₩*cluster_name*₩mm.runtime.prof₩config₩ConfigService.properties" -prefix "Mashups_"} 를 실행하고 $AdminConfig save를 실행하십시오.
3. Deployment Manager를 다시 시작하십시오.

보안이 사용 가능하지 않은 경우 슈퍼유저를 변경하려면 독립형 서버에서 다음 단계를 수행하십시오.

1. 구성 파일 *profile_root*₩BusinessSpace₩*node_name*₩*server_name*₩mm.runtime.prof₩config₩ConfigService.properties에서 noSecurityAdminInternalUserOnly 메트릭을 수정하십시오.
2. 프로파일의 wsadmin 환경에서 updatePropertyConfig 명령 $AdminTask updatePropertyConfig {-serverName *server_name* -nodeName *node_name* -propertyFileName "*profile_root*₩BusinessSpace₩*node_name*₩*server_name*₩mm.runtime.prof₩config₩ConfigService.properties" -prefix "Mashups_"} 를 실행하고 $AdminConfig save를 실행하십시오.
3. 서버를 다시 시작하십시오.

보안이 사용 가능하지 않은 경우 슈퍼유저를 변경하려면 클러스터에서 다음 단계를 수행하십시오.

1. 구성 파일 *deployment_manager_profile_root*₩BusinessSpace₩*cluster_name*

₩mm.runtime.prof₩config₩ConfigService.properties에서 noSecurityAdminInternalUserOnly 메트릭을 수정하십시오.

2. 전개 환경 프로파일의 wsadmin 환경에서 updatePropertyConfig 명령 $AdminTask updatePropertyConfig {-clusterName *cluster_name* -propertyFileName "*deployment_manager_profile_root*₩BusinessSpace₩*cluster_name* ₩mm.runtime.prof₩config₩ConfigService.properties" -prefix "Mashups_"} 를 실행하고 $AdminConfig save를 실행하십시오.
3. Deployment Manager를 다시 시작하십시오.

엔드 투 엔드 보안 작성

잠재적인 엔드 투 엔드 보안 시나리오가 많이 있습니다. 이들 각각에 대한 보안 단계가 서로 다를 수 있습니다. 필요한 보안 옵션이 있는 전형적인 여러 가지 시나리오가 제공됩니다.

시작하기 전에

이 시나리오는 모두 관리 보안이 강화된 것으로 가정합니다.

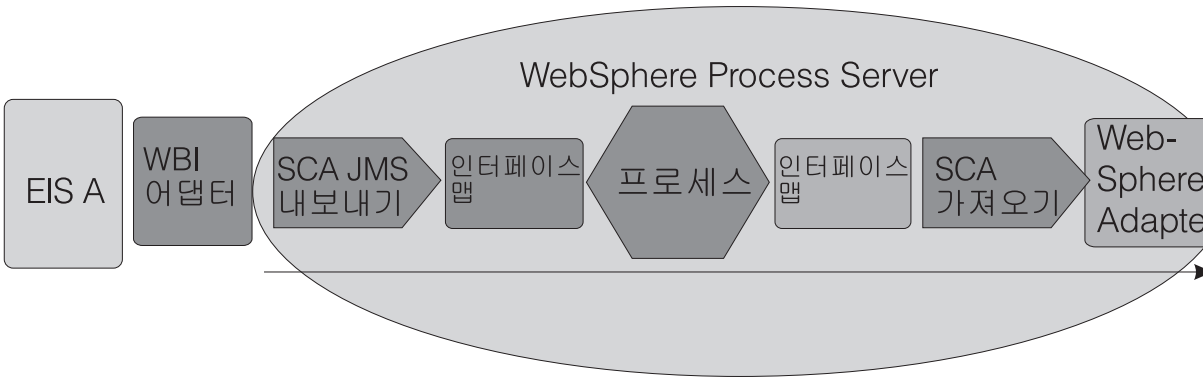
프로시저

1. 이 절에 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

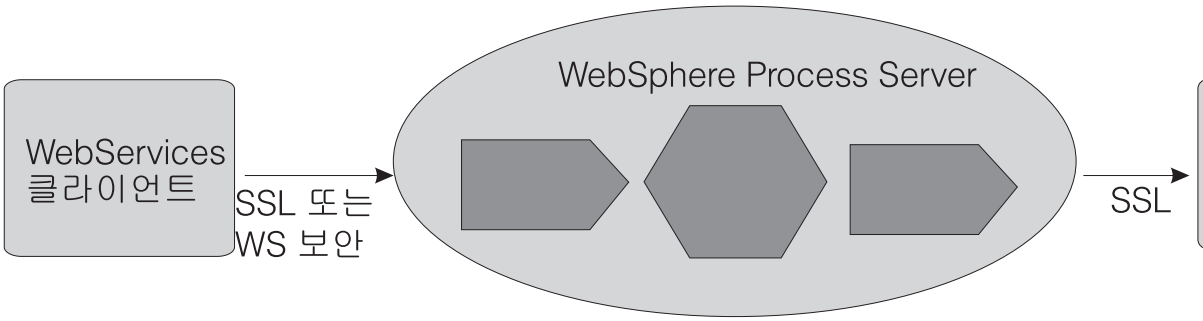
인바운드 요청이 WebSphere Business Integration Adapter에서 나옵니다. SCA(Service Component Architecture)는 SCA 내보내기를 기반으로 하는 인터페이스 맵을 호출합니다. 요청이 프로세스 컴포넌트 및 두 번째 인터페이스 맵을 거친 후 WebSphere Adapter를 통해 두 번째 EIS(B)로 전달됩니다. 이는 하나의 컴포넌트가 다음 컴포넌트의 메소드를 호출하는 SCA 호출입니다.



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

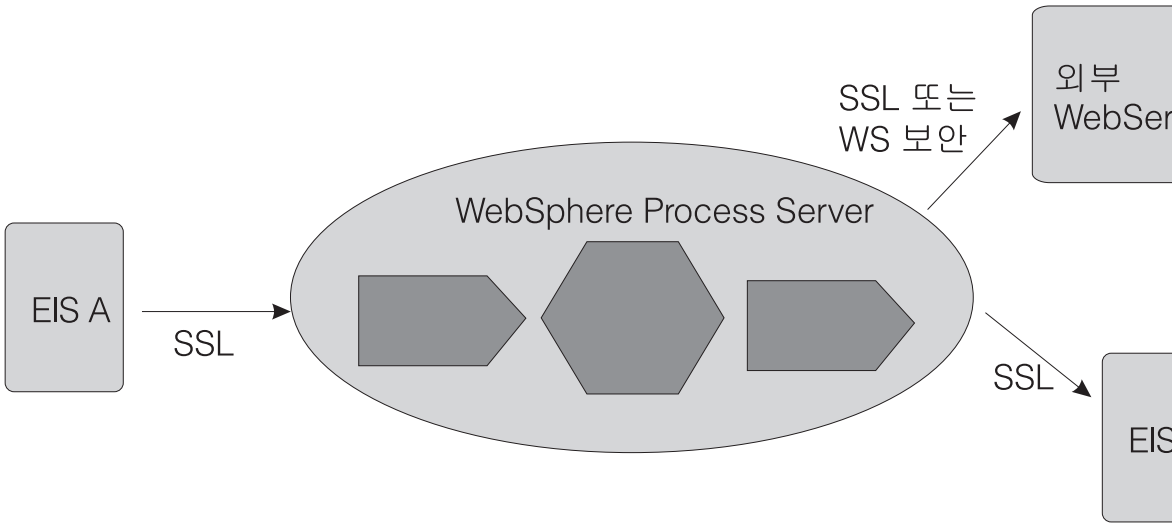
이 시나리오에서 웹 서비스 클라이언트가 WebSphere Process Server 컴포넌트를 호출합니다. 요청이 어댑터에 의해 EIS로 전달되기 전에 WebSphere Process Server 환경의 여러 컴포넌트를 거칩니다.



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 보안화할 수 있습니다. SSL이 파이프 전체를 보안화하는 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.



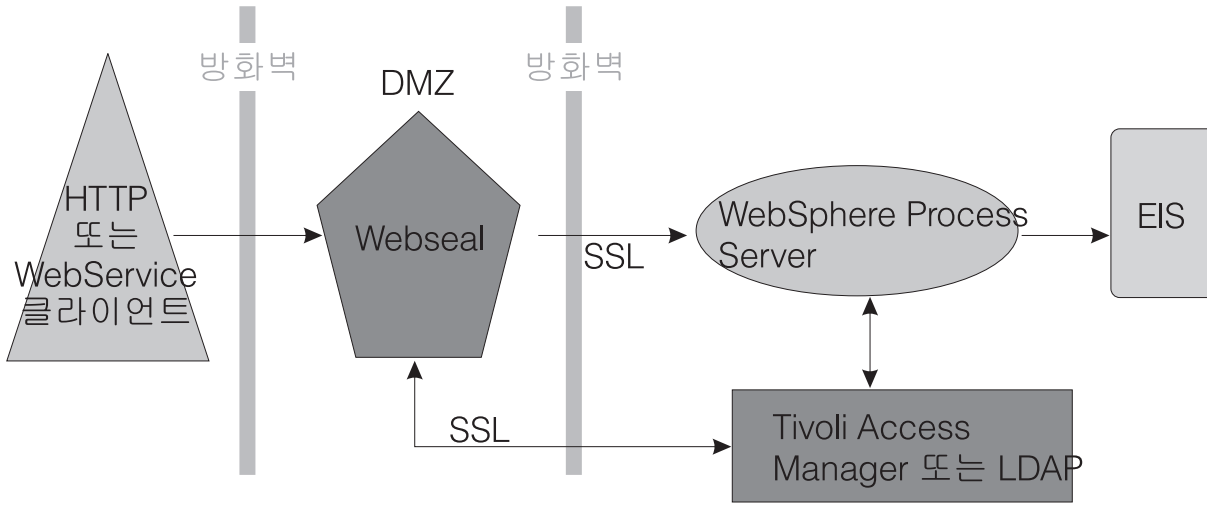
인바운드 웹 서비스 요청의 경우 HTTP 기본 인증 또는 WS-Security 인증을 사용하여 외부 웹 서비스를 SSL 클라이언트로 인증할 수 있습니다. LTPACallBackHandler를 콜백 메커니즘으로 사용하여 현재 RunAs주제에서 usernameToken을 추출하십시오. WebSphere Process Server와 대상 웹 서비스 사이에서 WS-Security를 사용하여 데이터 프라이버시 및 무결성을 보장할 수 있습니다.

웹 응용프로그램 - WebSphere Process Server에 대한 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.


방화벽
DMZ
방화벽
HTTP
또는
WebService
클라이언트
Webseal
SSL
WebSphere Process
Server
EIS
SSL
Tivoli Access
Manager 또는 LDAP