WebSphere® Process Server for Multiplatforms

Versión 6.1.0

Seguridad de las aplicaciones y sus entornos

WebSphere® Process Server for Multiplatforms

Versión 6.1.0

Seguridad de las aplicaciones y sus entornos

Nota

Antes de utilizar esta información, asegúrese de leer la información general de la sección Avisos al final de este documento.

31 de marzo de 2008

Esta edición se aplica a la versión 6, release 1, modificación 0 de WebSphere Process Server for Multiplatforms (número de producto 5724-L01) y a todos los releases y las modificaciones subsiguientes hasta que se indique lo contrario en nuevas ediciones.

Para enviar comentarios sobre este documento, envíe un mensaje de correo electrónico a doc-comments@us.ibm.com. Esperamos sus comentarios.

Cuando se envía información a IBM, se otorga a IBM un derecho no exclusivo de utilizar o distribuir la información del modo que estime apropiado sin incurrir por ello en ninguna obligación con el remitente.

Contenido

Protección de aplicaciones y su entorno

La seguridad del entorno de WebSphere Process Server y sus aplicaciones es muy importante.

1. La información presentada en este tema está disponible en formato Adobe PDF en el enlace siguiente: Documentación de WebSphere Process Server (en formato PDF).
2. Los mapas de información de Business Process Management en IBM developerWorks organizan la información disponible sobre WebSphere Process Server y los demás miembros de la misma familia de productos.

Estos documentos son complementarios de la documentación de seguridad básica que se encuentra en el Centro de información de WebSphere Application Server Network Deployment, versión 6 y específicamente en la Documentación de seguridad de WebSphere Application Server Network Deployment, versión 6.

La seguridad de los datos y los procesos es una cuestión crítica. La seguridad de WebSphere Process Server se basa en la seguridad de WebSphere Application Server versión 6.1. Consulte el Centro de información de WebSphere Application Server Network Deployment, versión 6 para obtener información detallada sobre seguridad.

Visión general

La seguridad de los datos y los procesos es una cuestión crítica.

La seguridad de WebSphere Process Server está basada en la seguridad de WebSphere Application Server versión 6.1. Consulte el Centro de información de WebSphere Application Server Network Deployment, versión 6 para obtener información detallada sobre la seguridad.

Las tareas de seguridad pueden dividirse generalmente entre aquellas relacionadas con la administración de seguridad en el entorno de WebSphere Process Server y las relacionadas con las aplicaciones que se ejecutan en WebSphere Process Server. La seguridad del entorno del servidor es fundamental para la seguridad de las aplicaciones y por tanto las dos partes no deberían plantearse de forma aislada.

La seguridad del entorno implica habilitar la seguridad administrativa, habilitar la seguridad de las aplicaciones, crear perfiles con seguridad y restringir el acceso a las funciones críticas a los usuarios seleccionados.

Hay varios aspectos para proteger una aplicación. Estos son:

- **"Autenticación" en la página 36**; un usuario o un proceso que invoca una aplicación debe autenticarse.
- **"Control de acceso" en la página 38**; ¿el usuario autenticado tiene permiso para realizar la operación?
- **"Integridad y privacidad de los datos" en la página 38**; los datos a los que accede una aplicación deben estar protegidos para que ninguna parte no autorizada pueda verlos o modificarlos de alguna manera.

- **"Inicio de sesión individual" en la página 39**; inicio de sesión individual que permite al usuario proporcionar los datos de autenticación una sola vez y después pasar esta información de autenticación a los componentes en sentido descendente.

El resto de este apartado detalla las consideraciones de seguridad en diversas fases de la operación de WebSphere Process Server.

Consideraciones de seguridad específicas de WebSphere Process Server

La seguridad de WebSphere Process Server se basa en la seguridad de WebSphere Application Server 6.1. Se listan las consideraciones específicas de WebSphere Process Server.

Características de seguridad de WebSphere Process Server

- El panel de la consola administrativa de la seguridad de Business Integration Security es exclusivo de WebSphere Process Server. Se puede llegar al mismo, expandiendo **Seguridad** y pulsando **Seguridad de Business Integrity**. Este panel permite a los usuarios asignar identidades específicas de su registro de usuarios a los alias de autenticación. Asimismo, puede administrar los valores de seguridad de Business Process Choreographer en este panel.
- La seguridad de las aplicaciones está activada por omisión en WebSphere Process Server. Esto no es así en WebSphere Application Server.
- Hay un conjunto de roles de seguridad específicos de los componentes.

Iniciación a la seguridad

La seguridad es una consideración integral al planificar la instalación de WebSphere Process Server, al desarrollar y desplegar aplicaciones y en la ejecución cotidiana del servidor de procesos.

Acerca de esta tarea

Para mantener la seguridad de los datos importantes, debe proteger el entorno del servidor de procesos y las aplicaciones que despliega en dicho entorno.

Procedimiento

1. Considere la seguridad al instalar WebSphere Process Server. Consulte "Instalación de WebSphere Process Server: consideraciones sobre la seguridad" en la página 3
2. Compruebe que la seguridad está activada para la instalación standalone o del entorno de despliegue.
   a. Compruebe que la "Seguridad administrativa" en la página 9 está activada. La seguridad administrativa está activada por omisión.
   b. Compruebe que la "Seguridad de aplicaciones" en la página 10 está activada. La seguridad de las aplicaciones está activada por omisión.
   c. Si es necesario, active "Seguridad Java 2" en la página 10.
   d. Utilice el Asistente de configuración de seguridad en la consola administrativa para configurar las opciones de seguridad.
   e. Configure un mecanismo de seguridad seguro y un repositorio de cuentas de usuario.

f. Asigne nombres de usuario y contraseñas a los alias de autenticación de Business Integration que sean importantes.
g. Asigne usuarios a los roles de seguridad administrativa adecuados.

3. Proteja las aplicaciones que despliegue en el entorno del servidor de procesos.
   a. Desarrolle las aplicaciones en WebSphere Integration Developer utilizando todas las características de seguridad apropiadas.
   b. Despliegue las aplicaciones en el entorno de WebSphere Process Server.
   c. Asigne usuarios o grupos a los roles de seguridad adecuados para controlar el acceso a la aplicación recién desplegada.
   d. Mantenga la seguridad del entorno de WebSphere Process Server.

Instalación de WebSphere Process Server: consideraciones sobre la seguridad

Complete estas tareas para implementar la seguridad antes, durante y después de la instalación de WebSphere Process Server.

Acerca de esta tarea

Estas tareas deben realizarse durante la instalación de WebSphere Process Server.

Procedimiento

1. Proteja el entorno antes de la instalación.

   Los mandatos necesarios para instalar WebSphere Process Server con la seguridad adecuada están en función del sistema operativo. Para obtener información detallada sobre los pasos a realizar antes de instalar, consulte el tema **Protección del entorno antes de la instalación** en el Centro de información de WebSphere Application Server.

   i5/OS Los mandatos necesarios para instalar WebSphere Process Server con la seguridad adecuada están en función del sistema operativo. ara obtener información detallada sobre los pasos a realizar antes de instalar, consulte el tema **Preparación de sistemas i5/OS para la instalación** en las tareas relacionadas.

2. Prepare el sistema operativo para realizar la instalación de WebSphere Process Server.

   Este paso incluye información sobre cómo preparar los distintos sistemas operativos para la instalación de WebSphere Process Server. Para obtener información detallada sobre la preparación del sistema operativo para la instalación, consulte el tema **Preparación del sistema operativo para instalar el producto** en el Centro de información de WebSphere Application Server.

3. Proteja el entorno después de la instalación.

   Esta tarea proporciona información sobre cómo proteger la información de contraseña después de instalar WebSphere Process Server. Para obtener información detallada sobre cómo proteger el entorno después de la instalación, consulte el tema **Protección del entorno después de la instalación** en el Centro de información de WebSphere Application Server.

Qué hacer a continuación

Cuando haya completado la instalación, podrá administrarse la seguridad desde la consola administrativa.

Tareas relacionadas

Preparación de sistemas i5/OS para la instalación

Obtenga más información sobre cómo preparar un sistema i5/OS para la instalación de WebSphere Process Server.

Información relacionada

Protección del entorno antes de la instalación

Preparación del sistema operativo para la instalación del producto

Protección del entorno después de la instalación

Información de autenticación proporcionada en el momento de la instalación

En los releases anteriores de WebSphere Process Server se le solicitaba diferente información de autenticación durante el proceso de instalación. Ahora, todos los componentes aceptan por omisión los credenciales administrativos que proporcione. Estos valores por omisión proporcionan seguridad básica, pero para mejorar la seguridad de su instalación debe utilizar la consola administrativa para configurar los diferentes componentes de WebSphere Process Server de modo que tengan identidades de seguridad adecuadas.

Cuando crea un perfil de WebSphere Process Server, se le solicitará un nombre de usuario y una contraseña si mantiene seleccionado **Habilitar la seguridad administrativa**. Esta identidad se utiliza como un valor por omisión para todos los componentes subyacentes. Una vez más, debe configurar estas identidades después de crear el perfil para poder reforzar su seguridad.

Varios componentes de WebSphere Process Server utilizan alias de autenticación. Estos alias se utilizan para autenticar el componente de tiempo de ejecución para que acceda a las bases de datos y motores de mensajería. Estos alias se pueden modificar en el panel de seguridad de Business Integration de la consola administrativa.

Creación de perfiles de WebSphere Process Server con seguridad

Cuando se crea un perfil de WebSphere Process Server se utilizan valores predeterminados para las credenciales de seguridad. Debe configurar estos valores de seguridad en la consola administrativa después de crear el perfil.

Acerca de esta tarea

Cuando se crea un perfil de WebSphere Process Server hay tres componentes de WebSphere Process Server que toman por omisión la identidad de usuario del administrador.

Estos componentes son:

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

Las identidades asociadas con estos componentes se utilizan para crear alias de autenticación que son necesarios cuando se habilita la seguridad. Es importante cambiar estas identidades por los usuarios adecuados del depósito de cuentas.

Procedimiento

1. En la consola administrativa, vaya al panel de Seguridad de Business Integration. Expanda Seguridad y pulse Seguridad de Business Integration.
2. Para cada alias de autenticación de Service Component Architecture, Business Process Choreographer y Common Event Infrastructure, proporcione un nombre de usuario y una contraseña adecuados para utilizarlos como alias de autenticación. Seleccione el alias que desea cambiar; para ello, marque el recuadro de selección en la columna Seleccionar, pulse Editar y, en el panel siguiente, proporcione el nombre de usuario y la contraseña que se van a utilizar como alias de autenticación para este componente. Las credenciales que proporcione deben existir en el repositorio de cuentas de usuario que utilice.

Qué hacer a continuación

En temas posteriores se proporciona información adicional sobre la gestión de alias de autenticación.

Tareas relacionadas

"Modificación de alias de autenticación" en la página 37
Tal vez tenga que modificar los alias de autenticación existentes.

Configuración de la seguridad de WebSphere Process Server para un servidor autónomo

Siga los enlaces siguientes para obtener información acerca de cómo configurar la instalación autónoma de WebSphere Process Server.

Protección de una instalación autónoma de WebSphere Process Server

La seguridad en el entorno de WebSphere Process Server se controla desde la consola administrativa. Los usuarios con privilegios suficientes pueden activar y desactivar toda la seguridad de las aplicaciones desde la consola administrativa. Por ese motivo es crítico proteger el entorno antes de desplegar aplicaciones seguras.

Antes de empezar

Antes de iniciar estas tareas, deberá instalar WebSphere Process Server y verificar la instalación.

Acerca de esta tarea

El entorno de WebSphere Process Server se define en un perfil. Abra la consola administrativa para el perfil que desea proteger. Inicie la sesión en la consola utilizando cualquier identidad de usuario; mientras no se proteja el perfil, se aceptará cualquier nombre de usuario.

Procedimiento

1. Asegúrese de que está activada la seguridad administrativa. "Habilitación de la seguridad administrativa" en la página 7.
2. Asegúrese de que está activada la seguridad de aplicaciones. "Protección de aplicaciones en WebSphere Process Server" en la página 35.

3. Añada usuarios o grupo al rol de administración. Puede conceder derechos administrativos a usuarios individuales o a un grupo de usuarios siguiendo los **Roles de usuario administrativo** o **Roles de grupo administrativo**, respectivamente.
4. Seleccione el depósito de cuentas de usuario que desea utilizar.

   La tabla siguiente describe las opciones de registro de usuario y las acciones necesarias para seleccionar y configurar un registro de usuario.

Registro de usuario	Acción
Depósitos federados	Especifique este valor para gestionar los perfiles de varios depósitos bajo un solo reino. El reino puede constar de identidades en: • El repositorio basado en archivos que incorporado en el sistema, • Uno o más repositorios externos, • Tanto el repositorio basado en archivos incorporado como uno o más repositorios externos. **Nota:** Sólo un usuario con privilegios de administrador puede ver la configuración de repositorios federados. Para obtener más información, consulte Gestión del reino en una configuración de depósito federado.
Sistema operativo local	Registro de usuario por omisión. Para obtener detalles sobre cómo configurar el registro de cuenta de usuario, consulte “Configuración del depósito de cuentas de usuario” en la página 12.
Registro LDAP autónomo	Para configurar LDAP como su registro de usuario, siga las instrucciones de Configuración de LDAP (Lightweight Directory Access Protocol) como registro de usuario.
Registro de usuarios autónomo	Para obtener detalles sobre cómo configurar el registro de cuenta de usuario, consulte “Configuración del depósito de cuentas de usuario” en la página 12.

5. Aplique estos cambios.

   Pulse el botón **Aplicar** de la parte inferior del panel.
6. Vaya al panel Seguridad de Business Integration. Expanda **Seguridad** y pulse **Seguridad de Business Integration**.
7. Proporcione las identidades de usuario adecuadas para los alias de autenticación de la lista. La credencial que proporcione debe existir en el depósito de cuentas de usuario que esté empleando.
8. En el mismo panel puede configurar la seguridad de Business Process Choreographer.

   Establezca las correlaciones de rol de usuario de Business Process Choreographer para Business Flow Manager y Human Task Manager:

   • **Administrador**: Nombre o nombres de usuario y/o de grupo para el rol de administrador de Business Flow Manager y de Human Task Manager. Los usuarios asignados a este rol tienen todos los privilegios.

- **Supervisor** : Nombre o nombres de usuario y/o de grupo para el rol de supervisor de Business Flow Manager y de Human Task Manager. Los usuarios asignados a este rol pueden ver las propiedades de todos los objetos de procesos de empresa y de tarea.

Los alias de autenticación de Business Process Choreographer se pueden configurar en cada destino de despliegue en el que se haya instalado Business Process Choreographer. Se incluyen los alias de autenticación siguientes:

- **Autenticación de la API de JMS**: autenticación del bean controlado por mensajes de Business Flow Manager para procesar llamadas asíncronas a la API.
- **Autenticación de usuario de escalada**: autenticación del bean controlado por mensajes de Human Task Manager para procesar llamadas asíncronas a la API.

9. Aplique estos cambios.

   Pulse el botón **Aplicar** de la parte inferior del panel.

10. Guarde los cambios en la configuración local.

    Pulse **Guardar** en el panel del mensaje.

11. Si es necesario, detenga y reinicie el servidor.

    Si fuese necesario reiniciar el servidor, aparecerá un mensaje en la consola administrativa indicándolo.

Resultado

La próxima vez que inicie la sesión en la consola administrativa, deberá proporcionar un nombre de usuario y contraseña válidos.

Cada perfil que cree deberá protegerse de esta manera Se puede utilizar la identidad de usuario del administrador del sistema en varios lugares durante la instalación y la configuración del entorno. Se recomienda sustituir esta identidad con las credenciales de usuario adecuadas desde el depósito de cuentas de usuario para todas las funciones excepto para las funciones principales de seguridad. Utilice el panel **Seguridad de Business Integration** en la consola administrativa para administrar las identidades y los alias.

Tareas relacionadas

Utilización de las herramientas de verificación de instalación de WebSphere Process Server

Utilice las herramientas de verificación de la instalación para verificar que la instalación de WebSphere Process Server y que la creación de perfiles de servidor autónomo o de gestor de despliegue ha sido satisfactoria. Un *perfil* está formado por archivos que definen el entorno de ejecución para un gestor de despliegue o un servidor. Verifique los archivos básicos del producto con la herramienta de suma de comprobación installver_wbi. Verifique cada perfil con la herramienta de prueba de verificación de instalación (IVT).

Habilitación de la seguridad administrativa

El primer paso para proteger su entorno y sus aplicaciones de WebSphere Process Server es habilitar la seguridad administrativa.

Antes de empezar

Instale WebSphere Process Server y verifique la instalación antes de comenzar estas tareas.

Acerca de esta tarea

Abra la consola administrativa para el perfil que desea proteger. Inicie la sesión en la consola utilizando cualquier identidad de usuario; mientras no se proteja el perfil, se aceptará cualquier nombre de usuario.

Procedimiento

1. Abra el panel de seguridad administrativa en la consola administrativa.

   Expanda **Seguridad** y pulse **Proteger la administración, las aplicaciones y la infraestructura**.
2. Habilite la seguridad administrativa.

   Seleccione **Habilitar seguridad administrativa**.
3. Opcional: Si es necesario, fuerce la seguridad de Java 2.

   Seleccione **Utilice la seguridad de Java 2 para restringir el acceso de las aplicaciones a los recursos locales** para forzar la comprobación de permisos de seguridad de Java 2.

   Cuando está habilitada la seguridad de Java, las aplicaciones que requieren más permisos de seguridad de Java,2 que los otorgados en la política por omisión, pueden no funcionar correctamente hasta que se otorguen los permisos necesarios en el archivo app.policy o was.policy de la aplicación. Las aplicaciones que no tienen todos los permisos generan excepciones AccessControl. Para obtener más información sobre la seguridad de Java 2, consulte el tema sobre Configuración de archivos de política de seguridad de Java 2 en el Centro de información de WebSphere Application Server.

   Nota: Las actualizaciones del archivo app.policy sólo se aplican a las aplicaciones empresariales del nodo al que pertenece app.policy.

   a. Opcional: Seleccione **Avisar si se otorgan permisos personalizados a las aplicaciones**. El archivo filter.policy contiene una lista de permisos que la aplicación no debe tener según la especificación J2EE 1.3. Si una aplicación se instala con un permiso especificado en este archivo de política y la opción está habilitada, se emite un aviso. El valor por omisión es habilitado.
   b. Opcional: Seleccione **Restringir el acceso a los datos de autenticación de recursos**. Habilite esta opción si necesita restringir el acceso de las aplicaciones a datos importantes de autenticación de correlaciones JCA (Java Connector Architecture).
4. Aplique estos cambios.

   Pulse el botón **Aplicar** de la parte inferior del panel.
5. Guarde los cambios en la configuración local.

   Pulse **Guardar** en el panel del mensaje.
6. Si es necesario, detenga y reinicie el servidor.

   Si fuese necesario reiniciar el servidor, aparecerá un mensaje en la consola administrativa indicándolo.

Qué hacer a continuación

Debe activar la seguridad administrativa para cada perfil que cree.

Información relacionada

Configuración de archivos de política de seguridad de Java 2

Seguridad administrativa

La seguridad administrativa determina si se utiliza la seguridad o no, el tipo de registro en el que se lleva a cabo la autenticación y otros valores, muchos de los cuales actúan como valores por omisión. Es necesario planificarla debidamente, debido a que si se habilita incorrectamente la seguridad administrativa puede quedar bloqueado el uso de la consola administrativa o hacer que el servidor finalice de forma anómala.

La seguridad administrativa puede considerarse un ″gran conmutador″ que activa una amplia gama de valores de seguridad para WebSphere Process Server. Los valores se pueden especificar pero no entrarán en vigor hasta que se active la seguridad administrativa. Los valores incluyen la autenticación de los usuarios, el uso de SSL (Secure Sockets Layer) y la opción del depósito de cuentas de usuario. En particular, la seguridad de las aplicaciones, incluida la autenticación y la autorización basada en roles, no se aplica a menos que esté activa la seguridad administrativa. Por omisión, la seguridad administrativa está habilitada.

La seguridad administrativa representa la configuración de seguridad que entra en vigor para todo el dominio de seguridad. Un dominio de seguridad consta de todos los servidores que están configurados con el mismo nombre de dominio de registro de usuarios. En algunos casos, el dominio puede ser el nombre de la máquina o un registro del sistema operativo local. En este caso, todos los servidores de aplicaciones deben residir en la misma máquina física. En otros casos, el dominio puede ser el nombre de la máquina o un registro LDAP (Lightweight Directory Access Protocol) autónomo.

Se da soporte a una configuración de varios nodos debido a que puede acceder de forma remota a los registros de usuarios que soportan el protocolo LDAP. Por lo tanto, puede habilitar la autenticación desde cualquier lugar.

El requisito básico para un dominio de seguridad es que el ID de acceso que devuelve el registro o el depósito desde un servidor dentro del dominio de seguridad es el mismo ID de acceso que se devuelve desde el registro o repositorio en cualquier otro servidor, dentro del mismo dominio de seguridad. El ID de acceso es el identificador exclusivo de un usuario y se utiliza durante la autorización para determinar si se permite el acceso al recurso.

La configuración de la seguridad administrativa se aplica a cada servidor dentro del dominio de seguridad.

¿Por qué se ha de activar la seguridad administrativa?

Al activar la seguridad administrativa se activan los valores que protegen su servidor de usuarios no autorizados. La seguridad administrativa se activa por omisión durante la creación de perfiles. Es posible que existan algunos entornos en los que no es necesaria la seguridad, por ejemplo, en un sistema de desarrollo. En estos sistemas puede optar por inhabilitar la seguridad administrativa. No obstante, en la mayor parte de entornos debe impedir que los usuarios no autorizados accedan a la consola administrativa y a sus aplicaciones de empresa. La seguridad administrativa debe estar habilitada para limitar el acceso.

¿Qué protege la seguridad administrativa?

La configuración de la seguridad administrativa para un dominio de seguridad requiere configurar las tecnologías siguientes:

- Autenticación de clientes HTTP

- Autenticación de clientes IIOP
- Seguridad de la consola administrativa
- Seguridad de nombres
- Uso de transportes SSL
- Comprobaciones de autorización basada en roles para servlets, enterprise beans y MBeans
- Propagación de identidades (RunAs)
- El registro de usuarios común
- El mecanismo de autenticación
- Otra información de seguridad que definen el comportamiento de un dominio de seguridad es:
  - El protocolo de autenticación, la seguridad RMI/IIOP (Remote Method Invocation over the Internet Inter-ORB Protocol)
  - Otros atributos diferentes

Seguridad de aplicaciones

La seguridad de las aplicaciones habilita la seguridad de las aplicaciones de su entorno. Este tipo de seguridad proporciona el aislamiento de las aplicaciones y los requisitos para autenticar a los usuarios de las aplicaciones.

En los releases anteriores de WebSphere Process Server, cuando un usuario habilitaba la seguridad global, se habilitaba la seguridad administrativa y la de las aplicaciones. la noción de la seguridad global se ha dividido ahora en la seguridad administrativa y la seguridad de las aplicaciones, cada una de las cuales se puede habilitar por separado.

La seguridad administrativa está habilitada por omisión. La seguridad de las aplicaciones también está habilitada por omisión. La seguridad de las aplicaciones sólo entra en vigor cuando se ha habilitado la seguridad administrativa.

Seguridad Java 2

La seguridad Java 2 proporciona un mecanismo de control de acceso basado en políticas de alta precisión que aumenta la integridad general del sistema ya que comprueba los permisos antes de permitir el acceso a determinados recursos protegidos del sistema. Seguridad Java 2 vigila el acceso a los recursos del sistema como, por ejemplo, E/S de archivos, sockets y propiedades. La seguridad J2EE (Java 2 Platform, Enterprise Edition) acceden a recursos Web como, por ejemplo, servlets, archivos JSP (JavaServer Pages) y métodos EJB (Enterprise JavaBeans).

La seguridad de WebSphere Process Server incluye las tecnologías siguientes:

- Java 2 Security Manager
- JAAS (Java Authentication and Authorization Service)
- Entradas de datos de autenticación de Java 2 Connector
- Autorización basada en roles J2EE
- Configuración SSL (Secure Sockets Layer)

Dado que la seguridad Java 2 es relativamente nueva, es posible que muchas aplicaciones existentes o incluso nuevas no estén preparadas para el modelo de programación de control de acceso de alta precisión que puede aplicar la seguridad de Java 2. Los administradores deben comprender las posibles consecuencias que tiene habilitar la seguridad de Java 2 si las aplicaciones no están preparadas para

la seguridad de Java 2. La seguridad deJava 2 impone nuevos requisitos para los desarrolladores de aplicaciones y para los administradores.

Consulte la información relacionada para obtener más detalles acerca de la seguridad de Java 2.

Información relacionada

Seguridad Java 2

Configuración de un repositorio de cuentas de usuario

Los nombres de usuario y contraseñas de los usuarios registrados se almacenan en un repositorio de cuentas de usuario. Puede utilizar el repositorio de cuentas de usuario del sistema operativo local (valor predeterminado), el LDAP (Lightweight Directory Access Protocol), repositorios federados o un repositorio de cuentas personalizado.

Acerca de esta tarea

El repositorio de cuentas de usuario es el registro de usuarios y grupos que consulta el mecanismo de autenticación cuando realiza la autenticación. Elija un repositorio de cuentas de usuario en la consola administrativa.

Nota: Windows Linux UNIX i5/OS En un entorno de Network Deployment debe utilizar LDAP como registro de usuario.

Procedimiento

1. Vaya al panel Proteger la administración, las aplicaciones y la infraestructura de la consola administrativa. Expanda **Seguridad** y pulse **Proteger la administración, las aplicaciones y la infraestructura**.
2. Seleccione el registro de usuario que desea utilizar.

   La tabla siguiente describe las opciones de registro de usuario y las acciones necesarias para seleccionar y configurar un registro de usuario.

Registro de usuario	Acción
Repositorios federados	Especifique este valor para gestionar perfiles en diversos repositorios de un solo reino. El reino puede consistir en identidades en: • El repositorio basado en archivos que se genera en el sistema. • Uno o varios repositorios externos. • El repositorio incorporado basado en archivos y uno o varios repositorios externos. **Nota:** Solo un usuario con privilegios de administrador puede ver la configuración de los repositorios federados. Consulte Gestión del reino en una configuración de depósito federado para obtener más información.

Registro de usuario	Acción
Sistema operativo local	Registro de usuario por omisión. En **Definiciones de reino disponibles**, seleccione **Sistema operativo local** y pulse **Configurar**. En la página Registro de usuario de sistema operativo local, proporcione un nombre de usuario y una contraseña. Este nombre de usuario se utiliza como la identidad del servidor. El usuario se añade automáticamente al rol **Administrador**. **Nota:** No utilice el sistema operativo local como registro de usuario en un entorno de Network Deployment.
LDAP (Lightweight Directory Access Protocol)	Siga las instrucciones del apartado Configuración de LDAP (Lightweight Directory Access Protocol) como registro de usuario para configurar LDAP como su registro de usuario.
Registro de usuario personalizado	Elija un repositorio de cuentas personalizado y configúrelo según sus necesidades.
Tivoli Access Manager	**Nota:** Esta opción no está disponible a través de la consola administrativa y debe configurarse mediante el mandato wsadmin.

Configuración del depósito de cuentas de usuario

Puede configurar el depósito de cuentas de usuario utilizando la consola administrativa. Puede elegir una identidad de usuario de servidor o generar automáticamente una identidad de servidor.

Acerca de esta tarea

Puede configurar el depósito de cuentas de usuario utilizando la consola administrativa. Puede elegir permitir que WebSphere Process Server genere automáticamente una identidad de usuario de servidor o puede especificar una desde el depósito de cuentas de usuario que está utilizando. Esta última opción mejora la capacidad de auditoría de las acciones administrativas.

Procedimiento

1. Desde la consola administrativa, abra la página de configuración **Depósito de cuentas de usuario** para el registro de usuarios.

   Expanda **Seguridad**, pulse **Proteger la administración, las aplicaciones y la infraestructura** y seleccione el registro de usuarios que está utilizando en el menú **Definiciones del reino disponibles**. Pulse **Configurar**.
2. Opcional: Especifique un **Nombre de usuario administrativo primario**. Especifique el nombre de un usuario con privilegios administrativos que esté definido en el sistema operativo local. El nombre de usuario se utiliza para iniciar la sesión en la consola administrativa cuando está habilitada la seguridad administrativa.
3. Seleccione la opción **Identidad de servidor generada automáticamente** o **Identidad de servidor que se almacena en el depósito**.

   Si selecciona la opción **Identidad de servidor que se almacena en el depósito**, especifique la información siguiente:

   - ID de usuario del servidor o usuario administrativo.

- Contraseña asociada a este usuario.

Esta identidad debe existir en el depósito de cuentas de usuario.

Configuración de WebSphere Process Server para utilizar Tivoli Access Manager como repositorio de cuentas de usuario

Para utilizar Tivoli Access Manager como repositorio de cuentas de usuario, debe configurarlo con el mandato wsadmin, fuera de la consola administrativa.

Acerca de esta tarea

Tivoli Access Manager se puede utilizar como repositorio de cuentas de usuario. No se puede configurar en la consola administrativa y debe utilizarse el mandato wsadmin. Consulte el tema del centro de información de WebSphere Application Server: Cómo propagar la política de seguridad de aplicaciones instaladas al proveedor de JACC utilizando scripts wsadmin.

Configuración de LDAP (Lightweight Directory Access Protocol) como registro de usuario

Por omisión, el registro de usuario es el registro del sistema operativo local. Si lo prefiere, utilice un LDAP (Lightweight Directory Access Protocol) como registro de usuario. En un entorno de Network Deployment debe utilizar LDAP.

Acerca de esta tarea

En esta tarea se da por sentado que tiene la seguridad global activada.

Procedimiento

1. Inicie WebSphere Process Server.
2. Inicie la consola administrativa.
3. Abra la página de configuración del Registro de usuario LDAP.

   Expanda **Seguridad**, pulse **Proteger la administración, las aplicaciones y la infraestructura** y seleccione **LDAP** en el menú **Definiciones del reino disponibles**. Pulse **Configurar**.
4. Especifique un nombre de usuario válido en el campo **Nombre de usuario administrativo primario**. Este valor es el nombre de un usuario con privilegios administrativos definido en el registro. Este nombre de usuario se utiliza para acceder a la consola administrativa o se utiliza con el mandato wsadmin.
5. Pulse **Aplicar**.
6. Seleccione la opción **Identidad de servidor generada automáticamente** o **Identidad de servidor que se almacena en el depósito**.

   Si selecciona la opción **Identidad de servidor que se almacena en el depósito**, especifique la información siguiente:

   - ID de usuario del servidor o usuario administrativo.
   - Contraseña asociada a este usuario.

   Aunque este ID no es el ID de usuario del administrador LDAP, sin embargo, la entrada debe existir en LDAP.
7. Elija el tipo de LDAP que utiliza.

   En la lista **Tipo**, elija el LDAP específico que desea utilizar como registro de usuario.
8. Especifique el nombre del sistema donde reside LDAP.

En el campo **Sistema principal**, especifique el nombre del servidor donde reside LDAP.

9. Especifique el número de puerto en el que escucha LDAP.

   En el campo **Puerto**, especifique el número de puerto en el que escucha el servidor LDAP.

10. Especifique el **Nombre distinguido básico**.

    Este valor especifica el nombre distinguido básico del servicio de directorios, que indica el punto de partida para búsquedas LDAP del servicio de directorios.

    Para fines de autorización, este campo es sensible a las mayúsculas y minúsculas. Esta especificación implica que si se recibe un símbolo (por ejemplo, de otra célula o Domino Server) el nombre distinguido (DN) básico del servidor debe coincidir exactamente con el DN básico de la otra célula o Domino Servidor. Si no es necesario tener en cuenta la sensibilidad a mayúsculas y minúsculas para la autorización, habilite el campo **Ignorar mayúsculas/minúsculas**. Este campo es necesario para todos los directorios LDAP excepto para Domino Directory, donde este campo es opcional.

11. Deje los valores por omisión en los parámetros restantes y confirme los cambios.

    Pulse **Aceptar**.

Inicio y detención del servidor

Cuando está habilitada la seguridad administrativa, para concluir el servidor es necesario proporcionar el nombre de usuario y contraseña apropiados. El servidor se iniciará sin autenticación, pero la autenticación es necesaria para acceder a la consola administrativa.

Antes de empezar

La seguridad administrativa debe estar habilitada.

Procedimiento

1. Inicie el servidor.

   La siguiente tabla describe las opciones para iniciar el servidor.

Iniciar el servidor	Detalles
Desde la interfaz de usuario Primeros pasos	Pulse Iniciar el servidor.
Desde la línea de mandatos	Entre: • Windows **En las plataformas Windows:** startserver *nombre_servidor* • Linux UNIX **En las plataformas Linux y UNIX:** startserver.sh *nombre_servidor* • i5/OS **En System i (desde la línea de mandatos de QShell):** startserver *nombre_servidor* desde el indicador de mandatos en el directorio *dir_instalación*/bin.

Nota: No es necesario que proporcione un nombre de usuario y contraseña para iniciar el servidor. Sin embargo, tendrá que autenticarse si intenta iniciar la consola administrativa o realizar otras tareas administrativas.
El servidor se inicia o se devuelve un mensaje de error.

2. Detenga el servidor.

   La siguiente tabla describe las opciones para detener el servidor.

Detener el servidor	Detalles
Desde la interfaz de usuario Primeros pasos	Pulse Detener el servidor y proporcione un nombre de usuario y contraseña válidos cuando se soliciten. El nombre de usuario que proporciona debe estar en el rol operador o administrador.
Desde la línea de mandatos	Entre: • Windows **En las plataformas Windows:** stopserver *nombre_servidor* -profileName *nombre_perfil* -username *nombre_usuario* -password *contraseña* • Linux UNIX **En las plataformas Linux y UNIX:** stopserver.sh *nombre_servidor* -profileName *nombre_perfil* -username *nombre_usuario* -password *contraseña* • i5/OS **En System i (desde la línea de mandatos de QShell):** stopserver *nombre_servidor* -profileName *nombre_perfil* -username *nombre_usuario* -password *contraseña* desde el indicador de mandatos en el directorio *dir_instalación*/bin. El nombre de usuario proporcionado debe ser un miembro del rol operador o administrador.

Nota: Es necesario que proporcione un nombre de usuario y contraseña para detener el servidor.
Si el nombre de usuario y contraseña que proporcione son miembros del rol operador o administrador, el servidor se detendrá.

3. Compruebe que el servidor se haya detenido correctamente

   La siguiente tabla describe las opciones para verificar que el servidor se ha detenido correctamente.

Compruebe que el servidor se haya detenido correctamente	Detalles
Desde la interfaz de usuario	La ventana de salida de Primeros pasos muestra detalles de los resultados de su petición.
Desde la línea de mandatos	El resultado de su petición se muestra en la ventana de mandatos desde donde haya realizado la petición.

Roles de seguridad de administración

Se proporcionan roles de seguridad de administración como parte de la instalación de WebSphere Process Server.

Se proporcionan siete roles como parte de la consola administrativa. Estos roles otorgan permisos de distintos rangos de funcionalidad en la consola administrativa. Cuando está habilitada la seguridad administrativa, debe correlacionarse un usuario con uno de estos cuatro roles para poder acceder a la consola administrativa.

El primer usuario que inicia la sesión en el servidor después de la instalación se añade al rol administrador.

Tabla 1. Roles de seguridad de administración

Rol de seguridad de administración	Descripción
Supervisor	Los miembros del rol supervisor pueden visualizar la configuración de WebSphere Process Server y el estado actual del servidor.
Configurador	Los miembros del rol configurador pueden editar la configuración de WebSphere Process Server.
Operador	Los miembros del rol operador tienen privilegios de supervisor y la capacidad de modificar el estado de tiempo de ejecución, a saber, iniciar y detener el servidor.
Administrador	El rol administrador es una combinación de los roles configurador y operador además de privilegios adicionales otorgados únicamente al rol administrador. Entre ellos se incluyen: • Modificación del ID y la contraseña de usuario del servidor • Correlación de usuarios y grupos con el rol administrador También dispone de los permisos necesarios para acceder a información importante como: • Contraseña LTPA • Claves .
Adminsecuritymanager	Sólo los usuarios que tienen concedido este rol pueden correlaciones usuarios con roles administrativos. Asimismo, cuando se utiliza la seguridad administrativa de alta precisión, sólo los usuarios que tienen concedido este rol pueden gestionar los grupos de autorización. Consulte los roles administrativos, para obtener más información.
Desplegador (Deployer)	Los usuarios que tienen este rol puede realizar acciones de configuración y operaciones de tiempo de ejecución en las aplicaciones.

Tabla 1. Roles de seguridad de administración (continuación)

Rol de seguridad de administración	Descripción
iscadmins	Este rol sólo está disponible para los usuarios de la consola administrativa y no para los usuarios wsadmin. Los usuarios que tienen este rol poseen privilegios administrativos para gestionar usuarios y grupos en depósitos federados. Por ejemplo, un usuario con el rol iscadmins puede realizar las tareas siguientes: • Crear, actualizar o suprimir usuarios en la configuración de depósitos federados. • Crear, actualizar o suprimir grupos en la configuración de depósitos federados.

El ID de servidor que se especifica al habilitar la seguridad administrativa, se correlaciona automáticamente con el rol administrador. Los usuarios o grupos pueden añadirse o eliminarse de los roles de administración en cualquier momento mediante la consola administrativa de WebSphere Process Server. Sin embargo, es necesario reiniciar el servidor para que los cambios entren en vigor. Lo más adecuado es correlacionar un grupo o grupos, en lugar de usuarios específicos, con roles de administración porque de esta forma la administración es más fácil y flexible. Si se correlaciona un grupo con un rol de administración, la adición o eliminación de usuarios en el grupo se produce fuera de WebSphere Process Server y no es necesario reiniciar el servidor para que el cambio entre en vigor.

Además de correlacionar usuarios o grupos, también puede correlacionarse un sujeto especial con los roles de administración. Un sujeto especial es una generalización de una clase de usuarios concreta. El sujeto especial AllAuthenticated significa que la comprobación de acceso del rol de administración garantiza que el usuario que realiza la petición esté al menos autenticado. El sujeto especial Everyone significa que cualquiera pueda realizar la acción, autenticado o no, como si la seguridad no estuviese habilitada.

Seguridad por omisión de los componentes instalados

Varios componentes importantes de WebSphere Process Server tienen información de seguridad por omisión. En esta información se incluyen los alias con los que se correlacionan los usuarios por omisión y los roles de seguridad a los que se debe otorgar acceso a los usuarios para poder invocar estos componentes.

Finalidad

Varios de los componentes importantes de WebSphere Process Server utilizan alias predefinidos para autenticarse en motores de mensajería y bases de datos. Durante la creación de perfiles, a estos alias de autenticación se les asigna un valor por omisión con el ID de usuario y la contraseña del administrador principal. Debe configurar estos alias de modo que se correspondan con otros usuarios del depósito de cuentas de usuario..

Alias de autenticación de Business Process Choreographer

Los procesos de empresa tienen los siguientes alias de autenticación. Modifique estos alias mediante la consola administrativa.

Los alias de la Tabla 2 se utilizan para invocar los componentes independientemente de la identidad del usuario que invoque.

Tabla 2. Alias de autenticación asociados con procesos de empresa.

Alias	Descripción	Información
BPEAuthDataAliasJMS_*nodo_servidor*	Se utiliza para autenticar con el motor de mensajería.	Entre el nombre de usuario y la contraseña en el panel de configuración de Business Process Choreographer del asistente de perfiles.
BPEAuthDataAlias*TipoBD_nodo_servidor*	Se utiliza para autenticar con bases de datos.	Configure la base de datos mediante los scripts proporcionados.

La Tabla 3 describe los roles RunAs creados para los procesos de empresa.

Tabla 3. Roles RunAs asociados con procesos de empresa.

Rol RunAs	Descripción	Información
JMSAPIUser	Se utiliza por MDB de API de BFM JMS en bpecontainer.ear.	Entre el nombre de usuario y la contraseña en el panel de configuración de Business Process Choreographer del asistente de perfiles.
EscalationUser	Se utiliza por MDB task.ear.	Entre el nombre de usuario y la contraseña en el panel de configuración de Business Process Choreographer del asistente de perfiles.

El nombre de usuario suministrado se añade al rol RunAs.

Alias de autenticación de Common Event Infrastructure

Common Event Infrastructure tiene los siguientes alias de autenticación. Modifique estos alias mediante la consola administrativa.

Los alias de la Tabla 4 se utilizan para invocar los componentes independientemente de la identidad del usuario que invoque.

Tabla 4. Alias de autenticación asociados con Common Event Infrastructure.

Alias	Descripción	Información
CommonEventInfrastructure JMSAuthAlias Se ha añadido un carácter de espacio a esta entrada para permitir que entre en la celda de la tabla. El nombre de alias real no contiene un carácter de espacio.	Se utiliza para autenticar con el motor de mensajería.	Entre el nombre de usuario y la contraseña en el panel de configuración de Common Event Infrastructure del asistente de perfiles.

Tabla 4. Alias de autenticación asociados con Common Event Infrastructure. (continuación)

Alias	Descripción	Información
EventAuthAlias*TipoBD*	Se utiliza para autenticar con bases de datos.	Entre el nombre de usuario y la contraseña en el panel de configuración de Common Event Infrastructure del asistente de perfiles.

Alias de autenticación de SCA (Service Component Architecture)

La arquitectura de componentes de servicio (SCA) tiene los siguientes alias de autenticación. Modifique estos alias mediante la consola administrativa.

Los alias de la Tabla 5 se utilizan para invocar los componentes independientemente de la identidad del usuario que invoque.

Tabla 5. Alias de autenticación asociados con componentes SCA.

Alias	Descripción	Información
SCA_Auth_Alias	Se utiliza para autenticar con el motor de mensajería.	Entre el nombre de usuario y la contraseña en el panel de configuración de SCA del asistente de perfiles.

Control de acceso en aplicaciones de procesos de empresa y tareas de usuario

Los siguientes archivos EAR (Enterprise Archive) se instalan con control de acceso como parte de la instalación de Business Process Choreographer. Business Process Choreographer se instala como parte de la instalación de WebSphere Process Server. El gestor de tareas de usuario utiliza los roles para determinar las posibilidades del usuario en un sistema de producción.

Archivo EAR	Roles	Permiso por omisión	Notas
bpecontainer.ear	BPESystemAdministrator	Nombre de grupo entrado durante la instalación.	Tiene acceso a todos los procesos de empresa y a todas las operaciones.
bpecontainer.ear	BPESystemMonitor	Todos los usuarios autenticados.	Tiene acceso a operaciones de lectura.
task.ear	TaskSystemAdministrator	Nombre de grupo entrado durante la instalación.	Tiene acceso a todas las tareas de usuario.
task.ear	TaskSystemMonitor	Todos los usuarios autenticados.	Tiene acceso a operaciones de lectura.
Bpcexplorer.ear	WebClientUser	Todos los usuarios autenticados.	Puede acceder a Business Process Choreographer Explorer.

Control de acceso en aplicaciones de Common Event Infrastructure

El siguiente archivo EAR (Enterprise Archive) se instala con control de acceso como parte de la instalación de Common Event Infrastructure. Common Event Infrastructure se instala como parte de la instalación de WebSphere Process Server.

El archivo EventServer.ear es el único archivo EAR instalado como parte de la instalación de Common Event Infrastructure.

Roles	Permiso por omisión
eventAdministrator	Todos los usuarios autenticados.
eventConsumer	Todos los usuarios autenticados.
eventUpdater	Todos los usuarios autenticados.
eventCreator	Todos los usuarios autenticados.
catalogAdministrator	Todos los usuarios autenticados.
catalogReader	Todos los usuarios autenticados.

Configuración de la seguridad de WebSphere Process Server para un servidor del entorno de despliegue

Siga los enlaces siguientes para obtener información acerca de cómo configurar la seguridad de una instalación del entorno de despliegue de WebSphere Process Server.

Protección de un entorno de despliegue de WebSphere Process Server

La seguridad en el entorno de WebSphere Process Server se controla desde la consola administrativa. Los usuarios con privilegios suficientes pueden activar y desactivar toda la seguridad de las aplicaciones desde la consola administrativa. Por ese motivo es crítico proteger el entorno antes de desplegar aplicaciones seguras.

Antes de empezar

Antes de iniciar estas tareas, deberá instalar WebSphere Process Server y verificar la instalación.

Acerca de esta tarea

El entorno de WebSphere Process Server se define en un perfil. Abra la consola administrativa para el perfil que desea proteger. Inicie la sesión en la consola utilizando cualquier identidad de usuario; mientras no se proteja el perfil, se aceptará cualquier nombre de usuario.

Procedimiento

1. Compruebe que la seguridad administrativa esté activada. “Habilitación de la seguridad administrativa” en la página 7.
2. Compruebe que la seguridad de aplicaciones esté activada. “Protección de aplicaciones en WebSphere Process Server” en la página 35.

3. Añada usuarios o grupos al rol administrativo. Puede otorgar derechos administrativos a usuarios individuales o a un grupo de usuarios; para ello, siga los **Roles de usuario administrativo** o **Roles de grupo administrativo**, respectivamente.
4. Seleccione el repositorio de cuentas de usuario que desea utilizar.

   La tabla siguiente describe las opciones de registro de usuario y las acciones necesarias para seleccionar y configurar un registro de usuario.

Registro de usuario	Acción
Repositorios federados	Especifique este valor para gestionar perfiles en diversos repositorios de un solo reino. El reino puede consistir en identidades en: • El repositorio basado en archivos que se genera en el sistema. • Uno o varios repositorios externos. • El repositorio incorporado basado en archivos y uno o varios repositorios externos. **Nota:** Solo un usuario con privilegios de administrador puede ver la configuración de los repositorios federados. Consulte Gestión del reino en una configuración de depósito federado para obtener más información.
Sistema operativo local	Registro de usuario por omisión. Consulte "Configuración del depósito de cuentas de usuario" en la página 12 para ver información detallada sobre cómo configurar el registro de cuentas de usuario.
Registro LDAP autónomo	Siga las instrucciones del apartado Configuración de LDAP (Lightweight Directory Access Protocol) como registro de usuario para configurar LDAP como su registro de usuario.
Registro personalizado autónomo	Consulte "Configuración del depósito de cuentas de usuario" en la página 12 para ver información detallada sobre cómo configurar el registro de cuentas de usuario.

5. Aplique estos cambios.

   Pulse el botón **Aplicar** de la parte inferior del panel.
6. Vaya al panel de Seguridad de Business Integration. Expanda **Seguridad** y pulse **Seguridad de Business Integration**.
7. Proporcione las identidades de usuario adecuadas para los alias de autenticación que se listan. La credencial que proporcione debe existir en el repositorio de cuentas de usuario que emplee. Es importante para la seguridad del sistema que elija identidades de usuario adecuadas para actuar como alias de autenticación.
8. En el mismo panel puede configurar la seguridad para Business Process Choreographer.

   Establezca las correlaciones de roles de usuario de Business Process Choreographer para Business Flow Manager y Human Task Manager:

- **Administrador**: nombre(s) de usuario y/o nombre(s) de grupo para el rol de administrador de Business Flow y Human Task. Los usuarios asignados a este rol tienen todos los privilegios.
- **Supervisor**: nombre(s) de usuario y/o nombre(s) de grupo para el rol de supervisor de Business Flow y Human Task. Los usuarios asignados a este rol pueden ver las propiedades de todos los objetos de tarea y procesos de empresa.

Los alias de autenticación de Business Process Choreographer pueden configurarse para cada destino de despliegue donde se haya instalado Business Process Choreographer. Se listan los siguientes alias de autenticación:

- **Autenticación de API de JMS**: autenticación para el bean controlado por mensajes de Business Flow Manager para procesar llamadas a API asíncronas.
- **Autenticación de usuario de escalada**: autenticación para el bean controlado por mensajes de Human Task Manager para procesar llamadas a API asíncronas.

9. Aplique estos cambios.

   Pulse el botón **Aplicar** de la parte inferior del panel.
10. Guarde los cambios en la configuración local.

    Pulse **Guardar** en el panel del mensaje.
11. Asegúrese de que la información de seguridad se ha propagado a los nodos de la célula.

    Expanda **Administración del sistema** en la consola administrativa y pulse **Nodos**. Pulse **Resincronización completa**.
12. Si es necesario, detenga y reinicie el servidor.

    Si fuese necesario reiniciar el servidor, aparecerá un mensaje en la consola administrativa indicándolo.

Resultado

La próxima vez que inicie la sesión en la consola administrativa, deberá proporcionar un nombre de usuario y contraseña válidos.

Los perfiles que se crean deben protegerse de esta manera. La identidad de usuario del administrador del sistema se puede haber utilizado en diversos lugares durante la instalación y configuración del entorno. Es aconsejable sustituir esta identidad por credenciales de usuario adecuadas desde el repositorio de cuentas de usuario para todas las funciones excepto para las de seguridad básica. Utilice el panel **Seguridad de Business Integration** de la consola administrativa para administrar también estas identidades y alias.

Tareas relacionadas

Utilización de las herramientas de verificación de instalación de WebSphere Process Server

Utilice las herramientas de verificación de la instalación para verificar que la instalación de WebSphere Process Server y que la creación de perfiles de servidor autónomo o de gestor de despliegue ha sido satisfactoria. Un *perfil* está formado por archivos que definen el entorno de ejecución para un gestor de despliegue o un servidor. Verifique los archivos básicos del producto con la herramienta de suma de comprobación installver_wbi. Verifique cada perfil con la herramienta de prueba de verificación de instalación (IVT).

Habilitación de la seguridad administrativa

El primer paso para proteger su entorno y sus aplicaciones de WebSphere Process Server es habilitar la seguridad administrativa.

Antes de empezar

Instale WebSphere Process Server y verifique la instalación antes de comenzar estas tareas.

Acerca de esta tarea

Abra la consola administrativa para el perfil que desea proteger. Inicie la sesión en la consola utilizando cualquier identidad de usuario; mientras no se proteja el perfil, se aceptará cualquier nombre de usuario.

Procedimiento

1. Abra el panel de seguridad administrativa en la consola administrativa.

   Expanda **Seguridad** y pulse **Proteger la administración, las aplicaciones y la infraestructura**.
2. Habilite la seguridad administrativa.

   Seleccione **Habilitar seguridad administrativa**.
3. Opcional: Si es necesario, fuerce la seguridad de Java 2.

   Seleccione **Utilice la seguridad de Java 2 para restringir el acceso de las aplicaciones a los recursos locales** para forzar la comprobación de permisos de seguridad de Java 2.

   Cuando está habilitada la seguridad de Java, las aplicaciones que requieren más permisos de seguridad de Java,2 que los otorgados en la política por omisión, pueden no funcionar correctamente hasta que se otorguen los permisos necesarios en el archivo app.policy o was.policy de la aplicación. Las aplicaciones que no tienen todos los permisos generan excepciones AccessControl. Para obtener más información sobre la seguridad de Java 2, consulte el tema sobre Configuración de archivos de política de seguridad de Java 2 en el Centro de información de WebSphere Application Server.

   Nota: Las actualizaciones del archivo app.policy sólo se aplican a las aplicaciones empresariales del nodo al que pertenece app.policy.

   a. Opcional: Seleccione **Avisar si se otorgan permisos personalizados a las aplicaciones**. El archivo filter.policy contiene una lista de permisos que la aplicación no debe tener según la especificación J2EE 1.3. Si una aplicación se instala con un permiso especificado en este archivo de política y la opción está habilitada, se emite un aviso. El valor por omisión es habilitado.
   b. Opcional: Seleccione **Restringir el acceso a los datos de autenticación de recursos**. Habilite esta opción si necesita restringir el acceso de las aplicaciones a datos importantes de autenticación de correlaciones JCA (Java Connector Architecture).
4. Aplique estos cambios.

   Pulse el botón **Aplicar** de la parte inferior del panel.
5. Guarde los cambios en la configuración local.

   Pulse **Guardar** en el panel del mensaje.
6. Si es necesario, detenga y reinicie el servidor.

   Si fuese necesario reiniciar el servidor, aparecerá un mensaje en la consola administrativa indicándolo.

Qué hacer a continuación

Debe activar la seguridad administrativa para cada perfil que cree.

Información relacionada

Configuración de archivos de política de seguridad de Java 2

Seguridad administrativa

La seguridad administrativa determina si se utiliza la seguridad o no, el tipo de registro en el que se lleva a cabo la autenticación y otros valores, muchos de los cuales actúan como valores por omisión. Es necesario planificarla debidamente, debido a que si se habilita incorrectamente la seguridad administrativa puede quedar bloqueado el uso de la consola administrativa o hacer que el servidor finalice de forma anómala.

La seguridad administrativa puede considerarse un ″gran conmutador″ que activa una amplia gama de valores de seguridad para WebSphere Process Server. Los valores se pueden especificar pero no entrarán en vigor hasta que se active la seguridad administrativa. Los valores incluyen la autenticación de los usuarios, el uso de SSL (Secure Sockets Layer) y la opción del depósito de cuentas de usuario. En particular, la seguridad de las aplicaciones, incluida la autenticación y la autorización basada en roles, no se aplica a menos que esté activa la seguridad administrativa. Por omisión, la seguridad administrativa está habilitada.

La seguridad administrativa representa la configuración de seguridad que entra en vigor para todo el dominio de seguridad. Un dominio de seguridad consta de todos los servidores que están configurados con el mismo nombre de dominio de registro de usuarios. En algunos casos, el dominio puede ser el nombre de la máquina o un registro del sistema operativo local. En este caso, todos los servidores de aplicaciones deben residir en la misma máquina física. En otros casos, el dominio puede ser el nombre de la máquina o un registro LDAP (Lightweight Directory Access Protocol) autónomo.

Se da soporte a una configuración de varios nodos debido a que puede acceder de forma remota a los registros de usuarios que soportan el protocolo LDAP. Por lo tanto, puede habilitar la autenticación desde cualquier lugar.

El requisito básico para un dominio de seguridad es que el ID de acceso que devuelve el registro o el depósito desde un servidor dentro del dominio de seguridad es el mismo ID de acceso que se devuelve desde el registro o repositorio en cualquier otro servidor, dentro del mismo dominio de seguridad. El ID de acceso es el identificador exclusivo de un usuario y se utiliza durante la autorización para determinar si se permite el acceso al recurso.

La configuración de la seguridad administrativa se aplica a cada servidor dentro del dominio de seguridad.

¿Por qué se ha de activar la seguridad administrativa?

Al activar la seguridad administrativa se activan los valores que protegen su servidor de usuarios no autorizados. La seguridad administrativa se activa por omisión durante la creación de perfiles. Es posible que existan algunos entornos en los que no es necesaria la seguridad, por ejemplo, en un sistema de desarrollo. En estos sistemas puede optar por inhabilitar la seguridad administrativa. No obstante, en la mayor parte de entornos debe impedir que los usuarios no autorizados accedan a la consola administrativa y a sus aplicaciones de empresa.

La seguridad administrativa debe estar habilitada para limitar el acceso.

¿Qué protege la seguridad administrativa?

La configuración de la seguridad administrativa para un dominio de seguridad requiere configurar las tecnologías siguientes:

- Autenticación de clientes HTTP
- Autenticación de clientes IIOP
- Seguridad de la consola administrativa
- Seguridad de nombres
- Uso de transportes SSL
- Comprobaciones de autorización basada en roles para servlets, enterprise beans y MBeans
- Propagación de identidades (RunAs)
- El registro de usuarios común
- El mecanismo de autenticación
- Otra información de seguridad que definen el comportamiento de un dominio de seguridad es:
  - El protocolo de autenticación, la seguridad RMI/IIOP (Remote Method Invocation over the Internet Inter-ORB Protocol)
  - Otros atributos diferentes

Seguridad de aplicaciones

La seguridad de las aplicaciones habilita la seguridad de las aplicaciones de su entorno. Este tipo de seguridad proporciona el aislamiento de las aplicaciones y los requisitos para autenticar a los usuarios de las aplicaciones.

En los releases anteriores de WebSphere Process Server, cuando un usuario habilitaba la seguridad global, se habilitaba la seguridad administrativa y la de las aplicaciones. la noción de la seguridad global se ha dividido ahora en la seguridad administrativa y la seguridad de las aplicaciones, cada una de las cuales se puede habilitar por separado.

La seguridad administrativa está habilitada por omisión. La seguridad de las aplicaciones también está habilitada por omisión. La seguridad de las aplicaciones sólo entra en vigor cuando se ha habilitado la seguridad administrativa.

Seguridad Java 2

La seguridad Java 2 proporciona un mecanismo de control de acceso basado en políticas de alta precisión que aumenta la integridad general del sistema ya que comprueba los permisos antes de permitir el acceso a determinados recursos protegidos del sistema. Seguridad Java 2 vigila el acceso a los recursos del sistema como, por ejemplo, E/S de archivos, sockets y propiedades. La seguridad J2EE (Java 2 Platform, Enterprise Edition) acceden a recursos Web como, por ejemplo, servlets, archivos JSP (JavaServer Pages) y métodos EJB (Enterprise JavaBeans).

La seguridad de WebSphere Process Server incluye las tecnologías siguientes:

- Java 2 Security Manager
- JAAS (Java Authentication and Authorization Service)
- Entradas de datos de autenticación de Java 2 Connector
- Autorización basada en roles J2EE
- Configuración SSL (Secure Sockets Layer)

Dado que la seguridad Java 2 es relativamente nueva, es posible que muchas aplicaciones existentes o incluso nuevas no estén preparadas para el modelo de programación de control de acceso de alta precisión que puede aplicar la seguridad de Java 2. Los administradores deben comprender las posibles consecuencias que tiene habilitar la seguridad de Java 2 si las aplicaciones no están preparadas para la seguridad de Java 2. La seguridad deJava 2 impone nuevos requisitos para los desarrolladores de aplicaciones y para los administradores.

Consulte la información relacionada para obtener más detalles acerca de la seguridad de Java 2.

Información relacionada

Seguridad Java 2

Configuración de un repositorio de cuentas de usuario

Los nombres de usuario y contraseñas de los usuarios registrados se almacenan en un repositorio de cuentas de usuario. Puede utilizar el repositorio de cuentas de usuario del sistema operativo local (valor predeterminado), el LDAP (Lightweight Directory Access Protocol), repositorios federados o un repositorio de cuentas personalizado.

Acerca de esta tarea

El repositorio de cuentas de usuario es el registro de usuarios y grupos que consulta el mecanismo de autenticación cuando realiza la autenticación. Elija un repositorio de cuentas de usuario en la consola administrativa.

Nota: Windows Linux UNIX i5/OS En un entorno de Network Deployment debe utilizar LDAP como registro de usuario.

Procedimiento

1. Vaya al panel Proteger la administración, las aplicaciones y la infraestructura de la consola administrativa. Expanda **Seguridad** y pulse **Proteger la administración, las aplicaciones y la infraestructura**.
2. Seleccione el registro de usuario que desea utilizar.

   La tabla siguiente describe las opciones de registro de usuario y las acciones necesarias para seleccionar y configurar un registro de usuario.

Registro de usuario	Acción
Repositorios federados	Especifique este valor para gestionar perfiles en diversos repositorios de un solo reino. El reino puede consistir en identidades en: • El repositorio basado en archivos que se genera en el sistema. • Uno o varios repositorios externos. • El repositorio incorporado basado en archivos y uno o varios repositorios externos. **Nota:** Solo un usuario con privilegios de administrador puede ver la configuración de los repositorios federados. Consulte Gestión del reino en una configuración de depósito federado para obtener más información.

Registro de usuario	Acción
Sistema operativo local	Registro de usuario por omisión. En **Definiciones de reino disponibles**, seleccione **Sistema operativo local** y pulse **Configurar**. En la página Registro de usuario de sistema operativo local, proporcione un nombre de usuario y una contraseña. Este nombre de usuario se utiliza como la identidad del servidor. El usuario se añade automáticamente al rol **Administrador**. **Nota:** No utilice el sistema operativo local como registro de usuario en un entorno de Network Deployment.
LDAP (Lightweight Directory Access Protocol)	Siga las instrucciones del apartado Configuración de LDAP (Lightweight Directory Access Protocol) como registro de usuario para configurar LDAP como su registro de usuario.
Registro de usuario personalizado	Elija un repositorio de cuentas personalizado y configúrelo según sus necesidades.
Tivoli Access Manager	**Nota:** Esta opción no está disponible a través de la consola administrativa y debe configurarse mediante el mandato wsadmin.

Configuración del depósito de cuentas de usuario

Puede configurar el depósito de cuentas de usuario utilizando la consola administrativa. Puede elegir una identidad de usuario de servidor o generar automáticamente una identidad de servidor.

Acerca de esta tarea

Puede configurar el depósito de cuentas de usuario utilizando la consola administrativa. Puede elegir permitir que WebSphere Process Server genere automáticamente una identidad de usuario de servidor o puede especificar una desde el depósito de cuentas de usuario que está utilizando. Esta última opción mejora la capacidad de auditoría de las acciones administrativas.

Procedimiento

1. Desde la consola administrativa, abra la página de configuración **Depósito de cuentas de usuario** para el registro de usuarios.

   Expanda **Seguridad**, pulse **Proteger la administración, las aplicaciones y la infraestructura** y seleccione el registro de usuarios que está utilizando en el menú **Definiciones del reino disponibles**. Pulse **Configurar**.
2. Opcional: Especifique un **Nombre de usuario administrativo primario**. Especifique el nombre de un usuario con privilegios administrativos que esté definido en el sistema operativo local. El nombre de usuario se utiliza para iniciar la sesión en la consola administrativa cuando está habilitada la seguridad administrativa.
3. Seleccione la opción **Identidad de servidor generada automáticamente** o **Identidad de servidor que se almacena en el depósito**.

   Si selecciona la opción **Identidad de servidor que se almacena en el depósito**, especifique la información siguiente:

   - ID de usuario del servidor o usuario administrativo.

- Contraseña asociada a este usuario.

Esta identidad debe existir en el depósito de cuentas de usuario.

Configuración de WebSphere Process Server para utilizar Tivoli Access Manager como repositorio de cuentas de usuario

Para utilizar Tivoli Access Manager como repositorio de cuentas de usuario, debe configurarlo con el mandato wsadmin, fuera de la consola administrativa.

Acerca de esta tarea

Tivoli Access Manager se puede utilizar como repositorio de cuentas de usuario. No se puede configurar en la consola administrativa y debe utilizarse el mandato wsadmin. Consulte el tema del centro de información de WebSphere Application Server: Cómo propagar la política de seguridad de aplicaciones instaladas al proveedor de JACC utilizando scripts wsadmin.

Configuración de LDAP (Lightweight Directory Access Protocol) como registro de usuario

Por omisión, el registro de usuario es el registro del sistema operativo local. Si lo prefiere, utilice un LDAP (Lightweight Directory Access Protocol) como registro de usuario. En un entorno de Network Deployment debe utilizar LDAP.

Acerca de esta tarea

En esta tarea se da por sentado que tiene la seguridad global activada.

Procedimiento

1. Inicie WebSphere Process Server.
2. Inicie la consola administrativa.
3. Abra la página de configuración del Registro de usuario LDAP.

   Expanda **Seguridad**, pulse **Proteger la administración, las aplicaciones y la infraestructura** y seleccione **LDAP** en el menú **Definiciones del reino disponibles**. Pulse **Configurar**.
4. Especifique un nombre de usuario válido en el campo **Nombre de usuario administrativo primario**. Este valor es el nombre de un usuario con privilegios administrativos definido en el registro. Este nombre de usuario se utiliza para acceder a la consola administrativa o se utiliza con el mandato wsadmin.
5. Pulse **Aplicar**.
6. Seleccione la opción **Identidad de servidor generada automáticamente** o **Identidad de servidor que se almacena en el depósito**.

   Si selecciona la opción **Identidad de servidor que se almacena en el depósito**, especifique la información siguiente:

   - ID de usuario del servidor o usuario administrativo.
   - Contraseña asociada a este usuario.

   Aunque este ID no es el ID de usuario del administrador LDAP, sin embargo, la entrada debe existir en LDAP.
7. Elija el tipo de LDAP que utiliza.

   En la lista **Tipo**, elija el LDAP específico que desea utilizar como registro de usuario.
8. Especifique el nombre del sistema donde reside LDAP.

En el campo **Sistema principal**, especifique el nombre del servidor donde reside LDAP.

9. Especifique el número de puerto en el que escucha LDAP.

   En el campo **Puerto**, especifique el número de puerto en el que escucha el servidor LDAP.

10. Especifique el **Nombre distinguido básico**.

    Este valor especifica el nombre distinguido básico del servicio de directorios, que indica el punto de partida para búsquedas LDAP del servicio de directorios.

    Para fines de autorización, este campo es sensible a las mayúsculas y minúsculas. Esta especificación implica que si se recibe un símbolo (por ejemplo, de otra célula o Domino Server) el nombre distinguido (DN) básico del servidor debe coincidir exactamente con el DN básico de la otra célula o Domino Servidor. Si no es necesario tener en cuenta la sensibilidad a mayúsculas y minúsculas para la autorización, habilite el campo **Ignorar mayúsculas/minúsculas**. Este campo es necesario para todos los directorios LDAP excepto para Domino Directory, donde este campo es opcional.

11. Deje los valores por omisión en los parámetros restantes y confirme los cambios.

    Pulse **Aceptar**.

Inicio y detención del servidor

Cuando está habilitada la seguridad administrativa, para concluir el servidor es necesario proporcionar el nombre de usuario y contraseña apropiados. El servidor se iniciará sin autenticación, pero la autenticación es necesaria para acceder a la consola administrativa.

Antes de empezar

La seguridad administrativa debe estar habilitada.

Procedimiento

1. Inicie el servidor.

   La siguiente tabla describe las opciones para iniciar el servidor.

Iniciar el servidor	Detalles
Desde la interfaz de usuario Primeros pasos	Pulse Iniciar el servidor.
Desde la línea de mandatos	Entre: • Windows **En las plataformas Windows:** startserver *nombre_servidor* • Linux UNIX **En las plataformas Linux y UNIX:** startserver.sh *nombre_servidor* • i5/OS **En System i (desde la línea de mandatos de QShell):** startserver *nombre_servidor* desde el indicador de mandatos en el directorio *dir_instalación*/bin.

Nota: No es necesario que proporcione un nombre de usuario y contraseña para iniciar el servidor. Sin embargo, tendrá que autenticarse si intenta iniciar la consola administrativa o realizar otras tareas administrativas.
El servidor se inicia o se devuelve un mensaje de error.

2. Detenga el servidor.

   La siguiente tabla describe las opciones para detener el servidor.

Detener el servidor	Detalles
Desde la interfaz de usuario Primeros pasos	Pulse Detener el servidor y proporcione un nombre de usuario y contraseña válidos cuando se soliciten. El nombre de usuario que proporciona debe estar en el rol operador o administrador.
Desde la línea de mandatos	Entre: • Windows **En las plataformas Windows:** stopserver *nombre_servidor* -profileName *nombre_perfil* -username *nombre_usuario* -password *contraseña* • Linux UNIX **En las plataformas Linux y UNIX:** stopserver.sh *nombre_servidor* -profileName *nombre_perfil* -username *nombre_usuario* -password *contraseña* • i5/OS **En System i (desde la línea de mandatos de QShell):** stopserver *nombre_servidor* -profileName *nombre_perfil* -username *nombre_usuario* -password *contraseña* desde el indicador de mandatos en el directorio *dir_instalación*/bin. El nombre de usuario proporcionado debe ser un miembro del rol operador o administrador.

Nota: Es necesario que proporcione un nombre de usuario y contraseña para detener el servidor.
Si el nombre de usuario y contraseña que proporcione son miembros del rol operador o administrador, el servidor se detendrá.

3. Compruebe que el servidor se haya detenido correctamente

   La siguiente tabla describe las opciones para verificar que el servidor se ha detenido correctamente.

Compruebe que el servidor se haya detenido correctamente	Detalles
Desde la interfaz de usuario	La ventana de salida de Primeros pasos muestra detalles de los resultados de su petición.
Desde la línea de mandatos	El resultado de su petición se muestra en la ventana de mandatos desde donde haya realizado la petición.

Roles de seguridad de administración

Se proporcionan roles de seguridad de administración como parte de la instalación de WebSphere Process Server.

Se proporcionan siete roles como parte de la consola administrativa. Estos roles otorgan permisos de distintos rangos de funcionalidad en la consola administrativa. Cuando está habilitada la seguridad administrativa, debe correlacionarse un usuario con uno de estos cuatro roles para poder acceder a la consola administrativa.

El primer usuario que inicia la sesión en el servidor después de la instalación se añade al rol administrador.

Tabla 6. Roles de seguridad de administración

Rol de seguridad de administración	**Descripción**
Supervisor	Los miembros del rol supervisor pueden visualizar la configuración de WebSphere Process Server y el estado actual del servidor.
Configurador	Los miembros del rol configurador pueden editar la configuración de WebSphere Process Server.
Operador	Los miembros del rol operador tienen privilegios de supervisor y la capacidad de modificar el estado de tiempo de ejecución, a saber, iniciar y detener el servidor.
Administrador	El rol administrador es una combinación de los roles configurador y operador además de privilegios adicionales otorgados únicamente al rol administrador. Entre ellos se incluyen: • Modificación del ID y la contraseña de usuario del servidor • Correlación de usuarios y grupos con el rol administrador También dispone de los permisos necesarios para acceder a información importante como: • Contraseña LTPA • Claves .
Adminsecuritymanager	Sólo los usuarios que tienen concedido este rol pueden correlaciones usuarios con roles administrativos. Asimismo, cuando se utiliza la seguridad administrativa de alta precisión, sólo los usuarios que tienen concedido este rol pueden gestionar los grupos de autorización. Consulte los roles administrativos, para obtener más información.
Desplegador (Deployer)	Los usuarios que tienen este rol puede realizar acciones de configuración y operaciones de tiempo de ejecución en las aplicaciones.

Tabla 6. Roles de seguridad de administración (continuación)

Rol de seguridad de administración	Descripción
iscadmins	Este rol sólo está disponible para los usuarios de la consola administrativa y no para los usuarios wsadmin. Los usuarios que tienen este rol poseen privilegios administrativos para gestionar usuarios y grupos en depósitos federados. Por ejemplo, un usuario con el rol iscadmins puede realizar las tareas siguientes: • Crear, actualizar o suprimir usuarios en la configuración de depósitos federados. • Crear, actualizar o suprimir grupos en la configuración de depósitos federados.

El ID de servidor que se especifica al habilitar la seguridad administrativa, se correlaciona automáticamente con el rol administrador. Los usuarios o grupos pueden añadirse o eliminarse de los roles de administración en cualquier momento mediante la consola administrativa de WebSphere Process Server. Sin embargo, es necesario reiniciar el servidor para que los cambios entren en vigor. Lo más adecuado es correlacionar un grupo o grupos, en lugar de usuarios específicos, con roles de administración porque de esta forma la administración es más fácil y flexible. Si se correlaciona un grupo con un rol de administración, la adición o eliminación de usuarios en el grupo se produce fuera de WebSphere Process Server y no es necesario reiniciar el servidor para que el cambio entre en vigor.

Además de correlacionar usuarios o grupos, también puede correlacionarse un sujeto especial con los roles de administración. Un sujeto especial es una generalización de una clase de usuarios concreta. El sujeto especial AllAuthenticated significa que la comprobación de acceso del rol de administración garantiza que el usuario que realiza la petición esté al menos autenticado. El sujeto especial Everyone significa que cualquiera pueda realizar la acción, autenticado o no, como si la seguridad no estuviese habilitada.

Seguridad por omisión de los componentes instalados

Varios componentes importantes de WebSphere Process Server tienen información de seguridad por omisión. En esta información se incluyen los alias con los que se correlacionan los usuarios por omisión y los roles de seguridad a los que se debe otorgar acceso a los usuarios para poder invocar estos componentes.

Finalidad

Varios de los componentes importantes de WebSphere Process Server utilizan alias predefinidos para autenticarse en motores de mensajería y bases de datos. Durante la creación de perfiles, a estos alias de autenticación se les asigna un valor por omisión con el ID de usuario y la contraseña del administrador principal. Debe configurar estos alias de modo que se correspondan con otros usuarios del depósito de cuentas de usuario..

Alias de autenticación de Business Process Choreographer

Los procesos de empresa tienen los siguientes alias de autenticación. Modifique estos alias mediante la consola administrativa.

Los alias de la Tabla 2 en la página 18 se utilizan para invocar los componentes independientemente de la identidad del usuario que invoque.

Tabla 7. Alias de autenticación asociados con procesos de empresa.

Alias	Descripción	Información
BPEAuthDataAliasJMS_*nodo_servidor*	Se utiliza para autenticar con el motor de mensajería.	Entre el nombre de usuario y la contraseña en el panel de configuración de Business Process Choreographer del asistente de perfiles.
BPEAuthDataAlias*TipoBD_nodo_servidor*	Se utiliza para autenticar con bases de datos.	Configure la base de datos mediante los scripts proporcionados.

La Tabla 3 en la página 18 describe los roles RunAs creados para los procesos de empresa.

Tabla 8. Roles RunAs asociados con procesos de empresa.

Rol RunAs	Descripción	Información
JMSAPIUser	Se utiliza por MDB de API de BFM JMS en bpecontainer.ear.	Entre el nombre de usuario y la contraseña en el panel de configuración de Business Process Choreographer del asistente de perfiles.
EscalationUser	Se utiliza por MDB task.ear.	Entre el nombre de usuario y la contraseña en el panel de configuración de Business Process Choreographer del asistente de perfiles.

El nombre de usuario suministrado se añade al rol RunAs.

Alias de autenticación de Common Event Infrastructure

Common Event Infrastructure tiene los siguientes alias de autenticación. Modifique estos alias mediante la consola administrativa.

Los alias de la Tabla 4 en la página 18 se utilizan para invocar los componentes independientemente de la identidad del usuario que invoque.

Tabla 9. Alias de autenticación asociados con Common Event Infrastructure.

Alias	Descripción	Información
CommonEventInfrastructure JMSAuthAlias Se ha añadido un carácter de espacio a esta entrada para permitir que entre en la celda de la tabla. El nombre de alias real no contiene un carácter de espacio.	Se utiliza para autenticar con el motor de mensajería.	Entre el nombre de usuario y la contraseña en el panel de configuración de Common Event Infrastructure del asistente de perfiles.

Tabla 9. Alias de autenticación asociados con Common Event Infrastructure. (continuación)

Alias	Descripción	Información
EventAuthAlias*TipoBD*	Se utiliza para autenticar con bases de datos.	Entre el nombre de usuario y la contraseña en el panel de configuración de Common Event Infrastructure del asistente de perfiles.

Alias de autenticación de SCA (Service Component Architecture)

La arquitectura de componentes de servicio (SCA) tiene los siguientes alias de autenticación. Modifique estos alias mediante la consola administrativa.

Los alias de la Tabla 5 en la página 19 se utilizan para invocar los componentes independientemente de la identidad del usuario que invoque.

Tabla 10. Alias de autenticación asociados con componentes SCA.

Alias	Descripción	Información
SCA_Auth_Alias	Se utiliza para autenticar con el motor de mensajería.	Entre el nombre de usuario y la contraseña en el panel de configuración de SCA del asistente de perfiles.

Control de acceso en aplicaciones de procesos de empresa y tareas de usuario

Los siguientes archivos EAR (Enterprise Archive) se instalan con control de acceso como parte de la instalación de Business Process Choreographer. Business Process Choreographer se instala como parte de la instalación de WebSphere Process Server. El gestor de tareas de usuario utiliza los roles para determinar las posibilidades del usuario en un sistema de producción.

Archivo EAR	Roles	Permiso por omisión	Notas
bpecontainer.ear	BPESystemAdministrator	Nombre de grupo entrado durante la instalación.	Tiene acceso a todos los procesos de empresa y a todas las operaciones.
bpecontainer.ear	BPESystemMonitor	Todos los usuarios autenticados.	Tiene acceso a operaciones de lectura.
task.ear	TaskSystemAdministrator	Nombre de grupo entrado durante la instalación.	Tiene acceso a todas las tareas de usuario.
task.ear	TaskSystemMonitor	Todos los usuarios autenticados.	Tiene acceso a operaciones de lectura.
Bpcexplorer.ear	WebClientUser	Todos los usuarios autenticados.	Puede acceder a Business Process Choreographer Explorer.

Control de acceso en aplicaciones de Common Event Infrastructure

El siguiente archivo EAR (Enterprise Archive) se instala con control de acceso como parte de la instalación de Common Event Infrastructure. Common Event Infrastructure se instala como parte de la instalación de WebSphere Process Server.

El archivo EventServer.ear es el único archivo EAR instalado como parte de la instalación de Common Event Infrastructure.

Roles	Permiso por omisión
eventAdministrator	Todos los usuarios autenticados.
eventConsumer	Todos los usuarios autenticados.
eventUpdater	Todos los usuarios autenticados.
eventCreator	Todos los usuarios autenticados.
catalogAdministrator	Todos los usuarios autenticados.
catalogReader	Todos los usuarios autenticados.

Protección de aplicaciones en WebSphere Process Server

En las aplicaciones que se despliegan en una instancia de WebSphere Process Server es necesario integrar la seguridad y aplicarla en tiempo de ejecución.

Antes de empezar

Para proteger las aplicaciones se da por supuesto que está habilitada la seguridad administrativa.

Acerca de esta tarea

Las aplicaciones albergadas en el entorno de WebSphere Process Server realizan muchas funciones empresariales críticas que requieren seguridad. Algunas aplicaciones acceden, transfieren o alteran información confidencial (por ejemplo: información sobre nómina o detalles de tarjetas de crédito). Otras realizan la gestión de facturación o inventario. Naturalmente la seguridad de estas aplicaciones es de vital importancia.

Proteja las aplicaciones realizando las tareas siguientes:

Procedimiento

1. Asegúrese de que está habilitada la seguridad administrativa. Consulte “Habilitación de la seguridad administrativa” en la página 7 para obtener más detalles.
2. Asegúrese de que está habilitada la seguridad de aplicaciones. En la consola administrativa, expanda **Seguridad** y pulse **Proteger la administración, las aplicaciones y la infraestructura**. Seleccione **Habilitar seguridad de aplicaciones** para que WebSphere Process Server solicite la autenticación de los usuarios que intenten acceder a una aplicación protegida.
3. Desarrolle las aplicaciones en WebSphere Process Server utilizando todas las características de seguridad apropiadas.
4. Despliegue las aplicaciones en el entorno de WebSphere Process Server asignando usuarios o grupos a los roles de seguridad apropiados.
5. Mantenga la seguridad del entorno de WebSphere Process Server.

Elementos de la seguridad de aplicaciones

Las aplicaciones que se ejecutan en WebSphere Process Server se protegen mediante autenticación y control de acceso. Además, los datos transferidos durante la invocación de una aplicación se mantienen protegidos mediante diversos mecanismos; estos mecanismo aseguran que los datos no puedan leerse ni alterarse en el recorrido. El elemento final de seguridad es la propagación de la información de seguridad a través de varios sistemas, para que el usuario no tenga que introducir repetidamente el nombre de usuario y contraseña.

Es posible dividir la seguridad de WebSphere Process Server en tres grupos generales:

- Seguridad de aplicaciones
- Integridad y privacidad de los datos
- Propagación de la identidad

Seguridad de aplicaciones

La seguridad de sus aplicaciones WebSphere Process Server se mantiene de dos formas:

- **Autenticación** Los usuarios que deseen utilizar una aplicación deberán proporcionar un nombre de usuario y contraseña del registro de usuario.
- **Control de acceso** Los usuarios deberán tener permiso para invocar la aplicación. Los roles están asociados con la invocación de la aplicación. Un usuario autenticado debe formar parte del rol apropiado porque de lo contrario la aplicación no se ejecutará.

Integridad y privacidad de los datos

La seguridad de los datos a los que accede una aplicación se garantiza en el origen, destino y tránsito:

- **Integridad** Los datos enviados a través de la red no se pueden alterar durante el tránsito.
- **Privacidad/confidencialidad** Los datos enviados a través de la red no pueden interceptarse ni leerse durante el tránsito.

Propagación de la identidad

El elemento final de la seguridad es el de la propagación de la identidad:

- **Inicio de sesión individual** Cuando una petición de cliente necesita pasar por varios sistemas dentro de la empresa, el cliente no está obligado a proporcionar los datos de autenticación varias veces. El método de inicio de sesión individual se utiliza para propagar la información de autenticación a los sistemas en sentido descendente que por turno van aplicando el control de acceso.

Autenticación

Cuando se activa la seguridad administrativa, es preciso autenticar los clientes.

Si un cliente intenta acceder a una aplicación segura sin estar autenticado, se genera una excepción.

La Tabla 11 en la página 37 lista los clientes típicos que pueden invocar componentes de WebSphere Process Server y las opciones de autenticación disponibles para cada tipo de cliente.

Tabla 11. Opciones de autenticación para diversos clientes

Cliente	Opciones de autenticación	Notas
Clientes de servicios Web	Se puede utilizar autenticación WS-Security/SOAP.	
Clientes Web o HTTP	Autenticación HTTP básica (el navegador solicita al cliente el nombre de usuario y contraseña).	Estos clientes hacen referencia a JSP, servlets y documentos HTML.
Clientes Java	JAAS.	
Todos los clientes	Autenticación de cliente SSL.	

Algunos de los componentes de la infraestructura de WebSphere Process Server tienen alias de autenticación que se utilizan para autenticar el código de tiempo de ejecución para obtener acceso a las bases de datos y al motor de mensajería. Estos alias de autenticación de Business Process Choreographer y Common Event Infrastructure se describen en temas posteriores. El instalador de WebSphere Process Server recopila los nombres de usuario y las contraseñas para crear estos alias.

Algunos componentes de tiempo de ejecución tienen beans controlados por mensajes (MDB) que se configuran con un rol runAs. El instalador de WebSphere Process Server recopila el nombre de usuario y la contraseña para el rol runAs.

Modificación de alias de autenticación:

Tal vez tenga que modificar los alias de autenticación existentes.

Acerca de esta tarea

Modifique los alias de autenticación de la consola administrativa.

Procedimiento

1. Acceda al panel Alias de autenticación de Business Integration.
   En la consola administrativa, expanda **Seguridad** y pulse **Alias de autenticación de Business Integration**.

   Nota: También puede acceder a este panel desde diversos paneles de la consola administrativa que requieren información de alias de autenticación.
2. Seleccione el alias de autenticación que desea modificar.
   El panel Alias de autenticación de Business Integration contiene una lista de alias de autenticación, el componente asociado, el ID de usuario asociado con este alias y, opcionalmente, una descripción del alias. Pulse en el alias que desea modificar. También puede marcar el recuadro de selección en la columna **Seleccionar** correspondiente al alias de autenticación que desea editar y, a continuación, pulse el botón **Editar**. Aparece el panel Configuración del alias de autenticación.
3. Cambie las propiedades del alias.
   En el panel de configuración del alias de autenticación para el alias seleccionado, puede modificar el nombre de alias o el ID de usuario y la contraseña asociados. También puede modificar la descripción de la entrada de datos de autenticación.
4. Confirme los cambios.

Pulse **Aceptar** o **Aplicar**. Vuelva al panel Alias de autenticación de Business Integration y pulse **Aplicar** para aplicar los cambios a la configuración maestra.

Nota: Para la instalación de Network Deployment, asegúrese de llevar a cabo una operación de sincronización de archivos para propagar los cambios a los demás nodos.

Para obtener información relacionada, consulte *Aumento de perfiles de WebSphere Process Server con seguridad*

Tareas relacionadas

"Creación de perfiles de WebSphere Process Server con seguridad" en la página 4

Cuando se crea un perfil de WebSphere Process Server se utilizan valores predeterminados para las credenciales de seguridad. Debe configurar estos valores de seguridad en la consola administrativa después de crear el perfil.

Control de acceso

El control de acceso hace referencia a asegurar que un usuario autenticado tenga los permisos necesarios para acceder a los recursos o para realizar una operación específica.

Cuando un usuario general se ha autenticado en WebSphere Process Server, es importante para la seguridad que no todas las operaciones posibles estén disponibles para ese usuario. Permitir que algunos usuarios realicen ciertas tareas, al tiempo que se deniegan estas tareas a otros usuarios, se denomina control de acceso.

El control de acceso puede disponerse para los componentes que desarrolle para hacerlos seguros. Esto se consigue utilizando calificadores de arquitectura de componentes de servicio durante el desarrollo. Consulte el Centro de información de WebSphere Integration Developer para obtener más información.

Algunos componentes de WebSphere Process Server, empaquetados como archivos EAR (Enterprise Archive), aseguran su operación mediante la seguridad basada en roles de J2EE. Se proporcionan detalles de estos componentes. Business Process Choreographer y Common Event Infrastructure se instalan como parte de WebSphere Process Server. La seguridad basada en roles asociada con estos componentes se describe de manera detallada en temas posteriores.

Integridad y privacidad de los datos

La privacidad e integridad de los datos que se acceden cuando se invocan los procesos de WebSphere Process Server son críticas para su seguridad.

La privacidad de los datos y la integridad de los datos son conceptos estrechamente relacionados. Para obtener una descripción más detallada, consulte la información relacionada.

Privacidad

Privacidad significa que un usuario no autorizado no podrá interceptar ni leer los datos.

Integridad

Integridad significa que un usuario no autorizado no podrá alterar los datos.

Soluciones proporcionadas en WebSphere Process Server

WebSphere Process Server da soporte a dos de las soluciones ampliamente utilizadas para la privacidad e integridad de los datos:

- Protocolo SSL (Secure Sockets Layer). SSL utiliza un protocolo de intercambio para autenticar los puntos finales e intercambiar la información que se utiliza para generar la clave de sesión que utilizarán los puntos finales para el cifrado y descifrado. SSL es un protocolo síncrono y es adecuado para comunicaciones punto a punto. SSL requiere que los dos puntos finales mantengan una conexión entre ellos lo que dure la sesión SSL.
- WS-Security. Este estándar define las extensiones SOAP (Simple Object Access Control) para la seguridad de los mensajes SOAP. WS-Security añade soporte para autenticación, integridad y privacidad de un único mensaje SOAP. A diferencia de SSL, no existe un protocolo de intercambio para establecer una clave de sesión. Esto hace que WS-Security sea adecuado para la seguridad de los mensajes en entornos asíncronos, como SOAP sobre JMS (Java Message Service) o SOAP sobre SIB (Service Integration Bus). Los descriptores de despliegue de WS-Security se pueden establecer en la aplicación antes del despliegue. Consulte la información relacionada para obtener más detalles.

En un entorno de integración empresarial con múltiples sistemas interactuando entre ellos, es posible que algunas de las comunicaciones sean asíncronas. Por lo tanto, en la mayoría de los casos, WS-Security es la solución superior.

Información relacionada

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

Configuración de un cliente Web de servicios Web para utilizar SSL:

Puede configurar un cliente de servicios Web para invocar un servicio Web con SSL (Secure Sockets Layer).

Acerca de esta tarea

Los detalles sobre cómo configurar el cliente Web de servicios Web para utilizar SSL se proporcionan en esta nota técnica WebSphere Application Server. Puede encontrar una descripción más general de la protección de servicios Web en el tema de WebSphere Application Server: Protección de aplicaciones de servicios Web a nivel de transporte.

Inicio de sesión individual

La información de nombre de usuario y contraseña se le solicita al cliente una sola vez. La identidad proporcionada se propaga por el sistema.

Cuando una petición de cliente necesita pasar por múltiples sistemas dentro de la empresa, el cliente sólo tiene que autenticarse una vez. Este concepto de propagación de la identidad se soluciona utilizando el método de inicio de sesión individual.

El contexto autenticado se propaga a los sistemas en sentido descendente, que pueden aplicar el control de acceso.

El plugin de Tivoli Access Manager WebSEAL o Tivoli Access Manager para servidores Web se puede utilizar como servidores proxy de retroceso para proporcionar gestión de acceso y la función de inicio de sesión individual a los recursos de WebSphere Process Server. Podrá encontrar detalles de cómo configurar estas herramientas en la documentación de WebSphere Application Server.

Información relacionada

Configuración de la posibilidad de inicio de sesión individual con Tivoli Access Manager o WebSEAL

Desarrollo de componentes seguros

Proteja los componentes que desarrolle. Los componentes implementan las interfaces que tienen métodos. Utilice el calificador de SCA (Service Component Architecture) SecurityPermission para proteger una interfaz o un método.

Antes de empezar

Desarrolle la aplicación protegida en WebSphere Integration Developer. Exporte la aplicación como un archivo EAR (Enterprise Archive) para el despliegue en WebSphere Process Server.

Acerca de esta tarea

Importe una aplicación protegida a WebSphere Process Server siguiendo estos pasos.

Procedimiento

1. Instale el archivo EAR de aplicación.

   En la consola administrativa, expanda **Aplicaciones** y pulse **Aplicaciones de empresa**. Pulse **Instalar** y rellene los detalles de la nueva aplicación.
2. Asigne roles de seguridad a la nueva aplicación.

   Pulse **Correlacionar roles de seguridad con usuarios y grupos**. Tiene cuatro opciones de roles para la aplicación.

Opción	Descripción
Todos	Equivale a que no haya seguridad.
Todos los autenticados	Cualquier usuario que se autentique con un nombre de usuario y contraseña válidos es miembro del rol.
Usuarios correlacionados	Los usuarios individuales se listan como miembros del rol.
Grupos correlacionados	Los grupos son la manera más conveniente de añadir los usuarios y todos los miembros de los grupos identificados se convierten en miembros del rol.

   Utilice **Buscar usuarios** y **Buscar grupos** para listar los usuarios y grupos que se pueden correlacionar con el rol.

En el SCDL de ejemplo que se muestra a continuación, el acceso al método **onewayinvoke** está restringido a los usuarios que son miembros del rol **gestor**.

```
<?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>
```

Despliegue (instalación) de aplicaciones seguras

El despliegue de aplicaciones que tienen restricciones de seguridad (aplicaciones seguras) es similar a desplegar aplicaciones que no las tienen. La única diferencia está en que será necesario asignar usuarios y grupos a roles en el caso de una aplicación segura, lo que implica tener activo el registro de usuario correcto. Si instala una aplicación segura, los roles se deberán haber definido en la aplicación. Si la aplicación requiere delegación, también se definen roles RunAs y deben proporcionarse un nombre de usuario y contraseña correctos.

Antes de empezar

Antes de realizar esta tarea, verifique que ha diseñado, desarrollado y ensamblado la aplicación con todas las configuraciones de seguridad relevantes. Para obtener más información sobre estas tareas consulte el centro de información de WebSphere Integration Developer. En este contexto, el despliegue e instalación de una aplicación se consideran la misma tarea.

Acerca de esta tarea

Uno de los pasos necesarios para desplegar aplicaciones seguras es asignar usuarios y grupos a los roles que se definieron cuando se construyó la aplicación. Esta tarea se completa como parte del paso titulado ″Correlacionar roles de seguridad con usuarios y grupos″. Si se ha utilizado una herramienta de ensamblaje, esta asignación puede haberse completado con anterioridad. En ese caso, puede confirmar la correlación efectuando este paso. Durante este paso puede añadir usuarios y grupos, así como modificar la información existente.

Si se ha definido un rol RunAs en la aplicación, la aplicación invocará métodos utilizando una identidad configurada durante el despliegue. Utilice el rol RunAs para especificar la identidad bajo la cual se efectúan las invocaciones en sentido descendente. Por ejemplo, si el rol RunAs se asigna al usuario “bob” y el cliente “alice” está invocando un servlet, que tiene establecido el permiso de delegación, que llama a los enterprise beans, el método de los enterprise beans se invoca con “bob” como la identidad. Como parte del proceso de despliegue, uno de los pasos es asignar o modificar usuarios a los roles RunAs. Este paso se titula ″Correlacionar roles RunAs con usuarios″. Utilice este paso para asignar nuevos usuarios o modificar usuarios existentes a roles RunAs cuando la política de delegación se establece en SpecifiedIdentity.

Los pasos descritos a continuación son comunes tanto en la instalación de una aplicación como en la modificación de una aplicación existente. Si la aplicación contiene roles, verá el enlace "Correlacionar roles de seguridad con usuarios y grupos" durante la instalación de la aplicación y también durante la gestión de las aplicaciones, como un enlace de la sección Propiedades adicionales.

Procedimiento

1. En la consola administrativa, expanda Aplicaciones y pulse Instalar una nueva aplicación.

   Complete los pasos que son necesarios para instalar las aplicaciones antes del paso titulado, "Correlacionar roles de seguridad con usuarios y grupos".
2. Asigne usuarios y grupos a roles.
3. Correlacione usuarios con roles RunAs si existen roles RunAs en la aplicación.
4. Pulse Uso correcto de la identidad del sistema para especificar los roles RunAs, si es necesario.

   Efectúe esta acción si la aplicación tiene el permiso de delegación establecido en identidad del sistema, que es sólo aplicable a enterprise beans. La identidad del sistema utiliza el ID de servidor de seguridad de WebSphere Process Server para invocar métodos en sentido descendente. Utilice este ID con precaución porque este ID tiene más privilegios que otras identidades al acceder a los métodos internos de WebSphere Process Server. Esta tarea se ha proporcionado para asegurarse de que el desplegador es consciente del hecho de que los métodos listados en el panel tienen la identidad del sistema que se ha configurado para la delegación y para corregirlos, si es necesario. Si no es necesario efectuar ningún cambio, omita esta tarea.
5. Efectúe los pasos restantes no relacionados con la seguridad para finalizar la instalación y despliegue de la aplicación.

Qué hacer a continuación

Una vez desplegada la aplicación segura, compruebe que puede acceder a los recursos de la aplicación con las credenciales correctas. Por ejemplo, si la aplicación tiene un módulo Web protegido, asegúrese de que sólo los usuarios que ha asignado a los roles pueden utilizar la aplicación.

Información relacionada

Asignación de usuarios y grupos a roles

Asignación de usuarios a roles RunAs

Asignación de usuarios a roles

Una aplicación segura utiliza uno o los dos calificadores de seguridad securityPermission y securityIdenitity. Cuando están presentes estos calificadores, es necesario realizar pasos adicionales en el momento del despliegue para que la aplicación y sus características de seguridad funcionen correctamente.

Antes de empezar

En esta tarea se da por supuesto que la aplicación segura está preparada para desplegarse como un archivo EAR en WebSphere Process Server.

Acerca de esta tarea

Las aplicaciones implementan las interfaces que tienen métodos. Puede proteger una interfaz o un método con el calificador securityPermission de SCA ((Service Component Architecture). Cuando invoque este calificador especifique un rol (por ejemplo, “supervisores”) que tenga permiso para invocar el método seguro. Cuando despliegue la aplicación tendrá la oportunidad de asignar usuarios al rol especificado.

El calificador securityIdentity es equivalente al rol RunAs utilizado para delegaciones en WebSphere Application Server. El valor asociado con esta calificador es un rol. Durante el despliegue, el rol se correlaciona con una identidad. La invocación de un componente protegido con securityIdentity toma la identidad especificada, independientemente de la identidad del usuario que invoca la aplicación.

Procedimiento

1. Siga las instrucciones para desplegar aplicaciones en WebSphere Process Server. Consulte el apartado Instalación de un módulo en un servidor de producción para obtener más detalles.
2. Asocie los usuarios correctos con los roles.

Calificador de seguridad	Acción a realizar
Permiso de seguridad	Asignar un usuario o usuarios al rol especificado. Existen cuatro opciones: • Todos: equivalente a sin seguridad. • Todos autenticados: todos los usuarios autenticados son miembros del rol. • Usuarios correlacionados: se añaden usuarios individuales al rol. • Grupos correlacionados: se añaden grupos de usuario al rol. La opción más flexible es Grupos correlacionados, porque se pueden añadir usuarios al grupo y de esta forma que obtengan acceso a la aplicación sin reiniciar el servidor.
Identidad de seguridad	Proporcione un nombre de usuario y contraseña válidos para la identidad con la que se correlaciona el rol.

Información relacionada

Delegaciones

Protección de adaptadores

Se admiten dos tipos de adaptadores en WebSphere Process Server: WebSphereBusiness Integration Adapters y WebSphere Adapters. Se analiza la seguridad de ambos tipos de adaptadores.

Acerca de esta tarea

Los adaptadores son el mecanismo por el cual las aplicaciones se comunican con los sistemas EIS (Enterprise Information Systems). La información que se intercambia entre una aplicación y un EIS puede ser muy confidencial. Es importante garantizar la seguridad de esta transacción de información.

Los WebSphere Business Integration Adapters constan de una colección de software, interfaces de programas de aplicación (API) y herramientas que permiten a las aplicaciones intercambiar datos de empresa a través de un intermediario de integración. WebSphere Business Integration Adapters se basan en la mensajería JMS y JMS no da soporte a la propagación de contexto de seguridad.

Los WebSphere Adapters habilitan la conectividad bidireccional gestionada entre los EIS (Enterprise Information Systems) y los componentes J2EE soportados por WebSphere Process Server.

Para la comunicación entrante de ambos tipos de adaptadores con WebSphere Process Server, no hay ningún mecanismo de autenticación. Para WebSphere Business Integration Adapters, basarse en la mensajería JMS impide la propagación de contexto de seguridad. J2C también carece de soporte de seguridad entrante, por lo que los WebSphere Adapters tampoco tienen ningún mecanismo de autenticación para la comunicación entrante.

La entrada de un adaptador en WebSphere Process Server emplea siempre una exportación de arquitectura de componentes de servicio (SCA). La exportación SCA tiene que conectarse a un componente SCA como, por ejemplo, la mediación, el proceso de empresa, el componente Java SCA o Selector.

La solución de seguridad consiste en definir un rol runAs en el componente que es el destino de la exportación del adaptador WebSphere. Esto se realiza mediante el calificador SCA SecurityIdentity durante el desarrollo (consulte el WebSphere Integration Developer Centro de información de para obtener más información). Cuando se ejecuta el componente, lo hace bajo la identidad definida en el rol runAs.

El valor de SecurityIdentity es un rol y no un usuario. Sin embargo, cuando se despliega el archivo EAR en WebSphere Process Server debe proporcionarse un nombre de usuario y contraseña para la identidad que se va a utilizar. La utilización de SecurityIdentity evita que se generen excepciones si un componente en sentido descendente está protegido y requiere que el cliente tenga una identidad autenticada.

Nota: La utilización de SecurityIdentity no protege la comunicación entre el adaptador y el EIS.

WebSphere Business Integration Adapters envían datos a WebSphere Process Server como mensajes JMS sobre el bus de integración de servicios.

Los WebSphere Adapters residen en la JVM de WebSphere Process Server y por tanto sólo es necesario proteger la comunicación entre el adaptador y el EIS de destino. El protocolo entre el adaptador y el EIS es específico del EIS. La documentación del EIS proporcionará información sobre cómo proteger este enlace.

Conceptos relacionados

Consideraciones sobre la seguridad de los buses de integración de servicios

Seguridad en tareas de usuario y procesos de empresa

Hay varios roles asociados con tareas de usuario y procesos de empresa. Este tema describe los roles disponibles.

Las tareas de usuario, por definición, requieren intervención de usuario para completarse. Algunos procesos de empresa también pueden necesitar intervención de usuario. Estas tareas de usuario y procesos de empresa se desarrollan utilizando WebSphere Integration Developer y se invocan mediante Business Process Choreographer. Cuando desarrolle la tarea o proceso, debe asignar roles a usuarios o grupos implicados en las tareas de usuario y los procesos de empresa. Consulte el centro de información de WebSphere Integration Developer si desea más información sobre cómo asignar los roles o cómo consultar los roles asociados a roles específicos.

El Gestor de tareas de usuario utiliza los roles para determinar las posibilidades de los usuarios en un sistema de producción.

Roles asociados con tareas de usuario y procesos de empresa

Importante: Estos roles son exclusivos de las tareas y procesos que se ejecutan en el contenedor de empresa y el contenedor de tareas de usuario de Business Process Choreographer.

WebSphere Process Server da soporte a los roles siguientes para tareas y procesos:

Administrador
Los usuarios que pertenecen a este rol pueden supervisar, finalizar o suprimir tareas y procesos, así como visualizar información sobre tareas y procesos.

Lector Los usuarios que pertenecen a este rol sólo pueden visualizar tareas y procesos.

Iniciador
Los usuarios que pertenecen a este rol pueden iniciar o visualizar tareas y procesos.

Las tareas también tienen estos roles adicionales:

Propietario
Los usuarios que pertenecen a este rol pueden guardar, cancelar, completar o visualizar las tareas que ya hayan reclamado.

Propietario potencial
Los usuarios que pertenecen a este rol pueden reclamar y visualizar tareas.

Conceptos relacionados

Autorización y asignación de usuarios a procesos

Información relacionada

Autorización y asignación de usuarios

Guías de aprendizaje

Existen guías de aprendizaje que le proporcionan información acerca de los escenarios de seguridad más importantes.

Creación de seguridad de extremo a extremo

Existente muchos escenarios potenciales de seguridad de extremo a extremo. Cada uno de ellos podría implicar distintos pasos de seguridad. Aquí se presentan varios escenarios típicos con las opciones de seguridad necesarias.

Antes de empezar

En todos estos escenarios se asume que se impone la seguridad global.

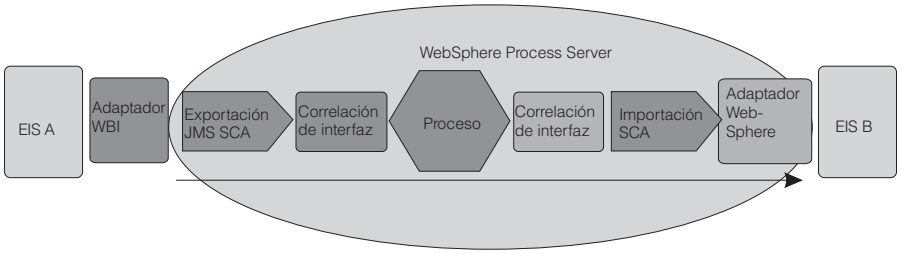
Acerca de esta tarea

Procedimiento

1. Determine cuál de los ejemplos proporcionados en este apartado se aproximan más a sus necesidades de seguridad. En ciertos casos, su escenario incluirá una combinación de información de más de uno de los ejemplos.
2. Lea la información de seguridad de los escenarios relevantes y aplíquela a sus necesidades de seguridad.

Escenario de integración clásico: adaptadores de entrada y salida

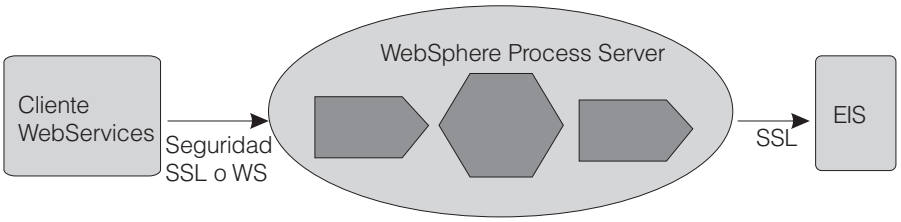
Las peticiones de entrada provienen de un WebSphere Business Integration Adapter. SCA (Service Component Architecture) invoca una correlación de interfaz basada en la exportación SCA. La petición pasa a través de un componente de proceso, una segunda correlación de interfaz y después se pasa a un segundo EIS (B), mediante un adaptador WebSphere. Se trata de invocaciones SCA con un componente invocando un método sobre el siguiente componente.



No hay mecanismo de autenticación para el adaptador de entrada. Puede establecer el contexto de seguridad definiendo el calificador SecurityIdentity en el primer componente; en esta instancia, el primer componente de correlación de interfaz. Desde ese punto, SCA propagará el contexto de seguridad desde cada componente al siguiente. El control de acceso de cada componente se define mediante el calificador SecurityPermission.

Petición de servicio Web de entrada para WebSphere Process Server

En este escenario un cliente del servicio Web invoca un componente de WebSphere Process Server. La petición pasa a través de varios componentes en el entorno de WebSphere Process Server antes de que un adaptador lo pase a un EIS.

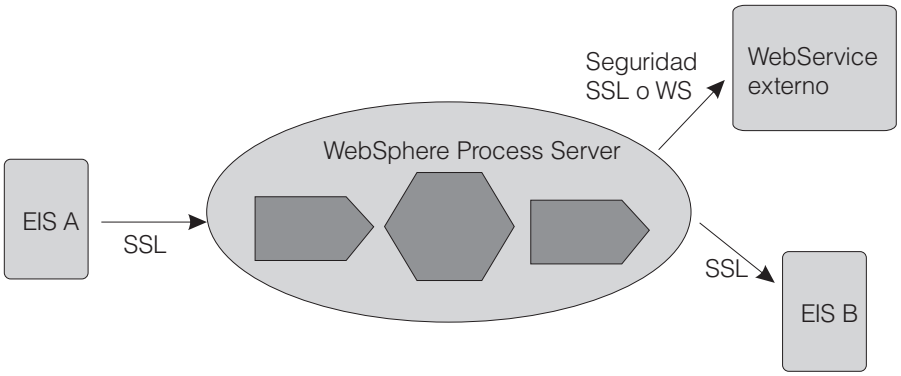


Puede autenticar un cliente de servicio Web como un cliente SSL, utilizando autenticación básica HTTP o utilizando una autenticación WS-Security. Cuando se autentica el cliente, se aplica el control de acceso basado en el calificador

SecurityPermission. Entre el cliente y la instancia de WebSphere Process Server puede proteger la integridad y privacidad de los datos utilizando SSL o WS-Security. Con SSL se protege todo el conducto, mientras que con WS-Security se puede cifrar o firmar digitalmente partes del mensaje SOAP. Para los servicios Web, WS-Security es el estándar preferido.

Petición de servicio Web de salida desde WebSphere Process Server

En este escenario la petición de entrada puede ser desde un adaptador, un cliente de servicio Web o un cliente HTTP. Un componente de WebSphere Process Server (por ejemplo, un componente BPEL) invoca un servicio Web externo.



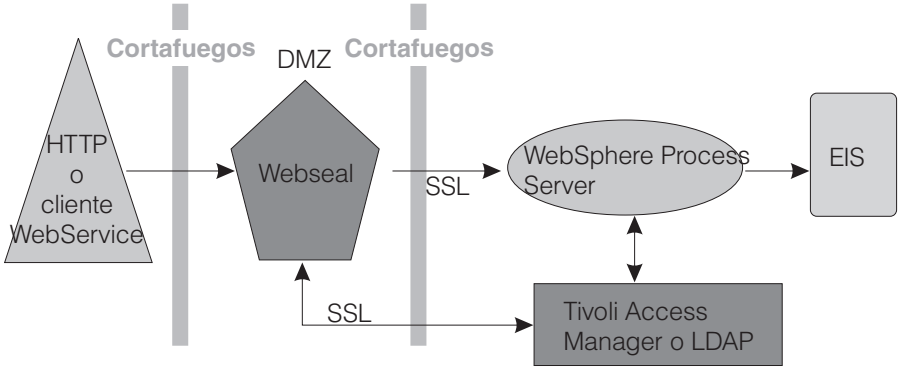
Al igual que con la petición de servicio Web de entrada, puede autenticar con el servicio Web externo como un cliente SSL, utilizando autenticación básica HTTP o autenticación WS-Security. Utilice LTPACallBackHandler como mecanismo de retorno de llamada para extraer el usernameToken del asunto RunAs actual. Entre WebSphere Process Server y el servicio Web de destino, puede proteger la privacidad e integridad de los datos utilizando WS-Security.

Aplicación Web: petición de entrada HTTP para WebSphere Process Server

WebSphere Process Server da soporte a tres tipos de autenticación para HTTP:

- Autenticación básica HTTP
- Autenticación basada en formularios HTTP
- Autenticación de clientes basada en HTTPS SSL.

Además, para proteger la intranet frente a intrusos, puede situar un servidor Web en la zona desmilitarizada (DMZ) y WebSphere Process Server dentro del cortafuegos interior. En este ejemplo, se utiliza WebSEAL como proxy de retroceso, que realiza la autenticación. Tiene una asociación de confianza con WebSphere Process Server detrás del cortafuegos y puede reenviar peticiones autenticadas.



Conceptos relacionados

Consideraciones sobre la seguridad de los buses de integración de servicios

Guía de aprendizaje: escritura de un script Jacl que liste los roles de seguridad

Esta guía de aprendizaje trata acerca de cómo escribir y ejecutar un script Jacl simple que puede acceder a un JMX MBean y gestionarlo. Este script concreto se refiere a llamar a roles cuando se habilita la seguridad global. Si utiliza este script, podrá imprimir el nombre de rol para cada rol de una relación.

Objetivo de esta guía de aprendizaje

Después de completar esta guía de aprendizaje, podrá realizar las acciones siguientes:

- Escribir un script Jacl que llame a un JMX MBean solicitando una lista de todas las relaciones.

Para obtener más información sobre cómo escribir scripts, consulte "Utilización de scripts (wsadmin)" en el Centro de información de WebSphere Application Server Network Deployment, versión 6.

Tiempo necesario para completar esta guía de aprendizaje

Esta guía de aprendizaje requiere para completarse aproximadamente 15-30 minutos.

Requisitos previos

Este guía de aprendizaje utiliza un script que se incluye con el ejemplo de Seguridad de JMX. Este ejemplo muestra la función de MBean de imprimir una lista de relaciones de rol.

Nota: Para utilizar este script, debe seleccionar la opción de instalar ejemplos de código durante la instalación de WebSphere Process Server.

El script Jacl de ejemplo se encuentra en *raíz_instalación*/samples/JMXSample/scripts y *raíz_instalación*\samples\JMXSample\scripts. El nombre del script es: `RelServicesAdmin.jacl`.

Para ejecutar el script, entre: UNIX Linux

```
wsadmin -f raíz_instalación/samples/JMXSample/scripts/RelServicesAdmin.jacl
 -server nombre_servidor -node
nombre_nodo
```

script, entre: Windows

```
wsadmin -f raíz_instalación\samples\JMXSample\scripts\RelServicesAdmin.jacl
 -server nombre_servidor -node
nombre_nodo
```

Este script llamará a un máximo de 10 relaciones en el entorno y un máximo de 10 roles para cada relación que se imprimirá en la consola.

Ejercicio: escritura de un script Jacl

Acerca de esta tarea

Los conceptos básicos de este script pueden utilizarse para comunicarse con cualquier MBean del sistema. Todo lo necesario es el nombre y tipo del MBean y los métodos y atributos disponibles en el MBean. Para los atributos se utilizan los mandatos getAttribute y setAttribute. El mandato invoke se utiliza para los métodos. Siga estos pasos para crear un script `.jacl` que gestiona el MBean de seguridad JMX.

Nota: El código de cada paso va precedido de una sentencia que explica lo que realiza el código.

Procedimiento

1. Determine el **nombre_nodo**

   La primera parte del script que aparece a continuación determina el nombre_nodo. Si el `nombre_nodo` no se especifica correctamente, se imprime la sintaxis correcta y se sale del script.

   ```
   # leer y validar argumentos

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

2. Identifique el **MBean**

   Un MBean se identifica con un tipo y un nombre.

   Nota: El nombre y el tipo están codificados en este caso, ya que sabe el MBean específico que desea utilizar.
   La segunda parte del script identifica el MBean.

   ```
   # se utilizan estas dos variables, mbeanName y mbeanType,
     para identificar el mbean de manera exclusiva.
          # para este ejemplo, se utilizará el mbean que accede
            a los servicios de relaciones.

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

3. Localice y establezca la **referencia** en el MBean.

   Debe utilizar el código que aparece aquí para establecer la referencia para el MBean.

   ```
   # localizar el mbean y establecer una referencia en variable "relSvcsMBean"

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

4. Llame a la **relación** utilizando el mandato getAttribute.

La documentación de este MBean específico define un atributo llamado `allRelationshipNames`. Solicite este atributo al MBean mediante el mandato getAttribute. El valor de atributo será una lista que se recorre en el paso siguiente que invoca el mandato.

```
# solicitar la lista de relaciones del mbean

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

5. Invoque el **mandato** de cada nombre de relación, imprima el nombre y luego vuelva al MBean para obtener información adicional.

   En este ejemplo, el MBean define un método denominado getAllRoleNames con un solo parámetro para el nombre de relación específico. Utilice el mandato invoke para llamar a este método, pasando el nombre de relación actual. Para cada rol de la relación, se imprime un nombre de rol.

```
# recorrer en bucle la lista de nombres de rol e imprimir nombre

         foreach roleName $roles {
           puts "    Role: $roleName"
         }
      }
   } else {
         # argumentos incorrectos, imprimir sintaxis correcto
            puts "Usage: wsadmin -f RelServicesAdmin.jacl -nodeName nombre_nodo"
   }
```

Resultado

Ya ha escrito un script para llamar a relaciones.

Avisos

Esta información se ha creado para productos y servicios ofrecidos en los Estados Unidos.

Es posible que en otros países IBM no ofrezca los productos, los servicios o las características que se describen en este documento. Consulte con el representante de IBM de su localidad para obtener información sobre los productos y servicios disponibles actualmente en su área. Cualquier referencia a un producto, programa o servicio de IBM no pretende afirmar o implicar que sólo se pueda utilizar dicho producto, programa o servicio de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran el tema principal que se describe en este documento. La entrega de este documento no le otorga ninguna licencia sobre estas patentes. Puede enviar consultas de licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
EE.UU.

Para realizar consultas sobre licencias relativas a la información de doble byte (DBCS), póngase en contacto con el Departamento de propiedad intelectual de IBM de su país o envíe sus consultas, por escrito, a:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japón

El párrafo siguiente no se aplica al Reino Unido o a ningún otro país donde tales disposiciones estén en contradicción con la legislación local:INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGUNA CLASE, EXPRESA O IMPLÍCITA, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN DETERMINADO. Algunos países no permiten la declaración de limitación de responsabilidad de las garantías expresas o implícitas en determinadas transacciones, por lo que puede esta declaración no se aplique a su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. En cualquier momento IBM puede realizar mejoras y/o cambios en el producto o los productos y/o el programa o los programas que se describen esta publicación sin previo aviso.

Las referencias contenidas en esta información a sitios Web no IBM sólo se proporcionan por comodidad y no son de modo alguno ningún respaldo de dichos sitios Web. El material de esos sitios Web no forma parte del material de este producto de IBM y el uso de esos sitios Web es a cuenta y riesgo del usuario.

IBM puede utilizar o distribuir la información que se le proporcione del modo que estime apropiado sin incurrir por ello en ninguna obligación con el remitente.

Los propietarios de licencia de este programa que deseen tener información sobre el mismo con el fin de poder: (i) intercambiar información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) utilizar de forma mutua la información que se ha intercambiado, deberán ponerse en contacto con:

IBM Corporation
577 Airport Blvd., Suite 800
Burlingame, CA 94010
EE.UU.

Esta información puede estar disponible, sujeta a los términos y condiciones apropiados, que incluyen en algunos casos, el pago de un cargo.

IBM proporciona el programa bajo licencia descrito en este documento y todo el material con licencia disponible para el mismo bajo los términos del Acuerdo de cliente de IBM, el Acuerdo de licencia de programa internacional de IBM o cualquier acuerdo equivalente entre las dos partes.

Los datos de rendimiento aquí contenidos se han determinado en un entorno controlado. Por consiguiente, los resultados obtenidos en otros entornos operativos pueden variar significativamente. Es posible que algunas mediciones se hayan realizado en sistemas a nivel de desarrollo y no hay ninguna garantía de que dichas mediciones vayan a ser las mismas en sistemas disponibles de forma general. Además, es posible que algunas mediciones se haya estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deberán verificar los datos aplicables al entorno específico.

La información relacionada con productos no IBM se ha obtenido de los proveedores de esos productos, de sus anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado esos productos y no puede confirmar la precisión del rendimiento, la compatibilidad ni ninguna otra afirmación relacionada con los productos no IBM. Las preguntas sobre las posibilidades de los productos no IBM se deben dirigir a los proveedores de esos productos.

Todas las declaraciones relacionadas con una futura intención o dirección de IBM están sujetas a cambios o se pueden retirar sin previo aviso y sólo representan objetivos y metas.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con los nombres o las direcciones utilizados por una empresa real es pura coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente, que ilustran técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier modo sin realizar ningún pago a IBM, con el fin de desarrollar, utilizar, comercializar o distribuir programas de aplicación que se ajusten a la interfaz de programación de aplicaciones para la plataforma operativa para la que se han escrito los programas de ejemplo. Estos ejemplos no se han probado de forma completa bajo todas las condiciones. Por consiguiente, IBM no puede garantizar o implicar la fiabilidad, el servicio o la función de estos programas.

Cada copia o cualquier parte de estos programas de ejemplo o de cualquier trabajo derivado debe incluir un aviso de copyright como se indica a continuación: (c) (nombre de empresa) (año). Partes de este código se derivan de los programas de ejemplo de IBM Corp. (c) Copyright IBM Corp. _entre el año o los años_. Reservados todos los derechos.

Si está viendo esta información en copia software, es posible que las fotografías y las ilustraciones en color no aparezca.

Información de interfaz de programación

La información de interfaz de programación, si se proporciona, está destinada a ayudarle a crear software de aplicación utilizando este programa.

Las interfaces de programación de uso general le permiten escribir software de aplicación que obtiene los servicios de las herramientas de este programa.

Sin embargo, esta información también puede contener información de diagnóstico, modificación y ajuste. La información de diagnóstico, modificación y ajuste se proporciona para ayudarle a depurar el software de aplicación.

Aviso: No utilice esta información de diagnóstico, modificación y ajuste como interfaz de programación porque está sujeta a cambios.

Marcas registradas y marcas de servicio

IBM, el logotipo de IBM, Domino, Tivoli, WebSphere y z/OS son marcas registradas de International Business Machines Corporation en los Estados Unidos y/o en otros países.

Java y todas las marcas registradas basadas en Java son marcas registradas de Sun Microsystems, Inc. en los Estados Unidos y/o en otros países.

Windows es una marca registrada de Microsoft Corporation en los Estados Unidos y/o en otros países.

UNIX es una marca registrada de The Open Group en los Estados Unidos y en otros países.

Linux es una marca registrada de Linus Torvalds en los Estados Unidos y/o en otros países.

Otros nombres de compañías, productos o servicios pueden ser marcas registradas o marcas de servicio de otras empresas.

Este producto incluye software desarrollado por Eclipse Project (http://www.eclipse.org).

IBM WebSphere Process Server for Multiplatforms, Versión 6.1.0