WebSphere® Process Server for Multiplatforms

Versión 6.2.0

Seguridad de las aplicaciones y sus entornos

WebSphere® Process Server for Multiplatforms

Versión 6.2.0

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.

12 de diciembre de 2008

Esta edición se aplica a la versión 6, release 2, 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.

Manuales en PDF y Centro de información

Estos manuales en PDF se proporcionan a efectos prácticos para su impresión o su lectura cuando esté fuera de línea. Para ver la información más reciente, vea el Centro de información en línea.

En conjunto, los manuales en PDF contienen el mismo contenido que el Centro de información.

La documentación en PDF está disponible en un plazo de un trimestre después de un release importante del Centro de información como, por ejemplo, las versiones 6.0 ó 6.1.

La documentación en PDF se actualiza con menos frecuencia que el Centro de información, pero con más frecuencia que los Redbooks. En general, los manuales en PDF se actualizan cuando se han acumulado cambios suficientes para el manual.

Los enlaces externos del manual en PDF se dirigen al Centro de información en la Web. Los enlaces a destinos externos del manual en PDF están marcados con iconos que indican si el destino es un manual en PDF o una página Web.

Tabla 1. Iconos que preceden a enlaces externos a este manual

Icono	Descripción

	Un enlace a una página Web, incluido un enlace a una página del Centro de información.
	
	Los enlaces al Centro de información van a través de un servicio de direccionamiento indirecto, de modo que siguen funcionando aunque el tema de destino se haya desplazado a otra ubicación.
	
	Si desea encontrar una página enlazada en un Centro de información local, puede buscar el título del enlace. Alternativamente, puede buscar el ID del tema. Si los resultados de la búsqueda abarcan diferentes temas para diferentes variantes de producto, puede utilizar los controles de resultado de búsqueda **Agrupar por** para identificar el tema que desea ver. Por ejemplo:
	1. Copie el URL de enlace; por ejemplo, haga clic con el botón derecho en el enlace y seleccione Copiar ubicación del enlace. Por ejemplo: `http://www14.software.ibm.com/webapp/wsbroker/redirect?version=wbpm620 &product=wesb-dist&topic=tins_apply_service`
	2. Copie el ID de tema tras `&topic=`. Por ejemplo: `tins_apply_service`
	3. En el campo de búsqueda del Centro de información local, pegue el ID del tema. Si la característica de documentación está instalada de forma local, el resultado de búsqueda incluirá el tema. Por ejemplo:
	`1 resultado(s) encontrado para`
	
	`Agrupar por: Ninguno | Plataforma | Versión | Producto`
	`Mostrar resumen`
	
	`Instalación de fixpacks y paquetes de renovación con el instalador de actualizaciones`
	
	4. Haga clic en el enlace del resultado de la búsqueda para mostrar el tema.

Tabla 1. Iconos que preceden a enlaces externos a este manual (continuación)

Icono	Descripción
	Un enlace a un manual en PDF.

Contenido

Protección de aplicaciones y su entorno

La protección del entorno de WebSphere Process Server 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.

La seguridad de WebSphere Process Server se basa en la seguridad de WebSphere Application Server versión 6.1. Estos documentos son complementarios de la documentación de seguridad básica que se encuentra en el Centro de información de WebSphere Application Server y específicamente en la Documentación de seguridad de WebSphere Application Server, "Protección de aplicaciones y su entorno".

Información relacionada

 Documentación en PDF
Documentación de WebSphere Process Server (en formato PDF)

 Mapas de información
Los mapas de información de Business Process Management en IBM developerWorks organizan información sobre WebSphere Process Server, WebSphere ESB y los otros productos del grupo.

 IBM Education Assistant
Módulos educativos multimedia sobre WebSphere Process Server, proporcionados por IBM Education Assistant.

 Notas técnicas
Búsqueda en Soporte de WebSphere Process Server > notas técnicas de documentos de categoría de seguridad 6.2. Utilice los campos tipo de documento, categoría de producto y términos de búsqueda para encontrar la información necesaria.

 Visión general
Pestaña Visión general, en la página Web de la biblioteca de productos. Utilice esta página para acceder a los anuncios, las hojas de datos y otros documentos de bibliotecas generales relacionados con WebSphere ESB.

Visión general de la seguridad

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 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 aspectos incluyen:

- Autenticación de usuarios - Un usuario o un proceso que invoca una aplicación debe autenticarse. Con un inicio de sesión individual, un usuario puede proporcionar los datos de autenticación una sola vez y después pasar esta información de autenticación a los componentes en sentido descendente.
- Control de accesos - ¿El usuario autenticado tiene permiso para realizar la operación?
- Integridad y privacidad de los datos - Los datos a los que accede una aplicación deben estar protegidos para que ninguna parte no autorizada pueda verlos o modificarlos de alguna manera.

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

Conceptos relacionados

"Autenticación de usuarios" en la página 48
Cuando se activa la seguridad administrativa, es preciso autenticar los clientes.

"Control de acceso" en la página 49
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.

"Integridad y privacidad de los datos" en la página 51
La privacidad e integridad de los datos que se acceden cuando se invocan los procesos de WebSphere Process Server son críticas para su seguridad.

"Inicio de sesión individual" en la página 52
La información de nombre de usuario y contraseña se le solicita al cliente una sola vez. La identidad proporcionada se propaga por el sistema.

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.

- El panel de la consola administrativa de la seguridad de Business Integration Security es exclusivo de WebSphere Process Server. Para mostrar este panel, expanda **Seguridad** y pulse **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.
- WebSphere Process Server contiene un conjunto de roles de seguridad específicos de los componentes.

Iniciación a la seguridad

La seguridad es una consideración integral cuando se planifica la instalación de WebSphere Process Server, se desarrollan y despliegan aplicaciones, y en la ejecución cotidiana del servidor de procesos.

En la siguiente lista se proporciona una visión general de las tareas que lleva a cabo asegura WebSphere Process Server.

1. Considere la seguridad al instalar WebSphere Process Server.
2. Compruebe que la seguridad está activada para la instalación autónoma o del entorno de despliegue.
   a. Asegúrese de que la seguridad administrativa está activada.
   b. Asegúrese de que la seguridad de la aplicación está activada.
   c. Si es necesario, active la seguridad de Java 2.
   d. Utilice el asistente de configuración de seguridad en la consola administrativa para configurar las opciones de seguridad.
   e. Configure un mecanismo de autenticación seguro y un depósito de cuentas de usuario.
   f. Asigne nombres de usuario y contraseñas a los alias de autenticación de integración empresarial importantes.
   g. Asigne usuarios a roles de seguridad de administración apropiados.
3. Configure la seguridad para componentes de WebSphere Process Server específicos. Por ejemplo, puede utilizar el Gestor de seguridad para configurar el control de acceso basado en roles para los calendarios del Gestor de calendarios de empresa.
4. 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 apropiados para controlar el acceso a la aplicación recién desplegada.
5. Mantenga la seguridad del entorno de WebSphere Process Server.

Tareas relacionadas

"Instalación de WebSphere Process Server: consideraciones sobre la seguridad"
Considere cómo se implementará la seguridad antes, durante y después de la instalación de WebSphere Process Server.

"Habilitación de la seguridad" en la página 10
El primer paso para proteger su entorno y sus aplicaciones de WebSphere Process Server es habilitar la seguridad administrativa.

"Configuración de un depósito de cuentas de usuario" en la página 13
Los nombres de usuario y contraseñas de los usuarios registrados se almacenan en un depósito de cuentas de usuario. Puede utilizar el depósito de cuentas de usuario del sistema operativo local (es el valor por omisión), el protocolo LDAP (Lightweight Directory Access Protocol), depósitos federados o un depósito de cuentas personalizado.

 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.

"Despliegue (instalación) de aplicaciones seguras" en la página 52
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.

"Asignación de usuarios a roles" en la página 54
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.

"Seguridad para el Gestor de calendarios de empresa" en la página 55
El Gestor de seguridad le proporciona la capacidad de garantizar el asegurar el acceso a calendarios individuales en el Gestor de calendarios de empresa. Utilice el Gestor de seguridad para asignar roles a los miembros de la organización. Estos roles son los que determinan el nivel de acceso a los calendarios.

Información relacionada

"Configuración de la seguridad de WebSphere Process Server para un servidor autónomo" en la página 7
Configurar la seguridad de una instalación autónoma de WebSphere Process Server incluye tareas como la habilitación de seguridad administrativa y configuración de un registro de cuenta de usuario.

"Configuración de la seguridad de WebSphere Process Server para un servidor del entorno de despliegue" en la página 26
Configurar la seguridad de una instalación de entorno de despliegue de WebSphere Process Server incluye tareas como la habilitación de seguridad administrativa y configuración de un registro de cuenta de usuario.

Instalación de WebSphere Process Server: consideraciones sobre la seguridad

Considere cómo se implementará la seguridad antes, durante y después de 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.

Conceptos relacionados

"Iniciación a la seguridad" en la página 2
La seguridad es una consideración integral cuando se planifica la instalación de WebSphere Process Server, se desarrollan y despliegan aplicaciones, y en la ejecución cotidiana del servidor de procesos.

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

Preparación de sistemas i5/OS para la instalación

Información de autenticación proporcionada en el momento de la instalación

Durante la instalación, se le solicita información de seguridad para que el entorno de WebSphere Process Server quede protegido inmediatamente.

En los releases anteriores de WebSphere Process Server, se le solicitaba diferente información de autenticación durante la 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 cree 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 cree un perfil de WebSphere Process Server, se utilizan los valores por omisión para las credenciales de seguridad. Debe configurar estos valores de seguridad en la consola administrativa después de crear el perfil.

Por qué y cuándo se efectúa 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, muestre al panel 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.
   a. Seleccione el alias que desea cambiar; para ello, pulse su nombre en la columna **Alias**.

      Nota: En algunos casos, puede que la columna **Alias** no proporcione un enlace, en cuyo caso puede activar el recuadro de selección de la columna **Seleccionar** correspondiente al alias que desea editar y, a continuación, pulsar el botón **Editar**.
   b. En el panel siguiente, proporcione el nombre de usuario y la contraseña que se van a utilizar como alias de autenticación para este componente.

Nota: Las credenciales que proporcione deben existir en el depósito de cuentas de usuario que utilice.

c. Pulse **Aceptar**.

Tareas relacionadas

"Modificación de alias de autenticación" en la página 48
Tal vez tenga que modificar los alias de autenticación existentes.

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

Configurar la seguridad de una instalación autónoma de WebSphere Process Server incluye tareas como la habilitación de seguridad administrativa y configuración de un registro de cuenta de usuario.

Conceptos relacionados

"Iniciación a la seguridad" en la página 2
La seguridad es una consideración integral cuando se planifica la instalación de WebSphere Process Server, se desarrollan y despliegan aplicaciones, y en la ejecución cotidiana del servidor de procesos.

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.

Por qué y cuándo se efectúa 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.

Los pasos siguientes proporcionan un mapa de las tareas que debe realizar para habilitar la seguridad. En los temas que vienen a continuación se proporcionan detalles más concretos sobre estas tareas.

Procedimiento

1. Asegúrese de que está activada la seguridad administrativa. "Habilitación de la seguridad" en la página 10.
2. Asegúrese de que está activada la seguridad de aplicaciones. "Protección de aplicaciones en WebSphere Process Server" en la página 46.
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 depósito basado en archivos que incorporado en el sistema • Uno o más depósitos externos • El depósito incorporado basado en archivos y uno o varios depósitos 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. Consulte "Configuración del depósito de cuentas de usuarios del sistema operativo local o personalizado autónomo" en la página 15 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 cuentas de usuario.
Registro de usuarios autónomo	Consulte "Configuración del depósito de cuentas de usuarios del sistema operativo local o personalizado autónomo" en la página 15 para ver información detallada sobre cómo configurar el registro de cuentas de usuario.

5. Asegúrese de que ha establecido el registro seleccionado como registro actual.

   Si todavía no lo ha hecho, pulse **Establecer como actual** en la parte inferior de la página Proteger la administración, las aplicaciones y la infraestructura.
6. Asegúrese de aplicar los cambios después de seleccionar el registro de usuarios

   Si todavía no lo ha hecho, pulse **Aplicar** en la parte inferior de la página Proteger la administración, las aplicaciones y la infraestructura.
7. Vaya al panel Seguridad de Business Integration. Expanda **Seguridad** y pulse **Seguridad de Business Integration**.
8. 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.
9. 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**: Nombres de usuario y/o nombres 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**: Nombres de usuario y/o nombres 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 empresariales 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.

10. Aplique estos cambios.

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

11. Guarde los cambios en la configuración local.

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

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

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

Resultados

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

Qué hacer a continuación

Cada perfil que cree deberá 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. 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** de la consola administrativa para administrar las identidades y los alias.

Tareas relacionadas

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

"Protección de aplicaciones en WebSphere Process Server" en la página 46
En las aplicaciones que se despliegan en una instancia de WebSphere Process Server es necesario integrar la seguridad y aplicarla en tiempo de ejecución.

Información relacionada

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

Habilitación de la seguridad

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

Antes de empezar

Antes de iniciar estas tareas, instale WebSphere Process Server y verifique la instalación.

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.

Por qué y cuándo se efectúa esta tarea

Para obtener más información sobre la seguridad administrativa, la seguridad de aplicaciones y la seguridad de Java 2, consulte la información contenida en **Subtemas**.

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. Habilite la seguridad de aplicaciones.
   Seleccione **Habilitar seguridad de aplicaciones**.
4. 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 necesarios generan excepciones de control de accesos. 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).

5. Aplique estos cambios.

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

6. Guarde los cambios en la configuración local.

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

7. 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.

Conceptos relacionados

"Iniciación a la seguridad" en la página 2
La seguridad es una consideración integral cuando se planifica la instalación de WebSphere Process Server, se desarrollan y despliegan aplicaciones, y en la ejecución cotidiana del servidor de procesos.

Tareas relacionadas

"Protección de aplicaciones en WebSphere Process Server" en la página 46
En las aplicaciones que se despliegan en una instancia de WebSphere Process Server es necesario integrar la seguridad y aplicarla en tiempo de ejecución.

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 depósito 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 (por ejemplo, un sistema de desarrollo) en los que no es necesaria la seguridad. 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.

Por omisión, la seguridad administrativa de WebSphere Process Server esta habilitada. 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 de Java 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 depósito de cuentas de usuario

Los nombres de usuario y contraseñas de los usuarios registrados se almacenan en un depósito de cuentas de usuario. Puede utilizar el depósito de cuentas de usuario del sistema operativo local (es el valor por omisión), el protocolo LDAP (Lightweight Directory Access Protocol), depósitos federados o un depósito de cuentas personalizado.

Por qué y cuándo se efectúa esta tarea

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

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 usuarios que desea utilizar.

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

Registro de usuario	Acción
Depósitos federados	Especifique este valor para gestionar perfiles en diversos depósitos de un solo reino. El reino puede consistir en identidades en: • El depósito basado en archivos que incorporado en el sistema • Uno o más depósitos externos • El depósito incorporado basado en archivos y uno o varios depósitos externos. **Nota:** Solo un usuario con privilegios de administrador puede ver la configuración de los depósitos federados. Consulte Gestión del reino en una configuración de depósito federado para obtener más información.
Sistema operativo local	Éste es el registro de usuarios por omisión. Siga las instrucciones de "Configuración del depósito de cuentas de usuarios del sistema operativo local o personalizado autónomo" en la página 15. **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 usuarios.
Registro de usuarios personalizado	Siga las instrucciones del apartado "Configuración del depósito de cuentas de usuarios del sistema operativo local o personalizado autónomo" en la página 15 para elegir un depósito de cuentas personalizado y configúrelo según sus necesidades.

Registro de usuario	Acción
Tivoli Access Manager	**Nota:** Esta opción no está disponible mediante la consola administrativa. Se debe configurar utilizando el mandato wsadmin.

Conceptos relacionados

"Iniciación a la seguridad" en la página 2
La seguridad es una consideración integral cuando se planifica la instalación de WebSphere Process Server, se desarrollan y despliegan aplicaciones, y en la ejecución cotidiana del servidor de procesos.

Configuración del depósito de cuentas de usuarios del sistema operativo local o personalizado autónomo

Puede configurar el depósito de cuentas de usuario utilizando la consola administrativa. Los pasos para configurar el registro de cuentas del sistema operativo local, que es el valor por omisión, o uno personalizado autónomo son similares.

Por qué y cuándo se efectúa esta tarea

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 del 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: Escriba un nombre de usuario válido en el campo **Nombre de usuario administrativo primario**.

   Este valor es el nombre de un usuario con los privilegios administrativos que se define en el registro. Este nombre de usuario se utiliza para acceder a la consola administrativa. También lo utiliza el mandato wsadmin.
3. Seleccione la opción **Identidad de servidor generada automáticamente** o bien **Identidad de servidor almacenada en el depósito**.
   - Si selecciona **Identidad de servidor generada automáticamente**, el servidor de aplicaciones genera la identidad de servidor que se utiliza para la comunicación interna de procesos.

     Puede cambiar la identidad de este servidor en la página Mecanismos de autenticación y caducidad. Para acceder a la página Mecanismos de autenticación y caducidad, pulse **Seguridad → Proteger administración, aplicaciones e infraestructura → Mecanismos de autenticación y caducidad**. Cambie el valor del campo **ID de servidor interno**.
   - Si selecciona la opción **Identidad de servidor que se almacena en el depósito**, especifique la información siguiente:
     - En **ID de usuario o usuario administrativo del servidor en un nodo de la Versión 6.0.x**, especifique un ID de usuario que se utilice para ejecutar el servidor de aplicaciones para cuestiones de seguridad.
     - En **Contraseña**, especifique la contraseña asociada con este usuario.

4. Opcional: Para los registros personalizados autónomos, siga estos pasos:
   a. Verifique que el valor de **Nombre de clase del registro personalizado** sea el correcto o cámbielo si es necesario.
   b. Seleccione o desmarque el recuadro de selección **Ignorar mayúsculas para autorización**.

      Si selecciona esta opción, la comprobación de autorización es sensible a mayúsculas y minúsculas.
5. Pulse **Aplicar**.
6. En la parte inferior de la página Proteger administración, aplicaciones e infraestructura, pulse **Establecer como actual**.
7. Pulse **Aceptar** y **Aplicar** o **Guardar**.

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

Puede utilizar Tivoli Access Manager como depósito de cuentas de usuario; no obstante, debe configurarlo con el mandato wsadmin, fuera de la consola administrativa.

Por qué y cuándo se efectúa esta tarea

Tivoli Access Manager se puede utilizar como depósito 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, puede utilizar un LDAP (Lightweight Directory Access Protocol) externo como registro de usuarios.

Antes de empezar

En esta tarea se supone que tiene la seguridad administrativa activada.

Para acceder a un registro de usuarios utilizando LDAP, debe tener un nombre de usuario (ID) y una contraseña válidos, el sistema principal del servidor y el puerto del servidor de registro, el nombre distinguido base (DN) y, si es necesario, el DN de enlace y la contraseña de enlace.

En un entorno de Network Deployment, debe utilizar LDAP.

Puede elegir el usuario válido que desee en el registro de usuarios donde se pueden realizar búsquedas. Puede utilizar cualquier ID de usuario que tenga el rol administrativo para iniciar la sesión.

Procedimiento

1. Inicie la consola administrativa.
   - Si la seguridad está inhabilitada actualmente, se le solicitará un ID de usuario. Inicie una sesión con un ID de usuario cualquiera.
   - Si la seguridad está habilitada actualmente, se le solicitará un ID de usuario y una contraseña. Inicie la sesión con un ID de usuario administrativo y una contraseña predefinidos.

2. Expanda **Seguridad** y pulse **Proteger la administración, las aplicaciones y la infraestructura**.
3. En la página Proteger la administración, las aplicaciones y la infraestructura, siga estos pasos:
   a. Asegúrese de que esté seleccionado **Habilitar seguridad administrativa**.
   b. En la lista **Definiciones de reino disponibles**, seleccione **Registro LDAP autónomo**.
   c. Pulse **Configurar**.
4. En la pestaña **Configuración** de la página Registro LDAP autónomo, siga estos pasos:
   a. 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. También lo utiliza el mandato wsadmin.

      Puede especificar el nombre distinguido completo (DN) del usuario o el nombre abreviado del usuario, tal como se define en el filtro de usuario en la página Valores LDAP avanzados.
   b. Opcional: Seleccione la opción **Identidad de servidor generada automáticamente** o **Identidad de servidor que se almacena en el depósito**.
      - Si selecciona **Identidad de servidor generada automáticamente**, el servidor de aplicaciones genera la identidad de servidor que se utiliza para la comunicación de procesos internos.

        Puede cambiar esta identidad de servidor en la página Mecanismos de autenticación y caducidad. Para acceder a la página Mecanismos de autenticación y caducidad, pulse **Seguridad → Proteger la administración, las aplicaciones y la infraestructura → Mecanismos de autenticación y caducidad**. Cambie el valor del campo **ID de servidor interno**.
      - Si selecciona la opción **Identidad de servidor que se almacena en el depósito**, especifique la información siguiente:
        – Para **ID de usuario de servidor o usuario administrativo en un nodo de la Versión 6.0.x**, especifique un ID de usuario que se utiliza para ejecutar el servidor de aplicaciones a efectos de seguridad.
        – Para **Contraseña**, especifique la contraseña asociada con este usuario.

      Aunque este ID no es el ID de usuario del administrador LDAP, la entrada debe existir en LDAP.
   c. Opcional: Seleccione el servidor LDAP que desea utilizar en la lista **Tipo de servidor LDAP**.

      El tipo de servidor LDAP determina los filtros por omisión que utiliza WebSphere Process Server. Estos filtros por omisión cambian el campo **Tipo de servidor LDAP** a **Personalizado**, lo que indica que se utilizan filtros personalizados. Esta acción se produce después de pulsar **Aceptar** o **Aplicar** en la página Valores LDAP avanzados. Seleccione el tipo **Personalizado** en la lista y modifique los filtros de usuario y grupo para que utilicen otros servidores LDAP, si es necesario.

      Los usuarios de IBM Tivoli Directory Server pueden seleccionar **IBM Tivoli Directory Server** como tipo de directorio. Utilice el tipo de directorio IBM Tivoli Directory Server para aumentar el rendimiento.
   d. En el campo **Sistema principal**, especifique el nombre plenamente cualificado del sistema donde reside LDAP.

Puede especificar la dirección IP o el nombre del sistema de nombres de dominio (DNS).

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

   El nombre de sistema principal y el número de puerto representan el reino de este servidor LDAP en la célula de WebSphere Process Server. Por lo tanto, si los servidores en distintas células se comunican entre ellos utilizando símbolos LTPA (Lightweight Third Party Authentication), estos reinos deben coincidir exactamente en todas las células.

   El valor por omisión es 389.

   Si hay instalados varios WebSphere Process Server y se han configurado para ejecutarse en el mismo dominio de inicio de sesión individual, o si WebSphere Process Server interactúa con la versión anterior de WebSphere Process Server, asegúrese de que el número de puerto coincida en todas las configuraciones.

f. Opcional: Especifique el nombre distinguido base en el campo **Nombre distinguido base (DN)**.

   El nombre distinguido base indica que punto de partida de las búsquedas LDAP en este servidor de directorio LDAP. Por ejemplo, para un usuario con un DN `cn=John Doe, ou=Rochester, o=IBM, c=US`, especifique el DN base como una de estas opciones (suponiendo un sufijo c=us): `ou=Rochester, o=IBM, c=us`, `o=IBM c=us` o `c=us`.

   A efectos 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 un Lotus 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 **Ignorar mayúsculas/minúsculas para la autorización**.

   En WebSphere Process Server, el nombre distinguido se normaliza de acuerdo con la especificación LDAP (Lightweight Directory Access Protocol). La normalización cosiste en eliminar los espacios en el nombre distinguido base antes o después de las comas y los signos de igual. Un ejemplo de un nombre distinguido base no normalizado es `o = ibm, c = us` o `o=ibm, c=us`. Un ejemplo de un nombre distinguido base normalizado es `o=ibm,c=us`.

   Este campo es necesario para todos los directorios LDAP excepto para Domino Directory, donde este campo es opcional.

g. Opcional: especifique el nombre DN de enlace en el campo **Nombre distinguido base**.

   El DN de enlace es necesario si no se pueden utilizar enlaces anónimos en el servidor LDAP para obtener información de usuarios y grupos.

   Si el servidor LDAP se configura para utilizar enlaces anónimos, deje este campo en blanco. Si no se especifica un nombre, el servidor de aplicaciones se enlaza de forma anónima. Consulte la descripción del campo Nombre distinguido base para ver ejemplos de nombres distinguidos.

h. Opcional: Especifique la contraseña correspondiente al DN de enlace en el campo **Contraseña de enlace**.

i. Opcional: Modifique el valor de **Tiempo de espera de búsqueda**.

   Este valor de tiempo de espera es la cantidad máxima de tiempo que el servidor LDAP espera antes de enviar una respuesta al cliente del producto antes de detener la solicitud. El valor por omisión es de 120 segundos.

j. Asegúrese de que esté seleccionado **Reutilizar conexión**.

Esta opción especifica que el servidor debe reutilizar la conexión LDAP. Deseleccione esta opción sólo en casos excepcionales, cuando se utilice un direccionador para enviar solicitudes a varios servidores LDAP y el direccionador no dé soporte a la afinidad. Deje esta opción seleccionada en los demás casos.

k. Opcional: Compruebe que esté habilitada la opción **Ignorar mayúsculas y minúsculas para autorización**.

   Cuando habilita esta opción, la comprobación de autorización no es sensible a las mayúsculas y minúsculas.

   Normalmente, una comprobación de autorización implica una comprobación del DN completo de un usuario, que es exclusivo en el servidor LDAP y es sensible a las mayúsculas y minúsculas. No obstante, cuando utiliza los servidores LDAP IBM Directory Server o Sun ONE (anteriormente iPlanet) Directory Server, debe habilitar esta opción porque la información de grupo que se obtiene de los servidores LDAP no es coherente en cuanto al uso de mayúsculas y minúsculas. Esta incoherencia afecta sólo a la comprobación de autorización. De lo contrario, este campo es opcional y puede habilitarse cuando se necesita una comprobación de autorización sensible a las mayúsculas y minúsculas.

   Por ejemplo, puede seleccionar esta opción cuando utiliza certificados y el contenido del certificado no coincide con las mayúsculas y minúsculas de la entrada en el servidor LDAP. También puede habilitar **Ignorar mayúsculas y minúsculas para autorización** cuando utiliza el inicio de sesión individual (SSO) entre el producto y Lotus Domino.

   El valor por omisión es habilitado.

l. Opcional: Seleccione **Habilitado para SSL** si desea utilizar comunicaciones de Capa de sockets seguros con el servidor LDAP.

   Si selecciona la opción **Habilitado para SSL**, puede seleccionar **Gestionado centralmente** o **Utilizar alias SSL específico**.

   - **Gestionado centralmente**

     Esta opción permite especificar una configuración SSL para un ámbito concreto como, por ejemplo, la célula, el nodo, el servidor o el clúster en una ubicación. Para utilizar la opción **Gestionado centralmente**, debe especificar la configuración SSL para el conjunto específico de puntos finales.

     La página Gestionar configuraciones de seguridad de punto final muestra todos los puntos finales de entrada y salida que utilizan el protocolo SSL.

     Expanda la sección **Entrada** o **Salida** de la página Gestionar configuraciones de seguridad de punto final y pulse el nombre de un nodo para especificar una configuración SSL que se utiliza para cada punto final del nodo. Para un registro LDAP, puede alterar temporalmente la configuración SSL heredada especificando una configuración SSL para LDAP.

   - **Utilizar alias SSL específico**

     Esta opción se utiliza para seleccionar una de las configuraciones SSL en la lista debajo de la opción.

     Esta configuración se utiliza sólo cuando SSL está habilitado para LDAP. El valor por omisión es **NodeDefaultSSLSettings**.

m. Pulse **Aceptar** y **Aplicar** o **Guardar** hasta que vuelva a la página Proteger la administración, las aplicaciones y la infraestructura.

5. En la página Proteger la administración, las aplicaciones y la infraestructura, pulse **Establecer como actual**.

6. Pulse **Aceptar** y **Aplicar** o **Guardar**.

Qué hacer a continuación

Guarde, detenga y reinicie todos los servidores para que se apliquen las actualizaciones.

Si el servidor se inicia sin problemas, la configuración es correcta.

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* en un indicador de mandatos del 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.

Detener el servidor	Detalles
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* en un indicador de mandatos en el *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 siete 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 2. 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 (es decir, 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 El 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.
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.

El gestor de sucesos anómalo puede estar operado por cualquier usuario con el rol de administrador u operador.

Los selectores pueden estar configurados por cualquier usuario con el rol de administrador o configurador.

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.

Los componentes de Business Process Choreographer, Common Event Infrastructure y Service Component Architecture 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 empresariales tienen alias de autenticación predefinidos. Modifique estos alias mediante la consola administrativa.

Los alias de la Tabla 3 en la página 24 se utilizan para invocar los componentes independientemente de la identidad del usuario que invoque.

Tabla 3. Alias de autenticación asociados con procesos empresariales.

Alias	Descripción	Información
BPEAuthDataAliasJMS_*nodo_servidor*	Se utiliza para autenticar con el motor de mensajería.	Entre los valores de nombre de usuario y contraseña en el panel de configuración de Business Process Choreographer de la Herramienta de gestión 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 4 describe los roles RunAs creados para los procesos empresariales.

Tabla 4. Roles RunAs asociados con procesos empresariales.

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

El nombre de usuario suministrado se añade al rol RunAs.

Alias de autenticación de Common Event Infrastructure

Common Event Infrastructure tiene alias de autenticación predefinidos. 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 Common Event Infrastructure.

Alias	Descripción	Información
CommonEventInfrastructure JMSAuthAlias **Nota:** El nombre de alias real no contiene un carácter de espacio.	Se utiliza para autenticar con el motor de mensajería.	Entre los valores de nombre de usuario y contraseña en el panel de configuración de Common Event Infrastructure de la Herramienta de gestión de perfiles.

Tabla 5. Alias de autenticación asociados con Common Event Infrastructure. (continuación)

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

Alias de autenticación de Service Component Architecture

SCA (Service Component Architecture) tiene un alias de autenticación predefinido. Modifique el alias utilizando la consola administrativa.

El alias de la Tabla 6 se utiliza para invocar los componentes independientemente de la identidad del usuario que invoque.

Tabla 6. Alias de autenticación asociado a componentes SCA

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

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

Business Process Choreographer se instala como parte de la instalación de WebSphere Process Server. Durante la instalación, se instalan los archivos EAR (enterprise archive) que tienen roles asociados (para el control de accesos). El gestor de tareas de usuario utiliza los roles para determinar las posibilidades del usuario en un sistema de producción.

Los archivos EAR y los roles asociados se muestran en Tabla 7.

Tabla 7. Roles y permisos por omisión para archivos EAR

Archivo EAR	Roles	Permiso por omisión	Notas
bpecontainer.ear	BPESystem Administrator	Nombre de grupo entrado durante la instalación.	Tiene acceso a todos los procesos empresariales y a todas las operaciones.
bpecontainer.ear	BPESystemMonitor	Todos los usuarios autenticados.	Tiene acceso a operaciones de lectura.
task.ear	TaskSystem Administrator	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.

Tabla 7. Roles y permisos por omisión para archivos EAR (continuación)

Archivo EAR	Roles	Permiso por omisión	Notas
Bpcexplorer.ear	WebClientUser	Todos los usuarios autenticados.	Puede acceder a Business Process Choreographer Explorer.

Control de acceso en aplicaciones de Common Event Infrastructure

Common Event Infrastructure se instala como parte de la instalación de WebSphere Process Server. Durante la instalación, se instala el archivo EventServer.ear, que tiene roles asociados (para el control de accesos).

El archivo EventServer.ear tiene asociados los roles siguientes:

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

Configurar la seguridad de una instalación de entorno de despliegue de WebSphere Process Server incluye tareas como la habilitación de seguridad administrativa y configuración de un registro de cuenta de usuario.

Conceptos relacionados

"Iniciación a la seguridad" en la página 2
La seguridad es una consideración integral cuando se planifica la instalación de WebSphere Process Server, se desarrollan y despliegan aplicaciones, y en la ejecución cotidiana del servidor de procesos.

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.

Por qué y cuándo se efectúa 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.

Los pasos siguientes proporcionan un mapa de las tareas que debe realizar para habilitar la seguridad. En los temas que vienen a continuación se proporcionan detalles más concretos sobre estas tareas.

Procedimiento

1. Compruebe que la seguridad administrativa esté activada. "Habilitación de la seguridad" en la página 10.
2. Compruebe que la seguridad de aplicaciones esté activada. "Protección de aplicaciones en WebSphere Process Server" en la página 46.
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 depósito basado en archivos que incorporado en el sistema • Uno o más depósitos externos • El depósito incorporado basado en archivos y uno o varios depósitos 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 usuarios del sistema operativo local o personalizado autónomo" en la página 15 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 de usuario	Acción
Registro personalizado autónomo	Consulte "Configuración del depósito de cuentas de usuarios del sistema operativo local o personalizado autónomo" en la página 15 para ver información detallada sobre cómo configurar el registro de cuentas de usuario.

5. Asegúrese de que ha establecido el registro seleccionado como registro actual.

   Si todavía no lo ha hecho, pulse **Establecer como actual** en la parte inferior de la página Proteger la administración, las aplicaciones y la infraestructura.
6. Asegúrese de aplicar los cambios después de seleccionar el registro de usuarios

   Si todavía no lo ha hecho, pulse **Aplicar** en la parte inferior de la página Proteger la administración, las aplicaciones y la infraestructura.
7. Vaya al panel de Seguridad de Business Integration. Expanda **Seguridad** y pulse **Seguridad de Business Integration**.
8. Proporcione las identidades de usuario adecuadas para los alias de autenticación que se listan. La credencial que proporcione debe existir en el depósito 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.
9. En el mismo panel, puede configurar la seguridad de Business Process Choreographer.

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

   - **Administrador**: Nombres de usuario y/o nombres 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**: Nombres de usuario y/o nombres 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 empresariales y de tarea.

   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.
10. Aplique estos cambios.

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

    Pulse **Guardar** en el panel del mensaje.
12. 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**.
13. Si es necesario, detenga y reinicie el servidor.

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

Resultados

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

Qué hacer a continuación

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 depósito 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

"Habilitación de la seguridad" en la página 10
El primer paso para proteger su entorno y sus aplicaciones de WebSphere Process Server es habilitar la seguridad administrativa.

"Protección de aplicaciones en WebSphere Process Server" en la página 46
En las aplicaciones que se despliegan en una instancia de WebSphere Process Server es necesario integrar la seguridad y aplicarla en tiempo de ejecución.

Información relacionada

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

Habilitación de la seguridad

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

Antes de empezar

Antes de iniciar estas tareas, instale WebSphere Process Server y verifique la instalación.

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.

Por qué y cuándo se efectúa esta tarea

Para obtener más información sobre la seguridad administrativa, la seguridad de aplicaciones y la seguridad de Java 2, consulte la información contenida en **Subtemas**.

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. Habilite la seguridad de aplicaciones.

   Seleccione **Habilitar seguridad de aplicaciones**.

4. 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 necesarios generan excepciones de control de accesos. 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).

5. Aplique estos cambios.

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

6. Guarde los cambios en la configuración local.

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

7. 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.

Conceptos relacionados

"Iniciación a la seguridad" en la página 2
La seguridad es una consideración integral cuando se planifica la instalación de WebSphere Process Server, se desarrollan y despliegan aplicaciones, y en la ejecución cotidiana del servidor de procesos.

Tareas relacionadas

"Protección de aplicaciones en WebSphere Process Server" en la página 46
En las aplicaciones que se despliegan en una instancia de WebSphere Process Server es necesario integrar la seguridad y aplicarla en tiempo de ejecución.

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 depósito 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 (por ejemplo, un sistema de desarrollo) en los que no es necesaria la seguridad. 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.

Por omisión, la seguridad administrativa de WebSphere Process Server esta habilitada. 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 de Java 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 depósito de cuentas de usuario

Los nombres de usuario y contraseñas de los usuarios registrados se almacenan en un depósito de cuentas de usuario. Puede utilizar el depósito de cuentas de usuario del sistema operativo local (es el valor por omisión), el protocolo LDAP (Lightweight Directory Access Protocol), depósitos federados o un depósito de cuentas personalizado.

Por qué y cuándo se efectúa esta tarea

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

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 usuarios que desea utilizar.

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

Registro de usuario	Acción
Depósitos federados	Especifique este valor para gestionar perfiles en diversos depósitos de un solo reino. El reino puede consistir en identidades en: • El depósito basado en archivos que incorporado en el sistema • Uno o más depósitos externos • El depósito incorporado basado en archivos y uno o varios depósitos externos. **Nota:** Solo un usuario con privilegios de administrador puede ver la configuración de los depósitos federados. Consulte Gestión del reino en una configuración de depósito federado para obtener más información.
Sistema operativo local	Éste es el registro de usuarios por omisión. Siga las instrucciones de "Configuración del depósito de cuentas de usuarios del sistema operativo local o personalizado autónomo" en la página 15. **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 usuarios.
Registro de usuarios personalizado	Siga las instrucciones del apartado "Configuración del depósito de cuentas de usuarios del sistema operativo local o personalizado autónomo" en la página 15 para elegir un depósito de cuentas personalizado y configúrelo según sus necesidades.
Tivoli Access Manager	**Nota:** Esta opción no está disponible mediante la consola administrativa. Se debe configurar utilizando el mandato wsadmin.

Conceptos relacionados

"Iniciación a la seguridad" en la página 2
La seguridad es una consideración integral cuando se planifica la instalación de WebSphere Process Server, se desarrollan y despliegan aplicaciones, y en la ejecución cotidiana del servidor de procesos.

Configuración del depósito de cuentas de usuarios del sistema operativo local o personalizado autónomo

Puede configurar el depósito de cuentas de usuario utilizando la consola administrativa. Los pasos para configurar el registro de cuentas del sistema operativo local, que es el valor por omisión, o uno personalizado autónomo son similares.

Por qué y cuándo se efectúa esta tarea

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 del 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: Escriba un nombre de usuario válido en el campo **Nombre de usuario administrativo primario**.

   Este valor es el nombre de un usuario con los privilegios administrativos que se define en el registro. Este nombre de usuario se utiliza para acceder a la consola administrativa. También lo utiliza el mandato wsadmin.
3. Seleccione la opción **Identidad de servidor generada automáticamente** o bien **Identidad de servidor almacenada en el depósito**.
   - Si selecciona **Identidad de servidor generada automáticamente**, el servidor de aplicaciones genera la identidad de servidor que se utiliza para la comunicación interna de procesos.

     Puede cambiar la identidad de este servidor en la página Mecanismos de autenticación y caducidad. Para acceder a la página Mecanismos de autenticación y caducidad, pulse **Seguridad → Proteger administración, aplicaciones e infraestructura → Mecanismos de autenticación y caducidad**. Cambie el valor del campo **ID de servidor interno**.
   - Si selecciona la opción **Identidad de servidor que se almacena en el depósito**, especifique la información siguiente:
     - En **ID de usuario o usuario administrativo del servidor en un nodo de la Versión 6.0.x**, especifique un ID de usuario que se utilice para ejecutar el servidor de aplicaciones para cuestiones de seguridad.
     - En **Contraseña**, especifique la contraseña asociada con este usuario.
4. Opcional: Para los registros personalizados autónomos, siga estos pasos:
   a. Verifique que el valor de **Nombre de clase del registro personalizado** sea el correcto o cámbielo si es necesario.
   b. Seleccione o desmarque el recuadro de selección **Ignorar mayúsculas para autorización**.

      Si selecciona esta opción, la comprobación de autorización es sensible a mayúsculas y minúsculas.
5. Pulse **Aplicar**.
6. En la parte inferior de la página Proteger administración, aplicaciones e infraestructura, pulse **Establecer como actual**.
7. Pulse **Aceptar** y **Aplicar** o **Guardar**.

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

Puede utilizar Tivoli Access Manager como depósito de cuentas de usuario; no obstante, debe configurarlo con el mandato wsadmin, fuera de la consola administrativa.

Por qué y cuándo se efectúa esta tarea

Tivoli Access Manager se puede utilizar como depósito 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, puede utilizar un LDAP (Lightweight Directory Access Protocol) externo como registro de usuarios.

Antes de empezar

En esta tarea se supone que tiene la seguridad administrativa activada.

Para acceder a un registro de usuarios utilizando LDAP, debe tener un nombre de usuario (ID) y una contraseña válidos, el sistema principal del servidor y el puerto del servidor de registro, el nombre distinguido base (DN) y, si es necesario, el DN de enlace y la contraseña de enlace.

En un entorno de Network Deployment, debe utilizar LDAP.

Puede elegir el usuario válido que desee en el registro de usuarios donde se pueden realizar búsquedas. Puede utilizar cualquier ID de usuario que tenga el rol administrativo para iniciar la sesión.

Procedimiento

1. Inicie la consola administrativa.
   - Si la seguridad está inhabilitada actualmente, se le solicitará un ID de usuario. Inicie una sesión con un ID de usuario cualquiera.
   - Si la seguridad está habilitada actualmente, se le solicitará un ID de usuario y una contraseña. Inicie la sesión con un ID de usuario administrativo y una contraseña predefinidos.
2. Expanda **Seguridad** y pulse **Proteger la administración, las aplicaciones y la infraestructura**.
3. En la página Proteger la administración, las aplicaciones y la infraestructura, siga estos pasos:
   a. Asegúrese de que esté seleccionado **Habilitar seguridad administrativa**.
   b. En la lista **Definiciones de reino disponibles**, seleccione **Registro LDAP autónomo**.
   c. Pulse **Configurar**.
4. En la pestaña **Configuración** de la página Registro LDAP autónomo, siga estos pasos:
   a. 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. También lo utiliza el mandato wsadmin.

Puede especificar el nombre distinguido completo (DN) del usuario o el nombre abreviado del usuario, tal como se define en el filtro de usuario en la página Valores LDAP avanzados.

b. Opcional: Seleccione la opción **Identidad de servidor generada automáticamente** o **Identidad de servidor que se almacena en el depósito**.
   - Si selecciona **Identidad de servidor generada automáticamente**, el servidor de aplicaciones genera la identidad de servidor que se utiliza para la comunicación de procesos internos.

     Puede cambiar esta identidad de servidor en la página Mecanismos de autenticación y caducidad. Para acceder a la página Mecanismos de autenticación y caducidad, pulse **Seguridad → Proteger la administración, las aplicaciones y la infraestructura → Mecanismos de autenticación y caducidad**. Cambie el valor del campo **ID de servidor interno**.
   - Si selecciona la opción **Identidad de servidor que se almacena en el depósito**, especifique la información siguiente:
     – Para **ID de usuario de servidor o usuario administrativo en un nodo de la Versión 6.0.x**, especifique un ID de usuario que se utiliza para ejecutar el servidor de aplicaciones a efectos de seguridad.
     – Para **Contraseña**, especifique la contraseña asociada con este usuario.

   Aunque este ID no es el ID de usuario del administrador LDAP, la entrada debe existir en LDAP.

c. Opcional: Seleccione el servidor LDAP que desea utilizar en la lista **Tipo de servidor LDAP**.

   El tipo de servidor LDAP determina los filtros por omisión que utiliza WebSphere Process Server. Estos filtros por omisión cambian el campo **Tipo de servidor LDAP** a **Personalizado**, lo que indica que se utilizan filtros personalizados. Esta acción se produce después de pulsar **Aceptar** o **Aplicar** en la página Valores LDAP avanzados. Seleccione el tipo **Personalizado** en la lista y modifique los filtros de usuario y grupo para que utilicen otros servidores LDAP, si es necesario.

   Los usuarios de IBM Tivoli Directory Server pueden seleccionar **IBM Tivoli Directory Server** como tipo de directorio. Utilice el tipo de directorio IBM Tivoli Directory Server para aumentar el rendimiento.

d. En el campo **Sistema principal**, especifique el nombre plenamente cualificado del sistema donde reside LDAP.

   Puede especificar la dirección IP o el nombre del sistema de nombres de dominio (DNS).

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

   El nombre de sistema principal y el número de puerto representan el reino de este servidor LDAP en la célula de WebSphere Process Server. Por lo tanto, si los servidores en distintas células se comunican entre ellos utilizando símbolos LTPA (Lightweight Third Party Authentication), estos reinos deben coincidir exactamente en todas las células.

   El valor por omisión es 389.

   Si hay instalados varios WebSphere Process Server y se han configurado para ejecutarse en el mismo dominio de inicio de sesión individual, o si WebSphere Process Server interactúa con la versión anterior de WebSphere Process Server, asegúrese de que el número de puerto coincida en todas las configuraciones.

f. Opcional: Especifique el nombre distinguido base en el campo **Nombre distinguido base (DN)**.

El nombre distinguido base indica que punto de partida de las búsquedas LDAP en este servidor de directorio LDAP. Por ejemplo, para un usuario con un DN `cn=John Doe, ou=Rochester, o=IBM, c=US`, especifique el DN base como una de estas opciones (suponiendo un sufijo c=us): `ou=Rochester, o=IBM, c=us`, `o=IBM c=us` o `c=us`.

A efectos 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 un Lotus 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 **Ignorar mayúsculas/minúsculas para la autorización**.

En WebSphere Process Server, el nombre distinguido se normaliza de acuerdo con la especificación LDAP (Lightweight Directory Access Protocol). La normalización cosiste en eliminar los espacios en el nombre distinguido base antes o después de las comas y los signos de igual. Un ejemplo de un nombre distinguido base no normalizado es `o = ibm, c = us` o `o=ibm, c=us`. Un ejemplo de un nombre distinguido base normalizado es `o=ibm,c=us`.

Este campo es necesario para todos los directorios LDAP excepto para Domino Directory, donde este campo es opcional.

g. Opcional: especifique el nombre DN de enlace en el campo **Nombre distinguido base**.

   El DN de enlace es necesario si no se pueden utilizar enlaces anónimos en el servidor LDAP para obtener información de usuarios y grupos.

   Si el servidor LDAP se configura para utilizar enlaces anónimos, deje este campo en blanco. Si no se especifica un nombre, el servidor de aplicaciones se enlaza de forma anónima. Consulte la descripción del campo Nombre distinguido base para ver ejemplos de nombres distinguidos.

h. Opcional: Especifique la contraseña correspondiente al DN de enlace en el campo **Contraseña de enlace**.

i. Opcional: Modifique el valor de **Tiempo de espera de búsqueda**.

   Este valor de tiempo de espera es la cantidad máxima de tiempo que el servidor LDAP espera antes de enviar una respuesta al cliente del producto antes de detener la solicitud. El valor por omisión es de 120 segundos.

j. Asegúrese de que esté seleccionado **Reutilizar conexión**.

   Esta opción especifica que el servidor debe reutilizar la conexión LDAP. Deseleccione esta opción sólo en casos excepcionales, cuando se utilice un direccionador para enviar solicitudes a varios servidores LDAP y el direccionador no dé soporte a la afinidad. Deje esta opción seleccionada en los demás casos.

k. Opcional: Compruebe que esté habilitada la opción **Ignorar mayúsculas y minúsculas para autorización**.

   Cuando habilita esta opción, la comprobación de autorización no es sensible a las mayúsculas y minúsculas.

   Normalmente, una comprobación de autorización implica una comprobación del DN completo de un usuario, que es exclusivo en el servidor LDAP y es sensible a las mayúsculas y minúsculas. No obstante, cuando utiliza los servidores LDAP IBM Directory Server o Sun ONE (anteriormente iPlanet) Directory Server, debe habilitar esta opción porque la información de grupo que se obtiene de los servidores LDAP no es coherente en cuanto al uso de mayúsculas y minúsculas. Esta incoherencia afecta sólo a la comprobación

de autorización. De lo contrario, este campo es opcional y puede habilitarse cuando se necesita una comprobación de autorización sensible a las mayúsculas y minúsculas.

Por ejemplo, puede seleccionar esta opción cuando utiliza certificados y el contenido del certificado no coincide con las mayúsculas y minúsculas de la entrada en el servidor LDAP. También puede habilitar **Ignorar mayúsculas y minúsculas para autorización** cuando utiliza el inicio de sesión individual (SSO) entre el producto y Lotus Domino.

El valor por omisión es habilitado.

l. Opcional: Seleccione **Habilitado para SSL** si desea utilizar comunicaciones de Capa de sockets seguros con el servidor LDAP.

Si selecciona la opción **Habilitado para SSL**, puede seleccionar **Gestionado centralmente** o **Utilizar alias SSL específico**.

- **Gestionado centralmente**

  Esta opción permite especificar una configuración SSL para un ámbito concreto como, por ejemplo, la célula, el nodo, el servidor o el clúster en una ubicación. Para utilizar la opción **Gestionado centralmente**, debe especificar la configuración SSL para el conjunto específico de puntos finales.

  La página Gestionar configuraciones de seguridad de punto final muestra todos los puntos finales de entrada y salida que utilizan el protocolo SSL.

  Expanda la sección **Entrada** o **Salida** de la página Gestionar configuraciones de seguridad de punto final y pulse el nombre de un nodo para especificar una configuración SSL que se utiliza para cada punto final del nodo. Para un registro LDAP, puede alterar temporalmente la configuración SSL heredada especificando una configuración SSL para LDAP.

- **Utilizar alias SSL específico**

  Esta opción se utiliza para seleccionar una de las configuraciones SSL en la lista debajo de la opción.

  Esta configuración se utiliza sólo cuando SSL está habilitado para LDAP. El valor por omisión es **NodeDefaultSSLSettings**.

m. Pulse **Aceptar** y **Aplicar** o **Guardar** hasta que vuelva a la página Proteger la administración, las aplicaciones y la infraestructura.

5. En la página Proteger la administración, las aplicaciones y la infraestructura, pulse **Establecer como actual**.
6. Pulse **Aceptar** y **Aplicar** o **Guardar**.

Qué hacer a continuación

Guarde, detenga y reinicie todos los servidores para que se apliquen las actualizaciones.

Si el servidor se inicia sin problemas, la configuración es correcta.

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* en un indicador de mandatos del 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.

Detener el servidor	Detalles
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* en un indicador de mandatos en el *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 siete 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 8. 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 (es decir, 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 El 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.
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.

El gestor de sucesos anómalo puede estar operado por cualquier usuario con el rol de administrador u operador.

Los selectores pueden estar configurados por cualquier usuario con el rol de administrador o configurador.

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.

Los componentes de Business Process Choreographer, Common Event Infrastructure y Service Component Architecture 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 empresariales tienen alias de autenticación predefinidos. Modifique estos alias mediante la consola administrativa.

Los alias de la Tabla 3 en la página 24 se utilizan para invocar los componentes independientemente de la identidad del usuario que invoque.

Tabla 9. Alias de autenticación asociados con procesos empresariales.

Alias	Descripción	Información
BPEAuthDataAliasJMS_*nodo_servidor*	Se utiliza para autenticar con el motor de mensajería.	Entre los valores de nombre de usuario y contraseña en el panel de configuración de Business Process Choreographer de la Herramienta de gestión 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 4 en la página 24 describe los roles RunAs creados para los procesos empresariales.

Tabla 10. Roles RunAs asociados con procesos empresariales.

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

El nombre de usuario suministrado se añade al rol RunAs.

Alias de autenticación de Common Event Infrastructure

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

Los alias de la Tabla 5 en la página 24 se utilizan para invocar los componentes independientemente de la identidad del usuario que invoque.

Tabla 11. Alias de autenticación asociados con Common Event Infrastructure.

Alias	Descripción	Información
CommonEventInfrastructure JMSAuthAlias **Nota:** El nombre de alias real no contiene un carácter de espacio.	Se utiliza para autenticar con el motor de mensajería.	Entre los valores de nombre de usuario y contraseña en el panel de configuración de Common Event Infrastructure de la Herramienta de gestión de perfiles.

Tabla 11. Alias de autenticación asociados con Common Event Infrastructure. (continuación)

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

Alias de autenticación de Service Component Architecture

SCA (Service Component Architecture) tiene un alias de autenticación predefinido. Modifique el alias utilizando la consola administrativa.

El alias de la Tabla 6 en la página 25 se utiliza para invocar los componentes independientemente de la identidad del usuario que invoque.

Tabla 12. Alias de autenticación asociado a componentes SCA

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

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

Business Process Choreographer se instala como parte de la instalación de WebSphere Process Server. Durante la instalación, se instalan los archivos EAR (enterprise archive) que tienen roles asociados (para el control de accesos). El gestor de tareas de usuario utiliza los roles para determinar las posibilidades del usuario en un sistema de producción.

Los archivos EAR y los roles asociados se muestran en Tabla 7 en la página 25.

Tabla 13. Roles y permisos por omisión para archivos EAR

Archivo EAR	Roles	Permiso por omisión	Notas
bpecontainer.ear	BPESystem Administrator	Nombre de grupo entrado durante la instalación.	Tiene acceso a todos los procesos empresariales y a todas las operaciones.
bpecontainer.ear	BPESystemMonitor	Todos los usuarios autenticados.	Tiene acceso a operaciones de lectura.
task.ear	TaskSystem Administrator	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.

Tabla 13. Roles y permisos por omisión para archivos EAR (continuación)

Archivo EAR	Roles	Permiso por omisión	Notas
Bpcexplorer.ear	WebClientUser	Todos los usuarios autenticados.	Puede acceder a Business Process Choreographer Explorer.

Control de acceso en aplicaciones de Common Event Infrastructure

Common Event Infrastructure se instala como parte de la instalación de WebSphere Process Server. Durante la instalación, se instala el archivo EventServer.ear, que tiene roles asociados (para el control de accesos).

El archivo EventServer.ear tiene asociados los roles siguientes:

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.

Por qué y cuándo se efectúa 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. La seguridad de estas aplicaciones es de suma importancia.

Proteja las aplicaciones realizando las tareas siguientes:

Procedimiento

1. Asegúrese de que está habilitada la seguridad administrativa.
2. Asegúrese de que está habilitada la seguridad de aplicaciones.
   a. En la consola administrativa, expanda **Seguridad** y pulse **Proteger la administración, las aplicaciones y la infraestructura**.
   b. Seleccione **Habilitar la seguridad de la aplicación** para que WebSphere Process Server necesite la autenticación de los usuarios que intentan acceder a una aplicación protegida.
3. Desarrolle las aplicaciones en WebSphere Integration Developer utilizando todas las características de seguridad apropiadas.

4. Despliegue las aplicaciones en el entorno de WebSphere Process Server, asignando los usuarios y grupos a los roles de seguridad apropiados.
5. Mantenga la seguridad del entorno de WebSphere Process Server.

Tareas relacionadas

"Habilitación de la seguridad" en la página 10
El primer paso para proteger su entorno y sus aplicaciones de WebSphere Process Server es habilitar la seguridad administrativa.

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.

La seguridad en WebSphere Process Server puede dividirse en tres amplias agrupaciones:

- 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 usuarios.
- 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; de lo contrario, la aplicación no se ejecutará.

Integridad y privacidad de los datos

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, que se consigue a través del 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 pueden, por turno, aplicar el control de acceso.

Autenticación de usuarios

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.

Tabla 14 lista los clientes típicos que pueden invocar los componentes de WebSphere Process Server y las opciones de autenticación disponibles para cada tipo de cliente.

Tabla 14. 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.

Por qué y cuándo se efectúa esta tarea

Modifique los alias de autenticación de la consola administrativa.

Procedimiento

1. Acceda al panel Alias de autenticación de Business Integration.

   Desde la consola administrativa, expanda **Seguridad**, y pulse **Business Integration Security**.

   Nota: También puede acceder a este panel desde varios paneles de la consola administrativa que requieren la información del alias de autenticación. Aparece el panel Configuración del alias de autenticación.

Este panel contiene una lista de alias de autenticación, el componente asociado, el ID de usuario asociado con este alias y, opcionalmente, una descripción del alias.

2. Seleccione el alias de autenticación que desea modificar; para ello, pulse su nombre en la columna **Alias**.

   Nota: En algunos casos, puede que la columna **Alias** no proporcione un enlace, en cuyo caso puede activar el recuadro de selección de la columna **Seleccionar** correspondiente al alias que desea editar y, a continuación, pulsar el botón **Editar**.

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 6
Cuando cree un perfil de WebSphere Process Server, se utilizan los valores por omisión 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.

A diferencia de la seguridad basada en roles J2EE, que protege la operación de los componentes, el control de acceso basado en roles protege los *recursos*. Por ejemplo, en el Gestor de calendarios de empresa, puede especificar el tipo de acceso que tienen los usuarios a los calendarios individuales. Utilice el Gestor de seguridad en

Business Space para especificar, para cada calendario, el propietario del calendario, así como aquellos que tienen acceso de escritura y lectura al calendario.

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.

A continuación, se proporcionan detalles de estos componentes.

Tabla 15. Los archivos .ear y los roles J2EE asociados

Archivo EAR	**Rol J2EE**	**Asignación de usuario**
BPCExplorer_<nodo>_<servidor>	CleanupUser	Todos los autenticados
BPCObserver_<nodo>_<servidor>	ObserverUser	Todos los autenticados
BPEContainer_<nodo>_<servidor>	BPEAPIUser	Todos los autenticados
	BPESystemAdministrator	wsadmin
	BPESystemMonitor	wsadmin
	CleanupUser	Todos los autenticados
	JMSAPIUser	Todos los autenticados
Pasarela de servicios REST	RestServicesUser	Todos los autenticados
TaskContainer_<nodo>_<servidor>	TaskAPIUser	Todos los autenticados
	TaskSystemAdministrator	wsadmin
	TaskSystemMonitor	wsadmin
	EscalationUser	Todos los autenticados
	CleanupUser	Todos los autenticados
wpsFEMgr_6.2.0	WBIOperator	Todos
EventService (*)	eventAdministrator	Todos los autenticados
	eventConsumer	Todos los autenticados
	eventUpdater	Todos los autenticados
	eventCreator	Todos los autenticados
	catalogAdministrator	Todos los autenticados
	catalogReader	Todos los autenticados

(*) EventService es una aplicación del sistema y no aparece en la consola administrativa en Aplicaciones de empresa.

Tareas relacionadas

"Seguridad para el Gestor de calendarios de empresa" en la página 55
El Gestor de seguridad le proporciona la capacidad de garantizar el asegurar el acceso a calendarios individuales en el Gestor de calendarios de empresa. Utilice el Gestor de seguridad para asignar roles a los miembros de la organización. Estos roles son los que determinan el nivel de acceso a los calendarios.

Información relacionada


Centro de información de WebSphere Integration Developer

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

Visión general de la planificación de seguridad

Edición de las propiedades del despliegue de módulo

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

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

Por qué y cuándo se efectúa esta tarea

Los detalles sobre cómo configurar el cliente Web de los servicios Web para utilizar SSL se proporcionan en esta WebSphere Application Server nota técnica. En el WebSphere Application Server tema Protección de aplicaciones de servicios Web en el nivel de transporte se puede encontrar una descripción más general sobre cómo proteger los servicios Web.

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 pasa por múltiples sistemas dentro de la empresa, el cliente sólo debe 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

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.

Por qué y cuándo se efectúa 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 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.

Conceptos relacionados

"Iniciación a la seguridad" en la página 2
La seguridad es una consideración integral cuando se planifica la instalación de WebSphere Process Server, se desarrollan y despliegan aplicaciones, y en la ejecución cotidiana del servidor de procesos.

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.

Por qué y cuándo se efectúa 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.

Conceptos relacionados

"Iniciación a la seguridad" en la página 2
La seguridad es una consideración integral cuando se planifica la instalación de WebSphere Process Server, se desarrollan y despliegan aplicaciones, y en la ejecución cotidiana del servidor de procesos.

Información relacionada

Delegaciones

Seguridad para el Gestor de calendarios de empresa

El Gestor de seguridad le proporciona la capacidad de garantizar el asegurar el acceso a calendarios individuales en el Gestor de calendarios de empresa. Utilice el Gestor de seguridad para asignar roles a los miembros de la organización. Estos roles son los que determinan el nivel de acceso a los calendarios.

Para cada calendario en el Gestor de calendarios de empresa, puede asignar miembros a uno de los tres roles de recurso: Propietario, Grabador o Lector.

El Gestor de seguridad, que se utiliza para administrar el control de acceso basado en roles para el Gestor de calendarios de empresa, se encuentra en Business Space basado en WebSphere.

Este acceso basado en roles para el Gestor de calendarios de empresa se basa en XACML (eXtensible Access Control Markup Language), un estándar abierto.

Ventajas de la utilización del Gestor de seguridad

¿Cuáles son las ventajas de utilizar el Gestor de seguridad para el control de acceso basado en roles en el Gestor de calendarios de empresa?

- Puede controlar el acceso a una instancia específica de un calendario.

  Por ejemplo, puede especificar que un usuario sólo tenga acceso a su propio calendario y que no tenga la posibilidad de mirar o cambiar el calendario de otros usuarios.

- El control de acceso se realiza a nivel del rol, en lugar de a nivel del usuario individual.

  Debe correlacionar miembros con roles. El rol es el que define el permiso que tienen los miembros en la instancia específica del recurso.

Roles asociados con un calendario

Cuando se instala un calendario, se crean tres roles de recursos para dicho calendario: Propietario, Grabador y Lector.

¿Cómo se utilizan estos roles? Considere el caso de un calendario de vacaciones que se utiliza en una organización. Desea que todos los empleados tengan acceso al calendario, pero desea limitar el número de empleados que pueden actualizar el calendario.

Cuando se instala el calendario Vacaciones, se crean los siguientes roles:

- HolidayOwner

  Los miembros asignados a este rol pueden leer el calendario Vacaciones y grabar en él. Por ejemplo, si la compañía ha decidido añadir un día más de vacaciones, un miembro con el rol HolidayOwner podrá realizar el cambio.

  Los miembros de este rol también pueden asignar miembros al rol HolidayWriter y HolidayReader. Por ejemplo, el HolidayOwner puede decidir añadir un director superior al rol HolidayWriter.
- HolidayWriter

  Los miembros asignados a este rol pueden leer el calendario Vacaciones y grabar en él. Como en el caso del HolidayOwner, los miembros del rol HolidayWriter pueden añadir el día adicional de vacaciones.
- HolidayReader

  Los miembros asignados a este rol pueden leer el calendario Vacaciones, pero no pueden grabar en él.

Puede asignar el rol HolidayOwner al director de recursos humanos, el rol HolidayWriter al grupo de especialistas de recursos humanos y el rol HolidayReader al grupo de empleados, tal como se muestra en la figura siguiente:

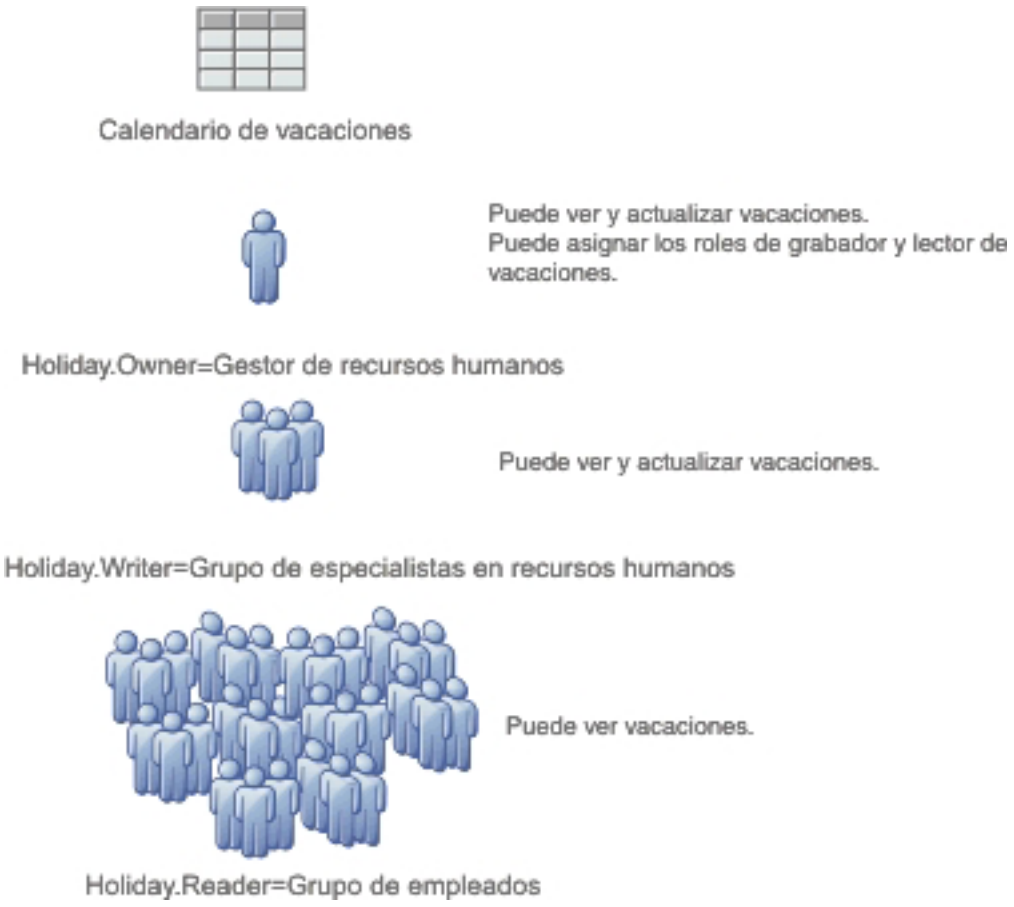


Figura 1. Ejemplos de roles asignados a un calendario

Cuando despliega un calendario, se crean los tres roles: Propietario, Grabador y Lector. El permiso para todos los roles se establece inicialmente en **Todos los autenticados**. Asegúrese de cambiar esta designación para asignar los miembros de la organización a los roles correctos.

Nota: Puede cambiar un miembro de rol (por ejemplo, puede eliminar un miembro del rol lector), pero no puede cambiar el nombre de un rol, añadir o suprimir un rol, o cambiar los permisos asociados con un rol. Los permisos se establecen de la siguiente manera:

- Los miembros del rol Propietario pueden leer y grabar en el calendario y pueden asignar otros miembros a los roles Grabador y Lector.
- Los miembros del rol Grabador pueden leer y grabar en el calendario.
- Los miembros del rol Lector pueden leer el calendario.

En el Gestor de seguridad, estos roles relacionados con el calendario también se conocen como *roles de módulo*.

Roles administrativos del Gestor de seguridad

Cuando reinicia el servidor después de instalar WebSphere Process Server (o actualizar a WebSphere Process Server 6.2), se crean los siguientes roles:

- BPMAdmin

  BPMAdmin tiene autoridad para añadir miembros o eliminar miembros del rol BPMRoleManager.

Por ejemplo, si la persona que ejecuta el rol BPMRoleManager deja de pertenecer la organización, sólo BPMAdmin puede asignar otro miembro a dicho rol.

BPMAdmin se asigna inicialmente a un miembro: el usuario administrativo principal. Cambie esta asignación a otro miembro tan pronto como reinicie el servidor después de la instalación o una actualización.

- BPMRoleManager

  BPMRoleManager tiene autoridad para añadir miembros o eliminar miembros de los tres roles relacionados con el calendario: Propietario, Grabador y Lector.

  Por ejemplo, si se crea un calendario Vacaciones, BPMRoleManager asigna miembros a los roles HolidayOwner, HolidayWriter y HolidayReader.

  BPMRoleManager se asigna inicialmente a un miembro: el usuario administrativo principal. Cambie esta asignación a otro miembro tan pronto como reinicie el servidor después de la instalación o una actualización.

Nota: En el Gestor de seguridad, estos roles también se conocen como *roles del sistema*.

Configuración de los roles

Una vez instalado WebSphere Process Server, deben realizarse las siguientes tareas en el Gestor de seguridad:

1. BPMAdmin reasigna el rol BPMRoleManager.
2. BPMRoleManager asigna miembros a uno de los tres roles asociados con el calendario.

Consulte el tema de ayuda en el Gestor de seguridad para obtener más información sobre cómo realizar estas tareas.

Conceptos relacionados

"Iniciación a la seguridad" en la página 2
La seguridad es una consideración integral cuando se planifica la instalación de WebSphere Process Server, se desarrollan y despliegan aplicaciones, y en la ejecución cotidiana del servidor de procesos.

"Control de acceso" en la página 49
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.

 Business Space basado en WebSphere
WebSphere Process Server incluye Business Space basado en WebSphere, que proporciona una interfaz común para que los usuarios de la aplicación creen, gestionen e integren las interfaces Web en el conjunto de productos de IBM WebSphere Business Process Management.

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.

Por qué y cuándo se efectúa esta tarea

Un adaptador es el mecanismo por el que una aplicación se comunica con un sistema de información empresarial (EIS). 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.

WebSphere Adapters habilitan la conectividad bidireccional gestionada entre un EIS 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 SCA (Service Component Architecture). 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 proporciona 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 empresariales

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

Las tareas de usuario, por definición, requieren intervención de usuario para completarse. Algunos procesos empresariales también pueden necesitar intervención de usuario. Estas tareas de usuario y procesos empresariales 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 empresariales. 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 empresariales

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 personas

Configuración de la seguridad de Business Space

Después de haber instalado y configurado Business Space basado en WebSphere para el producto, debe estudiar las opciones de seguridad sobre el modo como trabajará su equipo con los artefactos de Business Space. Es posible que desee configurar la seguridad de aplicaciones, que también requiere seguridad administrativa para la aplicación. Asimismo, debe ejecutar un script Jython para asignar un rol de superusuario para Business Space.

Establecimiento de la seguridad de aplicaciones para Business Space

Para activar la seguridad para Business Space, debe habilitar la seguridad de aplicaciones y la seguridad administrativa.

Antes de empezar

Antes de completar esta tarea, debe haber completado las tareas siguientes:

- Configurar un perfil, y configurar Business Space en ese perfil.
- Configurar las tablas de base de datos (si utiliza una base de datos remota o un entorno de despliegue).
- Configurar los puntos finales de servicio REST para los widgets que utilizará en Business Space.
- Comprobar que el ID de usuario está registrado en el registro de usuarios para su producto.

Por qué y cuándo se efectúa esta tarea

El archivo EAR (Enterprise Archive) de Business Space está preconfigurado para asegurar la autenticación y autorización de acceso. Business Space utiliza un rol J2EE por omisión, que se correlaciona con todos los usuarios autenticados, lo que asegura que se solicita a los usuarios que se autentiquen al acceder a los URL de Business Space. Los usuarios no autenticados son redirigidos a una página de inicio de sesión.

La autorización a los espacios y al contenido de las páginas de Business Space se gestiona internamente en Business Space como parte de la gestión de espacios.

Para habilitar el acceso autenticado (autorización basada en roles J2EE) en Business Space, debe tener un registro de usuarios configurado y la seguridad de aplicaciones habilitada.

Procedimiento

1. Para obtener instrucciones completas sobre seguridad, consulte la documentación sobre seguridad correspondiente a su producto.
2. Para la aplicación Business Space, en la página de la consola administrativa Administración, aplicaciones e infraestructura seguras, seleccione **Habilitar seguridad administrativa** y **Habilitar seguridad de aplicaciones**.
3. En la página de la consola administrativa, bajo **Depósito de cuentas de usuario**, puede designar **Depósitos federados**, **Sistema operativo local**, **Lightweight Directory Access Protocol (LDAP)** o **Registro de usuarios personalizado**. Sin embargo, si selecciona **Depósitos federados** para Business Space, tendrá prestaciones adicionales en los widgets e infraestructura como, por ejemplo, las prestaciones de búsqueda. Al buscar usuarios para compartir espacios y páginas, el ámbito de búsqueda incluye correo electrónico y un ID de usuario completo.

Qué hacer a continuación

- Tras activar la seguridad administrativa y de aplicaciones, recibirá una solicitud para un ID de usuario y una contraseña al iniciar una sesión en Business Space. Debe utilizar un ID de usuario y una contraseña válidos del registro de usuarios seleccionado para poder iniciar la sesión. Tras activar la seguridad administrativa, siempre que vuelva a la consola administrativa, debe iniciar la sesión con el ID de usuario que tiene autoridad administrativa.

- Si desea restringir el inicio de sesión en Business Space a un subconjunto de usuarios y grupos, puede cambiar la correlación del rol J2EE de Business Space. Pulse **Aplicaciones → Aplicaciones empresariales → *nombre de aplicación***. En el panel derecho, en Propiedades detalladas, seleccione **Correlación de roles de seguridad con usuarios/grupos**.
- Para establecer la autorización a páginas y espacios en Business Space, puede gestionar esto en Business Space cuando cree páginas y espacios.
- Para configurar la seguridad de los datos en los widgets basados en usuarios y grupos, debe modificar la correlación de usuarios con la aplicación de pasarela de servicios REST. Seleccione la aplicación de pasarela de servicios REST y, en el panel derecho, en Propiedades detalladas, seleccione **Correlación de roles de seguridad con usuarios/grupos**. Para el rol RestServicesUser, puede añadir usuarios y grupos al mismo para controlar el acceso a los datos en todos los widgets de servicios REST.
- Si desea restringir el acceso a los datos en los widgets basados en roles de grupo de usuarios, piense en cambiar los usuarios asignados a los roles de grupo administrativo. Puede ver la lista Roles para ver quién está asignado a estos roles abriendo la consola administrativa, pulsando **Seguridad → Administración, aplicaciones e infraestructura seguras → Roles de grupo administrativo** y seleccionando un grupo.

  Puede que desee estudiar el cambio de los usuarios asignados a los roles de grupo administrativo para widgets tales como, por ejemplo, Normas empresariales y Variables empresariales.

  Por ejemplo, para el widget Supervisor de salud, los siguientes roles administrativos tienen permisos de supervisión, permiten acceder a la consola administrativa y, por consiguiente, permiten a los usuarios asignados a esos roles acceder a los datos del Supervisor de salud:

  – Supervisor
  – Configurador
  – Operador
  – Administrador (Administrator)
  – Adminsecuritymanager
  – Desplegador (Deployer)
  – iscadmins

  Los usuarios correlacionados con esos roles de grupo administrativo tienen acceso a los datos en el Supervisor de salud. Los usuarios que no están correlacionados con esos roles no pueden acceder a los datos en el Supervisor de salud.
- Finalmente, algunos widgets tienen una capa adicional de acceso basado en rol para sus artefactos creados por usuarios empresariales. Para la gestión de soluciones, el widget Gestor de seguridad le permite asignar a usuarios y grupos unos roles de sistema o de módulo que determinan el nivel de acceso que tienen los miembros a los calendarios del widget Gestor de calendarios empresariales. Para la revisión, el widget Control de acceso de servidor de publicaciones gestiona los permisos para los usuarios que pueden revisar y comentar las revisiones. Para obtener más información, consulte la ayuda en línea del widget.

Asignación del rol de superusuario de Business Space

En Business Space, puede asignar usuarios para que sean superusuarios. Un superusuario puede ver, editar y suprimir todos los espacios y las páginas y puede designar si los espacios pueden ser plantillas de Business Space. Puede ejecutar un

script que asigne un rol de superusuario de Business Space para un ID de usuario, o bien puede utilizar el cliente de script wsadmin para crear scripts para habilitar el superusuario de Business Space.

Antes de empezar

El ID de usuario debe estar registrado en el registro de usuarios para su producto.

Procedimiento

1. Localice el script *raíz_instalación*/BusinessSpace/scripts/createSuperUser.py para asignar el rol de superusuario a un usuario.
2. Abra un indicador de mandatos y cambie los directorios al directorio siguiente: *raíz_perfil*/bin, donde *raíz_perfil* representa el directorio para el perfil donde Business Space está instalado.
3. Escriba el mandato siguiente: `wsadmin -lang jython -wsadmin_classpath raíz_instalación\plugins\com.ibm.bspace.plugin_6.2.0.jar -f createSuperUser.py nombre_corto_usuario_en_VMM`

Qué hacer a continuación

Se proporcionan dos scripts adicionales si desea consultar si un nombre de usuario tiene el rol de superusuario, o si desea eliminar un rol de superusuario. Ambos están disponibles en el directorio *raíz_instalación*/BusinessSpace/scripts/:

- isSuperUser.py para consultar si un nombre de usuario tiene un rol de superusuario.
- removeSuperUserAccess.py para eliminar el rol de superusuario de un usuario

Puede crear scripts adicionales basados en los tres proporcionados. Puede sustituir la llamada a MBean en el script por uno de los métodos siguientes para trabajar con el rol de superusuario:

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

Consulte el archivo de descriptor del MBean, BSpaceSecurityAdminMBean.xml, que se proporciona en *raíz_instalación*/BusinessSpace/scripts.

Para abrir Business Space, utilice el URL siguiente: http://*sistema_principal*:*puerto*/BusinessSpace, donde *sistema_principal* es el nombre del sistema principal donde se ejecuta el servidor y *puerto* es el número de puerto del servidor.

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 casos se supone que se aplica la seguridad administrativa.

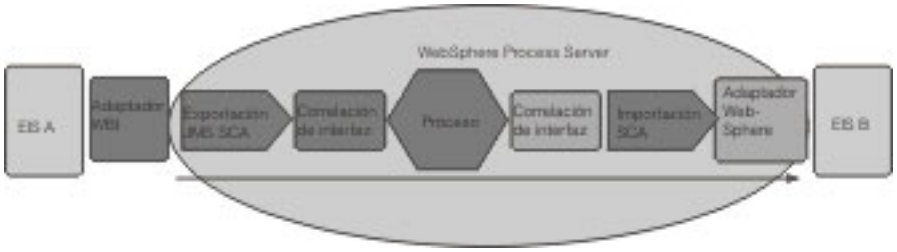
Procedimiento

1. Determine cuál de los ejemplos proporcionados en este apartado se aproximan más a sus necesidades de seguridad. En algunos casos, sus necesidades podrían incluir una 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.

Ejemplo

Escenario de integración clásico: adaptadores de entrada y salida

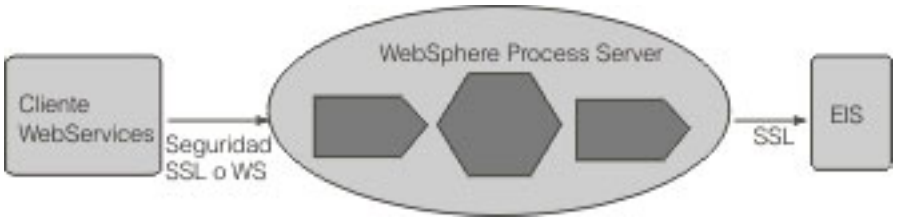
Las peticiones de entrada provienen de un WebSphere Business Integration Adapter. SCA (Service Component Architecture) invoca una correlación de interfaz basada en la exportación SCA. La petición pasa a través de un componente de proceso, una segunda correlación de interfaz y después se pasa a un segundo 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

En este caso, 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.

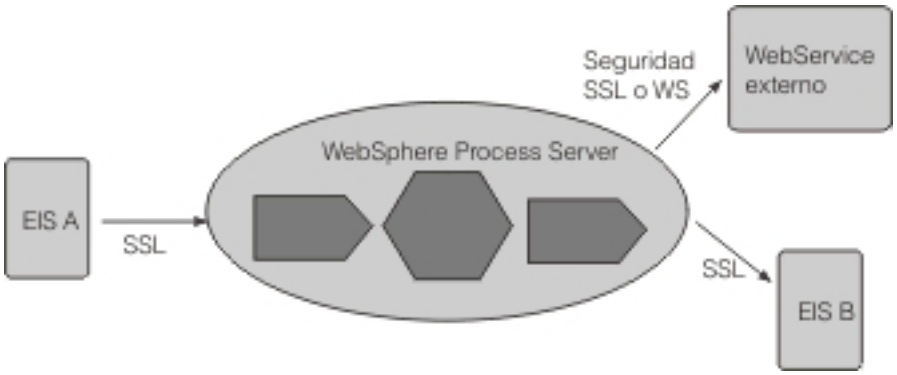


Puede autenticar un cliente de servicio Web como un cliente SSL, utilizando autenticación básica HTTP o utilizando una autenticación WS-Security. Cuando se autentica el cliente, se aplica el control de acceso basado en el calificador SecurityPermission. Entre el cliente y la instancia de WebSphere Process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

En este caso, la petición de entrada puede realizarse 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.



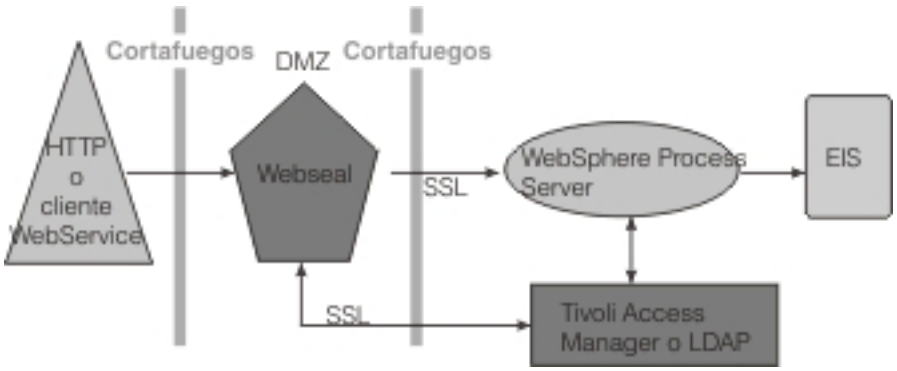
Al igual que con la petición de servicio Web de entrada, puede autenticar con el servicio Web externo como un cliente SSL, utilizando autenticación básica HTTP o autenticación WS-Security. Utilice LTPACallBackHandler como mecanismo de retorno de llamada para extraer el usernameToken del asunto RunAs 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 el 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

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 al representante de IBM de su localidad para obtener información acerca de los productos y servicios que están actualmente disponibles en su localidad. 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 del juego de caracteres 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 ni 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. IBM puede reservarse el derecho de realizar mejoras y/o cambios en los productos y/o programas descritos en esta publicación en cualquier momento 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. Los materiales de esos sitios Web no forman parte de los materiales de este producto de IBM y la utilización de esos sitios Web se realiza bajo el propio 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
1001 Hillsdale Blvd., Suite 400
Foster City, CA 94404
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 ni implicar la fiabilidad, la capacidad de servicio o el funcionamiento 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 e ibm.com son marcas registradas de International Business Machines Corporation en Estados Unidos y/o en otros países. Si estos términos de IBM u otros términos de marca registrada aparecen por primera vez en esta información con un símbolo de marca registrada (^{R} o ^{TM}), significa que son marcas registradas de EE.UU propiedad de IBM en el momento en que se publicó esta información. Dichas marcas registradas también pueden ser marcas registradas o marcas registradas de derecho común en otros países. Se dispone de una lista de marcas registradas de IBM en el apartado"Copyright and trademark information" del sitio Web: www.ibm.com/legal/copytrade.shtml.

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

Linux es una marca registrada de Linus Torvalds en EE.UU. y/o en otros países.

Java y JavaBeans son marcas registradas de Microsystems, Inc. en Estados Unidos y/o en otros países.

UNIX es una marca registrada de The Open Group en los Estados Unidos y 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 6.2