WebSphere® IBM WebSphere Process Server for Multiplatforms
Versión 7.0.0

Protección de aplicaciones y sus entornos

IBM®

WebSphere® IBM WebSphere Process Server for Multiplatforms
Versión 7.0.0

Protección de aplicaciones y sus entornos

IBM®

Abril de 2010

Esta edición se aplica a la versión 7, release 0, 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.

Contenido

Protección de WebSphere Process Server y de aplicaciones

La protección de WebSphere Process Server y de aplicaciones depende de la seguridad en el entorno de ejecución y en las aplicaciones.

La seguridad en el entorno de ejecución de WebSphere Process Server implica habilitar la seguridad administrativa y la seguridad de aplicaciones, la creación de perfiles con seguridad y la limitación del acceso de sólo ciertos usuarios a funciones importantes.

La protección de una aplicación incluye la autenticación de usuarios, la implementación del control de acceso en operaciones y recursos y proporcionar privacidad e integridad a los datos.

La seguridad de WebSphere Process Server se basa en la seguridad de WebSphere Application Server versión 7.0. 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 los temas del apartado "Protección de aplicaciones y su entorno".

Visión general de la seguridad

La seguridad de WebSphere Process Server se basa en la seguridad de WebSphere Application Server versión 7.0.

Consulte el centro de información de WebSphere Application Server Network Deployment si desea 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.

Consideraciones de seguridad específicas de WebSphere Process Server

La seguridad de WebSphere Process Server se basa en la seguridad de WebSphere Application Server 7.0. Se listan las consideraciones específicas de WebSphere Process Server.

- La página de la consola administrativa de Business Integration Security es exclusiva de WebSphere Process Server. Para mostrar esta página, expanda **Seguridad** y pulse **Seguridad de Business Integration**.

  Esta página 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 esta página.
- 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.
   a. Proteja el entorno antes de la instalación.
   b. Prepare el sistema operativo para realizar la instalación de WebSphere Process Server.
   c. Prepare el entorno después de la instalación.
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, utilice el widget Roles de seguridad para configurar el control de acceso basado en roles para los calendarios del widget Calendarios de negocio.
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.

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 **Preparación de la seguridad durante la instalación** en el Centro de información de WebSphere Application Server .

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

   Windows Linux UNIX 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.

Información de autenticación proporcionada en el momento de la instalación

Durante la instalación, 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 configurar los diferentes componentes de WebSphere Process Server de modo que tengan identidades de seguridad adecuadas.

Cuando cree un perfil de WebSphere Process Server y mantiene seleccionado **Habilitar la seguridad administrativa**, se le solicitará un nombre de usuario. 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 en tiempo de ejecución para

que acceda a las bases de datos y motores de mensajería. Estos alias se pueden modificar en la página 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.

Acerca de esta tarea

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

Estos componentes son:

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

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

Procedimiento

1. En la consola administrativa, muestre la página 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 la página 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**.

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

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

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.

Acerca de esta tarea

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".
2. Asegúrese de que está activada la seguridad de aplicaciones. "Habilitación de la seguridad".
3. Seleccione el depósito de cuentas de usuario que desea utilizar. "Configuración de un repositorio de cuentas de usuario" en la página 7

   Asegúrese de que ha seleccionado el registro seleccionado como registro actual utilizando **Establecer como actual**.
4. Añada usuarios o grupo al rol de administración.
5. Si es necesario, detenga y reinicie el servidor. "Inicio y detención del servidor" en la página 13
6. Configure alias de autenticación, control de acceso y otros mecanismos de seguridad para sus componentes instalados. "Protección de aplicaciones en WebSphere Process Server" en la página 30

Habilitación de la seguridad

El primer paso para establecer la seguridad en el entorno de WebSphere Process Server environment y sus aplicaciones es asegurarse de que esté habilitada 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.

Acerca de esta tarea

Con la consola administrativa, puede habilitar la seguridad administratia, la seguridad de aplicaciones y la seguridad de Java 2.

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

- 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.

  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.

- 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. También accede a recursos Web resources como, por ejemplo, servlets, archivos JSP (JavaServer Pages) y métodos EJB (Enterprise JavaBeans™).

  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. Los administradores deben comprender las posibles consecuencias que tiene habilitar la Java 2 si las aplicaciones no están preparadas para la seguridad. La seguridad deJava 2 impone nuevos requisitos para los desarrolladores de aplicaciones y para los administradores.

  Atención: Es posible que los fixpacks que incluyan actualizaciones del SDK (Software Development Kit) sobrescriban archivos de política sin restricciones. Realice una copia de seguridad de los archivos de política antes de aplicar un fixpack o de volver a aplicar estos archivos una vez que se haya aplicado el fixpack.

Procedimiento

1. Abra la página de seguridad administrativa en la consola administrativa.

   Expanda **Seguridad** y pulse **Seguridad global**.

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 1.4. 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 de la página.

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.

Configuración de un repositorio 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.

Acerca de 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 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 **Seguridad global**.
2. Seleccione el registro de usuario 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
Repositorios 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. **Nota:** Windows Linux UNIX No utilice el sistema operativo local como registro de usuario en un entorno de despliegue de red. Siga las instrucciones de "Configuración del depósito de cuentas de usuarios del sistema operativo local o personalizado autónomo".
LDAP (Lightweight Directory Access Protocol)	Siga las instrucciones del apartado "Configuración de LDAP (Lightweight Directory Access Protocol) como registro de usuario" en la página 10 para configurar LDAP como registro de usuario.
Registro de usuarios personalizado	Siga las instrucciones del apartado "Configuración del depósito de cuentas de usuarios del sistema operativo local o personalizado autónomo" 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.

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.

Acerca de 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 **Seguridad global** 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 → Seguridad global → 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 o usuario administrativo del servidor en un nodo de la Versión 7.0**, 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, pulse **Establecer como actual**.
7. 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.

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

Acerca de esta tarea

Tivoli Access Manager se puede utilizar como repositorio de cuentas de usuario. No se puede configurar en la consola administrativa y debe utilizarse el mandato wsadmin. Consulte el tema del Centro de información de WebSphere Application Server: Cómo propagar la política de seguridad de aplicaciones instaladas a un 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 **Seguridad global**.
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 → Seguridad global → 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 o usuario administrativo del servidor en un nodo de la Versión 7.0**, especifique un ID de usuario que se utilice para ejecutar el servidor de aplicaciones para cuestiones 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.

Evitar problema: Vista Windows 7 Si el control de cuentas de usuarios (UAC) está habilitado en algunos niveles, el servidor de aplicaciones se debe iniciar con los privilegios de administrador si está utilizando un indicador de mandatos. Inicie el servidor de aplicaciones desde una ventana de indicador de mandatos que se inicia realizando las siguientes acciones:

- Pulse con el botón secundario del ratón un atajo de indicador de mandatos.
- Pulse Ejecutar **como Administrador**.
- Cuando abra la ventana del indicador de mandatos como administrador, aparece un diálogo del sistema operativo que le pregunta si desea continuar. Pulse **Continuar** para continuar.

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`

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

2. Detenga el servidor.

   La siguiente tabla describe las opciones para detener el servidor.

Detener el servidor	Detalles
Desde la interfaz de usuario Primeros pasos	Pulse **Detener el servidor** y proporcione un nombre de usuario y contraseña válidos cuando se soliciten. El nombre de usuario que proporciona debe estar en el rol operador o administrador.
Desde la línea de mandatos	Entre: • Windows **En las plataformas Windows:** `stopserver nombre_servidor -profileName nombre_perfil -username nombre_usuario -password contraseña` • Linux UNIX **En las plataformas Linux y UNIX:** `stopserver.sh nombre_servidor -profileName nombre_perfil -username nombre_usuario -password contraseña`

   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 ocho 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, se debe correlacionar un usuario con uno de estos roles a fin de poder acceder a la consola administrativa.

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

Tabla 1. Roles de seguridad de administración

Rol de seguridad de administración	**Descripción**
Supervisor	Los miembros del rol supervisor pueden visualizar la configuración de WebSphere Process Server y el estado actual del servidor.
Configurador	Los miembros del rol configurador pueden editar la configuración de WebSphere Process Server.
Operador	Los miembros del rol operador tienen privilegios de supervisor y la capacidad de modificar el estado de tiempo de ejecución (es decir, iniciar y detener el servidor).

Tabla 1. Roles de seguridad de administración (continuación)

Rol de seguridad de administración	Descripción
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: • Contraseñas de LTPA (Lightweight Third Party Authentication) • Claves
Admins ISC	Este rol sólo está disponible para usuarios de la consola administrativa y no para usuarios wsadmin. Los usuarios que tienen este rol poseen privilegios administrativos para gestionar usuarios y grupos en depósitos federados. Por ejemplo, un usuario del rol Admins ISC puede completar las siguientes tareas: • Crear, actualizar o suprimir usuarios en la configuración de depósitos federados • Crear, actualizar o suprimir grupos en la configuración de depósitos federados
Desplegador (Deployer)	Los usuarios que tienen este rol puede realizar acciones de configuración y operaciones de tiempo de ejecución en las aplicaciones.
Gestor de seguridad admin	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.
Auditor	Los usuarios a los que se otorga este rol pueden ver y modificar los valores de configuración para el subsistema de auditoría de seguridad. **Nota:** El rol de auditor incluye el rol de supervisor. Esto permite que el auditor vea, pero no cambie, el resto de la configuración de seguridad.

Consulte Roles administrativos en el centro de información de WebSphere Application Server si desea más información.

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.

Consejo: Correlacione un grupo o grupos, en lugar de usuarios específicos, con roles administrativos porque es más flexible y fácil de administrar. 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.

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.

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.

Acerca de esta tarea

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 5.
2. Compruebe que la seguridad de aplicaciones esté activada. “Habilitación de la seguridad” en la página 5.
3. Seleccione el repositorio de cuentas de usuario que desea utilizar. “Configuración de un repositorio de cuentas de usuario” en la página 7

Asegúrese de que ha seleccionado el registro seleccionado como registro actual utilizando **Establecer como actual**.

4. Añada usuarios o grupos al rol administrativo.
5. Si es necesario, detenga y reinicie el servidor. “Inicio y detención del servidor” en la página 13
6. Configure alias de autenticación, control de acceso y otros mecanismos de seguridad para sus componentes instalados. “Protección de aplicaciones en WebSphere Process Server” en la página 30

Habilitación de la seguridad

El primer paso para establecer la seguridad en el entorno de WebSphere Process Server environment y sus aplicaciones es asegurarse de que esté habilitada 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.

Acerca de esta tarea

Con la consola administrativa, puede habilitar la seguridad administratia, la seguridad de aplicaciones y la seguridad de Java 2.

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

  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.
- 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. También accede a recursos Web resources como, por ejemplo, servlets, archivos JSP (JavaServer Pages) y métodos EJB (Enterprise JavaBeans).

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. Los administradores deben comprender las posibles consecuencias que tiene habilitar la Java 2 si las aplicaciones no están preparadas para la seguridad. La seguridad deJava 2 impone nuevos requisitos para los desarrolladores de aplicaciones y para los administradores.

Atención: Es posible que los fixpacks que incluyan actualizaciones del SDK (Software Development Kit) sobrescriban archivos de política sin restricciones. Realice una copia de seguridad de los archivos de política antes de aplicar un fixpack o de volver a aplicar estos archivos una vez que se haya aplicado el fixpack.

Procedimiento

1. Abra la página de seguridad administrativa en la consola administrativa.

   Expanda **Seguridad** y pulse **Seguridad global**.
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 1.4. 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 de la página.

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.

Configuración de un repositorio 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.

Acerca de 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 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 **Seguridad global**.
2. Seleccione el registro de usuario 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
Repositorios 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.

Registro de usuario	Acción
Sistema operativo local	Éste es el registro de usuarios por omisión. **Nota:** Windows Linux UNIX No utilice el sistema operativo local como registro de usuario en un entorno de despliegue de red. Siga las instrucciones de "Configuración del depósito de cuentas de usuarios del sistema operativo local o personalizado autónomo" en la página 8.
LDAP (Lightweight Directory Access Protocol)	Siga las instrucciones del apartado "Configuración de LDAP (Lightweight Directory Access Protocol) como registro de usuario" en la página 10 para configurar LDAP como registro de usuario.
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 8 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.

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.

Acerca de 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 **Seguridad global** 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 → Seguridad global → 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 o usuario administrativo del servidor en un nodo de la Versión 7.0**, 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, pulse **Establecer como actual**.
7. 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.

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

Acerca de esta tarea

Tivoli Access Manager se puede utilizar como repositorio de cuentas de usuario. No se puede configurar en la consola administrativa y debe utilizarse el mandato wsadmin. Consulte el tema del Centro de información de WebSphere Application Server: Cómo propagar la política de seguridad de aplicaciones instaladas a un 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 **Seguridad global**.
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 → Seguridad global → 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 o usuario administrativo del servidor en un nodo de la Versión 7.0**, especifique un ID de usuario que se utilice para ejecutar el servidor de aplicaciones para cuestiones 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.

Evitar problema: Vista Windows 7 Si el control de cuentas de usuarios (UAC) está habilitado en algunos niveles, el servidor de aplicaciones se debe iniciar con los privilegios de administrador si está utilizando un indicador de mandatos. Inicie el servidor de aplicaciones desde una ventana de indicador de mandatos que se inicia realizando las siguientes acciones:

- Pulse con el botón secundario del ratón un atajo de indicador de mandatos.
- Pulse Ejecutar **como Administrador**.
- Cuando abra la ventana del indicador de mandatos como administrador, aparece un diálogo del sistema operativo que le pregunta si desea continuar. Pulse **Continuar** para continuar.

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`

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

2. Detenga el servidor.

   La siguiente tabla describe las opciones para detener el servidor.

Detener el servidor	Detalles
Desde la interfaz de usuario Primeros pasos	Pulse **Detener el servidor** y proporcione un nombre de usuario y contraseña válidos cuando se soliciten. El nombre de usuario que proporciona debe estar en el rol operador o administrador.
Desde la línea de mandatos	Entre: • Windows **En las plataformas Windows:** `stopserver nombre_servidor -profileName nombre_perfil -username nombre_usuario -password contraseña` • Linux UNIX **En las plataformas Linux y UNIX:** `stopserver.sh nombre_servidor -profileName nombre_perfil -username nombre_usuario -password contraseña`

   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.

Compruebe que el servidor se haya detenido correctamente	Detalles
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 ocho 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, se debe correlacionar un usuario con uno de estos roles a fin de 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: • Contraseñas de LTPA (Lightweight Third Party Authentication) • Claves

Tabla 2. Roles de seguridad de administración (continuación)

Rol de seguridad de administración	Descripción
Admins ISC	Este rol sólo está disponible para usuarios de la consola administrativa y no para usuarios wsadmin. Los usuarios que tienen este rol poseen privilegios administrativos para gestionar usuarios y grupos en depósitos federados. Por ejemplo, un usuario del rol Admins ISC puede completar las siguientes tareas: • Crear, actualizar o suprimir usuarios en la configuración de depósitos federados • Crear, actualizar o suprimir grupos en la configuración de depósitos federados
Desplegador (Deployer)	Los usuarios que tienen este rol puede realizar acciones de configuración y operaciones de tiempo de ejecución en las aplicaciones.
Gestor de seguridad admin	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.
Auditor	Los usuarios a los que se otorga este rol pueden ver y modificar los valores de configuración para el subsistema de auditoría de seguridad. **Nota:** El rol de auditor incluye el rol de supervisor. Esto permite que el auditor vea, pero no cambie, el resto de la configuración de seguridad.

Consulte Roles administrativos en el centro de información de WebSphere Application Server si desea más información.

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.

Consejo: Correlacione un grupo o grupos, en lugar de usuarios específicos, con roles administrativos porque es más flexible y fácil de administrar. 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.

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.

Acerca de esta tarea

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

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 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 único se utiliza para propagar la información de autenticación en sistemas en en sentido descendente, que pueden, a su vez, aplicar el control de accesos.

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 3 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 3. 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. 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.

Alias de autenticación por omisión:

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

Tabla 4. 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 la página 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 5 describe los roles RunAs creados para los procesos empresariales.

Tabla 5. 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 la página de configuración de Business Process Choreographer de la Herramienta de gestión de perfiles.

Tabla 5. Roles RunAs asociados con procesos empresariales. (continuación)

Rol RunAs	Descripción	Información
EscalationUser	Se utiliza por MDB `task.ear`.	Entre los valores de nombre de usuario y contraseña en la página 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 6 se utilizan para invocar los componentes independientemente de la identidad del usuario que invoque.

Tabla 6. 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 la página de configuración de Common Event Infrastructure de la Herramienta de gestión de perfiles.
EventAuthAlias*TipoBD*	Se utiliza para autenticar con bases de datos.	Entre los valores de nombre de usuario y contraseña en la página 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 7 se utiliza para invocar los componentes independientemente de la identidad del usuario que invoque.

Tabla 7. 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 la página de configuración de SCA de la Herramienta de gestión de perfiles.

Modificación de alias de autenticación:

Tal vez tenga que modificar los alias de autenticación existentes.

Acerca de esta tarea

Modifique los alias de autenticación de la consola administrativa.

Procedimiento

1. Acceda a la página Alias de autenticación de Business Integration.

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

   Nota: También puede acceder a esta página desde varias páginas de la consola administrativa que requieren la información del alias de autenticación. Aparece la página Configuración del alias de autenticación.

   Esta página 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 la página 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 a la página 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*

Control de acceso

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. Proporciona un control de accesos para los componentes a través del uso de los calificadores SCA (Service Component Architecture) durante el tiempo de desarrollo. Consulte el centro de información de WebSphere Integration Developer para obtener más información.

Algunos de los componentes de WebSphere Process Server, empaquetados como archivos EAR (Enterprise Archive), protegen su operación mediante la seguridad

basada en roles Java EE. A diferencia de la seguridad basada en código, que protege la operación de componentes, el control de accesos basado en roles protege los *recursos*. Por ejemplo, en el widget Calendarios de negocio, puede especificar el tipo de acceso que tienen los usuarios a los calendarios individuales.

Widget Roles de seguridad

Utilice el widget Roles 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.

La tabla siguiente muestra los roles administrativos y su permiso por omisión.

Roles	**Permiso por omisión**
BPMAdmin	Usuario administrativo primario
BPMRoleManager	Todos los usuarios autenticados

Archivos EAR y roles asociados

La instalación de Business Process Choreographer y Common Event Infrastructure se realiza como parte del producto WebSphere Process Server.

Tabla 8. Archivos EAR y roles asociados en WebSphere Process Server

Nombre del archivo .ear	**Rol**	**Valor por omisión**
BPEContainer_*nombre_nodo_nombre_servidor*.ear O BPEContainer_*nombre_clúster*	APIUser	Todos los autenticados
	SystemAdministrator	Ninguno
	SystemMonitor	Ninguno
	JMSAPIUser	Todos los autenticados
	AdminJobUser	Todos los autenticados
	JAXWSAPIUser	Todos
BPCExplorer_*nombre_nodo_nombre_servidor*.ear O BPCExplorer_*nombre_clúster*	WebClientUser	Todos los autenticados
BSpaceEAR_*nombre_nodo_servidor*.ear	businessspaceusers	Todos los autenticados
BSpaceWebformsEnabler_*nombre_nodo_servidor*.ear	WebFormUsers	Todos los autenticados
BusinessRulesManager.ear	BusinessRuleUsers	Todos los autenticados
	NoOne	Ninguno
	AnyOne	Todos
BusinessRules_*nombre_nodo_servidor*.ear	Administrador (Administrator)	Todos los autenticados
EventService.ear	eventAdministrator	Todos los autenticados
	eventConsumer	Todos los autenticados
	eventUpdater	Todos los autenticados
	eventCreator	Todos los autenticados
	catalogAdministrator	Todos los autenticados
	catalogReader	Todos los autenticados

Tabla 8. Archivos EAR y roles asociados en WebSphere Process Server (continuación)

Nombre del archivo .ear	Rol	Valor por omisión
mm.was_*nombre_nodo_servidor*.ear	Todos los autenticados	Todos los autenticados
	Todos	Todos
REST Services Gateway.ear	RestServicesUser	Todos los autenticados
Archivo .ear del gestor de despliegue de la pasarela de servicios REST	RestServicesUser	Todos los autenticados
TaskContainer_*nombre_nodonombre_servidor*.ear O TaskContainer_*nombre_clúster*	APIUser	Todos los autenticados
	SystemAdministrator	Ninguno
	SystemMonitor	Ninguno
	EscalationUser	Todos los autenticados
	AdminJobUser	Todos los autenticados
	JAXWSAPIUser	Todos
wpsFEMgr_7.0.0 Security	WBIOperator	Todos

Roles de Business Process Choreographer Java EE

La tabla siguiente lista los roles Java EE de Business Process Choreographer:

Tabla 9. Roles de Business Process Choreographer

Componente	Roles	Valor
BPEContainer	APIUser	Todos los usuarios autenticados
	SystemAdministrator	Nombres de usuario y/o nombres de grupo entrados durante la configuración
	SystemMonitor	Todos los usuarios autenticados
	JMSAPIUser	Nombre de usuario entrado durante la configuración
	AdminJobUser	Nombre de usuario entrado durante la configuración
	JAXWSAPIUser	Todos
TaskContainer	APIUser	Todos los usuarios autenticados
	SystemAdministrator	SystemAdministrator
	SystemMonitor	SystemMonitor
	EscalationUser	EscalationUser
	AdminJobUser	AdminJobUser
	JAXWSAPIUser	Todos

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

Business Process Choreographer, que se instala como parte de la instalación de WebSphere Process Server, utiliza roles para determinar las posibilidades del usuario en un sistema de producción.

Los roles de Business Process Choreographer se muestran en la Tabla 10 en la página 37.

Tabla 10. Roles y permisos por omisión

Roles	Permiso por omisión	Notas
Administrador del sistema	Nombres de usuario y/o nombres de grupo entrados durante la configuración	Tiene acceso a todos los procesos empresariales y a todas las operaciones.
Supervisor del sistema	Todos los usuarios autenticados	Tiene acceso a operaciones de lectura.
JMSAPIUser	Nombre de usuario entrado durante la configuración	Todas las API JMS de Business Process Choreographer se ejecutan en nombre de este ID de usuario individual.
EscalationUser	Nombre de usuario entrado durante la configuración	Utilizado por el gestor de tareas de usuario para procesar llamadas API asíncronas.
AdminJobUser	Nombre de usuario entrado durante la configuración **Nota:** El usuario proporcionado debe ser un miembro del rol de administrador del sistema de Business Process Choreographer.	Los trabajos administrativos (por ejemplo el servicio de limpieza o la migración de instancia de proceso empresarial) se ejecutan en nombre de este ID de usuario individual.

Nota: El rol WebClientUser, que está asociado con el archivo Bpcexlorer.ear, puede acceder a Business Process Choreographer Explorer. El permiso por omisión para este rol es Todos los autenticados.

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. Si desea una descripción más detallada, consulte el centro de información de WebSphere Application Server Network Deployment.

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.

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.

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).

Acerca de 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 en el nivel de transporte para servicios Web 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.

Despliegue (instalación) de aplicaciones seguras

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

Antes de empezar

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

Acerca de esta tarea

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

Si se ha definido un rol RunAs en la aplicación, la aplicación invocará métodos utilizando una identidad configurada durante el despliegue. Utilice el rol RunAs para especificar la identidad bajo la cual se efectúan las invocaciones en sentido descendente. Por ejemplo, si el rol RunAs se asigna al usuario “bob” y el cliente “alice” está invocando un servlet(que tiene establecido el permiso de delegación) que llama a los enterprise beans, el método de los enterprise beans se invoca con “bob” como la identidad.

Como parte del proceso de despliegue, uno de los pasos es asignar o modificar usuarios a los roles RunAs. Este paso se titula "Correlacionar roles RunAs con usuarios". Utilice este paso para asignar nuevos usuarios o modificar usuarios existentes a roles RunAs cuando la política de delegación se establece en SpecifiedIdentity.

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

Procedimiento

1. En la consola administrativa, expanda **Aplicaciones** y pulse **Instalar 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 asegurar que el desplegador es consciente del hecho de que los métodos

que se muestran en la página 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.

Asignación de usuarios a roles

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

Antes de empezar

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

Acerca de esta tarea

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

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

Procedimiento

1. Siga las instrucciones para desplegar aplicaciones en WebSphere Process Server. Consulte el apartado Despliegue de un módulo 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.

Seguridad para el widget Calendarios de empresa

El widget Roles de seguridad le proporciona la capacidad de proteger el acceso a calendarios individuales en el widget Calendarios de empresa. Utilice el widget Roles de seguridad para asignar roles a los miembros de una organización. Estos roles son los que determinan el nivel de acceso a los calendarios.

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

Este acceso basado en rol se basa en XACML (eXtensible Access Control Markup Language), un estándar abierto.

¿Cuáles son las ventajas de utilizar el control de acceso basado en rol del widget Roles de seguridad en el widget 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 a un calendario

Cuando se instala un calendario, se crean tres roles para dicho calendario: propietario, grabador y lector. Estos roles se conocen como roles específicos de componentes.

¿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:

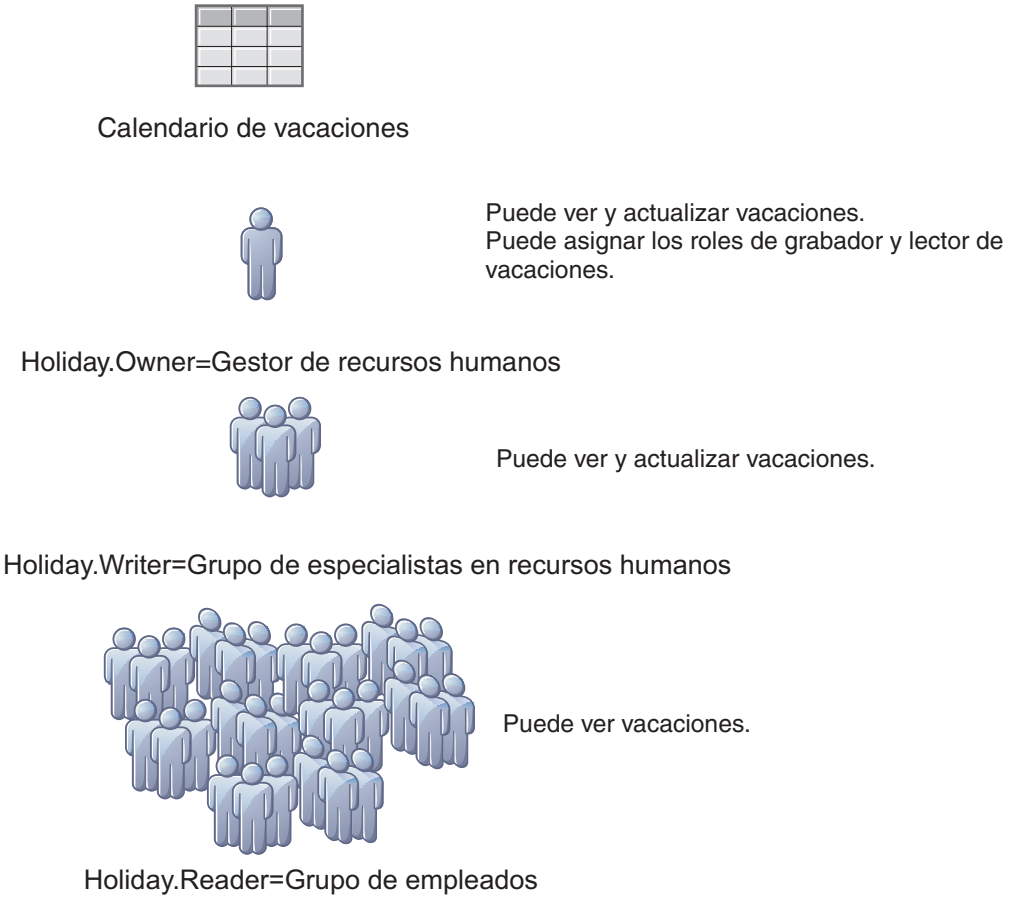


Figura 1. Ejemplos de roles asignados a un calendario

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

Roles de sistema para el widget Roles de seguridad

Los roles BPMAdmin y BPMRoleManager se crean automáticamente cuando se habilita la seguridad después de instalar WebSphere Process Server (o actualizando a WebSphere Process Server 7.0).

- BPMAdmin

  BPMAdmin tiene autoridad para añadir miembros o eliminar miembros del rol BPMRoleManager. Por ejemplo, si la persona que realiza el rol BPMRoleManager deja 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 la autoridad de añadir miembros o eliminarlos de los roles relacionados con 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.

Administración de roles en el widget Roles de seguridad

Si utiliza el widget Roles de seguridad, puede asignar un usuario o un grupo a los roles del sistema. También puede asignar un usuario o un grupo a los roles de componentes asociados a calendarios.

Asignación de roles de componentes

Los calendarios del widget Calendarios de empresa tienen tres roles asociados a ellos: Propietario, Escritor y Lector. Se utiliza el widget Roles de seguridad para asignar usuarios o grupos a estos roles.

Antes de empezar

Asegúrese de que aparezca el widget Seguridad de roles.

Acerca de esta tarea

BPMRoleManager puede asignar usuarios o grupos a roles de componentes.

El Propietario de un calendario también puede asignar usuarios o grupos al rol de Propietario, Escritor o Lector de ese calendario.

Procedimiento

1. Para asignar miembros individuales al rol de un módulo, complete los pasos siguientes:
   a. En la lista **Módulo**, seleccione un calendario.
   b. Para un rol (por ejemplo, el rol Escritor para el calendario), pulse el nombre del rol.
   c. En la parte derecha de la página, pulse **Añadir**.
   d. Escriba un nombre (o parte de un nombre) en el campo **Usuarios o grupos que buscar**.
   e. Para restringir el número de usuarios o grupos devueltos basándose en el criterio de búsqueda, cambie el valor del campo **Resultado máximo**. Establezca este valor en `0` para devolver todo el conjunto de resultados.
   f. Pulse **Buscar**.
   g. En la lista que aparezca, seleccione uno o más usuarios o grupos y pulse **Aceptar**.
   h. Cuando haya asignado todos los miembros, pulse **Guardar**.
2. Para asignar todos los miembros al rol de un módulo, complete los pasos siguientes:
   a. En la lista **Módulo**, seleccione un calendario.
   b. Para un rol (por ejemplo, el rol Lector para el calendario), pulse el nombre del rol.
   c. Seleccione **Todos los autenticados**.
   d. Pulse **Guardar**.

Protección de adaptadores

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

Acerca de esta tarea

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 Java EE 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. JCA 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 centro de información de WebSphere Integration Developer 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.

Seguridad en tareas de usuario y procesos de empresa

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

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

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

Roles asociados con tareas de usuario y procesos de empresa

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

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

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

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

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

Las tareas también tienen estos roles adicionales:

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

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

Configuración de la seguridad de Business Space

Si va a utilizar Business Space basado en WebSphere con su entorno, debe considerar las opciones de seguridad en lo concerniente al modo como el equipo trabajará con los artefactos de Business Space. Si desea activar la seguridad para Business Space, configure la seguridad de aplicaciones y designe un depósito de usuarios. Para definir administradores de Business Space, asigne un rol de superusuario.

Acerca de esta tarea

Para obtener los mejores resultados, habilite la seguridad antes de configurar Business Space. En la página de administración de la seguridad global de la consola administrativa, habilite la seguridad administrativa y la seguridad de aplicaciones. Designe también un depósito de cuentas de usuario.

Consideraciones para utilizar un registro de cuentas de usuario con Business Space:

- Según el tipo de configuración LDAP que vaya a utilizar, los valores pueden afectar a la capacidad de acceder a Business Space correctamente. Asegúrese de que los filtros de usuario, los filtros de grupo y los valores de correlación estén bien configurados. Para obtener más información, consulte Configuración de filtros de búsqueda de Lightweight Directory Access Protocol en la documentación de WebSphere Application Server.
- Según el tipo de configuración de depósito federado que vaya a utilizar, los valores pueden afectar a la capacidad para acceder a Business Space correctamente. Asegúrese de que los reinos estén bien configurados. Para obtener más información, consulte Gestión del reino en una configuración de depósito federado en la documentación de WebSphere Application Server.

- La seguridad LDAP está configurada por omisión para utilizar la propiedad de inicio de sesión `uid` (ID de usuario) para las búsquedas en Business Space. Si la seguridad LDAP se modifica para utilizar otro campo LDAP exclusivo como, por ejemplo, `mail` (dirección de correo electrónico) para la propiedad de inicio de sesión, debe modificar la propiedad userIdKey en el archivo `ConfigServices.properties` para que la búsqueda funcione en Business Space. El archivo `ConfigServices.properties` se encuentra en *raíz_perfil*`\BusinessSpace\`*nombre_nodo*`\`*nombre_servidor*`\mm.runtime.prof\config\ConfigService.properties` para un servidor autónomo o *raíz_perfil_gestor_despliegue*`\BusinessSpace\`*nombre_clúster*`\mm.runtime.prof\config\ConfigService.properties` para un clúster. Cambie el atributo userIdKey de `uid` para que coincida con la propiedad de inicio de sesión para la seguridad LDAP, por ejemplo, `mail`. A continuación, ejecute el mandato updatePropertyConfig utilizando el cliente de scripts wsadmin, que designa los siguientes parámetros: **-serverName** y **-nodeName** para un servidor autónomo o **-clusterName** para un clúster **-propertyFileName** con el valor de la vía de acceso para el archivo `ConfigServices.properties` y **-prefix** con el valor `Mashups_`.
- Si va a utilizar una base de datos de Microsoft® SQL Server y el registro **LDAP autónomo**, asegúrese de que el nombre distinguido de usuario (DN de usuario) no exceda de 131 caracteres. Si una cualquiera de las entradas DN de usuario excede los 131 caracteres, debe designar la opción **Repositorios federados** para el repositorio de cuenta de usuario. Si se conmuta entre repositorios federados y otros registros, todos los espacios existentes, ya no se puede acceder a las páginas en Business Space y se deben volver a crear.
- Si va a utilizar **Depósitos federados**, dispondrá de prestaciones adicionales en los widgets y la infraestructura, como pueden ser prestaciones de búsqueda mejoradas. Al buscar usuarios para compartir espacios y páginas, el ámbito de búsqueda incluye el correo electrónico, un nombre de usuario completo y un ID de usuario.

Si va a utilizar IBM® Tivoli Access Manager WebSEAL y desea utilizarlo con su entorno de Business Space, debe llevar a cabo pasos de configuración adicionales. Configure la seguridad de Tivoli Access Manager con un proveedor Java Authorization Contract for Containers (JACC) externo, configure WebSEAL con Tivoli Access Manager, configure WebSEAL con el servidor de aplicaciones del producto y configure las uniones de sistema principal para el entorno.

Para configurar los usuarios del entorno de Business Space que serán administradores, ejecute un script para asignar el rol de superusuario de Business Space.

Establecimiento de 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:

- Ha comprobado que el ID de usuario esté registrado en el registro de usuarios para el producto.

Si tiene previsto utilizar un entorno protegido, asegúrese de habilitar la seguridad antes de configurar Business Space. Si desea habilitar o eliminar la seguridad después de configurar Business Space, debe modificar las propiedades `MashupAdminForOOBSpace` y `noSecurityAdminInternalUserOnly` en el archivo `ConfigServices.properties` para establecer el ID de usuario correcto como ID de administrador válido. El archivo `ConfigServices.properties` se encuentra en *raíz_perfil*`\BusinessSpace\`*nombre_nodo*`\`*nombre_servidor*`\mm.runtime.prof\config\ConfigService.properties` para un servidor autónomo o *raíz_perfil_gestor_despliegue*`\BusinessSpace\`*nombre_clúster*`\mm.runtime.prof\config\ConfigService.properties` para un clúster. Copie el archivo modificado en una carpeta vacía del sistema. A continuación, ejecute el mandato updatePropertyConfig mediante el cliente de script wsadmin y designe los parámetros siguientes:

- **-serverName** y **-nodeName** para un servidor autónomo o **-clusterName** para un clúster
- **-propertyFileName** con el valor de la vía de acceso para el archivo `ConfigServices.properties`
- **-prefix** con el valor `Mashups_`

Acerca de esta tarea

Business Space está preconfigurado para asegurar la autenticación y autorización de acceso. Cuando los usuarios acceden a los URL de Business Space se les solicita autenticación. Se redirige a los usuarios no autenticados a una página de inicio de sesión. Se puede acceder a Business Space mediante HTTP o HTTPS, excepto para la página de inicio de sesión, que siempre se redirige a HTTPS. Por lo tanto, si utiliza un servidor web como, por ejemplo, IBM HTTP Server, debe configurarlo para soportar HTTPS.

La autorización de espacios y contenido de páginas en Business Space se maneja internamente en Business Space como parte de la gestión de espacios.

Para habilitar el acceso autenticado a 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 de seguridad correspondiente al producto.
2. Para la aplicación Business Space, en la página de la consola administrativa Seguridad global, seleccione **Habilitar seguridad administrativa** y **Habilitar seguridad de aplicaciones**.
3. En la misma página de la consola administrativa, bajo **Depósito de cuentas de usuario**, seleccione **Depósitos federados**, **Sistema operativo local**, **Registro de LDAP autónomo** o **Registro personalizado autónomo**. Revise las consideraciones para seleccionar un registro de usuarios en Configuración de la seguridad para Business Space.
4. Si Business Space es remoto respecto al lugar donde se ejecuta el producto, y si el nodo en que se ejecuta Business Space y el nodo en que se ejecuta el producto no están en la misma célula, debe realizar pasos manuales para asegurarse de que el inicio de sesión único (SSO) está habilitado. Por ejemplo, si utiliza más de un producto (WebSphere Business Compass, WebSphere Business Monitor, WebSphere Enterprise Service Bus o WebSphere Process Server), los servidores están en nodos diferentes y quiere que todos puedan

trabajar con el servidor de Business Space, deberá configurar el SSO manualmente. Para habilitar SSO, siga estos pasos:

a. En la consola administrativa para cada servidor, abra la página Seguridad global pulsando **Seguridad → Seguridad global**. Expanda **Web y seguridad SIP** y pulse **inicio de sesión único (SSO)** para asegurarse de que el recuadro de selección **Habilitado** está activo.

b. Asegúrese de que todos los nodos utilizan la misma información de **Depósito de cuentas de usuario** (vea el paso 3).

c. En la consola administrativa para el primer nodo, abra la página Seguridad global. Bajo Autenticación, pulse **LTPA**.

d. Bajo **Inicio de sesión individual en célula cruzada**, escriba una contraseña para el archivo de claves y un nombre de archivo de claves completo, que es un nombre de archivo y ubicación donde desea exportar el archivo de claves. El nombre de archivo de claves completo es la vía de acceso absoluta en el sistema donde está ejecutando el servidor.

e. Pulse **Exportar claves**. El archivo de claves se guarda en el sistema donde se ejecuta el servidor.

f. Si los dos nodos no están en el mismo sistema, copie el archivo de claves físicamente en los otros sistemas.

g. Importe el archivo de claves en todos los nodos utilizando el mismo archivo de claves: inicie una sesión en la consola administrativa para los demás nodos y vaya a la página Seguridad global > LTPA. Bajo **Inicio de sesión individual en célula cruzada**, escriba la contraseña para el archivo de claves y el nombre de archivo de claves completo (utilice la misma contraseña para el archivo de claves exportado que ha copiado) y pulse **Importar claves**.

h. Reinicie el servidor después de importar las claves en cada sistema.

5. Si va a utilizar HTTPS en el archivo de puntos finales, la ubicación de los puntos finales estará en un nodo distinto de Business Space y el certificado Secure Sockets Layer (SSL) será un certificado SSL autofirmado que deberá importar.

   a. Inicie la sesión en la consola administrativa para el servidor que contiene Business Space e importe el certificado SSL que utiliza el nodo remoto en que se ejecuta el producto.

      1) Bajo Seguridad, pulse **Gestión de certificados SSL y claves**.

      2) En la página Gestión de certificado SSL y de claves, bajo Elementos relacionados, pulse **Almacenes de claves y página de certificados**.

      3) En la página Almacenes de claves y página de certificados, pulse **NodeDefaultTrustStore** para modificar ese tipo de almacén de confianza.

      4) En la página NodeDefaultTrustStore, bajo Propiedades adicionales, pulse **Certificados de firmante**.

      5) En la página Certificados de firmante de **NodeDefaultTrustStore**, pulse el botón **Recuperar de puerto**.

      6) En la página Recuperar de puerto, bajo Propiedades generales, escriba el sistema principal, el puerto y el alias para donde se está ejecutando su producto. Pulse el botón **Recuperar información de firmante** y, a continuación, pulse **Aceptar**.

      7) Reinicie ambos servidores.

b. Inicie la sesión en la consola administrativa para el nodo de producto e importe el certificado SSL que utiliza el nodo en que se ejecuta Business Space.
   1) Repita los pasos a. i.-v.
   2) En la página Recuperar de puerto, bajo Propiedades generales, escriba el host y el puerto donde se ejecuta Business Space. Pulse el botón **Recuperar información de firmante** y, a continuación, pulse **Aceptar**.
   3) Reinicie ambos servidores.

Para obtener más información sobre SSO y SSL, consulte el Information Center de WebSphere Application Server.

Qué hacer a continuación

- Tras activar la seguridad administrativa y la seguridad 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 contraseña válidos del registro de usuarios seleccionado para iniciar la sesión. Después de activar la seguridad administrativa, siempre que vuelva a la consola administrativa, debe iniciar la sesión con el ID de usuario que tiene autoridad administrativa.
- Para establecer la autorización para páginas y espacios en Business Space, puede gestionar la autorización cuando cree páginas y espacios de Business Space.
- 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 la pasarela de servicios REST. Seleccione la aplicación de pasarela de servicios REST y, en el panel derecho, bajo Propiedades de detalle, seleccione **Rol de seguridad con la correlación de 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 grupos de usuarios, estudie cambiar los usuarios asignados a los roles de grupo administrativo. Puede ver la lista Roles para ver quién está asignado a esos roles abriendo la consola administrativa, pulsando **Seguridad → Administración, aplicaciones e infraestructura seguras → Roles de grupo administrativo** y seleccionando un grupo.

  Tal vez quiera considerar el cambio de los usuarios asignados a roles de grupo administrativo para widgets tales como, por ejemplo, reglas empresariales y variables empresariales.

  Por ejemplo, para el widget Salud del sistema, todos los roles administrativos siguientes tienen permisos de supervisión y, por lo tanto, permiten a los usuarios asignados a esos roles acceder a los datos del widget Salud del sistema:
  - **Supervisor**
  - **Configurador**
  - **Operador**
  - **Administrador (Administrator)**
  - **Adminsecuritymanager**
  - **Desplegador (Deployer)**
  - **iscadmins**

  Los usuarios que están correlacionados con esos roles de grupo administrativo tienen acceso a los datos en el widget Salud del sistema. Los usuarios que no están correlacionados con esos roles no pueden acceder a los datos en el widget Salud del sistema.

- Por último, algunos widgets tienen una capa adicional de acceso basado en roles para sus artefactos creados por usuarios empresariales. Para la gestión de soluciones, el widget de Roles de seguridad permite asignar a usuarios y grupos roles de sistema o roles de módulo que determinan el nivel de acceso que tienen los miembros para calendarios del widget de Calendarios empresariales. Para la revisión, el widget Revisar control de acceso gestiona los permisos para los usuarios que pueden revisar y comentar las revisiones. Para obtener más información, consulte la ayuda en línea correspondiente al widget.

Nota:

Si encuentra los siguientes errores en el archivo `SystemOut.log`, es posible que tenga atributos adicionales en el registro de usuarios que no se pueden procesar:

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

Establezca los siguientes atributos en el archivo `ConfigServices.properties` para ignorar esos atributos:

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

El archivo `ConfigServices.properties` se encuentra en *raíz_perfil*\BusinessSpace*nombre_nodo**nombre_servidor*\mm.runtime.prof\config\ConfigService.properties para un servidor autónomo o *raíz_perfil_gestor_despliegue*\BusinessSpace*nombre_clúster*\mm.runtime.prof\config\ConfigService.properties para un clúster. Tras modificar el archivo `ConfigServices.properties`, ejecute el mandato updatePropertyConfig utilizando el cliente de scripts wsadmin, que designa los siguientes parámetros: **-serverName** y **-nodeName** para un servidor autónomo o **-clusterName** para un clúster, **-propertyFileName** con el valor de la vía de acceso para el archivo `ConfigServices.properties`, y **-prefix** con el valor `Mashups_`.

Nota:

Si tiene la seguridad Java 2 habilitada en un clúster, considere la posibilidad de reforzar la entrada de la política de servidor aplicada a la ubicación de la ayuda de Business Space.

La política de la ubicación de la ayuda de Business Space es:

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

    permission java.security.AllPermission;

};
```

Refuerce la política modificándola:

```
grant codeBase     "file:${was.install.root}/profiles/nombre_perfil/temp/
nombre_nodo/nombre_servidor/
BusinessSpaceHelpEAR_nombre_nodo_nombre_servidor/BusinessSpaceHelp.war/-" {

    permission java.security.AllPermission;
```

```
};
```

Configuración de Tivoli Access Manager WebSEAL para que funcione con Business Space

Si tiene Tivoli Access Manager WebSEAL y desea utilizarlo con Business Space, debe seguir varios pasos de configuración adicionales.

Acerca de esta tarea

Si desea utilizar Tivoli Access Manager WebSEAL con Business Space, debe configurar la seguridad de Tivoli Access Manager con un proveedor de Java Authorization Contract for Containers (JACC) externo, configurar WebSEAL con Tivoli Access Manager, configurar WebSEAL con el servidor de aplicaciones del producto y configurar uniones de sistema principal para el entorno.

Procedimiento

1. Configure Tivoli Access Manager con JACC.
   a. Siga uno de estos pasos, según desee utilizar la consola administrativa o los mandatos de wsadmin.
      - Si desea utilizar la consola administrativa para configurar Tivoli Access Manager con JACC, siga estos pasos:
        1) Habilite la seguridad global.
           a) Seleccione **Seguridad** → **Seguridad global**.
           b) Habilite **Seguridad administrativa**, **Seguridad de aplicaciones** y **Seguridad Java 2** con el servidor LDAP con el que está configurado Tivoli Access Manager.
           c) Seleccione **Seguridad global** → **LDAP**, especifique la información siguiente y, a continuación, pulse **Aceptar**.

Nombre	Descripción
`ID de usuario de servidor`	Especifique el mismo ID de usuario que ha especificado para el DN de administrador en los valores de Tivoli Access Manager. Ejemplo: `user1`
`Contraseña de usuario de servidor`	`puser1`
`Sistema principal`	LDAP configurado con Tivoli Access Manager
`Puerto`	Ejemplo: `389`
`DN base`	Ejemplo: `o=ibm, c=us`
`DN de enlace`	Ejemplo: `cn=SecurityMaster,secAuthority=Default`
`Contraseña de enlace`	Contraseña del usuario SecurityMaster

           d) Guarde la configuración y reinicie el servidor.
        2) Habilite la autorización externa con Tivoli Access Manager y JACC.
           a) Seleccione **Seguridad** → **Seguridad global** → **Proveedores externos de autorización**.
           b) En la lista **Proveedor de autorización**, seleccione **Proveedor JACC externo** y, a continuación, pulse **Configurar**. Las propiedades por omisión para Tivoli Access Manager son correctas. No cambie los valores por omisión.

c) En **Propiedades adicionales**, seleccione **Propiedades de Tivoli Access Manager**. Seleccione **Habilitar Tivoli Access Manager incorporado**, especifique la información siguiente y, a continuación, pulse **Aceptar**.

Nombre	Valor
Conjunto de puertos de escucha de cliente	El valor por omisión es 8900 - 8999. Cámbielo sólo si desea utilizar otros puertos.
Servidor de políticas (nombre:puerto)	Especifique el *servidor_políticas*:*puerto*. Ejemplo: `windomain3.rtp.raleigh.ibm.com:7135`
Servidores de autorización y prioridad (nombre:puerto:prioridad)	Especifique *servidor_autorización*:*puerto*:*prioridad*. Ejemplo: `windomain3.rtp.raleigh.ibm.com:7136:1`
Nombre de usuario administrador	Deje el nombre de usuario como **sec_master (default)**, a menos que utilice otro nombre de administrador en el servidor de Tivoli Access Manager.
Contraseña de usuario administrador	`domino123`
Sufijo de nombre distinguido de registro de usuarios	Escriba el nombre que desee utilizar para el servidor de aplicaciones. Ejemplo: `o=ibm, c=us`
Dominio de seguridad	Deje el dominio de seguridad establecido en **Default**. Cambie este valor si no va a utilizar el dominio por omisión en el servidor de Tivoli Access Manager. Cambie este valor si tiene varios dominios creados en el servidor de Tivoli Access Manager y desea conectarse a o utilizar un dominio que no sea el dominio **Default**.
Nombre distinguido de usuario administrador	Escriba el nombre totalmente calificado del usuario. Ejemplo: `cn=user1,o=ibm,c=us` **Nota:** Este usuario es el mismo que el **ID de usuario de servidor** configurado en el panel de registro de usuarios LDAP.

El servidor se pone en contacto con el servidor de Tivoli Access Manager y crea varios archivo de propiedades en el servidor de aplicaciones. Este proceso puede tardar unos minutos. Si se produce un error, examine `system Out` y corrija el problema.

- Si desea utilizar el programa de utilidad wsadmin para configurar Tivoli Access Manager con JACC, siga estos pasos. Siga este procedimiento cuando esté en el servidor del gestor de despliegue. Los parámetros de configuración se reenvían a los servidores gestionados, incluidos los agentes de nodo, cuando se efectúa una sincronización. Los servidores gestionados tienen que reiniciarse individualmente para que los cambios en la configuración entren en vigor.
  1) Verifique que todos los servidores gestionados, incluidos los agentes de nodo, se hayan iniciado.
  2) Inicie el servidor.
  3) Inicie el programa de utilidad de línea de mandatos ejecutando el mandato wsadmin desde el directorio *raíz_instalación*`/bin`.
  4) En el indicador wsadmin, ejecute el mandato configureTAM, incluida la información adecuada de la tabla siguiente:

Ejemplo de Jacl:

```
$AdminTask configureTAM -interactive
```

Ejemplo de Jython:

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

A continuación, escriba la información siguiente:

Nombre	Valor
Nombre de nodo del servidor del producto	Especifique un solo nodo o escriba un asterisco (*) para elegir todos los nodos.
Tivoli Access Manager Policy Server	Escriba el nombre del servidor de políticas de Tivoli Access Manager y el puerto de conexión. Utilice el formato, *servidor_políticas*:*puerto*. El puerto de comunicación del servidor de políticas se establece al configurar Tivoli Access Manager. El puerto por omisión es 7135.
Tivoli Access Manager Authorization Server	Escriba el nombre del servidor de autorización de Tivoli Access Manager. Utilice el formato *servidor_autor*:*puerto*:*prioridad*. El puerto de comunicación del servidor de autorización se establece al configurar Tivoli Access Manager. El puerto por omisión es 7136. Puede especificar más de un servidor de autorización separando las entradas con comas. Tener más de un servidor de autorización configurado es útil para la migración tras error y el rendimiento. El valor de prioridad es el orden de uso del servidor de autorización. Por ejemplo: `servidor_autor1:7136:1, servidor_autor2:7137:2`. Una prioridad 1 sigue siendo necesaria cuando se configura con un solo servidor de autorización.
Nombre distinguido de administrador del servidor del producto	Escriba el nombre distinguido completo del ID de administrador de seguridad para el servidor del producto. Por ejemplo: `cn=wasadmin,o=organization,c=country`. Para obtener más información, consulte el enlace relacionado.
Tivoli Access Manager user registry distinguished name suffix	Por ejemplo: o=organization, c=country
Tivoli Access Manager administrator user name	Escriba el ID de usuario de administración de Tivoli Access Manager, según se haya creado durante la configuración de Tivoli Access Manager. Este ID suele ser sec_master.
Tivoli Access Manager administrator user password	Escriba la contraseña del administrador de Tivoli Access Manager.
Dominio de seguridad de Tivoli Access Manager	Escriba el nombre del dominio de seguridad de Tivoli Access Manager que se utilice para almacenar usuarios y grupos. Si no se ha establecido aún un dominio de seguridad durante la configuración de Tivoli Access Manager, pulse **Retorno** para aceptar el valor por omisión.

Nombre	Valor
Embedded Tivoli Access Manager listening port set	El servidor del producto está a la escucha en un puerto TCP/IP de las actualizaciones de base de datos de autorización procedentes del servidor de políticas. Puesto que se puede ejecutar más de un proceso en un nodo y una máquina concretos, se exige una lista de puertos para los procesos. Especifique los puertos que utilicen como puertos de escucha los clientes de Tivoli Access Manager, separados por una coma. Si especifica un rango de puertos, separe los valores inferior y superior con dos puntos. Por ejemplo, 7999, 9990:9999.
Defer	Establezca esta opción en yes; esta opción pospone la configuración del servidor de gestión al próximo reinicio. Si se establece en no, la configuración del servidor de gestión tiene lugar de inmediato. Los servidores gestionados se configuran en su próximo reinicio.

5) Una vez que haya especificado toda la información obligatoria, seleccione **F** para guardar las propiedades de configuración o **C** para cancelar el proceso de configuración y descartar la información especificada.

   Ejemplo con un servidor SVTM TAM60:

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

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

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

Configure embedded Tivoli Access Manager

F (Finish)
C (Cancel)

Select [F, C]: [F] F
WASX7278I: Generated command line: $AdminTask configureTAM {-policySvr
 windomain3.rtp.raleigh.ibm.com:7135 -authSvrs
 windomain3.rtp.raleigh.ibm.com:7136:1 -wasAdminDN cn=wa
```

```
Embedded Tivoli Access Manager configuration action parameters saved successfully.
 Restart all WebSphere Application Server instances running on the target node or
 nodes to
wsadmin>
```

6) En la consola administrativa, seleccione **Seguridad → Seguridad global → Proveedores de autorización externos**. A continuación, seleccione **Autorización externa con un proveedor JACC** y pulse **Aceptar**.

7) Vaya a la pantalla de seguridad principal y pulse **Aceptar**. Guarde y sincronice los cambios.

8) Reinicie todos los procesos en la célula.

b. Si ha instalado aplicaciones antes de habilitar Tivoli Access Manager (por ejemplo, ha habilitado la seguridad LDAP e instalado algunas aplicaciones protegidas y ha correlacionado usuarios y grupos con roles de seguridad), propague la información de correlación de roles de seguridad de los descriptores de despliegue al servidor de políticas de Tivoli Access Manager. Lleve a cabo uno de los pasos siguientes, en función de si desea utilizar la consola administrativa o los mandatos de wsadmin.

- Si desea utilizar el mandato de wsadmin propagatePolicyToJACCProvider, consulte Propagación de la política de seguridad de las aplicaciones instaladas a un proveedor JACC mediante scripts de wsadmin.
- Si desea utilizar la consola administrativa, consulte Propagación de políticas de seguridad y roles para aplicaciones desplegadas anteriormente.

2. Configure WebSEAL con Tivoli Access Manager.

a. Asegúrese de que WebSEAL se haya instalado y esté bien configurado.

b. Cree la unión entre WebSEAL y el servidor de aplicaciones del producto con la opción **-c iv_creds** para TAI++ y **-c iv_user** para TAI. Especifique uno de los mandatos siguientes en una línea utilizando las variables adecuadas para su entorno:

Para TAI++

```
server task webseald-server create -t tcp -b supply -c iv_creds
-h nombre_sistema_principal -p número_puerto_apl_websphere
nombre_unión
```

c. Para crear una cuenta de usuario fiable en Tivoli Access Manager, que se puede utilizar para configurar TAI, emita los mandatos siguientes:

```
pdadmin -a sec_master -p domino123
pdadmin sec_master> user create -gsouser -no-password-policy taiuser
"cn=taiuser,ou=websphere,o=ibm,c=us" taiuser taiuser ptaiuser
pdadmin sec_master> user modify taiuser password-valid yes
pdadmin sec_master> user modify taiuser account-valid yes
```

d. En el archivo de configuración de WebSEAL *directorio_instalación_webseal*/etc/webseald-default.conf, establezca el parámetro siguiente:

```
basicauth-dummy-passwd=contraseña_ID_usuario_webseal
```

Por ejemplo, si establece taiuser/ptaiuser en Tivoli Access Manager, establezca el parámetro siguiente: `basicauth-dummy-passwd = ptaiuser`

Si va a utilizar una autenticación basada en formularios, establezca los parámetros siguientes:

```
forms-auth=both
```

```
ba-auth=none
```

3. Configure WebSEAL con el servidor de aplicaciones del producto habilitando el interceptor de TAI++ en el servidor.
   a. En la consola administrativa, seleccione **Seguridad global → Mecanismos de autenticación y caducidad**.
   b. Expanda **Seguridad web y SIP** y, a continuación, seleccione **Asociación de confianza**. Seleccione el recuadro de selección y pulse **Aplicar**.
   c. Seleccione **Interceptores → TAMTrustAssociationInterceptorPlus → Propiedades personalizadas** y añada las propiedades siguientes:

Nombre	Valor
com.ibm.websphere.security.webseal.configURL	${RAÍZ_INSTALACIÓN_WAS}/java/jre/PdPerm.properties
com.ibm.websphere.security.webseal.id	iv-creds
com.ibm.websphere.security.webseal.loginId	taiuser (si el usuario taiuser/ptaiuser se ha creado en Tivoli Access Manager)

   d. Reinicie la célula.
   e. Para acceder al cliente, vaya a https://*nombre_servidor_webseal*:*puerto_webseal*/*nombre unión*/*uri_web_para_cliente*.
4. Configure las uniones de sistema principal para el entorno, de manera que aparezcan los widgets de Business Space. Siga uno de estos pasos, en función de si va a utilizar uniones de sistema principal virtuales o uniones de sistema principal transparentes.
   - Si va a utilizar uniones de sistema principal virtuales, cree una unión de sistema principal virtual. Una unión de sistema principal virtual elimina la necesidad de crear uniones independientes.
     a. Asegúrese de que se haya configurado un sistema principal virtual. Las uniones de sistema principal virtuales casan un sistema principal con un número de puerto y reenvían las direcciones al sistema principal de destino. No tiene lugar ningún filtrado de URL y todas las solicitudes que coinciden se reenvían al sistema principal de destino.
     b. Asegúrese de que las aplicaciones siguientes estén disponibles para el mismo sistema principal virtual. Puede que tenga algunas o todas las aplicaciones, según los productos que vaya a utilizar con Business Space.
        - BPMAdministrationWidgets_*nombre_nodo_nombre_servidor* (para WebSphere Enterprise Service Bus y WebSphere Process Server)
        - BusinessSpaceHelpEAR_*nombre_nodo_nombre_servidor* (para todos los productos)
        - BSpaceEAR_*nombre_nodo_nombre_servidor* (para todos los productos)
        - BSpaceWebformsEnabler_*nombre_nodo_nombre_servidor* (para todos los productos)
        - HumanTaskManagementWidgets_*nombre_nodo_nombre_servidor* (para WebSphere Process Server y WebSphere Business Monitor)
        - REST Services Gateway (para todos los productos)
        - REST Services Gateway Dmgr (para WebSphere Enterprise Service Bus y WebSphere Process Server)
        - mm.was_*nombre_nodo_nombre_servidor* (para todos los productos)
        - WBMDashboardWeb_*nombre_nodo_nombre_servidor* (para WebSphere Business Monitor)

- wesbWidgets_*nombre_nodo_nombre_servidor* (para WebSphere Enterprise Service Bus)
- widgets_busleader_*nombre_nodo_nombre_servidor* (para WebSphere Business Compass)
- widgets_pubserver_*nombre_nodo_nombre_servidor* (para WebSphere Business Compass)
- widgets_fabric_*nombre_nodo_nombre_servidor* (para WebSphere Business Services Fabric)

Nota: Esta lista de aplicaciones sólo cubre las aplicaciones que exige Business Space. Es posible que tenga que añadir otras aplicaciones a la lista de escenarios que no sean de Business Space y que utilicen Tivoli Access Manager WebSEAL.

c. Ejecute el mandato siguiente con pdadmin: `server task` *`servidor webseal`* `virtualhost create -t` *`transporte`* `-h` *`sistema_principal_destino`* `[-p` *`puerto`*`] [-v` *`nombre_sistema_principal_virtual`*`]` *`etiqueta_sistema_principal_virtual`*

Utilice la información siguiente:

- *servidor webseal* es el nombre del servidor WebSEAL, donde creará la entrada de sistema principal virtual.
- *transporte* es el tipo de transporte. Los entradas válidas son `tcp`, `ssl`, `tcpproxy` y `sslproxy`.
- *sistema_principal_destino* es el sistema principal de la aplicación necesaria.
- *nombre_sistema_principal_virtual* se utiliza para casar las solicitudes HTTP con una unión de sistema principal virtual. Si no se especifica ningún valor, el valor consta por omisión del sistema principal y el puerto de destino. Por ejemplo, si establece el *nombre_sistema_principal_virtual* en `myvirthost.ibm.com:80`, WebSEAL casa los URL que contienen `myvirthost.ibm.com:80` y lo direcciona al sistema principal proporcionado en el mandato pdadmin.
- *etiqueta_sistema_principal_virtual* es la etiqueta que se utiliza para identificar la entrada en WebSEAL. Debe ser exclusiva.

Para que Business Space se ejecute cuando se esperaba, las entradas tanto `ssl` como `tcp` deben crearse para el tipo de transporte. Si necesita que tanto Secure Sockets Layer (SSL) como Transmission Control Protocol (TCP) tengan soporte en la misma unión de sistema principal virtual, debe utilizar la opción -g *etiqueta_sistema_principal_v*, donde *etiqueta_sistema_principal_v* es la etiqueta virtual original para compartir la configuración. Esta opción busca una unión de sistema principal virtual creada anteriormente (una creada antes, donde *etiqueta_sistema_principal_virtual* coincide con la etiqueta que se proporciona en la opción -g) y compartirá esa configuración. La segunda entrada aún necesita una *etiqueta_sistema_principal_virtual* propia, pero puede compartir el sistema principal de destino, el puerto y otros valores. Si no proporciona esta opción -g, no se puede crear un segundo sistema principal virtual porque WebSEAL verá el sistema principal de destino y el puerto como idénticos a una unión creada anteriormente, lo cual no se permite.

- Si va a utilizar uniones de sistema principal transparentes, cree una serie de uniones de vía de acceso transparentes para los widgets de cada producto.

a. Ejecute el mandato siguiente con pdadmin: `server task` *`servidor webseal`* `create -t` *`tipo transporte (ssl) o (tcp)`* `-x -h hostname` *`vía acceso`*

   Por ejemplo, escriba: `server task webseald-default create -t tcp -x -h monServer.ibm.com /BusinessSpace`.

b. Cree las raíces de contexto siguientes para el producto: Correlación de URL de Business Space para un servidor proxy inverso.

5. Efectúe pasos de configuración adicionales para resolver los problemas con las cookies de navegador y los sistemas principales virtuales.

   a. Para resolver la reasignación de nombre de la cookie de Business Space, añada el contenido siguiente al archivo de configuración de WebSEAL:

      ```
      [preserve-cookie-names]
      name = com.ibm.bspace.UserName
      name = com.ibm.wbimonitor.UserName
      ```

   b. Opcional: Si va a utilizar sistemas principales virtuales que no son los que se establecen por omisión con una raíz de contexto, es posible que experimente problemas con las páginas de Business Space. Puede que tenga que hacer que la unión deje de reescribir el JavaScript™ en las páginas de Business Space añadiendo la unión -j a la raíz de contexto. Ejecute el mandato siguiente: `server task default-webseald create -f -h` *`nombre_sistema_principal`* `-p` *`número_puerto`* `-t tcp -b supply -c iv-user,iv-creds,iv-groups -x -s -j -J trailer/`*`raíz contexto`*

Asignación del rol de superusuario de Business Space

En Business Space, puede asignar usuarios para que sean superusuarios (o Business Space administradores). Un superusuario puede ver, editar y suprimir todos los espacios y páginas, puede gestionar y crear plantillas, y puede cambiar la propiedad de un espacio cambiando el ID de propietario.

Antes de empezar

Si la seguridad administrativa está habilitada cuando configure Business Space, tenga en cuenta la información siguiente sobre grupos y superusuarios:

- Los usuarios que pertenecen al grupo de usuarios especial, **administradores**, tienen el rol de superusuario por omisión. Por consiguiente, la asignación de rol de superusuario la gestiona la pertenencia al grupo de usuarios.
- En un entorno de servidor único, el servidor Business Space crea el grupo de usuarios **administradores** en el registro de usuarios predeterminado. El ID de administrador proporcionado durante la configuración se añade automáticamente como miembro de dicho grupo.
- En un entorno de despliegue de red, el grupo de usuarios **administradores** no se crea automáticamente. Utilice el script `createSuperUser.py` para crear el grupo de usuarios y añada miembros al grupo en el registro de usuarios predeterminado.
- Si se utiliza otro registro de usuarios (por ejemplo, LDAP) en lugar del registro de usuarios por omisión o si se utiliza el registro de usuarios por omisión pero no desea utilizar el grupo de usuarios **administradores**, debe identificar el grupo de usuarios que vaya a utilizar para los superusuarios de Business Space. Asegúrese de que el registro de usuarios pueda entender el valor que proporcione. Por ejemplo, para LDAP, puede proporcionar un nombre como `cn=administrators,dc=company,dc=com`. Para obtener más información acerca de

la identificación de este grupo de usuarios, consulte las instrucciones para cambiar el grupo administradores en el apartado Qué hacer a continuación.

- Para Business Space en WebSphere Portal, el grupo predeterminado **wpsadmins** también se utiliza para el rol de superusuario. A los miembros de este grupo se les otorga el rol de superusuario para Business Space.

  Nota: La seguridad se debe habilitar si desea utilizar Business Space en WebSphere Portal.

Si la seguridad administrativa no está habilitada cuando configure Business Space, sólo el ID de usuario especial **BPMAdministrator** tendrá el rol de superusuario de Business Space.

Si tiene un entorno de despliegue de red, debe ejecutar el script `createSuperUser.py` para asignar el rol de superusuario: para crear el grupo de usuarios y añadir miembros. Antes de ejecutar el script, siga estos pasos:

- Asegúrese de no cambiar el nombre de grupo predeterminado **administradores**.
- Utilice el depósito predeterminado para el registro de usuarios.
- Inicie el servidor o el gestor de despliegue para el entorno de Business Space para el perfil donde está instalado Business Space.

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 en el que está instalado Business Space.
3. Escriba el mandato siguiente: `wsadmin -lang jython -f` *raíz_instalación*`\BusinessSpace\scripts\createSuperUser.py` *nombre_corto_usuario contraseña* donde *nombre_corto_usuario* es el identificador exclusivo para un usuario en Virtual Member Manager (VMM) y *contraseña* es la contraseña de VMM para ese usuario. Si existe dicho usuario en VMM, se añadirá al grupo de administradores.

   Nota: Cuando la vía de acceso contiene un espacio, por ejemplo, si *raíz_instalación* es `My install dir`, debe encerrar los nombres de vía de acceso entre comillas. Por ejemplo, escriba el mandato siguiente: `wsadmin -lang jython -f "\My install dir\BusinessSpace\scripts\createSuperUser.py"` *nombre_corto_usuario_en_VMM*.

Qué hacer a continuación

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.

Puede cambiar el grupo de usuarios especial predeterminado denominado **adminstradores**. Efectúe los pasos siguientes para verificar el nombre de grupo actual o cambiarlo por otro nombre.

Inspeccione el valor de la medida `com.ibm.mashups.adminGroupName` en el archivo de configuración:

- *raíz_perfil*`\BusinessSpace\`*nombre_nodo*`\`*nombre_servidor*`\mm.runtime.prof\config\ConfigService.properties` en un servidor autónomo, o

- *raíz_perfil_gestor_despliegue*\BusinessSpace*nombre_clúster*\mm.runtime.prof\config\ConfigService.properties en un clúster.

Si desea cambiar un grupo administrativo, realice los pasos siguientes en un servidor autónomo:

1. Modifique la medida com.ibm.mashups.adminGroupName en el archivo de configuración *raíz_perfil*\BusinessSpace*nombre_nodo**nombre_servidor*\mm.runtime.prof\config\ConfigService.properties.
2. Ejecute el mandato updatePropertyConfig en el entorno wsadmin del perfil: $AdminTask updatePropertyConfig {-serverName *nombre_servidor* -nodeName *nombre_nodo* -propertyFileName "*raíz_perfil*\BusinessSpace*nombre_nodo**nombre_servidor*\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"} y ejecute $AdminConfig save.
3. Reinicie el servidor.

Si desea cambiar un grupo administrativo, siga estos pasos en un clúster:

1. Modifique la medida com.ibm.mashups.adminGroupName en el archivo de configuración *raíz_perfil_gestor_despliegue*\BusinessSpace*nombre_clúster*\mm.runtime.prof\config\ConfigService.properties.
2. Ejecute el mandato updatePropertyConfig en el entorno wsadmin del perfil de entorno de despliegue: $AdminTask updatePropertyConfig {-clusterName *nombre_clúster* -propertyFileName "*raíz_perfil_gestor_despliegue*\BusinessSpace*cluster_name*\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"} y ejecute $AdminConfig save.
3. Reinicie el gestor de despliegue.

Si desea cambiar el superusuario cuando la seguridad no está habilitada, siga estos pasos en un servidor autónomo:

1. Modifique la medida noSecurityAdminInternalUserOnly en el archivo de configuración *raíz_perfil*\BusinessSpace*nombre_nodo**nombre_servidor*\mm.runtime.prof\config\ConfigService.properties.
2. Ejecute el mandato updatePropertyConfig en el entorno wsadmin del perfil: $AdminTask updatePropertyConfig {-serverName *nombre_servidor* -nodeName *nombre_nodo* -propertyFileName "*raíz_perfil*\BusinessSpace*nombre_nodo**nombre_servidor*\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"} y ejecute $AdminConfig save.
3. Reinicie el servidor.

Si desea cambiar el superusuario cuando la seguridad no está habilitada, siga estos pasos en un clúster:

1. Modifique la medida noSecurityAdminInternalUserOnly en el archivo de configuración *raíz_perfil_gestor_despliegue*\BusinessSpace*nombre_servidor*\mm.runtime.prof\config\ConfigService.properties.
2. Ejecute el mandato updatePropertyConfig en el entorno wsadmin del perfil de entorno de despliegue: $AdminTask updatePropertyConfig {-clusterName *nombre_clúster* -propertyFileName "*raíz_perfil_gestor_despliegue*\BusinessSpace*cluster_name*\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"} y ejecute $AdminConfig save.
3. Reinicie el gestor de despliegue.

Creación de seguridad de principio a fin

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.

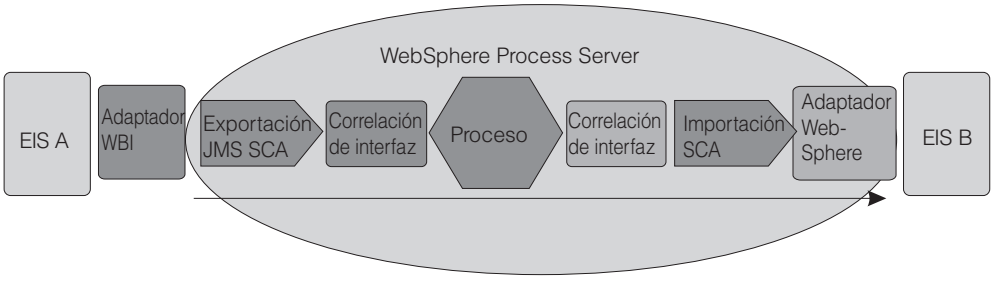
Procedimiento

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

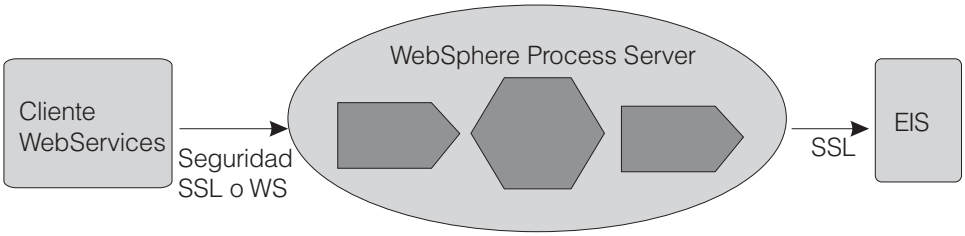
Las peticiones de entrada provienen de un WebSphere Business Integration Adapter. SCA (Service Component Architecture) invoca una correlación de interfaz basada en la exportación SCA. La petición pasa a través de un componente de proceso, una segunda correlación de interfaz y después se pasa a un segundo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

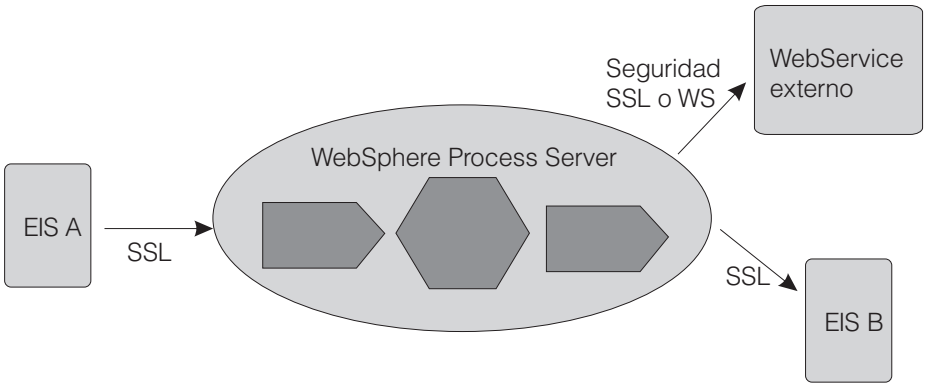
En este caso, un cliente del servicio Web invoca un componente de WebSphere Process Server. La petición pasa a través de varios componentes en el entorno de WebSphere Process Server antes de que un adaptador lo pase a un EIS.



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.



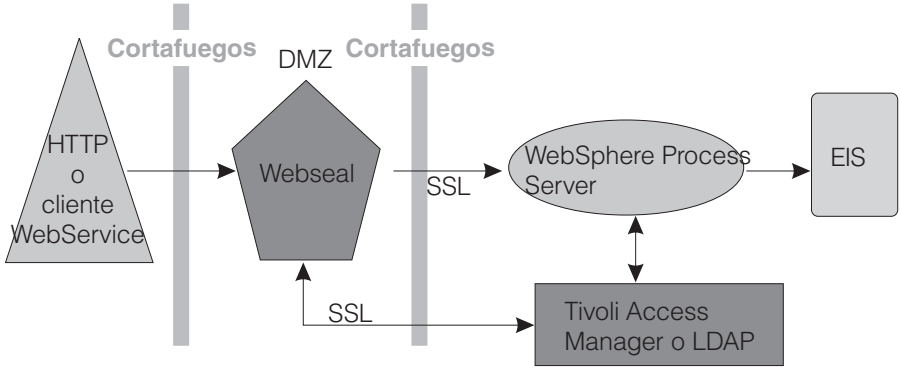
Al igual que con la petición de servicio Web de entrada, puede autenticar con el servicio Web externo como un cliente SSL, utilizando autenticación básica HTTP o autenticación WS-Security. Utilice LTPACallBackHandler como mecanismo de retorno de llamada para extraer el usernameToken del asunto RunAs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


Cortafuegos
DMZ
Cortafuegos
HTTP
o
cliente
WebService
Webseal
SSL
WebSphere Process
Server
EIS
SSL
Tivoli Access
Manager o LDAP