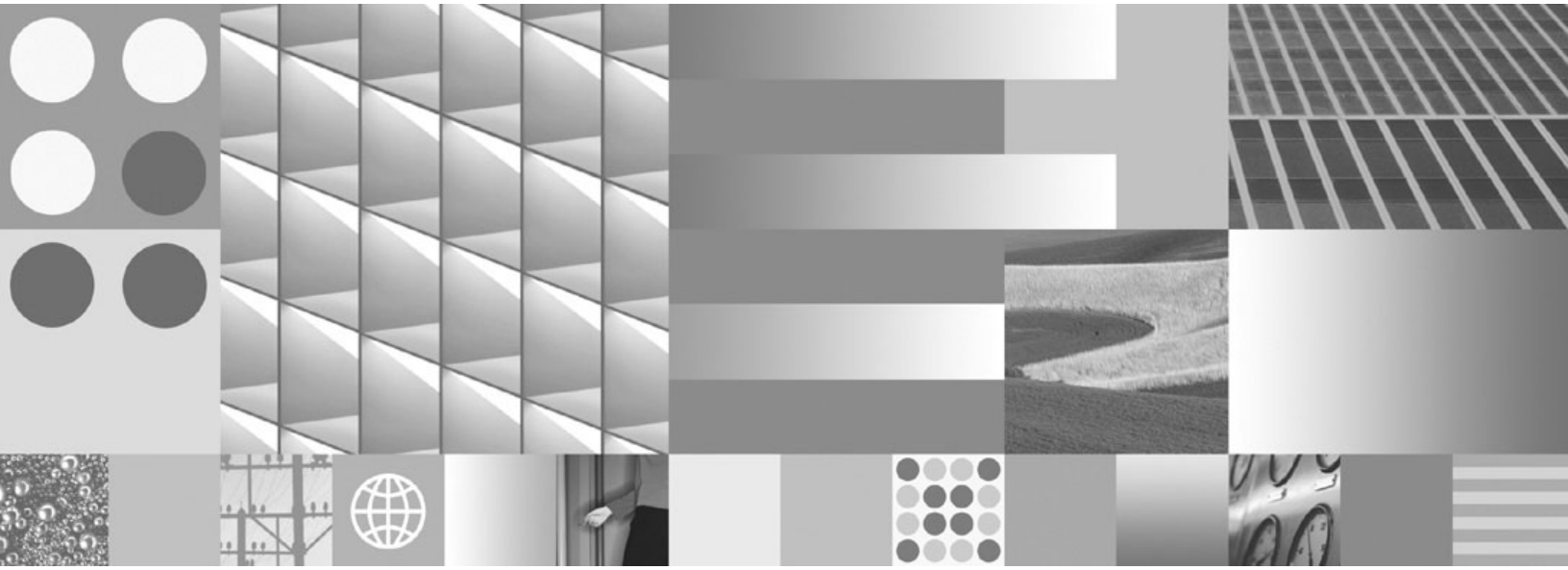
IBM Informix

Versión 11.1

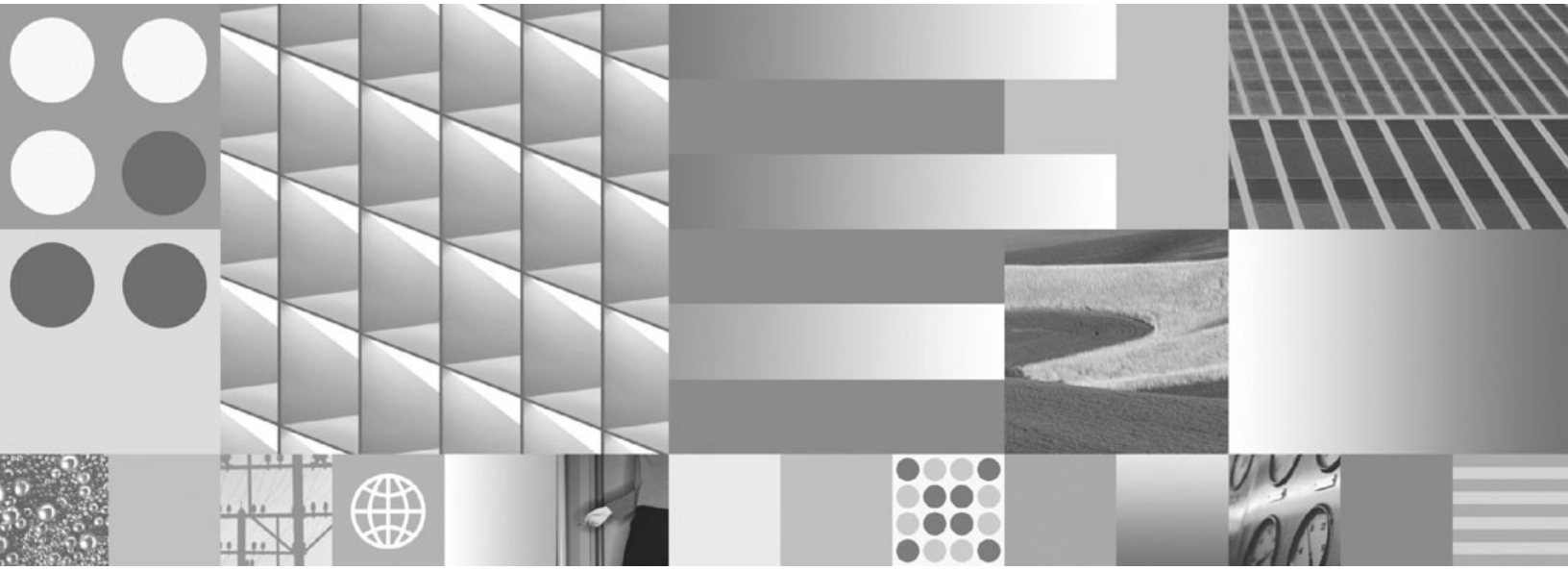


IBM Informix: Guía de seguridad

G229-6591-00

IBM Informix

Versión 11.1



IBM Informix: Guía de seguridad

G229-6591-00

Aviso:
Antes de utilizar esta información y el producto al que da soporte, lea la información contenida en el apartado "Avisos" en la página B-1.

Esta publicación es la traducción del original inglés *IBM Informix: Security Guide Version 11.1*, (G229-6389-00).

Contenido

Introducción

Acerca de esta publicación

Esta publicación documenta los métodos para proteger la seguridad de los datos impidiendo la visualización y modificación no autorizada de los datos o los objetos de base de datos.

Esta publicación también documenta el recurso de auditoría de seguridad del servidor de bases de datos.

Éste no es un manual de formación sobre seguridad de sistemas informáticos ni administración de recursos de confianza.

Tipos de usuarios

Esta publicación está escrita para los siguientes tipos de usuarios:

- Administradores de bases de datos
- Administradores de servidores de bases de datos
- Administradores de sistemas operativos
- Responsables de seguridad de los sistemas de bases de datos

En este manual se da por supuesto que el usuario cuenta con la siguiente preparación:

- Conocimientos prácticos del sistema, del sistema operativo y de los programas de utilidad que proporciona el sistema operativo
- Experiencia de trabajo con bases de datos relacionales o familiaridad con conceptos sobre bases de datos
- Experiencia en programación informática
- Experiencia en la administración de servidores de bases de datos, sistemas operativos o redes

Si tiene poca experiencia con las bases de datos relacionales, SQL o su sistema operativo, consulte la publicación *IBM Informix Guía de iniciación* para obtener una lista de títulos complementarios.

Nuevas funciones para IDS 11.1

Si desea obtener una lista completa de las nuevas funciones para este release, consulte la publicación *IBM Informix Guía de iniciación*. En este tema se enumeran las nuevas funciones que son relevantes para esta publicación.

Control de accesos basado en etiquetas

Esta función implementa Mandatory Access Control (control de accesos obligatorio), un requisito de seguridad que el gobierno federal de Estados Unidos y las agencias del sector público de otros países imponen en algunos sistemas de gestión de información que manejan información delicada o clasificada. Esta función proporciona mecanismos con los que definir una jerarquía de etiquetas de seguridad y asignar dicha jerarquía a objetos de base de datos y a usuarios de la base de datos.

Convenios de la documentación

Esta sección describe los convenios siguientes, los cuales se utilizan en la documentación de producto de IBM Informix Dynamic Server:

- Convenios tipográficos
- Convenios para componentes, productos y plataformas
- Diagramas de sintaxis
- Convenios de la línea de mandatos
- Convenios para código de ejemplo

Convenios tipográficos

Esta publicación utiliza los convenios siguientes para presentar términos nuevos, mostrar capturas de pantalla, describir la sintaxis de mandatos, etc.

Convenio	Significado
PALABRA CLAVE	Las palabras clave de SQL, SPL y algunos otros lenguajes de programación aparecen escritos en mayúsculas, con un font con remate.
cursiva	En el texto, aparecen en cursiva términos nuevos y palabras que se destacan. En la sintaxis y ejemplos de código, aparecen en cursiva valores de variable que debe especificar el usuario.
negrita	Aparecen en negrita los nombres de entidades de programas (tales como clases, sucesos y tablas), las variables de entorno, los nombres de archivos, las vías de acceso y los elementos de la interfaz (tales como iconos, opciones de menú y botones).
`monoespaciado`	La información que visualiza el producto y la información que especifica el usuario aparecen con el tipo de letra de monoespaciado.
`PULSACIÓN`	Las teclas que debe pulsar aparecen en letras mayúsculas escritas con un font sin remate (sans serif).
>	Este símbolo indica un elemento de menú. Por ejemplo, "Elija **Herramientas > Opciones**" significa que tiene que elegir el elemento **Opciones** en el menú **Herramientas**.

Señalización para funciones, productos y plataformas

La señalización para componentes, productos y plataformas identifica párrafos que contienen información específica de un componente, producto o plataforma. A

continuación, se muestran algunos ejemplos de esta señalización:

Dynamic Server

Identifica información que es específica de IBM Informix Dynamic Server

Fin de Dynamic Server

Windows solamente

Identifica información que es específica del sistema operativo Windows

Fin de Windows solamente

Esta señalización puede aplicarse a uno o más párrafos de un apartado. Cuando un apartado completo es aplicable a un producto o plataforma determinados, esto se indica en el texto de cabecera; por ejemplo:

Ordenación de tablas (Windows)

Convenios para código de ejemplo

Esta publicación contiene ejemplos de código de SQL a lo largo de toda ella. Excepto cuando se indique, el código no es específico de ninguna herramienta individual de desarrollo de aplicaciones de IBM Informix.

Si el ejemplo solamente contiene sentencias de SQL, las sentencias no están delimitadas por signos de punto y coma. A continuación sigue un código de ejemplo:

```
CONNECT TO stores_demo
...

DELETE FROM customer
   WHERE customer_num = 121
...

COMMIT WORK
DISCONNECT CURRENT
```

Para utilizar este código de SQL para un producto específico, debe aplicar las reglas de sintaxis de ese producto. Por ejemplo, si está utilizando DB–Access, debe delimitar varias sentencias con signos de punto y coma. Si está utilizando una API de SQL, debe utilizar EXEC SQL al principio de cada sentencia y un signo de punto y coma (u otro delimitador apropiado) al final de la sentencia.

Consejo: Los puntos suspensivos en un ejemplo de código indican que se añadiría más código en una aplicación completa, pero no es necesario mostrarlo para describir el concepto que se explica.

Para obtener instrucciones detalladas sobre la utilización de sentencias de SQL para una herramienta determinada de desarrollo de aplicaciones o para una API de SQL, consulte la documentación correspondiente al producto.

Documentación adicional

Puede ver, buscar e imprimir toda la documentación del producto desde el Centro de información de IBM Informix Dynamic Server, situado en esta dirección de la Web: http://publib.boulder.ibm.com/infocenter/idshelp/v111/index.jsp.

Para obtener documentación adicional sobre IBM Informix Dynamic Server y productos asociados, tales como notas de release, notas de máquina y notas de documentación, consulte la página de la biblioteca de productos en línea, situada en http://www.ibm.com/software/data/informix/pubs/library/. Como alternativa, puede consultar o instalar la documentación del producto a partir del CD de Iniciación rápida que se proporciona con el producto.

Cumplimiento de los estándares industriales

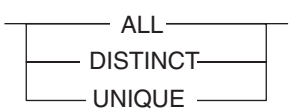
Las instituciones American National Standards Institute (ANSI) e International Organization of Standardization (ISO) han establecido conjuntamente un conjunto de normas de la industria para el Lenguaje de consulta estructurado (SQL). Los productos basados en SQL de IBM Informix se ajustan totalmente a la norma SQL-92 Entry Level (publicada como ANSI X3.135-1992), que es idéntica a ISO 9075:1992. Además, muchas funciones de los servidores de bases de datos IBM Informix cumplen las normas SQL-92 Intermediate y Full Level y X/Open SQL de Common Applications Environment (CAE).

Diagramas de sintaxis

Esta guía utiliza diagramas de sintaxis creados con los componentes siguientes para describir la sintaxis de las sentencias y todos los mandatos distintos de los que estén en el nivel del sistema.

Tabla 1. Componentes del diagrama de sintaxis

Componente representado en PDF	Componente representado en HTML	Significado
	`>>----------`	Comienza la sentencia.
	`---------->`	La sentencia continúa en la línea siguiente.
	`>----------`	La sentencia continúa desde la línea anterior.
	`----------><`	La sentencia finaliza.
	`--------SELECT----------`	Elemento necesario.
	`--+-----------------+---` `  '------LOCAL------'`	Elemento opcional.

	`---+-----ALL-------+---`
	`   +--DISTINCT-----+`
	`   '---UNIQUE------'`
		Elemento necesario a elegir. Debe haber un solo elemento.

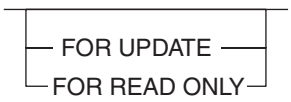
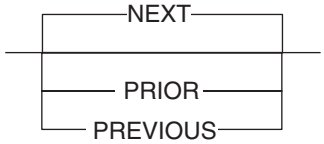
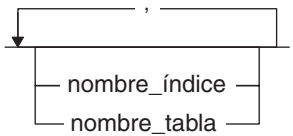
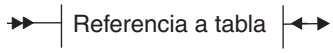
	`---+------------------+---`
	`    +--FOR UPDATE-----+`
	`    '--FOR READ ONLY--'`
		Los elementos opcionales a elegir se muestran debajo de la línea principal, de los cuales puede especificar uno.

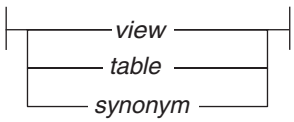
Tabla 1. Componentes del diagrama de sintaxis (continuación)

Componente representado en PDF	Componente representado en HTML	Significado

	<pre>.---NEXT---------.
	----+----------------+---
	+---PRIOR--------+
	'---PREVIOUS-----'</pre>
		Los valores debajo de la línea principal son opcionales, de los cuales puede especificar uno. Si no especifica uno, se utilizará como valor por omisión el valor por encima de la línea.

	<pre>.-------,-----------.
	V |
	---+-----------------+---
	+--nombre_índice-+
	'--nombre_tabla--'</pre>
		Elementos opcionales. Están permitidos varios elementos; cada repetición debe ir precedida de una coma.

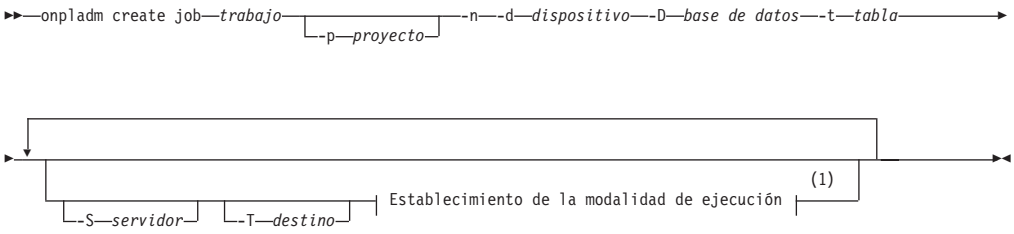
	<pre>>>-| Referencia a tabla |-><</pre>	Referencia a un segmento de la sintaxis.

Referencia a tabla
 
	<pre>Referencia a tabla
	|--+-----*view*--------+--|
	+------*table*------+
	'----*synonym*------'</pre>
		Segmento de sintaxis.

Cómo leer un diagrama de sintaxis de línea de mandatos

El siguiente diagrama de sintaxis de línea de mandatos utiliza algunos de los elementos listados en la tabla contenida en Diagramas de sintaxis.

Creación de un trabajo sin conversión

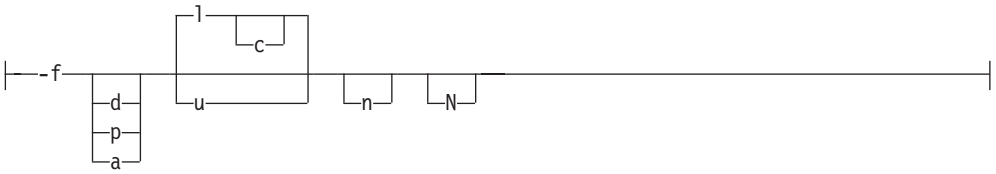


Notas:

1 Vea la página Z-1

La segunda línea de este diagrama contiene un segmento definido como "Establecimiento de la modalidad de ejecución", que de acuerdo con la nota al pie del diagrama, se encuentra en la página Z-1. Si se trataba de una referencia cruzada real, debería encontrar este segmento en la primera página del apéndice Z. En lugar de ello, este segmento se muestra en el diagrama de segmento siguiente. Observe que el diagrama utiliza componentes de comienzo y de final de segmento.

Establecimiento de la modalidad de ejecución:



Para ver el modo de construir un mandato correctamente, comience por la parte superior izquierda del diagrama principal. Siga el diagrama hacia la derecha, incluyendo los elementos que desee. Los elementos de este diagrama son sensibles a may/mín debido a que ilustran la sintaxis de programas de utilidad. Otros tipos de sintaxis, como por ejemplo de SQL, no son sensibles a may/mín.

El diagrama Creación de un trabajo sin conversión ilustra los pasos siguientes:

1. Escriba **onpladm create job** y, a continuación, el nombre del trabajo.
2. Opcionalmente, escriba **-p** y, a continuación, el nombre del proyecto.
3. Escriba los siguientes elementos necesarios:
   - **-n**
   - **-d** y el nombre del dispositivo
   - **-D** y el nombre de la base de datos
   - **-t** y el nombre de la tabla
4. Opcionalmente, puede elegir uno o más de los elementos siguientes y repetirlos un número arbitrario de veces:
   - **-S** y el nombre del servidor
   - **-T** y el nombre del servidor de destino
   - La modalidad de ejecución. Para establecerla, siga el diagrama de segmento Establecimiento de la modalidad de ejecución hasta escribir **-f**, escriba opcionalmente, **d**, **p** o bien **a**, y, a continuación, escriba opcionalmente **l** o bien **u**.
5. Siga el diagrama hasta el elemento final.

Palabras clave y signos de puntuación

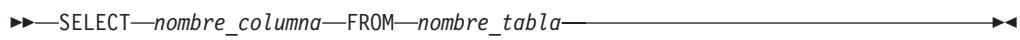
Las palabras clave son palabras reservadas para las sentencias y todos los mandatos, excepto los mandatos de nivel del sistema. Cuando aparece una palabra clave en un diagrama de sintaxis, se muestra en letras mayúsculas. Cuando utilice una palabra clave en un mandato, puede escribirla en letras mayúsculas o minúsculas, pero debe representar la palabra clave exactamente tal como aparezca en el diagrama de sintaxis.

También debe utilizar cualquier símbolo de puntuación en las sentencias y mandatos exactamente tal como se muestre en los diagramas de sintaxis.

Identificadores y nombres

Las variables sirven de contenedores para los identificadores y nombres en los diagramas de sintaxis y ejemplos. Puede sustituir una variable por un nombre, identificador o literal arbitrario, según el contexto. Las variables también se utilizan para representar elementos de sintaxis complejos que se amplían en diagramas de sintaxis adicionales. Cuando aparece una variable en un diagrama de sintaxis, ejemplo o texto, se muestra en *cursiva en minúsculas*.

En el diagrama de sintaxis siguiente se utilizan variables para ilustrar el formato general de una sentencia SELECT simple.



Cuando escribe una sentencia SELECT de esta forma, debe sustituir las variables *nombre_columna* y *nombre_tabla* por el nombre de una columna y tabla determinadas.

IBM agradece sus comentarios

Deseamos conocer cualquier corrección o clarificación que considere que pueda ser útil en nuestros manuales, lo cual nos ayudará a mejorar las ediciones futuras. Incluya la información siguiente:

- Nombre y versión de la publicación que está utilizando
- Apartado y número de página
- Sus sugerencias sobre la publicación

Envíenos sus comentarios a la siguiente dirección de correo electrónico:

hojacom@es.ibm.com

Esta dirección de correo electrónico está reservada para notificar errores y omisiones de nuestra documentación. Para obtener ayuda inmediata para un problema técnico, póngase en contacto con el Centro de soporte técnico de IBM. Para obtener instrucciones, visite el sitio Web de Soporte técnico de IBM Informix que se encuentra en http://www.ibm.com/planetwide/.

Valoramos en gran medida sus sugerencias.

Parte 1. Protección de datos

Esta sección trata sobre los métodos para proteger la seguridad de los datos impidiendo la visualización y la modificación no autorizada de los datos o de otros objetos de base de datos.

Capítulo 1. Programa de utilidad del servidor y seguridad de los directorios

Los programas de utilidad y directorios de productos de Informix Dynamic Server son seguros de forma predeterminada:

- Los programas de utilidad del servidor de bases de datos realizan comprobaciones de seguridad antes de que se inicie el servidor de bases de datos. Consulte el apartado "Comprobación de seguridad de los programas de utilidad del servidor en UNIX y Linux".
- La mayor parte de los programas de utilidad de IDS se ejecutan como usuarios protegidos y pertenecen a un grupo protegido. Consulte el apartado "Usuarios y pertenencia a grupos para ejecutar programas de utilidad de Dynamic Server" en la página 1-4.
- Los subdirectorios del directorio $INFORMIXDIR tienen propietarios y permisos de directorio específicos y pertenecen a un grupo específico según sus requisitos de seguridad. Consulte el apartado "Permisos del directorio INFORMIXDIR" en la página 1-4.
- Utilice el parámetro de configuración DB_LIBRARY_PATH para controlar la ubicación desde la que se pueden cargar objetos compartidos como, por ejemplo, módulos externos. Consulte el apartado "Seguridad para cargar módulos externos" en la página 1-5.

Comprobación de seguridad de los programas de utilidad del servidor en UNIX y Linux

Los programas de utilidad del servidor de bases de datos realizan comprobaciones de seguridad antes de que se inicie el servidor de bases de datos.

Cuando instale una nueva versión del servidor de bases de datos, deberá seguir las instrucciones de instalación para garantizar que los permisos de todos los archivos y directorios de claves se establezcan correctamente.

Para aumentar la seguridad, los programas de utilidad del servidor de claves realizan comprobaciones para determinar si el entorno es seguro. Antes de que se inicie el servidor de bases de datos, los siguientes valores deben permanecer sin cambios respecto a los valores establecidos durante la instalación:

- Los permisos sobre $INFORMIXDIR y algunos directorios incluidos en éste.

  Para cada directorio, el servidor de bases de datos comprueba que el directorio exista, que sea propiedad del usuario **informix** y el grupo correcto (tal como se muestra en el apartado "Permisos del directorio INFORMIXDIR" en la página 1-4) y que los permisos de directorio no incluyan permisos de grabación para el grupo o para otros usuarios.
- Los permisos sobre el archivo ONCONFIG.

  El archivo debe pertenecer al grupo del Administrador del servidor de bases de datos (DBSA). Si el grupo del DBSA es **informix** (el grupo predeterminado), el archivo ONCONFIG deberá ser propiedad del usuario **informix**; de lo contrario, la propiedad no estará restringida. El archivo no debe tener permisos de grabación para otras personas.
- Los permisos sobre el archivo **sqlhosts**.

En la configuración estándar, el archivo **sqlhosts** está ubicado en el directorio **$INFORMIXDIR/etc**. El propietario debe ser el usuario **informix**, el grupo debe ser el grupo **informix** o el grupo DBSA y el archivo no debe tener permisos de grabación. Si el archivo se especifica mediante una variable de entorno INFORMIXSQLHOSTS, el propietario y el grupo no se comprobarán; no obstante, no se permitirán los permisos de grabación públicos.

- Longitudes de los nombres de archivo.

  Las longitudes de los nombres de archivo **$INFORMIXDIR/etc/onconfig.std** y **$INFORMIXDIR/etc/$ONCONFIG** deben ser inferiores a 256 caracteres.

Si las pruebas de cualquiera de estas condiciones fallan, los programas de utilidad finalizarán con un mensaje de error.

Importante: El servidor de bases de datos no lee los archivos de configuración si se pueden grabar públicamente, a menos que la variable de entorno INFORMIXDIR esté designada como segura en el directorio **/etc/informix**. Consulte la información de los apartados "Inhabilitación de la comprobación de seguridad" y "Protección de un entorno inseguro".

Inhabilitación de la comprobación de seguridad

Aunque se recomienda encarecidamente no inhabilitar **nunca** la comprobación de seguridad, se puede inhabilitar parcialmente la comprobación de seguridad para un servidor de bases de datos que resida en un directorio $INFORMIXDIR específico.

Si opta por inhabilitar la comprobación de seguridad aunque se recomienda no hacerlo nunca, deberá utilizar el script **ibmifmx_security.sh** para limitar el número de programas SUID y SGID en el sistema.

Para inhabilitar la comprobación de seguridad:

Como usuario **root**, ejecute el script **INFORMIXDIR/etc/informixdir-is-insecure**. Después de ejecutar satisfactoriamente este script, los mensajes de aviso seguirán apareciendo cuando se ejecuten los programas de utilidad, pero los programas continuarán. Puede especificar el valor de INFORMIXDIR en la línea de mandatos como un argumento para el script. Por lo tanto, no es necesario establecer INFORMIXDIR en el entorno del usuario **root**.

El script **informixdir-is-insecure** crea un directorio **/etc/informix** (si es necesario) que es propiedad de **root** y tiene 555 permisos. En este directorio, el script crea un archivo denominado **server-*xx.xx.yyy*** que tiene 444 permisos. La parte *xx.xx* del nombre de archivo corresponde al número de versión principal y la parte *yyy* es el número de fix pack: por ejemplo, **server-11.10.UC1**. Este archivo ofrece una lista de los valores de $INFORMIXDIR para los que la comprobación de seguridad está inhabilitada.

Nota: Es posible que el formato del contenido de los archivos **server-*xx.xx.yyy*** cambie en futuros releases.

Protección de un entorno inseguro

Si el servidor de bases de datos informa de que el entorno ya no es seguro y que los programas se cierran, deberá restablecer los permisos de directorio relevantes.

Para proteger un entorno inseguro:

Como usuario **root**, ejecute el script **$INFORMIXDIR/etc/make-informixdir-secure**. Aunque el usuario **informix** tiene permiso para ejecutar el script, el script no podrá solucionar los problemas a menos que el directorio sea propiedad del usuario **informix**. No obstante, los mensajes de error indican lo que queda por arreglar. El script también muestra los archivos y directorios de $INFORMIXDIR que pertenecen a un propietario o a un grupo imprevisto o que tienen permiso de grabación público.

Mensajes de error y de aviso de las comprobaciones de seguridad de los programas de utilidad

Si la comprobación de seguridad que un programa de utilidad de un servidor realiza durante el inicio detecta un problema, la comprobación de seguridad devolverá un mensaje de error.

Estos mensajes se devuelven cuando el archivo de mensajes y el soporte de internacionalización no están disponibles; por lo tanto, los mensajes de error no tienen los números de error y no están traducidos.

Para los siguientes problemas, se muestra uno de los mensajes siguientes y el programa de utilidad continúa:

- `INFORMIXDIR or ONCONFIG is too long. Maximum length for $INFORMIXDIR/etc/$ONCONFIG is 255 characters.`
- `INFORMIXSQLHOSTS is too long.  Maximum length is 255 characters.`
- `ONCONFIG not set; TBCONFIG set.  TBCONFIG will not be supported in future.`

Para los siguientes problemas, el programa de utilidad termina y muestra uno de los siguientes mensajes:

- User informix not found.
- Group informix not found.
- Could not access *nombre archivo lógico*.
- *nombre archivo lógico* is not owned by user with id *UID*.
- *nombre archivo lógico* not owned by group with id *GID*.
- *nombre archivo lógico* has insecure mode *modalidad*.
- Could not access *nombre archivo lógico*.

La tabla siguiente define las variables utilizadas en los mensajes anteriores.

Variable	Explicación
nombre	Nombre del archivo o del directorio
archivo lógico	ONCONFIG, INFORMIXSQLHOSTS, INFORMIXDIR o INFORMIXDIR/*xxx* (donde *xxx* es uno de varios subdirectorios de $INFORMIXDIR). Por ejemplo, si INFORMIXDIR se establece en **/usr/informix**, el mensaje sería el siguiente: `INFORMIXSQLHOSTS /usr/informix/etc/sqlhosts is not owned by the user with id 1234.`
modalidad	Valor de permisos octal
UID	Un número

Variable	Explicación
GID	Un número

Usuarios y pertenencia a grupos para ejecutar programas de utilidad de Dynamic Server

La mayor parte de los programas de utilidad de IDS se ejecutan como usuarios protegidos y pertenecen a un grupo protegido.

Los siguientes programas de utilidad de Dynamic Server son SUID **root** y SGID **informix**:

- **onaudit**
- **onbar_d**
- **ondblog**
- **onedcu**
- **oninit**
- **onmode**
- **ON-Monitor**
- **onshowaudit**
- **onsmsync**
- **onsnmp**
- **onsrvapd**
- **ontape**
- **snmpdm**

Los siguientes programas de utilidad de Dynamic Server son SGID **informix**:

- **oncheck**
- **onedpdu**
- **onload**
- **onlog**
- **onparams**
- **onpload**
- **onspaces**
- **onstat**
- **onunload**
- **xtree**

Permisos del directorio INFORMIXDIR

Los subdirectorios del directorio $INFORMIXDIR tienen propietarios y permisos de directorio específicos y pertenecen al grupo específico según sus requisitos de seguridad.

La tabla siguiente lista los directorios de $INFORMIXDIR y sus respectivos propietarios, grupos y permisos.

Subdirectorio	Propietario	Grupo	Permisos
. ($INFORMIXDIR)	informix	informix	755

Subdirectorio	Propietario	Grupo	Permisos
bin	informix	informix	755
lib	informix	informix	755
gls	informix	informix	755
msg	informix	informix	755
etc	informix	DBSA	775
aaodir	informix	AAO	775
tmp	informix	informix	770

Consulte la publicación "Roles administrativos y separación de roles" en la página 8-1 para obtener más información sobre los grupos de administrador del servidor de bases de datos (DBSA), del responsable del análisis de auditoría (AAO) y del responsable de seguridad del sistema de bases de datos (DBSSO).

Seguridad para cargar módulos externos

Utilice el parámetro de configuración DB_LIBRARY_PATH para controlar la ubicación desde la que se pueden cargar objetos compartidos como, por ejemplo, módulos externos.

Utilice el parámetro de configuración DB_LIBRARY_PATH para especificar una lista separada por comas de ubicaciones de prefijo de directorio válidas desde las que el servidor de bases de datos puede cargar módulos externos como, por ejemplo, módulos DataBlade. DB_LIBRARY_PATH entra en vigor cuando el servidor de bases de datos reinicia después de que se haya establecido el parámetro.

El parámetro de configuración DB_LIBRARY_PATH permite controlar la ubicación desde la que se pueden cargar objetos compartidos y permite aplicar políticas y estándares sobre los formatos de la cláusula EXTERNAL NAME de las sentencias CREATE FUNCTION, CREATE PROCEDURE y CREATE ROUTINE.

Si el parámetro de configuración DB_LIBRARY_PATH no está establecido o no se cuenta en el archivo ONCONFIG, no se realizarán comprobaciones de seguridad para cargar módulos externos.

Debe incluir en los valores de DB_LIBRARY_PATH cada sistema de archivos en el que sus políticas de seguridad autoricen la presencia de módulos DataBlade y UDR. Los módulos DataBlade proporcionados con Dynamic Server se almacenan en el directorio **$INFORMIXDIR/extend**. Para que la capacidad de ampliación funcione debidamente cuando la seguridad esté activada, la serie `"$INFORMIXDIR/extend"` debe formar parte de DB_LIBRARY_PATH.

Para obtener más información sobre el parámetro de configuración DB_LIBRARY_PATH, consulte la publicación *IBM Informix Dynamic Server Administrator's Reference*.

Capítulo 2. Cifrado de datos de red

Utilice el cifrado de red para cifrar datos transmitidos por la red. Esto incluye los datos transmitidos entre el servidor de bases de datos y los sistemas cliente.

El *cifrado* es el proceso de transformación de los datos a un formato ininteligible para impedir el uso no autorizado de los datos. Para leer un archivo cifrado, se debe tener acceso a una clave secreta o una contraseña que permita descifrarlo. Los datos descifrados se denominan *texto sin formato*; los datos cifrados se denominan *texto cifrado*. Un *cifrado* es un algoritmo de cifrado-descifrado.

El Estándar de cifrado de datos (DES, del inglés Data Encryption Standard) es un algoritmo criptográfico diseñado para cifrar y descifrar datos utilizando bloques de 8 bytes y una clave de 64 bits.

EL DES triple (DES3) es una variación de en la que se utilizan claves de 64 bits para una clave de 192 bits. DES3 funciona cifrando primer lugar el texto sin formato utilizando los 64 primeros bits de la clave. Luego el texto cifrado se descifra utilizando la siguiente parte de la clave. Por último, el texto cifrado resultante se vuelve a cifrar utilizando la última parte de la clave.

El Estándar de cifrado avanzado (AES, del inglés Advanced Encryption Standard) es un algoritmo de sustitución utilizado por el gobierno de los Estados Unidos.

Dos modalidades de cifrado son:

- *Modalidad de bloques*, un método de cifrado en el que el mensaje se divide en bloques y el cifrado se realiza individualmente en cada bloque. Puesto que cada bloque tiene, como mínimo, una longitud de 8 bytes, la modalidad de bloques permite la digna aritmética de 64 bits en el algoritmo de cifrado.
- *Modalidad de secuencia*, un método de cifrado en el que se cifra cada byte individualmente. Se considera generalmente una forma de cifrado débil.

Blowfish es un cifrado de bloques que funciona en bloques de datos de 64 bits (8 bytes). Utiliza una clave de tamaño variable, aunque normalmente las claves de 128 bits (16 bytes) se consideran buenas para un cifrado fuerte. Blowfish se puede utilizar en las mismas modalidades que DES.

El modo en que debe configurar el cifrado de red depende del tipo de comunicación de red que utilice:

- Comunicaciones servidor-cliente normales: utilice módulos de soporte de comunicaciones. Consulte el apartado “Módulos de soporte de comunicaciones para el cifrado de la transmisión de datos” en la página 2-2.
- Opciones de Enterprise Replication o alta disponibilidad (como High-Availability Data Replication, los servidores secundarios autónomos remotos y los servidores secundarios de disco compartido): utilice parámetros de configuración. Consulte el apartado “Cifrado de datos de red de Enterprise Replication y alta disponibilidad” en la página 2-12.

Módulos de soporte de comunicaciones para el cifrado de la transmisión de datos

Puede utilizar los módulos de soporte de comunicaciones (CSM) para cifrar transmisiones de datos, incluidas transacciones distribuidas, que se realicen por la red.

El CSM de cifrado, ENCCSM, proporciona el cifrado de transmisiones de red.

Esta opción proporciona el cifrado de datos completo con una biblioteca de criptografía estándar, con muchas opciones configurables. Se transmite un código de autenticación de mensajes (MAC) como parte de la transmisión de datos cifrada para garantizar la integridad de datos.. Un MAC es un resumen de mensaje cifrado.

Los CSM tienen las siguientes restricciones:

- No se puede utilizar un CSM de cifrado y un CSM de contraseña simple simultáneamente. Por ejemplo, si utiliza el CSM de contraseña simple, SPWDCSM, y decide cifrar los datos de la red, deberá eliminar las entradas correspondientes a SPWDCSM en los archivos **concsm.cfg** y **sqlhosts**.
- No se puede utilizar el CSM de contraseña simple ni el CSM de cifrado sobre una conexión multiplexada.
- Los clústeres de Enterprise Replication y de alta disponibilidad (Duplicación de datos de alta disponibilidad, servidores secundarios autónomos remotos y servidores secundarios de disco compartido) soportan el cifrado, pero no pueden utilizar una conexión configurada con un CMS.

  Para utilizar el cifrado de red con los clústeres de Enterprise Replication o de alta disponibilidad, establezca los parámetros de configuración del cifrado.
- No se pueden combinar en el mismo puerto conexiones cifradas y conexiones sin cifrar.

Habilitación del cifrado con módulos de soporte de comunicaciones

Para utilizar el cifrado con los módulos de soporte de comunicaciones, debe modificar el archivo de configuración **concsm.cfg**.

Para habilitar el cifrado de red:

1. Añada una línea al archivo de configuración **concsm.cfg**. El archivo **concsm.cfg** debe contener una entrada para cada módulo de soporte de comunicaciones (del mismo tipo) que se utilice.
2. Añada una entrada a la columna **opciones** del archivo **sqlhosts** o del registro. Para obtener información sobre cómo especificar el CSM en el archivo **sqlhosts** o en el registro, consulte *IBM Informix Dynamic Server Administrator's Guide*.

Archivo de configuración CSM

Si utiliza un módulo de soporte de comunicaciones (CSM), debe tener un archivo **concsm.cfg**.

Una entrada en el archivo **concsm.cfg** es una sola línea y está limitada a 1024 caracteres. Después de describir el CSM en el archivo **concsm.cfg**, puede habilitarlo en el parámetro de **opciones** del archivo **sqlhosts**, tal como se describe en la publicación *IBM Informix Dynamic Server Administrator's Guide*.

El archivo **concsm.cfg** reside en el directorio **$INFORMIXDIR/etc** de modo predeterminado. El directorio predeterminado del archivo **concsm.cfg** es **INFORMIXDIR/etc**. Si desea almacenar el archivo en otra ubicación, puede alterar temporalmente la ubicación predeterminada estableciendo como valor de la variable de entorno **INFORMIXCONCSMCFG** el nombre de la vía de acceso completa de la nueva ubicación. Para obtener información sobre cómo establecer la variable de entorno **INFORMIXCONCSMCFG**, consulte la publicación *IBM Informix Guide to SQL: Reference*.

Las entradas del archivo **concsm.cfg** deben ajustarse a las restricciones siguientes:

- Los caracteres siguientes no se permiten como parte de los nombres de las vías de acceso de bibliotecas:
  - = (signo igual)
  - " (comilla doble)
  - , (coma)
- No se pueden utilizar espacios en blanco a menos que éstos formen parte de un nombre de vía de acceso.

Tipos de cifrado y modalidades de cifrado

Debe especificar qué tipos de cifrado y modalidades de cifrado se deben utilizar durante el cifrado.

El cifrado y la modalidad que se utilizan se eligen aleatoriamente entre los cifrados comunes entre los dos servidores. Asegúrese de que todos los sistemas servidor y cliente que participan en la comunicación cifrada tengan cifrados y modalidades en común. El cifrado es más seguro si se incluyen más tipos de cifrado y modalidades entre los que el servidor de bases de datos pueda conmutar. Para obtener información sobre cómo conmutar entre cifrados, consulte el apartado "Frecuencia de conmutación" en la página 2-5.

Importante: Se recomienda encarecidamente no especificar cifrados específicos. Por motivos de seguridad, se deben permitir todos los cifrados. Si se descubre un cifrado tiene un punto débil, puede excluirlo.

Utilice la opción **allbut** para listar los cifrados y las modalidades que se deben excluir. Incluya la lista **allbut** entre corchetes (<>). La lista puede incluir entradas exclusivas abreviadas. Por ejemplo, **bf** puede representar **bf1**, **bf2** y **bf3**. No obstante, si la abreviación es el nombre de un cifrado real, entonces *sólo* se eliminará ese cifrado. Por lo tanto, **des** sólo elimina el cifrado DES, pero **de** elimina **des**, **ede** y **desx**.

Se soportan los siguientes cifrados **des**, **ede** y **desx**.

Cifrado	Explicación	Cifrado Blowfish	Explicación
des	DES (clave de 64 bits)	bf1	Blowfish (clave de 64 bits)
ede	DES triple	bf2	Blowfish (clave de 128 bits)
desx	DES ampliado (clave de 128 bits)	bf3	Blowfish (clave de 192 bits)

Importante: El cifrado **desx** sólo se puede utilizar en modalidad **cbc**.

Se soportan los siguientes cifrados AES.

Cifrado	Explicación
aes	AES (clave de 128 bits)
aes128	AES (clave de 128 bits)
aes192	AES (clave de 192 bits)
aes256	AES (clave de 256 bits)

Se soportan las siguientes modalidades.

Modalidad	Explicación
ecb	Electronic Code Book
cbc	Cipher Block Chaining
cfb	Cipher Feedback
ofb	Output Feedback

Como la modalidad **ecb** se considera débil, sólo se incluye si se solicita específicamente. No se incluye en la lista **all** ni en la lista **allbut**.

Archivos de claves MAC

Los archivos de claves MAC contienen claves de cifrado que se utilizan para cifrar mensajes.

Todos los servidores de bases de datos y los sistemas cliente que participan en el cifrado deben tener archivos de claves MAC en común. Para obtener información sobre cómo conmutar entre claves MAC, consulte el apartado “Frecuencia de conmutación” en la página 2-5.

El archivo de claves MAC predeterminado es el archivo incorporado proporcionado por Dynamic Server. Este archivo proporciona una verificación limitada de los mensajes (alguna validación del mensaje recibido y la determinación de que parece proceder de un cliente o servidor Informix Dynamic Server). La verificación más sólida la realiza un archivo de claves MAC generado por el sitio. Puede generar archivos de claves con el programa de utilidad **GenMacKey**.

Cada uno de los archivos de claves MAC recibe una prioridad y se negocia en el momento de la conexión. El programa de utilidad **GenMacKey** asigna la prioridad a los archivos de claves MAC de acuerdo con su hora de creación. El archivo de la claves incorporado tiene la prioridad más baja.

Consejo: Si no hay ningún archivo de claves MAC, se utiliza de modo predeterminado el archivo de claves MAC incorporado. No obstante, al utilizar un archivo de claves MAC, el archivo de claves MAC incorporado predeterminado se inhabilita.

Generación de un archivo de claves MAC nuevo

Puede generar un archivo de claves MAC nuevo.

Para generar un archivo de claves MAC nuevo:

1. Ejecute el mandato siguiente desde la línea de mandatos:

GenMacKey –o *nombre_archivo*

El *nombre_archivo* es la vía de acceso y el nombre de archivo del archivo de claves MAC nuevo.

2. Actualice la configuración del servidor central para incluir la ubicación del archivo de claves MAC nuevo de uno de los modos siguientes:
   - **Utilizando códigos de cifrado:** Edite la línea relevante del archivo **concsm.cfg** para añadir una vía de acceso y un nombre de archivo al código **mac**. Para obtener instrucciones, consulte el apartado "Código mac" en la página 2-10.
   - **Utilizando parámetros de cifrado:** Edite el archivo de parámetros de cifrado para modificar el valor del parámetro ENCCSM_MACFILES. Para obtener instrucciones, consulte el apartado "Parámetro ENCCSM_MACFILES" en la página 2-8.
3. Si es necesario, elimine de la configuración las entradas antiguas del archivo de claves MAC.
4. Distribuya el archivo de claves MAC nuevo a todos los sistemas adecuados.

Niveles de MAC

Los niveles de MAC determinan el tipo de generación de claves MAC.

Los niveles de generación soportados son:

- **high**. Utiliza la generación MAC SHA1 en todos los mensajes.
- **medium**. Utiliza la generación MAC SHA1 para todos los mensajes que tienen una longitud superior a los 20 bytes y la transformación XOR en mensajes más pequeños.
- **low**. Utiliza la transformación XOR en todos los mensajes.
- **off**. No utiliza la generación MAC.

Al nivel se le establece como prioridad el valor más alto. Por ejemplo, si un servidor de bases de datos tiene un nivel de **high** y **medium** habilitado y el otro servidor de bases de datos sólo tiene **low** habilitado, el intento de conexión fallará. La entrada **off** sólo se debe utilizar entre servidores cuando esté garantizado que hay una conexión de red segura.

Asegúrese de que todos los sistemas servidor y cliente que participan en la comunicación cifrada tengan niveles de MAC en común.

Frecuencia de conmutación

La frecuencia de conmutación define cuando se renegocian cifrados y/o claves secretas.

Como más tiempo se utilicen la clave secreta y el cifrado, más probable será que un atacante rompa las reglas de cifrado. Para evitarlo, los criptólogos recomiendan cambiar periódicamente la clave secreta y el cifrado en las conexiones de larga duración. El tiempo predeterminado al que se produce esta renegociación es de una vez por hora. Mediante el uso de opciones de conmutación, se puede establecer el tiempo en minutos al que se producirá la renegociación.

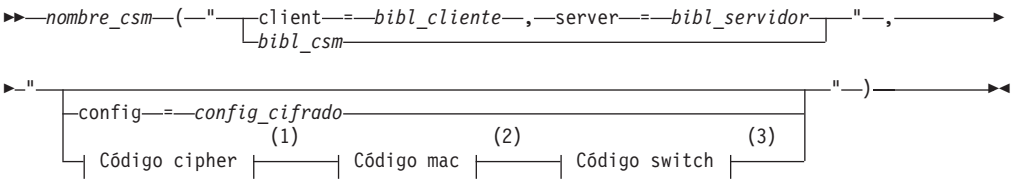
Sintaxis del cifrado de datos de red

Debe especificar las bibliotecas de cifrado de red y las opciones de cifrado en el archivo **concsm.cfg**.

Puede especificar los siguientes tipos de opciones de cifrado:

- Los tipos de cifrado DES y AES para utilizarlos durante el cifrado
- Las modalidades que se deben utilizar durante el cifrado
- Archivos de claves de código de autenticación de mensajes (MAC)
- Niveles de MAC
- La frecuencia de conmutación para los cifrados y las claves

Puede especificar las opciones de cifrado en un archivo distinto o utilizando códigos de cifrado en el archivo **concsm.cfg**. Para configurar el cifrado de red, utilice la sintaxis siguiente para añadir una o varias líneas al archivo **concsm.cfg**.



Notas:

1 Consulte el apartado "Código cipher" en la página 2-9.

2 Consulte el apartado "Código mac" en la página 2-10.

3 Consulte el apartado "Código switch" en la página 2-11.

Opción	Descripción
client=*bibl_cliente*	Es la vía de acceso completa y el nombre de la biblioteca compartida que es el CSM en el sistema cliente. Los sistemas cliente utilizan este CSM para comunicarse con el servidor de bases de datos. La biblioteca que Dynamic Server proporciona es **$INFORMIXDIR/lib/client/csm/iencs11a.so**.
config=*config_cifrado*	Es la vía de acceso completa y el nombre del archivo en el que se definen los parámetros de cifrado. Si el archivo no existe, se utilizan los valores predeterminados. No se devuelve ningún error. Para obtener más información sobre el uso de los parámetros de cifrado, consulte el apartado "Archivo de parámetros de cifrado" en la página 2-7.
bibl_csm	Es la vía de acceso completa y el nombre de la biblioteca compartida que es el CSM si el servidor de bases de datos y el sistema cliente comparten el CSM. La biblioteca que Dynamic Server proporciona es **$INFORMIXDIR/lib/csm/iencs11a.so**.
nombre_csm	Es el nombre que asigne al módulo de soporte de comunicaciones. Para el cifrado de red, utilice ENCCSM.

Opción	Descripción
server=*bibl_servidor*	Es la vía de acceso completa y el nombre de la biblioteca compartida que es el CSM en el servidor de bases de datos. La biblioteca proporcionada por Dynamic Server se instala normalmente en los directorios siguientes: • UNIX: **$INFORMIXDIR/lib/csm/iencs11a.so** • Windows: **%INFORMIXDIR%\bin\iencs11a.so**

Archivo de parámetros de cifrado

Puede configurar las opciones de cifrado estableciendo parámetros de cifrado en un archivo.

En los parámetros de cifrado que especifique en el archivo **concsm.cfg**, cada opción tiene un formato siguiente:

```
nombre_parámetro valor
```

Utilice los parámetros siguientes para establecer las opciones de cifrado:

- ENCCSM_CIPHERS: Cifrados que se deben utilizar
- ENCCSM_MAC: Niveles MAC
- ENCCSM_MACFILES: Ubicaciones de los archivos MAC
- ENCCSM_SWITCH: El cifrado y la clave cambian frecuentemente

Se aplican las restricciones siguientes a los valores de los parámetros:

- Cada entrada debe tener el formato *nombre_parámetro valor* separado por espacios en blanco.
- No se permiten los espacios en blanco dentro de un valor.
- Cada parámetro debe tener una entrada en el archivo de configuración. Si existen varias entradas, sólo se tendrá en cuenta la primera entrada.
- Si un parámetro no existe en el archivo de configuración, se utilizan los valores predeterminados.
- Los caracteres que van después de un carácter de comentario (#) se pasan por alto; no obstante, el valor del nombre de la vía de acceso no se pasa por alto.

Parámetro ENCCSM_CIPHERS:

El parámetro ENCCSM_CIPHERS especifica los cifrados y las modalidades que se deben utilizar durante el cifrado.

```
syntax ENCCSM_CIPHERS

all|allbut:<lista de cifras y
modalidades>|cipher:mode{,cipher:mode ...}
```

- `all`: Especifica que se deben incluir todos los cifrados y modalidades disponibles, excepto la modalidad ECB. Por ejemplo:

  ```
  ENCCSM_CIPHERS all
  ```

- `allbut:<`*`lista de cifrados y modalidades`*`>`: Especifica que se deben incluir todas los cifrados y modalidades a excepción de las que aparecen en la lista. Separe los cifrados o las modalidades mediante una coma. Por ejemplo:

  ```
  ENCCSM_CIPHERS allbut:<cbc,bf>
  ```

- *`cifrado`*`:`*`modalidad`*: Especifica los cifrados y las modalidades. Separe los pares de cifrado-modalidad mediante una coma. Por ejemplo:

  ```
  ENCCSM_CIPHERS des3:cbc,des3:ofb
  ```

- valor predeterminado: `allbut:<ecb>`

Para obtener más información sobre los cifrados y las modalidades, consulte el apartado "Tipos de cifrado y modalidades de cifrado" en la página 2-3.

Parámetro ENCCSM_MAC:

El parámetro ENCCSM_MAC especifica el nivel de MAC que se debe utilizar.

valor predeterminado
`medium`

rango de valores
Una o varias de las siguientes opciones, separadas por comas:
- `off` no utiliza la generación MAC.
- `low` utiliza la transformación XOR en todos los mensajes.
- `medium` utiliza la generación MAC SHA1 para todos los mensajes que tienen una longitud superior a los 20 bytes y la transformación XOR en mensajes más pequeños.
- `high` utiliza la generación MAC SHA1 en todos los mensajes.

Por ejemplo: `ENCCSM_MAC medium,high`

Para obtener más información sobre los niveles de MAC, consulte el apartado "Niveles de MAC" en la página 2-5.

Parámetro ENCCSM_MACFILES:

El parámetro ENCCSM_MACFILES especifica los archivos de clave MAC que se deben utilizar.

valor predeterminado
`builtin`

unidades
nombres de vía de acceso, con una longitud máxima de 1536 bytes

rango de valores
Uno o varios nombres de vía de acceso y de archivo completos separados por comas y la palabra clave opcional **builtin**. Por ejemplo:
```
ENCCSM_MACFILES /usr/local/bin/mac1.dat,/usr/local/bin/
mac2.dat,builtin
```

Para obtener más información, consulte el apartado "Archivos de claves MAC" en la página 2-4.

Parámetro ENCCSM_SWITCH:

El parámetro ENCCSM_SWITCH define el número de minutos entre el cifrado y la renegociación de la clave.

syntax ENCCSM_SWITCH`tiempo_conmut_cifrado,tiempo_conmut_clave`
- *tiempo_conmut_cifrado* específica los minutos entre las renegociaciones del cifrado
- *tiempo_conmut_clave* especifica los minutos entre las renegociaciones de la clave secreta

valor predeterminado
`60,60`

unidades
minutos

rango de valores
enteros positivos

Para obtener más información, consulte el apartado “Frecuencia de conmutación” en la página 2-5.

Ejemplo del archivo de parámetros de cifrado:

El archivo de parámetros de cifrado especifica valores para los parámetros de cifrado.

El ejemplo siguiente muestra un archivo de parámetros de cifrado:

```
ENCCSM_CIPHERS          all
ENCCSM_SWITCH           120,60
ENCCSM_MAC              medium
ENCCSM_MACFILE          /usr/informix/etc/MacKey.dat
```

El ejemplo siguiente muestra una línea del archivo **concsm.cfg** para especificar el cifrado con un archivo de parámetros denominado **encrypt.txt**:

```
ENCCSM("usr/informix/lib/cms/iencs11a.so",
"config=/usr/lib/encrypt.txt")
```

Códigos de cifrado

Puede utilizar códigos de cifrado para especificar opciones de cifrado en el archivo **concsm.cfg**.

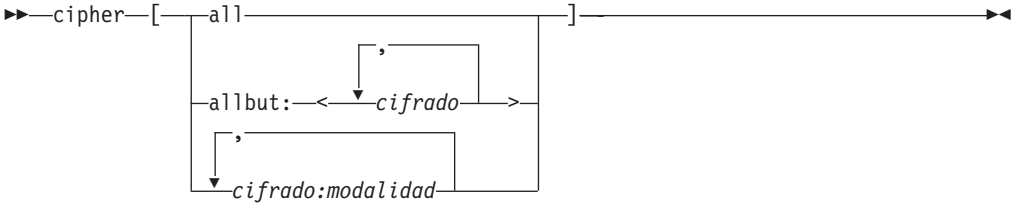
Hay tres códigos de cifrado:

- El código **cipher**
- El código **mac**
- El código **switch**

Código cipher:

El código cipher especifica los cifrados y las modalidades de cifrado que se deben utilizar para el cifrado.

El código **cipher** puede incluir las opciones de cifrado que se muestran en el siguiente diagrama de sintaxis.



Opción de cifrado	Descripción
all	Especifica que se deben incluir todos los cifrados y todas las modalidades disponibles, excepto la modalidad ECB. No hay ninguna lista de valores. Por ejemplo: `cipher[all],...`

allbut:<*lista de cifrados que se deben excluir***>**	Especifica que se deben incluir todos los cifrados a excepción de los de la lista.
	Para obtener más información, consulte el apartado "Tipos de cifrado y modalidades de cifrado" en la página 2-3.
	Por ejemplo:
	`cipher[allbut:<ecb,des>],...`
	`cipher[allbut:<cbc,bf>]`

cifrado:modalidad	Especifica uno o varios cifrados y modalidades. Por ejemplo: `cipher[des:cbc,des:ofb]`

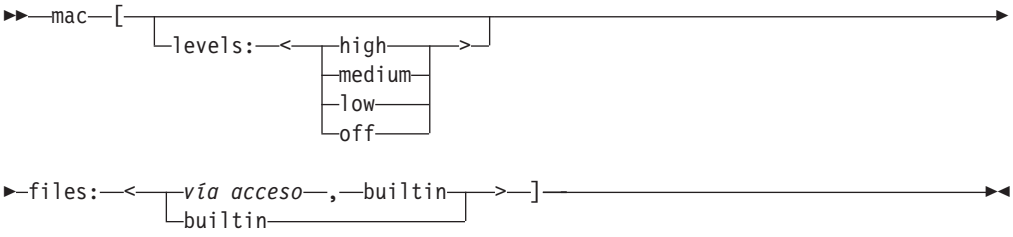
El valor predeterminado para el campo cipher es:
`cipher[allbut:<ecb>]`

Para obtener más información sobre los cifrados y las modalidades, consulte el apartado "Tipos de cifrado y modalidades de cifrado" en la página 2-3.

Código mac:

El código **mac** define los archivos de claves MAC y el nivel de generación de MAC que se debe utilizar durante la generación de MAC.

El código **mac** puede incluir las opciones de MAC que se muestran en el siguiente diagrama de sintaxis.



Opción de mac	Descripción
levels	Especifica una lista separada por comas de niveles de generación de MAC que la conexión soporta. Para obtener más información, consulte el apartado "Niveles de MAC" en la página 2-5.

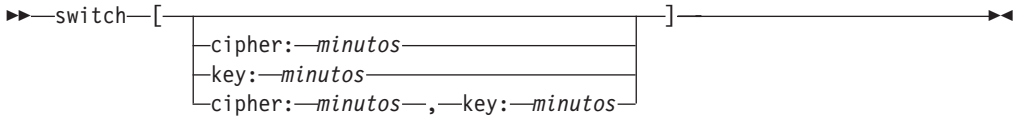
Opción de mac	Descripción

files	Especifica una lista separada por comas de los nombres de vía de acceso completos de los archivos de claves MAC.
	
	Para obtener más información, consulte el apartado "Archivos de claves MAC" en la página 2-4.
	
	Por ejemplo:
	`mac[levels:<high,low>,files:`
	`</usr/local/bin/mac1.dat,`
	`/usr/local/bin/mac2.dat,builtin>]`

Código switch:

El código **switch** define la frecuencia con que se renegocian los cifrados y/o las claves secretas.

El código **switch** puede incluir las opciones de conmutación que se muestran en el siguiente diagrama de sintaxis.



Opción de conmutación	Descripción
cipher:*minutos*	Especifica el tiempo en minutos entre cada renegociación del cifrado.
key:*minutos*	Especifica el tiempo en minutos entre cada renegociación de la clave secreta. Por ejemplo: `switch[cipher:120,key:20]`

Para obtener más información sobre la conmutación de cifrados y modalidades, consulte el apartado "Frecuencia de conmutación" en la página 2-5.

Ejemplos de uso de códigos de cifrado:

Los códigos de cifrado especifican valores para el cifrado de red.

Estos dos ejemplos ilustran posibles códigos del archivo **concsm.cfg** para definir el CSM de cifrado.

La serie de configuración siguiente indica que se deben utilizar todos los cifrados disponibles a excepción de los cifrados blowfish y que no se debe utilizar ningún cifrado en modalidad ECB:

```
ENCCSM("$INFORMIXDIR/lib/csm/iencs11a.so",
 "cipher[allbut:<ecb,bf>]")
```

La serie de configuración siguiente indica que se deben utilizar los cifrados de modalidad DES/CBC, modalidad EDE/OFB y modalidad DESX/CBC para esta

conexión y también para conmutar el cifrado que se esté utilizando cada 120 minutos y renegociar la clave secreta cada 15 minutos:

```
ENCCSM("/$INFORMIXDIR/lib/csm/iencs11a.so",
"cipher[des:cbc,ede:ofb,desx:cbc],switch[cipher:120,key:15]")
```

Cifrado de datos de red de Enterprise Replication y alta disponibilidad

Puede configurar el cifrado de datos de red para los clústeres de Enterprise Replication y de alta disponibilidad utilizando parámetros de configuración.

Puede utilizar parámetros de cifrado de Enterprise Replication y de alta disponibilidad para cifrar el tráfico de datos entre los servidores que participan en clústeres de Enterprise Replication y de alta disponibilidad (Duplicación de datos de alta disponibilidad, servidores secundarios autónomos remotos y servidores secundarios de disco compartido). El cifrado de alta disponibilidad funciona conjuntamente con el cifrado de Enterprise Replication y cada uno funciona tanto si el otro está habilitado como si no.

Los siguientes parámetros de configuración configuran el cifrado de clústeres de Enterprise Replication y de alta disponibilidad:

- ENCRYPT_CIPHERS: define todos los cifrados y modalidades que puede utilizar la sesión de base de datos actual
- ENCRYPT_MAC: controla el nivel de generación de código de autenticación de mensajes (MAC)
- ENCRYPT_MACFILE: especifica una lista de los nombres de vía de acceso completos de los archivos de claves MAC
- ENCRYPT_SWITCH: define la frecuencia con que se renegocian los cifrados o las claves secretas
- ENCRYPT_CDR: establece el nivel de cifrado para Enterprise Replication
- ENCRYPT_HDR: habilita o inhabilita el cifrado HDR
- ENCRYPT_SMX: establece el nivel de cifrado para los servidores autónomos remotos y de disco compartido

Cuando funcionan conjuntamente, la opción de alta disponibilidad y Enterprise Replication comparten los mismos parámetros de configuración ENCRYPT_CIPHERS, ENCRYPT_MAC, ENCRYPT_MACFILE y ENCRYPT_SWITCH.

Para dar soporte a conexiones de alta disponibilidad o Enterprise Replication cifradas conjuntamente con el cifrado de red del módulo de soporte de comunicaciones (CSM), se deben configurar dos puertos de red:

- Se debe configurar un puerto de red para la alta disponibilidad.
- Otro puerto de red se debe configurar para las conexiones CSM.

Importante: No se pueden iniciar las opciones de Enterprise Replication ni de alta disponibilidad en una conexión de red esté configurada para utilizar el cifrado CSM para las conexiones cliente/servidor.

Para obtener información sobre estos parámetros de configuración, consulte la publicación *IBM Informix Dynamic Server Administrator's Reference*.

Capítulo 3. Cifrado a nivel de columna

Puede utilizar el cifrado a nivel de columna para almacenar datos confidenciales en un formato cifrado. Después de cifrar los datos confidenciales, como los números de tarjetas de crédito, sólo los usuarios que puedan proporcionar una contraseña secreta podrán descifrar los datos.

Utilice las funciones de cifrado ENCRYPT_AES() y ENCRYPT_TDES() incorporadas para cifrar datos de columnas que contengan los siguientes tipos de datos de carácter o tipos de datos de objetos grandes inteligentes:

- CHAR
- NCHAR
- VARCHAR
- NVARCHAR
- LVARCHAR
- BLOB
- CLOB

También puede utilizar la sentencia SET ENCRYPTION PASSWORD para establecer una contraseña de cifrado para una sesión. Si lo hace, sólo los usuarios que puedan proporcionar una contraseña secreta podrán ver, copiar o modificar datos cifrados.

Las funciones de cifrado y descifrado ENCRYPT_AES(), ENCRYPT_TDES(), DECRYPT_CHAR() y DECRYPT_BINARY() incorporadas pueden utilizar la contraseña a nivel de sesión si la contraseña no se especifica explícitamente en la función de cifrado o descifrado. Si utiliza la sentencia SET ENCRYPTION PASSWORD, no es necesario que proporcione la misma contraseña en cada función de cifrado o descifrado.

Al establecer una contraseña de cifrado para una sesión, también puede especificar un indicador de contraseña. Si especifica un indicador, puede almacenar el indicador con la contraseña cifrada o en otra ubicación. La contraseña debe tener un mínimo de 6 bytes y puede tener un máximo de 128 bytes. La contraseña utilizada para el descifrado debe coincidir con la contraseña utilizada para el cifrado.

Al establecer contraseñas de cifrado para datos de columna, puede especificar los siguientes tipos de cifrado:

- **Cifrado a nivel de columna**. Todos los valores de una columna específica de una tabla de base de datos se cifran con la misma contraseña (palabra o frase), el mismo algoritmo de cifrado y la misma modalidad de cifrado. Para el cifrado a nivel de columna, puede almacenar el indicador fuera de la columna cifrada en lugar de repetirlo en cada fila.

  Consejo: Si no se utilizan funciones de cifrado, los usuarios finales pueden entrar datos sin cifrar en columnas destinadas a contener datos cifrados. Para garantizar que los datos entrados en un campo siempre se cifren, utilice vistas y desencadenantes INSTEAD OF.
- **Cifrado a nivel de celda** (también denominado *Fila-Columna* y *Cifrado a nivel de columna establecida*). Dentro de una columna de datos cifrados, se utilizan una

gran cantidad de contraseñas, algoritmos de cifrados o modalidades diferentes. Este tipo de cifrado puede resultar necesario para proteger los datos personales.

Las contraseñas y los indicadores que declare con SET ENCRYPTION PASSWORD como textos en formato en cualquier tabla del catálogo del sistema. Para impedir que otros usuarios accedan al texto sin formato de los datos cifrados o de una contraseña, debe evitar las acciones que puedan poner en riesgo el secreto de una contraseña:

- A menos que la base de datos sólo resulte accesible mediante una red segura, el módulo de soporte de comunicaciones de cifrado (ENCCSM) para proteger la transmisión de datos entre el servidor de bases de datos y cualquier sistema cliente.
- No indexe las columnas cifradas y no cree un índice funcional sobre una columna descifrada. De hacerlo, se almacenarían los datos del texto sin formato en la base de datos, frustrando de este modo el objetivo del cifrado.
- No almacene contraseñas en un desencadenante ni en una rutina definida por el usuario (UDR) que exponga la contraseña al público. Utilice la contraseña de la sesión antes de activar el desencadenante, invocar la UDR o pasar cualquier contraseña como parámetro a una UDR.

Cuando se establece una contraseña, Dynamic Server transfiera la contraseña y cualquier indicador a una clave de 128 bits que se utiliza para descifrar la contraseña y el indicador. Las contraseñas y los indicadores no se almacenan como texto no cifrado. La clave es un valor aleatorio basado en el tiempo por instancia. El servidor de bases de datos inicia la clave cuando se inicia el servidor; la clave se destruye cuando el servidor de bases de datos se cierra.

Aunque es posible almacenar tanto datos cifrados como sin cifrar en una sola columna, la aplicación debe determinar qué filas contienen datos cifrados y qué filas contienen datos sin cifrar. Además, la aplicación debe estipular el uso del código correcto para manejar la diferencia, porque las funciones de descifrado incorporadas fallan si se aplican a datos sin cifrar. El modo más simple de evitar este error es que todas las filas usan el cifrado en una columna en la que cualquier fila esté cifrada. Para obtener más información, consulte la publicación *IBM Informix Guide to SQL: Syntax*.

Una consulta de datos cifrados debe especificar una columna sin cifrar en la que se deben seleccionar las filas. Para obtener información sobre las consultas, la sintaxis y la reutilización de datos cifrados, consulte la publicación *IBM Informix Guide to SQL: Syntax*.

Un valor cifrado utiliza más espacio de almacenamiento en una columna que el correspondiente valor de texto sin formato. Esto sucede porque toda la información necesaria para descifrar el valor, la clave de cifrado, se almacena con el valor. Por lo tanto, no se recomienda incluir cero bytes en el resultado cifrado.

Dynamic Server incluye un procesador virtual de cifrado. Si la opción `encrypt` del parámetro VPCLASS no está definida en el archivo de configuración ONCONFIG, el servidor de bases de datos iniciará un procesador virtual de cifrado la primera vez que se llame a cualquier función de cifrado o descifrado definida para el cifrado a nivel de columna. Puede definir varios procesadores virtuales de cifrado si es necesario para disminuir el tiempo necesario para iniciar el servidor de bases de datos. Para obtener más información, consulte el capítulo sobre los parámetros de configuración de la publicación *IBM Informix Dynamic Server Administrator's Reference*.

Cuando el servidor de bases de datos está en modalidad en línea, se pueden utilizar el mandato **onmode -p** para añadir o eliminar procesadores virtuales de cifrado. Por ejemplo, para añadir cuatro procesadores virtuales de cifrado más, utilice:

```
onmode -p 4 encrypt
```

Para eliminar tres procesadores virtuales de cifrado, utilice:

```
onmode -p -3 encrypt
```

Para obtener más información sobre, consulte el capítulo sobre el programa de utilidad **onmode** de la publicación *IBM Informix Dynamic Server Administrator's Reference*.

Cifrados de datos de columnas

Puede almacenar datos confidenciales en formato cifrado.

Antes de establecer la contraseña de cifrado y los datos que se deben cifrar, debe asegurarse de que los datos cifrados puedan caber en la columna.

Para cifrar una columna:

1. Calcule el tamaño de la columna cifrada. Si es necesario, modifique la columna. Para obtener ejemplos de los dos métodos para calcular el tamaño de una columna cifrada, consulte el apartado "Ejemplo que muestra cómo determinar el tamaño de una columna cifrada".
2. Inserte información de la contraseña de cifrado en el código. Utilice la sentencia de SQL SET ENCRYPTION PASSWORD para especificar o una contraseña y un indicador. Utilice la función ENCRYPT_AES() o ENCRYPT_TDES() para definir datos cifrados. Para obtener un ejemplo de cómo insertar una contraseña en el código y utilizar la función ENCRYPT, consulte el apartado "Ejemplo que muestra cómo cifrar una columna" en la página 3-4.

Utilice las funciones DECRYPT_BINARY() y DECRYPT_CHAR() para consultar los datos cifrados. Para obtener un ejemplo de cómo consultar datos cifrados, consulte el apartado "Ejemplo que muestra cómo consultar datos cifrados" en la página 3-5.

Consulte la publicación *IBM Informix Guide to SQL: Syntax* para obtener más información sobre:

- La sentencia SET ENCRYPTION PASSWORD y la sintaxis que se debe utilizar para especificar la contraseña y el indicador.
- Las funciones ENCRYPT y DECRYPT

Ejemplo que muestra cómo determinar el tamaño de una columna cifrada

El tamaño de la columna debe ser suficientemente grande para almacenar los datos cifrados.

El ejemplo siguiente muestra cómo se calcula el tamaño de una columna **Tarjeta crédito**:

```
DATA SIZE  16 bytes
    ENCRYPTED DATA SIZE = (DATA SIZE + blocksize8) / blocksize8 *
blocksize8 = 24 bytes (operación de entero)
    OR ENCRYPTED DATA SIZE = (DATA SIZE - DATA SIZE% blocksize8 +
blocksize8 ) = 24 bytes
```

```
    (Para ENCRYPT_TDES, redondear al alza hasta (N + 1) * 8 bytes, por ejemplo
13 bytes se redondean a 16 bytes y 16 bytes a 24 bytes)
    HEADER SIZE = 11 bytes (para codificación Base64)
    IV SIZE = 8 bytes (tamaño fijo)
    HINT SIZE = 32 bytes (tamaño máximo)
    ENCRYPED HINT SIZE = 40 bytes (tamaño máximo)

BASE64 SIZE = ((INPUT DATA SIZE + 2) / 3) * 4
(operación de entero)
    OR BASE64 SIZE = ((INPUT DATA SIZE + 2) -
(INPUT DATA SIZE + 2) % 3) / 3 * 4

    TOTAL SIZE = HEADER SIZE
    + BASE64(IV SIZE + ENCRYPTED DATA SIZE + ENCRYPTED HINT)
                          = 11 + BASE64(8 + 24 + 40)
                = 11 + (72 + 2) / 3 * 4
                = 11 + 96 = 107
```

En el ejemplo anterior, el vector de inicialización (IV) es una serie de bytes pseudoaleatoria que se utiliza para iniciar el cifrado al utilizar algunas modalidades de cifrado. El tamaño de IV es el número de series aleatorias de bytes; para Dynamic Server, es de 8 bytes.

Si el indicador no se almacena en la columna, el tamaño total en el ejemplo anterior será de 55 bytes.

Otro modo de determinar el tamaño de la columna cifrada es calculándolo del modo siguiente:

```
SELECT LENGTH(ENCRYPT_TDES
("1234567890123456",
         "password", "long....hint"))
FROM "informix".systables WHERE tabid = 1
```

Sin el indicador, puede calcularlo del modo siguiente:

```
SELECT LENGTH(ENCRYPT_TDES("1234567890123456",
"password", ""))
FROM "informix".systables
WHERE tabid = 1
```

Importante: Si el tamaño de la columna es inferior al tamaño de los datos devueltos de las funciones ENCRYPT y DECRYPT, los datos cifrados se truncarán cuando se inserten y no será posible descifrar los datos (porque la cabecera indicará que la longitud debe ser superior a la de los datos recibidos).

Ejemplo que muestra cómo cifrar una columna

Puede utilizar la sentencia SET ENCRYPTION PASSWORD para restringir el acceso a los datos de una columna.

El ejemplo siguiente muestra cómo utilizar la contraseña de cifrado en una columna que contiene un número de la seguridad social:

```
create table emp
(    name char(40),
    salary money,
    ssn lvarchar(67)
    );
        set encryption password "one two three 123";
        insert into emp values ("Alice", 50000, encrypt_aes
('123-456-7890'));
```

```
        insert into emp values ("Bob", 65000, encrypt_aes
('213-656-0890'));
        select name, salary, decrypt_char(ssn, "one two three 123")
 from emp where name = 'Bob';
```

Ejemplo que muestra cómo consultar datos cifrados

Puede consultar datos cifrados con la función DECRYPT de la sentencia SET ENCRYPTION PASSWORD.

El ejemplo siguiente muestra cómo utilizar la función de descifrar para consultar datos cifrados:

```
select name, decrypt_char(ssn, "one two three 123") from emp;
        o bien
set encryption password "one two three 123";
select name, salary, decrypt_char(ssn) from emp where name = 'Bob';
```

Capítulo 4. Seguridad de la conexión

Puede impedir las conexiones no autorizadas a su servidor de bases de datos, mantener la seguridad de las contraseñas, proporcionar conexiones seguras para los clústeres de Enterprise Replication y de alta disponibilidad, mantener la seguridad de las conexiones locales y limitar los ataques de denegación de servicio. La mayoría de estas soluciones se pueden utilizar conjuntamente.

Puede configurar la autenticación de la conexión utilizando módulos de autenticación. Según la plataforma, puede utilizar uno de los módulos de autenticación siguientes:

- Pluggable Authentication Module (PAM) para sistemas Dynamic Server que se ejecuten en UNIX o en Linux. Estos módulos permiten implementar distintos módulos de autenticación para distintas aplicaciones. Consulte el apartado "Pluggable Authentication Modules para sistemas que se ejecuten en UNIX o Linux".
- Soporte de autenticación Lightweight Directory Access Protocol (LDAP) para Windows. Utilice el módulo de soporte de autenticación LDAP cuando desee utilizar un servidor LDAP para autenticar a los usuarios. Consulte el apartado "Soporte de autenticación LDAP en Windows" en la página 4-3.

Puede garantizar que las contraseñas de autenticación de la conexión sean seguras cifrándolas utilizando un módulo de soporte de comunicaciones. El CSM de contraseña simple (SPWDCSM) proporciona el cifrado de contraseñas. SPWDCSM está disponible en todas las plataformas. Consulte el apartado "Cifrado de contraseñas" en la página 4-9.

Las conexiones de Enterprise Replication y alta disponibilidad no pueden utilizar módulos de autenticación. En su lugar, se pueden proporcionar conexiones seguras limitando puertos específicos para que sólo tengan conexiones de Enterprise Replication o alta disponibilidad. Consulte el apartado "Seguridad de la conexión de Enterprise Replication y alta disponibilidad" en la página 4-12.

Puede configurar IDS para comprobar si el ID del usuario que está ejecutando el programa coincide con el ID del usuario que está intentando conectarse a la base de datos. Consulte el apartado "Conexiones locales seguras a un sistema principal" en la página 4-13.

Puede limitar las posibilidades de ataques de denegación de servicio para evitar que se bloqueen conexiones legítimas al servidor de bases de datos. Consulte el apartado "Limitación de los ataques de desbordamiento por denegación de servicio" en la página 4-14.

Pluggable Authentication Modules para sistemas que se ejecuten en UNIX o Linux

Un Pluggable Authentication Module (PAM) es una infraestructura bien definida para dar soporte a diferentes módulos de autenticación desarrollados originalmente por Sun Microsystems. PAM está soportado tanto en la modalidad de 32 bits como en la de 64 bits en Solaris, Linux, HP-UX y AIX.

PAM permite a los administradores de sistemas implementar distintos mecanismos de autenticación para distintas aplicaciones. Por ejemplo, las necesidades de un sistema como el programa de inicio de sesión de UNIX pueden ser distintas a las de una aplicación que acceda a información confidencial de una base de datos. PAM sirve para muchos escenarios en una sola máquina, ya que los servicios de autenticación se adjuntan a nivel de aplicación.

Además de habilitar una aplicación para seleccionar la autenticación del modo necesario, PAM permite apilar módulos. Se pueden apilar muchos módulos uno tras otro, permitiendo de este modo que la aplicación se autentique de diversos modos antes de otorgar acceso. PAM proporciona un conjunto de API para dar soporte a la autenticación, la gestión de cuentas, la gestión de sesiones y la gestión de contraseñas.

El administrador del sistema puede habilitar o inhabilitar el uso de PAM. De modo predeterminado, el servidor de bases de datos utiliza el mecanismo de autenticación tradicional de Informix (que se basa en el mecanismo BSD rhosts) para evitar forzar cambios importantes de los usuarios.

Para utilizar PAM con Dynamic Server:

- El servidor de bases de datos Informix debe estar en una plataforma de sistema operativo que soporte PAM.
- Las aplicaciones cliente deben estar escritas utilizando una versión suficientemente reciente de Client SDK.
- Debe tener el servicio PAM adecuado configurado en el sistema operativo.
- Debe saber si el servicio PAM simplemente aceptará la contraseña proporcionada o si utilizará un protocolo de desafío-respuesta (por ejemplo, un servidor de autenticación RADIUS).
- Si el servicio PAM va a utilizar un protocolo de desafío-respuesta, deberá modificar las aplicaciones para que puedan manejar el desafío y la respuesta. La aplicación debe saber que es posible que el módulo PAM emita diversos desafíos.
- Debe asegurarse de que los clústeres de Enterprise Replication y de alta disponibilidad no se vean afectados por la autenticación PAM.
- Debe modificar la entrada del servidor en el archivo sqlhosts tanto para la aplicación cliente como para el servidor de bases de datos (si están en distintas máquinas o en distintas ubicaciones de una sola máquina).

Nombre del servicio PAM

El nombre del servicio PAM identifica el módulo PAM.

Este módulo PAM se encuentra normalmente en el directorio **/usr/lib/security** y sus parámetros se listan en el archivo **/etc/pam.conf**.

En Linux, el archivo **/etc/pam.conf** se puede sustituir por un directorio denominado **/etc/pam.d**, donde hay un archivo para cada servicio PAM. Si **/etc/pam.d** existe, Linux pasará por alto **/etc/pam.conf**. Consulte la documentación del sistema para obtener información detallada sobre este archivo de configuración.

Modalidad de autenticación con el módulo PAM

El módulo PAM determina si una simple contraseña resulta suficiente o si se necesitan otros desafíos.

La implementación de PAM en Dynamic Server aprovecha el hecho de que, para las conexiones explícitas, el cliente envía una contraseña al servidor. Esta contraseña se puede utilizar para satisfacer los requisitos de PAM en los casos en los que se utiliza una simple contraseña. Si la modalidad de autenticación implica la respuesta a desafíos, las aplicaciones deben estar preparadas para responder a ellos. La aplicación debe saber que es posible que el módulo PAM emita diversos desafíos.

Tamaño de pila necesario de PAM

Puede personalizar el tamaño de pila disponible para los módulos PAM.

La característica PAM carga módulos (bibliotecas compartidas) PAM del sistema operativo o de terceros en la hebra de usuario **informix**. Los requisitos de tamaño de pila de estos módulos PAM no se pueden predecir. Por ejemplo, en Linux algunos módulos necesitan más de 128K de espacio de pila. Utilice el parámetro de configuración PAM_STACKSIZE para personalizar el tamaño de pila para los módulos PAM.

Por ejemplo, establezca PAM_STACKSIZE en el archivo ONCONFIG tal como se indica a continuación:

```
PAM_STACKSIZE 64 # Tamaño de pila necesario para los módulos PAM
(K Bytes)
```

En UNIX, el valor predeterminado de PAM_STACKSIZE es de 32 KB.

En Linux, el valor predeterminado es de 128 KB más el valor del parámetro de configuración STACKSIZE.

Configuración de un servidor de bases de datos para utilizar PAM

Para configurar un servidor para que utilice PAM, el administrador del sistema debe saber lo siguiente:

- El nombre del módulo PAM.
- Si el módulo emitirá PAM un desafío además de aceptar una combinación de usuario y contraseña simple.

El ejemplo siguiente muestra una entrada de sqlhosts con nombres ilustrativos:

```
Authentication mode: challenge
ifxserver2   oltlitcp   servermc   portnum2 opciones
 where options are "s=4, pam_serv=(pam_pass), pamauth=(challenge)"

PAM service: pam_password (Sólo necesita una contraseña)

Authentication mode: password
ifxserver2   oltlitcp   servermc   portnum2 opciones
 where options are "s=4, pam_serv=(pam_pass), pamauth=(password)"
```

Soporte de autenticación LDAP en Windows

La autenticación LDAP en Windows se configura como Pluggable Authentication Module (PAM), que se utiliza en UNIX y en Linux. Utilice el módulo de soporte de autenticación LDAP cuando desee utilizar un servidor LDAP para autenticar a los usuarios del sistema. El módulo contiene código fuente que puede modificar para su módulo de soporte de autenticación LDAP.

El módulo de autenticación es una DLL que normalmente se encuentra en el directorio %**INFORMIXDIR%\dbssodir\lib\security**. Los parámetros del módulo se listan en el archivo **%INFORMIXDIR%\dbssodir\pam.conf**. En el directorio **%INFORMIXDIR%\demo\authentication** se incluye el código fuente de un módulo de autenticación LDAP completamente funcional y ejemplos de los archivos de configuración necesarios.

El módulo de autenticación LDAP sólo proporciona autenticación de un solo módulo. El módulo no soporta características como el apilado de módulos. El administrador del sistema puede habilitar o inhabilitar la autenticación.

Instalación y configuración del módulo de soporte de autenticación LDAP

Para poder utilizar el módulo de autenticación LDAP de Dynamic Server para crear su módulo de autenticación, debe disponer de un servidor LDAP y del sistema cliente LDAP. Algunos ejemplos de sistemas LDAP son IBM Directory Server y openLDAP.

El sistema cliente LDAP incluye normalmente bibliotecas y archivos de cabecera de LDAP. Estas bibliotecas y estos archivos de cabecera son necesarios para compilar el módulo LDAP.

Para personalizar el módulo de soporte de autenticación LDAP:

1. Personalice el archivo **pam_ldap.c** que se incluye con Dynamic Server.
2. Compile el archivo **pam_ldap.c** en una DLL y colóquela en un directorio seguro.

   Consejo: Coloque el archivo **pam_ldap.c** en el directorio **%INFORMIXDIR%\dbssodir\lib**.

La instalación también incluye una plantilla de un archivo de configuración, **pam_ldap_tmpl**, para el módulo LDAP. Este archivo de configuración contiene información específica del sitio. Debe almacenar la información específica del sitio en este archivo de configuración, porque el archivo permite a un solo módulo LDAP trabajar en distintos valores.

Configuración del módulo LDAP

Utilice la plantilla de un archivo de configuración PAM para configurar el módulo LDAP.

Para configurar el módulo LDAP:

1. Copie el archivo de plantilla en **%INFORMIXDIR%\dbssodir\etc** y asígnele como nombre **pam.conf**.
2. Personalice el archivo de modo que se adapte a sus valores de seguridad locales. Para obtener información detallada sobre cómo configurar el archivo de plantilla, **pam.conf_tmpl**, vea el archivo.

Configuración de Dynamic Server para LDAP

Para configurar un servidor para que utilice un módulo de soporte de autenticación LDAP, edite el archivo **sqlhosts**. El administrador del sistema debe saber:

- El nombre del módulo.
- Si el módulo emitirá un desafío además de aceptar una combinación de usuario y contraseña simple.

El ejemplo siguiente muestra una entrada de **sqlhosts** con nombres descriptivos:

```
PAM service: pam_chal

Authentication mode: challenge
ifxserver1   oltlitcp   servermc   portnum1
 s=4, pam_serv=(pam_chal), pamauth=(challenge)

PAM service: pam_password (Sólo necesita una contraseña)

Authentication mode: password
ifxserver2   oltlitcp   servermc   portnum2
 s=4, pam_serv=(pam_pass), pamauth=(password)
```

Modalidad de autenticación con el módulo LDAP

El módulo de soporte de autenticación LDAP determina si una simple contraseña resulta suficiente o si se necesitan otros desafíos. La implementación del módulo en Dynamic Server aprovecha el hecho de que, para las conexiones explícitas, el cliente envía una contraseña al servidor. Esta contraseña se puede utilizar para satisfacer las necesidades del módulo de soporte de autenticación LDAP en los casos en los que se utiliza una simple contraseña. Si la modalidad de autenticación implica la respuesta a desafíos únicos o desafíos múltiples, las aplicaciones deben ser capaces de responder a los desafíos.

Despliegue del módulo de autenticación

Cuando utilice módulos de autenticación, tenga en cuenta las siguientes cuestiones:

- "Conexiones implícitas con módulos de autenticación"
- "Desarrollo de aplicaciones para módulos de autenticación"
- "Transacciones distribuidas y módulos de autenticación" en la página 4-7
- "API de cliente y módulos de soporte de autenticación" en la página 4-8
- "Cuestiones de compatibilidad con los módulos de autenticación" en la página 4-9

Conexiones implícitas con módulos de autenticación

Las respuestas de autenticación a los módulos de autenticación, como PAM y LDAP, esperan una respuesta. No obstante, en las conexiones implícitas al servidor de bases de datos no hay contraseña.

PAM y LDAP son sistemas orientados al desafío en los que la respuesta de autenticación (la contraseña) se proporciona en respuesta a un mensaje del módulo de autenticación. Las conexiones implícitas sólo pueden funcionar en PAM y LDAP en modalidad de desafío. Las conexiones implícitas en modalidad de contraseña resultarán anómalas.

Desarrollo de aplicaciones para módulos de autenticación

El método autenticación depende del módulo de soporte de autenticación PAM o LDAP instalado.

El método de autenticación puede puede implicar un desafío y una respuesta. Cuando el módulo de soporte de autenticación PAM o LDAP emite un desafío, se producen los procesos siguientes:

1. El servidor de bases de datos reenvía el desafío al cliente.
2. La aplicación debe responder al desafío utilizando una función de devolución de llamada proporcionada por el controlador CSDK de IBM Informix o JDBC de IBM Informix.
3. Si el servidor al que se está conectando el cliente está configurado para el desafío, la aplicación deberá registrar una función de devolución de llamada con CSDK o JDBC.
4. Cuando CSDK o JDBC reciben un desafío del servidor, la función de devolución de llamada reenvía el desafío a la aplicación.
5. La aplicación debe responder al desafío.
6. CSDK o JDBC reenvía la respuesta al servidor de bases de datos.

La aplicación debe estar preparada para responder a varios desafíos y no puede asumir el número de desafíos o los propios desafíos.

La función de devolución de llamada debe ser similar a la siguiente función:

```
mint ifx_pam_callback(mint (*callbackfunc_ptr)(char *challenge,
 char *response, mint msg_style))
```

char ******challenge*
: el almacenamiento intermedio de caracteres en el que el servidor proporciona el desafío. Su tamaño está fijado en 512, definido por PAM_MAX_MSG_SIZE en el archivo **pam_appl.h**.

char ******response*
: el almacenamiento intermedio de caracteres en el que el usuario proporciona la respuesta. Su tamaño está fijado en 512, definido por PAM_MAX_RESP_SIZE en el archivo **pam_appl.h**.

int *msg_style*
: contiene un número que indica el tipo de mensaje proporcionado por el servidor. Según el tipo de respuesta, la aplicación puede realizar la acción adecuada en la función de devolución de llamada.

La aplicación cliente debe registrar la función de devolución de llamada antes de realizar la primera conexión. Si la función de devolución de llamada no se registra cuando se realiza la primera conexión con el servidor de bases de datos y el servidor responde, ESQL/C devuelve el error -1809.

El ejemplo siguiente muestra un programa muy simple que primero registra una función de devolución de llamada y, a continuación, anula su registro.

```
#include <stdio.h>
#include <security/pam_appl.h>

static int user_callback(char *challenge, char *response,
 int msg_style);

int main(void)
{
    EXEC SQL char passwd[]="password";
    int retval = 0;

    /* primero registre la devolución de llamada */
    retval = ifx_pam_callback(user_callback);
```

```
    if (retval == -1)
    {
        printf("Error al registrar la devolución de llamada\n");
        return (-1);
    }
    else
    {
        EXEC SQL database test; /* conexión satisfactoria */
        /* Tenga en cuenta que esta es una conexión implícita. Por lo tanto,
         * la aplicación debe estar lista para responder a desafíos.*/
        printf ("sqlcode al conectar con pam = %d\n", SQLCODE);
    }

    retval = ifx_pam_callback(NULL); /* anular el registro de la función
                                      * de devolución de llamada */

    if (retval == -1)
    {
        printf("Error al registrar la devolución de llamada\n");
        return (-1);
    }
    else
    {
    /* Esta conexión ha emitido el error -1809, ya que se ha anulado el
    * registro de la función de devolución de llamada con la sentencia */
         EXEC SQL database test;
        printf ("sqlcode al conectar = %d\n", SQLCODE);
    }
    return 0;
}


static int user_callback(char *challenge, char *response,
 int msg_style)
{
    switch (msg_style)
    {
        /* Si msg_style es PAM_PROMPT_ECHO_OFF, la aplicación
         * no debe repetir la respuesta del usuario. */
        case PAM_PROMPT_ECHO_OFF:
        case PAM_PROMPT_ECHO_ON :
                printf("%s: %d:", challenge, msg_style);
                scanf("%.*s", PAM_MAX_RESP_SIZE, response);
                break;

        case PAM_ERROR_MSG:
        case PAM_TEXT_INFO:
        default:
                printf("%s: %d\n", challenge, msg_style);
               break;
    }
    return 0;
}
```

Transacciones distribuidas y módulos de autenticación

Las conexiones distribuidas no pueden responder a los desafíos, porque no se puede predecir cuándo se puede realizar una conexión distribuida. La autenticación en los servidores remotos se debe realizar dentro de la base de datos.

Puede utilizar **sysuser** para administrar conexiones remotas.

Si PAM o un módulo de soporte de autenticación LDAP están habilitados en los servidores remotos, el administrador del sistema deberá entrar usuarios autorizados en la tabla **sysauth** de la base de datos **sysuser** para cada servidor remoto:

Base de datos: **sysuser**

Tabla: **sysauth**

La tabla **sysauth** de la base de datos **sysuser** tiene el siguiente esquema:

Columna	Tipo
username	CHAR(32)
groupname	CHAR(32)
servers	CHAR(128)
hosts	CHAR(128)

La tabla puede contener varias filas para un solo usuario para que se autentique para varios servidores y sistemas principales.

El ejemplo siguiente habilita el servidor para aceptar transacciones distribuidas del usuario **user1**, perteneciente al grupo **group1**, del servidor de bases de datos **server1** y del sistema principal **host1.mycompany.com**:

```
insert into sysauth values ("user1", "group1", "server1",
 "host1.mycompany.com");
```

API de cliente y módulos de soporte de autenticación

Sólo API de cliente específicas de IBM Informix soportan los módulos de soporte de autenticación PAM y LDAP. Para utilizar las demás API cuando haya un módulo de autenticación habilitado en Dynamic Server, puede conectarse a DBSERVERALIAS.

Las siguientes API de cliente de IBM Informix soportan los módulos de soporte de autenticación PAM y LDAP:

- ESQL/C
- ODBC
- JDBC

Las demás API no soportan los módulos de soporte de autenticación PAM y LDAP. Para utilizarlas sobre una versión de Dynamic Server que tenga un módulo de autenticación habilitado, conéctese a un DBSERVERALIAS que no tenga parámetros de PAM en el archivo **sqlhosts**.

Las API de cliente, las herramientas y las aplicaciones siguientes no soportan los módulos de soporte de autenticación PAM ni LDAP:

- LibC++
- API de Client DataBlade
- Bases de datos OLE
- Aplicaciones Visual Basic mediante ODBC
- Prueba de conexión Ilogin y ODBC
- Informix Server Administrator

Para obtener más información sobre ESQL/C, ODBC y JDBC, consulte la publicación *IBM Informix ESQL/C Programmer's Manual*, la publicación *IBM Informix ODBC Driver Programmer's Manual* y la publicación *IBM Informix JDBC Driver Guía del programador*.

Cuestiones de compatibilidad con los módulos de autenticación

Sólo productos IBM Informix específicos soportan los módulos de autenticación. Para utilizar los demás productos cuando haya un módulo de autenticación habilitado en Dynamic Server, puede conectarse a DBSERVERALIAS.

No todos los productos y herramientas IBM Informix soportan la autenticación PAM o LDAP:

- IBM Informix-4GL no soporta directamente la autenticación PAM o LDAP porque no dispone de ningún mecanismo para identificar las funciones de devolución de llamada. No obstante, si IBM Informix-4GL utiliza la versión correcta de CSDK, puede escribir código C al que se puede llamar desde IBM Informix-4GL para manejar el protocolo de desafío y respuesta. Para implementar PAM, migre a la nueva versión de CSDK, modifique sus aplicaciones para registrar una devolución de llamada que pueda manejar desafíos y respuestas y vuelva a compilar la aplicación.
- Los productos como Informix SQL no manejarán el protocolo de desafío y respuesta.
- Los programas de utilidad DB-Access, **dbexport**, **dbimport**, **dbload** y **dbschema** soportan PAM. Si reciben un desafío, pasan el desafío al usuario y esperan una respuesta. Esta operación se repite para cada desafío que el módulo PAM emite.
- Los programas de utilidad de administración del servidor **onmode**, **onstat** y **oncheck** no utilizan PAM. No obstante, puesto que todos estos programas de utilidad funcionan en puertos de Dynamic Server, los programas de utilidad pueden funcionar con un puerto habilitado para PAM.
- Otros programas de utilidad del servidor no soportan PAM.

Si utiliza cualquier herramienta que no soporte los módulos de autenticación PAM o LDAP, realice conexiones a un DBSERVERALIAS que no tenga los parámetros de PAM en el archivo SQLHOSTS.

Cifrado de contraseñas

Puede utilizar módulos de soporte de comunicaciones (CSM) para habilitar el cifrado de contraseñas.

El CSM de contraseña simple (SPWDCSM) proporciona el cifrado de contraseñas.

Este cifrado protege una contraseña cuando se debe enviar entre el cliente y el servidor de bases de datos para la autenticación. SPWDCSM está disponible en todas las plataformas.

No se puede utilizar el cifrado de contraseñas con CSM de cifrado (ENCCSM). Por ejemplo, si utiliza SPWDCSM y decide cifrar los datos de la red, deberá eliminar las entradas correspondientes a SPWDCSM en los archivos **concsm.cfg** y **sqlhosts**.

No se puede utilizar CSM de contraseña simple sobre una conexión multiplexada.

Archivo de configuración CSM

Si utiliza un módulo de soporte de comunicaciones (CSM), debe tener un archivo **concsm.cfg**.

Una entrada en el archivo **concsm.cfg** es una sola línea y está limitada a 1024 caracteres. Después de describir el CSM en el archivo **concsm.cfg**, puede habilitarlo en el parámetro de opciones del archivo **sqlhosts**, tal como se describe en la publicación *IBM Informix Dynamic Server Administrator's Guide*.

El archivo **concsm.cfg** reside en el directorio **$INFORMIXDIR/etc** de modo predeterminado. El directorio predeterminado del archivo **concsm.cfg** es **INFORMIXDIR/etc**. Si desea almacenar el archivo en otra ubicación, puede alterar temporalmente la ubicación predeterminada estableciendo como valor de la variable de entorno **INFORMIXCONCSMCFG** el nombre de la vía de acceso completa de la nueva ubicación. Para obtener información sobre cómo establecer la variable de entorno **INFORMIXCONCSMCFG**, consulte la publicación *IBM Informix Guide to SQL: Reference*.

Las entradas del archivo **concsm.cfg** deben ajustarse a las restricciones siguientes:

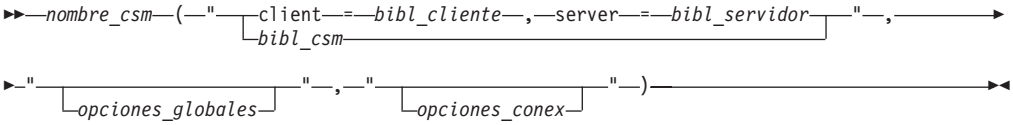
- Los caracteres siguientes no se permiten como parte de los nombres de las vías de acceso de bibliotecas:
  - = (signo igual)
  - ″ (comilla doble)
  - , (coma)
- No se pueden utilizar espacios en blanco a menos que éstos formen parte de un nombre de vía de acceso.

Configuración del cifrado de contraseñas

Para el cifrado de contraseñas, debe especificar bibliotecas de cifrado de contraseñas y opciones de conexión.

Sintaxis

Para configurar el cifrado de contraseñas, utilice la sintaxis siguiente para añadir una línea al archivo **concsm.cfg**.



Opción	Descripción
client=*bibl_cliente*	Especifica la vía de acceso completa y el nombre de la biblioteca compartida que es el CSM en el sistema cliente. Los sistemas cliente utilizan este CSM para comunicarse con el servidor de bases de datos. La biblioteca que Dynamic Server proporciona es **$INFORMIXDIR\lib\client\csm\libixspw.so**

Opción	Descripción
opciones_conex	La opción *opciones_conex* tiene las siguientes opciones: **Valor** **Resultado** **p=1** La contraseña es obligatoria para la autenticación. **p=0** La contraseña no es obligatoria. Si el cliente la proporciona, la contraseña se cifra y se utiliza para la autenticación. Si se pone una opción desconocida en *opciones_conex*, se producirá un error de inicialización del contexto. Puede poner un valor nulo en el campo *opciones_conex*, por ejemplo: `""`. Para una versión de CSDK anterior a la 2.3, si el campo *opciones_conex* es nulo, el comportamiento predeterminado será `p=1`. Para CSDK versión 2.3 y posteriores, si el campo *opciones_conex* es nulo, el comportamiento predeterminado es `p=0`.
bibl_csm	Es la vía de acceso completa y el nombre de la biblioteca compartida que es el CSM si el servidor de bases de datos y el sistema cliente comparten el CSM. La biblioteca que Dynamic Server proporciona es **$INFORMIXDIR\lib\csm\libixspw.so**.
nombre_csm	Es el nombre que asigne al módulo de soporte de comunicaciones. Por ejemplo, un nombre podría ser SPWDCSM.
opciones_globales	Esta opción no se utiliza actualmente.
server=*bibl_servidor*	Especifica la vía de acceso completa y el nombre de la biblioteca compartida que es el CSM en el servidor de bases de datos. La biblioteca proporcionada por Dynamic Server se instala normalmente en los directorios siguientes: • UNIX: **$INFORMIXDIR/lib/csm/libixspw.so** • Windows: **%INFORMIXDIR%/bin/libixspw.so**

Tablas SMI y valor de concsm.cfg

Si desea crear las tablas SMI al iniciar el servidor de bases de datos (**oninit -i**), no especifique la opción **p=1** en la entrada de CSM del servidor de bases de datos en el archivo **concsm.cfg**. El proceso **oninit** no tiene ninguna contraseña para el ID de usuario **informix** o **root**. Si especifica la opción **p=1** en el archivo **concsm.cfg** para el servidor de bases de datos, recibirá el siguiente mensaje de error:

```
-5013 CSM: cannot obtain credential:
authentication error.
```

Para especificar que la contraseña es obligatoria para el CSM del servidor de bases de datos cuando las tablas de SMI aún no se hayan creado:

1. No especifique la opción **p=1** en la entrada **concsm.cfg**.
2. Inicie el servidor de bases de datos con el mandato **oninit -i** para crear las tablas de SMI.

3. Detenga el servidor de bases de datos.
4. Especifique la opción **p=1** en la entrada de CSM del servidor de bases de datos en el archivo **concsm.cfg**.
5. Vuelva a iniciar el servidor de bases de datos con el mandato **oninit**.

Entradas de concsm.cfg de ejemplo para el cifrado de contraseñas

Debe especificar parámetros y campos en el archivo **concsm.cfg** para el cifrado de contraseñas.

Los dos ejemplos siguientes ilustran las dos alternativas para los parámetros que se deben entrar en el archivo **concsm.cfg** para definir el Módulo de soporte de comunicaciones de contraseña simple.

Alternativa 1:

```
SPWDCSM
("client=/usr/informix/lib/client/csm/libixspw.so,
```

Alternativa 2:

```
server=/usr/informix/lib/csm/
libixspw.so", "", "")

SPWDCSM("/usr/informix/lib/csm/
libixspw.so", "", "")
```

El ejemplo siguiente muestra el campo *opciones_conex* establecido en `0`, de modo que no se necesita ninguna contraseña:

```
SPWDCSM("/work/informix/csm/libixspw.so","","p=0")
```

Seguridad de la conexión de Enterprise Replication y alta disponibilidad

Puede aumentar la seguridad de las conexiones de clúster de Enterprise Replication y de alta disponibilidad (Duplicación de datos de alta disponibilidad, servidores secundarios autónomos remotos y servidores secundarios de disco compartido) configurando un puerto dedicado en el archivo INFORMIXSQLHOSTS.

Añada **s=6** al campo de opciones (el quinto) en los archivos INFORMIXSQLHOSTS para indicar que el puerto correspondiente sólo acepta solicitudes de conexión de clúster de Enterprise Replication o de alta disponibilidad. Cualquier otro tipo de solicitud de conexión se rechazará con el número de error -25539, tipo de conexión no válido.

A continuación se proporciona un esquema de una entrada del archivo INFORMIXSQLHOSTS:

```
nombre_servidor_bd   tipo_red   nombre_sist_pral   nombre_servicio   s=6
```

Por ejemplo:

```
  ifxer1  oltlitcp  mc001  er_port  s=6,Otros_parámetros_ER
```

Cuando establezca **s=6**, las solicitudes de conexión de clúster de Enterprise Replication o de alta disponibilidad se autenticarán utilizando un nuevo mecanismo. El administrador del sistema debe crear un archivo **hosts.equiv** en el

directorio **$INFORMIXDIR/etc** y añadir los nombres de los nodos de Enterprise Replication y HDR participantes (nombres de sistema principal, tal como se encontrarían en la tercera columna del archivo INFORMIXSQLHOSTS) en ese archivo, uno por línea. El formato del archivo es similar al del archivo **/etc/hosts.equiv** de UNIX. El archivo debe ser propiedad del usuario **informix**, pertenecer al grupo **informix** y los permisos deben estar restringidos de modo que, como máximo, el usuario informix pueda modificar el archivo (utilizando permisos octales, uno de los valores siguientes resulta adecuado: 644, 640, 444 ó 440).

Si la configuración es tal que los servidores de duplicación se encuentran en la misma máquina, el archivo **$INFORMIXDIR/etc/hosts.equiv** no será necesario.

Se aplican las restricciones siguientes a esta opción de seguridad:

- Para puertos sólo de clúster de Enterprise Replication o de alta disponibilidad, **s=6** debe ser la única opción de seguridad presente. Al utilizar **s=6**, no se debe utilizar ninguna otra opción de seguridad (s=0,1,2,3,4).
- Esta opción es específica del entorno del servidor de bases de datos para los clústeres de Enterprise Replication y de alta disponibilidad, por lo tanto, no se debe utilizar en el entorno cliente. Los clientes devolverán un error si esta opción se establece en el archivo SQLHOSTS y el cliente intenta utilizar el nombre del servidor asociado.

Recomendación: Dedique el nombre del servidor de bases de datos o un alias del servidor de bases de datos para la administración de la conectividad segura. Por ejemplo, si utiliza un clúster de alta disponibilidad, ejecute el mandato **onmode -d primary** ***nombre_servidor_secundario*** con INFORMIXSERVER establecido como el servidor de bases de datos o el nombre de alias seguro. A continuación, ejecute los mandatos de restauración **ontape** u **onbar** (por ejemplo, **ontape -p**) que forman parte de la inicialización de clúster de alta disponibilidad utilizando un valor de INFORMIXSERVER diferente no protegido. Del mismo modo, utilice un valor de INFORMIXSERVER diferente no protegido para otras aplicaciones cliente como, por ejemplo, DB-Access.

Para obtener información sobre los clústeres de alta disponibilidad, consulte la publicación *IBM Informix Dynamic Server Administrator's Guide*.

Para obtener información sobre cómo cifrar las comunicaciones de clúster de Enterprise Replication y de alta disponibilidad, consulte el apartado "Cifrado de datos de red de Enterprise Replication y alta disponibilidad" en la página 2-12.

Para obtener información sobre Enterprise Replication, consulte la publicación *IBM Informix Dynamic Server Guía de Enterprise Replication*.

Conexiones locales seguras a un sistema principal

El parámetro de configuración SECURITY_LOCALCONNECTION permite a un administrador del servidor de bases de datos (DBSA) configurar una comprobación de seguridad para las conexiones locales con el mismo sistema principal.

La tabla siguiente muestra los valores del parámetro de configuración SECURITY_LOCALCONNECTION que se pueden utilizar.

Tabla 4-1. Valor del parámetro de configuración SECURITY_LOCALCONNECTION

Valor	Explicación
0	No se realiza ninguna comprobación de seguridad.
1	Dynamic Server compara el ID de usuario del propietario que intenta conectarse con el ID de usuario de conexión. Si no coinciden, Dynamic Server rechaza la conexión.
2	Dynamic Server realiza la misma comprobación que se realiza cuando se establece 1 como valor de SECURITY_LOCALCONNECTION. Además, Dynamic Server obtiene el número de puerto par de la API de red y verifica que la conexión proceda del programa cliente. Si establece 2 como valor de SECURITY_LOCALCONNECTION, deberá tener los protocolos de red SOCTCP o IPCSTR.

Si se establece 1 ó 2 como valor de SECURITY_LOCALCONNECTION, Dynamic Server establecerá una conexión sólo si la conexión cumple los requisitos de la comprobación de seguridad.

Limitación de los ataques de desbordamiento por denegación de servicio

Dynamic Server dispone de varias hebras de escucha (**listen_authenticate**) para limitar los ataques de denegación de servicio (DOS, del inglés Denial-of-service).

Estas hebras autentican las solicitudes de clientes, mientras que la hebra de escucha principal sólo acepta las solicitudes entrantes y bifurca nuevas hebras para la autenticación.

Puede utilizar el parámetro de configuración MAX_INCOMPLETE_CONNECTIONS para configurar el número de las hebras que están realizando una autenticación en cualquier momento.

Puede utilizar el parámetro de configuración LISTEN_TIMEOUT para configurar el valor de tiempo de espera excedido para las conexiones incompletas.

Los ataques de DOS se pueden producir cuando se utilizan mecanismos externos como, por ejemplo, Telnet, para conectarse al puerto reservado para un servidor de bases de datos. Por ejemplo, si utiliza Telnet para conectarse al puerto reservado para un servicio de servidor de bases de datos pero no envía datos y una sesión distinta intenta conectarse al servidor mediante una aplicación como DB-Access, la hebra de escucha se bloquea mientras espera información de la sesión de Telnet y la hebra de escucha no puede aceptar la conexión a la aplicación utilizada en la segunda sesión. Si durante el periodo de espera, un atacante lanza un ataque de DOS distribuido (DDOS) en un bucle, se puede recibir un ataque de desbordamiento sobre la conexión que tiene como consecuencia un rendimiento deficiente de la conexión.

Parámetros de configuración LISTEN_TIMEOUT y MAX_INCOMPLETE_CONNECTIONS

Puede utilizar parámetros de configuración para reducir el riesgo de un ataque de desbordamiento por denegación de servicio (DOS) hostil.

Puede personalizar los siguientes parámetros de configuración:

- LISTEN_TIMEOUT. Establece el periodo de tiempo de espera excedido de conexión incompleta. El periodo de tiempo de espera excedido de conexión incompleta predeterminado es de 10 segundos.
- MAX_INCOMPLETE_CONNECTIONS. Restringe el número de solicitudes de conexión incompletas. El número máximo predeterminado de conexiones incompletas es de 1024.

Si no establecen los parámetros de configuración LISTEN_TIMEOUT y MAX_INCOMPLETE_CONNECTIONS y se produce una avalancha de ataques no autorizados, el procesador virtual de escucha puede volverse inseguro y es posible que no pueda escuchar una solicitud válida a tiempo.

Si establece los parámetros de configuración LISTEN_TIMEOUT y MAX_INCOMPLETE_CONNECTIONS y alguien intenta entrar por la fuerza del sistema y alcanza el límite máximo especificado, la siguiente información en el registro de mensajes en línea indicara que el sistema está sufriendo un ataque:

```
%d conexiones incompletas en estos momentos.
El sistema está en peligro a través de clientes no válidos
en el puerto de escucha.
```

Según la capacidad de la máquina de retener las hebras (en número), puede configurar MAX_INCOMPLETE_CONNECTIONS con un valor más alto y, según el tráfico de la red, puede establecer LISTEN_TIMEOUT con un valor más bajo para reducir las posibilidades de que al ataque pueda alcanzar el límite máximo.

Puede utilizar el mandato **onmode -wm** o **onmode -wf** para cambiar los valores de estos parámetros de configuración mientras el servidor está en línea. Para obtener más información, consulte la publicación *IBM Informix Dynamic Server Administrator's Reference*.

Capítulo 5. Control de acceso discrecional

El control de acceso discrecional verifica si se han otorgado los privilegios necesarios a un usuario para realizar una operación determinada. Puede realizar los siguientes tipos de control de acceso discrecional:

- Crear roles de usuario para controlar qué usuarios pueden realizar operaciones en objetos de base de datos concretos. Consulte el apartado "Roles de usuario".
- Controlar quién tiene permitido crear bases de datos. Consulte el apartado "Establecimiento del permiso para crear bases de datos" en la página 5-2.
- Evitar que usuarios no autorizados puedan registrar rutinas definidas por el usuario. Consulte el apartado "Seguridad para rutinas externas (UDR)" en la página 5-3.
- Controlar si otros usuarios, además del DBSA, tienen permitido visualizar sentencias SQL en ejecución. Consulte el apartado "Habilitación de los usuarios que no son DBSA para ver las sentencias de SQL que una sesión está ejecutando" en la página 5-4.

Roles de usuario

Un rol en una clasificación de una tarea de trabajo como, por ejemplo, nóminas o responsable de nóminas. A cada rol definido se le otorgan privilegios sobre el objeto de base de datos. Para definir un rol, debe utilizar la sentencia CREATE ROLE.

Después de crear un rol, debe utilizar la sentencia GRANT para otorgar privilegios a uno o varios usuarios asociados con el nombre del rol.

Cuando se otorga un rol a un usuario, el otorgante del rol o el usuario al que se otorga el rol deben utilizar la sentencia SET ROLE para activar el rol. A partir de entonces el usuario tendrá los privilegios del rol.

Para obtener más información sobre cómo crear y utilizar roles, consulte la publicación *IBM Informix Guide to SQL: Syntax*.

Separación de roles

Al instalar una instancia de servidor de bases de datos, implementa la separación de roles estableciendo un valor entero de no cero para la variable de entorno INF_ROLE_SEP. La separación de roles aplica la separación de tareas administrativas realizadas por personas que ejecutan y auditan el servidor de bases de datos. Si no se establece INF_ROLE_SEP, el usuario **informix** podrá realizar todas las tareas administrativas.

No se puede activar la separación de roles restableciendo el entorno después de que la instancia del servidor se haya instalado sin separación de roles y no se puede implementar selectivamente la separación de roles en sólo algunas de las bases de datos del mismo servidor de bases de datos.

Para obtener más información sobre la variable de entorno INF_ROLE_SEP, consulte la publicación *IBM Informix Guide to SQL: Reference*. Para obtener más información sobre la separación de roles, consulte el apartado "Separación de roles" en la página 8-4.

Roles predeterminados

Un administrador puede definir un rol predeterminado para asignarlo a usuarios individuales o al grupo PUBLIC para una determinada base de datos.

Cuando un usuario establece una conexión con la base de datos, se aplica automáticamente el rol predeterminado. Este permite a un usuario conectarse a una base de datos sin emitir una sentencia SET ROLE.

Cada usuario tiene los privilegios que se le otorguen individualmente además de los privilegios del rol predeterminado. Un usuario puede pasar del rol individual actual al rol predeterminado utilizando la sentencia SET ROLE DEFAULT.

Si se asignan roles predeterminados diferentes a un usuario y al grupo PUBLIC, el rol predeterminado del usuario tendrá precedencia. Si no se asigna un rol predeterminado a un usuario, el usuario sólo tendrá los privilegios que se le hayan otorgado individualmente y los públicos.

Otorgamiento de privilegios para un rol predeterminado

Para definir y otorgar privilegios para un rol predeterminado:

1. Seleccione un rol existente en la base de datos actual para utilizarlo como rol predeterminado o cree el rol que desee utilizar como rol predeterminado. Utilice la sentencia CREATE ROLE *nombre_rol* para crear un rol nuevo en la base de datos actual.
2. Utilice la sentencia GRANT para otorgar privilegios al rol.
3. Otorgue el rol a un usuario y establezca el rol como rol predeterminado del usuario o de PUBLIC, utilizando la sintaxis `GRANT DEFAULT ROLE` *`nombre_rol`* `TO` *`nombre_usuario`* o `GRANT DEFAULT ROLE` *`nombre_rol`* `TO PUBLIC`.

Utilice la sentencia REVOKE DEFAULT ROLE para eliminar la asociación de un rol predeterminado con usuario.

Un usuario debe utilizar la sentencia SET ROLE DEFAULT para establecer cualquier otro rol actual como rol predeterminado.

Para obtener más información sobre cómo utilizar estas sentencias, consulte la publicación *IBM Informix Guide to SQL: Syntax*.

Establecimiento del permiso para crear bases de datos

Utilice el parámetro de configuración DBCREATE_PERMISSION para conceder permiso para crear bases de datos a usuarios especificados e impedir de este modo que otros usuarios creen bases de datos.

Si no establece parámetros de configuración DBCREATE_PERMISSION, cualquier usuario podrá crear una base de datos.

El usuario **informix** siempre tiene permiso para crear bases de datos.

Para establecer el permiso para crear bases de datos:

1. Para limitar la capacidad de crear bases de datos al usuario **informix**, añada la línea siguiente al archivo ONCONFIG:

   ```
   DBCREATE_PERMISSION informix
   ```

2. Puede incluir varias instancias de DBCREATE_PERMISSION en el archivo ONCONFIG para conceder permiso para crear bases de datos a usuarios adicionales. Por ejemplo, para otorgar permiso a un usuario denominado **watsonjay**, añada la línea siguiente al archivo ONCONFIG:

   ```
   DBCREATE_PERMISSION watsonjay
   ```

Seguridad para rutinas externas (UDR)

Las rutinas externas con bibliotecas compartidas que están fuera del servidor de bases de datos pueden representar riesgos para la seguridad. Entre las rutinas externas se encuentran las rutinas definidas por el usuario (UDR) y las rutinas de los módulos DataBlade.

Un administrador del servidor de bases de datos (DBSA), el usuario **informix** de modo predeterminado, puede implementar medidas de seguridad que establezcan qué usuarios pueden registrar rutinas externas. Este impide a los usuarios no autorizados registrar las rutinas externas.

Utilice el parámetro de configuración IFX_EXTEND_ROLE para restringir la capacidad de los usuarios de registrar rutinas externas.

El valor predeterminado del parámetro de configuración IFX_EXTEND_ROLE es 1 (o `activado`).

Cuando se ha establecido `activado` como valor del parámetro de configuración IFX_EXTEND_ROLE:

- Se pueden otorgar a un usuario privilegios para crear o eliminar una UDR que tenga la cláusula EXTERNAL.
- El rol EXTEND está operativo y se pueden otorgar a un usuario privilegios para crear o eliminar una rutina externa que tenga la cláusula EXTERNAL.

Al otorgar el rol EXTEND a un usuario específico, la tabla de catálogo del sistema **sysroleauth** se actualiza a fin de reflejar el nuevo rol incorporado.

Después de que se haya establecido `Activado` como valor del parámetro de configuración IFX_EXTEND_ROLE, un DBSA puede utilizar la sintaxis siguiente para otorgar y revocar privilegios a usuarios específicos.

- GRANT extend To *nombre_usuario*
- REVOKE extend From *nombre_usuario*

Si no desea restringir el acceso a UDR, establezca `0` (o `Desactivado`) como valor del parámetro de configuración IFX_EXTEND_ROLE. Cuando se establece `Desactivado` como valor del parámetro de configuración IFX_EXTEND_ROLE, el rol EXTEND no está operativo y cualquier usuario puede registrar rutinas externas.

El programa de utilidad **dbimport**, concretamente, se ve afectado cuando el parámetro de configuración IFX_EXTEND_ROLE se establece en el valor `Activado` porque un usuario que utiliza **dbimport** para crear una base de datos nueva no ha recibido un rol ampliado sobre dicha base de datos.

Para obtener más información, consulte la publicación *IBM Informix Guide to SQL: Syntax*.

Habilitación de los usuarios que no son DBSA para ver las sentencias de SQL que una sesión está ejecutando

Los mandatos de **onstat** que muestran el texto de la sentencia de SQL que una sesión está ejecutando quedan normalmente restringidos a los usuarios DBSA. Se puede establecer 1 como valor del parámetro de configuración UNSECURE_ONSTAT para eliminar esta restricción. Al eliminar esta restricción se permite a otros usuarios ejecutar los mandatos **onstat -ses**, **onstat -stm**, **onstat -ssc** y **onstat -sql**.

El parámetro de configuración UNSECURE_ONSTAT entra en vigor cuando se cierra y se reinicia el servidor de bases de datos.

Capítulo 6. Control de accesos basado en etiquetas (Enterprise Edition)

El control de accesos basado en etiquetas (LBAC) es una implementación de la seguridad multinivel (MLS) que permite controlar quién tiene acceso de lectura y quién tiene acceso de grabación a filas y columnas de datos individuales.

Los sistemas MLS procesan información con distintos niveles de seguridad, permiten el acceso simultáneo a usuarios con distintas autorizaciones y permite a los usuarios acceder sólo a la información para la que tienen autorización. MLS es una implementación conocida de MAC (Mandatory Access Control, control de accesos obligatorio). Si dispone del rol de *administrador de seguridad de la base de datos (DBSECADM)* en IDS, puede configurar los objetos LBAC para que se ajusten a sus necesidades de seguridad:

1. *Políticas de seguridad.* Debe asociar una política de seguridad a una tabla que desee proteger frente a accesos no autorizados. Para crear una política de seguridad, debe definir etiquetas de seguridad que determinen quién puede acceder a los datos de la tabla. Puede tener una o varias políticas de seguridad en el sistema, según las necesidades de su organización.
2. *Etiquetas de seguridad.* Debe asociar etiquetas de seguridad con uno o varios objetos de una tabla (*etiquetas de datos*) y con usuarios (*etiquetas de usuario*). Cuando un usuario intenta acceder a un objeto de tabla protegido por LBAC, el sistema compara la etiqueta del usuario con la etiqueta de datos para determinar si el usuario puede tener acceso. Si no se ha otorgado ninguna etiqueta al usuario, el acceso se bloqueará automáticamente en la mayoría de las circunstancias.
3. *Componentes de etiqueta de seguridad.* Los componentes de etiqueta de seguridad son la base de las políticas de seguridad LBAC. Debe utilizar estos componentes para constituir políticas de seguridad que, en combinación con las etiquetas de seguridad, representan diferentes privilegios de acceso de usuario. La variedad de componentes de etiqueta de seguridad que se pueden crear y la flexibilidad de la que se dispone para construir políticas de seguridad y etiquetas de seguridad, ofrece flexibilidad para diseñar la solución LBAC de su organización.

LBAC sirve como complemento de DAC (Discretionary Access Control, control de accesos discrecional). Cuando un usuario intenta acceder a una tabla protegida, IDS aplica dos niveles de control de accesos. El primer nivel es DAC. Con DAC, IDS verifica si el usuario que intenta acceder a la tabla dispone de los privilegios necesarios para realizar la operación solicitada sobre dicha tabla. El segundo nivel es LBAC, que controla el acceso a nivel de fila, a nivel de columna o ambos niveles. La combinación de privilegios de DAC y del acceso a datos protegido por LBAC otorgado a un usuario se conoce como las *credenciales* del usuario.

Esta función sólo está disponible para la edición Dynamic Server Enterprise. Para obtener información detallada sobre las diferencias entre las ediciones, consulte el siguiente sitio web: http://www-306.ibm.com/software/data/informix/ids/ids-ed-choice

Configuración del control de accesos basado en etiquetas

El procedimiento general implica unas cuantas tareas basadas en SQL que definen objetos de seguridad de la base de datos precisos pero flexibles.

Antes de implementar el control de accesos basado en etiquetas (LBAC), debe identificar los datos que se deben proteger, quién puede acceder a los datos y qué tablas no se pueden proteger.

La lista siguiente ofrece un compendio de las principales tareas para la configuración de una implementación básica con IDS:

1. El Administrador del servidor de bases de datos (DBSA) otorga el rol DBSECADM.
2. El DBSECADM define los objetos de seguridad:
   a. Crea componentes de etiqueta de seguridad para definir los atributos de los datos confidenciales, así como los correspondientes atributos de los usuarios a los que se les permite disponer de acceso de lectura o acceso de grabación a estos datos.
   b. Crea políticas de seguridad para reflejar las restricciones de la organización sobre quién puede acceder a datos protegidos.
   c. Crea etiquetas de seguridad para las políticas de seguridad.
   d. Otorga etiquetas de seguridad a usuarios que deben tener acceso a los datos protegidos.
   e. *Para proteger tablas nuevas:* Utiliza la sentencia CREATE TABLE con la cláusula SECURITY POLICY y especifica cómo protegen los objetos de seguridad los datos a nivel de fila, de columna o ambos.
   f. *Para proteger tablas existentes:* Utiliza la sentencia ALTER TABLE con la cláusula ADD SECURITY POLICY y especifica cómo protegen los objetos de seguridad los datos a nivel de fila, de columna o ambos.

Tablas para excluir de la protección de LBAC

LBAC no protege las siguientes categorías de tablas:

- tablas de interfaz de tabla virtual (VTI)
- tablas con interfaz de índice virtual (VII)
- tablas temporales (TEMP)
- tablas con tipos
- tablas jerárquicas

Cómo controlan el acceso las etiquetas de seguridad

Las etiquetas de seguridad dependen de componentes de etiqueta de seguridad para almacenar información sobre la clasificación de los datos y sobre qué usuarios tienen autoridad de acceso.

El control de accesos basado en etiquetas (LBAC) funciona comparando las etiquetas que se han asociado con los usuarios con las etiquetas que han asociado con los datos utilizando un conjunto de reglas predefinido (IDSLBACRULES). Estas etiquetas se construyen con componentes de etiqueta de seguridad, que representan distintos niveles de clasificación de datos y autoridad de acceso. Antes de diseñar una implementación de LBAC, debe saber cómo almacenan las etiquetas información en los componentes y cómo afectan las operaciones de los usuarios y el tipo de componente a la comparación de etiquetas.

LBAC compara *valores* correspondientes a cada usuario y etiqueta de datos cuando alguien intenta acceder a una tabla protegida. Un usuario sin etiqueta de seguridad tiene un valor NULL. Al crear una etiqueta de seguridad, debe seleccionar sus valores eligiendo *elementos* de cada componente de etiqueta de seguridad que forme parte de la política. Las variaciones en el modo en que opte por agrupar los elementos proporcionan los valores diferentes entre las etiquetas que contienen los mismos componentes.

LBAC compara, uno por uno, cada valor de componente de una etiqueta de usuario con el valor de componente correspondiente de la etiqueta de datos. La comparación entre etiquetas se realiza en la secuencia en que se listan los componentes en las etiquetas. La comparación determina si el componente de etiqueta de usuario cumple el criterio IDSLBACRULE apropiado para el acceso. Cuando *todos* los valores de la etiqueta de usuario cumplen los criterios de acceso, la etiqueta de usuario *domina* la etiqueta de datos y puede funcionar con los datos protegidos. Si cualquier valor de la etiqueta de usuario no domina, las credenciales del usuario no se ajustarán a los criterios de la etiqueta de seguridad de protección. LBAC deniega el acceso a datos protegidos a un usuario con un valor NULL, a menos que el DBSECADM haya otorgado al usuario una exención a la política de seguridad que protege la tabla.

Cuando un usuario intenta recuperar datos de una tabla protegida por LBAC con una operación SELECT, la comparación sigue reglas de acceso de lectura.

Reglas de acceso de lectura:

- IDSLBACREADARRAY: El componente de matriz de la etiqueta de seguridad del usuario debe ser superior o igual al componente de matriz de la etiqueta de seguridad de los datos. El usuario sólo puede leer datos del nivel o por debajo del nivel del valor del componente de matriz de la etiqueta del usuario. El nivel se refiere al rango relativo del valor en el orden de elementos de la matriz.
- IDSLBACREADSET: El componente de conjunto de la etiqueta de seguridad del usuario debe incluir cada elemento del valor correspondiente al componente de conjunto de la etiqueta de seguridad de los datos.
- IDSLBACREADTREE: El componente de árbol de la etiqueta de seguridad del usuario debe incluir como mínimo uno de los elementos del valor correspondiente al componente de árbol de la etiqueta de seguridad de los datos o un ancestro de uno de dichos elementos.

Cuando un usuario intenta realizar una operación de inserción (INSERT), actualización (UPDATE) o supresión (DELETE) la comparación siguen las reglas de acceso de grabación.

Reglas de acceso de grabación:

- IDSLBACWRITEARRAY: El componente de matriz de la etiqueta de seguridad del usuario debe ser igual al componente de matriz de la etiqueta de seguridad de los datos. El usuario sólo puede grabar datos del nivel del valor del componente de matriz de la etiqueta del usuario. El nivel se refiere al rango relativo del valor en el orden de elementos de la matriz.
- IDSLBACWRITESET: El componente de conjunto de la etiqueta de seguridad del usuario debe incluir cada elemento del valor correspondiente al componente de conjunto de la etiqueta de seguridad de los datos.
- IDSLBACWRITETREE: El componente de árbol de la etiqueta de seguridad del usuario debe incluir como mínimo uno de los elementos del valor

correspondiente al componente de árbol de la etiqueta de seguridad de los datos o un ancestro de uno de dichos elementos.

Rol de administrador de seguridad de la base de datos

El rol de administrador de seguridad de la base de datos (DBSECADM) es necesario para la creación y el mantenimiento de objetos de seguridad de control de accesos basados en etiquetas.

DBSECADM es un potente rol del servidor que tiene las siguientes responsabilidades para todas las bases de datos que se ejecutan en la instalación de IDS:

- Crear, eliminar, modificar y renombrar componentes de etiqueta de seguridad
- Crear, eliminar y renombrar políticas de seguridad
- Crear, eliminar y renombrar etiquetas de seguridad
- Adjuntar políticas de seguridad o tablas y también separar políticas de seguridad
- Otorgar etiquetas de seguridad a usuarios y también revocar etiquetas de seguridad
- Otorgar y revocar exenciones de políticas de seguridad
- Otorgar y revocar el privilegio SETSESSIONAUTH

Otorgamiento del rol de administrador de seguridad de la base de datos

Un DBSA utiliza la sentencia GRANT DBSECADM para conceder autoridad de administrador de seguridad de la base de datos a un usuario.

Para otorgar DBSECADM, debe ser DBSA. No puede otorgar DBSECADM a un rol o a usted mismo.

Para otorgar el rol DBSECADM, emita la sentencia GRANT DBSECADM, tal como se describe en la publicación *IBM Informix Guide to SQL: Syntax*.

La sentencia siguiente otorga la autorización DBSECADM al usuario `sam`:

```
GRANT DBSECADM TO sam;
```

Revocación del rol de administrador de seguridad de la base de datos

Un DBSA utiliza la sentencia REVOKE DBSECADM para quitar la autoridad de administrador de seguridad de la base de datos a un usuario al que anteriormente se le ha otorgado este rol.

Para revocar el rol DBSECADM, debe ser DBSA. Debe conocer el nombre de inicio de sesión del usuario a quien desee revocar el rol DBSECADM.

Para revocar el rol DBSECADM, emita la sentencia REVOKE DBSECADM, tal como se describe en la publicación *IBM Informix Guide to SQL: Syntax*.

La sentencia siguiente revoca la autorización DBSECADM al usuario `sam`:

```
REVOKE DBSECADM FROM sam;
```

Componentes de etiqueta de seguridad

Los componentes de etiqueta de seguridad son objetos de seguridad para definir políticas de seguridad. Los elementos de estos componentes se utilizan para definir etiquetas de seguridad, que controlan el acceso a las tablas protegidas.

Los componentes de etiqueta de etiqueta representan cualquier criterio que su organización pueda utilizar para decidir si un usuario debe tener acceso a una fila o una columna de una tabla. Algunos ejemplos típicos de estos criterios son:

- Cuánta autoridad tiene el usuario en la organización
- Qué datos confidenciales, si los hay, tiene derecho a leer o grabar el usuario
- A qué departamento pertenece el usuario
- Si el usuario participa en un determinado proyecto

Antes de crear los componentes de etiqueta de seguridad, debe saber cómo se corresponde el plan de privacidad de su organización con un esquema de clasificación de datos. También debe identificar la política de seguridad y las etiquetas de seguridad que creará a partir de los componentes. Las clasificaciones de datos que implemente mediante el control de accesos basado en etiquetas (LBAC) se correlacionan con los elementos que liste al crear componentes de etiqueta de seguridad. Cuando un usuario intenta acceder a datos protegidos, los valores de la etiqueta de un usuario se comparan con los valores de la etiqueta de la fila o la columna. Los componentes de etiqueta de seguridad, y sus elementos que se utilizan en las etiquetas de seguridad, especifican estos valores.

Tipos de componentes de etiqueta de seguridad

Existen tres tipos de componentes de etiqueta de seguridad:

- ARRAY: Cada elemento representa un punto de una escala ordenada de valores relativos (consulte el apartado “Tipo de componente de etiqueta de seguridad: ARRAY” en la página 6-6)
- SET: Cada elemento representa un miembro de un conjunto no ordenado (consulte el apartado “Tipo de componente de etiqueta de seguridad: SET” en la página 6-7)
- TREE: Cada elemento representa un nodo de una jerarquía tipo árbol (consulte el apartado “Tipo de componente de etiqueta de seguridad: TREE” en la página 6-8)

Al diseñar una solución LBAC, debe identificar el tipo de componente de etiqueta de seguridad que refleje mejor la relación entre diversos niveles de autoridad y grupos de usuarios. Una implementación de LBAC básica puede recurrir a las categorizaciones existentes de la organización para nombrar y agrupar los elementos, de modo que los elementos sean entidades que la organización ya utilice. Como visión general, el ejemplo siguiente describe brevemente cómo pueden funcionar los componentes de etiqueta de seguridad en dos situaciones distintas.

Componente que refleja un esquema de clasificación de datos estrictamente clasificado

Ejemplo: Si crea un componente de etiqueta de seguridad para representar una clasificación simple y lineal de clasificaciones de acceso a datos, debe utilizar un componente de tipo ARRAY. Un componente de etiqueta de

seguridad de tipo ARRAY que represente cuatro clasificaciones de acceso de datos puede tener los componentes siguientes: `Top Secret`, `Secret`, `Confidential` y `Unclassified`.

Componente que refleja un organigrama

Ejemplo: La junta ejecutiva de una corporación de servicios de información ficticia de los Estados Unidos denominada ″JK Enterprises″ desea limitar el acceso a filas de datos específicas de una base de datos a la que todos los empleados tienen acceso. JK Enterprises ha dividido su organización nacional en regiones y subregiones. Gran parte de la política de privacidad de JK Enterprises que se debe implementar con LBAC permite o deniega el acceso según la afiliación del usuario a un nivel regional. Las regiones de nivel más alto abarcan áreas más grandes de la organización. Por ejemplo, a un empleado designado como parte del nivel regional Oeste se le otorga más autoridad que a los empleados designados con los niveles regionales subordinados Suroeste, California y Noroeste del Pacífico. El tipo de componente de etiqueta de seguridad que se ajusta mejor a este conjunto de criterios es TREE. Por lo tanto, el usuario con autoridad DBSECADM en JK Enterprises crea un componente de etiqueta de seguridad denominado `region` e identifica los siguientes como algunos de los elementos del componente:

- `Oeste`
- `Suroeste`
- `California`
- `Noroeste del Pacífico`

Puesto que las regiones de JK Enterprises abarcan todos los Estados Unidos, las cuatro regiones anteriores constituyen una lista parcial de elementos. El diagrama del apartado “Tipo de componente de etiqueta de seguridad: TREE” en la página 6-8 ilustra todos los elementos del componente de etiqueta de seguridad `region` de esta empresa.

Tipo de componente de etiqueta de seguridad: ARRAY

El tipo de componente de etiqueta de seguridad ARRAY representa un grupo de elementos ordenado.

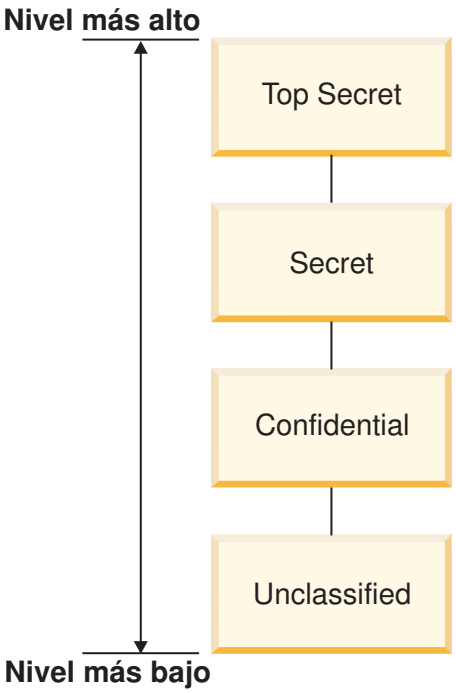
Los elementos de un componente ARRAY representan una escala ordenada de valores relativos; el primer elemento de la lista tiene el valor más alto y el último tiene el valor más bajo.

El número máximo de elementos de un componente de etiqueta de seguridad ARRAY es de 64. Un componente ARRAY de una etiqueta de seguridad tiene el valor de sólo uno de sus elementos cuando se compara siguiendo las reglas de IDSLBACRULES.

Ejemplo: Si la empresa ficticia JK Enterprises define el componente de etiqueta de seguridad `level` como una clasificación de los cuatro niveles de privacidad distintos de la empresa, como en la sentencia siguiente:

```
CREATE SECURITY LABEL COMPONENT level
   ARRAY [ 'Top Secret', 'Secret', 'Confidential', 'Unclassified' ];
```

Entonces el gráfico siguiente ilustra el orden de los elementos:



Cuando un componente ARRAY de la etiqueta de usuario se compara con un componente ARRAY de una etiqueta de datos:

- *Para el acceso de lectura*: La regla IDSLBACREADARRAY permite que el componente del usuario domine cuando su valor sea *superior o igual* al valor del componente de la etiqueta de seguridad de los datos. El usuario sólo puede leer datos del nivel o por debajo del nivel del valor del componente de matriz de la etiqueta del usuario.
- *Para el acceso de grabación:* La regla IDSLBACWRITEARRAY permite que el componente del usuario domine cuando su valor sea *igual* al valor del componente de la etiqueta de los datos. El usuario sólo puede grabar datos del nivel del valor del componente de matriz de la etiqueta del usuario.

Tipo de componente de etiqueta de seguridad: SET

El tipo de componente de etiqueta de seguridad SET se utiliza para representar un grupo de elementos sin ordenar.

Un componente de etiqueta de seguridad del tipo SET consta de una lista de elementos sin ordenar. No hay ningún rango ni otra relación entre los elementos de este tipo de componente.

El número máximo de elementos que pueden existir en un SET es de 64. El valor de un componente de tipo SET en una etiqueta de seguridad puede constar de uno o más elementos.

La siguiente sentencia de SQL crea un componente de etiqueta de seguridad de tipo SET denominado `function` con tres elementos:

```
CREATE SECURITY LABEL COMPONENT function
SET {'Developer', 'Administrative', 'Legal'};
```

Cuando un componente SET de la etiqueta de usuario se compara con un componente SET de una etiqueta de datos:

- *Para el acceso de lectura*: La regla IDSLBACREADSET permite que la etiqueta del usuario domine cuando el componente SET de la etiqueta de seguridad del usuario incluye todos los elementos del valor del componente SET de la etiqueta de seguridad de datos.
- *Para el acceso de grabación*: La regla IDSLBACWRITESET permite que la etiqueta del usuario domine cuando el componente SET de la etiqueta de seguridad del usuario incluye todos los elementos del valor del componente SET de la etiqueta de seguridad de datos.

Tipo de componente de etiqueta de seguridad: TREE

El tipo de componente de etiqueta de seguridad TREE contiene un grupo de elementos que representan una familia de relaciones padre-hijo.

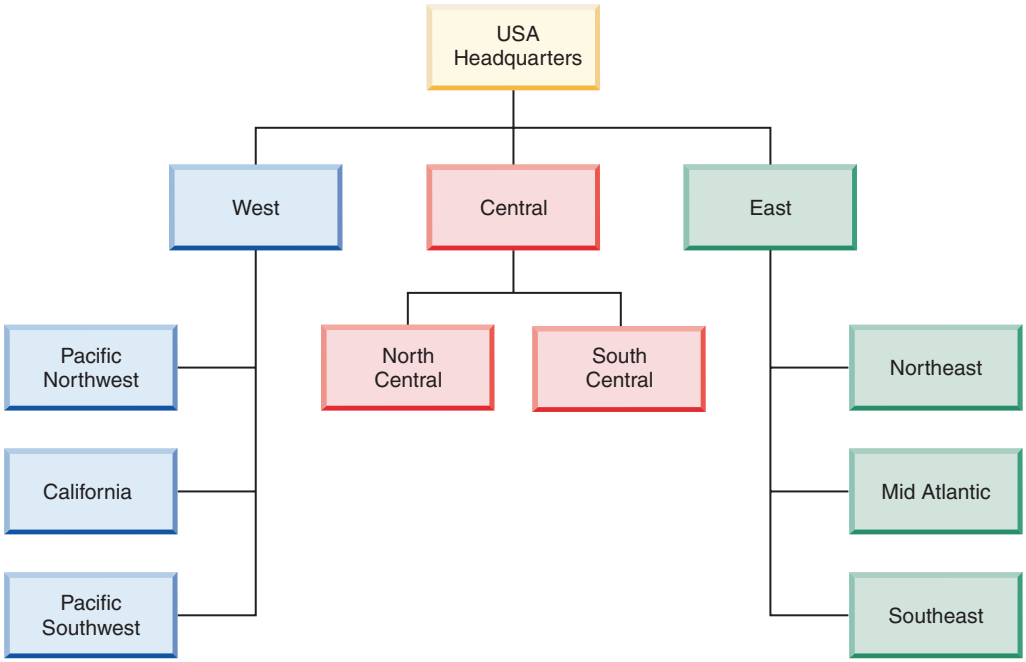
Los elementos de este tipo de componente de etiqueta de seguridad se pueden considerar como si estuviesen en un árbol. El primer elemento que debe especificar para un componente de tipo TREE es `ROOT`, que representa el nivel más alto de autoridad. Luego, debe especificar los demás elementos secuencialmente para seguir los distintos niveles de hijos y nietos que desee tener en el componente.

El número máximo de elementos de un componente de etiqueta de seguridad TREE es de 64. El valor de un componente TREE en una etiqueta es uno o más de sus nodos.

Ejemplo: JK Enterprises decide que sus niveles de autoridad para acceder a datos protegidos deben seguir su organigrama. La empresa podría utilizar este esquema para perfilar su componente de piqueta de seguridad TREE. A continuación se ofrece un ejemplo de una sentencia que crea el componente de etiqueta de seguridad `region`:

```
CREATE SECURITY LABEL COMPONENT region
TREE ( 'USA Headquarters' ROOT,
    'West' UNDER 'USA Headquarters',
    'Central' UNDER 'USA Headquarters',
    'East' UNDER 'USA Headquarters',
    'Pacific Northwest' UNDER 'West',
    'California' UNDER 'West'
    'Pacific Southwest' UNDER 'West'
    'North Central' UNDER 'Central'
   'South Central' UNDER 'Central'
   'Northeast'UNDER 'East'
   'Mid Atlantic' UNDER 'East'
   'Southeast' UNDER 'East');
```

El diagrama siguiente ilustra las relaciones entre los elementos del componente TREE en este ejemplo.



Cuando una etiqueta de usuario con uno o varios componentes TREE se compara con una etiqueta de datos con componentes TREE:

- *Para el acceso de lectura*: La regla IDSLBACREADTREE permite que la etiqueta de usuario domine y tenga acceso de lectura cuando el componente TREE de la etiqueta e incluya como mínimo uno de los elementos del valor correspondiente al componente de árbol de la etiqueta de datos o del ancestro de uno de dichos elementos.
- *Para el acceso de grabación:* La regla IDSLBACWRITETREE permite que la etiqueta del usuario domine y tenga acceso de grabación cuando cada uno de los componentes TREE de la etiqueta que incluya como mínimo uno de los elementos del valor correspondiente al componente de árbol de la etiqueta de datos o del ancestro de uno de dichos elementos.

Creación de componentes de etiqueta de seguridad

La sentencia CREATE SECURITY LABEL COMPONENT define el objeto de seguridad de esta base de datos.

Para crear componentes de etiqueta de seguridad, se debe disponer del rol DBSECADM.

Al crear un componente de etiqueta de seguridad, debe proporcionar la siguiente información:

- Un nombre para el componente
- El tipo de componente que es (ARRAY, SET o TREE)
- Una lista completa de elementos

Para crear un componente de etiqueta de seguridad, emita la sentencia CREATE SECURITY LABEL COMPONENT, tal como se describe en la publicación *IBM Informix Guide to SQL: Syntax*.

A continuación se ofrece un ejemplo de una sentencia CREATE SECURITY LABEL COMPONENT que crea un componente de tipo SET denominado `department` y los elementos `Marketing`, `HR` y `Finance`:

```
CREATE SECURITY LABEL COMPONENT department
   SET {'Marketing', 'HR', 'Finance'};
```

Modificación de componentes de etiqueta de seguridad

La sentencia ALTER SECURITY LABEL COMPONENT añade uno o varios elementos nuevos a un componente existente.

Para añadir uno o varios elementos a un componente de etiqueta de seguridad, se debe disponer del rol DBSECADM y se debe saber qué tipo de componente es.

Al modificar un componente de etiqueta de seguridad, recuerde lo siguiente:

- Un componente de etiqueta de seguridad no puede constar de más de 64 elementos.
- Si el componente que desea modificar es del tipo ARRAY o TREE, necesitará saber las relaciones que todos los elementos del componente resultante tendrán entre sí.
- La sentencia ALTER SECURITY LABEL COMPONENT no puede modificar ni eliminar ningún elemento existente.

Para añadir uno o varios elementos a un componente de etiqueta de seguridad, emita la sentencia ALTER SECURITY LABEL COMPONENT, tal como se describe en la publicación *IBM Informix Guide to SQL: Syntax*.

A continuación se ofrece un ejemplo de una sentencia ALTER SECURITY LABEL COMPONENT que añade a un componente de tipo SET los elementos `Training`, `QA` y `Security`:

```
ALTER SECURITY LABEL COMPONENT department
   ADD SET {'Training', 'QA', 'Security'};
```

Políticas de seguridad

Las políticas de seguridad son objetos de base de datos que se crean y se utilizan para proteger tablas frente a accesos no autorizados.

Una política de seguridad es un objeto de base de datos con nombre definido por un grupo de componentes de etiqueta de seguridad.

Una política de seguridad se asocia a una o varias tablas para permitir sólo a los usuarios con credenciales de control de acceso basadas en etiquetas válidas leer o grabar datos protegidos. Un usuario tiene credenciales válidas cuando el usuario tiene una etiqueta de seguridad que domina si se compara con una fila o columna con etiqueta de acuerdo con IDSLBACRULES. Una política de seguridad no tiene efecto sobre los datos sin etiqueta de seguridad.

No se puede asociar más de una política de seguridad de una tabla y una política de seguridad no puede incluir más de 16 componentes de etiqueta de seguridad. La política de seguridad se debe asociar a una tabla mediante una cláusula de una sentencia CREATE TABLE o ALTER TABLE. Consulte el apartado “Protección de tablas a nivel de fila y de columna” en la página 6-14 para obtener información sobre cómo asociar la política a una tabla.

Creación de políticas de seguridad

Después de crear componentes de etiqueta de seguridad, debe crear políticas de seguridad.

Para crear una política de seguridad, se debe disponer del rol DBSECADM. El número máximo de componentes de etiqueta de seguridad con el que se puede crear una política de seguridad es 16.

El orden en el que liste los componentes de etiqueta de seguridad al crear una política de seguridad no indica ningún orden de precedencia ni ninguna otra relación entre los componentes, pero es importante saber el orden al crear etiquetas de seguridad con funciones SECLABEL incorporadas.

Para crear una política de seguridad, emita la sentencia CREATE SECURITY POLICY, tal como se describe en la publicación *IBM Informix Guide to SQL: Syntax*.

A continuación se ofrece un ejemplo de esta sentencia de SQL, donde `company` es el nombre de la política de seguridad y `region` y `department` son componentes de etiqueta de seguridad utilizados en la política:

```
CREATE SECURITY POLICY company
   COMPONENTS region, department;
```

Etiquetas de seguridad

Las etiquetas de seguridad son objetos que se aplican a filas y columnas para proteger estos datos y se otorgan a los usuarios para concederles acceso a datos protegidos.

Cuando algún usuario intenta acceder a datos protegidos, el control de accesos basado en etiquetas compara la etiqueta del usuario con la etiqueta de los datos. El proceso de esta comparación se detalla en el apartado "Cómo controlan el acceso las etiquetas de seguridad" en la página 6-2.

Al crear una etiqueta de seguridad:

- Debe identificar a qué política de seguridad pertenece la etiqueta.
- Debe asignar un valor para cada componente de etiqueta de seguridad de la política de seguridad.

Sólo debe aplicar una etiqueta a una fila o a una columna. Para una determinada política de seguridad, normalmente otorgará un usuario una sola etiqueta para definir tanto el acceso de lectura como de grabación. Pero puede otorgar a un usuario una etiqueta para el acceso de lectura y una etiqueta diferente para el acceso de grabación a datos protegidos por la misma política de seguridad. Cuando la etiqueta de acceso de lectura difiere de la etiqueta de acceso de grabación otorgada a un usuario, el usuario sólo puede grabar en objetos de datos a los que pueda acceder mediante su etiqueta de acceso de lectura.

Creación de etiquetas de seguridad

La sentencia CREATE SECURITY LABEL define una etiqueta de seguridad nueva para una política de seguridad especificada.

Para crear una etiqueta de seguridad, se debe disponer del rol DBSECADM.

Al crear una etiqueta de seguridad, debe hacer lo siguiente:

- Especifique una política de seguridad a la que pertenezca la etiqueta.
- Identifique los componentes de dicha política.
- Identifique uno o varios elementos de cada componente.
- Asigne un nombre a la etiqueta.

Para crear una etiqueta de seguridad, emita la sentencia CREATE SECURITY LABEL, tal como se describe en la publicación *IBM Informix Guide to SQL: Syntax*.

A continuación se ofrece un ejemplo de una sentencia CREATE SECURITY LABEL:

```
CREATE SECURITY LABEL company.label2
   COMPONENT level 'Secret',
   COMPONENT function 'Administrative',
   COMPONENT region 'Southwest';
```

Esta sentencia define la etiqueta `label2` en la política de seguridad `company`.

Otorgamiento de etiquetas de seguridad

La sentencia GRANT SECURITY LABEL otorga una etiqueta de seguridad a un usuario o a una lista de usuarios.

Para otorgar una etiqueta a usuarios, se debe disponer del rol DBSECADM. Los usuarios especificados en una sentencia GRANT SECURITY LABEL no pueden ser el usuario DBSECADM que la emite.

Al emitir la sentencia GRANT SECURITY LABEL, puede especificar opcionalmente que los usuarios deben recibir la etiqueta para el acceso de lectura, el acceso de grabación o el acceso completo. Si no especifica el acceso, la sentencia otorgará a los usuarios una etiqueta de acceso completo.

Si a un usuario se le otorga una etiqueta de seguridad para el acceso de lectura diferente a la del acceso de grabación, los valores proporcionados para los componentes de etiqueta de seguridad deben seguir las reglas siguientes:

- Para los componentes de etiqueta de seguridad de tipo ARRAY, el valor debe ser el mismo en ambas etiquetas de seguridad.
- Para los componentes de etiqueta de seguridad de tipo SET, los valores proporcionados en la etiqueta de seguridad utilizada para el acceso de GRABACIÓN deben ser un subconjunto de los valores proporcionados en la etiqueta de seguridad utilizada para el acceso de LECTURA. Si todos los valores son iguales, esto se considera un subconjunto y se permite.
- Para los componentes de etiqueta de seguridad de tipo TREE, cada elemento del componente TREE de la etiqueta de seguridad para el acceso de grabación debe ser un elemento o un descendiente de un elemento del componente TREE de la etiqueta de seguridad para el acceso de lectura.

Para otorgar una etiqueta de seguridad, consulte la documentación sobre la sentencia GRANT SECURITY LABEL en la publicación *IBM Informix Guide to SQL: Syntax*

En el ejemplo siguiente de esta sentencia de SQL, se otorga al usuario `maria` la etiqueta `label2` de la política de seguridad `company`.

```
GRANT SECURITY LABEL company.label2
   TO maria;
```

Revocación de etiquetas de seguridad

La sentencia REVOKE SECURITY LABEL revoca una etiqueta de seguridad a un usuario o a una lista de usuarios.

Para emitir la sentencia REVOKE SECURITY LABEL, se debe disponer del rol DBSECADM.

Al emitir la sentencia, puede hacer opcionalmente lo siguiente:

- Revocar a usuarios todas las etiquetas de seguridad de una política de seguridad.
- Especificar la etiqueta de acceso de lectura o la etiqueta de acceso de grabación, o ambas etiquetas, si los usuarios tienen dos etiquetas distintas para una política de seguridad.

Para revocar una etiqueta de seguridad, emita la sentencia REVOKE SECURITY LABEL , tal como se describe en la publicación *IBM Informix Guide to SQL: Syntax*.

En el ejemplo siguiente de esta sentencia de SQL, se revoca al usuario `maria` la etiqueta `label2` de la política de seguridad `company`.

```
REVOKE SECURITY LABEL company.label2
   FROM maria;
```

Funciones de soporte de etiquetas de seguridad

Las funciones de soporte de etiquetas de seguridad son expresiones para manipular etiquetas de seguridad.

Normalmente, las funciones de soporte de etiquetas de seguridad (funciones SECLABEL) se utilizan para especificar una etiqueta en las operaciones de manipulación de datos (DML) sobre filas de tablas protegidas. No obstante, en estas operaciones las funciones de soporte de etiquetas de seguridad no proporcionan mayor acceso a los datos protegidos que el acceso proporcionado por las credenciales de seguridad del usuario. Hay tres funciones incorporadas para el control de accesos basado en etiquetas en IDS:

- La función SECLABEL_BY_NAME permite proporcionar una etiqueta de seguridad directamente especificando su nombre.
- La función SECLABEL_BY_COMP permite proporcionar una etiqueta de seguridad directamente, especificando los valores de sus componentes.
- La función SECLABEL_TO_CHAR devuelve una etiqueta de seguridad en el formato de serie de la etiqueta de seguridad.

Puede hacer referencia a una etiqueta de seguridad con estas funciones proporcionando uno de los elementos siguientes:

- Un nombre, tal como está declarado en la sentencia CREATE SECURITY LABEL o RENAME SECURITY LABEL.
- Una lista de valores para cada componente de la política de seguridad de la etiqueta de seguridad.
- Un valor codificado interno que el tipo de datos IDSSECURITYLABEL almacena.

Estas funciones pueden realizar conversiones entre los distintos formatos de una etiqueta de seguridad.

Consulta la publicación *IBM Informix Guide to SQL: Syntax* para obtener más información sobre las funciones de soporte de etiquetas de seguridad y ejemplos de éstas.

Protección de tablas a nivel de fila y de columna

Proteja filas y columnas asociándolas con objetos de seguridad mediante cláusulas en las sentencias CREATE TABLE y ALTER TABLE.

Después de haber creado los objetos de seguridad necesarios para la implementación del control de accesos basado en etiquetas (LBAC), debe aplicarlos a las tablas que desee proteger. Las principales acciones para proteger los datos en esta fase son las siguientes:

- Adjunte una política de seguridad a cada tabla que contenga datos que LBAC tenga que proteger.
- Asocie las filas y las columnas necesarias con etiquetas de seguridad.

Los datos de una tabla sólo se pueden proteger mediante etiquetas de seguridad que formen parte de la política de seguridad que protege la tabla. La protección de datos, incluida la adjunción de una política de seguridad a una tabla, se puede realizar al crear la tabla o posteriormente modificando la tabla.

Tabla protegida con granularidad de nivel de fila

Una tabla se puede marcar como protegida con granularidad de nivel de fila durante CREATE TABLE o ALTER TABLE adjuntando una política de seguridad y especificando la columna de etiqueta de seguridad. La columna de etiqueta de seguridad debe ser del tipo de datos IDSSECURITYLABEL.

Si los usuarios intentan acceder a una fila para la que no tengan las credenciales de LBAC necesarias, el sistema responderá a los usuarios como si la fila no existiera.

Tabla protegida con granularidad de nivel de columna

Una tabla de base de datos se puede marcar como protegida con granularidad de nivel de columna durante CREATE TABLE o ALTER TABLE adjuntando una política de seguridad a dicha tabla y adjuntando una etiqueta de seguridad a una o varias columnas de la tabla. Cuando una columna está asociada con una etiqueta de seguridad, dicha columa se conoce como una *columna protegida*. La política de seguridad adjuntada a la tabla afecta al nivel de seguridad que puede aplicarse a la columna.

Si los usuarios intentan acceder a una columna para la que no tengan las credenciales de LBAC necesarias, el sistema generará un mensaje de error.

Columna de etiqueta de seguridad (tipos de datos IDSSECURITYLABEL)

La columna que tenga la etiqueta para la granularidad a nivel de fila debe ser del tipo de datos IDSSECURITYLABEL. Sólo un usuario que disponga del rol DBSECADM puede crear, modificar o eliminar una columna de este tipo de datos. ISDSECURITYLABEL es un tipo de datos DISTINCT OF VARCHAR(128) incorporado. Una tabla que tenga una política de seguridad sólo puede tener una columna IDSSECURITYLABEL.

Lo siguiente no se puede aplicar a una columna de etiqueta de seguridad:

- Restricciones referenciales
- Restricciones de comprobación
- Restricción de clave primaria o de unicidad si la columna de etiqueta de seguridad es la única columna con restricciones
- Protección de columnas
- Cifrado

Para obtener más información sobre el tipo de datos IDSSECURITYLABEL, consulte la publicación *IBM Informix Guide to SQL: Reference* y la publicación *IBM Informix Guide to SQL: Syntax.*

Protección simultánea a nivel de fila y de columna en una tabla

Una tabla protegida se puede definir con granularidades a nivel de fila y de columna. Si se aplica tanto la granularidad de fila como de columna a una tabla, LBAC aplicará el control de accesos a nivel de columna antes del control de accesos a nivel de fila.

Puede aplicar la protección a nivel de fila y de columna sobre una tabla en una sola sentencia en lugar de emitir sentencias distintas para las dos granularidades cuando realice una de las siguientes acciones:

- Al crear una nueva tabla protegida por LBAC
- Al modificar una tabla para añadir protección a nivel de fila además de la protección a nivel de columna existente

A continuación se ofrece un ejemplo de una sentencia CREATE TABLE y una sentencia ALTER TABLE que crean dos tablas con protección a nivel de fila y de columna.

```
CREATE TABLE T5
   (C1 IDSSECURITYLABEL,
   C2 int,
   C3 char (10) COLUMN SECURED WITH label6)
   SECURITY POLICY company;

ALTER TABLE T6
   ADD ( C1 IDSSECURITYLABEL),
   MODIFY (C2 INT COLUMN SECURED WITH label7),
   ADD SECURITY POLICY company;
```

Para obtener más información sobre cómo funcionan estas sentencias, consulte los apartados “Aplicación de la protección a nivel de fila”, “Aplicación de la protección a nivel de columna” en la página 6-16, y las publicaciones *IBM Informix Guide to SQL: Reference* e *IBM Informix Guide to SQL: Syntax.*

Aplicación de la protección a nivel de fila

Proteja los datos a nivel de fila la asociando la tabla con una política de seguridad e insertando una columna de tipo IDSSECURITYLABEL.

Existen dos métodos para aplicar la protección a nivel de fila:

1. Para una tabla *nueva*: Utilice la sentencia CREATE TABLE con las cláusulas IDSSECURITYLABEL y SECURITY POLICY adecuadas, tal como se describe en la publicación *IBM Informix Guide to SQL: Syntax*.

2. Para una tabla *existente*: Utilice la sentencia ALTER TABLE con las cláusulas IDSSECURITYLABEL y ADD SECURITY POLICY adecuadas, tal como se describe en la publicación *IBM Informix Guide to SQL: Syntax*.

A continuación se ofrece un ejemplo de una sentencia que aplica la protección a nivel de fila cuando se crea una tabla nueva (T1), utilizando la política de seguridad denominada company y la etiqueta de seguridad denominada label2.

```
CREATE TABLE T1
   (C1 IDSSECURITYLABEL,
   C2 int,
   C3 char (10))
   SECURITY POLICY company;
```

La sentencia siguiente proporciona un ejemplo de la aplicación de la protección a nivel de fila sobre una tabla (T2) que ya existe en la base de datos utilizando la política de seguridad denominada company. El valor predeterminado para C1 es label3.

```
ALTER TABLE T2
  ADD (C1 IDSSECURITYLABEL DEFAULT label3),
  ADD SECURITY POLICY company;
```

Aplicación de la protección a nivel de columna

Proteja los datos a nivel de columna la asociando la tabla con una política de seguridad y adjuntando una etiqueta de seguridad a una o varias columnas.

Existen dos métodos para aplicar la protección a nivel de columna:

1. Para una tabla *nueva*: Utilice la sentencia CREATE TABLE con las cláusulas COLUMN SECURED WITH y SECURITY POLICY, tal como se describe en la publicación *IBM Informix Guide to SQL: Syntax*.
2. Para una tabla *existente*: Utilice la sentencia ALTER TABLE con las cláusulas MODIFY (*su_columna* COLUMN SECURED WITH) y ADD SECURITY POLICY, tal como se describe en la publicación *IBM Informix Guide to SQL: Syntax*.

A continuación se ofrece un ejemplo de una sentencia que aplica la protección a nivel de columna cuando se crea una tabla nueva (T3), utilizando la política de seguridad denominada company y una etiqueta de seguridad denominada label4.

```
CREATE TABLE T3
   (C1 CHAR (8),
   C2 int COLUMN SECURED WITH label4,
   C3 char (10))
   SECURITY POLICY company;
```

La sentencia siguiente proporciona un ejemplo de la aplicación de la protección a nivel de columna sobre una tabla (T4) que ya existe en la base de datos, utilizando la política de seguridad denominada company y una etiqueta de seguridad denominada label5.

```
ALTER TABLE T4
   MODIFY (C1 CHAR (8) COLUMN SECURED WITH label5),
   ADD SECURITY POLICY company;
```

Exenciones

Las exenciones modifican las credenciales de seguridad de los usuarios inhabilitando una o varias de las reglas IDSLBACRULES para un tipo de componente de una política de seguridad.

Dado que las exenciones se basan en un tipo de componente de etiqueta de seguridad para una política de seguridad concreta, esta exención no se aplica fuera de dicha política de seguridad. Dentro de la política de seguridad, la exención se aplica a *todas* las instancias del tipo de componente.

Las exenciones son útiles porque permiten que usuarios de confianza realicen tareas administrativas para las que resultaría engorroso otorgar todas las credenciales necesarias de control de accesos basado en etiquetas. Por ejemplo, si su trabajo consiste en clasificar datos entrantes, lo práctica habitual será que DBSECADM le otorgue exenciones para que pueda grabar en cualquier fila de datos de la política de seguridad.

Si los usuarios disponen de una exención de todas las reglas de una política de seguridad, tendrán acceso completo a todos los datos protegidos por dicha política.

Las exenciones proporcionan una capacidad de acceso muy elevada. No las otorgue sin considerarlo detenidamente.

Otorgamiento de exenciones

La sentencia GRANT EXEMPTION otorga a un usuario una exención de una o varias reglas de acceso de una política de seguridad.

Para otorgar exenciones, se debe disponer del rol DBSECADM.

Para otorgar una exención, emita la sentencia GRANT EXEMPTION, tal como se describe en la publicación *IBM Informix Guide to SQL: Syntax*.

La sentencia siguiente otorga al usuario `maria` una exención de la regla IDSLBACWRITETREE de la política de seguridad `company`:

```
GRANT EXEMPTION
ON RULE IDSLBACWRITETREE
FOR company
TO maria
```

Para otorgar a un usuario exenciones de todas las reglas IDSLBACRULES de una política de seguridad, especifique `ALL` en lugar del nombre de la política en la sentencia. Normalmente, este tipo de exención resulta práctico para el usuario que sea responsable de cargar y descargar datos en tablas protegidas.

Revocación de exenciones

La sentencia REVOKE EXEMPTION revoca a un usuario una exención sobre una o varias reglas de acceso de una política de seguridad.

Para revocar exenciones, se debe disponer del rol DBSECADM.

Para revocar una exención, emita la sentencia REVOKE EXEMPTION, tal como se describe en la publicación *IBM Informix Guide to SQL: Syntax*.

La sentencia siguiente revoca al usuario `maria` una exención de la regla IDSLBACWRITETREE de la política de seguridad `company`:

```
REVOKE EXEMPTION ON RULE IDSLBACWRITETREE FOR company FROM maria
```

Para revocar todas las exenciones de IDSLBACRULES que un usuario tiene para una política de seguridad, especifique `ALL` en lugar del nombre de la política en la sentencia.

Mantenimiento de una implementación de control de accesos basado en etiquetas

Para optimizar el rendimiento de la base de datos es posible que se tengan que ajustar los valores de los parámetros de configuración de las políticas de seguridad y las credenciales de usuario.

Ajuste de memoria caché de LBAC

Un rendimiento pobre de una base de datos con tablas protegidas por el control de accesos basado en etiquetas (LBAC) puede indicar que el sistema recurre innecesariamente a operaciones de disco más que al almacenamiento en la memoria caché relacionado con LBAC para recuperar información de la memoria.

El ajuste de uno o varios de los siguientes parámetros en el archivo ONCONFIG puede mejorar el rendimiento para las consultas ejecutadas frecuentemente sobre las tablas protegidas. Por ejemplo, si se establece un valor demasiado bajo para el parámetro PLCY_HASHSIZE, no habrá suficientes grupos de hash asignados para el almacenamiento en la memoria caché de información de políticas de seguridad y, por lo tanto, se producirá alguna disminución del rendimiento de la base de datos que implica tablas protegidas por LBAC.

PLCY_HASHSIZE

El parámetro PLCY_HASHSIZE especifica el número de grupos de hash que hay en la memoria caché de información de políticas de seguridad.

valor de onconfig.std
31

unidades
kilobytes

rango de valores
Cualquier entero positivo

entra en vigor
Cuando se cierra y se reinicia el servidor de bases de datos

consulte
la publicación *IBM Informix Dynamic Server Performance Guide* para obtener más información sobre los efectos de la configuración sobre la memoria

PLCY_POOLSIZE

El parámetro PLCY_POOLSIZE especifica el número máximo de entradas en cada grupo de hash de la memoria caché de información de políticas de seguridad.

valor de onconfig.std
127

unidades
kilobytes

rango de valores
Cualquier entero positivo

entra en vigor
Cuando se cierra y se reinicia el servidor de bases de datos

consulte
la publicación *IBM Informix Dynamic Server Performance Guide* para obtener más información sobre los efectos de la configuración sobre la memoria

USRC_HASHSIZE

El parámetro USRC_HASHSIZE especifica el número de grupos de hash que hay en la memoria caché de información de credenciales LBAC de usuario.

valor de onconfig.std
31

unidades
kilobytes

rango de valores
Cualquier entero positivo

entra en vigor
Cuando se cierra y se reinicia el servidor de bases de datos

consulte
la publicación *IBM Informix Dynamic Server Performance Guide* para obtener más información sobre los efectos de la configuración sobre la memoria

USRC_POOLSIZE

El parámetro USRC_POOLSIZE especifica el número máximo de entradas en cada grupo de hash de la memoria caché de información de credenciales LBAC de usuario.

valor de onconfig.std
127

unidades
kilobytes

rango de valores
Cualquier entero positivo

entra en vigor
Cuando se cierra y se reinicia el servidor de bases de datos

consulte
la publicación *IBM Informix Dynamic Server Performance Guide* para obtener más información sobre los efectos de la configuración sobre la memoria

Eliminación de objetos de seguridad

Utilice la sentencia DROP SECURITY para eliminar un componente de etiqueta de seguridad, una política de seguridad o una etiqueta de seguridad de la base de datos.

Para eliminar un objeto de seguridad, se debe disponer del rol DBSECADM.

Las tres definiciones de palabra clave válidas de la sentencia DROP SECURITY son las siguientes:

1. DROP SECURITY POLICY *política* elimina una política de seguridad; se puede utilizar en las modalidades RESTRICT y CASCADE
   - Ejemplo: `DROP SECURITY POLICY company` elimina la política denominada `company` de la base de datos

2. DROP SECURITY LABEL *política.etiqueta* elimina una etiqueta de seguridad; se puede utilizar en la modalidad RESTRICT
   - Ejemplo: `DROP SECURITY LABEL company.label2` elimina la etiqueta denominada `label2`.
3. DROP SECURITY LABEL COMPONENT *componente* elimina un componente de etiqueta de seguridad; se puede utilizar en la modalidad RESTRICT
   - Ejemplo: `DROP SECURITY LABEL COMPONENT department` elimina el componente `department`.

   Para obtener más información sobre la sentencia DROP SECURITY, incluidos detalles sobre las modalidades RESTRICT y CASCADE, consulte la publicación *IBM Informix Guide to SQL: Syntax*.

Cuando la sentencia DROP SECURITY se ejecuta satisfactoriamente, el servidor de bases de datos suprime las filas que hacen referencia al nombre o al identificador numérico del objeto especificado de las tablas del catálogo del sistema, incluidas las tablas siguientes:

- **sysecpolicies** para las políticas de seguridad
- **sysseclabels** para las etiquetas de seguridad
- **sysseclabelcomponents** para los componentes de etiqueta de seguridad

Cómo renombrar objetos de seguridad

Utilice la sentencia RENAME SECURITY para renombrar una política de seguridad, una etiqueta de seguridad o un componente de etiqueta de seguridad.

Para renombrar un objeto de seguridad, se debe disponer del rol DBSECADM.

Las tres cláusulas válidas para la sentencia RENAME SECURITY son las siguientes:

1. POLICY *nombre_anterior* TO *nombre_nuevo* renombra una política de seguridad
   - Ejemplo: `RENAME SECURITY POLICY company TO subsidiary;` renombra la política denominada `company` como `subsidiary`
2. LABEL *política_seguridad.nombre_anterior* TO *nombre_nuevo* renombra una política de seguridad; en esta sentencia, también se debe indicar la política de seguridad a la que pertenece la etiqueta
   - Ejemplo: `RENAME SECURITY LABEL subsidiary.label8 TO label9;` renombra `label8` como `label9`, que pertenece a la política de seguridad `subsidiary`
3. LABEL COMPONENT *nombre_anterior* TO *nombre_nuevo* especifica un componente de etiqueta de seguridad
   - Ejemplo: `RENAME SECURITY LABEL COMPONENT department TO division;` renombra el componente `department` como `division`.

   Para obtener más información sobre la sentencia RENAME SECURITY, consulte la publicación *IBM Informix Guide to SQL: Syntax*.

La sentencia RENAME SECURITY sustituye el *nombre_anterior* por el *nombre_nuevo* especificado en la tabla del catálogo del sistema en la que está registrado el objeto de seguridad:

- **sysecpolicies.secpolicyname** para las políticas de seguridad
- **sysseclabels.seclabelname** para las etiquetas de seguridad
- **sysseclabelcomponents.compname** para los componentes de etiqueta de seguridad.

No obstante, esta sentencia no cambia el valor numérico de **sysecpolicies.secpolicyid**, **sysseclabels.seclabelid** ni **sysseclabelcomponents.compid** del objeto de seguridad renombrado.

Consideraciones sobre la seguridad de IDS para el control de accesos basado en etiquetas

La amplia gama de posibilidades de IDS requiere determinadas precauciones y planificación para garantizar que se pueda acceder a las tablas protegidas debidamente.

Para realizar las acciones siguientes, se debe disponer del rol DBSECADM después de implementar el control de accesos basado en etiquetas (LBAC) en el servidor de bases de datos:

- Utilizar el privilegio SETSESSIONAUTH (consulte "SET SESSION AUTHORIZATION")
- Realizar una restauración a nivel de tabla con el programa de utilidad **archecker** (consulte "Copia de seguridad y restauración" en la página 6-22)
- Exportar esquemas y datos (consulte "Programas de utilidad dbschema, dbexport y dbimport" en la página 6-22)
- Importar datos (consulte "Programas de utilidad dbschema, dbexport y dbimport" en la página 6-22)

Para realizar estas acciones, el usuario debe tener credenciales de acceso de lectura y grabación:

- Realizar copias de seguridad y restauraciones con los programas de utilidad **onbar** y **ontape** (consulte "Copia de seguridad y restauración" en la página 6-22)
- "Carga y descarga de datos" en la página 6-23

Para evitar el acceso no autorizado a tablas protegidas, tome precauciones adicionales con las operaciones y los objetos de base de datos siguientes:

- "Programa de utilidad onlog" en la página 6-23
- Archivos de spool de transacciones canceladas y de spool de información de filas de "Enterprise Replication" en la página 6-23
- "Sentencia INSERT INTO . . . SELECT FROM" en la página 6-24
- Archivos .RET y .FLT de High Performance Loader (consulte "Carga y descarga de datos" en la página 6-23)
- "Tablas temporales creadas por la cláusula INTO TEMP" en la página 6-24
- "Rutinas definidas por el usuario" en la página 6-24 creadas con palabras clave de DBA

SET SESSION AUTHORIZATION

La sentencia SET SESSION AUTHORIZATION permite asumir la identidad de otro usuario, incluidas las credenciales LBAC del usuario para las tablas protegidas.

IDS 11.10 y versiones posteriores con capacidad de control de accesos basado en etiquetas (LBAC) manejan el privilegio SETSESSIONAUTH de modo diferente a las versiones anteriores del servidor de bases de datos que no tenían la funcionalidad LBAC. Las versiones más nuevas de IDS requieren que el DBSECADM otorgue el privilegio SETSESSIONAUTH. Como el privilegio SETSESSIONAUTH se puede

utilizar para asumir las credenciales LBAC de otro usuario, el DBSECADM debe tener cuidado al otorgar el privilegio SETSESSIONAUTH.

Si el servidor de bases de datos se ha convertido de una versión anterior que no soportaba LBAC, a los usuarios que disponían del privilegio de DBA se les otorga automáticamente el privilegio de acceso SETSESSIONAUTH para PUBLIC en el proceso de migración. Debe inicializar el servidor convertido como una versión que soporte las políticas de seguridad de LBAC para eliminar el privilegio SETSESSIONAUTH de todos los DBA y habilitar el rol DBSECADM para otorgar este privilegio.

Para obtener más información sobre cómo funciona SET SESSION AUTHORIZATION con LBAC, consulte la publicación *IBM Informix Guide to SQL: Syntax.*

Copia de seguridad y restauración

Los usuarios responsables de realizar copias de seguridad o restauraciones de datos protegidos con los programas de utilidad ON-Bar y **ontape** y deben disponer de las credenciales de acceso de lectura y grabación LBAC para las tablas del servidor correspondientes. La seguridad de LBAC permanece intacta durante la copia de seguridad y después de su restauración en el servidor, pero tenga en cuenta que para proteger los datos de copia de seguridad guardados necesita tomar otras precauciones.

IDS permite la restauración de una tabla específica o un conjunto de tablas de las que se haya hecho previamente una copia de seguridad con **onbar** u **ontape**. Estas tablas se pueden restaurar a un determinado punto del tiempo. Durante la restauración a nivel de tabla de tablas protegidas por LBAC, asegúrese de que los archivos de mandato de esquema especifiquen la política de seguridad con la tabla de destino. Puesto que durante la restauración se creará una tabla de destino protegida, el usuario que ejecute la restauración a nivel de tabla debe disponer del rol DBSECADM. Además, se aplicarán las reglas de LBAC cuando se ejecute la sentencia INSERT del archivo de mandato de esquema para cargar la tabla de destino. Si se debe restaurar toda la tabla, el usuario debe disponer de las credenciales de LBAC necesarias.

Programas de utilidad dbschema, dbexport y dbimport

Cuando se ejecuten los programas de utilidad **dbschema** y **dbexport**, se aplicarán las reglas de LBAC sobre tablas protegidas. Sólo esas filas se descargarán cuando la etiqueta de seguridad del usuario domine la etiqueta de columna, la etiqueta de fila o ambas. Puesto que tanto el programa de utilidad **dbschema** como **dbexport** necesitan leer catálogos de LBAC, el usuario que ejecuta estos programas de utilidad debe disponer de las exenciones o credenciales LBAC apropiadas para acceder a los datos.

El programa de utilidad **dbimport** crea y llena una base de datos a partir de archivos de texto. Las reglas de LBAC se aplicarán durante la carga de tablas protegidas. El usuario que ejecuta la importación debe disponer de las exenciones o credenciales LBAC apropiadas si la base de datos contiene objetos LBAC como una política, componentes y etiquetas.

Carga y descarga de datos

IDS proporciona diversos modos de cargar y descargar datos. Algunos de estos métodos son los siguientes:

- Sentencias LOAD y UNLOAD
- Programa de utilidad **dbload**
- Programas de utilidad **onpload** y **ipload** para High-Performance Loader (HPL)
- Programas de utilidad **onload** y **onunload**

Se aplican las reglas de LBAC cuando estas sentencias y estos programas de utilidad se ejecutan sobre tablas protegidas. La etiqueta de seguridad del usuario debe dominar la etiqueta de columna, la etiqueta de fila o ambas. Si se debe cargar/descargar una tabla entera, el usuario deberá tener las credenciales de LBAC necesarias para leer y grabar todas las filas y columnas etiquetadas. Asimismo, el DBSECADM puede otorgar una exención al usuario para pasar por alto la política de seguridad que protege las tablas.

Las filas que se rechazan cuando se ejecuta el programa de utilidad **onpload** se vuelcan en archivos .REJ y .FLT. Tome las precauciones necesarias para impedir el acceso no autorizado a estos archivos. Para las cargas de modalidad rápida utilizando HPL, las filas se insertan directamente en extensiones de tabla saltándose la capa SQL. Al usuario que ejecuta la carga en modalidad rápida se le deben otorgar las exenciones necesarias para pasar por alto la política de seguridad.

Los programas de utilidad **onload** y **onunload** transfieren los datos en unidades de página de disco binarias. Por lo tanto, estos programas de utilidad no leen ni graban en filas individuales. **onload** y **onunload** fallan sobre las tablas protegidas a menos que se hayan otorgado al usuario las exenciones necesarias para pasar por alto la política de seguridad.

Programa de utilidad onlog

El programa de utilidad **onlog** muestra todas las partes de la anotación lógica, o sólo las partes seleccionadas. Este mandato puede tomar datos de archivos de registro seleccionados, de toda la anotación lógica o de una cinta de copia de seguridad de archivos de registro anteriores. Los registros de anotación pueden exponer datos protegidos por LBAC en una base de datos activa. Asegúrese de que los datos no queden expuestos debido al uso indebido de este programa de utilidad.

Enterprise Replication

Para garantizar que los datos transferidos por Enterprise Replication estén protegidos después de haber implementado LBAC, debe proteger las tablas etiquetadas tanto en el servidor de origen como en el de destino con la misma política de seguridad. Durante la sincronización, el servidor pasa por alto internamente LBAC al comparar las tablas de origen y de destino. Los datos de las tablas protegidas de Enterprise Replication también pueden quedar expuestos si se habilita el spool de transacciones canceladas y el spool de información de filas para registrar transacciones fallidas, a menos que se impida el acceso no autorizado a dichos archivos.

Sentencia INSERT INTO . . . SELECT FROM

Cuando se utilice la sentencia INSERT INTO . . . SELECT FROM sobre una tabla protegida por LBAC para crear otra tabla, asegúrese de que la nueva tabla esté protegida por la misma política de seguridad que se utiliza para proteger la tabla de origen. De lo contrario, se corre el riesgo potencial de que la tabla nueva deje los datos expuestos, violando de este modo la política de privacidad de la organización. Tenga en cuenta que esta exposición opcional de los datos se puede producir si la sentencia se utiliza para crear tabla permanente o para crear una tabla temporal y luego insertarla en una de permanente.

Tablas temporales creadas por la cláusula INTO TEMP

La cláusula INTO TEMP de la sentencia SELECT crea una tabla temporal para mantener los datos de la consulta. Si la tabla de la que se selecciona es una tabla protegida, LBAC no protegerá los datos de resultados de la consulta en la tabla temporal intermedia. Tome las precauciones necesarias para garantizar que los datos de la tabla temporal no queden expuestos a usuarios no autorizados.

Rutinas definidas por el usuario

IDS permite el registro de rutinas definidas por el usuario (UDR) con la palabra clave DBA. Si a un usuario se le otorga el privilegio de ejecución sobre una UDR, el servidor de bases de datos otorga al usuario automáticamente los privilegios de DBA temporales que sólo se habilitan cuando el usuario ejecuta la UDR. El usuario que ejecuta la UDR de DBA asume la identidad de un DBA durante la ejecución de la UDR y, por lo tanto, tendrá la etiqueta de usuario del DBA durante ese tiempo. Evite el uso de tablas protegidas en UDR de DBA.

Otras funciones de IDS con control de accesos basado en etiquetas

IDS tiene funciones que no son de seguridad que funcionan de modo totalmente integrado con el control de accesos basado en etiquetas.

El control de accesos basado en etiquetas (LBAC) de IDS está diseñado para funcionar correctamente con todas las partes del servidor de bases de datos y sin excesiva intervención del usuario para contener la exposición no autorizada de los datos. Las siguientes áreas de IDS se destacan para hacer frente a posibles asuntos problemáticos.

Clústeres de alta disponibilidad

Los clústeres de alta disponibilidad (Duplicación de datos de alta disponibilidad, servidores secundarios de disco compartido y servidores secundarios autónomos remotos) proporcionan una o más copias del servidor de bases de datos. Los objetos LBAC creados en una base de datos del servidor primario se duplican en los servidores secundarios. Todas las tablas protegidas en el servidor primario también se protegerán en los servidores secundarios.

Consultas distribuidas

IDS permite consultar más de una base de datos en el mismo servidor de bases de datos o entre diversos servidores de bases de datos. Este tipo de consulta se conoce como una consulta distribuidas. Las reglas de LBAC se aplicarán a las consultas distribuidas que impliquen tablas protegidas y sinónimos locales de tablas protegidas remotas. Las consultas emitidas desde un servidor no LBAC pero que

impliquen tablas protegidas por LBAC en un servidor diferente también requerirán que el usuario disponga de las credenciales de LBAC necesarias para acceder a los datos protegidos en el otro servidor.

Fragmentación

La fragmentación es una característica del servidor de bases de datos que permite controlar qué datos se almacenan a nivel de tabla utilizando una estrategia de fragmentación. IDS garantiza que las tablas de origen y de destino tengan los objetos de seguridad LBAC idénticos necesarios para adjuntar y separar fragmentos.

Sinónimos y vistas

Se pueden crear vistas y sinónimos en tablas y vistas existentes que residen en la base de datos actual o en otra base de datos del servidor de bases de datos local o de un servidor de bases de datos remoto. Cuando un usuario intente acceder a datos mediante vistas y sinónimos en tablas protegidas se aplicarán las reglas de LBAC.

Tablas de violaciones

IDS proporciona un recurso para realizar un seguimiento de filas que violan restricciones. La sentencia START VIOLATIONS TABLE crea una tabla de violaciones especial que contiene filas disconformes que no satisfacen las restricciones e índices exclusivos durante operaciones de inserción (INSERT), actualización (UPDATE) y supresión (DELETE) sobre tablas de destino. Para impedir la exposición no autorizada de datos protegidos mediante una tabla de violaciones, IDS protege la tabla de violaciones con la misma política de seguridad que la tabla de destino cuando se ejecuta la sentencia START VIOLATIONS TABLE.

Exploraciones de integridad referencial

Cuando se especifica la opción ON DELETE CASCADE y cuando una sentencia INSERT para una tabla hijo genera una exploración de integridad referencial sobre la tabla padre, se aplican las reglas de LBAC.

Parte 2. Auditoría de la seguridad de los datos

Esta sección trata sobre cómo auditar la seguridad de la base de datos.

Capítulo 7. Visión general de la auditoría

Este capítulo proporciona una visión general de la auditoría y de la terminología de auditoría. Describe los sucesos de auditoría, explica de modo detallado cómo se configuran y se utilizan las máscaras de auditoría e indica cómo realizar el análisis de auditoría. También ofrece una introducción a los distintos roles de administración de auditoría.

Recurso de auditoría de seguridad

La auditoría crea un registro de actividades seleccionadas que los usuarios realizan. Un administrador de auditoría se analiza el seguimiento de auditoría o de utilizar estos registros con los siguientes objetivos:

- Detectar acciones del usuario inusuales o sospechosas e identificar a los usuarios específicos que han realizado estas acciones
- Detectar intentos de acceso no autorizados
- Evaluar daños de seguridad potenciales
- Proporcionar pruebas en investigaciones, si es necesario
- Proporcionar una medida de disuasión pasiva frente a las actividades no deseadas, siempre que los usuarios sepan que sus acciones pueden estar sometidas a auditoría

Importante: Asegúrese de que los usuarios sepan que cada acción que realicen sobre la base de datos se puede auditar y que se les puede responsabilizar de dichas acciones.

No se puede utilizar la auditoría para realizar un seguimiento de las transacciones para reconstruir una base de datos. El servidor de bases de datos tiene recursos de archivado y de copia de seguridad con este objetivo. La publicación *IBM Informix Guía de copia de seguridad y restauración* explica estos recursos.

Sucesos de auditoría

Cualquier actividad u operación del servidor de bases de datos que puede potencialmente modificar o revelar datos o la configuración de la auditoría se considera un *suceso*. El recurso de auditoría de seguridad del servidor de bases de datos permite auditar y llevar un registro de los sucesos tanto si resultan satisfactorios como si resultan anómalos o simplemente cuando se intenta realizar la actividad en cuestión. Puede identificar cada suceso de auditoría por el código de suceso de cuatro o cinco letras denominado *mnemónico del suceso de auditoría*. En el Capítulo 11, "Mnemónicos y campos de los sucesos de auditoría", en la página 11-1 se listan los mnemónicos de sucesos de auditoría y se describen los sucesos que se pueden auditar con el recurso de auditoría de seguridad.

Puede especificar los sucesos que desee auditar en una *máscara de auditoría*. La auditoría se basa en la noción de los sucesos de auditoría y las máscaras de auditoría.

Máscaras de auditoría

Las máscaras de auditoría especifican los sucesos que el servidor de bases de datos debe auditar. En una máscara se puede incluir cualquier suceso. Las máscaras se

asocian con ID de usuario, de modo que se registran las acciones especificadas que un ID de usuario realiza. Las máscaras globales **_default**, **_require** y **_exclude** se especifican para todos los usuarios del sistema.

Antes de utilizar la auditoría, debe especificar qué sucesos de auditoría se deben auditar. Para especificar sucesos auditados, añada los sucesos a las máscaras. También debe realizar otras tareas, que se describen en el Capítulo 8, "Administración de la auditoría", en la página 8-1.

El servidor de bases de datos no proporciona auditoría para objetos ni para procesos. Por ejemplo, no se puede solicitar al servidor de bases de datos que audite todos los intentos de acceso a un determinado objeto. No obstante, puede filtrar registros de auditoría del seguimiento de auditoría basándose en objetos con las herramientas de análisis de auditoría, que se describen en el Capítulo 9, "Análisis de auditoría", en la página 9-1.

La Figura 7-1 representa un conjunto de máscaras de auditoría. Las máscaras reales y sus características se explican en el apartado "Máscaras de auditoría e instrucciones de auditoría" en la página 7-5.

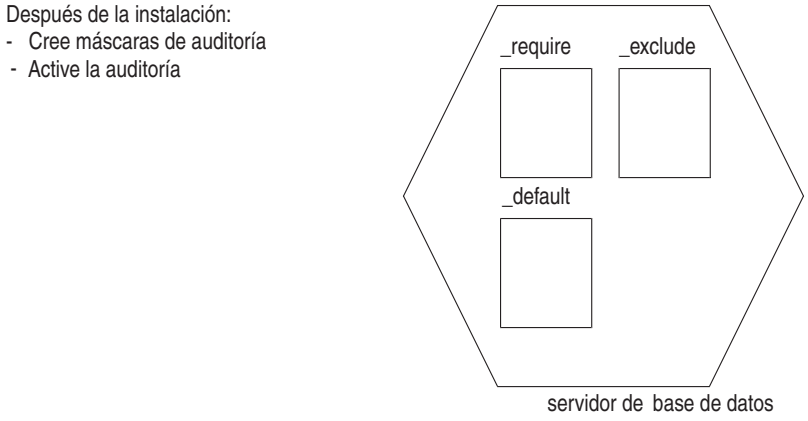


Figura 7-1. Máscaras de auditoría tras la instalación

Una vez finalizada la instalación, puede crear las máscaras de auditoría y activar la auditoría.

Importante: Si la auditoría está desactivada, el servidor de bases de datos no auditará ningún suceso, aunque se hayan especificado sucesos en las máscaras.

Además de las tres máscaras que se muestran en la Figura 7-1, puede especificar *máscaras de usuario* para usuarios individuales. Las máscaras de usuario permiten auditar a algunos usuarios más que otros y centrarse en tipos de actividades diferentes para usuarios diferentes. A excepción del administrador de la auditoría que realiza el mantenimiento de las máscaras, un usuario no puede saber qué sucesos se están auditando. Para obtener una descripción de las máscaras de usuario, consulte el apartado "Máscaras de usuario" en la página 7-6.

También puede crear *máscaras de plantilla* para crear nuevas máscaras de usuario. Para obtener una descripción de las máscaras de plantilla, consulte el apartado "Máscaras de plantilla" en la página 7-7.

Las máscaras y sus sucesos se denominan *instrucciones de auditoría*, tal como se muestra en la Figura 7-2. La flexibilidad por lo que respecta a las facetas auditables de Dynamic Server es considerable. Puede seleccionar cualquier opción, desde las instrucciones de auditoría mínimas, en las que no se audita ningún suceso, hasta las inserciones de auditoría máximas, en las que se auditan todos los sucesos del servidor de bases de datos relevantes por lo que respecta a la seguridad correspondientes a todos los usuarios.

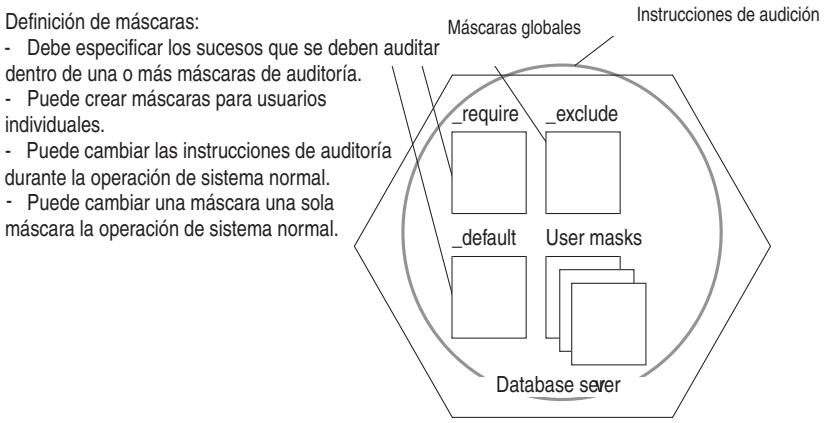


Figura 7-2. Instrucciones de auditoría

Después de definir las instrucciones de auditoría y activar la auditoría, puede modificar una o varias máscaras de auditoría según sus necesidades e identificar amenazas para la seguridad potenciales. Para obtener información sobre cómo cambiar máscaras de auditoría, consulte el Capítulo 8, "Administración de la auditoría", en la página 8-1.

Proceso de auditoría

Cuando se activa la auditoría, el servidor de bases de datos genera *registros de auditoría* para cada suceso que las instrucciones de la auditoría especifican, tal como se muestra en la Figura 7-3 en la página 7-4.

El servidor de bases de datos almacena los registros de auditoría en un archivo llamado *archivo de auditoría*, tal como se muestra en la Figura 7-3 en la página 7-4. La colección de registros de auditoría constituye el *seguimiento de auditoría*. (El seguimiento de auditoría puede constar de más de un archivo de auditoría).

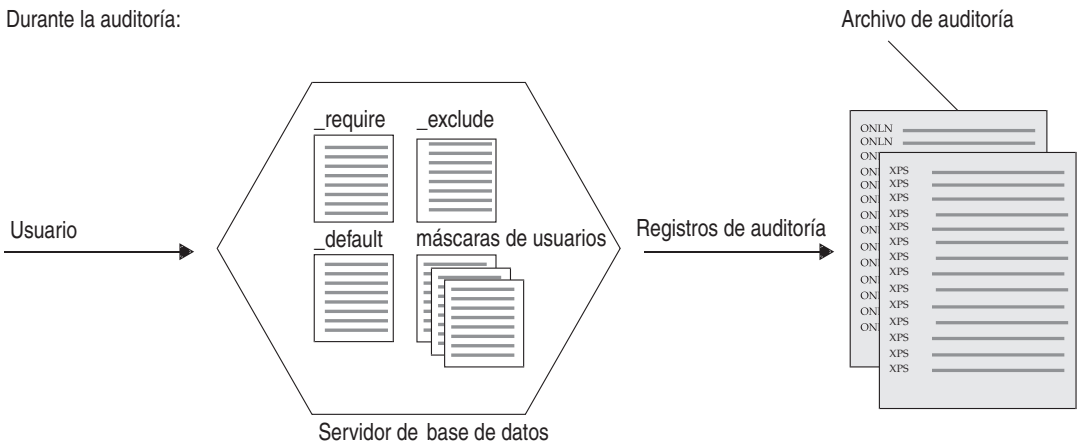


Figura 7-3. Proceso de auditoría

Un administrador de auditoría debe especificar y mantener la *configuración de la auditoría*, que incluye la siguiente información:

- La modalidad de auditoría
- Cómo se comporta el servidor de bases de datos si detecta un error al grabar registros de auditoría en el seguimiento de auditoría
- Para UNIX, el directorio en el que se encuentra el seguimiento de auditoría
- Para UNIX, el tamaño máximo que puede alcanzar un archivo de auditoría antes de que el servidor de bases de datos inicie automáticamente otro archivo de auditoría .

Estos temas se explican en el apartado "Configuración de la auditoría" en la página 7-10.

El servidor de bases de datos genera registros de auditoría y los graba en el archivo de auditoría o en un registro cronológico de sucesos independientemente de si el usuario cliente que realiza la acción auditada es local o remoto. El servidor de bases de datos incluye tanto el nombre de inicio de sesión del usuario como el nombre del servidor de bases de datos en cada registro de auditoría para ayudar a determinar qué persona específica ha iniciado una acción y dicha acción.

En los clústeres de alta disponibilidad, sólo el servidor de bases de datos primario realiza la auditoría de seguridad y produce un seguimiento de auditoría. El programa de utilidad **onaudit** se ejecuta en los servidores secundarios pero no audita ninguno de los sucesos de auditoría.

Seguimiento de auditoría

Revise el seguimiento de auditoría periódicamente. El servidor de bases de datos ofrece un programa de utilidad de extracción de datos, **onshowaudit**, que se puede utilizar para seleccionar datos de auditoría correspondientes a usuarios o servidores de bases de datos específicos.

Después de extraer datos, puede especificar que se les debe dar formato para cargarlos en una base de datos para su posterior manipulación mediante SQL. En el apartado "Visión general del análisis de auditoría" en la página 7-16 se explica este proceso.

Roles para la administración del servidor de bases de datos y de la auditoría

El administrador del sistema operativo (OSA) puede configurar los siguientes roles para la administración del servidor de bases de datos y la administración de la auditoría, además de los roles administrativos que pueda tener el sistema operativo:

- El Administrador del servidor de bases de datos (DBSA) mantiene y ajusta el servidor de bases de datos
- Un administrador de auditoría puede tener cualquiera de los dos roles siguientes o ambos:
  - Responsable de seguridad del sistema de base de datos (DBSSO), que especifica y mantiene las máscaras de auditoría
  - Responsable del análisis de auditoría (AAO), que activa y desactiva la auditoría, configura y mantiene la configuración de la auditoría y lee y analiza los datos del seguimiento de auditoría

Aunque la separación de roles proporciona una auditoría más segura, estos roles son opcionales. Antes de instalar el software de servidor de bases de datos, el OSA, o quien instale el servidor de bases de datos, decide si los roles de DBSSO y AAO deben estar separados o se deben combinar para la administración de la auditoría y quién debe desempeñar cada rol.

Para obtener información detallada sobre los roles y la separación de roles, consulte el apartado "Separación de roles" en la página 8-4. Para obtener información sobre cómo configurar la separación de roles y crear un grupo de usuarios para cada rol, consulte la publicación *IBM Informix Guía de instalación*.

Máscaras de auditoría e instrucciones de auditoría

Tal como se describe en el apartado "Máscaras de auditoría" en la página 7-1, una *máscara de auditoría* especifica un conjunto de sucesos que se deben auditar cuando un usuario los realiza. Los sucesos de auditoría se derivan de una combinación de máscaras de usuario y globales. En el Capítulo 11, "Mnemónicos y campos de los sucesos de auditoría", en la página 11-1 se ofrece una lista del conjunto de sucesos que se pueden auditar. El conjunto de sucesos es fijo, pero puede utilizar máscaras para especificar sólo los que necesite auditar.

La tabla siguiente ofrece una lista de los cuatro tipos de máscaras de auditoría.

Tipo de máscara
Nombre de la máscara

Máscaras de usuarios individuales
nombre_usuario

Máscara predeterminada
_default

Máscaras globales
_require y **_exclude**

Máscaras de plantilla
_nombre_máscara

La sección siguiente describe los tres primeros tipos de máscaras. Para obtener una descripción de las máscaras de plantilla, consulte el apartado “Máscaras de plantilla” en la página 7-7.

Máscaras de usuario

Las máscaras globales siempre se aplican a acciones de usuario que se realizan durante una sesión en la que la auditoría está activada. Las máscaras de auditoría se aplican en el siguiente orden:

1. Una máscara de usuario individual o, si no hay ninguna, la máscara **_default**
2. La máscara **_require**
3. La máscara **_exclude**

Cuando un usuario inicia el acceso a una base de datos, el servidor de bases de datos comprueba si existe una máscara de usuario individual con el mismo *nombre_usuario* que la cuenta que el usuario utiliza. Si existe una máscara de usuario individual, el servidor de bases de datos leerá las instrucciones de auditoría de ésta en primer lugar y pasará por alto la máscara **_default**. Si no existe ninguna máscara de usuario individual, el servidor de bases de datos leerá y aplicará las instrucciones de auditoría de la máscara **_default** para el usuario en cuestión.

Además de las máscaras predeterminada e individual, el servidor de bases de datos lee y aplica las instrucciones de auditoría de las máscaras **_require** y **_exclude**. Estas máscaras son *globales* porque se aplican a todos los usuarios. Los sucesos de auditoría de la máscara **_require** se auditan, aunque no se encuentren en las máscaras **_default** o de usuarios individuales. Los sucesos de auditoría de la máscara **_exclude** no se auditan, aunque las máscaras leídas anteriormente los requieran específicamente.

Importante: Si las instrucciones de auditoría de estas máscaras estén en conflicto, se utilizarán las instrucciones de la última máscara que se lea. Las máscaras se leen en el orden siguiente: *nombre_usuario*, **_default**, **_require** y **_exclude**.

Los usuarios no pueden saber si existen máscaras de usuario individual para sus cuentas. Asimismo, no es necesario que los usuarios hagan nada para habilitar la auditoría de sus acciones. Cuando un administrador de auditoría active la auditoría, ésta funcionará automáticamente y los usuarios no podrán inhabilitarla.

Cuando se instala el servidor de bases de datos, no existen máscaras de auditoría. Un administrador de auditoría debe especificar todas las máscaras, incluidas la máscara predeterminada y las máscaras globales.

Importante: Las acciones que al *DBSA*, un administrador de auditoría o un usuario **informix** realiza normalmente son potencialmente peligrosas para la seguridad del servidor de bases de datos. Para reducir el riesgo de abuso de la cuenta **informix** por parte de un usuario malintencionado, se recomienda auditar siempre las acciones de **informix**. Este procedimiento tiene como objetivo evitar que un usuario malintencionado utilice **informix** para interferir con la auditoría o que otorgue acceso discrecional a otro usuario malintencionado.

Máscaras de plantilla

A medida que se vaya acostumbrando a los tipos de auditoría que parezcan útiles para su sitio, es posible que se dé cuenta de que determinadas prácticas de auditoría se producen repetidamente. Puede crear máscaras de auditoría de *plantilla* para ayudar a configurar la auditoría para situaciones que se repiten o para distintos tipos de usuarios.

Por ejemplo, puede definir una máscara de plantilla denominada **_guest** y copiarla en máscaras de usuario individual correspondientes a personas que utilizan el servidor de bases de datos durante períodos breves. Puede copiar una máscara de plantilla en una máscara de usuario y modificarla al mismo tiempo; por ejemplo, desactivando sucesos que se auditaban en la máscara de plantilla.

Importante: Todos los nombres de máscara de plantilla deben ser exclusivos, deben contener menos de ocho caracteres y empezar con un símbolo de subrayado (_). Estas reglas de denominación distinguen las máscaras de plantilla de las máscaras de usuarios individuales.

No se pueden crear máscaras de plantilla con los nombres siguientes porque el servidor de bases de datos ya los utiliza:

- **_default**
- **_require**
- **_exclude**

Cuando se instala el servidor de bases de datos, no existen máscaras de plantilla. El número de máscaras de plantilla que se pueden crear es ilimitado.

Instrucciones de auditoría

Un ministro de auditoría establece las instrucciones de la auditoría que el servidor de bases de datos realiza. El administrador debe establecer un nivel de auditoría que sea suficientemente completo para resultar útil pero no tan exhaustivo como para repercutir negativamente sobre los recursos del sistema. Cuando existe la separación de roles, el DBSSO crea máscaras de auditoría y el AAO configura la auditoría obligatoria para el DBSA y el DBSSO. Puede encontrar consejos sobre cómo establecer las instrucciones de auditoría en la publicación *A Guide to Understanding Audit in Trusted Systems* (publicada por National Computer Security Center, NCSC-TG-001, junio de 1988).

Esta sección recomienda cómo seleccionar los sucesos que se deben auditar, cómo establecer las instrucciones de auditoría y cómo repercuten sobre el rendimiento las opciones seleccionadas. Para obtener información detallada sobre cómo crear y modificar máscaras de auditoría, consulte el Capítulo 8, "Administración de la auditoría", en la página 8-1.

Todas las máscaras de auditoría que el servidor de bases de datos utiliza se almacenan en la tabla **sysaudit** de la base de datos **sysmaster** de la interfaz de supervisión del sistema (SMI). Las máscaras se actualizan automáticamente cuando el servidor de bases de datos se actualiza a una versión más nueva. Aunque la información almacenada en la base de datos **sysmaster** está disponible mediante SQL, debe utilizar el programa de utilidad **onaudit** para todas las tareas de creación y mantenimiento de máscaras de auditoría. (Consulte el Capítulo 10, "Sintaxis del programa de utilidad", en la página 10-1). Consulte también la descripción de la base de datos **sysmaster** en la publicación *IBM Informix Administrator's Reference*.

Implicaciones sobre los recursos y el rendimiento

El nivel de auditoría del servidor de bases de datos habilitado en cualquier momento específico tiene una repercusión directa sobre los recursos del sistema operativo y el rendimiento del servidor de bases de datos. Los registros de auditoría que el servidor de bases de datos genera se almacenan en el disco. Como mayor sea el número de registros de auditoría generados, más espacio de disco se necesitará (para el almacenamiento) y más cantidad de tiempo de CPU se necesitará para procesar los registros de auditoría (para el almacenamiento, la visualización, la supresión, el archivado y la restauración).

El modo en que los recursos del sistema y el rendimiento se ven afectados depende de los factores siguientes:

- El número de usuarios/sucesos auditados
- La configuración del procesador
- La carga del sistema y de los usuarios
- El espacio disco
- La carga de trabajo

Por ejemplo, un sistema con posibilidades de proceso en paralelo, varios terabytes despacio disco disponible, 64 usuarios y puede experimentar poca degradación del rendimiento y una proporción de espacio de disco relativamente pequeña para los datos de auditoría. No obstante, una configuración de un solo procesador con poco espacio de disco, múltiples usuarios y auditoría completa puede experimentar una degradación importante de los recursos del sistema y un consumo del espacio de disco relativamente rápido por parte del seguimiento de auditoría.

Desde el punto de vista del rendimiento del sistema, la sobrecarga más grande se produce cuando se auditan todos los sucesos relacionados con la seguridad del servidor de base de datos que todos los usuarios realizan. La auditoría completa puede degradar gravemente el rendimiento del sistema y el tiempo de respuesta y exigir una cantidad importante de espacio disco para el almacenamiento de registros de auditoría (según la cantidad de actividad de los usuarios del servidor de bases de datos). No obstante, la auditoría completa proporciona la mayor cantidad de información de auditoría y, por lo tanto, reduce el riesgo para la seguridad.

Puede desactivar la auditoría para eliminar la repercusión sobre el rendimiento del sistema, pero entonces la auditoría no podrá contribuir a la seguridad del sistema. Como mínimo, debe auditar el inicio de nuevas sesiones de usuario.

El suceso del servidor de bases de datos que, si se audita, tiene la repercusión más importante sobre el rendimiento del sistema y el espacio disco es Read Row (RDRW) (Leer fila). En una base de datos establecida a la que accedan principalmente usuarios que buscan información, cada fila presentada a cada usuario genera un registro de auditoría. En un sistema con un volumen elevado, esto produce rápidamente grandes cantidades de registros de auditoría,

Consideraciones especiales sobre la auditoría

Determinadas organizaciones de certificación y acreditación requieren que se realice una auditoría del propio proceso de instalación. Después de configurar el sistema operativo para que acepte datos de auditoría, el OSA debe asegurarse de que el AAO audite las acciones que se realicen durante la instalación.

Nivel de granularidad de la auditoría

El recurso de auditoría de seguridad de Dynamic Server puede auditar los siguientes sucesos a nivel de fragmento de granularidad y muestra información adicional de los objetos fragmentados:

- **Alter Table (ALTB) (Modificar tabla).** La lista de particiones que va a continuación de la operación de modificación de tabla está en el registro de sucesos.
- **Create Index (CRIX) (Crear índice).** El índice se puede fragmentar; el registro de sucesos incluye información de fragmentación.
- **Create Table (CRTB) (Crear tabla).** La tabla se puede fragmentar; el registro de sucesos incluye información de fragmentación.
- **Delete Row (DLRW) (Suprimir fila).** La partición y el ID de registro que hay en la partición aparecen en el registro de sucesos.
- **Insert Row (INRW) (Insertar fila).** La partición y el ID de registro que hay en la partición aparecen en el registro de sucesos.
- **Read Row (RDRW) (Leer fila).** La partición y el ID de registro que hay en la partición aparecen en el registro de sucesos.
- **Update Row (UPRW) (Actualizar fila).** La partición y el ID de registro que hay en la partición aparecen en el registro de sucesos.

Atención: Utilice la auditoría a nivel de fila sólo cuando resulte absolutamente necesaria. La auditoría a nivel de fila ralentiza drásticamente el servidor de bases de datos y llena rápidamente los directorios de auditoría.

Para obtener más información sobre los campos de un registro de suceso de auditoría, consulte el Capítulo 11, "Mnemónicos y campos de los sucesos de auditoría", en la página 11-1.

Además, el servidor de bases de datos audita los siguientes sucesos al nivel de RESTRICT/CASCADE:

- Drop Table (DRTB) (Eliminar tabla)
- Drop View (DRVW) (Eliminar vista)
- Revoke Table Access (RVTB) (Revocar acceso a tabla)

Para obtener más información sobre las correspondientes sentencias de SQL, consulte la publicación *IBM Informix Guide to SQL: Syntax*.

Uso de diversas máscaras

La máscara **_require** puede ser una herramienta valiosa porque audita los sucesos especificados en esta máscara correspondientes a cada usuario del servidor de bases de datos. Puede utilizar esta máscara para realizar la mayor parte de la auditoría. La máscara **_require** permite realizar cambios rápidos en las configuraciones de la auditoría para todos los usuarios añadiendo o eliminando elementos de esta máscara.

La máscara **_exclude** también resulta útil. Se lee en último lugar, de modo que su contenido tiene prioridad sobre las instrucciones de las otras máscaras. Tal como su nombre indica, los sucesos de auditoría que se especifican en la máscara **_exclude** se excluyen de la auditoría. Esta exclusión se aplica a todos los sucesos, incluidos los especificados en la máscara **_require**. El suceso de auditoría Read Row (Leer fila), por ejemplo, es un buen candidato para la máscara **_exclude**. Read Row es un suceso común que puede generar grandes cantidades de datos potencialmente inútiles en el seguimiento de auditoría.

El modo de utilizar las máscaras **_default** y de usuarios individuales depende del número de usuarios y de sus actividades. Por ejemplo, si sólo tiene unos cuantos usuarios, es recomendable asignarle a cada uno una máscara individual. Entonces puede utilizar la máscara **_default** para auditar sucesos iniciados por usuarios que normalmente no utilizan la base de datos y configurar la máscara **_default** con un nivel de seguridad elevado. Para contrarrestar los posibles efectos negativos sobre el rendimiento del sistema, configure máscaras de usuario individual menos exhaustivas para los usuarios frecuentes. O bien, si tiene muchos usuarios y no desea crear muchas máscaras de usuario individual, deje la máscara **_default** vacía y recurra a la máscara **_require** para la mayor parte de la auditoría.

Configuración de la auditoría

El AAO puede supervisar la configuración de la auditoría, tal como se describe en el Capítulo 8, "Administración de la auditoría", en la página 8-1. Para establecer la configuración de la auditoría, se deben realizar las siguientes tareas:

- Activar o desactivar la auditoría
- Especificar modalidades de auditoría
- Utilizar el archivo **ADTCFG**
- En UNIX, determinar las propiedades de los archivos de auditoría

Las secciones siguientes describen estos temas.

Activación o desactivación de la auditoría

Un administrador de auditoría determina si la auditoría está activada o desactivada. La auditoría se desactiva de modo predeterminado cuando se instala el servidor de bases de datos. Tal como se describe en el Capítulo 8, "Administración de la auditoría", en la página 8-1, el AAO puede activar y desactivar la auditoría en cualquier momento utilizando el programa de utilidad **onaudit**, que se describe en el Capítulo 10, "Sintaxis del programa de utilidad", en la página 10-1. El servidor de bases de datos puede estar tanto en modalidad en línea como sin actividad para que los cambios entren en vigor.

Cuando el AAO activa la auditoría, todas las sesiones, nuevas y actuales, empiezan a auditar los sucesos auditables. Tanto las sesiones existentes como las nuevas producen registros. Todas las sesiones de usuario que se inician a partir de entonces también producen registros de auditoría.

De modo similar, cuando el AAO desactiva la auditoría, se detiene la auditoría para todas las sesiones existentes y las sesiones nuevas no se auditan. Si el AAO desactiva la auditoría y luego la vuelve activar mientras el servidor de bases de datos está en modalidad en línea, las sesiones existentes se reanudan y producen registros de auditoría.

Tipos de auditoría

Cuando el AAO activa la auditoría, el AAO puede establecer el parámetro ADTMODE en el archivo **ADTCFG** para especificar el tipo y el nivel de auditoría.

Para obtener información detallada, consulte el apartado "Cambio de la configuración de la auditoría" en la página 10-7 y el Capítulo 12, "El archivo ADTCFG", en la página 12-1. Para obtener más información sobre la administración de la auditoría, consulte el apartado "Roles administrativos y separación de roles" en la página 8-1.

Modalidades de auditoría

Al activar la auditoría, puede establecer el parámetro ADTMODE en el valor `0`, `1`, `3`, `5` o `7` en el archivo **ADTCFG** para especificar el tipo y el nivel de auditoría.

Por ejemplo, si establece `1` como valor del parámetro ADTMODE en el archivo **ADTCFG**, la auditoría se activará automáticamente durante la inicialización del servidor de bases de datos. Una vez activada la auditoría, el servidor de bases de datos sólo registrará los sucesos de auditoría definidos en las máscaras de auditoría.

El AAO configura la auditoría y especifica una modalidad de error por si se produce un error al almacenar un registro de auditoría.

Propiedades de los archivos de auditoría en UNIX

Tal como se describe en el apartado "Proceso de auditoría" en la página 7-3, con auditoría gestionada por el servidor de bases de datos en UNIX, el servidor de bases de datos graba registros de auditoría para auditar archivos en el seguimiento de auditoría. Esta sección describe los archivos de auditoría de modo más detallado.

Ubicación de los archivos de auditoría

Los archivos de auditoría están ubicados en un directorio que se especifica con el programa de utilidad **onaudit** o el parámetro de configuración ADTPATH en el archivo **$INFORMIXDIR/aaodir/adtcfg** de UNIX.

Si cambia la vía de acceso de la auditoría, el cambio entrará en vigor inmediatamente para todas las sesiones existentes. Esta característica permite cambiar el directorio cuando el servidor de bases de datos está en modalidad en línea, lo que resulta útil si el sistema de archivos que contiene los archivos de auditoría existentes se llena.

Mantenga limpio el sistema de archivos que contiene el seguimiento de auditoría para que siempre haya disponible un espacio de almacenamiento amplio.

Archivos de auditoría nuevos

Cuando el servidor de bases de datos graba un registro de auditoría, el servidor de bases de datos añade el registro al archivo de auditoría actual. Si se saca el servidor de bases de datos de la modalidad en línea y luego se vuelve a poner en modalidad en línea, el servidor de bases de datos continuará utilizando el mismo archivo de auditoría. El servidor de bases de datos inicia un archivo de auditoría nuevo sólo en las condiciones siguientes:

- Cuando el archivo alcanza un tamaño especificado
- Cuando se indica manualmente al servidor de bases de datos que debe iniciar un archivo de auditoría nuevo, tal como se describe en el Capítulo 8, "Administración de la auditoría", en la página 8-1
- Cuando se inicia la auditoría gestionada por el servidor de bases de datos

El servidor de bases de datos inicia un archivo de auditoría nuevo al tamaño predeterminado de 10.240 bytes, que es el tamaño mínimo para los archivos de auditoría. (El archivo **adtcfg.std** puede listar un valor de 50.000 bytes como directriz). Puede cambiar el tamaño de este archivo en cualquier momento cuando la auditoría esté activada auditoría, incluso cuando el servidor de bases de datos

grabe en un archivo de auditoría, tal como se describe en el Capítulo 10, “Sintaxis del programa de utilidad”, en la página 10-1.

El tamaño óptimo de los archivos de auditoría depende de la configuración. Los archivos más grandes contienen más datos, lo que tiene como resultado una cantidad inferior de archivos para revisar. No obstante, la contrapartida es que los archivos grandes son más difíciles de manipular.

Nombres de los archivos de auditoría

Independientemente de cómo se inicie un nuevo archivo de auditoría, seguirá el mismo convenio de denominación.

El convenio de denominación es *nombreservidorbd*.*entero*, donde *nombreservidorbd* es el nombre del servidor de bases de datos definido en el archivo **ONCONFIG** y *entero* es el siguiente entero. La serie empieza por `0`.

Por ejemplo, si se inicia un archivo de auditoría nuevo para un servidor de bases de datos **maple** y el último archivo de auditoría se ha guardado en el archivo **maple.123**, el siguiente archivo de auditoría se denominará **maple.124**. Si **maple.124** ya existe, se utilizará el siguiente número disponible. Los nombres son exclusivos para un directorio de auditoría específico, de modo que se puede tener **auditdir1/maple.123** y **auditdir2/maple.123**, etc.

Registro cronológico de sucesos de aplicación de Windows

Los sistemas Windows proporcionan un recurso de registro cronológico de sucesos como repositorio común para el registro cronológico de sucesos y otra información útil. El recurso de registro cronológico de sucesos también proporciona una interfaz para filtrar, ver y hacer una copia de seguridad de la información allí almacenada.

En las versiones de Windows anteriores a Windows XP, las aplicaciones con permisos apropiados podían grabar en el registro de seguridad y en el registro del sistema. En Windows XP y versiones posteriores, no obstante, las aplicaciones no pueden grabar en el registro cronológico de sucesos de sucesos de seguridad de Windows. Los mensajes de auditoría del servidor de bases de datos se envían ahora a un archivo de registro cuya vía de acceso de directorio se puede especificar utilizando el programa de utilidad **onaudit**. El nombre de vía de acceso predeterminado es **%INFORMIXDIR%\aaodir**.

Cualquier mensaje que el servidor de bases de datos graba en su archivo de registro también se graba en el registro cronológico de sucesos de aplicación de Windows.

Servidor de mensajes de Windows

Dynamic Server para Windows se ejecuta como un servicio con la cuenta de usuario **informix**.

El servicio **Servidor de mensajes** de Dynamic Server se comunica con el servidor de bases de datos mediante el mecanismo de comunicaciones interproceso de conductos con nombre para recibir información y grabarla en el registro cronológico de sucesos de aplicación de Windows y también en el archivo de registro **%INFORMIXDIR%\%INFORMIXSERVER%.log**.

El servidor de bases de datos inicia el **Servidor de mensajes** la primera vez que el servidor de bases de datos necesita grabar un mensaje en registro cronológico de sucesos. El **Servidor de mensajes** no termina automáticamente al terminar una instancia del servidor de bases de datos.

Modalidad de error para grabar en un archivo de auditoría

Si el servidor de bases de datos detecta un error al grabar en el archivo de auditoría, puede comportarse de diversos modos que se conocen como *modalidades de error*. Puede cambiar la modalidad de error, tal como se describe en el apartado "Establecimiento de la modalidad de error" en la página 8-7, en cualquier momento durante el funcionamiento del servidor de bases de datos, incluso después de que se produzca un error. Consulte también la información sobre las modalidades de error de **onaudit** en el Capítulo 10, "Sintaxis del programa de utilidad", en la página 10-1.

Modalidades de error de parada

Cuando el servidor de bases de datos está en una modalidad de error de *parada* (1 ó 3), no permite que la sesión que ha recibido el error continúe con el proceso después de grabarlo en el seguimiento de auditoría. Incluso es posible que el servidor de bases de datos termine la sesión o se apague según la modalidad de error. A continuación se ofrecen descripciones de las modalidades de error de parada:

- Modalidad 1: Se suspende una hebra pero la sesión continúa cuando el registro de auditoría se graba satisfactoriamente.
- Modalidad 3: El servidor de bases de datos se cierra y la sesión del usuario no puede continuar.

El proceso de la sesión no continuará hasta que la condición de error se resuelva.

Modalidad de error de continuación

Cuando el servidor de bases de datos está en una modalidad de error de *continuar* (0), permite que la sesión que ha recibido el error continúe con el proceso después de grabarlo en el seguimiento de auditoría. No obstante, el registro de auditoría que se estaba grabando cuando se produjo el error se perderá. El servidor de bases de datos graba un error en el registro de mensajes que indica que se ha producido un error durante la grabación de un registro de auditoría.

Si el error se sigue produciendo, todos los intentos posteriores de grabar en el seguimiento de auditoría también generarán mensajes en el registro de mensajes, que puede crecer muy rápidamente hasta alcanzar un gran tamaño.

Configuración de la auditoría y el archivo ADTCFG

Los parámetros de configuración del archivo **ADTCFG** especifican las propiedades de la configuración de la auditoría. Estos parámetros de configuración son ADTERR, ADTMODE, ADTPATH y ADTSIZE.

A continuación va el nombre de la vía de acceso del archivo **ADTCFG**.

Entorno	**Vía de acceso de ADTCFG**
UNIX	**$INFORMIXDIR/aaodir/adtcfg**

Windows
%INFORMIXDIR%\aaodir\adtcfg

Si edita el archivo **ADTCFG** para cambiar parámetros de auditoría, la configuración de la auditoría no cambiará hasta que se reinicialice la memoria compartida. Si utiliza el programa de utilidad **onaudit** para cambiar la configuración de la auditoría, los cambios se producirán inmediatamente.

Los cambios realizados con **onaudit** se graban en un archivo asociado **adtcfg.*número_servidor***. (SERVERNUM es un parámetro del archivo **ONCONFIG**, que se describe en la publicación *IBM Informix Administrator's Reference*). Un administrador de auditoría debe copiar manualmente los cambios del archivo **adtcfg.*número_servidor*** al archivo **ADTCFG**. La finalidad es dificultar que el DBSA pueda iniciar una instancia del servidor de bases de datos con parámetros de auditoría no válidos. Para obtener información detallada sobre cómo utilizar el programa de utilidad **onaudit** para configurar el archivo **ADTCFG**, consulte el Capítulo 10, "Sintaxis del programa de utilidad", en la página 10-1.

Acceso al seguimiento de auditoría

Los usuarios estándar no deben poder ver ni modificar los archivos de auditoría. Sólo se debe poder acceder al seguimiento de auditoría (es decir, los archivos de auditoría) con el programa de utilidad **onshowaudit**, que tiene su propia protección, tal como se indica a continuación:

- Con la separación de roles activada, sólo un AAO puede ejecutar **onshowaudit**.
- Con la separación de roles desactivada en UNIX, sólo el usuario **informix**, un miembro del grupo **informix** o el usuario **root** pueden ejecutar **onshowaudit**.
- Con la separación de roles desactivada en Windows, sólo el usuario **informix** puede ejecutar **onshowaudit.**

Acceso a archivos de auditoría en UNIX

Las características siguientes controlan el acceso a archivos de auditoría en un entorno UNIX y los protegen frente a la lectura o la destrucción accidental:

Propiedad:
informix

ID de grupo:
igual que **$INFORMIXDIR/aaodir**

Permisos:
660

Importante: El AAO debe tener cuidado al seleccionar el directorio en el que se almacenan los archivos de auditoría (ADTPATH). Los directorios de la vía de acceso deben tener la propiedad y los permisos de acceso adecuados para el nivel de riesgo que el AAO permite. El directorio predeterminado (**/tmp**) no tiene la protección adecuada.

Los ejemplos siguientes muestran la configuración de la seguridad para los archivos de auditoría de UNIX sin separación de roles:

aaodir

Propiedad:
informix

ID de grupo:
informix

Permisos:
775

aaodir/adtcfg.std

Propiedad:
informix

ID de grupo:
informix

Permisos:
644

Los ejemplos siguientes muestran la configuración de la seguridad de UNIX con separación de roles:

aaodir

Propiedad:
informix

ID de grupo:
<*grupo_aao*>

Permisos:
775

aaodir/adtcfg.std

Propiedad:
informix

ID de grupo:
<*grupo_aao*>

Permisos:
644

Importante: Puesto que cualquier cuenta con propiedad del ID de grupo **informix** o del superusuario (**root**), o ambos, puede acceder al seguimiento de auditoría, se debe tener cuidado y proteger estas cuentas y sus contraseñas.

Acceso a registros de auditoría en Windows

Las siguientes características controlan el acceso al archivo de auditoría de Windows y lo protegen frente a la visualización o la supresión accidental:

Propiedad:
informix

ID de grupo:
igual que **%INFORMIXDIR%\aaodir**

Los ejemplos siguientes muestran cómo controlar el acceso al archivo de auditoría de Windows:

aaodir

Propiedad:
informix

ID de grupo:
Administrador

aaodir\adtcfg.std

Propiedad:
administrador del servidor de bases de datos

ID de grupo:
Administrador

Visión general del análisis de auditoría

El AAO realiza el análisis de auditoría. Esta sección explica la importancia del análisis de auditoría, cómo prepararse para éste, algunas estrategias para el análisis de auditoría y cómo reaccionar frente a un problema de seguridad detectado.

Importancia del análisis de auditoría

El mecanismo de auditoría del servidor de bases de datos está diseñado tanto para impedir como para revelar intentos de violación de la seguridad y violaciones de la seguridad que se hayan hecho efectivas. No obstante, los datos de auditoría que genera sólo resultan tan útiles como el análisis y las revisiones que se realizan sobre ellos. No revisar ni analizar nunca los datos de auditoría equivale a inhabilitar la auditoría por completo (y, de hecho, resulta aún peor porque la auditoría puede reducir el rendimiento del servidor de bases de datos).

Si, por el contrario, analiza y revisa rutinariamente los datos de auditoría, es posible que descubra actividad sospechosa antes de que se haga efectiva una violación. El primer paso para poner fina a una violación de la seguridad consiste en detectar el problema. Si se produjera una violación del servidor de bases de datos, el seguimiento de auditoría permitiría reconstruir los sucesos que condujeron a la violación, incluida ésta.

Consejo: Para desempeñar el rol más importante en la seguridad del servidor de bases de datos, observe la actividad del servidor de bases de datos con regularidad.

Acostúmbrese a los tipos de actividad que se producen en diversos momentos del día en su sitio. Se convertirá en un experto en los tipos de actividad del usuario cuando realice las acciones siguientes:

- Revise el seguimiento de auditoría de seguridad del servidor de bases de datos diariamente o más frecuentemente si es necesario.
- Anote los tipos de actividades que cada usuario realiza.

Compruebe periódicamente los tipos de sucesos que se auditan comparándolos con los sucesos que aparecen realmente en el seguimiento de auditoría de seguridad para garantizar que el recurso de auditoría funcione debidamente.

La observación continua del seguimiento de auditoría puede ser el único modo de determinar si algunos usuarios examinan el servidor de bases de datos. Puede detectar que un usuario realiza una cantidad de actividad a las 2 de la mañana, una hora del día en la que usuario no está en al trabajo. Cuando identifiqué una anomalía de seguridad potencial, podrá investigar más para determinar si alguien

en el servidor de bases de datos intenta obtener información para la que no tiene autorización, si un usuario realiza un uso inadecuado del servidor de bases de datos o si un usuario se vuelve indulgente por lo que respecta a la aplicación de la seguridad autorregulada.

Preparación para el análisis de auditoría

Esta sección describe dos métodos de analizar los registros de auditoría del servidor de bases de datos:

- El primer método consiste simplemente en visualizar los datos de auditoría tal como aparecen en el seguimiento de auditoría, que puede someter a sus propias herramientas de análisis de auditoría. Este método garantiza la precisión porque no se realiza ningún proceso sobre los registros de auditoría en bruto.
- El segundo método convierte los registros de auditoría a un formato que se puede cargar en una tabla gestionada por el servidor de bases de datos. Luego puede utilizar SQL para generar informes basados en estos datos. Con el método basado en SQL, puede crear y utilizar formularios e informes y visualizar selectivamente datos de auditoría, lo que proporciona un procedimiento de análisis de auditoría flexible y potente. No obstante, asegúrese de que no se supriman ni se modifiquen registros del archivo intermedio ni de la base de datos antes del análisis.

Importante: El procedimiento basado en SQL resulta más cómodo pero sigue sin ser fiable porque los usuarios pueden utilizar sentencias de manipulación de datos SQL para manipular los registros que se copian en una tabla.

Ambos métodos dependen de un programa de utilidad denominado **onshowaudit**, que se describe en el Capítulo 9, “Análisis de auditoría”, en la página 9-1 y en el Capítulo 10, “Sintaxis del programa de utilidad”, en la página 10-1. Para cualquiera de los dos métodos, puede extraer sucesos de auditoría correspondientes a bases de datos o usuarios específicos o a ambos.

La Figura 7-4 en la página 7-18 muestra el proceso de preparación para los dos métodos de análisis. En el Capítulo 9, “Análisis de auditoría”, en la página 9-1 se explica cada paso de modo detallado.

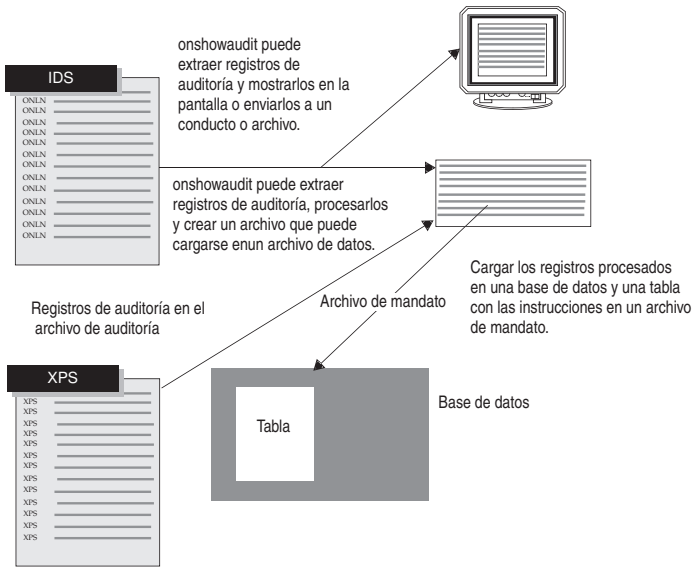


Figura 7-4. Preparación para el análisis de auditoría

Para realizar el análisis de auditoría, primero debe tener registros de auditoría en el servidor de bases de datos. El programa de utilidad **onshowaudit** no elimina datos del seguimiento de auditoría. Sólo lee registros del seguimiento de auditoría y permite visualizarlos o manipularlos con programas de utilidad SQL estándar.

Para borrar o eliminar registros de auditoría, suprima los archivos que contienen el seguimiento de auditoría.

Estrategias para el análisis de auditoría

La principal amenaza para la seguridad de un servidor de bases de datos es la divulgación o la modificación no autorizada de información confidencial. Esta sección trata sobre estas y otras amenazas que se pueden descubrir mediante el análisis de auditoría.

Anomalía de suceso

Los registros de auditoría que indican que una operación que se ha intentado realizar sobre el servidor de bases de datos ha fallado resultan especialmente importantes en el análisis de auditoría. El registro de auditoría puede indicar, por ejemplo, que un usuario está intentando proporcionar datos confidenciales a otro usuario que no tiene los permisos de UNIX correctos o los privilegios de acceso de Windows para acceder a los datos.

Éxito de suceso

Las operaciones que han resultado anómalas son los indicadores más comunes de un problema de seguridad en el seguimiento de auditoría. Las actividades satisfactorias pero inusuales de un determinado usuario resultan un poco más difíciles de encontrar, pero igual de importantes por lo que respecta a la seguridad.

Por ejemplo, un usuario que crea y elimina bases de datos repetidamente podría estar intentando descubrir y explotar un canal oculto para proporcionar información confidencial a un proceso o a un individuo no autorizado. Vigile los

aumentos considerables de la ocurrencia de sucesos del servidor de bases de datos que en condiciones normales se producirían con poca frecuencia durante el uso normal del servidor de bases de datos.

Quizás un determinado usuario que nunca haya otorgado privilegios muestra repentinamente mucha actividad en esta área o quizás un usuario que nunca ha grabado grandes cantidades de datos en una base de datos empieza a generar centenares de registros nuevos. Debe determinar el alcance de las anormalidades (por ejemplo, el número de objetos a los que ha accedido este usuario) y la posible gravedad del riesgo (por ejemplo, la importancia de los objetos a los que se ha accedido).

Ataque interno

Un *ataque interno* se produce cuando un usuario autorizado con intenciones maliciosas obtiene información confidencial y la facilita a usuarios no autorizados. Es posible que un usuario malintencionado de este tipo no muestre de un modo inmediato signos evidentes de un uso indebido del sistema. La auditoría es una contramedida para esta amenaza. Una auditoría minuciosa puede poner de manifiesto un ataque en curso o proporcionar pruebas de que un determinado individuo ha accedido a la información facilitada.

Examinar

Los usuarios que buscan entre los datos almacenados para localizar o adquirir información sin una necesidad legítima están *examinando*. Los buscadores no necesitan saber necesariamente si la información que están buscando existe ni su formato. Los buscadores ejecutan normalmente una gran cantidad de consultas similares, muchas de las cuales pueden fallar debido a que no tienen los privilegios suficientes. La auditoría es una contramedida para esta amenaza. El patrón de comportamiento hace que los buscadores resulten relativamente fáciles de identificar en el seguimiento de auditoría.

Agregación

Un *agregado* es una acumulación de información que se obtiene de una serie de consultas. Un agregado se convierte en una amenaza para la seguridad cuando consta de consultas a objetos que son poco significativos por sí mismos pero que, en su conjunto, proporcionan información que se considera más importante que cualquiera de los componentes individuales. La confidencialidad más elevada del agregado es la resultante de la confidencialidad de las asociaciones entre los componentes individuales. La auditoría es una contramedida para esta amenaza. Al igual que sucede con los usuarios buscadores, una auditoría minuciosa puede poner de manifiesto un ataque en curso o proporcionar pruebas de que un determinado individuo ha acumulado la información facilitada.

Respuestas a problemas de seguridad identificados

Después de identificar al usuario o los usuarios responsables de las irregularidades en el seguimiento de auditoría de seguridad, consulte los procedimientos de seguridad de su sitio. Si su sitio no tiene procedimientos de seguridad referentes a infracciones de seguridad potenciales, es recomendable que considere las siguientes acciones:

- Habilite la auditoría adicional para identificar el problema de modo más preciso.
- Apague el servidor de bases de datos para detener cualquier flujo de información no autorizado.

- Desarrolle un plan con el supervisor del usuario para hacer frente al problema.
- Haga frente al usuario en cuestión.

En algunos casos, es posible que encuentre que un usuario que sí que esté autorizado examina demasiado a fondo en el servidor de base de datos. Después de observar un poco más este comportamiento, es recomendable que hable con el supervisor del usuario. No es buena idea hablar directamente con un individuo cuyas acciones están supervisando.

Debe averiguar si un determinado problema identificado mediante el seguimiento de auditoría corresponde realmente a alguien que está intentando abrir una brecha en la seguridad o simplemente, por ejemplo, a un error de programación de una aplicación que se haya instalado recientemente.

El tipo exacto de irregularidad en la seguridad que se puede producir y la acción específica que se debe llevar a cabo como respuesta no forman parte de los temas a tratar en este manual.

Amenazas para la seguridad del sistema de gestión de bases de datos

Esta sección trata sobre las respuestas a distintos tipos de amenazas para la seguridad del sistema de gestión de bases de datos. Para obtener más información sobre diversos roles, consulte el apartado “Roles administrativos y separación de roles” en la página 8-1.

Amenazas principales

Entre las principales amenazas a la seguridad de un servidor de bases de datos se encuentran la divulgación o modificación no autorizada de información confidencial. Para contrarrestar estas medidas, el DBSSO, el DBSA y el OSA debe asegurarse de que todos los usuarios del sistema de gestión de bases de datos se identifiquen y se autentiquen para poder utilizar o acceder al software o a los datos.

Los usuarios deben pertenecer al grupo correcto para acceder al servidor de bases de datos. También deben tener un ID de inicio de sesión válido en el archivo de contraseñas del sistema operativo.

Además, todos los usuarios que intenten acceder a datos deben satisfacer las restricciones de DAC (Discretionary Access Control) para que se les otorgue el acceso. DAC utiliza sentencias de SQL para especificar qué usuarios pueden y no pueden acceder a datos de la base de datos. El acceso se puede permitir o revocar a los siguientes niveles:

- A nivel de base de datos
- A nivel de tabla
- A nivel de rutina SPL
- A nivel de rol
- A nivel de fragmentación

Estas contramedidas resultan adecuadas para el uso legítimo del producto cuando los usuarios intentan acceder a los datos directamente. No obstante, no pueden contrarrestar las amenazas de confidencialidad o modificación de los datos debidas al uso ilegítimo del producto, como por ejemplo si un usuario con privilegios abusa de sus permisos o privilegios de acceso.

Amenazas de actividad privilegiada

Las actividades indebidas o no comprobadas realizadas por usuarios con roles con privilegios (DBSSO, AAO, DBSA u OSA) pueden introducir en vulnerabilidades de seguridad y posibles amenazas para el servidor de bases de datos. Dynamic Server se ha diseñado cuidadosamente para proporcionar al DBSSO, al AAO y al DBSA sólo las capacidades necesarias para realizar sus trabajos. No obstante, estos roles, así como los de los administradores del sistema operativo, proporcionan suficiente poder para que el uso imprudente de dicho poder pueda tener como resultado brechas de seguridad.

Administrador del servidor de bases de datos

El DBSA controla y supervisa el servidor de bases de datos y puede configurar la separación de roles durante la instalación del servidor de bases de datos. La contramedida frente a una amenaza del DBSA es el escrutinio independiente del seguimiento de auditoría del sistema de gestión de bases de datos. El DBSSO puede habilitar la auditoría de todas las acciones del DBSA y el AAO puede revisar las acciones del DBSA en el seguimiento de auditoría.

Responsable de seguridad del sistema de base de datos

El DBSSO configura máscaras auditoría del sistema de gestión de bases de datos para usuarios individuales. La contramedida frente a una amenaza del DBSSO es el escrutinio independiente del seguimiento de auditoría del sistema de gestión de bases de datos porque el AAO habilita las acciones de auditoría del DBSSO.

Administrador del sistema operativo

Un OSA malintencionado también supone una grave amenaza para la seguridad porque el OSA puede violar los supuestos sobre el entorno del producto y los métodos que apuntalan sus funciones de seguridad. Al igual que sucede con un DBSSO, la contramedida a una amenaza del OSA es el escrutinio independiente de las actividades del OSA, registradas en el seguimiento de auditoría.

Responsable del análisis de auditoría

El AAO revisa el seguimiento de auditoría del sistema de gestión de bases de datos. La contramedida a esta amenaza consiste en asegurarse de que un AAO tenga autorización para ver información que se pueda proporcionar al revisar el seguimiento de auditoría de la base de datos. También es importante que la salida del programa de utilidad **onshowaudit** sólo resulte accesible para un AAO y que la manipulación de esta salida también se audite en el seguimiento de auditoría.

Amenazas para la memoria compartida en UNIX

Una conexión de memoria compartida proporciona un acceso rápido a un servidor de bases de datos si el cliente y el servidor están en el mismo sistema, pero supone algunos riesgos de seguridad. Aplicaciones falsas o no fiables podrían destruir o ver almacenamientos de mensajes de su propiedad o de otros usuarios locales. La comunicación de memoria compartida también resulta frente a los errores de programación si la aplicación cliente accede explícitamente a la memoria o sobreindexa matrices de datos.

El OSA garantiza que el método de conexión de memoria compartida no se especifique en el archivo de configuración para las conexiones cliente/servidor. Si

el cliente y el servidor están en el mismo sistema, un cliente puede conectarse a un servidor con una conexión de conducto de secuencias o con una conexión de bucle de retorno de red.

El nombre de la vía de acceso predeterminada para archivo de configuración en UNIX es **$INFORMIXDIR/etc/sqlhosts**.

Para obtener más información sobre las conexiones de memoria compartida, consulte la publicación *IBM Informix Administrator's Guide*.

Amenazas de software malicioso introducido

Un usuario normal puede ejecutar sin saberlo software malicioso como, por ejemplo, un troyano. Este software, por ejemplo, podría realizar una de las siguientes acciones:

- Intentar copiar datos para que un usuario no autorizado acceda a ellos posteriormente
- Otorgar privilegios de acceso DAC a un usuario no autorizado

Explique a todos los usuarios los peligros que entraña la ejecución de software de origen desconocido o no fiable. Además, siga los pasos que se indican a continuación:

- Todos los usuarios deben comprobar periódicamente la protección DAC del software con datos de los que sean propietarios para asegurarse de que no se hayan otorgado privilegios de acceso sin su conocimiento.
- El DAC del sistema operativo debe proteger el software frente a la modificación por parte de usuarios sin autorización.

Amenazas de acceso remoto

Cuando a una usuario se le otorgan privilegios de acceso DAC, el sistema principal del usuario no se especifica. Por lo tanto, el usuario puede obtener acceso a los datos con privilegios desde cualquier sistema que esté configurado para conectarse al sistema principal. En consecuencia, es posible que un usuario no sea consciente de que dispone de acceso remoto a datos con privilegios cuando el usuario otorga a otro usuario acceso directo a dichos datos. Esta situación puede provocar que haya datos a los que se acceda remotamente de modo inapropiado.

Asegúrese de que todos los usuarios sepan que los privilegios de acceso se otorgan a los nombres de usuario, sin depender del origen de la conexión remota.

Amenazas de usuarios obsoletos

Un usuario se identifica mediante un nombre de usuario o ID de usuario del sistema operativo o mediante ambos. Los privilegios de DAC y las máscaras de auditoría de usuarios individuales del software se basan en el nombre de usuario. Al nivel del sistema operativo, se podría eliminar una cuenta de usuario y este nombre de usuario quedaría sin asignar.

Si cualquiera de los privilegios de DAC del software o la máscara de auditoría del usuario individual asociada con dicho nombre de usuario no se eliminan antes de que el mismo nombre de usuario se asigne a un usuario nuevo, el usuario nuevo heredará sin saberlo los privilegios y la máscara de auditoría del usuario anterior.

Para evitar este problema, hará que el OSA envíe una notificación al DBSA cuando se elimine una cuenta de usuario del sistema operativo. Entonces, el DBSA podrá

realizar las acciones necesarias para eliminar referencias a este nombre en el sistema de gestión de bases de datos. Estas acciones pueden incluir la revocación de privilegios de DAC y la eliminación de una máscara de auditoría individual.

Software no fiable utilizado en un entorno con privilegios

Si los DBSA o los OSA ejecutan software no fiable, se pueden producir problemas. El software no fiable puede utilizar los privilegios del DBSA o el OSA para realizar acciones que pasen por alto o inhabiliten las funciones de seguridad del producto o que otorguen privilegios de acceso de DAC inapropiados.

La principal medida para hacer frente a esta vulnerabilidad consiste en asegurarse de los DBSA y los OSA no ejecuten software de origen desconocido o no fiable. También recomendamos que los controles de acceso del sistema operativo protejan todo el software que los DBSA y los OSA ejecuten frente a modificaciones no autorizadas.

Amenazas de configuración de bases de datos distribuidas

Al configurar una base de datos distribuida, configura dos o más instalaciones de software. Las configuraciones de estas instalaciones de software pueden ser incompatibles.

Un usuario de una base de datos distribuida podría ser capaz de obtener acceso a datos de un sistema remoto con una configuración incompatible cuando el mismo usuario no podría acceder directamente a dichos datos en el sistema remoto. En el peor de los casos, el software podría conectar dos sistemas que tuviesen una cuenta con el mismo nombre de usuario pero que fuesen propiedad de un usuario diferente. A cada usuario se le otorgan los privilegios del otro usuario al acceder a la base de datos que reside en el sistema principal del otro usuario.

Cuando dos estaciones de trabajo UNIX estén conectadas, el OSA debe asegurarse de que las cuentas con nombres de usuario en común sean propiedad del mismo usuario.

Capítulo 8. Administración de la auditoría

Este capítulo explica cómo configurar y administrar la auditoría en el servidor de bases de datos después una vez que el servidor de bases de datos se haya instalado y funcione correctamente. Este capítulo trata los temas siguientes:

- Roles administrativos y separación de roles
- Configuración de la auditoría
- Mantenimiento de máscaras de auditoría
- Mantenimiento de la configuración de la auditoría, incluida la desactivación de la auditoría

Roles administrativos y separación de roles

Esta sección describe los principales roles administrativos implicados en la auditoría segura:

- Administrador del servidor de bases de datos (DBSA)
- Roles de administrador de auditoría:
  - Responsable de seguridad del sistema de base de datos (DBSSO)
  - Responsable del análisis de auditoría (AAO)

Esta sección también trata sobre los roles y las responsabilidades de los administradores de bases de datos (DBA), los administradores del sistema operativo (OSA), los usuarios del sistema y los usuarios con privilegios. Explica cómo configurar la separación de roles y proporciona directrices sobre cómo asignar roles.

Administrador del servidor de bases de datos

El DBSA configura, mantiene y ajusta el servidor de bases de datos. El DBSA se implica en la seguridad de un servidor de bases de datos durante la instalación. La publicación *IBM Informix Administrator's Guide* define el rol general del DBSA.

Este rol lo debe desempeñar alguien que tenga los permisos de UNIX o los privilegios de acceso de Windows adecuados para ver todos los datos de un servidor de bases de datos. Recibe el soporte de una cuenta designada y de software diseñado para dar soporte a tareas de DBSA.

Para utilizar el software administrativo diseñado para este rol, la persona que desempeña el rol de DBSA debe iniciar la sesión en una o varias cuentas designadas y cumplir los requisitos de control de accesos.

Si el grupo de DBSA no es el grupo **informix**, los permisos sobre **oninit** se deberán modificar a 6755 (otorgar a otros permisos de ejecución) para que los miembros del nuevo grupo de DBSA puedan iniciar el servidor de bases de datos

El DBSA se encarga de otorgar o revocar el rol EXTEND para restringir los usuarios que pueden registrar módulos DataBlade y rutinas definidas por el usuario (UDR).

Responsable de seguridad del sistema de base de datos

El DBSSO es un administrador del sistema que realiza todas las tareas rutinarias relacionadas con el mantenimiento de la seguridad de un servidor de bases de datos. Entre estas tareas se encuentran las acciones siguientes:

- Mantenimiento de las máscaras de auditoría
- Respuesta a problemas de seguridad
- Formación de los usuarios

El DBSSO realiza estas tareas con el programa de utilidad **onaudit**. Para obtener información, consulte el apartado "Programa de utilidad onaudit" en la página 10-1.

El rol de DBSSO recibe el soporte de una cuenta designada y de software. Para utilizar las herramientas de auditoría, los usuarios que desempeñen el rol de DBSSO deberán iniciar la sesión en la cuenta designada y satisfacer los requisitos de control de accesos. Después de que los usuarios DBSSO cumplan los requisitos de control de accesos y utilicen el software administrativo, sus acciones se podrán auditar.

Consejo: En UNIX un DBSSO es cualquier usuario que pertenezca al grupo propietario de **$INFORMIXDIR/dbssodir**. En Windows, el administrador utiliza los valores del registro, mediante el recuadro de diálogo **Separación de roles** que aparece durante la instalación, para especificar los usuarios DBSSO.

Importante: EL programa de utilidad **onaudit** puede crear una amenaza potencial para la seguridad del servidor de bases de datos. Un usuario malintencionado puede abusar de una cuenta de DBSSO, por ejemplo, desactivando la auditoría para un usuario específico. Para reducir este riesgo, se deben auditar todas las acciones realizadas mediante **onaudit**.

Responsable del análisis de auditoría

El AAO configura la auditoría y lee y analiza el seguimiento de auditoría. El AAO puede especificar si la auditoría está habilitada y cómo lo está, cómo responde el sistema a las condiciones de error y quién es el responsable de gestionar el seguimiento de auditoría.

Para la auditoría gestionada por el servidor de bases de datos en UNIX, el AAO también determina el directorio del seguimiento de auditoría y el tamaño máximo de cada archivo de auditoría.

El AAO puede cargar los datos del seguimiento de auditoría en un servidor de bases de datos y utilizar SQL para analizarlos, ya sea mediante un programa de utilidad como DB–Access o mediante una aplicación personalizada desarrollada con una API SQL de IBM Informix o con una herramienta de desarrollo de aplicaciones.

El AAO realiza estas tareas con los programas de utilidad **onaudit** y **onshowaudit**, que se describen en el Capítulo 10, "Sintaxis del programa de utilidad", en la página 10-1. Si el AAO utiliza **onaudit** para cambiar los parámetros de configuración de la auditoría durante una sesión del servidor de bases de datos, los nuevos valores se grabarán en el archivo **adtcfg.***número_servidor* correspondientes a la instancia en cuestión del servidor de bases de datos.

El script de instalación del servidor de bases de datos crea un directorio **$INFORMIXDIR/aaodir** en UNIX o un directorio **%INFORMIXDIR%\aaodir** en Windows que contiene archivos que el AAO utiliza. Entre estos archivos se encuentran el archivo de configuración de la auditoría **adtcfg** y el archivo **adtcfg.std**, que contienen ejemplos de definiciones válidas para los parámetros de configuración de la auditoría.

El AAO necesita los permisos de UNIX o los privilegios de acceso de Windows adecuados para ver todos los datos del servidor de bases de datos para analizar los sucesos que puedan implicar el uso de información confidencial. El AAO decide si se deben auditar todas las acciones del DBSSO y del DBSA.

Consejo: En UNIX, un AAO es cualquier usuario que pertenezca al grupo propietario de **$INFORMIXDIR/aaodir**. En Windows, el administrador utiliza los valores del registro, mediante el recuadro de diálogo **Separación de roles** que aparece durante la instalación, para especificar los usuarios AAO.

Otros roles administrativos y usuarios

Existen algunos roles más, de tipo menor, que pueden están implicados en la auditoría de seguridad del servidor de bases de datos.

Administrador de base de datos

Un administrador de base de datos (DBA) gestiona el control de accesos para una base de datos específica. Un DBA no puede cambiar las modalidades del sistema de base de datos, añadir ni suprimir espacio ni mantener ni ajustar el sistema. Para obtener información sobre el rol y las responsabilidades de un DBA, consulte la publicación *IBM Informix Guide to SQL: Tutorial*. Para obtener información sobre este y otros roles y usuarios del servidor de bases de datos, consulte la publicación *IBM Informix Administrator's Guide*.

Administrador del sistema operativo

El Administrador del sistema operativo (OSA) desempeña responsabilidades y tareas que el servidor de bases de datos requiere del sistema operativo. El OSA habilita la separación de roles, otorga y revoca acceso a y desde el servidor de bases de datos si se aplica la separación de roles y añade nuevas cuentas de AAO, DBSSO y DBSA si es necesario. Además, el OSA se coordina con el DBSSO y AAO para realizar diversas funciones relacionadas con la seguridad del servidor de bases de datos, como las revisiones periódicas del seguimiento de auditoría del sistema operativo.

No existe ninguna cuenta especial para las necesidades referentes al sistema operativo del servidor de bases de datos y no hay mecanismos especiales de protección del servidor de bases de datos asociados con tareas del OSA. Para obtener más información sobre, consulte la documentación del sistema operativo.

Usuarios del sistema

Todas las cuentas del sistema operativo, incluidas las del DBSA, el DBSSO, el AAO y la cuenta denominada **informix**, pueden utilizar potencialmente el servidor de bases de datos. A todos los usuarios con cuentas que deseen utilizar el servidor de bases de datos se les deberá otorgar explícitamente acceso al servidor de bases de datos si se ha configurado la separación de roles para aplicar el control de accesos

a los usuarios del servidor de bases de datos. El DBSA puede revocar dicho acceso en cualquier momento, tanto si la separación de roles está habilitada como si no. Para obtener más información sobre cómo otorgar o revocar acceso, consulte el apartado “Configuración y aplicación de la separación de roles” en la página 8-5.

Usuarios con privilegios

Los usuarios con privilegios son los aquellos a los que el servidor de bases de datos reconoce como usuarios con privilegios y responsabilidades adicionales. Entre estos usuarios con privilegios están el DBSA, el DBSSO, el AAO y el DBA. Además, los usuarios **informix** y **root** también pueden operar como cualquier usuario con privilegios sobre los servidores de bases de datos configurados sin separación de robes. Incluso con la separación de roles, **root** puede ser un usuario con privilegios.

Separación de roles

La separación de roles es una opción del servidor de bases de datos que permite a los usuarios realizar tareas administrativas diferentes. La separación de roles se basa en el principio de la separación de funciones, que reduce los riesgos de seguridad con un mecanismo de comprobaciones y ajustes en el sistema. Por ejemplo, la persona que determina qué se debe auditar (DBSSO) debe ser una persona distinta de la que supervisa el seguimiento de auditoría (AAO) y éstas dos deben ser personas distintas a la que se encarga de las operaciones del servidor de bases de datos (DBSA).

Asignación de roles

Esta sección proporciona directrices generales sobre cómo asignar personas a cuentas y proporcionarles acceso a roles de actuación. Estas directrices se deben ajustar para que se adapten a los recursos y las políticas de seguridad de su sitio.

- Disponga de una cuenta para cada persona que desempeñe un rol.

  Por ejemplo, si tiene varios usuarios que desempeñan el rol de DBSA, haga que cada persona trabaje desde una cuenta distinta. Establezca una correlación de uno a uno entre las cuentas y los usuarios para facilitar el rastreo de sucesos de auditoría de un solo usuario.
- Disponga de la menor cantidad posible de cuentas de DBSA y DBSSO.

  Las cuentas de DBSA y DBSSO pueden poner en peligro la seguridad del servidor de bases de datos. Limite el número de cuentas que pueden provocar trastornos en el servidor de bases de datos para disminuir las posibilidades de que un usuario malintencionado pueda abusar de una cuenta privilegiada.
- Mantenga separados los roles de DBSA y DBSSO.

  Es posible que no disponga de los recursos o que vea la necesidad de disponer de distintos usuarios que desempeñen los roles de DBSA y DBSSO y que Dynamic Server tampoco exija estrictamente esta separación de roles. No obstante, si mantiene separados los roles de DBSA y DBSSO, los limitará a realizar sólo las tareas especificadas por sus responsabilidades y limitará el riesgo de poner en peligro la seguridad.
- Mantenga el rol de AAO separado de los roles de DBSA y DBSSO.

  El AAO determina si se deben auditar todas las acciones de los DBSA o DBSSO en el sistema. Resulta esencial que alguien con un rol distinto del de DBSA o DBSSO se encargue de la configuración de la auditoría, de modo que a todos los usuarios, incluidos el DBSA y el DBSSO, se les pueda responsabilizar de sus acciones en el sistema. De este modo se limita a los usuarios a realizar sólo las tareas especificadas por sus responsabilidades y se limita el riesgo de poner en peligro la seguridad.

- Limite el acceso a la cuenta **informix**, ya que esta puede pasar por alto la aplicación de la separación de roles y otros mecanismos de control de accesos del servidor de bases de datos.

Configuración y aplicación de la separación de roles

El DBSA, o la persona que instala el servidor de bases de datos, aplica la separación de roles y decide qué usuarios serán el DBSSO y el AAO. Para encontrar el grupo para el DBSA, el DBSSO o el AAO, busque en el subdirectorio adecuado de **$INFORMIXDIR** en UNIX o **%INFORMIXDIR%** en Windows.

En Windows, la separación de roles sólo se configura durante la instalación. En UNIX, la separación de roles se configura normalmente durante la instalación, pero también se puede configurar una vez finalizada la instalación o después de configurar el servidor de bases de datos. El OSA que instala el software aplica la separación de roles y decida qué usuarios (Windows) o grupos (UNIX) serán el DBSSO y el AAO. En UNIX, el grupo propietario de **$INFORMIXDIR/aaodir** es el grupo AAO; el grupo propietario de **$INFORMIXDIR/dbssodir** es el grupo DBSSO. De modo predeterminado, el grupo **informix** es el grupo DBSSO, AAO y DBSA.

En UNIX, si utiliza el instalador InstallShield MultiPlatform (ISMP) en modalidad de GUI o de terminal para instalar el software de la base de datos, se le preguntará si desea configurar la separación de roles. Si, por el contrario, utiliza el instalador de paquetes mediante scripts, la variable de entorno **INF_ROLE_SEP** controla si se le debe preguntar si desea configurar roles separados. Si la variable de entorno **INF_ROLE_SEP** existe (con o sin valor), la separación de roles se habilitará y se le solicitará que especifique los grupos DBSSO y AAO. (No se le preguntará por el grupo DBSA). Si la variable de entorno **INF_ROLE_SEP** no está establecida, se utilizará el grupo predeterminado **informix** para todos estos roles.

No es necesario establecer un valor para **INF_ROLE_SEP** para habilitar la separación de roles. Por ejemplo en un shell C, basta con emitir `setenv` INF_ROLE_SEP.

Una vez finalizada la instalación, **INF_ROLE_SEP** no tiene ningún efecto. Puede establecer la separación de roles manualmente cambiando el grupo propietario de los directorios **aaodir**, **dbssodir** o **etc**. Puede inhabilitar la separación de roles restableciendo el grupo propietario de estos directorios a **informix**. Puede habilitar la separación de roles para el AAO sin habilitar la separación de roles para el DBSSO.

El control de la separación de roles se realiza mediante la pertenencia a los siguientes grupos:

- Los usuarios que pueden desempeñar el rol de DBSA son miembros del grupo propietario del directorio **$INFORMIXDIR/etc**.
- Los usuarios que pueden desempeñar el rol de DBSSO son miembros del grupo propietario del directorio **$INFORMIXDIR/dbssodir**.
- Los usuarios que pueden desempeñar el rol de AAO son miembros del grupo propietario del directorio **$INFORMIXDIR/aaodir**.

Nota: Para cada uno de los grupos, el grupo predeterminado es el grupo **informix**.

El mandato **ls -lg** UNIX produce la salida que se muestra en la Figura 8-1 en la página 8-6.

```
total 14
drwxrwx---  2 informix       ix_aao    512 Nov 21 09:56 aaodir/
drwxr-xr-x  2 informix       informix 1536 Nov 30 18:35 bin/
drwxrwx---  2 informix       ix_dbsso  512 Nov 30 10:54 dbssodir/
drwxr-xr-x 10 informix       informix  512 Nov 21 09:55 demo/
drwxrwxr-x  2 informix       informix 1024 Nov 30 11:37 etc/
.
.
.
```

Figura 8-1. Ejemplo de salida que muestra la separación de roles

En la Figura 8-1, el AAO pertenece al grupo **ix_aao**, el DBSSO pertenece al grupo **ix_dbsso** y el DBSA pertenece al grupo **informix**.

Los usuarios deben pertenecer al grupo correcto para acceder al servidor de bases de datos. Para encontrar el grupo para los usuarios de la base de datos, debe examinar el contenido del archivo **$INFORMIXDIR/dbssodir/seccfg**. Por ejemplo el contenido de un archivo **seccfg** normal sería `IXUSERS=*`. Este valor de grupo significa que a todos los usuarios se les permite conectarse al servidor de bases de datos. Si el archivo contiene un nombre específico como, por ejemplo, `IXUSERS=engineer`, entonces sólo los miembros del grupo **engineer** podrán obtener acceso al servidor de bases de datos.

Para Windows, el control de la separación de roles se realiza mediante el recuadro de diálogo **Separación de roles**, que aparece durante la instalación, y mediante valores del registro. Si se marca el recuadro de selección **Habilitar separación de roles** en el recuadro de diálogo **Separación de roles**, el DBSA puede especificar distintos roles.

Para obtener más información sobre las variables de entorno, consulte la publicación *IBM Informix Guide to SQL: Reference*. Para obtener más información sobre cómo configurar la separación de roles, consulte la publicación *IBM Informix Administrator's Guide*.

Configuración de la auditoría

La auditoría no se inicia automáticamente cuando el servidor de bases de datos se instala por primera vez. Para que se puedan auditar acciones de los usuarios, el DBSSO o AAO debe realizar las siguientes tareas para configurar el servidor de bases de datos para la auditoría:

- Especificar suceso que se debe auditar en las máscaras de auditoría predeterminada, de usuario y global (DBSSO)
- Especificar cómo se debe comportar el servidor de bases de datos si se produce un error de auditoría al grabar un registro de auditoría (AAO)
- Determinar el nivel de auditoría deseado (AAO)
- Activar la auditoría (AAO)
- Especificar el directorio en el que se ubican los archivos de auditoría (AAO)

Configuración de las máscaras predeterminada y global

Antes de configurar las máscaras predeterminada y global, el DBSSO debe conocer cómo funcionan las distintas máscaras y cuáles son las implicaciones para las distintas instrucciones de auditoría. Además, el DBSSO debe saber qué sucesos de auditoría debe colocar en qué máscaras. Para obtener información detallada, consulte el Capítulo 7, "Visión general de la auditoría", en la página 7-1.

Utilice el programa de utilidad **onaudit** para añadir sucesos de auditoría a máscaras de auditoría. El Capítulo 11, "Mnemónicos y campos de los sucesos de auditoría", en la página 11-1 ofrece una lista de los sucesos de auditoría y sus mnemónicos. El Capítulo 10, "Sintaxis del programa de utilidad", en la página 10-1 muestra la sintaxis completa de **onaudit**.

El mandato siguiente muestra cómo se añaden los sucesos de auditoría Update Audit Mask (Actualizar máscara de auditoría) y Delete Audit Mask (Suprimir máscara de auditoría) a la máscara **_default** con sus códigos de suceso de cuatro letras o mnemónicos:

```
onaudit -m -u _default -e +UPAM,DRAM
```

Puede añadir sucesos de auditoría a las máscaras **_require** y **_exclude** del mismo modo. Para obtener información detallada, consulte el Capítulo 10, "Sintaxis del programa de utilidad", en la página 10-1.

Se auditan los sucesos especificados correspondientes a todos los usuarios que inician una sesión de base de datos tras la ejecución de este mandato (si la auditoría está activada).

Especificación de un directorio para el seguimiento de auditoría (UNIX)

El servidor de bases de datos almacena archivos de auditoría en un directorio del sistema de archivos. Puede especificar el directorio con el programa de utilidad **onaudit**. Por ejemplo, el mandato siguiente especifica **/work/audit** como sistema de archivos de UNIX en el que el servidor de bases de datos almacenará los archivos de auditoría:

```
onaudit -p /work/audit
```

Nota: El mandato `onaudit -p /work/audit` sólo funciona si el registro cronológico está habilitado o si las opciones `-l N` se incluyen en la línea de mandatos.

Puede cambiar el directorio de auditoría en cualquier momento. También puede configurar el tipo de auditoría y especificar el directorio con el archivo **ADTCFG**, que se describe en el Capítulo 12, "El archivo ADTCFG", en la página 12-1.

Para obtener más información sobre el programa de utilidad **onaudit**, consulte el Capítulo 10, "Sintaxis del programa de utilidad", en la página 10-1.

Establecimiento de la modalidad de error

Tal como se describe en el Capítulo 7, "Visión general de la auditoría", en la página 7-1, el servidor de bases de datos tiene tres acciones que puede realizar si se produce un error al grabar en el seguimiento de auditoría: una modalidad de error *continuar* y dos niveles de gravedad de modalidad de error *detener*. Asegúrese de entender, al igual que el AAO, las implicaciones de cada modalidad de error antes de seleccionar una.

Utilice al programa de utilidad **onaudit** o el archivo **ADTCFG** para establecer la modalidad de error. Para conocer la sintaxis de **onaudit,** consulte el Capítulo 10, "Sintaxis del programa de utilidad", en la página 10-1. Para obtener información sobre el parámetro de configuración ADTERR, consulte el Capítulo 12, "El archivo ADTCFG", en la página 12-1.

El siguiente mandato **onaudit** establece *continuar* como modalidad de error. El servidor de bases de datos procesa la hebra y anota el error en el registro de mensajes.

```
onaudit -e 0
```

El mandato siguiente establece como modalidad un error el nivel más grave de *detener*, que hace que el servidor de bases de datos se apague:

```
onaudit -e 3
```

Establecimiento del nivel de auditoría

El AAO o el DBSSO configura el nivel de auditoría en el sistema. El AAO supervisa el seguimiento de auditoría y realiza toda la gestión de los registros de auditoría.

El DBSSO tiene mucha libertad de acción por lo que respecta al nivel de auditoría del servidor de bases de datos. Por ejemplo, una configuración de auditoría mínima podría implicar la auditoría de sólo las acciones del DBSSO, los programas de utilidad del servidor de bases de datos y el inicio de cada nueva sesión de usuarios del servidor de bases de datos. Una configuración de auditoría máxima implica la auditoría de todos los sucesos del servidor de bases de datos relevantes para la seguridad correspondientes a todos los usuarios.

El AAO y el DBSSO deben coordinar sus esfuerzos para determinar el nivel de auditoría. Por ejemplo, para auditar las acciones del DBSA, el DBSSO utilizaría máscaras para las cuentas de DBSA y el AAO establecería la modalidad de auditoría con el programa de utilidad **onaudit** o el archivo **ADTCFG**.

Para garantizar que se supervisen las actividades del servidor de bases de datos adecuadas, revise los registros de auditoría que se almacenan en el seguimiento de auditoría del sistema operativo, los archivos de auditoría del servidor de bases de datos o el registro cronológico de sucesos de Windows. Debe configurar el servidor de bases de datos para que supervise estos sucesos.

Puede reconfigurar la auditoría a medida que se identifiquen cambios de uso y amenazas potenciales para la seguridad. Para conocer la sintaxis de **onaudit**, consulte el Capítulo 10, “Sintaxis del programa de utilidad”, en la página 10-1. Para obtener información sobre el parámetro de configuración ADTMODE, consulte el Capítulo 12, “El archivo ADTCFG”, en la página 12-1.

Importante: Aunque la generación de registros de auditoría del servidor de bases de datos pueda tener una repercusión negativa sobre el rendimiento y los recursos del servidor de bases de datos, debería realizar una auditoría de un nivel superior al mínimo. Esta auditoría adicional mejora las posibilidades de detectar violaciones de la seguridad e intentos de vulnerar los mecanismos de seguridad.

Si realiza la auditoría mínima o no realiza ninguna auditoría para los usuarios del servidor de bases de datos, es virtualmente imposible detectar intentos creativos de vulnerar la política de seguridad del servidor de bases de datos. Si alguien sospecha de una violación de la seguridad o un determinado usuario muestra un comportamiento inusual, se debe habilitar la auditoría completa del usuario sospechoso para obtener una visión completa de las actividades del usuario.

Equilibre las necesidades de seguridad de su sitio y la repercusión de los distintos niveles de auditoría sobre el rendimiento y los recursos. El nivel de auditoría de

cualquier momento específico tiene una repercusión directa sobre los recursos del sistema operativo y el rendimiento del servidor de bases de datos. La repercusión depende de los siguientes factores:

- El número de usuarios o de sucesos auditados, o ambos
- La configuración del procesador
- La carga del sistema (número de procesos y usuarios)
- El espacio disco
- La carga de trabajo (tipos de procesos realizados)

Consejo: Para especificara el espacio de disco, utilice la herramienta de administración Visor de sucesos de Windows.

Para obtener más información sobre las consideraciones sobre el rendimiento servidor de bases de datos, consulte la publicación *IBM Informix Performance Guide*.

Activación de la auditoría

La auditoría se desactiva de modo predeterminado cuando se instala el servidor de bases de datos. Utilice el programa de utilidad **onaudit** para activar la auditoría en tiempo de ejecución o establecer el parámetro de configuración ADTMODE en el archivo **ADTCFG**. Si utiliza el archivo un **ADTCFG**, el valor entrará en vigor cuando el servidor de bases de datos se inicialice.

El siguiente mandato **onaudit** activa la auditoría:

```
onaudit -l 1
```

Después de activar la auditoría, los cambios de la auditoría entran en vigor inmediatamente para todas las sesiones.

El AAO puede configurar el servidor de bases de datos para activar la auditoría cuando se inicia el servidor cuando el parámetro de configuración ADTMODE se establece en los números 1, 3, 5 o 7 en el archivo **ADTCFG**. Para obtener información detallada sobre los valores del parámetro ADTMODE consulte el apartado "Cambio de la configuración de la auditoría" en la página 10-7 y el Capítulo 12, "El archivo ADTCFG", en la página 12-1.

Cuando el servidor de bases de datos se inicializa con la auditoría activada, todas las sesiones de usuario generan registros de auditoría de acuerdo con la máscara individual, predeterminada o global (**_require**, **_exclude**) en vigor para cada usuario.

Para desactivar la auditoría después de que se haya iniciado, consulte el apartado "Desactivación de la auditoría" en la página 8-16.

Mantenimiento de máscaras de auditoría

Es posible que desee cambiar las instrucciones de auditoría a medida que sus necesidades de auditoría vayan cambiando. Esta sección explica los procedimientos siguientes, que se pueden utilizar para modificar máscaras de auditoría:

- Creación de máscaras de auditoría
- Visualización de máscaras de auditoría
- Modificación de máscaras de auditoría
- Supresión de máscaras de auditoría

Estas tareas, realizadas por el DBSSO, son aplicables tanto si el servidor de bases de datos administra los registros de auditoría como si lo hace el sistema operativo.

Creación de máscaras de auditoría

Puede crear máscaras que coincidan más estrechamente con los tipos de actividades que los usuarios individuales realizan que las máscaras predeterminadas y globales.

- Para crear máscaras de usuario individuales, especifique ID de usuario como nombres de máscara.
- Para crear máscaras de plantilla, añada al principio del nombre de una máscara un carácter de subrayado (_). En el Capítulo 7, "Visión general de la auditoría", en la página 7-1 se describen las máscaras de plantilla y las máscaras de usuario.

Debe especificar sucesos en la máscara al crearla, utilizando los sucesos de auditoría del listado alfabético de la tabla "Mnemónicos de sucesos de auditoría" en la página 11-1. Los sucesos para las máscaras de auditoría personalizadas (de plantilla y de usuario) se deben especificar del mismo modo que para las máscaras de auditoría **_default**, **_require** y **_exclude**.

Por ejemplo, es posible que desee crear tres máscaras de plantilla con distintos niveles de seguridad: **_low** (bajo), **_medium** (medio) y **_high** (alto). O bien podría necesitar sólo dos plantillas para los usuarios conocidos y desconocidos que copie en máscaras de usuarios individuales: **_guest** (invitado) y **_trusted** (fiable).

Creación de una máscara de plantilla

Para crear una máscara de auditoría de plantilla:

Utilice el programa de utilidad **onaudit**. En el Capítulo 10, "Sintaxis del programa de utilidad", en la página 10-1 se muestra la sintaxis. El ejemplo siguiente muestra cómo crear una máscara de plantilla denominada **_guest** con los sucesos de auditoría Create Database (Crear base de datos), Grant Database Access (Otorgar acceso a base de datos) y Grant Table Access (Otorgar acceso a tabla):

```
onaudit -a -u _guest -e +CRDB,GRDB,GRTB
```

Creación de una máscara de usuario a partir de una máscara de plantilla

Una máscara que se utiliza como base para una o varias otras máscaras se conoce como una *máscara base*.

Para crea una máscara de usuario a partir de una máscara de plantilla:

Cree la máscara de plantilla. Después de crear una máscara de plantilla para una determinada categoría de usuario, puede utilizarla como base de las máscaras de usuarios individuales, añadiendo o eliminando sólo los sucesos de auditoría que difieran entre sí.

El ejemplo siguiente crea una máscara de usuario para el usuario **terry**, basada en la máscara de plantilla **_guest**:

```
onaudit -a -u terry -r _guest -e -CRDB
```

La máscara **terry** tiene los mismos sucesos de auditoría que la máscara **_guest**, a excepción del suceso de auditoría CRDB (Create Database), que se ha eliminado.

En lugar de utilizar máscaras de plantilla, también puede utilizar máscaras de usuario **_default**, **_require** y **_exclude** existentes como máscaras base.

Consejo: Si utiliza una máscara de plantilla o de usuario como máscara base para otra máscara, la máscara nueva heredará los sucesos de la máscara base. La nueva máscara no hace referencia dinámicamente a la máscara base. Los cambios futuros a la máscara base no se reflejan en otras máscaras que se puedan haber creado o modificado con dicha máscara como base.

Creación de una máscara de usuario sin una máscara de plantilla

Para crear máscaras de usuario sin una máscara de plantilla:

Utilice sucesos como base para la máscara de usuario. El ejemplo siguiente crea una máscara para el usuario **pat** con el suceso Show Table Statistics (Mostrar estadísticas de tabla) y los intentos fallidos del suceso Alter Tabla (Modificar tabla):

```
onaudit -a -u pat -e +SSTB,FALTB
```

Para obtener información sobre la sintaxis para crear una máscara de usuario y otro ejemplo, consulte el Capítulo 10, "Sintaxis del programa de utilidad", en la página 10-1.

Adición de una o varias máscaras utilizando un archivo de entrada

Para añadir una o varias máscaras utilizando un archivo de entrada:

Utilice el programa de utilidad **onaudit** para añadir una o varias máscaras a la tabla de máscaras con instrucciones de un archivo que tenga el mismo formato que la salida de **onaudit -o**. El mandato siguiente lee un archivo de **/work/audit_up** y añade máscaras de auditoría a la tabla de máscaras de acuerdo con las instrucciones de dicho archivo:

```
onaudit -f /work/audit_up
```

La Figura 8-2 muestra un ejemplo de un archivo de entrada. La sintaxis del archivo de entrada se explica en el Capítulo 10, "Sintaxis del programa de utilidad", en la página 10-1.

```
kickt         _secure1
jacks         -         +ADCK,SRDRW,GRDB,OPDB
pat         _secure2          +ALTB -CRTB,CRIX,STSN
jaym         -
johns         akee         -SALIX
```

Figura 8-2. Archivo de entrada de ejemplo

El archivo de entrada de ejemplo de la Figura 8-2 incluye la siguiente información:

- En la primera línea, las instrucciones especifican la auditoría para el usuario **kickt** en la nueva plantilla **_secure1**.
- La segunda línea crea una nueva máscara denominada **jacks**, que contiene los sucesos Add Chunk (ADCK) (Añadir fragmento), los intentos satisfactorios de Read Row (SRDRW) (Leer fila) y todos los intentos de Grant Database Access (GRDB) (Otorgar acceso a base de datos) y Open Database (OPDB) (Abrir base de datos).

- En la tercera línea, se auditan todos los sucesos correspondientes al usuario **pat** especificados en la plantilla **_secure2** y también todos los intentos de Alter Table (ALTB) (Modificar tabla), pero no los intentos de Create Table (CRTB) (Crear tabla), Create Index (CRIX) (Crear índice) y Start New Session (STSN) (Iniciar sesión nueva).
- No se especifica ninguna plantilla para la máscara de destino **jaym** en la cuarta línea y no se indica ningún suceso; la máscara está vacía. (Esto impide que la máscara **_default** se aplique a **jaym**).
- En la quinta línea, la máscara de destino **johns** audita los mismos sucesos que la máscara **akee**, menos todos los intentos satisfactorios de Alter Index (SALIX) (Modificar índice).

Importante: Los cambios futuros de una máscara base no se reflejan en otras máscaras que se puedan haber creado o modificado con dicha máscara como base.

En el directorio **$INFORMIXDIR/aaodir** de UNIX o en el directorio **%INFORMIXDIR%\aaodir** de Windows se proporciona un ejemplo de un archivo de entrada de máscara de auditoría, **adtmasks.std**. El archivo **adtmasks.std** tiene como objetivo servir de guía para el DBSSO sobre cómo configurar una máscara de auditoría.

Las máscaras de auditoría no funcionan del mismo modo que los parámetros de configuración de la auditoría durante la inicialización del servidor de bases de datos. (Consulte el apartado "Configuración de la auditoría y el archivo ADTCFG" en la página 7-13). Específicamente, las máscaras de auditoría no se leen de un archivo ni se inicializan automáticamente.

Visualización de máscaras de auditoría

Para visualizar todas las máscaras de auditoría y los sucesos de auditoría que cada máscara contiene:

Utilice la opción **-o** del programa de utilidad **onaudit**. Cuando emita el mandato **onaudit -o -y**, la salida (nombre de máscara, máscara base, sucesos de auditoría) aparecerá tal como se indica a continuación:

```
_default     -     UPAM,DRAM
_require     -
_exclude     -
_guest       -     CRDB,GRDB,GRTB
terry        -     -CRDB
```

Puede especificar una máscara como argumento para la opción **-o**. El ejemplo siguiente muestra sólo la máscara correspondiente al usuario **terry**:

```
onaudit -o -u terry
```

Una lista de máscara de auditorías resulta útil cuando se necesita modificarlas. Puede utilizar la salida modificada como archivo de entrada para modificar una sola máscara o grupos de máscaras en un solo lote. Para obtener más información, consulte el apartado "Modificación de máscaras de auditoría" en la página 8-13. Para conocer la sintaxis completa de la opción **onaudit -o** y una descripción de la salida, consulte el Capítulo 10, "Sintaxis del programa de utilidad", en la página 10-1.

Consejo: Si utiliza una máscara base para crear o modificar una máscara, la propia máscara base no aparecerá en la salida de **onaudit -o** correspondiente a la máscara nueva. Si se crea o se modifica una máscara con una máscara base, ésta no hará referencia a la máscara base.

Modificación de máscaras de auditoría

El DBSSO puede modificar máscaras individualmente desde la línea de mandatos.

Para modificar máscaras de auditoría:

Utilice la opción **-m** del programa de utilidad **onaudit** para modificar una sola máscara. Esta opción permite utilizar otra máscara como base para añadir o eliminar sucesos de auditoría individuales. Para modificar varias máscaras a la vez, puede crear un nuevo archivo de entrada, cambiar las máscaras apropiadas y volver a cargarlas en la tabla de máscaras.

El ejemplo siguiente muestra cómo modificar la máscara de usuario **pat**. La máscara de plantilla **_guest** forma una base de la que se obtiene un conjunto completo de sucesos de auditoría. Los valores correspondientes a sucesos específicos de dicho archivo se sustituyen luego por los sucesos listados como argumentos para la opción **-e**.

```
onaudit -m -u pat -r _guest -e +ALTB,USTB
```

Cuando se proporciona una máscara base con la opción **-r**, se sustituyen todos los sucesos de auditoría en la máscara inicial. Al cambiar sólo unos cuantos sucesos de una máscara, es posible que no desee especificar una máscara base. Para conocer la sintaxis y ver otro ejemplo de cómo modificar una máscara, consulte el Capítulo 10, “Sintaxis del programa de utilidad”, en la página 10-1.

Supresión de máscaras de auditoría

Para suprimir una sola máscara o todas las máscaras a la vez:

Utilice la opción **-d** del programa de utilidad **onaudit**. El ejemplo siguiente suprime la máscara de usuario individual correspondiente al usuario **terry**:

```
onaudit -d -u terry
```

Para obtener más información sobre la sintaxis del programa de utilidad **onaudit**, consulte el Capítulo 10, “Sintaxis del programa de utilidad”, en la página 10-1.

Mantenimiento de la configuración de la auditoría

El AAO realiza normalmente las siguientes tareas para el mantenimiento de la configuración de la auditoría:

- Visualización de la configuración de la auditoría
- Cambio de la modalidad de auditoría (incluidos roles específicos de auditoría)
- Cambio de la modalidad de error de auditoría
- Desactivación de la auditoría
- Inicio de un nuevo archivo de auditoría (incluida la especificación de un directorio y de un tamaño máximo del archivo)).

Esta sección describe cómo utilizar **onaudit** para realizar estas tareas. Para obtener más información sobre la sintaxis del programa de utilidad **onaudit**, consulte el Capítulo 10, "Sintaxis del programa de utilidad", en la página 10-1.

Visualización de la configuración de auditoría

Para visualizar la configuración de auditoría actual, utilice la opción **-c** del programa de utilidad **onaudit**.

- Para UNIX, la Figura 8-3 muestra la salida del mandato **onaudit -c**.

```
onaudit -c

Onaudit -- Programa de utilidad de control del subsistema de auditoría
Copyright (c) IBM Corp., 1998 - 2007

Configuración actual del sistema auditor:
   ADTMODE =           1
   ADTERR =            0
   ADTPATH =           /tmp
   ADTSIZE =           20000
   Fichero auditor =   64
```

Figura 8-3. Ejemplo de salida del mandato onaudit -c en UNIX

  En la Figura 8-3, el sistema de auditoría actual está configurado del modo siguiente:
  - ADTMODE se ha establecido en 1, lo que indica que la auditoría gestionada por el servidor de bases de datos está activada.
  - ADTERR se ha establecido en 0, lo que indica una modalidad de error continuo.
  - ADTPATH muestra el directorio predeterminado para los archivos de auditoría.
  - Se ha especificado 20.000 bytes como valor de ADTSIZE, que representa el tamaño máximo del archivo de auditoría.
  - El número del archivo de auditoría actual del directorio de auditoría actual es 64.

  Si es el usuario **informix**, también puede recuperar esta información de la tabla **sysadtinfo** de SMI de la base de datos **sysmaster**. Para obtener información detallada, consulte la publicación *IBM Informix Administrator's Reference*.
- Para Windows, la Figura 8-4 muestra la salida del mandato **onaudit -c**.

```
onaudit -c

Onaudit -- Programa de utilidad de control del subsistema de auditoría
Copyright IBM Corporation 1996, 2007 Reservados todos los derechos

Configuración actual del sistema auditor:
   ADTMODE =              1
   ADTERR =               0
   ADTPATH =              %informixdir%/aaodir
   ADTESIZE =             50000
   Fichero auditor =      0
```

Figura 8-4. Ejemplo de salida del mandato onaudit -c en Windows

En la Figura 8-4 en la página 8-14, el sistema de auditoría actual está configurado del modo siguiente:

- ADTMODE se ha establecido en 1, lo que indica que la auditoría gestionada por el servidor de bases de datos está activada.
- ADTERR se ha establecido en 0, lo que indica una modalidad de error continuo.
- ADTPATH muestra el directorio predeterminado para los archivos de auditoría.
- Se ha especificado 50.000 bytes como valor de ADTSIZE, que representa el tamaño máximo del archivo de auditoría.
- El número del archivo de auditoría actual del directorio de auditoría actual es 0, lo que significa que no existe ningún otro archivo de auditoría en la serie actual.

Inicio de un nuevo archivo de auditoría

El mandato **onaudit** se utiliza para iniciar un archivo de auditoría nuevo. Para obtener información sobre la sintaxis de **onaudit** para iniciar un archivo de auditoría nuevo, cambiar el tamaño del archivo de auditoría o cambiar el nombre de la vía de acceso del directorio de auditoría, consulte el apartado "Programa de utilidad onaudit" en la página 10-1.

Puede utilizar más de un distintivo a la vez en un mandato **onaudit**.

Puede iniciar un archivo de auditoría nuevo de uno de los modos siguientes:

- Utilice **onaudit -s** para cambiar el tamaño máximo de un archivo de auditoría. Si el archivo de auditoría ya tiene un tamaño superior al nuevo tamaño que especifique, del programa de utilidad guardará el archivo actual y empezará a grabar en un archivo nuevo.

  El ejemplo siguiente cambia el tamaño predeterminado a 20.000 bytes:

  ```
  onaudit -s 20000
  ```

- Utilice **onaudit -n** para iniciar un archivo de auditoría nuevo sin cambiar el tamaño máximo.

  Esta opción, que se muestra en el ejemplo siguiente, guarda el registro de auditoría actual en otro archivo siempre que se ejecuta:

  ```
  onaudit -n
  ```

- Utilice **onaudit -p** para cambiar el directorio en el que el servidor de bases de datos graba los archivos de auditoría.

  El ejemplo siguiente especifica **/work/audit** como el sistema de archivos de UNIX en el que se deben guardar los archivos de auditoría:

  ```
  onaudit -p /work/audit
  ```

  El directorio que especifique debe existir.

- Inicie la auditoría gestionada por el servidor de bases de datos. Cada vez que se inicia la auditoría gestionada por el servidor de bases de datos, se inicia un archivo de auditoría nuevo.

Cambio de los niveles de auditoría

- Utilice el programa de utilidad **onaudit** para cambiar los niveles de auditoría del servidor de bases de datos y para cambiar la auditoría obligatoria del administrador del servidor de bases de datos.

  Por ejemplo, para iniciar la auditoría básica, entre el mandato siguiente:

```
onaudit -l 1
```

- Para iniciar la auditoría y auditar automáticamente las acciones de DBSA, entre el mandato siguiente:

```
onaudit -l 5
```

Cambio de la modalidad de error de auditoría

Tal como se explica en el Capítulo 7, "Visión general de la auditoría", en la página 7-1 y en el apartado "Establecimiento de la modalidad de error" en la página 8-7, el servidor de bases de datos se comporta de uno de tres modos posibles si se produce un error al grabar en el archivo de auditoría actual.

Para cambiar la modalidad de error de auditoría:

Utilice el programa de utilidad **onaudit**.

En el ejemplo siguiente se indica al servidor de bases de datos que debe suspender el proceso de la hebra actual y seguir intentando la grabación hasta que resulte satisfactoria:

```
onaudit -e 1
```

Desactivación de la auditoría

Para desactivar la auditoría:

Utilice el programa de utilidad **onaudit**.

El ejemplo siguiente muestra el mandato que desactiva la auditoría:

```
onaudit -l 0
```

Aviso: Aunque es posible que la auditoría esté correctamente configurada, para auditar la ejecución de un programa de utilidad por parte de un determinado usuario, es posible que no se generen registros de auditoría si el programa de utilidad no puede ejecutarse por cualquiera de los motivos siguientes:

- El usuario no tiene los permisos de UNIX o los privilegios de acceso de Windows correctos para ejecutar el programa de utilidad.
- El usuario especifica incorrectamente la sintaxis del mandato del programa de utilidad.
- El programa de utilidad no se puede conectar a la memoria compartida.

Capítulo 9. Análisis de auditoría

La importancia del análisis de auditoría nunca se puede destacar lo suficiente. Este capítulo explica los temas siguientes:

- El formato de los registros de auditoría que el servidor de bases de datos produce
- Cómo realizar análisis de auditoría con o sin SQL
- Cómo extraer información de auditoría del seguimiento de auditoría para una visualización rápida
- Cómo cargar estos datos en una base de datos para analizarlos con SQL
- Cómo realizar el mejor análisis de extracto sobre la información de auditoría extraída

Este capítulo sirve tanto en el caso de que utilice el servidor de bases de datos como en el caso de que utilice el sistema operativo para almacenar y mantener el seguimiento de auditoría. En el Capítulo 7, "Visión general de la auditoría", en la página 7-1 encontrará una visión general del proceso de análisis de auditoría.

Formato del registro de auditoría

El servidor de bases de datos genera la segunda parte del registro de auditoría, con campos que dependen del suceso de auditoría.

La Tabla 9-1 muestra el formato de los registros de auditoría del servidor de bases de datos.

Tabla 9-1. Formato del registro de auditoría

ONLN	fecha y hora	nombsistpral o nombsistpral. dominio.ext	pid	nombre servidor bases datos	nombre usuario	núm_ error	mnemónico del suceso	Campos adicionales
ONLN	2007-07-28 15:43:00.000	turk	4549	khan	jazt	0	CRDB	dbsch
ONLN	2007-07-28 15:43:18.000	turk	4549	khan	jazt	0	ACTB	dbsch:jazt:v1:103
ONLN	2007-07-28 15:43:19.000	turk	4549	khan	jazt	0	CLDB	dbsh
ONLN	2007-07-28 15:43:21.000	turk	4549	khan	jazt	0	ALFR	local:109:-:-:4:4: db1,db2,db3, rootdbs
ONLN	2007-07-28 15:43:28.000	turk	4549	khan	jazt	0	ALFR	local:109:aa5x:-: 32:4: db1,db2
ONLN	2007-07-28 15:43:29.000	turk	4549	khan	jazt	0	STDS	2:-
ONLN	2007-07-28 15:43:29.000	turk	4549	khan	jazt	0	STPR	100
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .

ONLN
Campo fijo utilizado para identificar sucesos de Dynamic Server

fecha y hora
Indica cuándo se ha registrado el suceso de auditoría

nombsistpral
Nombre del sistema principal UNIX de la aplicación cliente que ejecuta el suceso de auditoría

nombsistpral.dominio.ext
Nombre del sistema principal Windows, dominio y extensión de la aplicación cliente que ejecuta el suceso de auditoría

pid ID de proceso de la aplicación cliente que hace que el servidor de bases de datos ejecute el suceso de auditoría

nombre servidor bases datos
Nombre del servidor de bases de datos en el que se ejecuta el suceso de auditoría

nombre usuario
Nombre de inicio de sesión del usuario que solicita el suceso

núm_error
Resultado del suceso que contiene el número de error que el suceso devuelve, indicando un resultado satisfactorio (0) o anómalo

mnemónico del suceso
Suceso de auditoría del servidor de bases de datos que el servidor de bases de datos ha ejecutado, por ejemplo ALFR (Alter Fragment (Modificar fragmento))

campos adicionales
Cualquier campo que identifique bases de datos, tablas, etc. Estos campos adicionales son campos de sucesos de auditoría que contienen que el programa de utilidad **onshowaudit** captura en forma de tabla para el análisis de auditoría.

Para la auditoría gestionada por el sistema operativo en UNIX, el registro de auditoría del servidor de bases de datos es un campo adicional para el registro de auditoría del sistema operativo. En el Capítulo 11, "Mnemónicos y campos de los sucesos de auditoría", en la página 11-1 se ofrece una lista de los campos de sucesos de auditoría.

Análisis de auditoría sin SQL

Utilice el programa de utilidad **onshowaudit** para extraer datos para el análisis de auditoría. Este programa de utilidad puede realizar algún filtrado básico como el de un usuario o un nombre de servidor de bases de datos. Luego puede enviar los datos extraídos a una salida estándar (por ejemplo, su pantalla) y utilizar programas de utilidad de UNIX como, por ejemplo, **grep**, **sed** y **awk** o programas de utilidad de Windows para analizarlos. También puede optar por colocar los datos en una base de datos y analizarlos mediante SQL, tal como se describe en la siguiente sección.

Sólo el AAO puede ejecutar **onshowaudit**. Si la separación de roles no está habilitada, el usuario **informix** será el AAO. (El superusuario **root** en UNIX

siempre es un AAO). Puesto que la divulgación de registros de auditoría representa una amenaza para la seguridad, sólo el AAO debe leer los registros extraídos.

Por ejemplo, el mandato siguiente extrae registros de auditoría correspondientes al usuario **pat** de un archivo de auditoría denominado **laurel.12**, en UNIX, y envía los registros de auditoría a una salida estándar:

```
onshowaudit -I -f laurel.12 -u pat
```

La sintaxis de la línea de mandatos para extraer información con **onshowaudit** se explica en el Capítulo 10, "Sintaxis del programa de utilidad", en la página 10-1.

Análisis de auditoría con SQL

También puede utilizar el programa de utilidad **onshowaudit** para volver a dar formato a los datos extraídos y redirigirlos a un archivo de datos y, a continuación, utilizar el programa de utilidad **dbload** para cargar dichos datos en una tabla de base de datos. Esta sección explica este proceso.

Planificación del análisis de auditoría SQL

Cuando planifique el análisis de auditoría con el servidor de bases de datos, tenga en cuenta que el propio proceso de análisis de auditoría puede generar registros de auditoría, según cómo se haya configurado la auditoría. Un modo de evitar la generación de registros de auditoría no deseados como resultado del análisis de auditoría consiste en utilizar una instancia distinta no auditada del servidor de bases de datos.

Para realizar el análisis de auditoría con SQL, debe utilizar un programa para acceder a la base de datos y a la tabla que ha creado. Utilice el programa de utilidad DB–Access para crear y ejecutar sentencias de SQL o desarrollar una aplicación con una herramienta de desarrollo de aplicaciones IBM Informix o una API de SQL como, por ejemplo, IBM Informix ESQL/C.

Tanto si realiza el análisis con DB–Access como si crea una aplicación personalizada, recuerde los consejos proporcionados para la revisión de la auditoría en el apartado "Visión general del análisis de auditoría" en la página 7-16. Para ver sucesos de auditoría correspondientes a objetos específicos, seleccione filas de acuerdo con su valor en la columna **dbname**, **tabid** o **row_num**.

Si descubre una actividad sospechosa de acuerdo con el análisis inicial de la tabla de auditoría en el servidor de bases de datos, puede aumentar el ámbito de la recopilación de sucesos de auditoría para determinar el problema. Si está seguro de que tiene un problema de seguridad, consulte el apartado "Amenazas para la seguridad del sistema de gestión de bases de datos" en la página 7-20.

Revocación y otorgamiento de privilegios para proteger los datos de auditoría

Cuando cree una base de datos tal como se describe en las secciones siguientes, asegúrese de que la base de datos esté protegida frente a los accesos no autorizados.

Las tablas que cree en bases de datos que no sean compatibles con ANSI tienen privilegios que permiten el acceso de todos los usuarios. Aunque los permisos o los privilegios de acceso predeterminados de la base de datos impiden el acceso a

las tablas, las prácticas de seguridad adecuadas protegerán la tabla de análisis de auditoría en una base de datos que no es compatible con ANSI revocando el acceso de todos los demás usuarios en cuanto se cree la tabla.

Puede utilizar las siguientes sentencias de SQL para controlar el acceso:

```
REVOKE ALL ON tabla FROM PUBLIC
GRANT ALL ON tabla TO informix
```

Después de revocar los privilegios de tablas, normalmente con la sentencia REVOKE, puede otorgar a usuarios individuales (por ejemplo, al usuario **informix**) acceso a las tablas con la sentencia GRANT. Para obtener información sobre las sentencias de SQL, consulte la publicación *IBM Informix Guide to SQL: Syntax*.

Las tablas creadas en bases de datos compatibles con ANSI tienen privilegios que permiten el acceso sólo al propietario, que es la medida de seguridad adecuada.

También puede utilizar la variable de entorno **NODEFDAC** para controlar el acceso. Cuando se establece yes como valor, **NODEFDAC** no permite otorgar los privilegios de tabla predeterminados (Seleccionar, Insertar, Actualizar e Insertar) a PUBLIC cuando se crea una tabla nueva en una base de datos que no sea compatible con ANSI. Para obtener información detallada, consulte la publicación *IBM Informix Guide to SQL: Reference*.

Preparación de los registros de análisis de auditoría para el acceso de SQL

Para preparar los registros de auditoría para el análisis de SQL, siga los pasos que se indican a continuación:

1. Cree un archivo de datos para utilizarlo con **dbload**.
2. Cree una base de datos y una tabla en la que se almacenarán los datos de la auditoría.
3. Cree un archivo de mandato para utilizarlo con **dbload**.
4. Cargue los datos de la auditoría en la tabla.

Creación de un archivo de datos para dbload

El primer paso para prepararse para el análisis de auditoría basado en SQL es utilizar **onshowaudit -l** para extraer registros de auditoría seleccionados en formato **dbload** y colocarlos en un archivo de salida.

El ejemplo siguiente extrae registros de auditoría correspondientes al usuario **pat** del archivo de auditoría gestionados por el servidor **laurel.11** y dirige los registros al archivo de salida **records_pat**:

```
onshowaudit -I -f laurel.11 -u pat -l > records_pat
```

Importante: Debe eliminar las seis líneas de cabecera que aparecen en el archivo de salida antes de utilizar el archivo como entrada para el programa de utilidad **dbload** porque **dbload** no puede procesar las líneas de cabecera.

La sintaxis de la línea de mandatos para extraer información con **onshowaudit** se explica en el Capítulo 10, “Sintaxis del programa de utilidad”, en la página 10-1.

Creación de una base de datos para datos de auditoría

Para cargar archivos de datos en una base de datos con **dbload**, debe existir una base de datos para recibir los datos.

Cree una base de datos para contener copias de los registros de auditoría con la sentencia CREATE DATABASE. De modo predeterminado, la sentencia CREATE DATABASE crea la base de datos con privilegios que permiten el acceso sólo al propietario, que es la medida de seguridad adecuada. No es necesario utilizar el registro cronológico dentro de una base de datos creada estrictamente para el análisis de auditoría porque los datos no se deben modificar.

La siguiente sentencia de SQL crea una base de datos denominada **auditlogs97**:

```
CREATE DATABASE auditlogs97
```

También puede crear una base de datos compatible con ANSI. Aunque una base de datos compatible con ANSI implica la sobrecarga adicional del registro cronológico, su tratamiento de los permisos de tabla o de los privilegios de acceso hace que resulte atractiva en un entorno seguro. Para obtener más información sobre los permisos de UNIX o los privilegios de acceso de Windows, consulte el apartado "Revocación y otorgamiento de privilegios para proteger los datos de auditoría" en la página 9-3.

La siguiente sentencia de SQL crea una base de datos compatible con ANSI:

```
CREATE DATABASE auditlogs97 WITH LOG MODE ANSI
```

Creación de una tabla para datos de auditoría

Para cargar archivos de datos en una base de datos con **dbload**, debe existir una tabla para recibir los datos.

Cree una tabla para albergar los datos de auditoría con la sentencia CREATE TABLE. El orden y el tipo de datos de las columnas es importante.

Utilice el orden que se muestra en el ejemplo en la Figura 9-1 en la página 9-6. El esquema del ejemplo refleja el formato del archivo de datos **dbload** que **onshowaudit** ha creado.

La sentencia CREATE TABLE de ejemplo de la Figura 9-1 en la página 9-6 crea una tabla de auditoría denominada **frag_logs**. Para obtener información sobre el contenido de cada columna, consulte el apartado "Interpretación de datos extraídos de registros de auditoría" en la página 9-7.

La sentencia CREATE TABLE de ejemplo de la Figura 9-1 en la página 9-6 no incluye la opción WITH CRCOLS, que sirve para la resolución de conflictos durante la duplicación de bases de datos. Para duplicar la base de datos de auditoría, utilice WITH CRCOLS en la sentencia CREATE TABLE.

```
CREATE TABLE frag_logs (
    adttag CHAR(4),
    date_time DATETIME YEAR TO FRACTION(3),
    hostname CHAR(18),
    pid INT,
    server CHAR(18),
    username CHAR(8),
    errno INT,
    code CHAR(4),
    dbname CHAR(18),
    tabid INT,
    objname CHAR(18),
    extra_1 INT,
    partno INT,
    row_num INT,
    login CHAR(8),
    flags INT,
    extra_2 VARCHAR(160,1));
```

Figura 9-1. Sentencia CREATE TABLE de ejemplo para una tabla de auditoría de Dynamic Server

La tabla que la sentencia de la Figura 9-1 crea no tiene índices. Para aumentar el rendimiento del análisis de auditoría, puede colocar índices en columnas de la tabla, según el tipo de análisis que realice. Para obtener instrucciones sobre cómo indexar columnas, consulte la publicación *IBM Informix Performance Guide*.

Creación de un archivo de mandato para dbload

Para cargar la información de auditoría en la tabla que ha creado:

En primer lugar, cree un archivo de mandato ASCII para el programa de utilidad **dbload**. Este archivo de mandato debe especificar el número de columnas y el delimitador de campos que se utilizan en el archivo de datos que **onshowaudit** ha creado. Para obtener una descripción de los archivos de mandato y su uso con **dbload**, consulte la publicación *IBM Informix Migration Guide*.

Cuando cree el archivo de mandato para **dbload**, incluya la siguiente información:

Delimitador
: |

Número de columnas
: 17

Nombre de tabla
: Tabla que ha creado para recibir los datos

Nombre del archivo de datos
: Archivo de salida que ha creado (para que sirva como entrada para **dbload**)

El ejemplo siguiente utiliza la sentencia **FILE** para crear un archivo de mandato para **dbload**. El ejemplo incluye el archivo de datos **records_pat** creado en el apartado "Creación de un archivo de datos para dbload" en la página 9-4 y la tabla **frag_logs** creada en el apartado "Creación de una tabla para datos de auditoría" en la página 9-5.

```
FILE records_pat DELIMITER '|' 17;
INSERT INTO frag_logs;
```

Ahora dispone de las herramientas necesarias para cargar un archivo de datos en la tabla que ha creado.

Carga de datos de auditoría en una base de datos

Cuando disponga de la base de datos, la tabla, los datos y los archivos de mandato para el análisis de auditoría:

Utilice el mandato **dbload** para cargar los datos de auditoría en la tabla.

El ejemplo siguiente ejecuta los mandatos especificados en el archivo de mandato **user_records** para cargar datos en la base de datos **auditlogs97** creada en el apartado "Creación de una base de datos para datos de auditoría" en la página 9-5:

```
dbload -d auditlogs97 -c user_records
```

Una vez cargados los datos, inicie el análisis de auditoría con SQL.

Interpretación de datos extraídos de registros de auditoría

Al crear una tabla de base de datos para que contenga registros de auditoría que haya extraído de archivos de auditoría, debe proporcionar una columna para cada campo del registro de auditoría. La Figura 9-2 en la página 9-8 ofrece una lista de nombres de columna recomendados que se utilizan en la Figura 9-1 en la página 9-6 y describe la información que cada columna contiene.

Nombre de la columna
Descripción

adttag ONLN

date_time
Fecha y hora del suceso auditado

hostname
Nombre de servidor de la base de datos

pid ID del proceso

server Nombre del servidor de bases de datos

username
Nombre de usuario asociado con el suceso auditado

errno Número de error, si lo hay

code Código de error, si lo hay

dbname
Nombre de la base de datos

tabid Número de ID de la tabla afectada

objname
Nombre del índice y nombre de la tabla o un identificador similar (no en las tablas de auditoría creadas con servidores de bases de datos Informix anteriores a la Versión 7.0)

extra_1
Información específica del objeto y el suceso, tal como se muestra en el apartado "Campos de sucesos de auditoría" en la página 11-5

partno Información de fragmentación (no en las tablas de auditoría creadas con servidores de bases de datos Informix anteriores a la Versión 7.0)

row_num
Número de la fila física de la tabla aceptada, que combina el ID de fila y el ID de la fila anterior e identifica cada fila correspondiente a los sucesos Read Row (RDRW) (Leer fila), Insert Row (INRW) (Insertar fila), Update Current Row (UPRW) (Actualizar fila actual) y Delete Row (DLRW) (Suprimir fila)

login Nombre de inicio de sesión del usuario

flags Distintivo establecido para el suceso, tal como se muestra en el apartado "Campos de sucesos de auditoría" en la página 11-5

extra_2 Información determinada por el distintivo.

Figura 9-2. Columnas de sucesos de auditoría en la tabla de base de datos para el acceso de SQL

Capítulo 10. Sintaxis del programa de utilidad

Este capítulo contiene información sobre la sintaxis y el uso de los siguientes programas de utilidad:

- El programa de utilidad **onaudit** realiza las siguientes operaciones tanto sobre UNIX como sobre Windows:
  - Muestra máscaras de auditoría
  - Crea máscaras de auditoría
  - Modifica máscaras de auditoría
  - Suprime máscaras de auditoría
  - Muestra la configuración de la auditoría
  - Cambia actividades de auditoría globales
  - Habilita e inhabilita la auditoría
  - Establece la modalidad de error
  - Establece la auditoría obligatoria para diversos roles administrativos
  - Inicia un nuevo archivo de auditoría en el seguimiento de auditoría
  - Establece el directorio en el que residen los archivos de auditoría
  - Especifica el tamaño máximo para cada archivo de auditoría
- El programa de utilidad **onshowaudit** realiza las siguientes operaciones tanto sobre UNIX como sobre Windows:
  - Extrae información de auditoría del seguimiento de auditoría
  - Prepara datos de auditoría extraídos para el programa de utilidad **dbload**
- En UNIX, el programa de utilidad **onaudit** también realiza las siguientes operaciones:

  Determina si la auditoría de las acciones del usuario la gestiona el servidor de bases de datos o el sistema operativo.
- El programa de utilidad **onaudit** también realiza la siguiente operación en Windows:

  Establece la auditoría que el servidor de bases de datos gestiona

Programa de utilidad onaudit

El programa de utilidad **onaudit** gestiona las máscaras de auditoría y la configuración de la auditoría. Puede realizar las siguientes tareas con **onaudit**:

Debe realizar cada una de estas tareas individualmente en mandatos **onaudit** independientes. Si ejecuta el mandato **onaudit** sin ninguna opción, éste mostrará un resumen de uso.

Si su sistema tiene separación de roles, sólo el DBSSO o el AAO podrán ejecutar el programa de utilidad **onaudit.** El DBSSO sólo puede realizar funciones de **onaudit** que impliquen máscaras de auditoría y el AAO sólo puede realizar funciones de **onaudit** que impliquen parámetros de configuración de la auditoría. Sin la separación de roles, el usuario **informix** o **root** puede realizar todas estas tareas.

El DBSSO puede cambiar las máscaras de auditoría dinámicamente. Los cambios de las máscaras de usuario, predeterminadas, de plantilla y globales entran en vigor inmediatamente para todas las sesiones de usuario.

Cómo mostrar máscaras de auditoría

Elemento	Finalidad	Consideraciones clave
-o	Da salida a máscaras de auditoría.	Ninguna.
-u *máscara*	Nombra una máscara específica para visualizarla.	Puede ser cualquier máscara de auditoría existente.
-y	Responde `sí` automáticamente a la solicitud de confirmación.	Ninguna.

La opción **-o** del programa de utilidad **onaudit** envía la visualización de la máscara a la salida estándar, tal como se indica a continuación:

- Si la opción **-u** *máscara* se omite, se muestran todas las máscaras.
- Si las opciones **-y** y **-u** se omiten, **onaudit** solicita confirmación antes de mostrar todas las máscaras, que pueden constituir una gran cantidad de datos.

El ejemplo siguiente muestra el formato del archivo de salida. El formato es el mismo que el de un archivo de entrada para **onaudit**, tal como se describe en el apartado "Modificación de una máscara de auditoría".

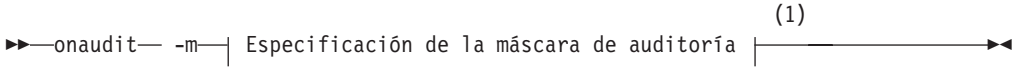
```
nombre_máscara máscara_base sucesos_auditoría
```

Puesto que el servidor de bases de datos no conserva ningún registro de la máscara base que se utiliza para crear o modificar una máscara, siempre aparece un solo guión (-) en el marcador *máscara_base*.

El ejemplo siguiente muestra la salida del mandato **onaudit -o -u pat**. Indica que la máscara de usuario individual **pat** contiene los sucesos de auditoría Lock Table (LKTB) (Bloquear tabla), Create Table (CRTB) (Crear tabla) e intentos fallidos de Add Chunk (ADCK) (Añadir fragmento).

```
pat             -       LKTB,CRTB,FADCK
```

Modificación de una máscara de auditoría



Notas:

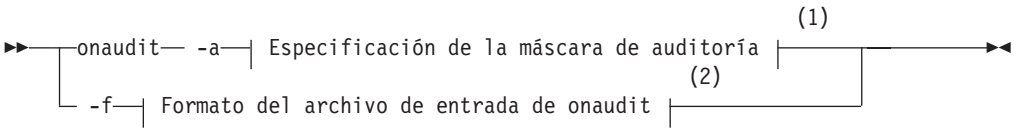
1 consulte la página "Especificación de la máscara de auditoría" en la página 10-3

Elemento	Finalidad	Consideraciones clave
-m	Modifica una máscara de auditoría existente.	Ninguna.

El ejemplo siguiente modifica una máscara de auditoría correspondiente al usuario **pat**. La máscara modificada audita los sucesos especificados en la máscara de plantilla **_Hsecure**, con la adición de todos los intentos de Lock Table (LKTB) (Bloquear tabla) y sólo los intentos fallidos de Alter Table (ALTB) (Modificar tabla).

```
onaudit -m -u pat -r _Hsecure -e +LKTB,FALTB
```

Creación o adición de una máscara de auditoría



Notas:

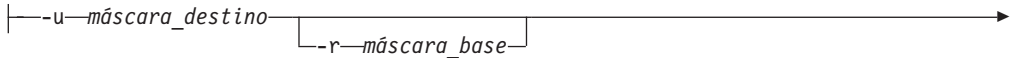
1 consulte la página "Especificación de la máscara de auditoría"

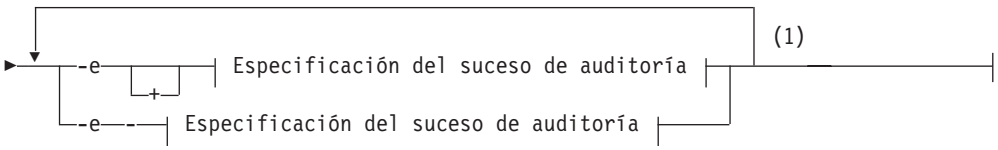
2 consulte la página "Formato del archivo de entrada de onaudit" en la página 10-4

Elemento	Finalidad	Consideraciones clave
-a	Añade una máscara de auditoría nueva.	Ninguna.
-f	Nombra un archivo que puede incluir instrucciones para añadir cualquiera o todas las máscaras de auditoría a la tabla de máscaras.	Referencias: La sintaxis del archivo de entrada se describe en el apartado "Formato del archivo de entrada de onaudit" en la página 10-4.

Especificación de la máscara de auditoría

Especificación de la máscara de auditoría:





Especificación del suceso de auditoría:

Notas:

1 Sólo se permite una ocurrencia de cada elección. No obstante, se permiten varias opciones en la misma invocación

Elemento	Finalidad	Consideraciones clave
+	Los sucesos que se indiquen aquí se deben añadir a la lista de sucesos de auditoría *máscara_destino*.	La opción + es la predeterminada y, por lo tanto, es opcional.
–	Los sucesos que se indiquen aquí se deben eliminar de la lista de sucesos de auditoría *máscara_destino*.	Ninguna.
-e	Indica que se deben añadir o eliminar sucesos de *máscara_destino*	Los sucesos especificados como argumentos para **-e** prevalecen sobre los sucesos listados en cualquier máscara base especificada con la opción **-r**.
-r *máscara_base*	Nombre de una máscara de auditoría existente. Los sucesos listados actualmente en *máscara_base* se aplican a *máscara_destino*.	Los cambios posteriores de *máscara_base* no se reflejan en las máscaras para las que *máscara_base* se haya utilizado como base. Si no se especifica ninguna *máscara_base* y no se especifica ningún suceso con el distintivo **-e**, **onaudit** creará una máscara de destino vacía.
-u *máscara_destino*	Nombra una máscara de usuario, plantilla, **_default**, **_require**o **_exclude** que se debe crear o modificar.	El identificador *máscara_destino* debe tener 32 caracteres o menos.
F*suceso*	Especifica que sólo se deben auditar los intentos de suceso anómalos.	El *suceso* puede incluir el código de suceso (mnemónico) correspondiente a cualquier suceso listado en la tabla "Mnemónicos de sucesos de auditoría" en la página 11-1.
S*suceso*	Especifica que sólo se deben auditar los intentos de suceso satisfactorios.	Igual que para **F***suceso*
suceso	Un suceso que se debe auditar, tanto si la ejecución del suceso resulta satisfactoria como si resulta anómala.	Igual que para **F***suceso*

Importante: No incluya espacios en la lista de sucesos. Se podrían producir resultados impredecibles.

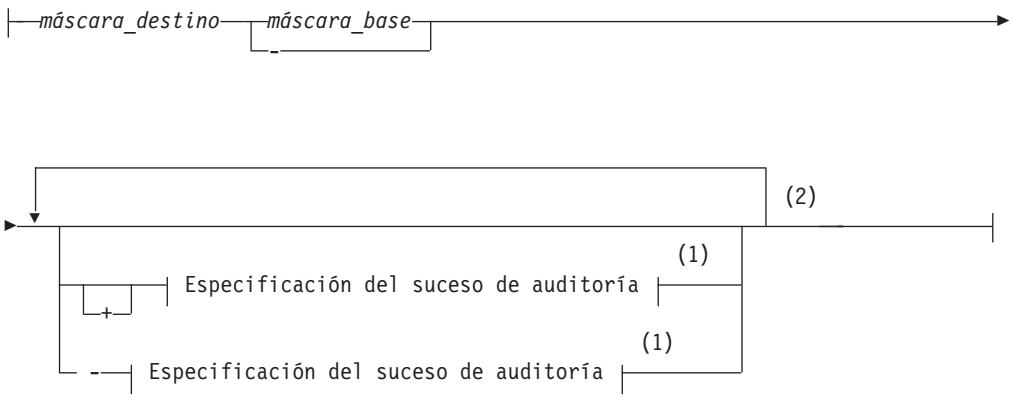
El ejemplo siguiente crea una nueva máscara de auditoría denominada **pat** para el usuario **pat**. La nueva máscara audita los sucesos especificados en la máscara de plantilla **_secureL** pero excluye los sucesos Read Row (RDRW) (Leer fila) e incluye Lock Table (LKTB) (Bloquear tabla), los intentos satisfactorios de Add Chunk (ADCK) (Añadir fragmento) y todos los intentos de Create Table (CRTB) (Crear tabla).

```
onaudit -a -u pat -r _secureL -e -RDRW, -e +LKTB,SADCK,CRTB
```

Una máscara de usuario es sólo una de las tres máscaras que especifican la auditoría para un individuo. Las instrucciones de auditoría se leen en primer lugar de la máscara de usuario y, a continuación, de las máscaras **_require** y **_exclude**. Para obtener información detallada, consulte el Capítulo 7, "Visión general de la auditoría", en la página 7-1.

Formato del archivo de entrada de onaudit

Formato del archivo de entrada de onaudit:



Notas:

1 Consulte la página "Especificación de la máscara de auditoría" en la página 10-3

2 Sólo se permite una ocurrencia de cada elección. No obstante, se permiten varias opciones en la misma invocación

Elemento	Finalidad	Consideraciones clave
+	Los sucesos que se indiquen aquí se deben añadir a la lista de sucesos de auditoría en *máscara_destino*.	Ninguna.
–	Se utiliza antes de un suceso e indica que los sucesos que se indiquen aquí se deben eliminar de la lista de sucesos de auditoría en *máscara_destino*. Si esta opción se utiliza sola, crea una máscara vacía.	Ninguna.
máscara_base	Nombre de una máscara de auditoría existente que se debe utilizar como base.	Las instrucciones de auditoría de la máscara base se copian a la máscara de destino además de (o a excepción de) los sucesos de auditoría que se indiquen aquí.
máscara_destino	Identifica la máscara de usuario, plantilla, **_default**, **_require** o **_exclude** que se debe añadir.	Los nombres de máscara no deben superar los ocho caracteres y los nombres de máscara de plantilla deben empezar con un símbolo de subrayado (_).

El ejemplo siguiente utiliza un archivo de salida modificado, creado por la opción **onaudit -o**, como archivo de entrada para **onaudit -f**:

```
onaudit -f /work/masks_feb.97
```

Para obtener un ejemplo de un archivo de entrada de **onaudit**, consulte el Capítulo 8, "Administración de la auditoría", en la página 8-1.

Supresión de una máscara de auditoría

Elemento	Finalidad	Consideraciones clave
-d	Suprime una máscara de auditoría.	Ninguna.

Elemento	Finalidad	Consideraciones clave
-u *máscara*	Nombra una máscara específica para suprimirla.	*Máscara* puede ser cualquier máscara existente.
-y	Responde `sí` automáticamente a la solicitud de confirmación.	Ninguna.

La opción **-d** del programa de utilidad **onaudit** suprime máscaras de auditoría, tal como se describe en la lista siguiente:

- Si la opción **-u** *máscara* se omite, se suprimen todas las máscaras, incluidas **_default**, **_require** y **_exclude**.
- Debido a las posibilidades de cometer un error importante, el programa de utilidad **onaudit** le solicitará confirmación antes de suprimir todas las máscaras. Por lo tanto, si las opciones **-y** y **-u** se omiten, **onaudit** solicitará confirmación.

Inicio de un nuevo archivo de auditoría

Elemento	Finalidad	Consideraciones clave
-n	Inicia un nuevo archivo de auditoría.	Ninguna.

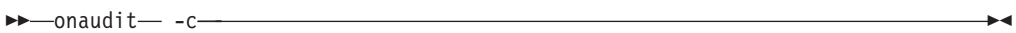
Almacenamiento de archivos de auditoría del servidor de bases de datos

Para la auditoría gestionada por el servidor de bases de datos, la opción **-n** del programa de utilidad **onaudit** cierra el archivo de auditoría del servidor de bases de datos actual, lo almacena en un directorio especificado y abre un nuevo archivo de auditoría denominado *nombre_servidor.entero*. El valor *nombre_servidor* es el nombre del servidor de bases de datos que se está auditando y *entero* es el siguiente entero disponible. Por ejemplo, si el último archivo de auditoría guardado para el servidor de bases de datos **maple** se denominaba **maple.123**, el siguiente archivo de auditoría se guardará con el nombre **maple.124**.

Almacenamiento de archivos de auditoría del sistema operativo

Para los archivos gestionados por el sistema operativo, la opción **-n** de **onaudit** cierra el archivo de auditoría del sistema operativo actual, lo almacena como parte del seguimiento de auditoría del sistema operativo y abre un nuevo archivo de auditoría. Para obtener información sobre los convenios de denominación para los archivos del seguimiento de auditoría, consulte la documentación del sistema operativo.

Cómo mostrar la configuración de la auditoría



Elemento	Finalidad	Consideraciones clave
-c	Muestra la configuración actual de la auditoría.	Ninguna.

La opción **-c** indica a **onaudit** que debe mostrar el estado actual de la auditoría.

La Figura 10-1 muestra un ejemplo de la salida de configuración de la auditoría en UNIX.

```
onaudit -c

Onaudit -- Programa de utilidad de control del subsistema de auditoría
Copyright (c) IBM Corp., 1998-2007

Configuración actual del sistema auditor:
      ADTMODE         = 1
      ADTERR          = 0
      ADTPATH         = /tmp
      ADTSIZE         = 20000
      Fichero auditor = 64
```

Figura 10-1. Ejemplo de salida de la configuración de la auditoría en UNIX

La Figura 10-2 muestra un ejemplo de la salida de configuración de la auditoría en Windows.

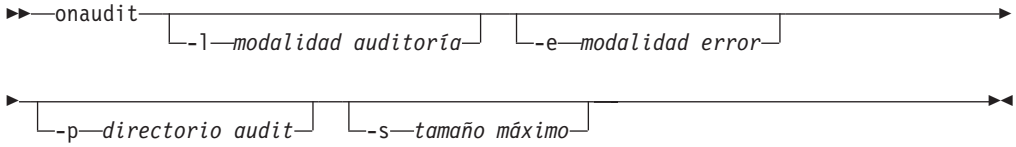
```
onaudit -c

Onaudit -- Programa de utilidad de control del subsistema de auditoría
Copyright (c) IBM Corp., 1998-2007

Configuración actual del sistema auditor:
      ADTMODE         = 1
      ADTERR          = 0
      ADTPATH         = %informixdir%/aaodir
      ADTESIZE        = 50000
      Fichero auditor = 0
```

Figura 10-2. Ejemplo de salida de la configuración de la auditoría en Windows

Cambio de la configuración de la auditoría



Elemento	Finalidad	Consideraciones clave
-e *modalidad error*	Especifica el método de manejo de errores para la auditoría que se debe emplear cuando un registro no se puede grabar en el archivo de auditoría o en el registro de sucesos.	**Restricciones**: El parámetro *modalidad error* puede tener uno de los valores siguientes: `0`, `1`, `3`. **Información adicional**: Esta opción pertenece al conjunto de valores para el parámetro de configuración ADTERR del archivo ADTCFG. El valor sólo se puede cambiar cuando la auditoría está activada. Para obtener información detallada sobre los valores válidos de *modalidad error*, consulte el apartado "Uso de la opción -e" en la página 10-8.

Elemento	Finalidad	Consideraciones clave
-l *modalidad auditoría*	Especifica la modalidad de auditoría.	**Restricciones:** El parámetro *modalidad auditoría* puede tener uno de los valores siguientes: `0`, `1`, `3`, `5`, `7`. **Información adicional**: Esta opción pertenece al conjunto de valores para el parámetro de configuración ADTMODE del archivo ADTCFG. Para obtener información detallada sobre los valores válidos de *modalidad auditoría*, consulte el apartado "Uso de la opción -l" en la página 10-9.
-p *directorio audit*	Especifica el directorio en el que el servidor de bases de datos crea archivos de auditoría.	**Restricciones**: Sólo se puede cambiar el valor de *directorio audit* para la auditoría gestionada por el servidor de bases de datos y sólo cuando la auditoría está en vigor. **Información adicional**: Esta opción pertenece al conjunto de valores para el parámetro de configuración ADTPATH del archivo ADTCFG. El cambio se produce en el siguiente intento de grabación. El servidor de bases de datos inicia un nuevo archivo de auditoría en el nuevo directorio, empezando con el primer número disponible igual o superior a 0.
-s *tamaño máximo*	Especifica el tamaño máximo (en bytes) de un archivo de auditoría.	**Restricciones**: El *tamaño máximo* puede ser cualquier valor entre 10.240 bytes y aproximadamente 2 gigabytes (el valor máximo de un entero de 32 bits). Si especifica un tamaño inferior al mínimo, automáticamente se establecerá como valor el tamaño mínimo. Sólo se puede especificar el valor de *tamaño máximo* para la auditoría gestionada por el servidor de bases de datos y sólo cuando la auditoría está en vigor. **Información adicional**: Esta opción pertenece al conjunto de valores para el parámetro de configuración ADTSIZE del archivo ADTCFG. Cuando un archivo de auditoría alcanza o supera el *tamaño máximo*, el servidor de bases de datos cierra el archivo actual e inicia un nuevo archivo de auditoría.

Para obtener información sobre los parámetros de configuración de la auditoría del archivo **ADTCFG**, consulte el Capítulo 12, "El archivo ADTCFG", en la página 12-1.

Los cambios realizados en la configuración de la auditoría con **onaudit** entran en vigor inmediatamente para todas las sesiones del usuario, incluidas las sesiones existentes. Para obtener información sobre cómo interactúan los cambios de la configuración de la auditoría con el archivo **ADTCFG**, consulte el Capítulo 7, "Visión general de la auditoría", en la página 7-1.

Uso de la opción -e

Esta sección trata sobre los valores que se pueden entrar para la opción **-e** *modalidad error* de **onaudit**.

Para especificar la *modalidad continua*, entre `0` como argumento para la opción **-e**. En la modalidad continua, el servidor de bases de datos sigue procesando la hebra y anota el error en el registro de mensajes. Los errores de los intentos posteriores de grabar en el archivo de auditoría también se envían al registro de mensajes. Para obtener información sobre el registro de mensajes, consulte la publicación *IBM Informix Administrator's Guide*.

Para especificar una de las *modalidades de parada*, que suspenden el proceso o cierran el servidor de bases de datos, entre uno de los argumentos siguientes en la opción **-e**:

- Entre `1` para suspender el proceso de una hebra cuando el servidor de bases de datos no pueda grabar un registro en el archivo de auditoría actual y tenga que seguir intentando la grabación hasta que resulte satisfactoria.
- Entre `3` para cerrar el servidor de bases de datos.

Uso de la opción -l

Esta sección trata sobre los valores que se pueden entrar para la opción **-l** *modalidad audit* de **onaudit**.

El valor `0` *desactiva* la auditoría. El servidor de bases de datos detiene la auditoría para todas las sesiones existentes y las sesiones nuevas no se auditan.

Todos los demás valores *activan* la auditoría, tal como se indica a continuación:

- `1` activa la auditoría para todas las sesiones, pero no audita automáticamente las acciones del DBSSO ni del DBSA.
- `3` activa la auditoría y audita automáticamente las acciones del DBSSO.
- `5` activa la auditoría y audita automáticamente las acciones del DBSA.
- `7` activa la auditoría y audita automáticamente las acciones del DBSSO y del DBSA.

Programa de utilidad onshowaudit

El programa de utilidad **onshowaudit** permite extraer información de un seguimiento de auditoría. Puede indica a este programa de utilidad que debe extraer información correspondiente a un determinado usuario o servidor de bases de datos o a ambos. Esta información permite aislar un determinado subconjunto de datos de un seguimiento de auditoría potencialmente grande.

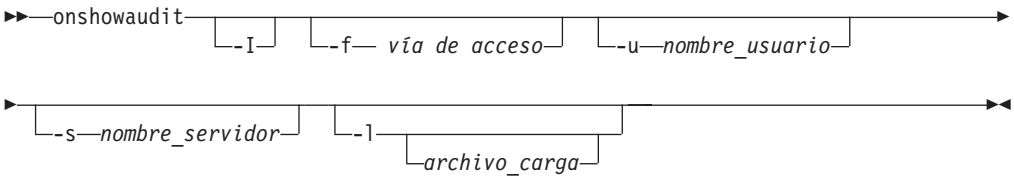
A los registros se les da formato para la salida. De modo predeterminado, **onshowaudit** muestra la información extraída en la pantalla. Puede redirigir la salida formateada a un archivo o un conducto y puede especificar que **onshowaudit** debe volver a dar formato a la salida para poder cargarla en una tabla de base de datos de Informix.

El programa de utilidad **onshowaudit** extrae datos de un seguimiento de auditoría pero no procesa los registros ni los suprime del seguimiento de auditoría. Acceda al seguimiento de auditoría sólo con el programa de utilidad **onshowaudit**, que tiene su propia protección:

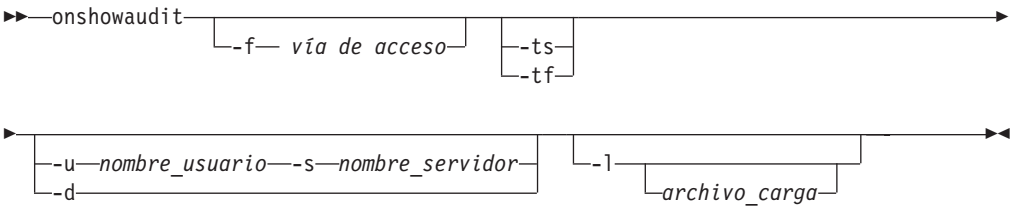
- Con la separación de roles desactivada, sólo el usuario **informix** (y el usuario **root** en UNIX) puede ejecutar **onshowaudit**.
- Con la separación de roles activada, sólo el AAO puede ejecutar **onshowaudit**.

Sintaxis

A continuación se detalla la sintaxis de la línea de mandatos de UNIX de **onshowaudit**.



A continuación se detalla la sintaxis de la línea de mandatos de Windows de **onshowaudit**.



Importante: Si incluye la opción **-l** del mandato **onshowaudit**, deberá eliminar las seis líneas de cabecera que aparecen en el archivo de salida antes de utilizar dicho archivo como entrada para **dbload** o para un archivo externo.

Elementos

La tabla siguiente identifica los términos de sintaxis que pueden aparecer en una línea de mandatos de **onshowaudit**.

Cualquier opción de la línea de mandatos que especifique determina qué parte del seguimiento de auditoría utiliza el programa de utilidad **onshowaudit**.

Elemento	Finalidad	Consideraciones clave
-d	En Windows, asume los valores predeterminados para el usuario (*usuario actual*) y el servidor de bases de datos (**INFORMIXSERVER**)	Ninguna
-f *vía de acceso*	Especifica un seguimiento de auditoría específico a examinar, sólo para la auditoría gestionada por el servidor de bases de datos	Si esta opción se omite o si la *vía de acceso* es sólo un *nombre de archivo*, consulte las notas que van inmediatamente a continuación de esta tabla.
-I	En UNIX, utiliza el seguimiento de auditoría del servidor de bases de datos Informix	Ninguna
-l	Indica a **onshowaudit** que debe extraer información con delimitadores para que se pueda redirigir a un archivo o a un conducto y se pueda cargar en una tabla de base de datos o en otra aplicación que acepte los datos delimitados	Para obtener información sobre el formato de archivo, consulte el Capítulo 9, "Análisis de auditoría", en la página 9-1. Para obtener información sobre el programa de utilidad **dbload**, consulte la publicación *IBM Informix Migration Guide*. Para obtener información sobre cómo cargar datos con tablas externas, consulte la publicación *IBM Informix Administrator's Reference*.
-tf	En Windows, muestra sólo registros de auditoría *anómalos*	Ninguna
-ts	En Windows, muestra sólo registros de auditoría *satisfactorios*	Ninguna
-s *nombre_servidor*	Especifica el servidor de bases de datos sobre el que se debe extraer información de auditoría	Ninguna

Elemento	Finalidad	Consideraciones clave
-u *nombre_usuario*	Especifica el nombre de inicio de sesión de un usuario sobre el que se debe extraer información de auditoría	Ninguna

Si se omite **-f**, **onshowaudit** buscará los archivos de auditoría en el directorio **ADTPATH** (establecido con el programa de utilidad **onaudit** o en el archivo **ADTCFG**). El programa de utilidad **onshowaudit** extrae datos de todos los archivos de auditoría que encuentra que están en secuencia, empezando por el entero más bajo.

La opción **-f** *vía de acceso* especifica el directorio y el nombre de archivo de los archivos de auditoría. El directorio y el nombre de archivo de auditoría deben cumplir los niveles de seguridad mínimos. El directorio debe ser propiedad del usuario **informix**, pertenecer al grupo de AAO y no debe permitir el acceso público (permiso 0770). Los archivos deben tener permisos comparables (permiso 0660). Los archivos no deben ser enlaces simbólicos a otras ubicaciones. El directorio, no obstante, puede ser un enlace simbólico. Si el directorio y los archivos de auditoría no son seguros, **onshowaudit** devolverá un mensaje de error y no mostrará los resultados de la auditoría.

Si se especifica un *nombre de vía de acceso incompleto* (sólo un nombre de archivo), el programa de utilidad **onshowaudit** buscará este archivo en el directorio **ADTPATH** y extraerá datos de auditoría de él.

Si se especifica un *nombre de vía de acceso completo*, el programa de utilidad **onshowaudit** extraerá datos de auditoría del archivo especificado.

Para obtener información sobre los parámetros de configuración de la auditoría del archivo **ADTCFG**, consulte el Capítulo 12, "El archivo ADTCFG", en la página 12-1.

El servidor de bases de datos no audita la ejecución del programa de utilidad **onshowaudit**.

Importante: La versión 7.2 y las versiones posteriores del programa de utilidad **onshowaudit** pueden analizar y procesar las estructuras de registros nuevas y actualizadas de tablas e índices fragmentados, que pueden abarcar varias particiones. Si utiliza la versión 7.2 o una versión posterior de **onshowaudit** para analizar registros creados por un servidor de bases de datos anterior a la versión 7.0, es posible que obtenga resultados imprecisos. La versión 7.2 y las versiones posteriores de **onshowaudit** esperan encontrar un campo adicional para la fragmentación (**partno**) en determinados registros de auditoría, pero este campo no se encuentran los registros de auditoría anteriores a la versión 7.0.

Capítulo 11. Mnemónicos y campos de los sucesos de auditoría

Este apéndice contiene las tablas siguientes:

- Los sucesos que se pueden auditar de cada servidor de bases de datos, listados alfabéticamente por mnemónico de suceso

  Consulte el apartado "Mnemónicos de sucesos de auditoría".
- Registros de sucesos de auditoría y sus campos

  Consulte el apartado "Campos de sucesos de auditoría" en la página 11-5.

Importante: El recurso de auditoría de seguridad de Dynamic Server sólo audita los sucesos listados en este apéndice. Es posible que se encuentre con sentencias de SQL adicionales que el recurso de auditoría de seguridad no audita.

Mnemónicos de sucesos de auditoría

Esta tabla contiene un listado alfabético de mnemónicos de sucesos de auditoría (códigos de suceso) correlacionados con el nombre del suceso.

Mnemónico	Nombre del suceso
ACTB	Access Table
ADCK	Add Chunk
ADLG	Add Transaction Log
ALFR	Alter Fragment
ALIX	Alter Index
ALLC	Alter Security Label Component
ALME	Alter Access Method
ALOC	Alter Operator Class
ALOP	Alter Optical Cluster
ALSQ	Alter Sequence
ALTB	Alter Table
BGTX	Begin Transaction
CLDB	Close Database
CMTX	Commit Transaction
CRAG	Create Aggregate
CRAM	Create Audit Mask
CRBS	Create Storage Space
CRBT	Create Opaque Type
CRCT	Create Cast
CRDB	Create Database
CRDM	Create Domain
CRDS	Create Dbspace

Mnemónico	Nombre del suceso
CRDT	Create Distinct Type
CRIX	Create Index
CRLB	Create Security Label
CRLC	Create Security Label Component
CRME	Create Access Method
CROC	Create Operator Class
CROP	Create Optical Cluster
CRPL	Create Security Policy
CRPT	Decryption failure or attempt
CRRL	Create Role
CRRT	Create Named Row Type
CRSN	Create Synonym
CRSP	Create SPL Routine
CRSQ	Create Sequence
CRTB	Create Table
CRTR	Create Trigger
CRVW	Create View
CRXD	Create XA Data Source
CRXT	Create XA Data Source Type
DLRW	Delete Row
DNCK	Bring Chunk Off-line
DNDM	Disable Disk Mirroring
DRAG	Drop Aggregate
DRAM	Delete Audit Mask
DRBS	Drop Storage Space
DRCK	Drop Chunk
DRCT	Drop Cast
DRDB	Drop Database
DRDM	Drop Domain
DRDS	Drop Dbspace
DRIX	Drop Index
DRLB	Drop Security Label
DRLC	Drop Security Label Component
DRLG	Drop Transaction Log
DRME	Drop Access Method
DROC	Drop Operator Class
DROP	Drop Optical Cluster
DRPL	Drop Security Policy
DRRL	Drop Role
DRRT	Drop Named Row Type
DRSN	Drop Synonym

Mnemónico	Nombre del suceso
DRSP	Drop SPL Routine
DRSQ	Drop Sequence
DRTB	Drop Table
DRTR	Drop Trigger
DRTY	Drop Type
DRVW	Drop View
DRXD	Drop XA Data Source
DRXT	Drop XA Data Source Type
EXSP	Execute SPL Routine
GRDB	Grant Database Access
GRDR	Grant Default Role
GRFR	Grant Fragment Access
GRLB	Grant Security Label
GRRL	Grant Role
GRSA	Grant DBSECADM
GRSS	Grant SETSESSIONAUTH
GRTB	Grant Table Access
GRXM	Grant Exemption
INRW	Insert Row
LGDB	Change Database Log Mode
LKTB	Lock Table
LSAM	List Audit Masks
LSDB	List Databases
MDLG	Modify Transaction Logging
ONAU	**onaudit**
ONBR	**onbar**
ONCH	**oncheck**
ONIN	**oninit**
ONLG	**onlog**
ONLO	**onload**
ONMN	**onmonitor**
ONMO	**onmode**
ONPA	**onparams**
ONPL	**onpload**
ONSP	**onspaces**
ONST	**onstat**
ONTP	**ontape**
ONUL	**onunload**
OPDB	Open Database
RDRW	Read Row
RLOP	Release Optical Cluster

Mnemónico	Nombre del suceso
RLTX	Rollback Transaction
RMCK	Clear Mirrored Chunks
RNDB	Rename Database
RNDS	Rename dbspace
RNIX	Rename Index
RNLB	Rename Security Label
RNLC	Rename Security Label Component
RNPL	Rename Security Policy
RNSQ	Rename Sequence
RNTC	Rename Table/Column
RSOP	Reserve Optical Cluster
RVDB	Revoke Database Access
RVDR	Revoke Default Role
RVFR	Revoke Fragment Access
RVLB	Revoke Security Label
RVRL	Revoke Role
RVTB	Revoke Table Access
RVSA	Revoke DBSECADM
RVSS	Revoke SETSESSIONAUTH
RVXM	Revoke Exemption
SCSP	SYSTEM Command, SPL Routine
STCO	Set Collation
STCN	Set Constraint
STDF	Set Debug File
STDP	Set Database Password
STDS	Set Dataskip
STEP	Set Encryption Password
STEV	Set Environment
STEX	Set Explain
STIL	Set Isolation Level
STLM	Set Lock Mode
STNC	Set No Collation
STOM	Set Object Mode
STOP	Stop Violations
STPR	Set Pdqpriority
STRL	Set Role
STRS	Set Resident
STRT	Start Violations
STSA	Set Session Authorization
STSC	Set Statement Cache
STSN	Start New Session

Mnemónico	Nombre del suceso
STTX	Set Transaction Mode
SVXD	Save External Directives
TCTB	Truncate Table
TMOP	Time Optical Cluster
ULTB	Unlock Table
UPAM	Update Audit Mask
UPCK	Bring Chunk Online
UPDM	Enable Disk Mirroring
UPRW	Update Row
USSP	Update Statistics, SPL Routine
USTB	Update Statistics, Table

Campos de sucesos de auditoría

La tabla siguiente contiene información de sucesos de auditoría en orden alfabético según el código mnemónico.

La tabla muestra la información del suceso de auditoría que el programa de utilidad **onshowaudit** captura en forma de tabla para el análisis de auditoría:

- La columna **Suceso** muestra el nombre del suceso.
- La columna **Mnemónico** contiene el acrónimo que los programas de utilidad del servidor de bases de datos utilizan para identificar sucesos de auditoría.
- La columna **Contenido de la variable** contiene otras categorías de información de **onshowaudit** que aparecen para el suceso en dicha fila. Estas categorías de información son las siguientes: **dbname**, **tabid**, **objname**, **extra_1**, **partno**, **row_num**, **login**, **flags** y **extra_2**.

  Para algunos sucesos, el programa de utilidad **onshowaudit** coloca dos informaciones diferentes en el campo **extra_2**. En este caso, las dos partes se separan mediante un punto y coma.
- La sección Notas incluida después de la tabla proporciona más información sobre algunas de las entradas de la columna **Contenido de la variable**.

Consejo: Las listas de otorgamientos pueden ser largas para sentencias de SQL como GRANT y REVOKE. Si la lista correspondiente a un suceso que se debe auditar no cabe en un solo registro, el servidor de bases de datos creará varios registros de auditoría para incluir la información completa.

Suceso	Mnemónico	Contenido de la variable
Access Table	ACTB	dbname: nombre bd tabid: nombre propietario, ID de tabla
Chunk, Add	ADCK	dbname: espacio bd, nombre extra_1: desplazamiento flags: estado duplicación[1] extra_2: vía de acceso y tamaño

Suceso	Mnemónico	Contenido de la variable
Transaction Log, Add	ADLG	dbname: espacio bd, nombre extra_1: tamaño del registro
Alter Fragment	ALFR	dbname: nombre bd tabid: ID de tabla objname: nombre índice extra_1: tipo operación[18] login: propietario flags: distintivos frag[15] extra_2: espacios bd
Index, Alter	ALIX	dbname: nombre bd tabid: ID de tabla login: propietario[14] flags: distintivo clúster[9,14] extra_2: nombre índice[14]
Security Label Component, Alter	ALLC	dbname: nombre bd objname: nombre de componente extra_2: tipo de componente
Access Method, Alter	ALME	dbname: nombre bd tabid: acceso, ID método objname: método acceso, nombre login: método acceso, propietario
Operator Class, Alter	ALOC	dbname: nombre bd extra_1: tamaño clúster login: propietario extra_2: nombre clúster
Optical Cluster, Alter	ALOP	dbname: nombre bd extra_1: tamaño clúster login: propietario extra_2: nombre clúster
Sequence, Alter	ALSQ	dbname: nombre bd tabid: ID de tabla

Suceso	Mnemónico	Contenido de la variable
Table, Alter	ALTB	dbname: nombre bd tabid: ID de tabla anterior extra_1: ID de tabla nuevo[14] partno: ID_frag extra_2: nueva lista núm. pieza[14]
Transaction, Begin	BGTX	
Database, Close	CLDB	dbname: nombre bd
Transaction, Commit	CMTX	
Aggregate, Create	CRAG	dbname: nombre bd objname: nombre agregado login: propietario
Audit Mask, Create	CRAM	login: ID usuario
Storage Space, Create	CRBS	dbname: almacenamiento, nombre espacio login: propietario flags: estado duplicación[1] extra_2: soporte
Opaque Type, Create	CRBT	dbname: nombre bd objname: nombre tipo opaco login: tipo opaco, propietario
Cast, Create	CRCT	dbname: nombre bd tabid: ID de tipo del tipo from objname: nombre función o ″-″ extra_1: xid del tipo from partno: ID de tipo del tipo to row_num: xid del tipo to login: propietario función o ″-″
Database, Create	CRDB	dbname: espacio bd extra_2: nombre bd
Domain, Create	CRDM	
Dbspace, Create	CRDS	dbname: espacio bd, nombre flags: estado duplicación[1]

Suceso	Mnemónico	Contenido de la variable
Distinct Type, Create	CRDT	dbname: nombre bd objname: nombre de tipo diferenciado login: tipo diferenciado, propietario
Index, Create	CRIX	dbname: nombre bd tabid: ID de tabla objname: nombre índice login: propietario flags: distintivos frag[15] extra_2: lista espacios bd
Security Label, Create	CRLB	dbname: nombre bd objname: nombre de policy.label (politica.etiqueta) extra_2: lista de valores de componente
Security Label Component, Create	CRLC	dbname: nombre bd objname: nombre de componente extra_2: lista de componentes
Access Method, Create	CRME	dbname: nombre bd tabid: ID método acceso objname: nombre método acceso login: propietario método acceso
Operator Class, Create	CROC	dbname: nombre bd tabid: ID clase operador objname: nombre clase operador login: propietario
Optical Cluster, Create	CROP	dbname: nombre bd tabid: ID de tabla extra_1: tamaño clúster login: propietario extra_2: nombre clúster
Security Policy, Create	CRPL	dbname: nombre bd objname: nombre de política extra_2: lista de componentes

Suceso	Mnemónico	Contenido de la variable
Encryption/Decryption	CRPT	dbname: nombre bd objname: sentencia
Create Role	CRRL	dbname: nombre bd objname: nombre rol
Named Row Type, Create	CRRT	dbname: nombre bd tabid: xid tipo fila objname: nombre tipo fila con nombre login: propietario tipo fila con nombre
Synonym, Create	CRSN	dbname: nombre bd tabid: ID tabla sin. extra_1: ID tabla base login: propietario flags: tipo sin.[7] extra_2: nombre sinónimo
SPL Routine, Create	CRSP	dbname: nombre bd tabid: ID proc. login: propietario extra_2: nombre procedimiento
Sequence, Create	CRSQ	dbname: nombre bd tabid: ID de tabla objname: propietario
Table, Create	CRTB	dbname: nombre bd tabid: ID de tabla objname: propietario login: nombre tabla flags: distintivos frag[15] extra_2: lista espacios bd
Trigger, Create	CRTR	dbname: nombre bd tabid: ID de tabla row_num: ID desencadenante[14] login: propietario[14] extra_2: nombre desencadenante[14]

Suceso	Mnemónico	Contenido de la variable
View, Create	CRVW	dbname: nombre bd tabid: ID tabla vista login: propietario extra_2: nombre vista
XADatasource, Create	CRXD	dbname: nombre bd objname: propietario objname: nombre de fuente de datos XA
XADatasource Type, Create	CRXT	dbname: nombre bd objname: propietario objname: nombre de tipo de fuente de datos XA
Row, Delete	DLRW	dbname: nombre bd tabid: ID de tabla extra_1: núm. pieza partno: ID_frag row_num: núm. fila[14]
Chunk, Bring Off-line	DNCK	extra_1: número fragmento flags: estado duplicación[1]
Disk Mirroring, Disable	DNDM	extra_1: número espacio bd
Display Page	DPPG	tabid: núm. página
Aggregate, Drop	DRAG	dbname: nombre bd objname: nombre agregado login: propietario
Audit Mask, Delete	DRAM	login: ID usuario
Storage Space, Drop	DRBS	dbname: nombre espacio almacenamiento
Chunk, Drop	DRCK	dbname: nombre espacio bd flags: estado duplicación[1] extra_2: vía acceso
Cast, Drop	DRCT	dbname: nombre bd tabid: ID de tipo del tipo from extra_1: xid del tipo **from** partno: tipo del tipo **to** row_num: xid del tipo **to**
Database, Drop	DRDB	dbname: nombre bd
Domain, Drop	DRDM	

Suceso	Mnemónico	Contenido de la variable
Dbspace, Drop	DRDS	dbname: nombre espacio bd
Index, Drop	DRIX	dbname: nombre bd tabid: ID de tabla login: propietario extra_2: nombre índice
Security Label, Drop	DRLB	dbname: nombre bd objname: nombre de policy.label (politica.etiqueta)
Security Label Component, Drop	DRLC	dbname: nombre bd objname: nombre de componente
Transaction Log, Drop	DRLG	extra_1: número registro
Access Method, Drop	DRME	dbname: nombre bd tabid: ID método acceso objname: nombre método acceso login: propietario método acceso
Operator Class, Drop	DROC	dbname: nombre bd objname: nombre clase operador login: propietario
Optical Cluster, Drop	DROP	dbname: nombre bd login: propietario extra_2: nombre clúster
Security Policy, Drop	DRPL	dbname: nombre bd objname: nombre de política
Role, Drop	DRRL	dbname: nombre bd objname: nombre rol
Named Row Type, Drop	DRRT	dbname: nombre bd tabid: ID de tipo eliminado
Synonym, Drop	DRSN	dbname: nombre bd tabid: ID tabla sin. login: propietario extra_2: nombre sin.
SPL Routine, Drop	DRSP	dbname: nombre bd login: propietario extra_2: nombre esp.
Sequence, Drop	DRSQ	dbname: nombre bd tabid: ID de tabla

Suceso	Mnemónico	Contenido de la variable
Table, Drop	DRTB	dbname: nombre bd tabid: ID de tabla objname: nombre tabla login: propietario flags: distint. elim.[21] extra_2: lista núm. pieza
Trigger, Drop	DRTR	dbname: nombre bd row_num: ID desencadenante login: propietario extra_2: nombre desenc.
Type, Drop	DRTY	dbname: nombre bd objname: nombre tipo login: propietario tipo
View, Drop	DRVW	dbname: nombre bd tabid: ID tabla vista flags: distint. elim.[21]
XADatasource, Drop	DRXD	dbname: nombre bd objname: propietario objname: nombre de fuente de datos XA
XADatasource Type, Drop	DRXT	dbname: nombre bd objname: propietario objname: nombre de tipo de fuente de datos XA
SPL Routine, Execute	EXSP	dbname: nombre bd tabid: ID proc.
Grant Database Access	GRDB	dbname: nombre bd extra_1: privilegio[5] extra_2: cesionarios[4]
Grant Default Role	GRDR	

Suceso	Mnemónico	Contenido de la variable
Grant Fragment Access	GRFR	dbname: nombre bd tabid: ID de tabla objname: fragmento extra_1: privilegio[5, 14] login: otorgante extra_2: cesionarios[4, 14]
Grant Security Label	GRLB	dbname: nombre bd objname: nombre de policy.label (politica.etiqueta) login2: cesionario[4]
Grant Role	GRRL	dbname: nombre bd objname: nombre rol login: otorgante extra_2: cesionarios[4]
Grant DBSECADM	GRSA	login2: cesionario
Grant SETSESSIONAUTH	GRSS	dbname: nombre bd extra_2: lista de usuarios alternativa[4] login2: cesionario[4]
Grant Table Access	GRTB	dbname: nombre bd tabid: ID de tabla extra_1: privilegio[5, 14] login: otorgante extra_2: cesionario[4, 14], actualizar columnas, seleccionar columnas[4, 14]
Grant Exemption	GRXM	dbname: nombre bd objname: nombre de política extra_2: regla login2: cesionario[4]
Row, Insert	INRW	dbname: nombre bd tabid: ID de tabla partno: ID_frag row_num: ID fila
Database Log Mode, Change	LGDB	dbname: nombre bd flags: estado registro[6]

Suceso	Mnemónico	Contenido de la variable
Table, Lock	LKTB	dbname: nombre bd tabid: ID de tabla flags: modalidad bloqueo[8]
Audit Masks, List	LSAM	
Databases, List	LSDB	
Modify Transaction Logging	MDLG	flags: distint. registro almac. interm[2]
onaudit	ONAU	extra_2: línea mandatos
onbar	ONBR	extra_2: línea mandatos
oncheck	ONCH	extra_2: línea mandatos
oninit	ONIN	extra_2: línea mandatos
onlog	ONLG	extra_2: línea mandatos
onload	ONLO	extra_2: línea mandatos
onmonitor	ONMN	extra_2: línea mandatos
onmode	ONMO	extra_2: línea mandatos
onparams	ONPA	extra_2: línea mandatos
onpload	ONPL	extra_2: línea mandatos
onspaces	ONSP	extra_2: línea mandatos
onstat	ONST	extra_2: línea mandatos
ontape	ONTP	extra_2: línea mandatos
onunload	ONUL	extra_2: línea mandatos
Database, Open	OPDB	dbname: nombre bd flags: distintivo exclusivo extra_2: contraseña bd
Row, Read	RDRW	dbname: nombre bd tabid: ID de tabla extra_1: núm. pieza partno: ID_frag row_num: ID fila[14]
Optical Cluster, Release	RLOP	dbname: nombre familia row_num: número volumen
Transaction, Rollback	RLTX	
Chunks, Clear Mirrored	RMCK	extra_1: número espacio bd
Rename Database	RNDB	dbname: nombre bd objname: nuevo nombre bd login: ID usuario

Suceso	Mnemónico	Contenido de la variable
Rename dbspace	RNDS	dbname: nombre espacio bd objname: nuevo nombre espacio bd
Rename index	RNIX	dbname: nombre de índice objname: nuevo nombre de índice
Security Label, Rename	RNLB	dbname: nombre bd objname: nombre anterior de policy.label (política.etiqueta) extra_2: nuevo nombre de etiqueta
Security Label Component, Rename	RNLC	dbname: nombre bd objname: nombre anterior de componente extra_2: nuevo nombre de componente
Security Policy, Rename	RNPL	dbname: nombre bd objname: nombre anterior de política extra_2: nuevo nombre de política
Sequence, Rename	RNSQ	dbname: nombre bd tabid: ID de tabla
Table/ Column, Rename	RNTC	dbname: nombre bd tabid: ID de tabla objname: nuevo nombre tabla/col. extra_1: núm. col(*) login: propietario extra_2: nombre tabla(**)
Optical Cluster, Reserve	RSOP	dbname: nombre familia row_num: número volumen
Revoke Database Access	RVDB	dbname: nombre bd extra_1: privilegio[5] extra_2: revocados[4]
Revoke Default Role	RVDR	

Suceso	Mnemónico	Contenido de la variable
Revoke Fragment Access	RVFR	dbname: nombre bd tabid: ID de tabla objname: fragmento extra_1: privilegio[5, 14] login: revocante extra_2: revocados[4, 14]
Revoke Security Label	RVLB	dbname: nombre bd objname: nombre de policy.label (politica.etiqueta) login2: cesionario[4]
Revoke Role	RVRL	dbname: nombre bd objname: nombre rol login: revocante extra_2: revocados[4]
Revoke DBSECADM	RVSA	login2: cesionario[4]
Revoke SETSESSIONAUTH	RVSS	dbname: nombre bd extra_2: lista de usuarios alternativa[4] login2: cesionario[4]
Revoke Table Access	RVTB	dbname: nombre bd tabid: ID de tabla extra_1: privilegio[5, 14] login: revocante flags: distint. elim.[21] extra_2: revocados[4, 14]
Revoke Exemption	RVXM	dbname: nombre bd objname: nombre de política extra_2: regla login2: cesionario[4]
SPL Routine, System Command	SCSP	extra_2: serie mandato
Collation, Set	STCO	dbname: nombre bd objname: nombre de entorno local
Constraint, Set	STCN	dbname: nombre bd flags: modalidad restricción[11] extra_2: nombres restricciones

Suceso	Mnemónico	Contenido de la variable
Set Debug File	STDF	dbname: nombre bd extra_2: vía acceso archivo
Set Database Password	STDP	dbname: nombre bd login: ID usuario
Set Dataskip	STDS	flags: distintivos salto[16] extra_2: lista espacios bd
Set Encryption Password	STEP	dbname: nombre bd
Set Environment	STEV	objname: variable y valor de entorno
Set Explain	STEX	flags: distintivos expl.[12]
Isolation Level, Set	STIL	extra_1: nivel aislamiento[3]
Set Lock Mode	STLM	flags: distintivos espera[13]
Set No Collation	STNC	dbname: nombre bd objname: nombre de entorno local
Set Object Mode	STOM	dbname: nombre bd tabid: ID de tabla extra_1: distintivo modalidad mandato[23] flags: distintivo tipo objeto[2 4] extra_2: nombres objetos
Stop Statement	STOP	dbname: nombre bd tabid: ID de tabla
Set Pdqpriority	STPR	flags: nivel pr[17]
Set Role	STRL	dbname: nombre bd objname: nombre rol
Set Resident	STRS	
Start Statement	STRT	dbname: nombre bd tabid: ID de tabla extra_1: Vio_tid flags: Dia_tid
Set Session Authorization	STSA	dbname: nombre bd login: nuevo nombre usuario
Set Statement Cache	STSC	objname: nombre sentencia
Start New Session	STSN	
Set Transaction Mode	STTX	extra_1: operación[20] flags: distintivos modalidad[19] extra_2:

Suceso	Mnemónico	Contenido de la variable
Save External Directives	SVXD	dbname: nombre bd objname: activo/inactivo/prueba objname: texto directivo
Truncate Table	TCTB	dbname: nombre bd tabid: ID de tabla objname: nombre tabla
Optical Cluster, Time	TMOP	flags: distintivo hora[13]
Table, Unlock	ULTB	dbname: nombre bd tabid: ID de tabla
Audit Mask, Update	UPAM	login: ID usuario
Chunk, Bring Online	UPCK	extra_1: número fragmento flags: estado duplicación[1]
Disk Mirroring, Enable	UPDM	extra_1: número espacio bd
Row, Update Current	UPRW	dbname: nombre bd tabid: ID de tabla extra_1: núm. pieza anterior row_num: ID fila anterior[14] flags: ID fila nueva extra_2: núm. pieza nuevo
SPL Routine, Update Statistics	USSP	dbname: nombre bd tabid: ID proc.
Table, Update Statistics	USTB	dbname: nombre bd tabid: ID de tabla

Notas

1. Estado de duplicación:
   - **0** No duplicado
   - **1** Duplicado
2. Distintivo de registro en almacenamiento intermedio:
   - **0** Almacenamiento intermedio desactivado
   - **1** Almacenamiento intermedio activado
3. Nivel de aislamiento:
   - **0** Sin transacciones
   - **1** Lectura sucia
   - **2** Lectura confirmada
   - **3** Estabilidad del cursor
   - **5** Lectura repetible
4. Cesionarios, Revocados, Seleccionar columnas, Actualizar columnas:

Pueden ser listas de nombres separados por comas. Si tienen una longitud superior a los 166 caracteres, el proceso de auditoría descrito en el apartado "Análisis de auditoría con SQL" en la página 9-3 truncará la lista a 166 caracteres.

5. Privilegios de la base de datos:

   Privilegios a nivel de tabla:
   1 Seleccionar
   2 Insertar
   4 Suprimir
   8 Actualizar
   16 Modificar
   32 Índice
   64 Referencia
   4096 Ejecutar procedimiento (Cuando se ejecuta Otorgar privilegio. tabid hace referencia al ID del procedimiento).

   Privilegios a nivel de base de datos:
   256 Conectar
   512 DBA
   1024 Recurso

6. Estado de registro:
   1 Registro cronológico activado
   2 Registro cronológico en almacenamiento intermedio
   4 Compatible con ANSI

7. Tipo de sinónimo:
   0 Privado
   1 Público

8. Modalidad de bloqueo:
   0 Exclusivo
   1 Compartido

9. Distintivo de clúster:
   0 No es un clúster
   1 Clúster

10. Distintivo de fragmento:
    0 Comprobar el tamaño de reserva de raíz
    1 Comprobar todo el fragmento
    <0 Comprobar silenciosamente

11. Modalidad de restricción:
    0 Diferida
    1 Inmediata

12. Distintivo de explicación:
    0 Explicación desactivada
    1 Explicación activada

13. Distintivo de espera:
    -1 Esperar indefinidamente
    0 No esperar
    >0 Periodo de espera (en segundos)

14. Si la solicitud del usuario se rechaza debido a la autorización, estos campos tendrán 0 como valor o estarán en blanco, según el tipo de datos.

15. Distintivo de fragmentación (*frag*):
    0 No fragmentado
    1 En espacio de bd
    2 Fragmento por turno rotatorio (round robin)
    4 Fragmento por expresión

8 Fragmento igual que tabla

16. Distintivo de salto:
    - **0** DATASKIP para todos los espacios de bd está desactivado (OFF)
    - **1** DATASKIP para los espacios de bd siguientes está activado (ON)
    - **2** DATASKIP para todos los espacios de bd está activado (ON)
    - **3** DATASKIP tiene establecido el valor predeterminado
17. Nivel de prioridad:
    - **-1** PDQPRIORITY tiene establecido el valor predeterminado
    - **0** PDQPRIORITY está desactivado (OFF)
    - **1** El valor de PDQPRIORITY es LOW
    - **100** El valor de PDQPRIORITY es HIGH
    - **n** cualquier otro entero positivo inferior a 100 que el usuario haya entrado en la sentencia SET PDQPRIORITY
18. Tipo de operación:
    - **4** Añadir un fragmento nuevo
    - **8** Modificar la fragmentación
    - **16** Eliminar un fragmento
    - **32** Inicializar la fragmentación
    - **64** Adjuntar tabla(s)
    - **128** Separar fragmento
19. Distintivo de modalidad:
    - **0** Lectura/grabación si la operación es Establecer nivel de acceso; Lectura sucia si la operación es Establecer nivel de aislamiento
    - **1** Sólo lectura si la operación es Establecer nivel de acceso; Lectura confirmada si la operación es Establecer nivel de aislamiento
    - **2** Estabilidad del cursor
    - **3** Lectura repetible
20. Operación:
    - **0** Establecer modalidad de acceso
    - **1** Establecer nivel de aislamiento
21. Distintivos de eliminación:
    - **0** Cascada
    - **1** Restringir
22. Distintivo de modalidad de mandato:
    - **1** Inhabilitado
    - **2** Filtrado sin error
    - **4** Filtrado con error
    - **8** Habilitado
23. Distintivo de tipo de objeto:
    - **1** Restricción
    - **2** Índice
    - **3** Restricciones e índices
    - **4** Desencadenante
    - **5** Desencadenantes y restricciones
    - **6** Desencadenantes e índices
    - **7** Todo

Capítulo 12. El archivo ADTCFG

Este apéndice contiene una lista de los parámetros de configuración del archivo **ADTCFG** y una breve descripción de cada parámetro de configuración.

Cada parámetro de configuración tiene uno o varios de los siguientes atributos (según su relevancia):

valor predeterminado
: Valor predeterminado que aparece en el archivo **adtcfg.std**

si falta Valor que se proporciona si el parámetro falta en el archivo **ADTCFG**

unidades
: Unidades en que se expresa el parámetro

separadores
: Separadores que se pueden utilizar cuando el valor del parámetro tiene varias partes. No utilice espacios en blanco en el valor de un parámetro

rango de valores
: Valores válidos para este parámetro

entra en vigor
: Momento en el que un cambio del valor del parámetro afecta realmente al funcionamiento del servidor de bases de datos

programa de utilidad
: Nombre del programa de utilidad de la línea de mandatos que se puede utilizar para cambiar el valor del parámetro

consulte
: Referencia cruzada a más información

Convenios del archivo ADTCFG

El archivo de UNIX **$INFORMIXDIR/aaodir/adtcfg** o el archivo de Windows **%INFORMIXDIR%\aaodir\adtcfg** se conoce como el archivo de configuración **ADTCFG** o simplemente el archivo **ADTCFG**. En el archivo **ADTCFG**, cada parámetro se encuentra en una línea distinta. El archivo también puede contener líneas en blanco y líneas de comentarios que empiezan por un símbolo de almohadilla (#). La sintaxis de una línea de parámetro es la siguiente:

```
NOMBRE_PARÁMETRO              valor_parámetro           # comentario
```

Los parámetros del archivo **ADTCFG** y sus valores son sensibles a las mayúsculas y minúsculas. Los nombres de los parámetros siempre van en mayúsculas. Se debe intercalar espacio en blanco (tabulaciones, espacios o ambos) entre el nombre del parámetro, su valor y el comentario opcional. No utilice tabulaciones ni espacios dentro del valor de un parámetro.

Para obtener información sobre parámetros de configuración adicionales de Dynamic Server consulte la publicación *IBM Informix Administrator's Reference*.

ADTERR

ADTERR especifica cómo se comporta el servidor de bases de datos cuando detecta un error mientras graba un registro de auditoría.

valor predeterminado
0

rango de valores
0, 1, 3

0 = modalidad de error *continuar*

Cuando detecta un error mientras graba un registro de auditoría, el servidor de bases de datos graba un mensaje sobre la anomalía en el registro de mensajes. Sigue procesando la hebra.

1 = modalidad de error de *parada*: suspender el proceso de la hebra

Cuando el servidor de bases de datos detecta un error mientras graba un registro de auditoría, el servidor de bases de datos suspende el proceso de la hebra hasta grabar satisfactoriamente un registro.

3 = modalidad de error de *parada*: cerrar el sistema

Cuando el servidor de bases de datos detecta un error mientras graba un registro de auditoría, el servidor de bases de datos se cierra.

entra en vigor
Cuando se ejecuta **onaudit** para cambiar el valor o después de que se inicialice la memoria compartida. ADTMODE debe tener un valor de no cero (la auditoría está activada).

programa de utilidad
onaudit (`onaudit -e` *modalidad_error*)

ADTMODE

ADTMODE controla el nivel de auditoría.

valor predeterminado
0

rango de valores
0, 1, 3, 5, 7

0 = auditoría inhabilitada

1 = auditoría activada; inicia la auditoría para todas las sesiones

3 = auditoría activada; audita las acciones del DBSSO

5 = auditoría activada; audita las acciones del administrador del servidor de bases de datos

7 = auditoría activada; audita las acciones del DBSSO y del administrador del servidor de bases de datos

entra en vigor
Cuando se ejecuta **onaudit** para cambiar el valor o después de que se inicie el servidor

programa de utilidad
onaudit (`onaudit -l` *modalidad_audit*)

ADTPATH

ADTPATH especifica el directorio en el que el servidor de bases de datos guarda archivos de auditoría. Asegúrese de que el directorio que especifique tenga los privilegios de acceso adecuados para impedir el uso no autorizado de los registros de auditoría.

Para cambiar el valor de ADTPATH con **onaudit**, la auditoría gestionada por el servidor de bases de datos debe estar activada.

Los valores de ADTPATH son:

valor predeterminado
/usr/informix/aaodir (en UNIX), **%informixdir%\aaodir** (en Windows)

rango de valores
Cualquier vía de acceso de directorio válida

entra en vigor
Cuando se ejecuta **onaudit** para cambiar el valor o después de que se inicialice la memoria compartida

programa de utilidad
onaudit (`onaudit -p` *dir_audit*)

ADTSIZE

ADTSIZE especifica el tamaño máximo de un archivo de auditoría. Cuando un archivo alcanza el tamaño máximo, el servidor de bases de datos guarda el archivo de auditoría y crea uno de nuevo. Este parámetro sólo es válido para la auditoría gestionada por el servidor de bases de datos.

valor predeterminado
10, 240

unidades
Bytes

rango de valores
Entre 10.240 bytes y aproximadamente 2 gigabytes (el valor máximo de un entero de 32 bits)

entra en vigor
Cuando se ejecuta **onaudit** para cambiar el valor o después de que se inicialice la memoria compartida

programa de utilidad
onaudit (`onaudit -s` *tamaño máximo*)

Parte 3. Apéndices

Apéndice. Accesibilidad

IBM se esfuerza por proporcionar productos que puedan ser utilizados por todas las personas, cualquiera que sea su edad o capacidad.

Funciones de accesibilidad de IBM Informix Dynamic Server

Las funciones de accesibilidad ayudan a un usuario que tenga una minusvalía física, tal como una movilidad restringida o una visión limitada, a utilizar satisfactoriamente productos de tecnología de la información.

Funciones de accesibilidad

La lista siguiente incluye las funciones de accesibilidad principales de IBM Informix Dynamic Server. Estas funciones permiten:

- Utilización del sistema basada en el teclado solamente.
- Interfaces que son utilizadas habitualmente por lectores de pantalla.
- Conexión de dispositivos alternativos de entrada y salida.

Consejo: El Centro de información de IBM Informix Dynamic Server y sus publicaciones asociadas están habilitados para el dispositivo IBM Home Page Reader. Puede utilizar todas las funciones mediante el teclado en lugar de utilizar el ratón.

Navegación mediante el teclado

El presente producto utiliza teclas de navegación estándar de Microsoft Windows.

Información afín sobre accesibilidad

IBM se compromete a que su documentación sea accesible para las personas con discapacidades. Nuestras publicaciones están disponibles en formato HTML, por lo que se puede acceder a ellas mediante tecnología de asistencia a discapacitados, tal como software lector de pantallas. Los diagramas de sintaxis contenidos en nuestras publicaciones están disponibles en el formato decimal con puntos. Para obtener más información sobre el formato decimal con puntos, consulte "Diagramas de sintaxis en formato decimal con puntos".

Puede visualizar las publicaciones de IBM Informix Dynamic Server en formato PDF (Portable Document Format) de Adobe, utilizando el lector Adobe Acrobat Reader.

IBM y accesibilidad

Consulte la publicación *IBM Accessibility Center* en http://www.ibm.com/able para obtener más información sobre el compromiso que IBM tiene con respecto al tema de la accesibilidad.

Diagramas de sintaxis en formato decimal con puntos

Los diagramas de sintaxis de nuestras publicaciones están disponibles en el formato decimal con puntos, que es un formato accesible que solamente se puede utilizar con un lector de pantallas.

En el formato decimal con puntos, cada elemento de sintaxis está escrito en una línea separada. Si dos o más elementos de sintaxis están siempre presentes a la vez (o están siempre ausentes a la vez), los elementos pueden aparecer en la misma línea porque se pueden considerar como un elemento de sintaxis individual compuesto.

Cada línea empieza por un número decimal con puntos; por ejemplo, 3 o 3.1 o 3.1.1. Para escuchar correctamente estos números, asegúrese de que su lector de pantallas esté establecido para leer los símbolos de puntuación. Todos los elementos de sintaxis que tienen el mismo número decimal con puntos (por ejemplo, todos los elementos de sintaxis que tienen el número 3.1) son alternativas mutuamente excluyentes. Si escucha las líneas 3.1 USERID y 3.1 SYSTEMID, la sintaxis puede incluir USERID o SYSTEMID, pero no ambas cosas.

El nivel de numeración decimal con puntos indica el nivel de anidamiento. Por ejemplo, si un elemento de sintaxis con un número decimal con puntos 3 va seguido de una serie de elementos de sintaxis con un número decimal con puntos 3.1, todos los elementos de sintaxis con el número 3.1 son subordinados del elemento de sintaxis con el número 3.

Se utilizan determinadas palabras y símbolos junto a los números decimales con puntos para añadir información sobre los elementos de sintaxis. Ocasionalmente, estas palabras y símbolos podrían aparecer al principio del propio elemento. Para facilitar la identificación, si la palabra o el símbolo forma parte del elemento de sintaxis, la palabra o el símbolo van precedidos por el carácter de barra inclinada invertida (\). El símbolo * se puede utilizar junto a un número decimal con puntos para indicar que se repite el elemento de sintaxis. Por ejemplo, el elemento de sintaxis *FILE con el número decimal con puntos 3 se lee como 3 * FILE. El formato 3* FILE indica que se repite el elemento de sintaxis FILE. El formato 3* * FILE indica que el elemento de sintaxis * FILE se repite.

Los caracteres como por ejemplo comas, que se utilizan para separar una serie de elementos de sintaxis, se muestran en la sintaxis justo antes de los elementos que separan. Estos caracteres pueden aparecer en la misma línea que cada elemento o en una línea separada con el mismo número decimal con puntos que los elementos relevantes. La línea también puede mostrar otro símbolo que proporciona información sobre los elementos de sintaxis. Por ejemplo, las líneas 5.1*, 5.1 LASTRUN, y 5.1 DELETE significan que si utiliza más de uno de los elementos de sintaxis LASTRUN y DELETE, los elementos deben ir separados por una coma. Si no se proporciona ningún separador, se presupone que se utiliza un espacio en blanco para separar cada elemento de sintaxis.

Si un elemento de sintaxis va precedido por el símbolo %, identifica una referencia que está definida en otro lugar. La serie que va a continuación del símbolo % es el nombre de un fragmento de sintaxis en vez de un literal. Por ejemplo, la línea 2.1 %OP1 indica que deberá consultar un fragmento de sintaxis independiente OP1.

Las palabras y símbolos que se indican a continuación se utilizan junto a los números decimales con puntos:

? Especifica un elemento de sintaxis opcional. Un número decimal con puntos seguido del símbolo ? indica que todos los elementos de sintaxis con un número decimal con puntos correspondiente, y cualquier elemento de sintaxis subordinado, son opcionales. Si sólo hay un elemento de sintaxis con un número decimal con puntos, el símbolo ? se visualiza en la misma línea que el elemento de sintaxis (por ejemplo, 5? NOTIFY). Si hay

más de un elemento de sintaxis con un número decimal con puntos, el símbolo ? se visualiza en una línea por sí mismo, seguido por los elementos de sintaxis que son opcionales. Por ejemplo, si aparecen las líneas `5 ?`, `5 NOTIFY` y `5 UPDATE`, significa que los elementos de sintaxis `NOTIFY` y `UPDATE` son opcionales; es decir, puede elegir uno de ellos o ninguno. El símbolo ? es equivalente a una línea de derivación en un diagrama de vía férrea.

! Especifica un elemento de sintaxis por omisión. Un número decimal con puntos seguido por el símbolo ! y un elemento de sintaxis indica que el elemento de sintaxis es la opción por omisión para todos los elementos de sintaxis que comparten el mismo número decimal con puntos. Sólo uno de los elementos de sintaxis que comparten el mismo número decimal con puntos puede especificar un símbolo ! . Por ejemplo, si escucha las líneas `2? FILE`, `2.1! (KEEP)` y `2.1 (DELETE)`, sabe que `(KEEP)` es la opción por omisión para la palabra clave `FILE`. En este ejemplo, si incluye la palabra clave `FILE` pero no especifica una opción, se aplica la opción por omisión `KEEP`. También se aplica una opción por omisión en el siguiente número decimal con puntos más alto. En este ejemplo, si se omite la palabra clave `FILE`, se utiliza el valor por omisión `FILE(KEEP)`. Sin embargo, si escucha las líneas `2? FILE`, `2.1`, `2.1.1! (KEEP)` y `2.1.1 (DELETE)`, la opción por omisión KEEP sólo se aplica al siguiente número decimal con puntos más alto, `2.1` (que no tiene una palabra clave asociada), y no se aplica a `2? FILE`. No se utiliza nada si se omite la palabra clave `FILE`.

***** Especifica un elemento de sintaxis que se puede repetir cero o más veces. Un número decimal con puntos seguido del símbolo * indica que este elemento de sintaxis se puede utilizar cero o más veces; es decir, es opcional y se puede repetir. Por ejemplo, si escucha la línea `5.1* área-datos`, sabe que puede incluir más de un área de datos o puede no incluir ninguno. Si escucha las líneas `3* , 3 HOST`, y `3 STATE`, sabe que puede incluir `HOST`, `STATE`, ambos a la vez, o bien nada.

Notas:

1. Si un número decimal con puntos tiene un asterisco (*) junto a él, y sólo hay un elemento con dicho número decimal con puntos, puede repetir el mismo elemento más de una vez.
2. Si un número decimal con puntos tiene un asterisco junto a él y varios elementos tienen dicho número decimal con puntos, puede utilizar más de un elemento de la lista, pero no puede utilizar los elementos más de una vez. En el ejemplo anterior, podía escribir `HOST STATE` , pero no podía escribir `HOST HOST`.
3. El símbolo * es equivalente a una línea de bucle de retorno en un diagrama de sintaxis de vía férrea.

+ Especifica un elemento de sintaxis que debe incluirse una o más veces. Un número decimal con puntos seguido del símbolo + indica que este elemento de sintaxis debe incluirse una o más veces. Por ejemplo, si escucha la línea `6.1+ área-datos`, debe incluir al menos un área de datos. Si escucha las líneas `2+`, `2 HOST` y `2 STATE`, sabe que debe incluir `HOST`, `STATE`, o ambos. En cuanto al símbolo *, sólo puede repetir un elemento específico si es el único elemento con ese número decimal con puntos. El símbolo +, al igual que el símbolo * es equivalente a una línea de bucle de retorno en un diagrama de sintaxis de vía férrea.

Avisos

Es posible que IBM no ofrezca en todos los países los productos, los servicios o las características que se describen en este documento. Consulte al representante local de IBM para obtener información sobre los productos y servicios que actualmente estén disponibles en su área. Las referencias a un producto, programa o servicio de IBM no pretenden indicar o implicar que solo se pueda utilizar ese producto, programa o servicio de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran temas tratados en este documento. El suministro de este documento no le confiere ninguna licencia sobre dichas patentes. Puede enviar consultas acerca de licencias, por escrito, a la dirección siguiente:

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

Para formular consultas acerca de licencias referentes a información de doble byte (DBCS), póngase en contacto con el Departamento de la Propiedad Intelectual de IBM de su país o envíe las consultas, por escrito, a la dirección siguiente:

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

El párrafo siguiente no es aplicable al Reino Unido ni a ningún otro país en el que tales disposiciones sean incompatibles con la legislación local:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGUNA CLASE, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIABILIDAD O ADECUACIÓN A UN PROPÓSITO DETERMINADO. Algunos estados no permiten la renuncia a las garantías explícitas o implícitas en determinadas transacciones, por lo que puede que esta declaración no le sea aplicable.

Esta información puede contener imprecisiones técnicas o errores tipográficos. Periódicamente, se efectúan cambios en la información aquí incluida; estos cambios se incorporarán en nuevas ediciones de la publicación. En cualquier momento y sin previo aviso, IBM puede efectuar mejoras y/o cambios en los productos y/o programas descritos en esta publicación.

Las referencias hechas en esta información a sitios Web que no sean de IBM se proporcionan únicamente por comodidad y de ningún modo suponen un aval de dichos sitios Web. El contenido de esos sitios Web no forma parte del contenido del presente producto de IBM y la utilización de esos sitios Web corre a cuenta y riesgo del usuario.

IBM puede utilizar o distribuir la información que se le facilite del modo que IBM considere oportuno sin incurrir en ninguna obligación con el remitente.

Los licenciatarios de este programa que deseen obtener información sobre el mismo con el fin de permitir: (i) el intercambio de información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) el uso mutuo de la información intercambiada, deben ponerse en contacto con:

IBM Corporation
J46A/G4
555 Bailey Avenue
San José, CA 95141-1003
EE.UU.

Esta información puede estar disponible, de acuerdo con los términos y condiciones pertinentes, incluido, en algunos casos, el pago de una tarifa.

IBM proporciona el programa bajo licencia descrito en esta información y todo el material bajo licencia disponible para el mismo según los términos del Acuerdo del cliente de IBM, del Acuerdo internacional de licencia de programas de IBM o de cualquier acuerdo equivalente entre ambas partes.

Los datos de rendimiento que contiene esta publicación se han determinado en un entorno controlado. Por ello, los resultados obtenidos en otros entornos operativos pueden variar significativamente. Algunas medidas pueden haberse tomado en sistemas en desarrollo y no se garantiza que tales medidas sean las mismas en los sistemas disponibles de forma generalizada. Además, es posible que algunas medidas se hayan calculado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deberán verificar los datos adecuados para su entorno específico.

La información concerniente a productos que no sean de IBM se ha conseguido de los suministradores de dichos productos, de sus anuncios publicados o bien de otras fuentes públicas. IBM no ha probado esos productos y no puede confirmar con precisión el rendimiento, la compatibilidad ni otras exigencias en relación con los productos que no son de IBM. Las preguntas sobre las prestaciones de los productos que no son de IBM deben ir dirigidas a los suministradores de dichos productos.

Todas las referencias a intenciones u orientaciones futuras de IBM están sujetas a cambios o retractación sin previo aviso, y representan únicamente metas y objetivos.

Todos los precios de IBM que se muestran en este documento son precios al por mayor recomendados por IBM, vigentes y están sujetos a cambios sin previo aviso. Los precios de los concesionarios pueden variar.

Esta información contiene ejemplos de datos e informes que se utilizan en las operaciones comerciales diarias. Para ilustrarlos lo más exhaustivamente posible, los ejemplos incluyen nombres de personas, compañías, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con los nombres y direcciones utilizados por una compañía comercial real es pura coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente, que ilustran técnicas de programación en diversas plataformas operativas. Puede

copiar, modificar y distribuir estos programas de ejemplo del modo que considere adecuado sin previo pago a IBM, con el objeto de desarrollar, utilizar, comercializar o distribuir programas de aplicación de acuerdo con la interfaz de programación de aplicaciones para la plataforma operativa para la cual se han escrito los programas de ejemplo. Estos ejemplos no se han probado en profundidad bajo todas las condiciones. Por lo tanto, IBM no puede garantizar ni implicar la fiabilidad, el servicio ni el funcionamiento de estos programas. Puede copiar, modificar y distribuir estos programas de ejemplo del modo que considere adecuado sin pagar a IBM con el objeto de desarrollar, utilizar, comercializar o distribuir programas de aplicación de acuerdo con las interfaces de programación de aplicaciones de IBM.

Cada copia o fragmento de estos programas de ejemplo o de cualquier trabajo derivado debe incluir un aviso de copyright como el que se muestra a continuación:

> © (nombre de la compañía) (año). Partes de este código proceden de IBM Corp. Programas de ejemplo. © Copyright IBM Corp. (escriba el año o años). Reservados todos los derechos.

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

Marcas registradas

Los términos siguientes se utilizan en una o más publicaciones de productos IBM Informix y los términos son marcas registradas de International Business Machines Corporation en los Estados Unidos o en otros países:

AIX	OS/2
AnalystStudio	OS/390
C-ISAM	OS/400
Cloudscape	Passport Advantage
DataBlade	ProjectConsole
DB2	Rational
DB2 Connect	Rational Suite
DB2 Universal Database	Rational Unified Process
Distributed Relational Database Architecture	RedBack
Domino	Red Brick
DRDA	RequisitePro
Dynamic Connect	RETAIN
IBM	SQL/DS
Informix	SystemBuilder
Lotus	Tivoli
Lotus Notes	TME 10
MQSeries	UniData
NetView	UniVerse
Notes	WebSphere
NUMA-Q	z/OS

Adobe, Acrobat, Portable Document Format (PDF) y PostScript son marcas registradas de Adobe Systems Incorporated en los Estados Unidos o en otros países.

Intel, el logotipo de Intel, Intel Inside, el logotipo de Intel Inside, Intel Centrino, el logotipo de Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium y Pentium son marcas registradas de Intel Corporation o de sus empresas filiales en los Estados Unidos y en otros países.

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

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en los Estados Unidos o en otros países.

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

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

Otros nombres de empresas, productos o servicios utilizados en esta publicación pueden ser marcas registradas o marcas de servicio de terceros.

Índice

Caracteres Especiales

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

G229-6591-00