Oracle Label Security - Mejores Prácticas para Aplicaciones de Gobierno y Defensa

Informe Ejecutivo de Oracle

Junio de 2007

ORACLE

Oracle Label Security – Mejores Prácticas para Aplicaciones de Gobierno y Defensa

Introducción..... 3
Etiquetas de Sensibilidad y Mediación de Acceso..... 3
Algoritmo de Lectura para Mediación de Acceso..... 4
Incorporar Oracle Label Security…..... 4
Paso 1: Analizar el Esquema de Aplicaciones..... 4
Paso 2: Analizar los Niveles de Sensibilidad..... 4
Paso 3: Analizar los Grupos de Datos..... 4
Paso 4: Analizar los Compartimentos de Datos..... 5
Paso 5: Analizar la población de usuarios..... 5
Paso 6: Analizar las autorizaciones especiales..... 5
Paso 7: Revisar y Documentar..... 5
Metodología de Análisis..... 5
Implementación..... 6
Etiquetar Datos Antiguos…..... 6
Ocultar la columna de políticas de Oracle Label Security..... 7
Administración de Oracle Label Security..... 7
Exención de Aplicación…..... 7
Ajuste de Desempeño..... 8
Proxy con el Comando SET_ACCESS_PROFILE..... 8
Anexo A - Oracle Label Security: Autorizaciones Especiales para Usuarios… 9
Anexo B - Oracle Label Security: Opciones para la Aplicación de Políticas 9
Anexo C - Oracle Label Security: Autorización a Usuarios…..... 10

Oracle Label Security – Mejores Prácticas para Aplicaciones de Gobierno y Defensa

INTRODUCCIÓN

De acuerdo con los exigentes requisitos de seguridad que pueden encontrarse en las organizaciones con un alto nivel de seguridad, Oracle Label Security brinda capacidades amplias y flexibles para el control de acceso basado en etiquetas (LBAC) a fin de respaldar la implementación de aplicaciones de seguridad de múltiples niveles (MLS) en el ámbito de gobierno y defensa. Oracle Label Security supera las limitaciones históricas de los sistemas MLS con una amplia disponibilidad de plataformas y controles extensivos de políticas que pueden ajustarse de acuerdo con los entornos específicos.

Disponible para Oracle8i Enterprise Edition y superior, Oracle Label Security puede implementarse con Oracle RAC y Data Guard para escalabilidad y alta disponibilidad. Este informe muestra las mejores prácticas que pueden utilizarse para incorporar Oracle Label Security en una aplicación nueva o existente.

ETIQUETAS DE SENSIBILIDAD Y MEDIACIÓN DE ACCESO

La mediación de acceso de Oracle Label Security MLS funciona al comparar una etiqueta de sensibilidad con las autorizaciones de etiquetas asignadas a un usuario de aplicaciones.

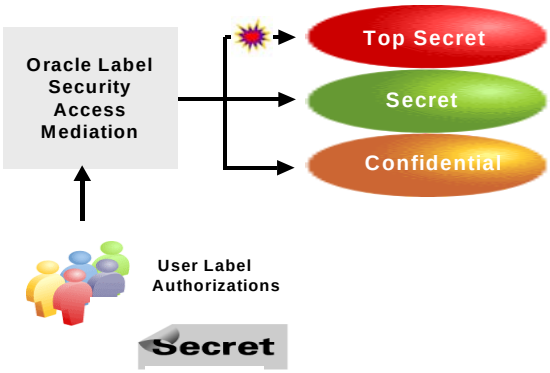

Figura 1. Generalidades sobre Oracle Label Security

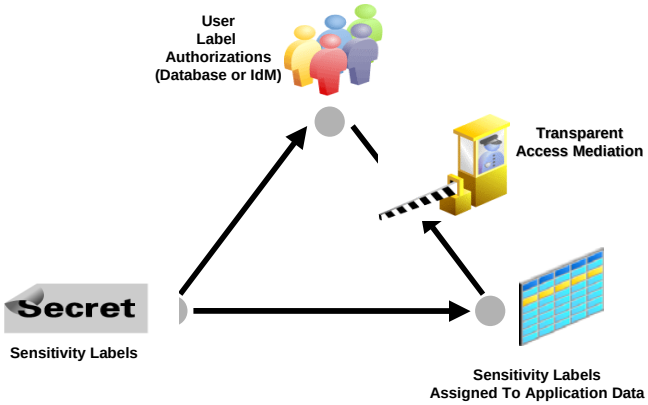

Figura 2. Generalidades sobre el Control de Acceso de Oracle Label Security

Las etiquetas de sensibilidad son fundamentales para Oracle Label Security. Las etiquetas de sensibilidad ofrecen controles sofisticados y determinan el acceso de un usuario de aplicaciones a los datos de aplicaciones. Las etiquetas de sensibilidad contienen un nivel, compartimentos opcionales y grupos opcionales.

Nivel—El nivel es un componente jerárquico que denota la sensibilidad de los datos. Una organización gubernamental típica puede definir los niveles como confidencial, sensible y altamente sensible.

Compartimento – El componente compartimento es opcional y a veces se lo califica como categoría y no es jerárquico. En general, se define un compartimento o más para segregar los datos. Los compartimentos pueden definirse para un area o proyecto de conocimiento específico, altamente sensible.

Grupo – Los grupos son similares a las categorías y también son opcionales. No obstante, los grupos pueden tener una relación principal-secundaria (*parent-child*). Asimismo, Oracle Label Security evalúa los grupos de manera diferente de los compartimentos. La Figura 3 muestra el algoritmo de mediación de lectura para las etiquetas de sensibilidad

La representación externa de una etiqueta utiliza los dos puntos y comas para separar los componentes. La etiqueta de sensibilidad *Sensitive: Alpha, Beta : UK* contiene el nivel *Sensitive*, dos compartimentos *Alpha* y *Beta,* y un grupo *UK*. Internamente, Oracle Label Security utiliza un identificador numérico denominado *label tag* para cada nivel de sensibilidad. Mientras que las etiquetas de sensibilidad y los label tags (identificación de etiquetas) pueden crearse dinámicamente en tiempo de ejecución, Oracle recomienda definir todas las etiquetas de sensibilidad y los label tags asociados por adelantado.

Algoritmo de Lectura para Mediación de Acceso

Oracle Label Security media el acceso al comparar las autorizaciones de las etiquetas de usuarios con un nivel de sensibilidad.

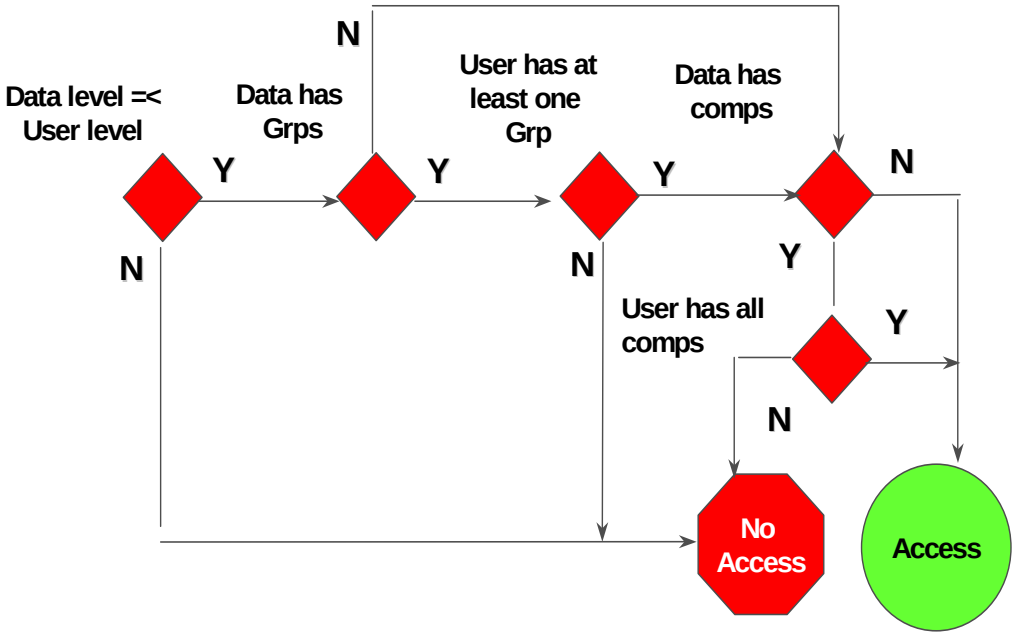

Figura 3. Algoritmo de Lectura de Oracle Label Security

Incorporar Oracle Label Security

El proceso de análisis es importante para el éxito de utilizar Oracle Label Security. El etiquetado avanzado de filas requiere determinar cómo y dónde aplicar Oracle Label Security.

Paso 1: Analizar el Esquema de Aplicaciones

Analizar la aplicación implica identificar las tablas que necesitan aplicar una política Oracle Label Security. Esto puede lograrse mejor con la ayuda de un administrador de aplicaciones o un desarrollador con amplios conocimientos del esquema de aplicación. En la mayoría de los casos, un pequeño porcentaje de las tablas de aplicaciones necesitará una política Oracle Label Security. Si la aplicación tiene un diagrama de relación de entidad (ER), puede resultar útil anotar en ER los niveles para cada entidad.

Paso 2: Analizar los Niveles de Sensibilidad

Una vez identificadas las tablas del candidato, los datos contenidos en las tablas necesitan evaluarse. Será necesaria la ayuda de un analista de datos o alguien con un profundo entendimiento de los datos. Los niveles de datos se refieren al nivel de sensibilidad de los datos. *No Clasificado, Sensible* y *Altamente Sensible* son ejemplos de niveles de sensibilidad. Se recomienda considerar también los datos de aplicaciones que pueden almacenarse en un futuro. Esto creará un conjunto grande de definiciones de etiquetas en Oracle Label Security.

Proyectos	Activos
No Clasificado Secreto	Secreto Ultrasecreto

Paso 3: Analizar los Grupos de Datos

Grupos útiles para controlar el acceso basado en la propiedad de datos y para compartir los datos en todas las organizaciones. Tal como con los niveles de datos, la ayuda de alguien con amplia familiaridad con las operaciones de negocio puede ser muy valiosa en esta etapa del análisis. Algunos ejemplos de grupos incluyen *Estados Unidos, Reino Unido, Europa, Asia.*

Secreto: Alpha, Beta: US, UK
Ultrasecreto: Alpha, Beta: UK

Paso 4: Analizar los Compartimentos de Datos

Los compartimentos de datos son principalmente utilizados en ámbitos de gobierno y defensa. Una aplicación comercial puede considerar que los grupos de datos son suficientes para brindar el nivel necesario de control de acceso. No obstante, las organizaciones comerciales pueden considerar que los compartimentos son útiles para etiquetar información personalmente identificable (PII). En los ámbitos de gobierno y defensa, los compartimentos son típicamente utilizados para restringir el acceso a proyectos o áreas especializadas de conocimiento.

Secreto: Alpha, Beta: US, UK
Ultrasecreto: Alpha, Beta: UK

Paso 5: Analizar la población de usuarios

Este paso requiere obtener un entendimiento de la gran cantidad de roles y responsabilidades implicados en la población de usuarios. Por ejemplo, se puede designar a un usuario como analista, usuario altamente privilegiado o usuario administrativo. Este proceso puede requerir la asistencia de gerentes o administradores de seguridad. Después de que la población de usuarios se ha separado en uno o más roles o áreas funcionales, se debe realizar una comparación entre los niveles de datos identificados en el paso 2 y las autorizaciones de etiquetas de la población de usuarios. Éstos deben corresponder adecuadamente con cada tabla identificada durante el análisis de esquema en el paso 1. Asimismo, la estructura organizacional de la población de usuarios necesita compararse con los grupos de datos identificados en el paso 3.

Paso 6: Analizar las autorizaciones especiales

Oracle Label Security cuenta con varias autorizaciones especiales que pueden asignarse a los usuarios y procedimientos almacenados. En este paso, examine a los usuarios administrativos y altamente privilegiados y determine si alguna de las autorizaciones especiales de Oracle Label Security debería asignarse al usuario. En general, muy pocos usuarios necesitarán autorizaciones especiales. Por favor, remítase al anexo A para obtener un listado completo de las autorizaciones especiales de Oracle Label Security.

Paso 7: Revisar y Documentar

El paso final antes de comenzar la implementación es revisar y documentar la información recopilada. Este paso es crucial para la continuidad en la empresa, y el documento resultante debería incluirse como parte de la política de seguridad de la

empresa. Incluya tablas, gráficos y argumentos narrativos para explicar en su totalidad los resultados del análisis. Por ejemplo, el documento debería incluir una lista de las tablas de esquema que necesiten protegerse y la justificación correspondiente. Este documento puede considerarse sensible después de creado.

METODOLOGÍA DE ANÁLISIS

Durante el análisis, puede resultar útil crear una matriz que compare la información recopilada en el paso 5 con la información recopilada sobre los datos reales. Esta técnica puede ayudar a identificar los problemas operacionales antes de la implementación real de Oracle Label Security. Este tipo de análisis puede ayudar a identificar las autorizaciones requeridas para un trabajo específico.

Tabla	Usuario / Datos	I	S	S:A:US	S:A,B:US,UK
Activos	I::UK	No Acceso	No Acceso	No Acceso	Acceso
	I::US	No Acceso	No Acceso	Acceso	Acceso
Proyectos	I	Acceso	Acceso	Acceso	Acceso
	S	No Acceso	Acceso	Acceso	Acceso
	S:A:US	No Acceso	No Acceso	Acceso	Acceso
	S:B:UK	No Acceso	No Acceso	No Acceso	Acceso
	S:A,B, US	No Acceso	No Acceso	No Acceso	Acceso

Tabla 1. Matriz para Análisis de Etiquetas

IMPLEMENTACIÓN

La implementación puede realizarse utilizando Oracle Enterprise Manager o la interface de línea de comando de Oracle Label Security.

1. Siga los pasos de análisis mencionados arriba

2. Cree la Política Oracle Label Security

3. Defina todos los componentes para etiquetas de datos válidos utilizando niveles, compartimentos y grupos con la información recopilada durante el análisis

4. Cree etiquetas de datos válidos para la política mediante el uso de los componentes definidos en el paso 3

5. Asigne autorizaciones de etiquetas a las poblaciones de usuarios y autorizaciones especiales adecuadas de Oracle Label Security utilizando los datos recopilados durante el análisis

6. Aplique la política a la tabla de aplicaciones. Si hay datos antiguos en la tabla, puede ser necesario aplicar la política a la tabla con la opción no aplicación de control inicialmente. Después de que la política es aplicada a la tabla, la etiqueta de sensibilidad estará vacía y ningún dato estará visible. Por favor, remítase a la sección sobre etiquetado de datos antiguos. De manera opcional, usted puede otorgar al usuario o al proceso que actualiza los datos antiguos la autorización *FULL* para seguridad de etiquetas.

7. Actualice los datos antiguos con las etiquetas adecuadas de datos

8. Si se aplicó la política pero está deshabilitada, active la política Oracle Label Security y configure las opciones adecuadas para la aplicación de la política

ETIQUETAR LOS DATOS ANTIGUOS

Una vez aplicada la política de Oracle Label Security en una tabla de aplicaciones con control de lectura, ninguna fila estará visible hasta que se hayan asignado las etiquetas de datos válidos a cada fila de datos. Existen varios métodos para etiquetar los datos antiguos.

El primer método para etiquetar los datos antiguos simplemente utiliza una sentencia de actualización frente a la tabla base.

```
UPDATE SALES SET SECLAB =
char_to_label:('FINANCE','S')
WHERE REGION_ID = 104;
```

Esta sentencia actualiza la tabla VENTAS y configura la columna SECLAB de etiqueta de política igual a la identificación de la etiqueta interna definida para SENSITIVE en la política FINANZAS, y VENTS columna REGION_ID es igual a 104.

El Segundo método para etiquetar los datos antiguos es cambiar las conexiones de base de datos durante la carga de datos.

```
CONNECT US_SALES_MGR
INSERT INTO SALES (Col1, Col2, Col3) VALUES
('ACME',......);

CONNECT EU_SALES_MGR
INSERT INTO SALES (Col1, Col2, Col3) VALUES
('WIDGET',......);
```

Si la política aplicada a la tabla VENTAS incluye la opción LABEL_DEFAULT, se utilizará el valor ROWLABEL por defecto de los usuarios para configurar la columna SECLAB.

El tercer método es escribir una función de etiquetado utilizando PL/SQL. Las funciones de etiquetado de Oracle Label Security se escriben en PL/SQL. Un ejemplo de una función de etiquetado puede encontrarse en la guía para el administrador de Oracle Label Security. La función de etiquetado puede incorporarse a una política utilizando una API de Oracle Label Security.

La función de etiquetado también puede escribirse para que muestre una etiqueta Oracle Label Security. Este tipo de función no debería incorporarse en una política Oracle Label Security porque no tiene el tipo de datos adecuados. Sin embargo, la función podría convocarse en el contexto de una sentencia de actualización en la tabla de aplicación objetivo.

```
UPDATE SALES SET SECLAB =
My_Function(sales.region_id);
```

El cuarto método para etiquetar datos antiguos es escribir un procedimiento almacenado que actualice la columna de la tabla de aplicación asociada con la política Oracle Label Security.

OCULTAR LA COLUMNA DE POLÍTICAS DE ORACLE LABEL SECURITY

Oracle Label Security requiere especificar el nombre de una columna cuando se crea una política. Cuando se aplica la política en una tabla de aplicaciones, el nombre de la columna especificado durante la creación de la política es anexado a la tabla de aplicaciones. Oracle Label Security cuenta con una opción para ocultar la columna de políticas cuando la política es anexada a una tabla de aplicaciones. Ocultar la columna hace que la columna no se despliegue durante una operación de descripción de tabla SQL Plus. Ocultar la columna también permite que las sentencias SQL que no especifican nombres de columna sigan funcionando a pesar de haberse anexado una nueva columna en la tabla de aplicaciones especificada en la sentencia SQL.

Es importante tener en cuenta que la columna de políticas de Oracle Label Security puede estar en una tabla de aplicaciones antes de la aplicación de una política de Oracle Label Security. Para aprovechar esto, el tipo de columna de las tablas de aplicaciones debe ser el número (10). Las aplicaciones pueden designarse con una columna Oracle Label Security incorporada.

ADMINISTRACIÓN DE ORACLE LABEL SECURITY

La cuenta LBACSYS es la cuenta de administración primaria de Oracle Label Security. No obstante, se puede otorgar autorización a otros usuarios para crear y administrar las políticas de Oracle Label Security. Cuando se crea una política Oracle Label Security, se crea un nuevo rol de base de datos. El nombre del rol de la base de datos es *policyname*_DBA. En el siguiente código, el usuario LBACSYS crea una política y otorga al usuario HR_INFOSEC las autorizaciones para administrar los componentes de las etiquetas de políticas y las autorizaciones de etiqueta.

```
CONNECT LBACSYS

EXECUTE SA_SYSDBA.CREATE_POLICY('HR_SECURITY', 'HR_LABEL');

GRANT HR_DBA TO HR_INFOSEC;
GRANT EXECUTE ON sa_components TO sub_admin;
GRANT EXECUTE ON sa_user_admin TO sub_admin;
GRANT EXECUTE ON sa_label_admin TO sub_admin;
GRANT EXECUTE ON sa_policy_admin TO sub_admin;
GRANT EXECUTE ON sa_audit_admin TO sub_admin;
```

EXENCIÓN DE APLICACIÓN

Las políticas para el control de acceso de Oracle Virtual Private Database y las políticas de Oracle Label Security no son obligatorias durante la exportación del proceso DIRECT. Asimismo, las políticas de Virtual Private Database y las políticas de Oracle Label Security no pueden aplicarse a objetos dentro del esquema SYS. Como consecuencia, el usuario SYS y los usuarios que realizan una conexión a la base de datos con privilegios de DBA (por ejemplo, CONNECT/AS SYSDBA) no tienen políticas VPD ni Oracle Label Security en sus acciones. Los administradores de base de datos necesitan poder administrar la base de datos. No sería suficiente exportar parte de una tabla debido a la aplicación de una política VPD. Los usuarios de base de datos a quienes se les otorga el privilegio Oracle EXEMPT ACCESS POLICY, directamente o a través de un rol de base de datos, están exentos de la aplicación de Virtual Private Database y Oracle Label Security. Los usuarios están exentos de la aplicación de Virtual Private Database y Oracle Label Security independientemente del modo de exportación, la aplicación o el servicio utilizado para extraer los datos de la base de datos. El privilegio EXEMPT ACCESS POLICY es un privilegio poderoso y debería administrarse con cuidado. El privilegio EXEMPT ACCESS POLICY no afecta la aplicación de los privilegios de objeto como SELECT, INSERT, UPDATE y DELETE. Estos privilegios son aplicados incluso si un usuario ha otorgado el privilegio EXEMPT ACCESS POLICY.

AJUSTE DE DESEMPEÑO

Al crear las etiquetas de datos, Oracle recomienda definir las identificaciones de etiquetas asociadas de manera que se incluyan en la categoría asociada con el nivel de la etiqueta de datos. Por ejemplo, supongamos que los niveles confidencial y sensible han sido definidos junto con dos compartimentos, alpha y beta. El número asociado con Confidencial es 5000, y el número asociado con Sensible es 10000. Cuando se definen las etiquetas de datos válidos, las etiquetas asociadas con confidencial deberían oscilar entre 5000 y 10000. Por ejemplo, la etiqueta de datos *confidential:alpha* podría tener una identificación de 5050, y la etiqueta de datos *sensitive:alpha,beta* podría tener una identificación de 10055.

Los índices compuestos existentes pueden modificarse para incluir la columna anexada por Oracle Label Security en la tabla de aplicaciones. Esto puede mejorar sustancialmente el desempeño para consultas complejas.

Según el uso de las aplicaciones, se deben tener en cuenta ciertos factores para crear índices bitmap en la columna anexada por Oracle Label Security en la tabla de aplicaciones. El porcentaje de etiquetas exclusivas comparado con el número de filas de datos en general es bajo.

Oracle Partitioning puede utilizarse con Oracle Label Security para particionar físicamente los datos de acuerdo con la sensibilidad de datos y ofrecer optimización de consultas mediante la eliminación del particionamiento. En algunos casos, particionar físicamente los datos por sensibilidad también puede constituir un requisito de seguridad.

```
CREAR TABLA DE EMPLEADOS

EMPNO NUMBER(10) CONSTRAINT PK_EMPLOYEE PRIMARY KEY,
ENAME VARCHAR2(10),
JOB VARCHAR2(9),
SEC_LABEL NUMBER(10))
TABLESPACE PERF_DATA
STORAGE (initial 2M
NEXT 1M
MINEXTENTS 1
MAXEXTENTS unlimited)
PARTITION BY RANGE (sec_label)
(partition sx1 VALUES LESS THAN (2000) NOLOGGING,
partition sx2 VALUES LESS THAN (3000),
partition sx3 VALUES LESS THAN (4000) );
```

PROXY CON EL COMANDO SET_ACCESS_PROFILE

Oracle Label Security proporciona la capacidad de que un usuario autorizado asuma un perfil de autorización de etiquetas de Oracle Label Security. La autorización PROFILE_ACCESS es requerida para ejecutar el procedimiento SET_ACCESS_PROFILE. Esta capacidad proxy de Oracle Label Security está disponible para que las arquitecturas de las aplicaciones que utilizan modelos de un solo usuario grande, seguridad de usuarios empresariales o autenticación proxy, puedan utilizar Oracle Label Security.

Oracle Label Security no impone el mapeo entre una cuenta de base de datos física y el nombre de usuario especificado al establecer las autorizaciones de etiquetas. Por ejemplo, la autorización de etiquetas podría asignarse a una dirección de IP.

Las aplicaciones pueden utilizar una de las variables Oracle SYS_CONTEXT para determinar qué perfil de autorización de Oracle Label Security debería especificarse en el comando SET_ACCESS_PROFILE. Para usuarios empresariales, el valor EXTERNAL_NAME SYS_CONTEXT podría pasar al comando SET_ACCESS_PROFILE.

```
SQL> execute sa_session.set_access_profile
(‘PRIVACY’,SYS_CONTEXT('userenv',’PROXY_USER’);

SQL> execute sa_session.set_access_profile
(‘PRIVACY’,SYS_CONTEXT('userenv','CLIENT_IDENTIFIER');

SQL> execute sa_session.set_access_profile
(‘PRIVACY’,SYS_CONTEXT('userenv','EXTERNAL_NAME');
```

ANEXO A - ORACLE LABEL SECURITY: AUTORIZACIONES ESPECIALES PARA USUARIOS

READ — La autorización READ permite que un usuario acceda a todos los datos protegidos por Oracle Label Security, sin embargo, la mediación de acceso todavía se aplica en las operaciones UPDATE, INSERT y DELETE. Oracle Label Security no realiza la verificación de mediaciones en las operaciones SELECT.

FULL — La autorización FULL desactiva todo tipo de mediación de acceso de Oracle Label Security. Un usuario con la autorización FULL puede realizar operaciones SELECT, UPATE, INSERT y DELETE sin autorización de etiquetas. Tenga en cuenta que las autorizaciones Oracle SYSTEM y OBJECT todavía se aplican. Por ejemplo, un usuario todavía debe tener SELECT en la tabla de aplicaciones. La autorización FULL desactiva la verificación de mediación de acceso en el nivel de fila individual.

WRITEDOWN — La autorización WRITEDOWN permite que un usuario modifique el componente de nivel de una etiqueta y reduce la sensibilidad de la etiqueta. Por ejemplo, los datos de aplicaciones con etiquetas *Top Secret: Alpha, Beta* podrían cambiar a *Secret: Alpha, Beta*. Esta autorización solo es aplicable a políticas que utilizan la opción de actualización de etiquetas.

WRITEUP — La autorización WRITEUP permite que un usuario modifique el componente de nivel de una etiqueta y aumente la sensibilidad de la etiqueta. Por ejemplo, los datos de aplicaciones con etiquetas *Secret: Alpha, Beta* podrían cambiar a *Top Secret: Alpha, Beta*. Tenga en cuenta que la autorización de la etiqueta *Nivel Máximo* asignada al usuario limitará la modificación. Esta autorización solo es aplicable a políticas que utilizan la opción de actualización de etiquetas.

WRITEACROSS — La autorización WRITEACROSS permite que un usuario modifique los compartimentos y grupos de una etiqueta en cualquier compartimento o grupo válido de Oracle Label Security para la política. Por ejemplo, los datos de aplicaciones con la etiqueta *Secret: Alpha, Beta* pueden ser modificados a *Secret: Alpha, Beta, Delta* incluso si el usuario no está autorizado para el compartimento *Delta*. Esta autorización solo es aplicable a políticas que utilizan la opción de actualización de etiquetas.

PROFILE ACCESS — La autorización PROFILE ACCESS permite que un usuario asuma las autorizaciones Oracle Label Security de cualquier otro usuario. Por ejemplo, el usuario *Scott* que tiene acceso a los compartimentos *A,B y C* podría asumir el perfil de usuario *Joe* que tiene acceso a los compartimentos *A,B, C y D*. Esta funcionalidad podría ser útil en un ámbito donde una aplicación utiliza una sola cuenta de aplicaciones para todos los usuarios de aplicaciones. La cuenta de aplicaciones podría utilizar la autorización PROFILE ACCESS para asumir inmediatamente un perfil designado para seguridad de etiquetas cuando un usuario de aplicaciones se conecta al sistema.

ANEXO B - ORACLE LABEL SECURITY: OPCIONES PARA LA APLICACIÓN DE POLÍTICAS

Las opciones para la aplicación de políticas de Oracle Label Security pueden personalizarse para cada política. Por ejemplo, una política de Recursos Humanos y una política de Defensa pueden estar en la misma base de datos Oracle y brindar diferentes grados de protección. La aplicación de Recursos Humanos podría utilizar la opción READ CONTROL y la política de Defensa podría utilizar las opciones READ CONTROL y WRITE CONTROL.

READ CONTROL — Aplica la política a todas las consultas; solo las filas autorizadas son accesibles par alas operaciones SELECT, UPDATE y DELETE.

INSERT CONTROL — Aplica la política a las operaciones INSERT, de acuerdo con el algoritmo Oracle Label Security para el acceso de escritura.

UPDATE CONTROL — Aplica la política a las operaciones UPDATE en las columnas de datos dentro de un fila, de acuerdo con el algoritmo Oracle Label Security para el acceso de escritura.

DELETE CONTROL — Aplica la política a las operaciones DELETE, de acuerdo con el algoritmo Oracle Label Security para el acceso de escritura.

WRITE CONTROL — Determina la capacidad de INSERTAR, ACTUALIZAR y ELIMINAR (INSERT, UPDATE AND DELETE) los datos de una fila. Si esta opción está configurada, impone INSERT_CONTROL, UPDATE_CONTROL y DELETE_CONTROL.

LABEL DEFAULT — Si el usuario no especifica explícitamente una etiqueta en INSERT, se utiliza el valor *row label (etiqueta de fila)* por defecto de los usuarios. Por defecto, el valor *row label* es internamente computado por Oracle Label Security mediante el uso de valores para autorización de etiquetas especificados para el usuario. Un usuario puede configurar la etiqueta de la fila de manera independiente, pero solo:

En un nivel que sea menor o igual al nivel de la etiqueta de sesión, y mayor o igual al nivel mínimo del usuario.

Para incluir un subgrupo de compartimentos y grupos de la etiqueta de sesión, para lo cual el usuario está autorizado con acceso de escritura.

LABEL UPDATE — Aplica la política a las operaciones UPDATE que establecen o cambian el valor de una etiqueta adjunta a una fila. Los privilegios WRITEUP, WRITEDOWN y WRITEACROSS solo son aplicados si la opción LABEL_UPDATE está configurada.

LABEL CHECK — Aplica la política READ_CONTROL a las sentencias INSERT y UPDATE (INSERTAR Y ACTUALIZAR) para asegurar que la nueva etiqueta de la fila puede ser accedida mediante lectura por cualquier usuario después de una sentencia INSERT o UPDATE.

NO CONTROL — No aplica opciones. No obstante, se puede aplicar una función de etiquetado o un predicado SQL.

ANEXO C - ORACLE LABEL SECURITY: AUTORIZACIÓN A USUARIOS

Las autorizaciones de usuarios Oracle Label Security deben ser establecidas por un administrador de seguridad antes de que un usuario de aplicaciones pueda acceder a una tabla de aplicaciones protegida por Oracle Label Security. Las autorizaciones de etiquetas de los usuarios de Oracle Label Security se definen de la siguiente manera:

Nivel Máximo— El nivel máximo de sensibilidad al que un usuario puede acceder. En un entorno *hosting,* solo puede haber un nivel único. En ámbitos de gobierno y defensa, pueden definirse cuatro o cinco niveles.

Nivel Mínimo— El nivel mínimo de sensibilidad en el que un usuario puede escribir los datos. Por ejemplo, un administrador puede evitar que los usuarios etiqueten los datos como *Públicos* o *Internet* al asignar un nivel mínimo de *Company Confidencial (Confidencial para la Empresa).*

Nivel por Defecto — El nivel utilizado por defecto cuando un usuario se conecta a la base de datos. Por ejemplo, un usuario puede configurar su nivel por defecto en Secret. Cuando se conecta al sistema, el nivel por defecto se iniciará en Secret.

Nivel de Filas— El nivel utilizado para etiquetar los datos ingresados por el usuario en la base de datos a través de la aplicación o directamente mediante una herramienta como SQL*Plus.

Compartimentos de Lectura— El grupo de compartimentos asignados al usuario y utilizados durante la mediación de acceso READ. Por ejemplo, si un usuario tiene compartimentos *A,B y C*, podría ver los datos con compartimentos *A y B* pero no los datos con compartimentos *A,B,C y D*. El algoritmo de lectura será definido en la próxima sección.

Compartimentos de Escritura— El grupo de compartimentos asignados al usuario y utilizados durante la mediación de acceso WRITE. Por ejemplo, se podría otorgar a un usuario acceso READ y WRITE a los compartimentos *A y B* pero acceso READ-ONLY (de solo lectura) al compartimento *C*. Si el registro de una aplicación tuviese etiquetas en los compartimentos *A,B y C,* el usuario no estaría autorizado a actualizar el registro ya que no tiene el acceso WRITE (de escritura) para el compartimento *C*.

Grupos de Lectura— El conjunto de grupos asignado a un usuario y utilizado durante la mediación de acceso READ. Por ejemplo, si un usuario tuviese el grupo *Manager (administrador)*, podría ver los datos del grupo *Manager* pero no los datos del grupo *Senior VP (VP Sénior)*. El algoritmo de lectura se definirá en la próxima sección.

Grupos de Escritura— El conjunto de grupos asignado al usuario y utilizado durante la mediación de acceso WRITE. Por ejemplo, un usuario podría estar autorizado con el acceso READ y WRITE al grupo *Senior VP* pero con el acceso READ-ONLY al grupo *Manager*. Si el registro de una aplicación tuviese la etiqueta de un grupo único, *Manager*, el usuario no estaría autorizado a actualizar el registro ya que no tendría acceso WRITE al grupo *Manager*.

Oracle Label Security – Mejores Prácticas para Aplicaciones de Gobierno y Defensa
Junio de 2007
Autor: Paul Needham
Coautor: Peter Wahl

Oracle Corporation
Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Consultas:
Teléfono: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Copyright © 2007, Oracle. **Todos los derechos reservados.**
El presente documento tiene solo fines informativos y su contenido está sujeto a cambios sin que medie notificación alguna. El presente documento puede contener errores y no está sujeto a ninguna otra garantía ni condición, ya sea oral o que se encuentre implícita en la ley, con inclusión de garantías y condiciones implícitas de comerciabilidad o aptitud para un fin específico. En especial, negamos cualquier responsabilidad con respecto al presente documento, el cual no crea obligación contractual alguna, sea en forma directa o indirecta. El presente documento no podrá ser reproducido ni transmitido de ninguna forma ni por ningún medio, sea electrónico o mecánico, con ningún fin, sin que hayamos otorgado previamente nuestro consentimiento por escrito. Oracle es marca registrada de Oracle Corporation y/o sus afiliadas. Otros nombres pueden ser marcas comerciales de sus respectivos propietarios.