Oracle® DIVAdirector

Guía de seguridad

Versión 5.3

E71136-01

Diciembre de 2015

ORACLE®

Oracle® DIVAdirector
Guía de seguridad

E71136-01

Tabla de contenidos

Prólogo

En la guía de seguridad de DIVAdirector de Oracle se incluye información sobre el producto DIVAdirector y se explican los principios generales de la seguridad de la aplicación.

Destinatarios

Esta guía está destinada a cualquier persona que se encargue de la utilización de funciones de seguridad y de la instalación y la configuración seguras de DIVAdirector.

Accesibilidad a la documentación

Para obtener información sobre el compromiso de Oracle con la accesibilidad, visite el sitio web del Programa de Accesibilidad de Oracle en http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Acceso a My Oracle Support
Los clientes de Oracle que hayan contratado servicios de soporte electrónico pueden acceder a ellos mediante My Oracle Support. Para obtener información, visite http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info o, si tiene alguna discapacidad auditiva, visite http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs.

1

Capítulo 1. Visión general

En este capítulo, se brinda una visión general del producto DIVAdirector y se explican los principios generales de la seguridad de la aplicación.

1.1. Visión general del producto

Oracle DIVAdirector es una herramienta que se utiliza para interactuar con sistemas Oracle DIVArchive existentes. La interfaz de usuario (IU) se entrega en formato de gráficos mediante un explorador web. DIVAdirector consta de los siguientes componentes principales:

1.1.1. Servidor de DIVAdirector

El servidor de DIVAdirector proporciona interfaces con DIVArchive mediante la API C++ para todas las operaciones requeridas por la web de DIVAdirector. También sincroniza la información de objetos detectados almacenada en DIVArchive en su propia base de datos. Supervisa las carpetas de entrega configuradas para proxies, metadatos y operaciones, y mantiene el historial de todas las carpetas de entrega y operaciones de IU.

1.1.2. Web de DIVAdirector

El módulo web de DIVAdirector proporciona una interfaz de usuario basada en web, lo cual permite a los usuarios buscar objetos detectados en DIVArchive, administrar los derechos de acceso de los usuarios, agregar metadatos para los activos, reproducir proxies de objetos y realizar operaciones, por ejemplo, de restauración y de supresión y restauración parcial, en elementos agregados a las ubicaciones de trabajo o a las listas de tomas. También brinda a los usuarios la capacidad de examinar archivos de manera local y de archivar contenido en el sistema DIVArchive.

1.1.3. Base de datos de DIVAdirector

DIVAdirector utiliza PostgreSQL para almacenar toda la información de valores de configuración, historial de operaciones, usuarios, proxies, metadatos y activos de DIVArchive.

1.1.4. Servicio de transcodificador de DIVAdirector

El servicio de transcodificador de DIVAdirector es un servicio aparte que es llamado por DIVAdirector para transcodificar clips de alta resolución a proxies de baja resolución que luego aparecen en la IU de la web de DIVAdirector.

1.1.5. Servicio de gestor de tareas de DIVAdirector

El servicio de gestor de tareas de DIVAdirector es una aplicación de servicio de ventanas visible en el cuadro de diálogo estándar de gestor de control de servicios. Esta aplicación se encarga de ejecutar las tareas que puedan ser de larga ejecución en un proceso en segundo plano.

1.1.6. Servicio API de DIVAdirector

Este servicio expone los puntos finales para la funcionalidad común de DIVAdirector. Inicialmente, solo un pequeño subjuego de la lógica de DIVAdirector se incluirá en este servicio. Los puntos finales expuestos mediante este servicio seguirán creciendo a medida que la funcionalidad migra gradualmente de la web de DIVAdirector.

1.2. Principios generales de seguridad

En las siguientes secciones se describen los principios fundamentales necesarios para utilizar cualquier aplicación de manera segura.

1.2.1. Mantenga el software actualizado

Mantenga actualizada la versión de DIVAdirector que ejecuta. Puede encontrar las versiones actuales del software para descargar en Oracle Software Delivery Cloud:

`https://edelivery.oracle.com/`

1.2.2. Restrinja el acceso de red a los servicios críticos

DIVAdirector utiliza los siguientes puertos TCP/IP:

- tcp/7680 para comandos de la interfaz de usuario
- tcp/8080 para el servidor HTTP

Para las versiones de DIVAdirector posteriores a 5.3.0 se requieren tres puertos adicionales:

- tcp/9763: integración con el servicio DIVArchiveWS
- tcp/9876: integración con el servicio DIVArchiveWS
- tcp/6543: integración con el servicio API de DIVAdirector

Nota:

Los números de puerto mencionados anteriormente son actuales, sin embargo, es probable que cambien en el futuro.

1.2.3. Ejecute el sistema como usuario ADMIN y utilice el principio de menor privilegio donde sea posible

DIVAdirector proporciona un usuario superadministrador por defecto cuya contraseña se debe cambiar después del primer inicio de sesión. Luego, este usuario puede crear otros usuarios con diferentes permisos de grupo para acceso y operaciones.

Si no se cambia la contraseña por defecto, el sistema puede ser víctima de actividades maliciosas. La contraseña por defecto de la cuenta de superadministrador se debe cambiar inmediatamente después de la instalación y la configuración, y, a partir de ese momento, cada 180 días (como mínimo). Después de realizar el cambio, debe guardar las contraseñas en una ubicación segura, fuera de línea, donde solo pueda acceder el soporte de Oracle, si fuera necesario.

1.2.4. Supervise la actividad del sistema

Puede supervisar la actividad del sistema para determinar el grado de eficiencia con el que está funcionando DIVAdirector. Los logs se ubican en C:/Program Files (x86)/DIVAdirector 5/cmg-server y C:/Program Files (x86)/DIVAdirector 5/www/logs.

1.2.5. Manténgase actualizado sobre la información de seguridad más reciente

Puede acceder a varias fuentes de información de seguridad. Para obtener información de seguridad y alertas para una gran variedad de productos de software, consulte:

`http://www.us-cert.gov`

La mejor manera de mantenerse actualizado en cuanto a la seguridad es ejecutar la versión más reciente del software de DIVAdirector.

2

Capítulo 2. Instalación segura

En este capítulo, se detallan los procesos de planificación para lograr una instalación segura y se describen varias topologías de despliegue recomendadas para los sistemas.

2.1. Comprensión del entorno

Para comprender mejor las necesidades de seguridad, debe hacerse las siguientes preguntas:

2.1.1. ¿Qué recursos necesitan protección?

Puede proteger muchos de los recursos en el entorno de producción. Tenga en cuenta el tipo de recursos que desea proteger cuando determine el nivel de seguridad que va a proporcionar. Cuando utilice DIVAdirector, proteja los siguientes recursos:

2.1.1.1. Disco de datos principales

Existen carpetas proxy que contienen clips de baja resolución. En general, se encuentran en discos locales o remotos conectados al sistema DIVAdirector. El acceso independiente a estos discos (no por medio de DIVAdirector) presenta un riesgo de seguridad. Este tipo de acceso externo podría ser desde un sistema no fiable que lee estos discos o escribe en ellos, o desde un sistema interno que accidentalmente proporciona acceso a estos dispositivos de disco.

2.1.1.2. Disco de base de datos y discos de copias de seguridad

Existen recursos de discos de base de datos y de discos de copia de seguridad que se usan para conformar DIVAdirector. En general, son discos locales o remotos conectados a los sistemas DIVAdirector. El acceso independiente a estos discos (no por medio de DIVAdirector) presenta un riesgo de seguridad. Este tipo de acceso externo podría ser desde un sistema no fiable que lee estos discos o escribe en ellos, o desde un sistema interno que accidentalmente proporciona acceso a estos dispositivos de disco.

2.1.1.3. Archivos y valores de configuración

Los valores de configuración de los sistemas DIVAdirector deben estar protegidos de usuarios que no sean administradores en el nivel del sistema operativo. En general, estos valores de configuración están protegidos automáticamente por usuarios administradores en el nivel del sistema operativo. Tenga en cuenta que si habilita la opción de escritura de los archivos de

configuración para usuarios del sistema operativo que no sean administradores, se genera un riesgo para la seguridad. Los archivos confidenciales abarcan todos los archivos de configuración de la aplicación incluidos en el directorio de instalación, entre ellos:

- www/Web.config
- Api/Oracle.DIVAdirector.Api.exe.config
- TaskManager/Oracle.DIVAdirector.TaskManager.exe.config
- cmgserver/cmgserver.ini

2.1.2. ¿De quién se protegen los recursos?

En general, los recursos descritos en la sección anterior deben estar protegidos del acceso de todos los usuarios que no sean administradores en un sistema configurado, o de un sistema externo no fiable que pueda acceder a estos recursos por medio de tejido de FC o WAN.

2.1.3. ¿Qué sucede si falla la protección de los recursos estratégicos?

Los fallos de protección de recursos estratégicos pueden incluir desde el acceso inadecuado (acceso a datos más allá de las operaciones normales de DIVAdirector) hasta daños en los datos (escritura en el disco o cinta más allá de los permisos normales).

3

Capítulo 3. Funciones de seguridad

Para evitar amenazas de seguridad potenciales, los clientes que utilizan DIVAdirector deben preocuparse por la autenticación y autorización del sistema.

Estas amenazas de seguridad pueden minimizarse con una configuración apropiada y siguiendo la lista de comprobación posterior a la instalación en Apéndice A, *Lista de comprobación de despliegue seguro*.

3.1. El modelo de seguridad

Las funciones de seguridad críticas que ofrecen protección frente a las amenazas de seguridad son:

- Autenticación: permite garantizar que solo las personas autorizadas tengan acceso al sistema y a los datos.
- Autorización: permite controlar el acceso a los privilegios y los datos del sistema. Esta función se basa en la autenticación para garantizar que las personas obtengan solo el acceso apropiado.

Apéndice A

Apéndice A. Lista de comprobación de despliegue seguro

1. Establezca contraseñas seguras para la cuenta de administrador y cualquier otra cuenta del sistema operativo que tenga roles de servicio o administrador de DIVArchive o DIVAdirector asignados.
2. No utilice una cuenta de sistema operativo de administrador local, en cambio, asigne roles según sea necesario a otras cuentas de usuario.
3. Establezca una contraseña segura para el usuario administrador de DIVAdirector. Cambie inmediatamente la contraseña instalada por defecto por una contraseña segura. Puede hacerlo desde la pantalla de configuración **Admin** (Administrador), **Personal** (Personal) de DIVAdirector.
4. Instale un firewall en el sistema y aplique las reglas por defecto de los puertos DIVAdirector.
5. Instale actualizaciones del sistema operativo y de DIVAdirector periódicamente, puesto que estas incluyen parches de seguridad.
6. Instale un antivirus y excluya el almacenamiento y los procesos de DIVAdirector por motivos de rendimiento.