Oracle® DIVArchive

Guía de seguridad

Versión 7.4

E77634-01

Junio de 2016

ORACLE®

Oracle® DIVArchive
Guía de seguridad

E77634-01

Tabla de contenidos

Prólogo

En la guía de seguridad de DIVArchive de Oracle se incluye información sobre el producto DIVArchive 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 DIVArchive.

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 DIVArchive y se explican los principios generales de la seguridad de la aplicación.

1.1. Visión general del producto

DIVArchive de Oracle es un sistema de gestión de almacenamiento de contenido distribuido. DIVArchive consta de los siguientes componentes principales:

1.1.1. Oracle DIVArchive Manager

DIVArchive Manager es el componente principal en un sistema DIVArchive. DIVArchive Manager controla y gestiona todas las operaciones de archivos. Las aplicaciones de iniciador envían las solicitudes de operaciones mediante la API de cliente de DIVArchive. Como opción de compra, DIVArchive también es compatible con los componentes de gestión principal y secundario de DIVArchive Manager. Para obtener más información sobre DIVArchive, consulte la biblioteca de documentación del cliente del software DIVArchive versión 7.4 en:

https://docs.oracle.com/en/storage/#csm

1.1.2. Oracle DIVArchive Actor

DIVArchive Actor se encarga de mover los datos entre los dispositivos en el sistema de producción. Admite la transferencia de datos entre los distintos tipos de dispositivos y gestiona las operaciones de transcodificación con el software de transcodificación Telestream (opcional).

DIVArchive Manager inicia y coordina todas las operaciones de Actor. Un solo DIVArchive Manager puede configurar y controlar uno o más componentes Actor.

1.1.3. Gestor de robot de DIVArchive

Si bien puede utilizar DIVArchive solo para gestionar el almacenamiento de disco, se puede expandir la capacidad de almacenamiento agregando una o más bibliotecas de cintas. En estos casos, el módulo de gestor de robot de DIVArchive proporciona una capa de software intermedia para que DIVArchive Manager pueda interactuar con distintos tipos de bibliotecas

de cintas. Se conecta a DIVArchive Manager mediante TCP/IP. El gestor de robot de DIVArchive interactúa con la biblioteca por medio de una interfaz directa a la biblioteca (mediante una SCSI nativa o una SCSI sobre canal de fibra) o por medio de una conexión Ethernet al software de control de bibliotecas del fabricante.

1.1.4. Servicio de copia de seguridad de DIVArchive

Para garantizar la fiabilidad y la supervisión de las copias de seguridad de la base de datos de Oracle y la base de datos de metadatos, se introdujo el servicio de copia de seguridad de DIVArchive.

El componente de servicio de copia de seguridad de DIVArchive se instala como parte integral de la instalación estándar del sistema DIVArchive. Por lo general, el componente se instala en el mismo servidor en el que se instalan DIVArchive Manager y Oracle Database. El servicio de copia de seguridad de DIVArchive permite la configuración de copias de seguridad programadas mediante el archivo de configuración. El servicio de copia de seguridad de DIVArchive gestiona y supervisa todo el proceso de creación de copias de seguridad.

El servicio de copia de seguridad de DIVArchive ahora incorpora la capacidad de enviar correos electrónicos en caso de que surjan problemas en el proceso de creación de copias de seguridad de los archivos de la base de datos y la base de datos de metadatos. Para aprovechar esta función, debe configurar DIVArchive para que esté conectado a un proveedor de correo electrónico SMTP. Las notificaciones por correo electrónico se configuran por medio de la utilidad de configuración de DIVArchive en el separador Manager Setting (Configuración de Manager).

Para obtener más información sobre cómo instalar y configurar el servicio de copia de seguridad de DIVArchive, consulte la biblioteca de documentación del cliente del software DIVArchive versión 7.4 en:

https://docs.oracle.com/en/storage/#csm

1.1.5. Oracle DIVArchive Avid Connectivity

El propósito de Avid Connectivity con DIVArchive es transferir datos de archivo desde DIVArchive, y hacia él, en formatos de video específicos, y permitir el archivado y la recuperación de clips únicos o de una secuencia de clips. Los componentes relacionados AMC y TMC se instalan junto con la instalación principal de DIVArchive. Se requiere una instalación adicional para ciertos plugins de AMC y TMC.

1.1.6. Supervisor de carpetas de entrega de DIVArchive

El supervisor de carpetas de entrega de DIVArchive supervisa de manera automática los archivos creados recientemente hasta en 20 carpetas locales o carpetas de FTP (o combinaciones de estas). Se admiten uno o varios archivos (en carpetas de FTP) por objeto

de DIVArchive. Cuando se identifica un nuevo archivo (o carpeta de FTP), el supervisor de carpetas de entrega envía automáticamente una solicitud de almacenamiento a DIVArchive para almacenar el archivo nuevo o las carpetas nuevas. Una vez que los archivos se almacenan de manera correcta, se suprimen automáticamente del origen.

1.1.7. SNMP de DIVArchive

El agente del Protocolo Simple de Administración de Redes (SNMP) de DIVArchive y la base de información de gestión (MIB) admiten la supervisión del estado y de las actividades de DIVArchive y de sus subsistemas mediante una aplicación de supervisión de terceros mediante el protocolo SNMP. SNMP de DIVArchive solo se admite en entornos de Windows.

1.1.8. DIVArchive Storage Plan Manager (SPM)

DIVArchive Storage Plan Manager (SPM) proporciona la migración automática y gestiona el ciclo de vida del material dentro del archivo según las reglas y las políticas definidas en la configuración de SPM.

El componente SPM también se utiliza para suprimir material de las matrices gestionadas de SPM (según las marcas de agua en el espacio del disco).

1.1.9. Servicio de migración de DIVArchive

DIVArchive incluye un servicio de migración incrustado. Es un servicio interno (de DIVArchive) nuevo e independiente que ayuda a los usuarios a programar y ejecutar trabajos para migrar contenido entre los distintos medios dentro del sistema DIVArchive. Puede utilizar la interfaz gráfica de usuario de control o el cliente de línea de comandos.

1.1.10. VACP de DIVArchive

El Protocolo de Comando de Archivo de Video (VACP, Video Archive Command Protocol) es un protocolo desarrollado por Harris Automation para interactuar con un sistema de archivo. DIVArchive tiene su propia API para comunicarse con DIVArchive Manager, que no es compatible con VACP.

1.1.11. Interfaz gráfica de usuario de control de DIVArchive

La interfaz gráfica de usuario de control de DIVArchive se utiliza para supervisar y controlar las operaciones en DIVArchive. Se pueden ejecutar y conectar varias interfaces gráficas de usuario de DIVArchive en el mismo sistema DIVArchive al mismo tiempo.

1.1.12. Utilidad de configuración de DIVArchive

La utilidad de configuración de DIVArchive se usa para configurar un sistema DIVArchive. Aunque se utiliza principalmente para configurar DIVArchive, algunas funciones operacionales también se ejecutan desde la utilidad de configuración.

1.1.13. Puerta de enlace de acceso de DIVArchive

La puerta de enlace de acceso permite el uso y la interacción de varios sistemas DIVArchive independientes desde una sola computadora. Es la solución global para la distribución de contenido. La replicación automática de archivos para reflejar sitios proporciona un método sencillo para la distribución local, la creación de copias de seguridad y la recuperación ante desastres con seguridad, control de ancho de banda y verificación del total de control. Se supervisan las redes y DIVAnet garantiza la entrega final del contenido.

1.1.14. Supresión local de DIVArchive

La supresión local es un servicio que supervisa las funciones de replicación de objetos entre un sistema DIVArchive local (por ejemplo, DIVAlocal) y uno (o más) sistemas DIVArchive remotos (por ejemplo, DIVAdr). Una vez que el objeto se replicó correctamente en el sistema DIVArchive remoto, se marca como elegible para suprimirse del sistema DIVArchive local.

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. Mantener el software actualizado

Manténgase actualizado con la versión de DIVArchive que ejecute. Puede encontrar las versiones actuales del software para descargar en Oracle Software Delivery Cloud:

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

1.2.2. Restringir el acceso de red a los servicios críticos

DIVArchive usa los siguientes puertos TCP/IP:

- El gestor de robot de DIVArchive usa *`tcp/8500`*
- DIVArchive Manager usa tcp/9000
- El servicio de copia de seguridad de DIVArchive usa tcp/9300
- La puerta de enlace de acceso de DIVArchive usa tcp/9500
- DIVArchive Actor usa *`tcp/9900`*
- El servicio de migración de DIVArchive usa tcp/9191

1.2.3. Ejecutar el sistema como usuario DIVA y usar el principio de menor privilegio cuando sea posible

No ejecute los servicios de DIVArchive por medio de una cuenta de usuario de sistema operativo de administrador (o root). Siempre debe ejecutar todos los servicios de DIVArchive por medio de un usuario (o grupo) de sistema operativo dedicado llamado DIVA.

La interfaz gráfica de usuario de control de DIVArchive proporciona tres perfiles de usuario fijos (administrador, operador y usuario). Las cuentas de administrador y de operador requieren una contraseña para obtener acceso. Debe asignar una contraseña de administrador u operador en la utilidad de configuración antes de usar estos perfiles.

Las contraseñas de las cuentas de administrador y de operador se crean durante la instalación y la configuración. A partir de ese momento, las contraseñas se deben cambiar cada 180 días (como mínimo). Las contraseñas deben estar disponibles para el soporte de Oracle si es necesario.

1.2.4. Supervisar la actividad del sistema

Supervise la actividad del sistema para determinar si DIVArchive está funcionando correctamente y si está registrando alguna actividad inusual. Consulte los archivos log ubicados en el directorio de instalación de */Program/log/*.

1.2.5. Mantenerse 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 DIVArchive.

2

Capítulo 2. Instalación segura

En este capítulo, se describe el proceso de planificación para una instalación segura y se describen varias topologías de despliegue recomendadas para los sistemas.

2.1. Descripción 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 DIVArchive, proteja los siguientes recursos:

2.1.1.1. Disco de datos principales

Para crear sistemas DIVArchive se utilizan recursos de discos de datos y de discos de caché. En general, son discos locales o remotos conectados a los sistemas DIVArchive. El acceso independiente a estos discos (por otros medios que no sean DIVArchive) 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, disco de metadatos y discos de copias de seguridad

Para crear sistemas DIVArchive con objetos complejos se utilizan recursos de discos de base de datos, de discos de metadatos y de discos de copias de seguridad. En general, son discos locales o remotos conectados a los sistemas DIVArchive. El acceso independiente a estos discos (por otros medios que no sean DIVArchive) 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. Cintas de DIVArchive

Permitir el acceso independiente a las cintas, que generalmente se encuentran en una biblioteca de cintas controlada por los sistemas DIVArchive, donde se escriben los datos, es un riesgo de seguridad.

2.1.1.4. Metadatos de cintas de exportación

Los volcados de metadatos de cintas creados a partir de la operación de exportación contienen datos y metadatos. Los permisos de datos y metadatos deben restringirse solo a la cuenta de sistema operativo de administrador (o root) o al usuario (o grupo) de sistema operativo DIVA durante una actividad de exportación o importación de rutina.

2.1.1.5. Archivos y valores de configuración

Los valores de configuración de los sistemas DIVArchive deben estar protegidos de usuarios que no sean administradores en el nivel del sistema operativo. Permitir la escritura de los archivos de configuración a los usuarios del sistema operativo que no sean administradores presenta un riesgo para la seguridad; por lo tanto, se deben restringir los permisos para estos archivos solo a la cuenta de administrador (o root) del sistema operativo o al usuario (o grupo) de sistema operativo DIVA.

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 DIVArchive) hasta daños en los datos (escritura en el disco o cinta más allá de los permisos normales).

2.2. Topologías de despliegue recomendadas

En esta sección, se describe cómo instalar y configurar un componente de infraestructura de manera segura. Para obtener más información sobre cómo instalar DIVArchive, consulte la biblioteca de documentación del cliente de DIVArchive 7.4 en:

https://docs.oracle.com/en/storage/#csm

Tenga en cuenta los siguientes puntos cuando instale y configure DIVArchive:

2.2.1. Red de metadatos independiente

Para lograr la conexión de los componentes de servicios de DIVArchive entre sí, la conexión a la base de datos de metadatos y la conexión desde sus clientes, proporcione una red TCP/IP independiente y hardware de switch que no esté conectado a ninguna WAN. Como el tráfico de metadatos se implementa mediante TCP/IP, un ataque externo a este tráfico es posible en teoría. Si se configura una red de metadatos independiente, se reduce este riesgo y se obtiene un mejor rendimiento. Si no es posible configurar una red independiente, al menos, debe denegar el tráfico a los puertos de DIVArchive desde una WAN externa y desde cualquier host que no sea de confianza en la red. Consulte Restringir el acceso de red a los servicios críticos.

2.2.2. Zonas de canal de fibra

Utilice las zonas de canal de fibra para denegar el acceso a los discos DIVArchive conectados mediante canal de fibra desde cualquier servidor que no requiera acceso a los discos. Preferiblemente, utilice un switch de canal de fibra separado para conectar físicamente sólo los servidores que necesitan acceso al disco.

2.2.3. Protección del acceso de configuración a los discos SAN

Por lo general, puede accederse a los discos SAN RAID por motivos administrativos mediante TCP/IP o, lo que ocurre más habitualmente, mediante HTTP. Debe proteger los discos de acceso externo; para esto, limite el acceso administrativo a los discos SAN RAID sólo a sistemas dentro de un dominio de confianza. Además, cambie la contraseña por defecto en las matrices de discos.

2.2.4. Instalación del paquete DIVArchive

En primer lugar, instale solo aquellos servicios de DIVArchive que necesite. Por ejemplo, si no piensa ejecutar la interfaz gráfica de usuario ni la utilidad de configuración desde un sistema, anule la selección de la casilla correspondiente en la lista de componentes que se instalarán. Los permisos y los propietarios de directorio de la instalación por defecto de DIVArchive se deben restringir solo a la cuenta de administrador (o root) o al usuario (o grupo) de sistema operativo DIVA.

2.2.5. Seguridad de cintas de DIVArchive

Impida el acceso externo a las cintas de DIVArchive dentro de una biblioteca de cintas controlada por el sistema DIVArchive. El acceso sin autorización a cintas de DIVArchive puede poner en peligro o destruir datos del usuario.

2.2.6. Copias de seguridad

Configure y realice copias de seguridad de la base de datos utilizando el servicio de copias de seguridad de DIVArchive. Los permisos para los volcados de copias de seguridad se deben

restringir solo a la cuenta de administrador (o root) del sistema operativo o al usuario (o grupo) de sistema operativo DIVA.

2.3. Configuración después de la instalación

Después de instalar cualquier componente de DIVArchive, revise la lista de comprobación de seguridad en el Apéndice A, *Lista de comprobación de despliegue seguro*.

3

Capítulo 3. Funciones de seguridad

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

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

3.1. El modelo de seguridad

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

- Autenticación: garantiza que solo personas autorizadas tengan acceso al sistema y a los datos.
- Autorización: control de acceso para los privilegios y los datos del sistema. Esta función se basa en la autenticación para garantizar que las personas solo obtengan el nivel de acceso adecuado.

3.2. Autenticación

La interfaz gráfica de usuario de control de DIVArchive proporciona tres perfiles de usuario fijos (administrador, operador y usuario). Las cuentas de administrador y de operador requieren una contraseña para obtener acceso. Debe asignar una contraseña de administrador u operador en la utilidad de configuración antes de usar estos perfiles.

Las contraseñas de las cuentas de administrador y de operador se deben cambiar cada 180 días (o menos). Las contraseñas deben estar disponibles para el soporte de Oracle si es necesario.

3.3. Control de acceso

El control de acceso en DIVArchive está dividido en tres perfiles. Las cuentas de administrador y de operador requieren una contraseña para obtener acceso. Debe asignar una contraseña de cuenta de administrador u operador en la utilidad de configuración antes de usar estos perfiles.

Usuario: después de establecer la conexión con DIVArchive Manager, la interfaz gráfica de usuario de control solo le permitirá al usuario supervisar las operaciones de DIVArchive y recuperar datos de la base de datos. Esto se conoce como perfil de usuario. No se puede acceder a todas las funciones que ejecutan comandos en DIVArchive por medio del modo de perfil de usuario. Esto permite que existan situaciones en las que se requiere supervisión, pero no se permite el envío de comandos a DIVArchive.

Administrador: para enviar solicitudes a DIVArchive, como solicitudes de archivo o de restauración, o para expulsar una cinta de una biblioteca, debe pasar al perfil de administrador. El perfil de administrador está protegido por una contraseña. La contraseña para este perfil se debe asignar en la utilidad de configuración antes de usar el perfil. Para obtener más información, consulte la biblioteca de documentación del cliente de Oracle DIVArchive 7.4 en:

https://docs.oracle.com/en/storage/#csm

Operador: además de los permisos del perfil de usuario, el perfil de operador brinda acceso a la utilidad de transferencia de objetos y requiere una contraseña que se debe configurar en la utilidad de configuración antes de usar el perfil.

Apéndice A

Apéndice A. Lista de comprobación de despliegue seguro

1. Establezca contraseñas seguras para la cuenta de administrador (o root) y cualquier otra cuenta del sistema operativo que tenga roles de servicio o administrador de DIVArchive asignados, incluidos:
   - Los lD de usuario de Oracle DIVA (si se usan)
   - Cualquier cuenta administrativa de matriz de discos
2. No utilice una cuenta de sistema operativo de administrador local. Asigne roles según sea necesario a otras cuentas de usuario.
3. Establezca contraseñas seguras para las cuentas de administrador y operador en la interfaz gráfica de usuario de control. Debe asignar una contraseña para estos perfiles en la utilidad de configuración antes de usarlos.
4. Establezca una contraseña segura para iniciar sesión en la base de datos de Oracle.
5. Instale un firewall en todos los sistemas y aplique las reglas por defecto de los puertos de DIVArchive. Restrinja el acceso a la API (`tcp/9000`) de DIVArchive de los IP que requieren acceso utilizando las reglas de firewall.
6. Instale actualizaciones del sistema operativo y de DIVArchive periódicamente, puesto que estas incluyen actualizaciones de seguridad.
7. Instale un antivirus y excluya el almacenamiento y los procesos de DIVArchive (por motivos de rendimiento).
8. Se recomienda separar las unidades de disco de canal de fibra y de cinta de canal de fibra, ya sea físicamente o mediante zonas de canal de fibra, de manera que los discos y los dispositivos de cinta no compartan el mismo puerto de HBA. Para los discos gestionados, solo los usuarios de DIVArchive Actor deben tener acceso a las unidades de disco y de cinta. Esta práctica de seguridad ayuda a evitar los accidentes de pérdida de datos debido a la sobrescritura accidental de la cinta o el disco.
9. Configure un conjunto de copias de seguridad apropiado para la configuración y la base de datos de DIVArchive. Las copias de seguridad forman parte de la seguridad y proporcionan una manera de restaurar los datos perdidos, ya sea accidentalmente o por algún tipo de infracción de seguridad. La copia de seguridad debe incluir alguna política cuando se la transporta a una ubicación externa. Las copias de seguridad tienen que estar protegidas de la misma manera que las cintas y los discos de DIVArchive.