Oracle® DIVArchive

Guía de seguridad

Versión 7.3

E70867-01

Diciembre de 2015

ORACLE®

Oracle® DIVArchive
Guía de seguridad

E70867-01

Tabla de contenidos

Prefacio 5

Destinatarios 5
Accesibilidad a la documentación 5

1. Visión general 7

1.1. Visión general del producto 7
1.1.1. DIVArchive Manager 7
1.1.2. DIVArchive Actor 7
1.1.3. DIVArchive Robot Manager 7
1.1.4. DIVArchive Backup Service 8
1.1.5. Oracle Avid Connectivity 8
1.1.6. DIVArchive Drop Folder Monitor 8
1.1.7. DIVArchive SNMP 8
1.1.8. DIVArchive SPM 9
1.1.9. DIVArchive Migrate Service 9
1.1.10. DIVArchive VACP 9
1.1.11. DIVArchive Control GUI 9
1.1.12. DIVArchive Configuration Utility 9
1.1.13. DIVArchive Access Gateway 9
1.1.14. DIVArchive Lynx Local delete 10
1.2. Principios generales de seguridad 10
1.2.1. Mantenga el software actualizado 10
1.2.2. Restrinja el acceso de red a los servicios críticos 10
1.2.3. Ejecute el sistema como usuario DIVA y utilice el principio de menor privilegio donde sea posible 10
1.2.4. Supervise la actividad del sistema 11
1.2.5. Manténgase actualizado sobre la información de seguridad más reciente 11

2. Instalación segura 13

2.1. Comprensión del entorno 13
2.1.1. ¿Qué recursos necesitan protección? 13
2.1.1.1. Disco de datos principales 13
2.1.1.2. Disco de base de datos, disco de metadatos y discos de copias de seguridad 13

2.1.1.3. Cintas de DIVArchive 13
2.1.1.4. Metadatos de cintas de exportación 14
2.1.1.5. Archivos y valores de configuración 14
2.1.2. ¿De quién se protegen los recursos? 14
2.1.3. ¿Qué sucede si falla la protección de los recursos estratégicos? 14
2.2. Topologías de despliegue recomendadas 14
2.2.1. Red de metadatos independiente 14
2.2.2. Zonas de canal de fibra 15
2.2.3. Protección del acceso de configuración de los discos SAN 15
2.2.4. Instalación del paquete DIVArchive 15
2.2.5. Seguridad de cintas de DIVArchive 15
2.2.6. Copias de seguridad 15
2.3. Configuración posterior a la instalación 15

3. Funciones de seguridad 17

3.1. El modelo de seguridad 17
3.2. Autenticación 17
3.3. Control de acceso 17

A. Lista de comprobación de despliegue seguro 19

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. 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 7.3 en:

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

1.1.2. 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. DIVArchive Robot Manager

Si bien DIVArchive puede utilizarse solo para gestionar el almacenamiento del disco, se puede expandir la capacidad de almacenamiento al agregar una o más bibliotecas de cintas. En estos casos, el módulo DIVArchive Robot Manager 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. DIVArchive Robot Manager 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. DIVArchive Backup Service

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 DIVArchive Backup Service.

El componente DIVArchive Backup Service 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 instala DIVArchive Manager y Oracle Database. DIVArchive Backup Service permite la configuración de copias de seguridad programadas mediante el archivo de configuración. DIVArchive Backup Service gestiona y supervisa todo el proceso de creación de copias de seguridad.

DIVArchive Backup Service 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 DIVArchive Configuration Utility en el separador Manager Setting (Configuración de Manager).

Para obtener más información sobre cómo instalar y configurar DIVArchive Backup Service, consulte la biblioteca de documentación del cliente del software DIVArchive versión 7.3 en:

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

1.1.5. Oracle Avid Connectivity

El propósito de Avid Connectivity con DIVArchive es transferir datos de archivos desde DIVArchive, y hacia él, en formatos de video específicos, y permitir el almacenamiento 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. DIVArchive Drop Folder Monitor

DIVArchive Drop Folder Monitor (DFM) supervisa automáticamente los archivos creados recientemente hasta en 20 carpetas locales o carpetas de FTP (o sus combinaciones). Se admiten uno o varios archivos (en carpetas de FTP) por objeto de DIVArchive. Cuando se identifica un nuevo archivo (o carpeta de FTP), DFM envía automáticamente una solicitud de almacenamiento a DIVArchive para almacenar el archivo nuevo o las carpetas nuevas. Una vez que los archivos se almacenaron correctamente, se suprimen automáticamente del origen.

1.1.7. DIVArchive SNMP

El protocolo simple de administración de redes de DIVArchive (SNMP) 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.

1.1.8. DIVArchive 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 del 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. DIVArchive Migrate Service

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. DIVArchive VACP

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. DIVArchive Control GUI

DIVArchive Control GUI (interfaz gráfica de usuario) se utiliza para supervisar y controlar las operaciones en DIVArchive. Se pueden ejecutar y conectar varias GUI de DIVArchive en el mismo sistema DIVArchive al mismo tiempo.

1.1.12. DIVArchive Configuration Utility

DIVArchive Configuration Utility se utiliza 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. DIVArchive Access Gateway

Access Gateway permite la operación e 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, el control de ancho de banda y la verificación del total de control. Se supervisan las redes y DIVAnet garantiza la entrega final del contenido.

1.1.14. DIVArchive Lynx Local delete

LYNXLocalDelete es un servicio que supervisa las funciones de replicación de objetos entre un sistema DIVArchive local (por ejemplo, LYNXlocal) y uno (o más) sistemas DIVArchive remotos (por ejemplo, LYNXdr). Una vez que el objeto se replicó correctamente en el sistema DIVArchive remoto, se marca como elegible para ser suprimido 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. Mantenga 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. Restrinja el acceso de red a los servicios críticos

DIVArchive utiliza los siguientes puertos TCP/IP:

- DIVArchive Robot Manager utiliza el puerto tcp/8500
- DIVArchive Manager utiliza el puerto tcp/9000
- DIVArchive Backup Service utiliza el puerto tcp/9300
- DIVArchive Access Gateway utiliza el puerto tcp/9500
- DIVArchive Actor utiliza el puerto tcp/9900
- DIVArchive Migrate Service utiliza el puerto tcp/9191

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

Todos los servicios DIVArchive se ejecutan como usuario DIVA. DIVArchive Control GUI proporciona tres perfiles de usuario fijos (administrador, operador y usuario). Las cuentas de administrador y de operador requieren una contraseña para obtener acceso. El sistema DIVArchive viene instalado con contraseñas por defecto que pueden cambiarse en cualquier momento mediante DIVArchive Configuration Utility. Si no cambia las contraseñas por defecto, el sistema DIVArchive puede ser víctima de actividades maliciosas. **Las contraseñas por defecto deben ser cambiadas inmediatamente después de la instalación y configuración de las cuentas de administrador y de operador, y a partir de ese momento, cada 180 días (como mínimo). Luego de haber realizado 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

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

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 DIVArchive.

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 se 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 cache. En general, son discos locales o remotos conectados a los sistemas DIVArchive. El acceso independiente a estos discos (no por medio de 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 (no por medio de 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. Estos datos y metadatos deben estar protegidos a fin de evitar el acceso que no sea del administrador del sistema operativo 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. 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.

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 canal de fibra 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 del software DIVArchive versión 7.3 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 conmutación 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 DIVArchive desde una WAN externa y desde cualquier host que no sea de confianza en la red. Consulte Sección 1.2.2, “Restrinja 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 independiente para conectar físicamente solo los servidores que necesitan acceso.

2.2.3. Protección del acceso de configuración de los discos SAN

Por lo general, es posible acceder a los discos SAN RAID para fines administrativos mediante TCP/IP o, lo que ocurre más habitualmente, mediante HTTP. Debe proteger los discos del acceso externo; para esto, limite el acceso administrativo a los discos SAN RAID solo a sistemas que estén 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 DIVArchive que necesite. Por ejemplo, si no piensa ejecutar la interfaz gráfica de usuario ni la utilidad de configuración desde un sistema, desactívelas en la lista de componentes que se instalarán. Los permisos y los propietarios de directorio de la instalación por defecto de DIVArchive no se deben cambiar después de la instalación sin tener en cuenta las consecuencias para la seguridad que puedan tener estos cambios.

2.2.5. Seguridad de cintas de DIVArchive

Impida el acceso externo a las cintas DIVArchive dentro de la 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 DIVArchive Backup Service. Limite el acceso al volcado de las copias de seguridad solo a usuarios administradores en el nivel de sistema operativo.

2.3. Configuración posterior a la instalación

Después de instalar cualquier componente DIVArchive, revise la lista de comprobación de seguridad en 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 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.

3.2. Autenticación

DIVArchive Control GUI proporciona tres perfiles de usuario fijos (administrador, operador y usuario). Las cuentas de administrador y de operador requieren una contraseña para obtener acceso. El sistema DIVArchive viene instalado con contraseñas por defecto que pueden cambiarse en cualquier momento mediante DIVArchive Configuration Utility. Si no cambia las contraseñas por defecto, el sistema DIVArchive puede ser víctima de actividades maliciosas. **Es necesario cambiar las contraseñas por defecto inmediatamente después de la instalación y configuración de las cuentas de administrador y de operador, y a partir de ese momento, cada 180 días (como mínimo). Luego de haber realizado el cambio, debe guardar las contraseñas en una ubicación segura, fuera de línea, donde solo pueda acceder el soporte de Oracle, si fuera necesario.**

3.3. Control de acceso

El control de acceso en DIVArchive está dividido en tres perfiles:

Usuario: luego de establecer 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 es posible acceder a todas las funciones para ejecutar comandos en DIVArchive en el modo de perfil de usuario. Esto permite que cuando haya situaciones en las que se requiera supervisión pero no se permita la ejecución de comandos, estas se envíen a DIVArchive.

Administrador: para enviar solicitudes a DIVArchive, como solicitudes de archivos 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 por defecto para este perfil es diva, sin embargo esta puede ser (o puede haber sido) cambiada en la utilidad de configuración. Para obtener más información, consulte la biblioteca de documentación del cliente del software DIVArchive versión 7.3 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 el ingreso de la misma contraseña que el perfil de administrador.

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 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, en cambio, asigne roles según sea necesario a otras cuentas de usuario.
3. Establezca contraseñas seguras para administrador y operador, para la interfaz gráfica de usuario de control. Cambie inmediatamente la contraseña instalada por defecto por una contraseña segura. Puede hacerlo desde la utilidad de configuración en Tools (Herramientas).
4. Establezca una contraseña segura para iniciar sesión en la base de datos de Oracle. Cambie las contraseñas por defecto de los usuarios de la base de datos de Oracle desde los valores por defecto instalados.
5. Instale firewall en todos los sistemas y aplique las reglas por defecto de los puertos 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 el disco gestionado, solo los actores de DIVArchive deben tener acceso a las unidades de disco y también de cinta. Esta práctica de seguridad ayuda a prevenir los accidentes de pérdida de datos en caso de sobrescribir accidentalmente el disco o la cinta.
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 cualquier infracción de seguridad. Su 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.