Oracle® DIVAnet

Guía de seguridad

Versión 2.1

E77643-01

Junio de 2016

ORACLE®

Oracle® DIVAnet
Guía de seguridad

E77643-01

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. Servicio ClientAdapter de DIVAnet 7
1.1.2. Servicio ManagerAdapter de DIVAnet 7
1.1.3. Servicio DbSync de DIVAnet 7
1.1.4. Interfaz de usuario de DIVAnet (DIVAnetUI) 8
1.2. Principios generales de seguridad 8
1.2.1. Cómo mantener el software actualizado 8
1.2.2. Restricción del acceso de red a los servicios críticos 8
1.2.3. Uso del principio de menor privilegio donde sea posible 8
1.2.4. Supervisión de la actividad del sistema 9
1.2.5. Cómo mantenerse actualizado sobre la información de seguridad más reciente 9

2. Instalación segura 11

2.1. Comprensión del entorno 11
2.1.1. ¿Qué recursos necesitan protección? 11
2.1.1.1. Servidores de DIVAnet 11
2.1.1.2. Base de datos 11
2.1.1.3. Medios de archivo, destinos y orígenes de DIVArchive 11
2.1.1.4. Archivos y valores de configuración 12
2.1.2. ¿De quién se protegen los recursos? 12
2.1.3. ¿Qué sucede si falla la protección de los recursos estratégicos? 12
2.2. Tecnologías de despliegue recomendadas 12
2.2.1. Instalación de DIVAnet 12
2.2.2. Conexión a DIVArchive 13
2.2.3. Sistemas de protección de discos 13
2.3. Configuración después de la instalación 13

3. Funciones de seguridad 15

3.1. El modelo de seguridad 15
3.2. Autenticación 15
3.3. Control de acceso 16
3.4. Configuración de **SSL/TLS** 17
3.4.1. Almacén de claves privadas 17
3.4.2. Almacén de claves públicas 17

A. Lista de comprobación de despliegues seguros 19

Prefacio

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

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 ofrece una visión general del producto Oracle DIVAnet 2.1 y se explican los principios generales de la seguridad de aplicaciones.

1.1. Visión general del producto

Oracle DIVAnet proporciona una vista unificada de contenido archivado en varios sistemas Oracle DIVArchive distribuidos. DIVArchive de Oracle es un sistema de gestión escalable de almacenamiento de contenido compatible con el archivo en bibliotecas de cintas y sistemas de disco. DIVAnet facilita el traslado de contenido de un lugar a otro entre los sitios de DIVArchive, y de discos y servidores de origen y de destino del cliente. Realiza sus tareas a los efectos de la recuperación ante desastres, la distribución de contenido, el control de acceso, el rendimiento y la disponibilidad de contenido.

DIVAnet consta de los siguientes componentes principales:

1.1.1. Servicio ClientAdapter de DIVAnet

Los clientes de la aplicación que desean usar la API de DIVArchive o la GUI de DIVAnet, se conectan al **servicio ClientAdapter de DIVAnet**. Este servicio de DIVAnet acepta conexiones web y mediante socket desde las aplicaciones y los procesos que solicita. Se configura un **ClientAdapter** en cada sitio que tiene aplicaciones locales del sitio donde están instalados DIVArchive y DIVAnet.

1.1.2. Servicio ManagerAdapter de DIVAnet

El **servicio ManagerAdapter de DIVAnet** funciona como un puente entre DIVAnet y Oracle DIVArchive Manager. Se debe configurar para proporcionar acceso remoto mediante otros sistemas DIVAnet.

1.1.3. Servicio DbSync de DIVAnet

El **servicio DbSync de DIVAnet** es responsable de sincronizar la información de activos de varios sitios de DIVArchive y de almacenar la información en la base de datos de DIVAnet. **DbSync** se comunica de manera remota con los servicios **ManagerAdapter** en varios sitios para sincronizar información de objetos archivados. **DbSync** se despliega, normalmente, junto con **ClientAdapter**. Los servicios **DbSync** y **ClientAdapter** requieren acceso directo a la base de datos de DIVAnet.

1.1.4. Interfaz de usuario de DIVAnet (DIVAnetUI)

DIVAnetUI es una aplicación de la interfaz gráfica de usuario que le permite al usuario supervisar las solicitudes de DIVAnet, además de ver, copiar y suprimir activos de DIVAnet (objetos archivados de DIVA) en varios sitios de DIVArchive. Todas las solicitudes del nivel de DIVAnet se pueden supervisar, ya sea que se hayan ejecutado por medio de la API o por medio de la IU propiamente dicha. También puede ver información de los activos de todos los sitios configurados de DIVArchive, independientemente de si el activo se archivó por medio de DIVAnet. **DIVAnetUI** proporciona maneras flexibles de consultar sobre la información de solicitudes y activos.

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. Cómo mantener el software actualizado

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

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

1.2.2. Restricción del acceso de red a los servicios críticos

DIVAnet utiliza los siguientes puertos TCP/IP por defecto:

- *`tcp/9801`* es el puerto de **WebService** por defecto que utiliza el servicio **ClientAdapter** de DIVAnet.
- *`tcp/7101`* es el puerto del socket de la API por defecto que utiliza el servicio **ClientAdapter** de DIVAnet (es posible configurar otros puertos).
- *`tcp/9800`* es el puerto de **WebService** por defecto que utiliza el servicio **ManagerAdapter** de DIVAnet.

Nota:

No todos estos puertos se deben exponer externamente; además, se basan en la configuración y el uso.

1.2.3. Uso del principio de menor privilegio donde sea posible

Los servicios de DIVAnet no se deben ejecutar como usuario *`admin`* o *`root`*. La ejecución de los servicios con un usuario diferente del sistema operativo (distinto del usuario que se usa para administrar la aplicación) contribuye a la seguridad general del sistema.

El instalador de DIVAnet Linux requiere dos usuarios para completar la instalación de DIVAnet: un usuario *`diva`* y un usuario del sistema operativo. Los administradores y los

operadores usan la cuenta de *diva* para instalar y supervisar DIVAnet. El usuario del sistema operativo controla los servicios de DIVAnet.

Los firewalls deben restringir los puertos solo a los necesarios. DIVAnet incluye funciones de control de acceso (descritas brevemente en Control de acceso), que se usan para restringir a los usuarios y los sistemas al menor privilegio posible.

1.2.4. Supervisión de la actividad del sistema

Debe supervisar la actividad del sistema para determinar si DIVAnet está funcionando bien y para determinar si está registrando alguna actividad inusual. Consulte los archivos log ubicados en la carpeta *$DIVANET_HOME/Program/log*.

1.2.5. Cómo mantenerse actualizado sobre la información de seguridad más reciente

Para acceder a varias fuentes de información y alertas de seguridad de una gran variedad de productos de software, puede hacer clic en el siguiente enlace:

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 DIVAnet.

2

Capítulo 2. Instalación segura

En este capítulo, se describe el proceso de planificación para una instalación segura y se describen viarias topologías de implementación 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.

Al usar DIVAnet, debe proteger los siguientes recursos:

2.1.1.1. Servidores de DIVAnet

DIVAnet se instala es un servidor conectado a uno o más discos (ya sea un disco local o remoto conectado directamente al sistema DIVAnet). El acceso independiente a estos discos (no por medio de DIVAnet) 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. Base de datos

Se utilizan software de base de datos y recursos de datos para crear sistemas DIVAnet. Los datos, normalmente, se encuentran en discos locales o remotos conectados a los sistemas DIVAnet. El acceso independiente a estos discos (no por medio de DIVAnet) 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. Medios de archivo, destinos y orígenes de DIVArchive

DIVAnet utiliza orígenes y destino de DIVArchive, además de sistemas de archivos DIVA (disco o cinta) mientras responde a sus solicitudes. El acceso independiente injustificado a estos discos de servidor y medio del sistema, que suelen ser controlados por los sistemas

DIVArchive, constituye un riesgo de seguridad. Los **orígenes/destinos** que se utilizan como almacenes de datos temporales para operaciones de copia de DIVAnet deben tener acceso restringido, y usted debe considerar la posibilidad de dedicar estos **orígenes/destinos** únicamente a las operaciones de DIVAnet y de asegurarse que las transferencias estén cifradas o se inicien en una red de confianza.

2.1.1.4. Archivos y valores de configuración

Los valores de configuración de los sistemas DIVAnet 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. 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 sistemas externos no fiables que puedan 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 (supresión errónea de archivos, o escritura en el disco o la cinta más allá de los permisos normales).

2.2. Tecnologías de despliegue recomendadas

En esta sección, se describen la instalación y la configuración de un componente de infraestructura segura.

Para obtener información acerca de la instalación de DIVAnet, consulte la *Guía de instalación, configuración y operaciones de Oracle DIVAnet* en la biblioteca de *Documentación de DIVAnet 2.1*, disponible en:

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

Tenga en cuenta los siguientes puntos cuando instale y configure DIVAnet.

2.2.1. Instalación de DIVAnet

Debe instalar solo los componentes de DIVAnet que necesita. Por ejemplo, si planifica ejecutar solamente **DIVAnetUI** desde una computadora cliente, anule la selección de

DIVAnet Services (Servicios de DIVAnet) de la lista de componentes que se deben instalar durante la instalación. Los permisos y los propietarios del directorio de instalación por defecto de DIVAnet no se deben cambiar después de la instalación sin tener en cuenta las consecuencias para la seguridad que puedan tener estos cambios.

2.2.2. Conexión a DIVArchive

Oracle recomienda la instalación del componente **ManagerAdapter** en el sistema DIVArchive Manager para una mayor seguridad del sistema. Si no se requiere acceso externo al puerto de DIVArchive Manager, se recomienda bloquear el puerto con software de firewall. Además, a menudo no será necesario permitir el acceso de redes externas al puerto del **DIVAnet DbSync WebService** (Servicio web DbSync de DIVAnet).

Si se conecta a una instancia remota de DIVArchive mediante una WAN, asegúrese de conectarse por medio de una red de confianza. También considere la posibilidad de conectarse al sitio mediante *SSL/TLS* al puerto **ManagerAdapter** del sitio remoto.

2.2.3. Sistemas de protección de discos

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

Por lo general, se puede acceder a los discos SAN RAID por motivos administrativos mediante TCP/IP o, con mayor frecuencia, mediante HTTP. Debe proteger los discos de acceso externo; para esto, limite el acceso administrativo a los discos SAN RAID solo a sistemas que se encuentran dentro de un dominio de confianza. Además, cambie la contraseña por defecto en las matrices de disco.

2.3. Configuración después de la instalación

Después de instalar cualquier parte de DIVAnet, revise la lista de comprobación de seguridad en el Apéndice A, *Lista de comprobación de despliegues seguros*.

3

Capítulo 3. Funciones de seguridad

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

Estas amenazas de seguridad se pueden minimizar con una configuración apropiada y siguiendo la lista de comprobación posterior a la instalación, disponible en el Apéndice A, *Lista de comprobación de despliegues seguros*.

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 tendrán acceso al sistema y a los datos.
- **Autorización:** control de acceso a privilegios y datos del sistema. Esta característica se basa en la autenticación para garantizar que las personas solo obtengan el nivel de acceso adecuado.

3.2. Autenticación

Los servicios de DIVAnet pueden realizar la autenticación mediante varios métodos:

- **Certificados SSL/TLS:** DIVAnet consulta a un almacén de confianza de certificados cuando crea una conexión saliente a un servicio remoto de DIVAnet. Esto permite asegurarse de que DIVAnet se está conectando a servicios de DIVAnet auténticos. Para crear una conexión segura desde el servicio **ClientAdapter** de DIVAnet a una instancia de DIVArchive, debe conectarse mediante el servicio **ManagerAdapter** con un `ConnectionType` identificado como **WebServices**.
- **Reglas de acceso:** si bien técnicamente constituyen una forma de control de acceso, las reglas de acceso pueden filtrar conexiones entrantes en función de la dirección IP entrante. Esta característica es necesaria para asegurarse de que solo los sistemas aprobados tengan el acceso correspondiente a los servicios de DIVAnet.

ADVERTENCIA:

Los servicios de DIVAnet utilizan contraseñas de base de datos como parte de su configuración. Las contraseñas se deben cambiar de inmediato después de la instalación y cada 180 días (como mínimo) posteriormente. 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.

3.3. Control de acceso

Se pueden crear reglas de acceso para limitar las operaciones que determinados usuarios o sistemas pueden realizar en el sistema de archivos distribuidos. Las reglas de acceso se pueden ejecutar de las siguientes maneras:

- **Modo ClientAdapter/MultiDiva:** restringe los tipos de solicitudes de DIVAnet que se pueden ejecutar.
- **ManagerAdapter:** restringe los tipos de solicitudes de DIVArchive que se pueden ejecutar para satisfacer una solicitud de DIVAnet (posiblemente solicitada por un sistema remoto).

Las reglas de acceso pueden afectar las solicitudes iniciadas desde **DIVAnetUI** o desde una conexión de socket de la API (posiblemente iniciada por un sistema de automatización o un sistema de gestión de activos de medios).

Las reglas de acceso se pueden ejecutar en una solicitud de DIVAnet, en el nivel de DIVAnet o DIVArchive. En el nivel de DIVAnet, el servicio **ClientAdapter** procesa la solicitud donde esta se recibió. En el nivel de DIVArchive, un servicio **ManagerAdapter** remoto procesa las solicitudes de DIVArchive ejecutadas para satisfacer la solicitud de DIVAnet.

Oracle recomienda crear el juego de reglas más restrictivo que cumpla con los requisitos de su aplicación. Por ejemplo, si solo los administradores deben realizar supresiones globales, asegúrese de que a los demás usuarios se les niegue el acceso a esa funcionalidad. Si un grupo de usuarios del sistema solo necesita acceso a una lista limitada de orígenes y destinos, asegúrese de que esos usuarios solo puedan ejecutar solicitudes relacionadas con dichos orígenes y destinos específicos.

También tenga en cuenta los sitios utilizados para satisfacer las solicitudes. Por ejemplo, si los usuarios del sitio local no tienen motivo para realizar copias en los casos en que los sitios de origen o destino no constituyen el sitio local (esto es posible cuando se usa DIVAnet), configure estas reglas en la configuración del servicio **ClientAdapter**.

Finalmente, tenga en cuenta las construcciones específicas de las solicitudes que desee excluir por completo. Por ejemplo, si no necesita objetos de dirección que tengan solo un nombre de objeto (sin la categoría), excluya todas las solicitudes que tengan categorías en blanco.

Asimismo, cada WorkflowProfile de ClientAdapter contiene la lista de mensajes válidos que pueden ser procesados por solicitudes asignadas al WorkflowProfile. En el **modo MultiDiva**, esto ofrece una manera de excluir mensajes específicos del procesamiento (incluidos los mensajes informativos).

Oracle recomienda comenzar con las reglas por defecto definidas en el archivo `AccessRules.xml.ini`, aunque no defina sus propias reglas de acceso. Para obtener más información sobre las funciones de control de acceso de DIVAnet, consulte la *Guía de instalación, configuración y operaciones de Oracle DIVAnet*, disponible en:

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

3.4. Configuración de SSL/TLS

DIVAnet contiene datos de certificados en dos lugares: un *almacén de claves privadas*, que se utiliza para los servicios web alojados en el sistema local, y un *almacén de claves públicas*, que se utiliza para verificar los servicios web que se invocan de manera remota. Puede usar la **utilidad de herramienta de claves de Java** para cambiar la contraseña del almacén de claves, y agregar y suprimir certificados.

Consulte lo siguiente para obtener más información sobre cómo crear almacenes de claves:

http://docs.oracle.com/javase/8/docs/technotes/guides/security/jsse/JSSERefGuide.html#CreateKeystore

Solo las conexiones a los servicios web de DIVAnet utilizan *SSL/TLS*. En esta versión, la conexión a DIVArchive o DIVAnet mediante una conexión de socket de la API de DIVArchive no usa *SSL/TLS*.

3.4.1. Almacén de claves privadas

Los datos del certificado de clave privada de DIVAnet se almacenan en:

$DIVANET_HOME/Program/divanet/lib/diva129.jks

Debe aparecer exactamente un certificado en este almacén de claves. Este certificado se usa para servicios web alojados por servicios que se ejecutan desde este directorio de *$DIVANET_HOME*. Se recomienda sustituir el certificado enviado por un nuevo certificado y usar un certificado distinto para cada sitio de DIVAnet de la red.

Debe cambiar la contraseña de este almacén de claves. Almacene la información de la contraseña en un nuevo archivo con el nombre *$DIVANET_HOME/Program/divanet/lib/diva129.properties* y otorgue acceso de lectura a los servicios de DIVAnet (en Linux, este usuario es *divanetsvc*), pero no otorgue acceso a usuarios casuales del sistema (por ejemplo, el usuario *diva* en Linux). Use el siguiente formato para el archivo:

keystorePassword=newpassword

3.4.2. Almacén de claves públicas

Los datos de este almacén que, en ocasiones, se denomina *almacén de confianza*, se encuentran en:

$DIVANET_HOME/Java/lib/security/cacerts2

Los datos de este certificado se usan en llamadas salientes del servicio web (incluidas las llamadas de **DIVAnetUI**). Se pueden cargar varias claves públicas en este almacén de claves.

Si agregó un nuevo certificado autofirmado al almacén de claves privadas de DIVAnet, exporte el certificado mediante la utilidad de herramienta de claves. Todas las aplicaciones (servicios de DIVAnet, DIVAnetUI, etc.) que llaman a **WebServices** (Servicios web) en este sitio deben agregar el certificado exportado a su propio almacén de claves públicas.

Apéndice A

Apéndice A. Lista de comprobación de despliegues seguros

1. Establezca contraseñas seguras para la cuenta de administrador y cualquier otra cuenta del sistema operativo que tenga roles de servicio o administrador de DIVAnet asignados. Esto incluye:
   - *`diva`*, *`divanetsvc`* y los ID de usuario de Oracle, si se usan
   - Cualquier cuenta administrativa 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. Utilice certificados específicos del sitio para cada instalación de DIVAnet y defina una contraseña segura para el almacén de claves privadas y la base de datos de Oracle. Establezca una contraseña segura para iniciar sesión en el sistema operativo de la base de datos de Oracle.
4. Instale software de firewall en todos los sistemas DIVAnet y aplique las reglas por defecto de los puertos DIVAnet. Restrinja el acceso al socket de la API de DIVAnet (*`tcp 7101`*) para las direcciones IP que requieren acceso por medio de las reglas de firewall. Realice este paso mediante las reglas de acceso de DIVAnet.
5. Instale actualizaciones del sistema operativo y de DIVAnet 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.
7. Las mejores prácticas indican que debe 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. Esta práctica de seguridad ayuda a evitar los accidentes de pérdida de datos debido a la sobrescritura accidental de datos importantes.
8. Configure un juego apropiado de copias de seguridad para la base de datos y la configuración de DIVAnet. 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 los discos de DIVAnet.