Oracle® DIVArchive

Guia de Segurança

Release 7.4

E77633-01

Junho de 2016

ORACLE®

Oracle® DIVArchive
Guia de Segurança

E77633-01

Índice

Prefácio

O Guia de Segurança do Oracle DIVArchive inclui informações sobre o produto DIVArchive e explica os princípios gerais de segurança do aplicativo.

Público-alvo

Este guia destina-se a todos os envolvidos com o uso dos recursos de segurança e da instalação e configuração seguras do DIVArchive.

Acessibilidade da Documentação

Para obter informações sobre o comprometimento da Oracle com a acessibilidade, visite o site do Oracle Accessibility Program em http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Acesso ao Oracle Support
Os clientes da Oracle que adquiriram serviços de suporte têm acesso a suporte eletrônico por meio do My Oracle Support. Para obter informações, visite http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info ou http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs se você for portador de deficiência auditiva.

1

Capítulo 1. Visão Geral

Este capítulo fornece uma visão geral do produto DIVArchive e explica os princípios gerais de segurança do aplicativo.

1.1. Visão Geral do Produto

O Oracle DIVArchive é um sistema de gerenciamento de armazenamento de conteúdo distribuído. O DIVArchive consiste nos seguintes componentes principais:

1.1.1. Oracle DIVArchive Manager

O DIVArchive Manager é o principal componente de um DIVArchive System. Todas as operações de arquivamento são controladas e tratadas pelo DIVArchive Manager. As solicitações de operação são enviadas pelos aplicativos iniciadores por meio da API de Cliente do DIVArchive. Por ser uma opção que pode ser comprada, o DIVArchive também suporta o DIVArchive Manager Principal e o DIVArchive Manager para Backup. Para obter mais informações sobre o DIVArchive, consulte a Biblioteca de Documentação do Cliente do DIVArchive Software Release 7.4 em:

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

1.1.2. Oracle DIVArchive Actor

O DIVArchive Actor é o movimentador de dados entre dispositivos no sistema de produção. Ele suporta a transferência de dados entre muitos diferentes tipos de dispositivos e trata as operações de Transcodificação com um Software de Transcodificação Telestream (opcional).

Todas as operações do Actor são iniciadas e coordenadas pelo DIVArchive Manager. Um único DIVArchive Manager pode configurar e controlar um ou mais Actors.

1.1.3. DIVArchive Robot Manager

Apesar de o DIVArchive poder ser usado apenas para gerenciar o armazenamento em disco, a capacidade de armazenamento pode ser expandida por meio da adição de uma ou mais bibliotecas de fitas. Nesses casos, o módulo DIVArchive Robot Manager fornece uma camada de software intermediária para o DIVArchive Manager interagir com muitos diferentes tipos de bibliotecas de fitas. É conectado com o DIVArchive Manager por meio de TCP/IP. O

DIVArchive Robot Manager interage com a biblioteca usando uma interface direta com a própria biblioteca (por meio de SCSI nativa ou SCSI sobre Fibre Channel) ou por meio de uma conexão de Ethernet intermediária com o software de controle de biblioteca do próprio fabricante.

1.1.4. DIVArchive Backup Service

O DIVArchive Backup Service foi lançado para garantir a confiabilidade e o monitoramento dos backups do Banco de Dados Oracle e do Banco de Dados de Metadados.

O componente DIVArchive Backup Service é instalado como parte integrante da instalação do DIVArchive System padrão. Normalmente, o componente é instalado no mesmo servidor que o DIVArchive Manager e o Banco de Dados Oracle. O DIVArchive Backup Service permite a configuração de backups agendados por meio de um arquivo de configuração. O DIVArchive Backup Service gerencia e monitora o processo de backup como um todo.

O DIVArchive Backup Service agora incorpora a capacidade de enviar e-mails sobre problemas ocorridos durante o processo de backup dos arquivos do Banco de Dados e do Banco de Dados de Metadados. Para se beneficiar dessa funcionalidade, o DIVArchive deverá ser configurado para conexão com um provedor de e-mail SMTP. As notificações de e-mail são configuradas por meio do Utilitário de Configuração do DIVArchive, na Guia Definição do Gerenciador.

Para obter informações sobre a instalação e a configuração do DIVArchive Backup Service, consulte a Biblioteca de Documentação do Cliente do DIVArchive Software Release 7.4 em:

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

1.1.5. Oracle DIVArchive Avid Connectivity

O objetivo do Avid Connectivity com o DIVArchive é transferir e receber dados de arquivamento DIVArchive em formatos de vídeo específicos e permitir o arquivamento e a recuperação de clipes únicos ou de uma sequência de clipes. Os componentes relacionados ao AMC e ao TMC são instalados juntamente com a instalação principal do DIVArchive. São necessárias informações adicionais para determinados plug-ins tanto em relação ao AMC quanto ao TMC.

1.1.6. DIVArchive DFM (Drop Folder Monitor)

O DIVArchive DFM (Drop Folder Monitor) fornece monitoramento automático para arquivos recém-criados em até 20 pastas locais ou de FTP (ou combinações das duas opções). São suportados um arquivo ou vários arquivos (em pastas de FTP) por Objeto do DIVArchive. Quando um novo arquivo (ou pasta de FTP) é identificado, o DFM emite uma solicitação de arquivamento automaticamente para que o DIVArchive arquive o novo arquivo ou as novas pastas de FTP. Assim que forem arquivados com sucesso, os arquivos ou pastas serão automaticamente excluídos da origem.

1.1.7. DIVArchive SNMP

O Agente DIVArchive Simple Network Management Protocol (SNMP) e a Management Information Base (MIB) suportam o monitoramento do status e da atividade do DIVArchive e de seus subsistemas por meio de um aplicativo de monitoramento de terceiros utilizando o protocolo SNMP. O DIVArchive SNMP só é suportado em ambientes Windows.

1.1.8. DIVArchive SPM (Storage Plan Manager)

O DIVArchive SPM (Storage Plan Manager) fornece migração automática e controle do ciclo de vida útil do material dentro do arquivo compactado com base nas regras e nas políticas definidas na configuração do SPM.

O componente SPM também é usado para disparar a exclusão de material dos arrays gerenciados do SPM (com base nos limites de espaço em disco).

1.1.9. DIVArchive Migrate Service

O DIVArchive inclui um serviço de migração embutido. Trata-se de um novo serviço interno e separado (do DIVArchive) que ajuda os usuários a agendar e executar jobs para migrar o conteúdo entre diferentes mídias dentro do DIVArchive System. Você pode usar o Control Gui ou o cliente de linha de comando.

1.1.10. DIVArchive VACP

O VACP (Video Archive Command Protocol) é um protocolo desenvolvido pela Harris Automation para estabelecer uma interface com um Sistema de Arquivamento. O DIVArchive tem sua própria API para comunicação com o DIVArchive Manager que, por sua vez, não é compatível com o VACP.

1.1.11. DIVArchive Control GUI

Você utiliza o DIVArchive Control GUI (Graphical User Interface) para monitorar, controlar e supervisionar operações no DIVArchive. Diversas GUIs do DIVArchive podem ser executadas e conectadas com o mesmo DIVArchive System ao mesmo tempo.

1.1.12. Utilitário de Configuração do DIVArchive

Você usa o Utilitário de Configuração do DIVArchive para configurar um DIVArchive System. Apesar de ser usado principalmente para configurar o DIVArchive, o Utilitário de Configuração também pode ser usado para executar algumas funções operacionais.

1.1.13. DIVArchive Access Gateway

O Access Gateway permite a operação e a interação de vários DIVArchive Systems independentes com base em um único computador. Ele é a solução global para a distribuição

de conteúdo. Uma replicação automatizada de arquivos que espelha instalações fornece um método simples e fácil para distribuição local, backup e recuperação de desastres com segurança, controle de largura de banda e verificação de checksum. As redes são monitoradas, e a DIVAnet garante a entrega final do conteúdo.

1.1.14. DIVArchive Local Delete

O Local Delete é um serviço que monitora funções entre um DIVArchive System local (por exemplo, DIVAlocal) e um (ou mais) DIVArchive Systems remotos (por exemplo, DIVAdr). Assim que o objeto tiver sido replicado com sucesso para o DIVArchive System remoto, ele será marcado como elegível para exclusão do DIVArchive System local.

1.2. Princípios Gerais de Segurança

As seções a seguir descrevem os princípios fundamentais exigidos para usar qualquer aplicativo de modo seguro.

1.2.1. Mantenha o Software Atualizado

Mantenha-se atualizado com a versão do DIVArchive executada no seu sistema. É possível localizar as versões atuais do software para download no Oracle Software Delivery Cloud:

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

1.2.2. Restrinja o Acesso à Rede aos Serviços Críticos

O DIVArchive usa as seguintes portas TCP/IP:

- O DIVArchive Robot Manager usa *`tcp/8500`*
- O DIVArchive Manager usa tcp/9000
- O DIVArchive Backup Service usa tcp/9300
- O DIVArchive Access Gateway usa tcp/9500
- O DIVArchive Actor usa *`tcp/9900`*
- O DIVArchive Migrate Service usa tcp/9191

1.2.3. Execute o sistema como um Usuário DIVA e utilize o Privilégio Mínimo sempre que Possível

Não execute os serviços do DIVArchive usando uma conta de usuário do sistema operacional para Administrador (ou Root). Você sempre deverá executar todos os serviços do DIVArchive usando um usuário (ou grupo) denominado DIVA, que é dedicado ao sistema operacional.

O DIVArchive Control GUI fornece três perfis de usuário fixos (Administrador, Operador e Usuário). As contas de Administrador e Operador exigem uma senha para que o acesso seja

concedido. Você deverá designar uma senha de Administrador e (ou) uma senha de Operador no Utilitário de Configuração antes de usar esses perfis.

Você cria senhas durante a instalação e a configuração das contas de Administrador e Operador. Daí em diante, as senhas deverão ser alteradas a cada 180 dias (no mínimo). Se necessário, as senhas deverão ser disponibilizadas para o Oracle Support.

1.2.4. Monitore a Atividade do Sistema

Monitore a atividade do sistema para determinar a eficiência da operação do DIVArchive e se ele está registrando alguma atividade fora do normal. Verifique os arquivos de log localizados no diretório de instalação sob */Program/log/*.

1.2.5. Mantenha-se Atualizado com as Informações Mais Recentes sobre Segurança

É possível acessar várias fontes de informações de segurança. Para obter informações e alertas de segurança para uma grande variedade de produtos de software, consulte:

http://www.us-cert.gov

A principal maneira de se manter atualizado sobre os problemas de segurança é executar a versão mais recente do software DIVArchive.

2

Capítulo 2. Instalação Segura

Este capítulo destaca o processo de planejamento para uma instalação segura e descreve várias topologias de implantação recomendadas para os sistemas.

2.1. Compreenda o Seu Ambiente

Para compreender melhor as suas necessidades de segurança, as seguintes perguntas devem ser feitas:

2.1.1. Quais recursos precisam ser protegidos?

É possível proteger muitos dos recursos no ambiente de produção. Considere o tipo dos recursos que deseja proteger ao determinar o nível de segurança a ser oferecido.

Ao usar o DIVArchive, proteja os seguintes recursos:

2.1.1.1. Disco de Dados Principais

Para construir DIVArchive Systems, são utilizados os recursos de Disco de Dados e de Disco de Cache. Em geral, há discos locais ou remotos conectados com os DIVArchive Systems. O acesso independente (não realizado por meio do DIVArchive) a esses discos representa um risco de segurança. Esse tipo de acesso externo pode ser feito por meio de um sistema fraudulento que leia ou grave dados nesses discos ou por meio de um sistema interno que acidentalmente permita acesso a esses dispositivos de disco.

2.1.1.2. Disco de Banco de Dados, Disco de Metadados e Discos de Backup

Para construir DIVArchive Systems com objetos complexos, são utilizados os recursos Disco de Banco de Dados, Disco de Metadados e Disco de Backup. Em geral, há discos locais ou remotos conectados com os DIVArchive Systems. O acesso independente (não realizado por meio do DIVArchive) a esses discos representa um risco de segurança. Esse tipo de acesso externo pode ser feito por meio de um sistema fraudulento que leia ou grave dados nesses discos ou por meio de um sistema interno que acidentalmente permita acesso a esses dispositivos de disco.

2.1.1.3. Fitas do DIVArchive

É um risco de segurança permitir o acesso independente a fitas, em geral, em uma biblioteca de fitas controlada por DIVArchive Systems, onde os dados são gravados.

2.1.1.4. Metadados de Fita de Exportação

Os dumps de Metadados de Fita criados com base em uma operação de exportação contêm dados e metadados. Essas permissões de dados e de metadados deverão ser restritas apenas à conta de Administrador (ou Root) do sistema operacional ou ao usuário (ou grupo) DIVA do sistema operacional durante uma atividade de importação ou de exportação de rotina.

2.1.1.5. Definições e Arquivos de Configuração

As definições de configuração do DIVArchive System devem ser protegidas em relação a usuários não administradores no nível do sistema operacional. Tornar os arquivos de configuração graváveis para usuários não administrativos do sistema operacional representa um risco de segurança. Portanto, essas permissões de arquivos deverão ser restritas apenas à conta de Administrador (ou Root) do sistema operacional ou ao usuário (ou grupo) DIVA do sistema operacional.

2.1.2. Contra quem os recursos estão sendo protegidos?

Em geral, os recursos descritos na seção anterior devem ser protegidos contra todos os acessos que não sejam root ou administrativos em um sistema configurado ou contra um sistema externo fraudulento que possa acessar esses recursos por meio da malha WAN ou FC.

2.1.3. O que acontecerá se as proteções dos recursos estratégicos falharem?

As falhas de proteção nos recursos estratégicos podem variar de acesso inadequado (ou seja, acesso a dados fora de operações normais do DIVArchive) a corrupção de dados (gravação em disco ou fita fora das permissões normais).

2.2. Topologias de Implantação Recomendadas

Esta seção descreve como instalar e configurar um componente de infraestrutura de forma segura. Para obter informações sobre a instalação do DIVArchive, consulte a Biblioteca de Documentação do Cliente do DIVArchive Software Release 7.4 em:

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

Considere os seguintes pontos ao instalar e configurar o DIVArchive:

2.2.1. Rede de Metadados Separada

Para conectar os componentes de serviços do DIVArchive entre si, estabelecer conexão com o Banco de Dados de Metadados e estabelecer conexão a partir de seus clientes, forneça uma rede TCP/IP separada e alterne os componentes de hardware não conectados com nenhuma WAN. Como o tráfego de metadados é implementado usando o TCP/IP, um ataque externo nesse tráfego é teoricamente possível. A configuração de uma rede de metadados separada mitiga esse risco e também fornece um desempenho melhor. Se uma rede de metadados separada for inviável, pelo menos negue o tráfego às portas do DIVArchive por meio da WAN externa e de qualquer host não confiável na rede. Consulte Restrinja o Acesso à Rede aos Serviços Críticos.

2.2.2. Zoneamento FC

Utilize o zoneamento FC para negar acesso aos discos do DIVArchive conectados por meio de canal de fibra em relação a qualquer servidor que não exija acesso aos discos. De preferência, use um switch FC separado para estabelecer conexão física apenas com os servidores que necessitam de acesso.

2.2.3. Acesso de Configuração aos Discos de Proteção SAN

Em geral, os discos SAN RAID podem ser acessados para fins administrativos por meio de TCP/IP ou, com mais frequência, por HTTP. Você deve proteger os discos do acesso externo limitando o acesso administrativo aos discos SAN RAID somente a sistemas que estejam dentro de um domínio confiável. Além disso, altere a senha padrão nos arrays de discos.

2.2.4. Instale o Pacote do DIVArchive

Primeiro, instale os serviços do DIVArchive de que necessita. Por exemplo, caso você não planeje executar a GUI ou o Utilitário de Configuração em um sistema, desmarque-os na lista de componentes a serem instalados durante a instalação. Os proprietários e as permissões padrão do diretório de instalação do DIVArchive devem ser restritos apenas à conta de Administrador (ou Root) do sistema operacional ou ao usuário (ou grupo) DIVA do sistema operacional.

2.2.5. Segurança de Fita do DIVArchive

Impeça o acesso externo a fitas do DIVArchive contidas em uma biblioteca de Fitas controlada pelo DIVArchive System. O acesso não autorizado às fitas do DIVArchive pode comprometer ou destruir dados do usuário.

2.2.6. Backups

Configure e execute backups de banco de dados usando o DIVArchive Backup Service. Permissões para o dump de Backup deverão ser restritas apenas à conta de Administrador (ou Root) do sistema operacional ou ao usuário (ou grupo) DIVA do sistema operacional.

2.3. Configuração Pós-Instalação

Após a instalação do DIVArchive, consulte a lista de verificação de segurança em Apêndice A, *Lista de Verificação para uma Implantação Segura*.

3

Capítulo 3. Funcionalidades de Segurança

Para evitar possíveis ameaças de segurança, os clientes que utilizam o DIVArchive deverão estar muito atentos a questões de autenticação e autorização do sistema.

Essas ameaças de segurança podem ser minimizadas pela configuração adequada e seguindo a lista de verificação de pós-instalação no Apêndice A, *Lista de Verificação para uma Implantação Segura*.

3.1. O Modelo de Segurança

As funcionalidades de segurança críticas que fornecem proteção contra ameaças de segurança são:

- Autenticação - Permite que apenas indivíduos autorizados recebam acesso ao sistema e aos dados.
- Autorização - Controle de acesso a privilégios e dados do sistema. Esta funcionalidade se baseia na autenticação para garantir que os indivíduos obtenham apenas o acesso adequado.

3.2. Autenticação

O DIVArchive Control GUI fornece três perfis de usuário fixos (Administrador, Operador e Usuário). As contas de Administrador e Operador exigem uma senha para que o acesso seja concedido. Você deverá designar uma senha de Administrador e (ou) uma senha de Operador no Utilitário de Configuração antes de usar esses perfis.

As senhas das contas de Administrador e Operador deverão ser alteradas a cada 180 dias (ou antes). Se necessário, as senhas deverão ser disponibilizadas para o Oracle Support.

3.3. Controle de Acesso

O controle de acesso no DIVArchive é dividido em três perfis. As contas de Administrador e Operador exigem uma senha para que o acesso seja concedido. Você deverá designar uma senha de conta de Administrador e (ou) de Operador no Utilitário de Configuração antes de usar esses perfis.

Usuário - Depois que a conexão com o DIVArchive Manager for estabelecida, o Control GUI permitirá que o usuário apenas monitore operações do DIVArchive e recupere dados do banco

de dados. Este verbo é usado para modificar o Perfil de Usuário. Nem todas as funções que emitem comandos para o DIVArchive estão acessíveis no modo de perfil Usuário, o que é adequado para situações em que o monitoramento é necessário, mas não há permissão para enviar comandos ao DIVArchive.

Administrador - Para emitir solicitações ao DIVArchive, como solicitações de arquivamento ou de restauração, ou para ejetar uma fita de uma biblioteca, você deverá usar o Perfil de Administrador. O Perfil do Administrador é protegido por senha. A senha desse perfil deverá ser designada no Utilitário de Configuração antes de o perfil ser utilizado. Para obter mais informações, consulte a Biblioteca de Documentação do Cliente do Oracle DIVArchive 7.4 em:

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

Operador - Além das permissões do Perfil de Usuário, o perfil de operador permite acesso ao Utilitário de Transferência de Objetos e requer que uma senha seja configurada no Utilitário de Configuração antes de o perfil ser utilizado.

Apêndice A

Apêndice A. Lista de Verificação para uma Implantação Segura

1. Defina senhas fortes para o Administrador (ou Root) e para quaisquer outras contas do sistema operacional que tenham atribuições de serviço ou de administrador do DIVArchive designadas a elas, incluindo:
   - DIVA, IDs de Usuário Oracle (se estiverem sendo usados)
   - Quaisquer contas administrativas do array de discos
2. Não utilize uma conta de administrador local do sistema operacional. Conforme necessário, designe atribuições a outras contas de usuários.
3. Defina uma senha forte para o Administrador e o Operador do Control GUI. Você deverá designar uma senha a esses perfis no Utilitário de Configuração antes de usá-los.
4. Defina uma senha forte para o log-in no banco de dados Oracle.
5. Instale um firewall em todos os sistemas e aplique as regras de porta padrão do DIVArchive. Utilizando as regras de firewall, restrinja o acesso à API do DIVArchive (*tcp/9000*) apenas aos IPs que realmente necessitam desse acesso.
6. Instale atualizações do sistema operacional e do DIVArchive em uma base periódica, pois elas incluem atualizações de segurança.
7. Instale o Antivírus e exclua os processos do DIVArchive e de armazenamento (por motivos de desempenho).
8. É uma prática recomendada segregar discos FC e unidades de fita FC fisicamente ou por meio do Zoneamento FC. Isso impede que os discos e dispositivos de fita compartilhem a mesma porta HBA. Para Discos gerenciados, somente DIVArchive Actors deverão ter acesso ao disco e também às unidades de fita. Esta prática de segurança ajuda a impedir a perda de dados resultante da sobregravação acidental da fita ou do disco.
9. Configure um conjunto de backups apropriado para o DIVArchive e o banco de dados. Os backups fazem parte da segurança e fornecem uma maneira de restaurar dados perdidos acidentalmente ou por meio de alguma falha. O backup deverá incluir alguma política enquanto estiver sendo transportado para um local externo. Backups devem ser protegidos da mesma forma que as fitas e os discos do DIVArchive.