Oracle® DIVAdirector

Guia de Segurança

Release 5.3

E71135-01

Dezembro de 2015

Oracle® DIVAdirector

Guia de Segurança

E71135-01

Copyright © 2015, Oracle e/ou suas empresas afiliadas. Todos os direitos reservados.

Este programa de computador e sua documentação são fornecidos sob um contrato de licença que contém restrições sobre seu uso e divulgação, sendo também protegidos pela legislação de propriedade intelectual. Exceto em situações expressamente permitidas no contrato de licença ou por lei, não é permitido usar, reproduzir, traduzir, divulgar, modificar, licenciar, transmitir, distribuir, expor, executar, publicar ou exibir qualquer parte deste programa de computador e de sua documentação, de qualquer forma ou através de qualquer meio. Não é permitida a engenharia reversa, a desmontagem ou a descompilação deste programa de computador, exceto se exigido por lei para obter interoperabilidade.

As informações contidas neste documento estão sujeitas a alteração sem aviso prévio. A Oracle Corporation não garante que tais informações estejam isentas de erros. Se você encontrar algum erro, por favor, envie-nos uma descrição de tal problema por escrito.

Se este programa de computador, ou sua documentação, for entregue/distribuído(a) ao Governo dos Estados Unidos ou a qualquer outra parte que licencie os Programas em nome daquele Governo, a seguinte nota será aplicável:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Este programa de computador foi desenvolvido para uso em diversas aplicações de gerenciamento de informações. Ele não foi desenvolvido nem projetado para uso em aplicações inerentemente perigosas, incluindo aquelas que possam criar risco de lesões físicas. Se utilizar este programa em aplicações perigosas, você será responsável por tomar todas e quaisquer medidas apropriadas em termos de segurança, backup e redundância para garantir o uso seguro de tais programas de computador. A Oracle Corporation e suas afiliadas se isentam de qualquer responsabilidade por quaisquer danos causados pela utilização deste programa de computador em aplicações perigosas.

Oracle e Java são marcas comerciais registradas da Oracle Corporation e/ou de suas empresas afiliadas. Outros nomes podem ser marcas comerciais de seus respectivos proprietários.

Intel e Intel Xeon são marcas comerciais ou marcas comerciais registradas da Intel Corporation. Todas as marcas comerciais da SPARC são usadas sob licença e são marcas comerciais registradas da SPARC International, Inc. AMD, Opteron, a logomarca da AMD e a logomarca da AMD Opteron são marcas comerciais ou marcas comerciais registradas da Advanced Micro Devices. UNIX é uma marca comercial registrada do The Open Group.

Este programa ou hardware e sua documentação podem oferecer acesso ou informações relativas a conteúdos, produtos e serviços de terceiros. A Oracle Corporation e suas empresas afiliadas não fornecem quaisquer garantias relacionadas a conteúdos, produtos e serviços de terceiros e estão isentas de quaisquer responsabilidades associadas a eles, a menos que isso tenha sido estabelecido entre você e a Oracle em um contrato vigente. A Oracle Corporation e suas empresas afiliadas não são responsáveis por quaisquer tipos de perdas, despesas ou danos incorridos em consequência do acesso ou da utilização de conteúdos, produtos ou serviços de terceiros, a menos que isso tenha sido estabelecido entre você e a Oracle em um contrato vigente.

Índice

Prefácio	5
Público-alvo	5
Acessibilidade da Documentação	5
1. Visão Geral	7
1.1. Visão Geral do Produto	7
1.1.1. DIVAdirector Server	7
1.1.2. DIVAdirector Web	7
1.1.3. DIVAdirector Database	7
1.1.4. DIVAdirector Transcoder Service	7
1.1.5. DIVAdirector Task Manager Service	8
1.1.6. DIVAdirector API Service	8
1.2. Princípios Gerais de Segurança	8
1.2.1. Mantenha o Software Atualizado	8
1.2.2. Restrinja o Acesso à Rede aos Serviços Críticos	8
1.2.3. Execute o sistema como usuário ADMIN e utilize o Princípio do Privilégio Mínimo sempre que Possível	8
1.2.4. Monitore a Atividade do Sistema	9
1.2.5. Mantenha-se Atualizado com as Informações Mais Recentes sobre Segurança	9
2. Instalação Segura	11
2.1. Compreenda o Seu Ambiente	11
2.1.1. Quais recursos precisam ser protegidos?	11
2.1.1.1. Disco de Dados Principais	11
2.1.1.2. Disco do Banco de Dados e Discos de Backup	11
2.1.1.3. Definições e Arquivos de Configuração	11
2.1.2. Contra quem os recursos estão sendo protegidos?	12
2.1.3. O que acontecerá se as proteções dos recursos estratégicos falharem?	12
3. Funcionalidades de Segurança	13
3.1. O Modelo de Segurança	13
A. Lista de Verificação para uma Implantação Segura	15

Prefácio

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

Público-alvo

Este guia destina-se a todos os envolvidos na utilização das funcionalidades de segurança e na instalação e configuração seguras do DIVAdirector.

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.

Capítulo 1. Visão Geral

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

1.1. Visão Geral do Produto

O Oracle DIVAdirector é uma ferramenta para interação com Oracle DIVArchive Systems existentes. A Interface do Usuário (User Interface, UI) é disponibilizada graficamente por meio de um Web browser. O DIVAdirector consiste nos seguintes componentes principais:

1.1.1. DIVAdirector Server

O DIVAdirector Server oferece uma interface com o DIVArchive por meio da API C++ para todas as operações solicitadas pelo DIVAdirector Web. Ele também sincroniza informações sobre objetos descobertos armazenadas no DIVArchive com o seu próprio banco de dados. Ele monitora as pastas-depósito configuradas para proxies, metadados e operações, além de manter um histórico de todas as pastas-depósito e operações de UI.

1.1.2. DIVAdirector Web

O módulo Web do DIVAdirector fornece uma interface UI baseada na Web, permitindo que os usuários procurem objetos descobertos no DIVArchive, administrem os direitos de acesso dos usuários, adicione metadados para ativos, sejam proxies de objetos e executem operações, como restauração, restauração parcial e exclusão, nos itens adicionados a áreas de trabalho e listas de segmentos. Ele também permite que os usuários pesquisem arquivos localmente e arquivem conteúdo no DIVArchive system.

1.1.3. DIVAdirector Database

O DIVAdirector usa PostgreSQL para armazenar todas as informações sobre ativos, metadados, informações sobre proxy, informações sobre o usuário, informações históricas sobre operações e definições de configuração.

1.1.4. DIVAdirector Transcoder Service

O DIVAdirector Transcoder Service é um serviço separado que é chamado pelo DIVAdirector para transcodificar clipes de alta resolução em proxies de baixa resolução que, por sua vez, são mostrados na UI do DIVAdirector Web.

1.1.5. DIVAdirector Task Manager Service

O DIVAdirector Task Manager Service é um aplicativo de serviço do Windows visível na caixa de diálogo Gerenciador de Controle de Serviços. Este aplicativo é responsável por processar tarefas de execução potencialmente longa em um processo de background.

1.1.6. DIVAdirector API Service

Este serviço expõe pontos finais para a funcionalidade comum do DIVAdirector. Inicialmente, apenas um pequeno subconjunto da lógica do DIVAdirector estará contido neste serviço. Os pontos finais expostos por meio deste serviço continuarão a crescer à medida que a funcionalidade for gradualmente migrada do DIVAdirector Web.

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 atualizada a versão do DIVAdirector 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 DIVAdirector usa as seguintes portas TCP/IP:

- a tcp/7680 para comandos da interface do usuário
- a tcp/8080 para o HTTP Server

Para as releases do DIVAdirector posteriores à 5.3.0, são necessárias três portas adicionais:

- tcp/9763 - integração com o DIVArchiveWS Service.
- tcp/9876 - integração com o DIVAtranscode Service.
- tcp/6543 - integração com o DIVAdirector API Service.

Observação:

Os números de porta listados acima são atuais; no entanto, eles podem mudar no futuro.

1.2.3. Execute o sistema como usuário ADMIN e utilize o Princípio do Privilégio Mínimo sempre que Possível

O DIVAdirector fornece um usuário Superadmin padrão cuja senha deve ser alterada após o primeiro log-in. Depois, este usuário poderá criar outros usuários com diferentes permissões de grupos para o acesso e a execução de operações.

Se a senha padrão não for alterada, o sistema poderá ser acessado por atividades mal-intencionadas. A senha padrão deverá ser alterada imediatamente após a instalação e a configuração da conta de Superadmin, a cada 180 dias (no mínimo) daí em diante. Após fazer a alteração, você deverá armazenar as senhas em um local seguro, off-line, onde elas poderão ser disponibilizadas para o Suporte Técnico Oracle, se necessário.

1.2.4. Monitore a Atividade do Sistema

Você pode monitorar a atividade do sistema para determinar a eficiência da operação do DIVAdirector. Os logs ficam localizados em C:/Program Files (x86)/DIVAdirector 5/cmgs-server and C:/Program Files (x86)/DIVAdirector 5/www/logs.

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 DIVAdirector.

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 DIVAdirector, proteja os seguintes recursos:

2.1.1.1. Disco de Dados Principais

Há pastas proxy que contêm cliques de baixa resolução. Elas ficam localizadas principalmente em discos remotos ou locais conectados ao DIVAdirector System. O acesso independente (não realizado por meio do DIVAdirector) 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 do Banco de Dados e Discos de Backup

Recursos de Disco de Banco de Dados e de Disco de Backup são usados para construir o DIVAdirector. Normalmente, eles são discos remotos ou locais conectados aos DIVAdirector Systems. O acesso independente (não realizado por meio do DIVAdirector) 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. Definições e Arquivos de Configuração

As definições de configuração do DIVAdirector System devem ser protegidas em relação a usuários não administradores no nível do Sistema Operacional (SO). Em geral, essas definições são protegidas automaticamente por usuários administrativos no nível do Sistema

Operacional. Observe que tornar os arquivos de configuração graváveis para usuários não administrativos do Sistema Operacional representa um risco de segurança. Os arquivos que contêm informações sigilosas abrangem todos os arquivos de configuração de aplicativos contidos no diretório de instalação, incluindo:

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

2.1.2. Contra quem os recursos estão sendo protegidos?

Em geral, os recursos descritos na seção anterior devem ser protegidos em relação a todos os acessos não realizados pelo administrador em um sistema configurado ou em relação a 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 DIVAdirector) a corrupção de dados (gravação em disco ou fita fora das permissões normais).

Capítulo 3. Funcionalidades de Segurança

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

Essas ameaças de segurança podem ser minimizadas pela configuração adequada e pela utilização da lista de verificação de pós-instalação contida 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 tenham 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.

Apêndice A

Apêndice A. Lista de Verificação para uma Implantação Segura

1. Defina senhas fortes para o Administrador e para quaisquer outras contas do Sistema Operacional que tenham atribuições de serviço ou de administrador do DIVAdirector designadas a elas.
2. Não use uma conta do Sistema Operacional para administrador local; em vez disso, designe atribuições, conforme necessário, a outras contas de usuário.
3. Defina uma senha forte para o usuário Administrador do DIVAdirector. Altere a senha imediatamente. Mude a senha instalada padrão para uma senha forte. Você pode fazer isso na tela **Admin, Definições Pessoais** do DIVAdirector.
4. Instale um firewall no sistema e aplique as regras de porta padrão do DIVAdirector.
5. Instale atualizações do Sistema Operacional e do DIVAdirector periodicamente, pois elas incluem patches de segurança.
6. Instale o antivírus e exclua os processos do DIVAdirector e de armazenamento por motivos de desempenho.