Oracle® DIVArchive

Guia de Segurança

Release 2.1

E77642-01

Junho de 2016

ORACLE®

Oracle® DIVArchive
Guia de Segurança

E77642-01

Índice

Prefácio

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

Público-alvo

Este guia destina-se a todos os envolvidos no uso das funcionalidades de segurança e na instalação e configuração seguras do DIVAnet.

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 Oracle DIVAnet 2.1 e explica os princípios gerais de segurança do aplicativo.

1.1. Visão Geral do Produto

O Oracle DIVAnet fornece uma visão unificada do conteúdo arquivado entre vários Oracle DIVArchive Systems distribuídos. O Oracle DIVArchive é um sistema de gerenciamento de armazenamento de conteúdo escalável que suporta o arquivamento de bibliotecas de fitas e sistemas de discos. O DIVAnet facilita a movimentação de conteúdo entre ambientes do DIVArchive e entre discos e servidores de Origem e de Destino do cliente. Ele executa tarefas para fins de recuperação de desastres, distribuição de conteúdo, controle de acesso, desempenho e disponibilidade de conteúdo.

O DIVAnet consiste nos seguintes componentes principais:

1.1.1. DIVAnet ClientAdapter Service

Os clientes dos aplicativos que deverão usar a API do DIVArchive ou a GUI do DIVAnet são conectados ao **DIVAnet ClientAdapter Service**. Este serviço do DIVAnet aceita conexões web e de soquete provenientes de aplicativos e processa as solicitações. Um **ClientAdapter** é configurado em cada sistema que tem aplicativos locais no ambiente em que o DIVArchive e o DIVAnet estão instalados.

1.1.2. DIVAnet ManagerAdapter Service

O **DIVAnet ManagerAdapter Service** funciona como uma ponte entre o DIVAnet e o Oracle DIVArchive Manager. Ele deve ser configurado para permitir acesso remoto por meio de outros DIVAnet Systems.

1.1.3. DIVAnet DbSync Service

O **DIVAnet DbSync Service** é responsável por sincronizar informações sobre ativos provenientes de vários ambientes DIVArchive e armazená-las no banco de dados DIVAnet. O **DbSync** se comunica remotamente com serviços do **ManagerAdapter** em vários ambientes para sincronizar informações sobre objetos arquivados. Normalmente, o **DbSync** é implantado com o **ClientAdapter**. O serviço **DbSync** e o **ClientAdapter** requerem acesso direto ao banco de dados do DIVAnet.

1.1.4. DIVAnetUI (DIVAnet User Interface)

O **DIVAnetUI** é um aplicativo GUI que permite ao usuário monitorar solicitações do DIVAnet e exibir, copiar e excluir ativos do DIVAnet (objetos arquivados pelo DIVA) entre vários ambientes do DIVArchive. Todas as solicitações no nível do DIVAnet podem ser monitoradas, independentemente de terem sido enviadas por meio da API ou da própria interface do usuário. Você também pode exibir informações sobre todos os ambientes DIVArchive configurados, independentemente do fato de o ativo ter sido arquivado ou não por meio do DIVAnet. O **DIVAnetUI** fornece formas flexíveis de consultar informações sobre solicitações e sobre ativos.

1.2. Princípios Gerais de Segurança

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

1.2.1. Mantenha o Software Atualizado

Mantenha-se atualizado com a versão do DIVAnet 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. Restringir o Acesso à Rede aos Serviços Críticos

Por padrão, o DIVAnet utiliza as seguintes portasTCP/IP:

- A porta *`tcp/9801`* é a porta de **WebService** padrão usada pelo **ClientAdapter** do DIVAnet
- A porta *`tcp/7101`* é a porta de soquete API padrão utilizada pelo **ClientAdapter** do DIVAnet (você pode configurar outras portas)
- A porta *`tcp/9800`* é a porta de **WebService** padrão usada pelo **ManagerAdapter** do DIVAnet

Observação:

Nem todas essas portas devem ser expostas externamente. Elas são baseadas na configuração e na utilização.

1.2.3. Utilize o Princípio do Privilégio Mínimo Sempre que Possível

Os serviços do DIVAnet não devem ser executados como o usuário *`admin`* ou *`root`*. Executar os serviços usando outro usuário do sistema operacional (diferente do usuário utilizado para administrar o aplicativo) contribui para a segurança geral do sistema.

O instalador do DIVAnet no ambiente Linux requer dois usuários para concluir a instalação do DIVAnet - o usuário *diva* e um usuário do sistema operacional. Administradores e Operadores utilizam a conta *diva* para instalar e monitorar o DIVAnet. O usuário do sistema operacional controla os serviços do DIVAnet.

Os firewalls devem restringir o uso de portas somente às que são necessárias. O DIVAnet contém funcionalidades de controle de acesso (brevemente descritos em Controle de Acesso) utilizados para restringir usuários e sistemas ao privilégio mínimo possível.

1.2.4. Monitore a Atividade do Sistema

Você deverá monitorar a atividade do sistema para determinar a eficiência da operação do DIVAnet e se ele está registrando alguma atividade fora do normal. Verifique os arquivos de log localizados na pasta *$DIVANET_HOME/Program/log*.

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

Você pode acessar diversas fontes de informações e alertas de segurança para uma grande variedade de produtos de software em:

http://www.us-cert.gov

A principal maneira de manter-se atualizado sobre os problemas de segurança é executar a release mais recente do software DIVAnet.

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 funcionalidades precisam ser protegidas?

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

Ao usar o DIVAnet, proteja os seguintes recursos:

2.1.1.1. Servidores do DIVAnet

O DIVAnet é instalado em um servidor ligado a um ou mais discos (um disco local ou remoto diretamente conectado com o sistema DIVAnet). O acesso independente (não realizado por meio do DIVAnet) 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. Banco de Dados

Recursos de dados e softwares de banco de dados são usados para construir sistemas DIVAnet. Geralmente, os dados residem nos discos locais ou remotos conectados com os DIVAnet Systems. O acesso independente (não realizado por meio do DIVAnet) 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. Origens e Destinos do DIVArchive e Mídia de Arquivamento

O DIVAnet utiliza Origens e Destinos do DIVArchive, além de sistemas de arquivamento DIVA (disco ou fita) no processo de satisfazer as suas solicitações. O acesso independente

indevido a esses discos do servidor e à mídia do sistema, que é geralmente controlado por DIVArchive Systems, é um risco à segurança. **Origens/Destinos** usados como áreas temporárias de armazenamento de dados para operações de cópia do DIVAnet devem ter acesso restrito, e você deve cogitar dedicar **Origens/Destinos** unicamente a operações do DIVAnet - e também deverá se certificar de que as transferências sejam criptografadas ou aconteçam em uma rede confiável.

2.1.1.4. Definições e Arquivos de Configuração

As definições de configuração do DIVAnet System devem ser protegidas em relação a usuários não administradores no nível do sistema operacional. Em geral, essas definições são protegidas automaticamente por usuários administrativos no nível do sistema operacional. Tornar os arquivos de configuração graváveis para usuários não administrativos do sistema operacional representa um risco à segurança.

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?

Falhas de proteção nos recursos estratégicos podem variar entre acesso inadequado (ou seja, acesso a dados fora das operações normais do DIVAdirector) e corrupção de dados (exclusão inapropriada de ativos ou gravação em disco ou fita fora das permissões normais).

2.2. Tecnologias de Implantação Recomendadas

Esta seção descreve a instalação e a configuração de um componente de uma infraestrutura segura.

Para obter informações sobre a instalação do DIVAnet, consulte o manual *Oracle DIVAnet Installation, Configuration, and Operations Guide* na biblioteca de *Documentação do DIVAnet 2.1*:

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

Considere os seguintes pontos ao instalar e configurar o DIVAnet.

2.2.1. Instalação do DIVAnet

Você deverá instalar apenas os componentes necessários do DIVAnet. Por exemplo, se você pretende utilizar somente o **DIVAnetUI** em um computador cliente, cancele a seleção de **Serviços DIVAnet** na lista de componentes a serem instalados. Os proprietários e as

permissões do diretório de instalação padrão do DIVAnet não devem ser alterados após a instalação sem que sejam consideradas as implicações de segurança dessas alterações.

2.2.2. Estabelecendo conexão com o DIVArchive

A Oracle recomenda que você instale o componente **ManagerAdapter** no DIVArchive Manager System para oferecer mais segurança ao sistema. Se for necessário acesso externo à porta do DIVArchive Manager, recomendamos bloquear a porta usando o software de firewall. Além disso, geralmente não será necessário permitir acesso externo à porta do **DIVAnet DbSync WebService**.

Se você estabelecer conexão com uma instância remota do DIVArchive por meio de uma WAN, certifique-se de utilizar uma rede confiável. Além disso, considere se conectar com o site usando *SSL/TLS* na porta **ManagerAdapter** do site remoto.

2.2.3. Proteja os Sistemas de Discos

Utilize o Zoneamento FC para negar acesso aos discos do DIVAnet 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 exigem acesso.

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 contra 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.

2.3. Configuração Pós-Instalação

Após a instalação de qualquer parte do DIVAnet, percorra 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 DIVAnet 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 pós-instalação contida no documento 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.

3.2. Autenticação

Os serviços do DIVAnet podem executar a autenticação usando diversos métodos:

- **Certificados SSL / TLS -** O DIVAnet consulta uma área de armazenamento confiável quando cria uma conexão de saída com um serviço DIVAnet remoto. Isso ajuda a garantir que o DIVAnet está sendo conectado com serviços genuínos do DIVAnet. Para criar uma conexão segura entre o **ClientAdapter** do DIVAnet e uma instância do DIVArchive, você deverá estabelecer a conexão por meio do **ManagerAdapter** usando um `ConnectionType` identificado como **WebServices**.
- **Regras de Acesso** - Apesar de serem tecnicamente uma forma de controle de acesso, as regras de acesso podem filtrar as conexões de entrada com base no endereço IP de entrada. Esta funcionalidade é necessária para ajudar a assegurar que apenas os sistemas aprovados tenham o acesso apropriado a serviços do DIVAnet.

ADVERTÊNCIA:

Os serviços do DIVAnet utilizam senhas de banco de dados como parte de sua configuração. As senhas deverão ser imediatamente alteradas após a instalação e, após isso, a cada 180 dias (no mínimo). Após a alteração ter sido feita, você deverá armazenar as senhas em um local seguro, off-line, onde estarão disponíveis para o Oracle Support, se necessário.

3.3. Controle de Acesso

É possível criar regras de acesso para limitar as operações que determinados usuários ou sistemas poderão executar no sistema de arquivamento distribuído. As regras de acesso podem ser executadas das seguintes maneiras:

- **Modo ClientAdapter /MultiDiva** - Restringe os tipos de solicitações do DIVAnet que podem ser executadas.
- **ManagerAdapter** - Restringe os tipos de solicitações do DIVArchive que podem ser executadas para satisfazer uma solicitação do DIVAnet (possivelmente feita por um sistema remoto).

As regras de acesso podem afetar solicitações iniciadas no **DIVAnetUI** ou em uma conexão de soquete da API (possivelmente iniciada por um sistema MAM ou um sistema de automação).

Uma solicitação do DIVAnet pode ter regras de acesso executadas no nível do DIVAnet ou no nível do DIVArchive. No nível do DIVAnet, o **ClientAdapter** processa a solicitação em que a requisição foi recebida. No nível do DIVArchive, um **ManagerAdapter** remoto processa solicitações do DIVArchive emitidas para satisfazer a solicitação do DIVAnet.

A Oracle recomenda que você crie regras mais restritivas que atendam às necessidades do seu aplicativo. Por exemplo, se apenas administradores precisarem executar exclusões globais, certifique-se de que outras pessoas tenha o acesso negado a essa funcionalidade. Se um grupo de usuários do sistema exigir acesso apenas a uma lista finita de Origens e Destinos, certifique-se de que esses usuários possam emitir somente solicitações para Origens e Destinos específicos.

Também considerem os ambientes usados para satisfazer solicitações. Por exemplo, se os usuários do ambiente local não tiverem motivo para fazer cópias onde os ambientes de origem de destino e os ambientes de destino não estejam no ambiente local (isso é possível por meio da utilização do DIVAnet), defina essas regras na configuração do **ClientAdapter**.

Por fim, considere construtos específicos nas solicitações que deseja excluir indistintamente. Por exemplo, se não for necessário incluir objetos que tenham somente o Nome do Objeto (sem a categoria), exclua todas as solicitações com categorias em branco.

Além disso, cada ClientAdapter WorkflowProfile contém a lista de mensagens válidas que podem ser processadas por solicitações designadas ao WorkflowProfile. No **Modo MultiDiva**, esse recurso fornece uma forma de excluir mensagens específicas do processamento (incluindo mensagens informativas).

A Oracle recomenda começar com as regras padrão definidas no arquivo `AccessRules.xml.ini`, mesmo que não defina as suas próprias regras de acesso. Para obter mais informações sobre as funcionalidades de Controle de Acesso do DIVAnet, consulte o manual *Oracle DIVAnet Installation, Configuration, and Operations Guide* em:

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

3.4. Configurando SSL/TLS

O DIVAnet contém dados de certificado em dois lugares: uma *área de armazenamento de chaves privadas*, usada para Web services hospedados no sistema local e uma *área de armazenamento de chaves públicas*, usada para verificar Web services chamados remotamente. Você pode usar o **Utilitário Java Keytool** para alterar a senha da área de armazenamento de chaves e adicionar ou excluir certificados.

Consulte os seguintes itens para obter mais informações sobe a criação de áreas de armazenamento de chaves:

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

Somente as conexões de Web services do DIVAnet utilizam *SSL/TLS*. Nesta release, a conexão com o DIVArchive ou o DIVAnet por meio de um soquete de API do DIVArchive não utilizará *SSL/TLS*.

3.4.1. Área de Armazenamento de Chaves Privadas

Os dados de certificado de chave privada do DIVAnet são armazenados em:

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

Exatamente um certificado deverá ser exibido nesta área de armazenamento de chaves. Este certificado é usado para Web services hospedados por serviços executados neste diretório *$DIVANET_HOME*. Recomendamos substituir o certificado enviado por um novo certificado e usar um certificado específico para cada ambiente DIVAnet na sua rede.

Você deverá alterar a senha desta área de armazenamento de chaves. Armazene as informações da senha em um novo arquivo chamado *$DIVANET_HOME/Program/divanet/lib/diva129.properties* e torne esse arquivo legível para serviços DIVAnet (no Linux esse usuário é *divanetsvc*), mas não legível para usuários eventuais do sistema (por exemplo, o usuário *diva* no Linux). Use o seguinte formato para o arquivo:

keystorePassword=newpassword

3.4.2. Área de Armazenamento de Chaves Públicas

Às vezes chamados de *armazenamento confiável*, esses dados ficam localizados em:

$DIVANET_HOME/Java/lib/security/cacerts2

Estes dados de certificado são usados em chamadas de saída de Web services (incluindo o **DIVAnetUI**). É possível carregar várias chaves públicas nesta área de armazenamento de chaves.

Se você tiver adicionado um novo certificado autoassinado à área de armazenamento de chaves privadas do DIVAnet, exporte o certificado usando o utilitário keytool. Todos os aplicativos (serviços DIVAnet, DIVAnetUI etc.) que chamam **WebServices** neste ambiente deverão adicionar o certificado exportado à sua própria área de armazenamento de chaves públicas.

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 DIVAnet designadas a elas. Isso inclui:
   - *diva*, *divanetsvc* e outros ID de Usuário Oracle que estiverem sendo usados
   - Quaisquer contas administrativas de discos
2. Não utilize uma conta de sistema operacional para administrador local; em vez disso, designe atribuições, conforme necessário, a outras contas de usuário.
3. Utilize certificados específicos para os sites em cada instalação do DIVAnet e defina uma senha forte para o banco de dados Oracle e a área de armazenamento de chaves privadas. Defina uma senha forte para o log-in no sistema operacional do banco de dados Oracle.
4. Instale software de firewall em cada sistema DIVAnet e aplique as regras de porta padrão do DIVAnet. Restrinja o acesso ao soquete de API do DIVAnet (*tcp 7101*) a IPs que exigem acesso usando regras de firewall. Execute esta etapa com as Regras de Acesso do DIVAnet.
5. Instale atualizações do sistema operacional e do DIVAnet em uma base periódica, pois elas incluem patches de segurança.
6. Instale o antivírus e, por motivos de desempenho, exclua os processos do DIVAdirector e de armazenamento.
7. As melhores práticas impõem a segregação de discos FC e de unidades de fita FC fisicamente ou por meio de Zoneamento FC, para que os discos e os dispositivos de fita não compartilhem a mesma porta HBA. Esta prática de segurança ajuda a impedir acidentes de perda de dados em decorrência da sobregravação acidental de dados importantes.
8. Configure um conjunto apropriado de backups para o banco de dados e a configuração do DIVAnet. Os backups fazem parte da segurança e fornecem uma maneira de restaurar dados perdidos acidentalmente ou em decorrência de alguma falha. O backup deverá incluir alguma política enquanto estiver sendo transportado para um local externo. Os backups devem ser protegidos da mesma forma que os discos do DIVAnet.