Oracle® DIVAdirector

Guide de sécurité

Version 5.3

E71131-01

Décembre 2015

ORACLE®

Oracle® DIVAdirector
Guide de sécurité

E71131-01

Table des matières

Préface

Le guide de sécurité de DIVAdirector d'Oracle contient une présentation du produit et explique les principes généraux de sécurité de l'application.

Public

Ce guide s'adresse à toute personne pouvant être amenée à utiliser les fonctions de sécurité et à effectuer des opérations d'installation et de configuration de DIVAdirector.

Accessibilité de la documentation

Pour plus d’informations sur l’engagement d’Oracle pour l’accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Accès aux services de support Oracle
Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

1

Chapitre 1. Présentation

Ce chapitre fournit une présentation du produit DIVAdirector et explique les principes généraux de sécurité de l'application.

1.1. Présentation du produit

Oracle DIVAdirector est un outil permettant l'interaction avec des systèmes Oracle DIVArchive existants. L'interface utilisateur graphique fonctionne au moyen d'un navigateur Web. DIVAdirector contient les composants principaux suivants :

1.1.1. DIVAdirector Server

DIVAdirector Server fournit les interfaces avec DIVArchive via l'API C++ pour toutes les opérations demandées par DIVAdirector Web. Il synchronise également, dans sa propre base de données, les informations des objets détectés stockées dans DIVArchive. Il surveille les dossiers cible configurés pour les proxies, les métadonnées et les opérations et gère l'historique de l'ensemble des dossiers cible et opérations de l'interface utilisateur.

1.1.2. DIVAdirector Web

Le module Web de DIVAdirector fournit une interface Web permettant aux utilisateurs de rechercher des objets détectés dans DIVArchive, d'administrer les droits d'accès utilisateur, d'ajouter des métadonnées aux ressources, d'utiliser des proxies d'objet et d'effectuer des opérations telles que la restauration, la restauration partielle et la suppression des éléments ajoutés aux emplacements de travail ou aux listes de plans et séquences. Les utilisateurs peuvent également consulter des fichiers en local et archiver du contenu dans le système DIVArchive.

1.1.3. Base de données DIVAdirector

DIVAdirector utilise PostgreSQL pour stocker toutes les informations sur les ressources, les proxies, les utilisateurs ainsi que les métadonnées, l'historique des opérations et les paramètres de configuration.

1.1.4. DIVAdirector Transcoder Service

DIVAdirector Transcoder Service est un service distinct appelé par DIVAdirector pour transcoder des clips haute résolution en proxies basse résolution qui sont ensuite affichés dans l'interface utilisateur de DIVAdirector Web.

1.1.5. DIVAdirector Task Manager Service

DIVAdirector Task Manager Service est une application de service Windows visible dans la boîte de dialogue standard de Services Control Manager. Cette application permet d'exécuter des tâches dont l'exécution est potentiellement longue en tant que processus en arrière-plan.

1.1.6. DIVAdirector API Service

Ce service expose les points de terminaison pour la fonctionnalité commune de DIVAdirector. Au départ, seul un petit sous-ensemble de la logique de DIVAdirector est contenu dans ce service. Les points de terminaison exposés à travers ce service continuent de se développer à mesure que la fonctionnalité est migrée depuis DIVAdirector Web.

1.2. Principes généraux de sécurité

Les sections suivantes décrivent les principes fondamentaux nécessaires pour utiliser toutes les applications en toute sécurité.

1.2.1. Mise à jour du logiciel

Assurez-vous de toujours exécuter la dernière version de DIVAdirector. Vous pouvez trouver les versions actuelles du logiciel à télécharger sur Oracle Software Delivery Cloud :

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

1.2.2. Limitation de l'accès via le réseau aux services critiques

DIVAdirector utilise les ports TCP/IP suivants :

- tcp/7680 pour les commandes de l'interface utilisateur
- tcp/8080 pour le serveur HTTP

Pour les versions DIVAdirector postérieures à la version 5.3.0, trois ports supplémentaires sont nécessaires :

- tcp/9763 - Intégration de DIVArchiveWS Service.
- tcp/9876 - Intégration de DIVAtranscode Service.
- tcp/6543 - Intégration de DIVAdirector API Service.

Remarque:

Les numéros de port indiqués ci-dessus sont les numéros actuels ; toutefois, ils sont susceptibles de changer dans le futur.

1.2.3. Exécution en tant qu'utilisateur ADMIN et utilisation du principe du moindre privilège si possible

DIVAdirector fournit un utilisateur Super Admin par défaut dont le mot de passe doit être modifié après la première connexion. Cet utilisateur peut ensuite créer d'autres comptes utilisateur disposant de différentes autorisations de groupe pour l'accès et les opérations.

Si le mot de passe par défaut n'est pas modifié, le système demeure accessible pour une activité malveillante potentielle. Le mot de passe par défaut doit être modifié immédiatement après l'installation et la configuration pour le compte Super administrateur, et tous les 180 jours (au minimum) après cela. Une fois la modification apportée, vous devez stocker les mots de passe dans un emplacement sécurisé, hors ligne, où ils seront disponibles pour le support technique Oracle, le cas échéant.

1.2.4. Surveillance de l'activité du système

Vous pouvez surveiller l'activité du système afin de déterminer si DIVAdirector fonctionne correctement. Les journaux sont situés sous C:/Program Files (x86)/DIVAdirector 5/cmg-server et C:/Program Files (x86)/DIVAdirector 5/www/logs.

1.2.5. Consultation des dernières informations de sécurité

Vous pouvez accéder à plusieurs sources d'informations de sécurité. Pour les informations de sécurité et les alertes pour une grande variété de produits logiciels, voir :

`http://www.us-cert.gov`

La principale façon de rester à jour en matière de sécurité consiste à exécuter la version la plus récente du logiciel DIVAdirector.

2

Chapitre 2. Installation sécurisée

Ce chapitre vous indique le processus de planification pour une installation sécurisée. Il décrit également plusieurs topologies de déploiement recommandées pour ces systèmes.

2.1. Analyse de votre environnement

Les réponses aux questions suivantes peuvent vous aider à comprendre les exigences de sécurité :

2.1.1. Quelles sont les ressources à protéger ?

Vous pouvez protéger un grand nombre de ressources dans l'environnement de production. Lorsque vous choisissez le niveau de sécurité à mettre en oeuvre, tenez compte des ressources qui nécessitent une protection. Lors de l'utilisation de DIVAdirector, protégez les ressources suivantes :

2.1.1.1. Disque de données principal

Il s'agit des dossiers proxy contenant les clips basse résolution. Ces derniers figurent principalement sur les disques locaux et distants connectés au système DIVAdirector. L'accès indépendant à ces disques (sans passer par DIVAdirector) présente un risque de sécurité. Un tel accès externe peut se faire à partir d'un système non fiable qui lit ou écrit sur ces disques ou à partir d'un système interne qui fournit un accès à ces unités de disque par accident.

2.1.1.2. Disque de base de données et disques de sauvegarde

Il s'agit des ressources de disque de base de données et de disque de sauvegarde utilisées pour créer le système DIVAdirector. Ce sont généralement des disques locaux et distants connectés aux systèmes DIVAdirector. L'accès indépendant à ces disques (sans passer par DIVAdirector) présente un risque de sécurité. Un tel accès externe peut se faire à partir d'un système non fiable qui lit ou écrit sur ces disques ou à partir d'un système interne qui fournit un accès à ces unités de disque par accident.

2.1.1.3. Fichiers et paramètres de configuration

Les paramètres de configuration du système DIVAdirector doivent être protégés contre l'accès par des utilisateurs autres que des administrateurs de niveau système d'exploitation. En général, ces paramètres sont protégés automatiquement par les utilisateurs administrateurs

de niveau système d'exploitation. Notez que rendre les fichiers de configuration accessibles en écriture à des utilisateurs non administratifs présente un risque de sécurité. Les fichiers sensibles englobent tous les fichiers de configuration de l'application figurant dans le répertoire d'installation, notamment :

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

2.1.2. De quels utilisateurs les ressources doivent-elles être protégées ?

En général, les ressources décrites dans la section précédente doivent être protégées contre l'accès par des utilisateurs non-administrateurs sur un système configuré, ou contre un système externe non fiable qui peut accéder à ces ressources via le WAN ou le Fabric FC.

2.1.3. Que se passera-t-il si la protection des ressources stratégiques échoue ?

Les conséquences d'un échec de la protection des ressources peuvent aller d'un accès inapproprié (accès à des données en dehors des opérations DIVAdirector normales) à l'altération des données (écriture sur le disque ou la bande en dehors des autorisations normales).

3

Chapitre 3. Fonctions de sécurité

Pour éviter des menaces de sécurité potentielles, les clients exécutant DIVAdirector doivent faire attention à l'authentification et l'autorisation du système.

Ces menaces de sécurité peuvent être réduites grâce à une configuration adéquate et en suivant la liste de contrôle post-installation de l'Annexe A, *Liste de contrôle du déploiement sécurisé*.

3.1. Modèle de sécurité

Les fonctionnalités de sécurité critiques suivantes protègent contre les menaces de sécurité :

- Authentification : garantit que seules les personnes autorisées peuvent accéder au système et aux données.
- Autorisation : fournit un contrôle d'accès aux privilèges du système et aux données. Cette fonctionnalité repose sur l'authentification afin de garantir que les personnes disposent uniquement de l'accès dont elles ont besoin.

Annexe A

Annexe A. Liste de contrôle du déploiement sécurisé

1. Définissez des mots de passe forts pour le compte Administrateur et tous les autres comptes de niveau système d'exploitation (SE) auxquels des rôles administrateur ou service DIVArchive ou DIVAdirector sont affectés.
2. N'utilisez pas le compte d'administrateur SE local mais affectez les rôles comme nécessaire aux autres comptes utilisateur.
3. Définissez un mot de passe fort pour l'utilisateur administrateur DIVAdirector. Remplacez immédiatement le mot de passe par défaut de l'installation par un mot de passe fort. Vous pouvez effectuer cette modification dans l'écran des paramètres **Admin**, **Personal** de DIVAdirector.
4. Installez le pare-feu sur le système et appliquez les règles de port DIVAdirector par défaut.
5. Installez les mises à jour du SE et de DIVAdirector sur une base périodique car ces dernières incluent les patches de sécurité.
6. Installez l'antivirus et excluez les processus DIVAdirector et le stockage à des fins de performance.