Oracle® DIVArchive

Guide de sécurité

Version 7.4

E77628-01

Juin 2016

ORACLE®

Oracle® DIVArchive
Guide de sécurité

E77628-01

Table des matières

Préface

Le guide de sécurité de DIVArchive 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 DIVArchive.

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 DIVArchive et explique les principes généraux de sécurité de l'application.

1.1. Présentation du produit

Le produit DIVArchive d'Oracle est un système de gestion de stockage de contenu distribué. DIVArchive est constitué des composants suivants :

1.1.1. Oracle DIVArchive Manager

DIVArchive Manager est le composant principal d'un système DIVArchive. Toutes les opérations d'archivage sont contrôlées et gérées par DIVArchive Manager. Les demandes d'opération sont envoyées par les applications initiatrices par le biais de l'API client DIVArchive. DIVArchive prend également en charge des gestionnaires principal et de sauvegarde DIVArchive, en tant qu'option payante. Pour plus d'informations sur DIVArchive, reportez-vous à la bibliothèque de documentation client du logiciel DIVArchive version 7.4 à l'adresse suivante :

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

1.1.2. Oracle DIVArchive Actor

DIVArchive Actor est le programme de déplacement des données entre les périphériques dans le système de production. Il prend en charge le transfert de données entre différents types de périphériques et gère les opérations de transcodage à l'aide du logiciel Telestream (facultatif).

Toutes les opérations d'Actor sont initiées et coordonnées par DIVArchive Manager. Une même instance de DIVArchive Manager peut configurer et contrôler plusieurs instances Actor.

1.1.3. DIVArchive Robot Manager

Vous pouvez utiliser DIVArchive pour gérer uniquement le stockage sur disque, mais il est possible d'étendre la capacité de stockage en ajoutant une ou plusieurs bandothèques. Dans ces cas, le module DIVArchive Robot Manager fournit une couche logicielle intermédiaire à DIVArchive Manager pour interagir avec différents types de bibliothèques de bandes. Il

est connecté à DIVArchive Manager via TCP/IP. DIVArchive Robot Manager s'interface avec la bibliothèque en utilisant une interface directe vers la bibliothèque elle-même (via une connexion SCSI ou SCSI native sur Fibre Channel) ou au moyen d'une connexion Ethernet intermédiaire avec le logiciel de contrôle de la bibliothèque propre au fabricant.

1.1.4. DIVArchive Backup Service

DIVArchive Backup Service a été introduit pour assurer la fiabilité et la surveillance des sauvegardes des bases de données et de métadonnées Oracle.

Le composant DIVArchive Backup Service est installé en tant que partie intégrante de l'installation standard du système DIVArchive. Ce composant est généralement installé sur le même serveur que DIVArchive Manager et Oracle Database. DIVArchive Backup Service permet la configuration de sauvegardes planifiées au moyen de son fichier de configuration. Il gère et surveille la totalité du processus de sauvegarde.

DIVArchive Backup Service permet désormais d'envoyer des e-mails concernant les problèmes survenus au cours du processus de sauvegarde des fichiers de base de données et de base de métadonnées. Pour tirer parti de cette fonctionnalité, DIVArchive doit être configuré pour se connecter à un fournisseur de messagerie SMTP. Les notifications par e-mail sont configurées à l'aide de l'utilitaire de configuration de DIVArchive figurant sous l'onglet Manager Setting.

Pour plus d'informations sur l'installation et la configuration du service de sauvegarde de DIVArchive, reportez-vous à la bibliothèque de documentation client de DIVArchive 7.4 à l'adresse suivante :

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

1.1.5. Oracle DIVArchive Avid Connectivity

L'utilisation d'Avid Connectivity avec DIVArchive vise à transférer les données d'archivage vers et depuis DIVArchive dans des formats vidéo spécifiques et à permettre l'archivage et l'extraction de clips individuels ou d'une séquence de clips. Les composants AMC et TMC connexes sont installés avec l'installation principale de DIVArchive. Une installation supplémentaire est requise pour certains plug-ins, que ce soit pour AMC ou TMC.

1.1.6. DIVArchive Drop Folder Monitor (DFM)

Le composant DIVArchive Drop Folder Monitor (DFM) assure la surveillance automatique des fichiers nouvellement créés dans 20 dossiers locaux ou dossiers FTP maximum (ou des combinaisons des deux). Un fichier ou plusieurs fichiers (dans des dossiers FTP) par objet DIVArchive sont pris en charge. Quand un nouveau fichier (ou dossier FTP) est identifié, DFM envoie automatiquement une demande d'archivage à DIVArchive pour archiver le nouveau fichier ou dossier. Dès lors que ces fichiers sont archivés avec succès, ils sont automatiquement supprimés de la source.

1.1.7. DIVArchive SNMP

L'agent SNMP et la base d'informations de gestion (MIB) de DIVArchive prennent en charge la surveillance des statuts et de l'activité de DIVArchive et de ses sous-systèmes au moyen d'une application de surveillance tierce via le protocole SNMP. DIVArchive SNMP n'est pris en charge que dans les environnements Windows.

1.1.8. DIVArchive Storage Plan Manager (SPM)

Le composant DIVArchive Storage Plan Manager (SPM) assure la migration automatique et la gestion du cycle de vie du support dans l'archive en fonction des règles et stratégies définies dans la configuration SPM.

Le composant SPM permet également de déclencher la suppression du support dans les baies gérées par SPM (en fonction des filigranes d'espace disque).

1.1.9. DIVArchive Migrate Service

DIVArchive inclut un service de migration intégré. Il s'agit d'un nouveau service interne et distinct (de DIVArchive) qui aide les utilisateurs à planifier et exécuter des travaux pour migrer du contenu entre différents médias au sein d'un système DIVArchive. Vous pouvez utiliser l'interface graphique de contrôle ou le client de ligne de commande.

1.1.10. DIVArchive VACP

VACP (Video Archive Command Protocol) est un protocole développé par Harris Automation pour assurer l'interface vers un système d'archive. DIVArchive a sa propre API pour communiquer avec DIVArchive Manager, qui n'est pas compatible avec VACP.

1.1.11. DIVArchive Control GUI

L'interface graphique (GUI) de contrôle de DIVArchive permet de surveiller, contrôler et superviser les opérations DIVArchive. Plusieurs interfaces graphiques DIVArchive peuvent être en cours d'exécution et connectées au même système DIVArchive en même temps.

1.1.12. DIVArchive Configuration Utility

L'utilitaire de configuration DIVArchive permet de configurer un système d'archivage DIVArchive. Utilisé principalement pour la configuration de DIVArchive, il permet néanmoins d'exécuter quelques fonctions opérationnelles.

1.1.13. DIVArchive Access Gateway

Access Gateway permet le fonctionnement et l'interaction de plusieurs systèmes DIVArchive indépendants à partir d'un seul ordinateur. C'est la solution globale pour la distribution de contenu. La réplication automatique de fichiers vers des sites en miroir fournit une méthode

simple et pratique pour la distribution locale, la sauvegarde et la récupération après sinistre en toute sécurité, avec contrôle de bande passante et vérification de checksum. Les réseaux sont surveillés et DIVAnet assure la livraison finale du contenu.

1.1.14. DIVArchive Local Delete

Local Delete est un service qui surveille les fonctions de réplication d'objet entre un système DIVArchive local (par exemple DIVAlocal) et un ou plusieurs systèmes DIVArchive distants (par exemple, DIVAdr). Une fois répliqué vers le système DIVArchive distant, l'objet est marqué comme éligible pour suppression dans le système DIVArchive local.

1.2. Principes généraux de sécurité

Les sections suivantes décrivent les principes fondamentaux à respecter pour utiliser les applications en toute sécurité.

1.2.1. Mise à jour du logiciel

Assurez-vous de toujours exécuter la dernière version de DIVArchive. 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 réseau aux services critiques

DIVArchive utilise les ports TCP/IP suivants :

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

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

N'exécutez pas les services DIVArchive avec un compte d'utilisateur (de niveau système d'exploitation) Administrateur (ou Root). Vous devez toujours exécuter tous les services DIVArchive avec un compte d'utilisateur (ou de groupe) dédié du système d'exploitation, nommé DIVA.

L'interface graphique (GUI) de contrôle de DIVArchive fournit trois profils utilisateur fixes (Administrateur, Opérateur et Utilisateur). Les comptes Administrateur et Opérateur

requièrent un mot de passe pour l'obtention de l'accès. Vous devez affecter le mot de passe d'administrateur et/ou d'opérateur dans l'utilitaire de configuration avant d'utiliser ces profils.

Vous créez les mots de passe des comptes Administrateur et Opérateur au moment de l'installation et de la configuration. Ces mots de passe doivent être renouvelés au moins tous les 180 jours. Les mots de passe doivent être communiqués au support technique Oracle si nécessaire.

1.2.4. Surveillance de l'activité du système

Surveillez l'activité du système afin de déterminer si DIVArchive fonctionne correctement et si une activité inhabituelle est signalée. Consultez les fichiers journaux dans le répertoire d'installation sous */Program/log/*.

1.2.5. Consultation des dernières informations de sécurité

Vous pouvez accéder à plusieurs sources d'informations de sécurité. Le site suivant fournit des informations de sécurité et des alertes concernant une grande variété de produits logiciels :

`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 DIVArchive.

2

Chapitre 2. Installation sécurisée

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

2.1. Analyse de l'environnement

Les questions suivantes peuvent vous aider à déterminer les besoins de votre environnement en matière 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.

Lorsque vous utilisez DIVArchive, protégez les ressources suivantes :

2.1.1.1. Disque de données principal

Il s'agit des ressources de disque de données et de disque cache utilisées pour créer les systèmes DIVArchive. Ce sont généralement des disques locaux ou distants connectés aux systèmes DIVArchive. L'accès indépendant (autre que par DIVArchive) à ces disques présente un risque pour la sécurité. Un tel accès externe peut se faire à partir d'un système non fiable qui lit et écrit sur ces disques ou à partir d'un système interne qui fournit accidentellement l'accès à ces périphériques.

2.1.1.2. Disque de base de données, disque de métadonnées et disques de sauvegarde

Il s'agit des ressources de disque de base de données, de métadonnées et de sauvegarde utilisées pour créer des systèmes DIVArchive avec des objets complexes. Ce sont généralement des disques locaux ou distants connectés aux systèmes DIVArchive. L'accès indépendant (autre que par DIVArchive) à ces disques présente un risque pour la sécurité. Un tel accès externe peut se faire à partir d'un système non fiable qui lit et écrit sur ces disques ou à partir d'un système interne qui fournit accidentellement l'accès à ces périphériques.

2.1.1.3. Bandes DIVArchive

Autoriser l'accès indépendant à des bandes, notamment dans une bandothèque contrôlée par des systèmes DIVArchive où des données sont écrites, présente un risque de sécurité.

2.1.1.4. Exportation des métadonnées de bande

Les vidages de métadonnées de bande créés à partir de l'opération d'exportation contiennent des données et des métadonnées. Les autorisations sur ces données et métadonnées doivent être limitées au seul compte Administrateur (ou Root) du système d'exploitation ou au compte d'utilisateur (ou de groupe) DIVA du système d'exploitation lors d'une activité d'exportation ou d'importation de routine.

2.1.1.5. Fichiers et paramètres de configuration

Les paramètres de configuration des systèmes DIVArchive doivent être protégés contre l'accès par des utilisateurs autres que des administrateurs de niveau système d'exploitation. Comme il est risqué d'autoriser d'autres utilisateurs à écrire dans ces fichiers, les autorisations sur les fichiers de configuration doivent être restreintes au compte Administrateur (ou Root) du système d'exploitation ou au compte d'utilisateur (ou de groupe) du système d'exploitation DIVA.

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 tout accès par des utilisateurs non-administrateurs sur un système configuré ou contre les systèmes externes non fiables qui peuvent accéder à ces ressources via le WAN ou la topologie fabric FC.

2.1.3. Que peut-il se passer en cas de défaillance de la protection des ressources stratégiques ?

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

2.2. Topologies de déploiement recommandées

Cette section décrit l'installation et la configuration sécurisées d'un composant d'infrastructure. Pour plus d'informations sur l'installation de DIVArchive, reportez-vous à la bibliothèque de documentation client de DIVArchive 7.4 à l'adresse suivante :

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

Tenez compte des points suivants lors de l'installation et de la configuration de DIVArchive :

2.2.1. Réseau de métadonnées séparé

Pour la connexion entre les différents composants de service de DIVArchive, la connexion à la base de métadonnées et la connexion à partir de ses clients, fournissez un réseau TCP/IP séparé et un commutateur qui n'est connecté à aucun WAN. Le trafic des métadonnées étant mis en oeuvre à l'aide de TCP/IP, une attaque externe sur ce trafic est théoriquement possible. La configuration d'un réseau de métadonnées séparé limite ce risque et permet également une performance améliorée. S'il est impossible de réaliser un réseau distinct, interdisez au moins le trafic sur les ports DIVArchive à partir du WAN externe et de tous les hôtes non autorisés sur le réseau. Voir Limitation de l'accès réseau aux services critiques.

2.2.2. Zonage FC

Utilisez le zonage FC pour refuser l'accès aux disques DIVArchive connectés au moyen de Fibre Channel par tout serveur ne nécessitant pas l'accès à ces disques. Utilisez de préférence un commutateur FC séparé pour établir une connexion physique uniquement avec les serveurs qui requièrent l'accès.

2.2.3. Protection de l'accès à la configuration des disques SAN

Les disques SAN RAID sont généralement accessibles à des fins d'administration via le protocole TCP/IP ou plus souvent via HTTP. Vous devez protéger les disques d'un accès externe en limitant l'accès administratif aux disques SAN RAID aux seuls systèmes figurant dans un domaine de confiance. D'autre part, modifiez le mot de passe par défaut sur les baies de disques.

2.2.4. Installation du package DIVArchive

Tout d'abord, installez uniquement les services DIVArchive dont vous avez besoin.
Par exemple, si vous ne planifiez pas d'exécuter l'interface graphique ou l'utilitaire de configuration à partir d'un système, désélectionnez-les dans la liste des composants à installer au cours de l'installation. Les autorisations et propriétaires du répertoire d'installation de DIVArchive par défaut doivent être limités au compte Administrateur (ou Root) ou au compte d'utilisateur (ou de groupe) DIVA.

2.2.5. Sécurité des bandes DIVArchive

Empêchez tout accès externe aux bandes DIVArchive au sein d'une bandothèque contrôlée par le système DIVArchive. L'accès non autorisé aux bandes DIVArchive peut compromettre ou détruire les données d'utilisateur.

2.2.6. Sauvegardes

Configurez et exécutez des sauvegardes de base de données à l'aide du service DIVArchive Backup. Les autorisations pour le vidage de sauvegarde doivent être limitées au seul compte

Administrateur (ou Root) du système d'exploitation ou au compte d'utilisateur (ou de groupe) DIVA du système d'exploitation.

2.3. Configuration après l'installation

Après avoir installé un composant DIVArchive, passez en revue la liste de contrôles de sécurité dans l'Annexe A, *Liste de contrôle pour un déploiement sécurisé*.

3

Chapitre 3. Fonctions de sécurité

Pour éviter des menaces de sécurité potentielles, les clients exécutant DIVArchive 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 contrôles post-installation de l'Annexe A, *Liste de contrôle pour un 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 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.

3.2. Authentification

L'interface graphique (GUI) de contrôle de DIVArchive fournit trois profils utilisateur (Administrateur, Opérateur et Utilisateur). Les comptes Administrateur et Opérateur requièrent un mot de passe pour l'obtention de l'accès. Vous devez affecter le mot de passe d'administrateur et/ou d'opérateur dans l'utilitaire de configuration avant d'utiliser ces profils.

Les mots de passe de ces deux profils doivent être modifiés au moins tous les 180 jours. Les mots de passe doivent être communiqués au support technique Oracle si nécessaire.

3.3. Contrôle d'accès

Dans DIVArchive, le contrôle d'accès comprend trois profils. Les comptes Administrateur et Opérateur requièrent un mot de passe pour l'obtention de l'accès. Vous devez affecter le mot de passe d'administrateur et/ou d'opérateur dans l'utilitaire de configuration avant d'utiliser ces profils.

Utilisateur : Une fois la connexion à DIVArchive Manager établie, l'interface graphique de contrôle autorise uniquement l'utilisateur à surveiller les opérations DIVArchive et à extraire

les données de la base de données. Il s'agit du profil Utilisateur. Ce profil ne permet pas d'accéder à toutes les fonctions qui envoient des commandes à DIVArchive. Il est utile dans les cas où il est nécessaire d'effectuer une surveillance sans autoriser l'envoi de commandes à DIVArchive.

Administrateur : Pour transmettre des demandes à DIVArchive, telles que des demandes d'archivage ou de restauration, ou pour éjecter une bande d'une bandothèque, vous devez basculer vers le profil Administrateur. Le profil Administrateur est protégé par un mot de passe. Avant de l'utiliser, vous devez lui affecter un mot de passe à l'aide de l'utilitaire de configuration. Pour plus d'informations, consultez la bibliothèque de documentation client d'Oracle DIVArchive 7.4 à l'adresse suivante :

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

Opérateur : Outre les autorisations du profil Utilisateur, le profil Opérateur fournit l'accès à l'utilitaire de transfert d'objet. Son utilisation requiert l'affectation préalable d'un mot de passe dans l'utilitaire de configuration.

Annexe A

Annexe A. Liste de contrôle pour un déploiement sécurisé

1. Définissez des mots de passe forts pour le compte Administrateur (ou Root) et tout autre compte de niveau système d'exploitation pourvu de rôles d'administrateur ou de service DIVArchive, notamment :
   - Les ID utilisateur Oracle et DIVA (le cas échéant)
   - Tout compte d'administration de baie de disques
2. N'utilisez pas de compte d'administrateur local au niveau système d'exploitation. Affectez les rôles appropriés aux autres comptes d'utilisateur.
3. Définissez un mot de passe fort pour les comptes Administrateur et Opérateur pour l'interface graphique (GUI) de contrôle. Avant utilisation, vous devez affecter un mot de passe à ces profils dans l'utilitaire de configuration.
4. Définissez un mot de passe fort pour la connexion à la base de données Oracle.
5. Installez un pare-feu sur chaque système et appliquez les règles de port DIVArchive par défaut. Limitez l'accès à l'API DIVArchive (`tcp/9000`) aux seules adresses IP qui en ont besoin à l'aide des règles de pare-feu.
6. Installez les mises à jour du système d'exploitation et de DIVArchive de façon régulière car elles contiennent des correctifs liés à la sécurité.
7. Installez l'antivirus et excluez les processus DIVArchive et le stockage (pour des raisons de performances).
8. Il est recommandé de séparer les disques FC et les lecteurs de bande FC, physiquement ou via le zonage FC, de sorte que les deux types de périphérique ne partagent pas le même port HBA. Pour les disques gérés, seuls les acteurs DIVArchive doivent avoir accès aux disques et également aux lecteurs de bande. Cette pratique de sécurité permet d'éviter les pertes de données accidentelles résultant de l'écrasement d'une bande ou d'un disque.
9. Configurez un ensemble approprié de sauvegardes de la configuration DIVArchive et de la base de données. Les sauvegardes font partie de la sécurité. Elles permettent de restaurer des données perdues suite à un accident ou en raison d'une faille. Vos sauvegardes doivent inclure des règles stratégiques lors du transport vers un emplacement hors site. Les sauvegardes doivent être protégées au même niveau que les bandes et disques DIVArchive.