Oracle® DIVArchive

Guide de sécurité

Version 7.3

E70864-01

Décembre 2015

ORACLE®

Oracle® DIVArchive
Guide de sécurité

E70864-01

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

DIVArchive d'Oracle est un système de gestion de stockage de contenu distribué. DIVArchive contient les composants suivants :

1.1.1. DIVArchive Manager

DIVArchive Manager est le composant principal du 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 les 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 7.3 à l'adresse suivante :

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

1.1.2. 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 les différents types de périphériques et gère les opérations de transcodage à l'aide du logiciel Tele stream (facultatif).

Toutes les opérations d'Actor sont initiées et coordonnées par DIVArchive Manager. Un ou plusieurs acteurs peuvent être configurés et contrôlés par un seul DIVArchive Manager.

1.1.3. DIVArchive Robot Manager

Bien que DIVArchive puisse être utilisé pour ne gérer que le stockage sur disque, la capacité de stockage peut être étendue par l'ajout d'une ou de plusieurs bibliothèques de bandes. 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 Fiber Channel), ou au moyen d'une connexion intermédiaire Ethernet vers le logiciel de contrôle de la bibliothèque propre au fabricant.

1.1.4. DIVArchive Backup Service

Pour assurer la fiabilité et la surveillance des sauvegardes des bases de données Oracle et de métadonnées, le composant DIVArchive Backup Service a été introduit.

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 la base de données Oracle. 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.

Il 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 du logiciel DIVArchive version 7.3 à l'adresse suivante :

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

1.1.5. Oracle 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 pour les composants AMC et TMC.

1.1.6. DIVArchive Drop Folder Monitor

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 émet une demande d'archivage automatiquement 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.

1.1.8. DIVArchive 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, de contrôler et de superviser les opérations dans DIVArchive. Plusieurs interfaces graphiques DIVArchive peuvent être en cours d'exécution et connectées au même système DIVArchive en même temps.

1.1.12. Utilitaire de configuration DIVArchive

L'utilitaire de configuration DIVArchive permet de configurer un système DIVArchive. Bien qu'utilisé principalement pour la configuration de DIVArchive, l'utilitaire de configuration sert également à exécuter d'autre 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 de fichiers automatique 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 Lynx Local delete

LYNXLocalDelete est un service qui surveille les fonctions de réplication d'objet entre un système DIVArchive local (par exemple LYNXlocal) et un (ou plusieurs) systèmes DIVArchive distants (par exemple, LYNXdr). Une fois l'objet répliqué avec succès vers le

système DIVArchive distant, il est marqué comme éligible pour suppression dans le système DIVArchive local.

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 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 via le réseau aux services critiques

DIVArchive utilise les ports TCP/IP suivants :

- tcp/8500 est utilisé par DIVArchive Robot Manager
- tcp/9000 est utilisé par DIVArchive Manager
- tcp/9300 est utilisé par DIVArchive Backup Service
- tcp/9500 est utilisé par DIVArchive Access Gateway
- tcp/9900 est utilisé par DIVArchive Actor
- tcp/9191 est utilisé par DIVArchive Migrate Service

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

Tous les services DIVArchive sont exécutés avec le compte d'utilisateur DIVA. 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. Le système DIVArchive est livré avec des mots de passe par défaut qui peuvent être modifiés à tout moment à l'aide de l'utilitaire de configuration de DIVArchive. Si les mots de passe par défaut ne sont pas modifiés, le système DIVArchive demeure accessible pour une activité malveillante potentielle. **Les mots de passe par défaut doivent être modifiés immédiatement après l'installation et la configuration pour les comptes Administrateur et Opérateur, 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

Contrôlez l'activité du système afin de déterminer si DIVArchive fonctionne correctement et si une activité anormale est détectée. 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. 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 DIVArchive.

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 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 les disques locaux et distants connectés aux systèmes DIVArchive. L'accès indépendant à ces disques (sans passer par DIVArchive) présente un risque de 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 un accès à ces unités de disque par accident.

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 disque de métadonnées et de disque de sauvegarde utilisées pour créer les systèmes DIVArchive avec des objets complexes. Ce sont généralement des disques **locaux ou distants** connectés aux systèmes DIVArchive. L'accès indépendant à ces disques (sans passer par DIVArchive) présente un risque de 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 un accès à ces unités de disque par accident.

2.1.1.3. Bandes DIVArchive

Autoriser l'accès indépendant à des bandes, notamment dans une bibliothèque de bandes contrôlée par les systèmes DIVArchive, où les 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. Ces données et métadonnées doivent être protégées contre tout accès autre que par l'administrateur du système d'exploitation au cours d'une activité d'exportation ou d'importation de routine.

2.1.1.5. Fichiers et paramètres de configuration

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

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

Les conséquences d'un échec de la protection des ressources stratégiques 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 du logiciel DIVArchive version 7.3 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 données des 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 Section 1.2.2, « Limitation de l'accès via le réseau aux services critiques ».

2.2.2. Zonage FC

Utilisez le zonage FC pour refuser l'accès aux disques DIVArchive connectés via Fiber Channel à partir d'un serveur qui ne requiert pas d'accès aux 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 généralement le protocole HTTP. Vous devez protéger les disques d'un accès externe en limitant l'accès administratif aux disques SAN RAID pour les systèmes figurant uniquement dans un domaine de confiance. D'autre part, modifiez le mot de passe par défaut sur des 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 d'accès au répertoire d'installation DIVArchive par défaut et les propriétaires ne doivent pas être modifiés après l'installation sans envisager les implications en termes de sécurité de telles modifications.

2.2.5. Sécurité des bandes DIVArchive

Empêchez l'accès externe aux bandes DIVArchive figurant dans la bibliothèque de bandes 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. Limitez l'accès au vidage de sauvegarde aux administrateurs de niveau système d'exploitation uniquement.

2.3. Configuration après l'installation

Après avoir installé un composant DIVArchive, consultez la liste de contrôle de sécurité dans l'Annexe A, *Liste de contrôle du 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 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.

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. Le système DIVArchive est livré avec des mots de passe par défaut qui peuvent être modifiés à tout moment au moyen de l'utilitaire de configuration DIVArchive. Si les mots de passe par défaut ne sont pas modifiés, le système DIVArchive demeure accessible pour une activité malveillante potentielle. **Les mots de passe par défaut doivent être modifiés immédiatement après l'installation et la configuration pour les comptes Administrateur et Opérateur, 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.**

3.3. Contrôle d'accès

Dans DIVArchive, le contrôle d'accès comprend trois 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. En mode profil Utilisateur, les fonctions émettant des commandes pour DIVArchive ne sont pas toutes accessibles. Ce profil s'avère 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 bibliothèque, vous devez basculer vers le profil Administrateur. Le profil Administrateur est protégé par mot de passe. Le mot de passe par défaut pour ce profil est diva ; toutefois, celui-ci peut être (ou a pu être) modifié dans l'utilitaire de configuration. Pour plus d'informations, reportez-vous à la bibliothèque de documentation client du logiciel DIVArchive version 7.3 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 et requiert la saisie du même mot de passe que celui du profil Administrateur.

Annexe A

Annexe A. Liste de contrôle du déploiement sécurisé

1. Définissez des mots de passe forts pour le compte Administrateur et tout autre compte de niveau système d'exploitation (SE) auxquels un rôle administrateur ou service DIVArchive est affecté, notamment :
   - Les ID utilisateur Oracle et DIVA (s'il est utilisé)
   - Tout compte d'administration de baie de disques.
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 les comptes Administrateur et Opérateur pour l'interface utilisateur (GUI) de contrôle. Remplacez immédiatement le mot de passe par défaut de l'installation par défaut par un mot de passe fort. Vous pouvez effectuer cette modification à partir de l'utilitaire de configuration sous Tools (Outils).
4. Définissez un mot de passe fort pour la connexion à la base de données Oracle. Modifiez les mots de passe par défaut définis lors de l'installation.
5. Installez le pare-feu sur chaque système et appliquez les règles de port DIVArchive par défaut. Limitez l'accès à l'API DIVArchive (tcp 9000) pour l'IP qui a besoin de l'accès à l'aide des règles de pare-feu.
6. Installez les mises à jour du SE et de DIVArchive sur une base périodique car ces dernières incluent les mises à jour de sécurité.
7. Installez l'antivirus et excluez les processus DIVArchive et le stockage à des fins de performance.
8. Séparez les disques FC et les lecteurs de bande FC physiquement ou via le zonage FC de sorte que les disques et les lecteurs de bande ne partagent pas le même port HBA. Pour le disque géré uniquement, les acteurs DIVArchive doivent avoir accès au disque et également aux lecteurs de bande. Cette pratique de sécurité aide à 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 et fournissent un moyen de restaurer des données perdues accidentellement ou en raison d'une faille. Votre sauvegarde doit inclure des politiques lors du transport vers un emplacement hors site. Les sauvegardes doivent être protégées au même niveau que les bandes et disques DIVArchive.