Oracle® DIVAnet

Guide de sécurité

Version 2.0

E74314-01

Mars 2016

ORACLE®

Oracle® DIVAnet
Guide de sécurité

E74314-01

Table des matières

Préface

Le guide de sécurité DIVAnet d'Oracle contient des informations sur le produit Oracle DIVAnet 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 DIVAnet.

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 présente Oracle DIVAnet 2.0 et explique les principes généraux de sécurité de l'application.

1.1. Présentation du produit

Oracle DIVAnet offre une vue unifiée du contenu archivé dans plusieurs systèmes Oracle DIVArchive distribués. DIVArchive d'Oracle est un système de gestion de stockage de contenu évolutif, prenant en charge l'archivage dans des bibliothèques de bandes et des systèmes de disques. DIVAnet facilite le déplacement du contenu entre les sites DIVArchive ainsi qu'à partir des serveurs et disques de sources et destinations. Il effectue ses tâches à de fins de récupération après sinistre, de distribution de contenu, de contrôle d'accès, de performances et de disponibilité de contenu.

DIVAnet contient les principaux composants suivants :

1.1.1. Service DIVAnet ClientAdapter

Les clients d'application qui veulent utiliser l'API DIVArchive ou l'interface utilisateur graphique DIVAnet, sont connectés au **service DIVAnet ClientAdapter**. Ce service DIVAnet accepte les connexions Web et de socket à partir des applications et traite les demandes. Un **ClientAdapter** est configuré sur chaque site comportant des applications locales sur le site d'installation de DIVArchive et de DIVAnet.

1.1.2. Service DIVAnet ManagerAdapter

Le **service DIVAnet ManagerAdapter** sert de pont entre DIVAnet et Oracle DIVArchive Manager. Il doit être configuré pour fournir un accès distant par d'autres systèmes DIVAnet.

1.1.3. Service DIVAnet DbSync

Le **service DIVAnet DbSync** est responsable de la synchronisation des informations relatives aux ressources provenant de plusieurs sites DIVArchive et du stockage des informations dans la base de données DIVAnet. **DbSync** communique à distance avec les services **ManagerAdapter** sur plusieurs sites pour synchroniser les informations relatives aux objets archivés. **DbSync** est généralement déployé en même temps que le service **ClientAdapter**. Les services **DbSync** et **ClientAdapter** requièrent tous les deux un accès direct à la base de données DIVAnet.

1.1.4. Interface utilisateur DIVAnet (DIVAnetUI)

DIVAnetUI est une interface utilisateur graphique qui permet à l'utilisateur de surveiller les demandes DIVAnet, et de voir, copier et supprimer les ressources DIVAnet (objets archivés DIVA) dans plusieurs sites DIVArchive. Toutes les demandes de niveau DIVAnet peuvent être surveillées, qu'elles soient émises via l'API ou l'interface utilisateur elle-même. Vous pouvez également consulter les informations relatives aux ressources pour tous les sites DIVArchive configurés, que les ressources soient archivées ou non au moyen de DIVAnet. **DIVAnetUI** permet d'interroger avec une plus grande souplesse à la fois les informations relatives aux demandes et celles relatives aux ressources.

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 DIVAnet. 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

DIVAnet utilise les ports TCP/IP par défaut suivants :

- *`tcp/9801`* est le port **WebService** par défaut utilisé par le service **ClientAdapter** de DIVAnet.
- *`tcp/7101`* est le port par défaut de socket d'API utilisé par le service **ClientAdapter** de DIVAnet (vous pouvez configurer d'autres ports).
- *`tcp/9800`* est le port **WebService** par défaut utilisé par le service **ManagerAdapter** de DIVAnet.

Remarque:

Ces ports n'ont pas tous besoin d'être exposés en externe. Ils sont basés sur la configuration et l'utilisation.

1.2.3. Utilisation du principe du moindre privilège si possible

Les services DIVAnet ne doivent pas être exécutés comme rôle *`admin`* ou *`superutilisateur`*. Exécuter ces services en utilisant un autre utilisateur de système d'exploitation (différent de l'utilisateur utilisé pour administrer l'application) contribue à la sécurité générale du système. Des pare-feux doivent limiter les ports à ceux qui sont requis seulement. DIVAnet contient des fonctionnalités de contrôle d'accès (brièvement décrites

dans la rubrique " Contrôle d'accès "), utilisées pour limiter les utilisateurs et les systèmes aux privilèges les plus faibles possibles.

1.2.4. Surveillance de l'activité du système

Vous devez contrôler l'activité du système afin de déterminer si DIVAnet fonctionne correctement et si une activité anormale est détectée. Vérifiez les fichiers journaux situés dans le dossier *$DIVANET_HOME/Program/log/*.

1.2.5. Consultation des dernières informations de sécurité

Vous pouvez accéder à plusieurs sources d'informations et d'alertes de sécurité pour des produits divers à l'adresse :

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

La meilleure manière de rester à jour en termes de sécurité est d'exécuter la version la plus récente du logiciel DIVAnet.

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. Présentation 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 DIVAnet, protégez les ressources suivantes :

2.1.1.1. Serveurs DIVAnet

DIVAnet est installé sur un serveur connecté à un ou plusieurs disques (un disque local ou distant directement connecté au système DIVAnet). L'accès indépendant à ces disques (sans passer par DIVAnet) 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. Base de données

Une base de données et des ressources de données sont utilisées pour créer des systèmes DIVAnet. Les données figurent généralement sur des disques locaux ou distants connectés aux systèmes DIVAnet. L'accès indépendant à ces disques (sans passer par DIVAnet) 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. Sources et destinations DIVArchive, et média d'archivage

DIVAnet utilise des sources et destinations DIVArchive ainsi que les systèmes d'archivage DIVA (disque ou bande) pour satisfaire ses demandes. L'accès indépendant injustifié à ces

disques du serveur et médias de système, qui sont généralement contrôlés par les systèmes DIVArchive, présente un risque de sécurité. Les **sources/destinations** qui sont utilisées comme magasins de données temporaires pour les opérations de copie DIVAnet, doivent être dotées d'un accès limité. Vous devez envisager de dédier ces **sources/destinations** aux opérations DIVAnet seulement, et vous assurer également que les transferts sont chiffrés ou lancés sur un réseau sécurisé.

2.1.1.4. Fichiers et paramètres de configuration

Les paramètres de configuration du système DIVAnet 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 disposant de privilèges administratifs au niveau du système d'exploitation. Rendre les fichiers de configuration accessibles en écriture à des utilisateurs du système d'exploitation 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 tout accès par des utilisateurs non-administrateur sur un système configuré ou contre les systèmes externes non fiables qui peuvent 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 défaillances de la protection contre les ressources stratégiques peuvent aller d'un accès inapproprié (c'est-à-dire, accès à des données en dehors des opérations normales de DIVAdirector) à l'altération des données (suppression erronée de ressources ou écriture sur le disque ou la bande en dehors des autorisations normales).

2.2. Technologies de déploiement recommandées

Cette section décrit l'installation et la configuration d'un composant d'infrastructure sécurisé.

Pour plus d'informations sur l'installation de DIVAnet, reportez-vous au manuel *Guide d'Oracle DIVAnet* dans la bibliothèque de documentation DIVAnet 2.0, à l'adresse :

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

Tenez compte des points suivants lors de l'installation et de la configuration de DIVAnet.

2.2.1. Installation de DIVAnet

Installez uniquement les composants DIVAnet dont vous avez besoin. Par exemple, si vous prévoyez d'exécuter seulement **DIVAnetUI** à partir d'un système, désélectionnez les **services**

DIVAnet dans la liste des composants à installer. Les autorisations d'accès au répertoire d'installation DIVAnet par défaut et les propriétaires ne doivent pas être modifiés après l'installation sans envisager les implications en termes de sécurité de telles modifications.

2.2.2. Connexion à DIVArchive

Oracle vous recommande d'installer le composant **ManagerAdapter** sur le système DIVArchive Manager pour garantir une sécurité supplémentaire. Si un accès externe au port DIVArchive Manager n'est pas nécessaire, il est recommandé de bloquer le port au moyen d'un pare-feu. En outre, il n'est souvent pas nécessaire d'autoriser un accès réseau externe au port **DIVAnet DbSync WebService**.

Si vous vous connectez à une instance DIVArchive distante sur un WAN, assurez-vous d'utiliser un réseau sécurisé. Envisagez également de vous connecter au site en utilisant le protocole *SSL/TLS* pour la connexion au port **ManagerAdapter** du site distant.

2.2.3. Protection des systèmes de disques

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

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 contre un accès externe en limitant l'accès administratif aux disques SAN RAID pour les systèmes figurant uniquement dans un domaine sécurisé. D'autre part, modifiez le mot de passe par défaut sur des baies de disques.

2.3. Configuration après l'installation

Après avoir installé n'importe quelle partie de DIVAnet, vérifiez la liste de contrôle de sécurité dans Annexe A, *Liste de contrôle du déploiement sécurisé*.

3

Chapitre 3. Fonctions de sécurité

Pour éviter des menaces de sécurité potentielles, les clients exécutant DIVAnet 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 et aux données du système. Cette fonctionnalité repose sur l'authentification afin de garantir que les personnes disposent uniquement de l'accès dont elles ont besoin.

3.2. Authentification

Les services DIVAnet peuvent utiliser plusieurs méthodes pour effectuer l'authentification :

- **Certificats SSL/TLS** : DIVAnet consulte un truststore de certificats lorsqu'il crée une connexion sortante à un service DIVAnet distant. Cela permet de garantir que DIVAnet est connecté à des services DIVAnet authentiques. Pour créer une connexion sécurisée à partir du service **ClientAdapter** de DIVAnet vers une instance DIVArchive, vous devez vous connecter via le service **ManagerAdapter** en utilisant un type de connexion `<ConnectionType>` identifié comme **WebServices**.
- **Règles d'accès** : bien qu'elles soient techniquement une forme de contrôle d'accès, les règles d'accès peuvent filtrer les connexions entrantes en fonction de l'adresse IP entrante. Cette fonctionnalité est nécessaire pour aider à garantir que seuls les systèmes approuvés ont un accès approprié aux services DIVAnet.

AVERTISSEMENT:

Les services DIVAnet utilisent les mots de passe de la base de données pour leur configuration. Les mots de passe doivent être changés immédiatement après l'installation et tous les 180 jours (au minimum) par la suite. Une fois que vous avez changé les mots de passe, vous devez les stocker dans un emplacement sécurisé, hors ligne, où ils peuvent être mis à la disposition du support technique Oracle si nécessaire.

3.3. Contrôle d'accès

Vous pouvez créer des règles d'accès pour limiter les opérations que certains utilisateurs ou systèmes peuvent effectuer dans le système d'archivage distribué. Les règles d'accès peuvent être exécutées comme suit :

- **ClientAdapter/Mode MultiDiva** : limite les types de demandes DIVAnet pouvant être exécutés.
- **ManagerAdapter** : limite les types de demandes DIVArchive pouvant être exécutés pour satisfaire une demande DIVAnet (potentiellement demandée par un système distant).

Les règles d'accès peuvent affecter les demandes lancées à partir de l'interface utilisateur **DIVAnetUI** ou d'une connexion de socket d'API (potentiellement lancée par une solution MAM ou un système d'automatisation).

Les règles d'accès peuvent être exécutées sur une demande DIVAnet au niveau de DIVAnet ou de DIVArchive. Au niveau de DIVAnet, le service **ClientAdapter** traite la demande où elle est reçue. Au niveau de DIVArchive, un service **ManagerAdapter** distant traite les demandes DIVArchive émises pour satisfaire la demande DIVAnet.

Oracle vous recommande de créer l'ensemble de règles le plus restrictif possible répondant aux exigences de l'application. Par exemple, si seuls les administrateurs ont besoin d'effectuer des suppressions globales, assurez-vous que les autres utilisateurs ne peuvent pas accéder à cette fonctionnalité. Si un groupe d'utilisateurs système a seulement besoin d'accéder à une liste déterminée de sources et destinations, assurez-vous que ces utilisateurs peuvent émettre des demandes uniquement pour ces sources et destinations spécifiques.

Tenez compte également des sites utilisés pour satisfaire aux demandes. Par exemple, si les utilisateurs sur le site local n'ont aucune raison d'effectuer des copies alors que ni le site source ni le site cible n'est le site local (cela est possible en utilisant DIVAnet), configurez ces règles dans la configuration du service **ClientAdapter**.

Enfin, tenez compte des constructions spécifiques dans les demandes que vous voulez exclure systématiquement. Par exemple, si vous n'avez pas besoin d'adresser les objets avec seulement le nom d'objet (sans la catégorie), excluez toutes les demandes dont les catégories sont vides.

De plus, chaque ***`ClientAdapter WorkflowProfile`*** contient la liste des messages valides pouvant être traités par les demande affectées au WorkflowProfile. En **mode MultiDiva**, cela permet d'exclure des messages spécifiques du traitement (notamment les messages d'information).

Oracle recommande de commencer par les règles par défaut définies dans le fichier *`AccessRules.xml.ini`*, même si vous ne définissez pas votre propres règles d'accès. Pour plus d'informations sur les fonctionnalités de contrôle d'accès DIVAnet, reportez-vous au manuel *Guide d'Oracle DIVAnet* à l'adresse :

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

3.4. Configuration des certificats SSL/TLS

DIVAnet stocke les données des certificats dans deux endroits : un *fichier de clés privées*, utilisé pour les services Web hébergés sur le système local ; et un *fichier de clés publiques*, utilisé pour vérifier les services Web qui sont appelés à distance. Vous pouvez utiliser l'**utilitaire Java Keytool** pour changer le mot de passe du fichier de clés et ajouter ou supprimer des certificats.

Reportez-vous au site suivant pour plus d'informations sur la création des fichiers de clés :

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

Seules les connexions aux services Web DIVAnet utilisent des certificats *SSL/TLS*. Dans cette version, la connexion à DIVArchive ou DIVAnet au moyen d'une connexion de socket d'API DIVArchive n'utilisera pas *SSL/TLS*.

3.4.1. Fichier de clés privées

Les données des certificats de clés privées DIVAnet sont stockées dans :

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

Un seul certificat exactement doit apparaître dans ce fichier de clés. Ce certificat est utilisé pour les services Web hébergés par les services exécutés à partir du répertoire *$DIVANET_HOME*. Il est recommandé de remplacer le certificat fourni par un nouveau certificat et d'utiliser un certificat différent pour chaque site DIVAnet du réseau.

Vous devez changer le mot de passe de ce fichier de clés. Stockez les informations relatives au mot de passe dans un nouveau fichier intitulé *$DIVANET_HOME/Program/divanet/lib/diva129.properties* et rendez ce fichier lisible par les services DIVAnet, mais non lisible par les utilisateurs occasionnels du système. Utilisez le format suivant pour le fichier :

keystorePassword=[newpassword]

3.4.2. Fichier de clés publiques

Parfois appelé *truststore*, ces données sont situées dans :

$DIVANET_HOME/Java/lib/security/cacerts2

Ces données de certificat sont utilisées dans les appels de service Web sortants (notamment **DIVAnetUI**). Vous pouvez charger plusieurs clés publiques dans ce fichier de clés.

Si vous avez ajouté un nouveau certificat autosigné dans le fichier de clés privées DIVAnet, exportez le certificat au moyen de l'utilitaire keytool. Toutes les applications (services

DIVAnet, interface DIVAnetUI, etc.) qui appellent **WebServices** sur ce site doivent ensuite ajouter le certificat exporté à leur propre fichier de clés publiques.

Annexe A

Annexe A. Liste de contrôle du déploiement sécurisé

1. Définissez des mots de passe renforcés pour le compte administrateur et tous les autres comptes du système d'exploitation auxquels des rôles d'administrateur et de service DIVAnet sont affectés. Sont inclus :
   - ID utilisateur Oracle *`divanet`*, le cas échéant
   - Tout compte d'administration de disque
2. N'utilisez pas un compte de système d'exploitation local doté de privilèges administratifs, affectez plutôt des rôles aux autres comptes utilisateur selon les besoins.
3. Utilisez des certificats propres au site pour chaque installation DIVAnet et définissez un mot de passe renforcé pour la base de données Oracle et le fichier de clés privées. Définissez un mot de passe renforcé pour la connexion utilisateur à la base de données Oracle.
4. Installez un pare-feu sur chaque système DIVAnet et appliquez les règles pour port DIVAnet par défaut. Limitez l'accès au socket d'API DIVAnet (*`tcp 7101`*) aux adresses IP requérant l'accès au moyen des règles de pare-feu. Effectuez cette étape en utilisant les règles d'accès de DIVAnet.
5. Installez les mises à jour du système d'exploitation et de DIVAnet régulièrement, car elles contiennent des patchs de sécurité.
6. Installez l'antivirus et excluez les processus DIVAdirector et le stockage à des fins de performance.
7. Selon les meilleures pratiques, les disques FC et les lecteurs de bande FC doivent être séparés physiquement ou au moyen du zonage FC, afin que les périphériques de disque et à bande ne partagent pas le même port HBA. Cette pratique de sécurité permet d'éviter les pertes de données accidentelles résultant de l'écrasement de données importantes.
8. Configurez un ensemble de sauvegardes approprié pour la configuration DIVAnet et 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 disques DIVAnet.