

Oracle® DIVAdirector

セキュリティーガイド

Release 5.3

E71133-01

2015 年 12 月

Copyright © 2015, Oracle and/or its affiliates. All rights reserved.

このソフトウェアおよび関連ドキュメントの使用と開示は、ライセンス契約の制約条件に従うものとし、知的財産に関する法律により保護されています。ライセンス契約で明示的に許諾されている場合もしくは法律によって認められている場合を除き、形式、手段に関係なく、いかなる部分も使用、複写、複製、翻訳、放送、修正、ライセンス供与、送信、配布、発表、実行、公開または表示することはできません。このソフトウェアのリバース・エンジニアリング、逆アセンブル、逆コンパイルは互換性のために法律によって規定されている場合を除き、禁止されています。

ここに記載された情報は予告なしに変更される場合があります。また、誤りが無いことの保証はいたしかねます。誤りを見つけた場合は、オラクルまでご連絡ください。

このソフトウェアまたは関連ドキュメントを、米国政府機関もしくは米国政府機関に代わってこのソフトウェアまたは関連ドキュメントをライセンスされた者に提供する場合、次の通知が適用されます。

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

このソフトウェアまたはハードウェアは様々な情報管理アプリケーションでの一般的な使用のために開発されたものです。このソフトウェアまたはハードウェアは、危険が伴うアプリケーション (人的傷害を発生させる可能性があるアプリケーションを含む) への用途を目的として開発されていません。このソフトウェアまたはハードウェアを危険が伴うアプリケーションで使用する際、安全に使用するために、適切な安全装置、バックアップ、冗長性 (redundancy)、その他の対策を講じることは使用者の責任となります。このソフトウェアまたはハードウェアを危険が伴うアプリケーションで使用したこと起因して損害が発生しても、Oracle Corporation およびその関連会社は一切の責任を負いかねます。

Oracle および Java はオラクルおよびその関連会社の登録商標です。その他の社名、商品名等は各社の商標または登録商標である場合があります。

Intel, Intel Xeon は、Intel Corporation の商標または登録商標です。すべての SPARC の商標はライセンスをもとに使用し、SPARC International, Inc. の商標または登録商標です。AMD, Opteron, AMD ロゴ、AMD Opteron ロゴは、Advanced Micro Devices, Inc. の商標または登録商標です。UNIX は、The Open Group の登録商標です。

このソフトウェアまたはハードウェア、そしてドキュメントは、第三者のコンテンツ、製品、サービスへのアクセス、あるいはそれらに関する情報を提供することがあります。適用されるお客様と Oracle Corporation との間の契約に別段の定めがある場合を除いて、Oracle Corporation およびその関連会社は、第三者のコンテンツ、製品、サービスに関して一切の責任を負わず、いかなる保証もいたしません。適用されるお客様と Oracle Corporation との間の契約に定めがある場合を除いて、Oracle Corporation およびその関連会社は、第三者のコンテンツ、製品、サービスへのアクセスまたは使用によって損失、費用、あるいは損害が発生しても一切の責任を負いかねます。

目次

はじめに	5
対象読者	5
ドキュメントのアクセシビリティについて	5
1. 概要	7
1.1. 製品の概要	7
1.1.1. DIVAdirector サーバー	7
1.1.2. DIVAdirector Web	7
1.1.3. DIVAdirector データベース	7
1.1.4. DIVAdirector Transcoder Service	8
1.1.5. DIVAdirector Task Manager Service	8
1.1.6. DIVAdirector API Service	8
1.2. 一般的なセキュリティー原則	8
1.2.1. ソフトウェアを最新に維持する	8
1.2.2. クリティカルなサービスへのネットワークアクセスを制限する	8
1.2.3. 管理者ユーザーとして実行して可能なかぎり最小特権の原則を使用 する	9
1.2.4. システムアクティビティをモニターする	9
1.2.5. セキュリティー情報を最新に維持する	9
2. セキュアなインストール	11
2.1. 環境を理解する	11
2.1.1. 保護する必要があるリソースはどれか	11
2.1.1.1. プライマリデータディスク	11
2.1.1.2. データベースディスクおよびバックアップディスク	11
2.1.1.3. 構成ファイルおよび設定	12
2.1.2. だれからリソースを保護するか	12
2.1.3. 戦略的リソースの保護に失敗した場合に何が起こるか	12

3. セキュリティー機能	13
3.1. セキュリティーモデル	13
A. セキュアな配備のためのチェックリスト	15

はじめに

オラクルの DIVAdirector セキュリティーガイドには、DIVAdirector 製品に関する情報が含まれており、アプリケーションのセキュリティーの一般的な原則が説明されています。

対象読者

このガイドは、DIVAdirector のセキュリティー機能の使用およびセキュアなインストールと構成に関与するすべてのユーザーを対象にしています。

ドキュメントのアクセシビリティについて

オラクルのアクセシビリティについての詳細情報は、Oracle Accessibility Program の Web サイト (<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>) を参照してください。

Oracle Support へのアクセス

サポートをご契約のお客様には、My Oracle Support を通して電子支援サービスを提供しています。詳細情報は (<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info>) か、聴覚に障害のあるお客様は (<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>) を参照してください。

第1章 概要

この章では、DIVAdirector 製品の概要と、アプリケーションのセキュリティーの一般的な原則について説明します。

1.1. 製品の概要

Oracle DIVAdirector は、既存の Oracle DIVArchive システムと対話するためのツールです。Web ブラウザを介してユーザーインターフェース (UI) がグラフィカルに提供されます。DIVAdirector は、次の主要コンポーネントで構成されています。

1.1.1. DIVAdirector サーバー

DIVAdirector サーバーは、DIVAdirector Web からリクエストされるすべての操作で C++ API を介して DIVArchive とのインターフェースを提供します。また、DIVArchive に格納されている検出済みのオブジェクト情報を同期化して、独自のデータベースに入れます。プロキシ、メタデータ、および操作用に構成されたドロップフォルダをモニターし、すべてのドロップフォルダおよび UI 操作の履歴を保持します。

1.1.2. DIVAdirector Web

DIVAdirector の Web モジュールは Web ベースの UI インターフェースを提供します。これにより、ユーザーは DIVArchive での検出済みオブジェクトの検索、ユーザーアクセス権の管理、アセットのメタデータの追加、オブジェクトのプロキシの実行、および作業用 bin またはショットリストに追加された項目に対する操作 (復元、部分的復元、削除など) を行えます。さらに、ユーザーはローカルでファイルを参照したり、コンテンツを DIVArchive システムにアーカイブしたりすることもできます。

1.1.3. DIVAdirector データベース

DIVAdirector では PostgreSQL を使用して DIVArchive のすべてのアセット情報、メタデータ、プロキシ情報、ユーザー情報、操作履歴、および構成設定を格納します。

1.1.4. DIVAdirector Transcoder Service

DIVAdirector Transcoder Service は、高解像度のクリップを低解像度のプロキシにトランスコードするために DIVAdirector から呼び出される個別のサービスです。トランスコードされた低解像度のプロキシは、その後 DIVAdirector Web UI 内に表示されます。

1.1.5. DIVAdirector Task Manager Service

DIVAdirector Task Manager Service は、標準のサービスコントロールマネージャーのダイアログボックスで表示可能な Windows サービスアプリケーションです。このアプリケーションは、長時間続く可能性のあるタスクをバックグラウンドプロセスで実行します。

1.1.6. DIVAdirector API Service

このサービスは、一般的な DIVAdirector 機能のエンドポイントを公開します。最初、DIVAdirector のほんの一部のロジックのみがこのサービスに含まれます。このサービスを通じて公開されるエンドポイントは、機能が DIVAdirector Web から徐々に移行されるのに伴って増え続けます。

1.2. 一般的なセキュリティ原則

以降のセクションでは、すべてのアプリケーションをセキュアに使用するために必要な基本原則について説明します。

1.2.1. ソフトウェアを最新に維持する

実行する DIVAdirector のバージョンを最新の状態に維持してください。ソフトウェアの最新バージョンは、Oracle Software Delivery Cloud からダウンロードできます。

<https://edelivery.oracle.com/>

1.2.2. クリティカルなサービスへのネットワークアクセスを制限する

DIVAdirector では、次の TCP/IP ポートを使用します。

- tcp/7680 (ユーザーインタフェースコマンド用)
- tcp/8080 (HTTP サーバー用)

5.3.0 よりもあとのリリースの DIVAdirector では、そのほかに 3 つのポートが必要です。

- tcp/9763 - DIVArchiveWS Service の統合。

- tcp/9876 - DIVAtranscode Service の統合。
- tcp/6543 - DIVAdirector API Service の統合。

注記:

上記のポート番号は現在のもので、将来変更される可能性があります。

1.2.3. 管理者ユーザーとして実行して可能な限り最小特権の原則を使用する

DIVAdirector にはデフォルトのスーパー管理者ユーザーが用意されており、最初のログイン後にそのパスワードを変更する必要があります。その後、このユーザーはアクセスおよび操作に異なるグループアクセス権を持つほかのユーザーを作成できます。

デフォルトのパスワードを変更しないと、システムが悪質なアクティビティの対象になる可能性のある状態のままになります。デフォルトのパスワードは、インストール後およびスーパー管理者アカウントの構成後すぐに変更し、その後は最低でも 180 日ごとに変更する必要があります。変更が完了したら、それらのパスワードを安全な場所 (オフライン) に保管し、必要に応じて Oracle サポートが利用できるようにする必要があります。

1.2.4. システムアクティビティをモニターする

システムアクティビティをモニターして、DIVAdirector がどれだけ適切に動作しているかを判断できます。ログは C:/Program Files (x86)/DIVAdirector 5/cmg-server および C:/Program Files (x86)/DIVAdirector 5/www/logs にあります。

1.2.5. セキュリティ情報を最新に維持する

セキュリティ情報の複数のソースにアクセスできます。さまざまなソフトウェア製品のセキュリティ情報や警告については、次を参照してください。

<http://www.us-cert.gov>

最新のセキュリティ情報を維持するための主な方法は、DIVAdirector ソフトウェアの最新バージョンを実行することです。

第2章 セキュアなインストール

この章では、セキュアなインストールの計画プロセスについて説明し、システムの推奨される配備トポロジをいくつか紹介します。

2.1. 環境を理解する

セキュリティーニーズをよりよく理解するには、次の問題を考慮する必要があります。

2.1.1. 保護する必要があるリソースはどれか

本番環境における多くのリソースを保護できます。提供するセキュリティーのレベルを決定する際は、保護対象のリソースの種類を考慮してください。DIVAdirector を使用している場合は、次のリソースを保護します。

2.1.1.1. プライマリデータディスク

低解像度のクリップを含むプロキシフォルダがあります。それらは主として、DIVAdirector システムに接続されているローカルまたはリモートディスク上にあります。こうしたディスクに (DIVAdirector を使わずに) 単独でアクセスすると、セキュリティー上のリスクが生じます。この種の外部アクセスは、こうしたディスクに対して読み取りや書き込みを行う悪質なシステムか、またはこうしたディスクデバイスへのアクセスを誤って提供する内部システムから発生している可能性があります。

2.1.1.2. データベースディスクおよびバックアップディスク

DIVAdirector の構築に使用されるデータベースディスクおよびバックアップディスクのリソースがあります。それらは通常、DIVAdirector システムに接続されているローカルまたはリモートディスクです。こうしたディスクに (DIVAdirector を使わずに) 単独でアクセスすると、セキュリティー上のリスクが生じます。この種の外部アクセスは、こうしたディスクに対して読み取りや書き込みを行う悪質なシステムか、またはこうしたディスクデバイスへのアクセスを誤って提供する内部システムから発生している可能性があります。

2.1.1.3. 構成ファイルおよび設定

DIVAdirector システムの構成設定は、オペレーティングシステム (OS) レベルの管理者以外のユーザーから保護する必要があります。一般に、これらの設定は OS レベルの管理ユーザーによって自動的に保護されます。管理ユーザー以外の OS ユーザーが書き込むことのできる構成ファイルを作成すると、セキュリティ上のリスクが生じることに注意してください。機密ファイルには、インストールディレクトリに格納されているすべてのアプリケーション構成ファイル (次のものを含む) が含まれます。

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

2.1.2. だれからリソースを保護するか

一般に、前のセクションで説明したリソースは、構成されているシステム上の管理者以外のすべてのアクセスから、あるいは WAN または FC ファブリックを使用してこれらのリソースにアクセスできる悪質な外部システムから保護する必要があります。

2.1.3. 戦略的リソースの保護に失敗した場合に何が起こるか

戦略的なリソースに対する保護の失敗には、不適切なアクセス (通常の DIVAdirector 操作以外のデータへのアクセス) から、データ破壊 (通常のアクセス権以外のディスクまたはテープへの書き込み) までさまざまな場合があります。

第3章 セキュリティー機能

潜在的なセキュリティーの脅威を回避するには、DIVAdirector を運用しているお客様がシステムの認証と承認を考慮する必要があります。

こうしたセキュリティーの脅威は、適切な構成によって、また付録A「セキュアな配備のためのチェックリスト」にあるインストール後のチェックリストに従うことによって最小限に抑えることができます。

3.1. セキュリティーモデル

セキュリティーの脅威からの保護を実現するための重要なセキュリティー機能は次のとおりです。

- 認証 - 承認された個人にのみシステムおよびデータへのアクセスが許可されるようにします。
- 承認 - システム権限およびデータへのアクセス制御。この機能は、認証に基づいて、個人が適切なアクセスのみを取得することを保証します。

付録A セキュアな配備のためのチェックリスト

1. DIVArchive または DIVAdirector の管理者ロールまたはサービスロールが割り当てられている Administrator およびほかのすべての OS アカウントに対して強力なパスワードを設定します。
2. ローカル管理者の OS アカウントを使用せず、必要に応じてほかのユーザーアカウントにロールを割り当てます。
3. DIVAdirector の Administrator ユーザーに対して強力なパスワードを設定します。インストール時のデフォルトのパスワードから強力なパスワードにただちに変更してください。これは、DIVAdirector の「**Admin**」、「**Personal**」の設定画面から実行できます。
4. ファイアウォールをシステムにインストールし、デフォルトの DIVAdirector ポート規則を適用します。
5. セキュリティーパッチが含まれているため、OS と DIVAdirector の更新を定期的にインストールします。
6. ウィルス対策機能をインストールし、パフォーマンス上の理由で DIVAdirector のプロセスおよびストレージを除外します。

