Oracle® DIVAnet

セキュリティーガイド

リリース 2.2

E86308-01

2017 年 1 月

ORACLE®

Oracle® DIVAnet
セキュリティーガイド

E86308-01

目次

はじめに

Oracle の『DIVAnet セキュリティーガイド』では、Oracle DIVAnet 製品について説明し、アプリケーションセキュリティーの一般的な原則についても説明します。

対象読者

このガイドは、DIVAnet 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。

1

第1章 概要

この章では、Oracle DIVAnet 2.2 製品の概要を示し、アプリケーションセキュリティーの一般原則について説明します。

1.1. 製品の概要

Oracle DIVAnet は、複数の分散型 Oracle DIVArchive システム全体において、アーカイブされた内容の統一的なビューを提供します。Oracle の DIVArchive は、テープライブラリおよびディスクシステムへのアーカイブをサポートするスケーラブルなコンテンツストレージ管理システムです。DIVAnet は DIVArchive サイト間でコンテンツをあちこち移動させたり、お客様のソースおよび接続先サーバーおよびディスクから移動させたりするのに役立ちます。このタスクは、障害回復、コンテンツ配信、アクセス制御、パフォーマンス、およびコンテンツ可用性のために実行されます。

DIVAnet は、次の主要コンポーネントで構成されています。

1.1.1. DIVAnet ClientAdapter サービス

DIVArchive API を使用する必要があるか、DIVAnet GUI を使用する必要があるアプリケーションクライアントは、**DIVAnet ClientAdapter サービス**に接続します。この DIVAnet サービスは、アプリケーションから Web 接続およびソケット接続を受け入れ、要求を処理します。**ClientAdapter** は、DIVArchive および DIVAnet がインストールされているサイトにローカルのアプリケーションを持つ各サイト上で構成されます。

1.1.2. DIVAnet ManagerAdapter サービス

DIVAnet ManagerAdapter サービスは、DIVAnet と Oracle DIVArchive Manager の橋渡しとして機能します。ほかの DIVAnet システムによるリモートアクセスを提供するように構成する必要があります。

1.1.3. DIVAnet DbSync サービス

DIVAnet DbSync サービスは、複数の DIVArchive サイトからの資産情報を同期させ、情報を DIVAnet データベースに格納する役割を担います。**DbSync** は、複数のサイトの **ManagerAdapter** サービスとリモート通信し、アーカイブ済みのオブジェクト情報を同期します。**DbSync** は通常 **ClientAdapter** とともに配備されます。**DbSync** サービスと **ClientAdapter** は、どちらも DIVAnet データベースへの直接アクセスが必要です。

1.1.4. DIVAnet ユーザーインタフェース (DIVAnetUI)

DIVAnetUI は、DIVAnet 要求をモニターし、複数の DIVArchive サイトにわたって DIVAnet 資産 (DIVA アーカイブ済みオブジェクト) を表示、コピー、および削除できる GUI アプリケーションです。DIVAnet レベルのすべての要求は、それが API を介して発行されたか UI 自体によって発行されたかにかかわらずモニターされます。アセットが DIVAnet を介してアーカイブされたかどうかに関係なく、すべての構成済み DIVArchive サイトのアセット情報を表示することもできます。**DIVAnetUI** は、要求情報と資産情報の両方を照会するための柔軟な方法を提供します。

1.2. 一般的なセキュリティー原則

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 DIVAnet のバージョンを最新の状態に維持します。ソフトウェアのダウンロード用最新バージョンは、Oracle Software Delivery Cloud で見つかります。

`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

DIVAnet はデフォルトで、次の TCP/IP ポートを使用します。

- *`tcp/9801`* は、DIVAnet **ClientAdapter** によって使用されるデフォルト **WebService** ポートです。
- *`tcp/7101`* は、DIVAnet **ClientAdapter** によって使用されるデフォルト API ソケットポートです (ほかのポートを構成できます)

- *tcp/9800* は、DIVAnet **ManagerAdapter** によって使用されるデフォルト **WebService** ポートです

> **注記:**
>
> これらのポートは必ずしもすべて外部に公開する必要はなく、構成と使用法に基づきます。

1.2.3. 可能なかぎり最小特権の原則に従う

DIVAnet サービスは、*admin* または *root* として実行されないようにします。サービスを実行するとき、(アプリケーションを管理するために使用されるユーザーではなく) 別のオペレーティングシステムユーザーを使用することは、システム全体のセキュリティーに寄与します。

DIVAnet Linux インストーラでは 2 人のユーザー (*diva* およびオペレーティングシステムユーザー) が DIVAnet のインストールを完了する必要があります。管理者とオペレータは、*diva* アカウントを使用して、DIVAnet をインストールおよびモニターします。オペレーティングシステムユーザーは、DIVAnet サービスを制御します。

ファイアウォールでは、必要とするものだけにポートを制限する必要があります。DIVAnet には、ユーザーおよびシステムを最小特権に制限するために使用されるアクセス制御機能 (アクセス制御で簡単に説明されています) があります。

1.2.4. システムアクティビティーのモニター

システムアクティビティーをモニターして、DIVAnet がどれだけ適切に動作しているか、および何らかの異常なアクティビティーがロギングされているかどうかを判断する必要があります。*$DIVANET_HOME/Program/log* フォルダにあるログファイルを確認してください。

1.2.5. セキュリティー情報を最新に維持する

さまざまなソフトウェア製品のセキュリティー情報や警告のソースには、次の場所からアクセスできます。

http://www.us-cert.gov

最新のセキュリティー情報に遅れないための一番の方法は、DIVAnet ソフトウェアの最新リリースを実行することです。

2

第2章 セキュアインストール

この章では、セキュア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、次の質問を尋ねる必要があります。

2.1.1. どのリソースを保護する必要があるか

本番環境内の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レベルを決定する際は、保護するリソースの種類を考慮してください。

DIVAnet を使用している場合は、次のリソースを保護する必要があります。

2.1.1.1. DIVAnet サーバー

DIVAnet は、1 つ以上のディスク (DIVAnet システムに直接接続されたローカルディスクまたはリモートディスク) に接続されたサーバーにインストールされます。こうしたディスクに (DIVAnet 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

DIVAnet システムを構築するために、データベースソフトウェアおよびデータリソースが使用されます。データは通常、DIVAnet システムに接続されたローカルディスクまたはリモートディスク上に存在します。こうしたディスクに (DIVAnet 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. DIVArchive のソース、接続先、およびアーカイブメディア

DIVAnet は DIVArchive ソースおよび接続先を使用し、要求を満たすプロセスで DIVA アーカイブシステム (ディスクまたはテープ) を使用します。DIVArchive システムによって通常制御される、これらのサーバーディスクおよびシステム媒体への正当でない単独のアクセスは、セキュリティーリスクです。DIVAnet コピー操作の一時的なデータストアとして使用される**ソース/接続先**には、制限付きアクセス権を割り当てるべきであり、これらの**ソース/接続先**を DIVAnet 操作専用とするよう考慮し、さらに転送が信頼されたネットワーク上で暗号化または開始されることを確認してください。

2.1.1.4. 構成ファイルおよび設定

DIVAnet システムの構成設定は、オペレーティングシステムレベル非管理者ユーザーから保護する必要があります。一般に、これらの設定はオペレーティングシステムレベル管理ユーザーによって自動的に保護されます。非管理オペレーティングシステムユーザーが構成ファイルを書き込めるようにすると、セキュリティーリスクが発生します。

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意のある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 操作の外部でのデータへのアクセス) から、データ破壊 (資産の誤った削除または通常のアクセス権の外部で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。

2.2. 推奨される配備技術

このセクションでは、セキュアインフラストラクチャーコンポーネントのインストールおよび構成について説明します。

DIVAnet のインストールについては、次にある *DIVAnet 2.2* ドキュメントライブラリの『*Oracle DIVAnet* インストール、構成、および操作ガイド』を参照してください。

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

DIVAnet をインストールして構成する際は、次の点を考慮してください。

2.2.1. DIVAnet のインストール

必要な DIVAnet コンポーネントのみをインストールしてください。たとえば、**DIVAnetUI** のみをクライアントコンピュータから実行することを計画している場合、インストール中にインストールされるコンポーネントのリストから「**DIVAnet Services**」チェックボックスを選択解除してください。DIVAnet インストールディレクトリのデフォルトのアクセス権や所有者をインストール後に変更することは、このような変更のセキュリティーへの影響を考慮せずに行うべきではありません。

2.2.2. DIVArchive への接続

システムセキュリティーを高めるために、**ManagerAdapter** コンポーネントを DIVArchive Manager システムにインストールすることをお勧めします。DIVArchive Manager ポートへの外部アクセスが不要な場合は、ファイアウォールソフトウェアを使用してポートをブロックすることをお勧めします。さらに通常は、**DIVAnet DbSync WebService** ポートへの外部ネットワークアクセスを許可する必要はありません。

WAN 経由でリモート DIVArchive インスタンスに接続する場合は、信頼されたネットワーク上で接続するようにしてください。また、サイトに接続するときは、*SSL/TLS* を使用してリモートサイトの **ManagerAdapter** ポートに接続することを検討してください。

2.2.3. ディスクシステムの保護

FC ゾーニングを使用して、ファイバチャネルを介して接続された DIVAnet ディスクへのアクセスのうち、ディスクへのアクセスを必要としないサーバーからのものは拒否してください。個別の FC スイッチを使用して、アクセスを必要とするサーバーにのみ物理的に接続することをお勧めします。

SAN RAID ディスクには通常、管理のために TCP/IP (より一般的には HTTP) 経由でアクセスできます。SAN RAID ディスクへの管理アクセスを信頼できるドメイン内のシステムのみに制限することによって、ディスクを外部アクセスから保護する必要があります。また、ディスクアレイ上のデフォルトのパスワードも変更します。

2.3. インストール後の構成

DIVAnet の一部をインストールしたあと、付録A「セキュアな配備のためのチェックリスト」のセキュリティーチェックリストを確認してください。

3

第3章 セキュリティー機能

潜在的なセキュリティー脅威を回避するには、DIVAnet 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** - システム特権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。

3.2. 認証

DIVAnet サービスは、次に示すいくつかの方法を使用して認証を実行できます。

- **SSL / TLS 証明書** - DIVAnet はリモート DIVAnet サービスへのアウトバウンド接続を作成するとき、証明書トラストストアを調べます。このことは、DIVAnet が本物の DIVAnet サービスに接続していることの確認に役立ちます。DIVAnet **ClientAdapter** から DIVArchive インスタンスへのセキュアな接続を作成するには、**WebServices** として識別される *`ConnectionType`* を使用して、**ManagerAdapter** を介して接続する必要があります。
- **アクセスルール** - アクセスルールは技術的にはアクセス制御の一形態で、インバウンド IP アドレスに基づいてインバウンド接続をフィルタリングできます。この

機能は、許可されたシステムのみが DIVAnet サービスに適切にアクセスできることを保証するために必要です。

注意:

DIVAnet サービスは構成の一部としてデータベースパスワードを使用します。パスワードはインストールの直後およびその後 (最低でも) 180 日ごとに変更する必要があります。変更を行なったら、パスワードはオフラインの安全な場所に保管し、必要に応じて Oracle サポート用に使用できるようにする必要があります。

3.3. アクセス制御

アクセスルールは、分散アーカイブシステム内で特定のユーザーまたはシステムが実行できる操作を制限するために作成できます。アクセスルールは次のいずれかの方法で実行できます。

- **ClientAdapter/MultiDiva モード** - 実行可能な DIVAnet 要求のタイプを制限します。
- **ManagerAdapter** - (おそらくリモートシステムによって要求される) DIVAnet 要求を満たすために実行できる DIVArchive 要求のタイプを制限します。

アクセスルールは、**DIVAnetUI** または API ソケット接続から開始される (おそらく MAM または自動システムによって開始される) 要求に影響を与えることがあります。

DIVAnet 要求には、DIVAnet レベルまたは DIVArchive レベルのアクセスルールが実行される可能性があります。DIVAnet レベルでは、**ClientAdapter** は、要求が受信された場合に要求を処理します。DIVArchive レベルでは、リモート **ManagerAdapter** は DIVAnet 要求を満たすために発行された DIVArchive 要求を処理します。

アプリケーション要件を満たすもっとも制限の厳しいルールセットを作成することをお勧めします。たとえば、管理者だけがグローバル削除を実行する必要がある場合、ほかのユーザーはその機能へのアクセスを拒否されるようにします。あるシステムユーザーのグループが、ソースおよび接続先の有限リストへのアクセスのみを必要とする場合は、これらのユーザーがそれらの特定のソースおよび接続先に対してのみ要求を発行できるようにします。

要求を満たすために使用されるサイトも考慮します。たとえば、ローカルサイトのユーザーが、ソースサイトもターゲットサイトもローカルサイトでなく、コピー

を実行する理由を持たない場合 (DIVAnet を使用すれば可能)、これらのルールを **ClientAdapter** 構成に構成します。

最後に、要求内で全般的に除外する特定の構文について考慮します。たとえば、オブジェクト名のみ持つ (カテゴリのない) オブジェクトに対処する必要がない場合は、カテゴリがブランクのすべての要求を除外します。

さらに、個々の ClientAdapter WorkflowProfile には、WorkflowProfile に割り当てられている要求によって処理できる有効なメッセージのリストが含まれています。**MultiDiva モード**では、これによって特定のメッセージ (情報メッセージを含む) を処理から除外するための方法が提供されます。

独自のアクセスルールを定義しない場合でも、*AccessRules.xml.ini* ファイルで定義されたデフォルトルールで始めることをお勧めします。DIVAnet アクセス制御機能の詳細については、次にある『*Oracle DIVAnet* インストール、構成、および操作ガイド』を参照してください。

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

3.4. SSL/TLS の構成

DIVAnet では証明書データを 2 つの場所に保管します。非公開キーストアは、ローカルシステム上でホストされている Web サービス用に使用され、公開キーストアは、リモートで呼び出される Web サービスを検証するために使用されます。**Java Keytool ユーティリティー** を使用して、キーストアパスワードを変更し、証明書を追加および削除できます。

キーストアの作成に関する詳細情報については、次を参照してください。

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

DIVAnet Web サービス接続のみが *SSL/TLS* を使用します。このリリースでは、DIVArchive API ソケット接続を使用する DIVArchive または DIVAnet への接続では、*SSL/TLS* は使用されません。

3.4.1. 非公開キーストア

DIVAnet 非公開鍵証明書データは次の場所に保管されています。

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

このキーストアには、正確に 1 つの証明書が存在する必要があります。この証明書は、この *$DIVANET_HOME* ディレクトリから実行されているサービスによってホストされる Web サービスのために使用されます。出荷時に提供された証明書を新しい証明書に置き換えることと、ネットワーク内の DIVAnet サイトごとに別の証明書を使用することをお勧めします。

このキーストアのパスワードを変更する必要があります。パスワード情報を、*$DIVANET_HOME/Program/divanet/lib/diva129.properties* という名前の新しいファイルに格納し、このファイルを DIVAnet サービス (Linux ではこのユーザーは *divanetsvc*) から読み取り可能にし、システムの一時的ユーザー (Linux での *diva* ユーザーなど) からは読み取り不能にします。ファイルには、次の書式を使用します。

keystorePassword=newpassword

3.4.2. 公開キーストア

このデータはトラストストアと呼ばれることもあり、次の場所にあります。

$DIVANET_HOME/Java/lib/security/cacerts2

この証明書データは、アウトバウンド Web サービス呼び出し (**DIVAnetUI** を含む) で使用されます。このキーストアには複数の公開鍵をロードできます。

新しい自己署名付き証明書を DIVAnet 非公開キーストアに追加した場合は、keytool ユーティリティーを使用して証明書をエクスポートします。このサイトで **WebServices** を起動するすべてのアプリケーション (DIVAnet サービス、DIVAnetUI など) は、エクスポートされた証明書を独自の公開キーストアに追加するべきです。

付録A

付録A セキュアな配備のためのチェックリスト

1. DIVAnet 管理者役割またはサービス役割が割り当てられている管理者およびその他のオペレーティングシステムアカウントに強力なパスワードを設定します。これには、次のものが含まれます。
   - *diva*、*divanetsvc*、および Oracle ユーザー ID (使用されている場合)
   - すべてのディスク管理者アカウント
2. ローカル管理者オペレーティングシステムアカウントを使用する代わりに、ほかのユーザーアカウントに必要に応じて役割を割り当てるようにします。
3. DIVAnet インストールごとにサイト固有の証明書を使用して、Oracle データベースと非公開キーストアに強力なパスワードを定義します。Oracle データベースオペレーティングシステムログインのための強力なパスワードを設定します。
4. ファイアウォールソフトウェアをすべての DIVAnet システムにインストールし、デフォルトの DIVAnet ポートルールを適用します。DIVAnet API ソケット (*tcp 7101*) へのアクセス権を、ファイアウォールルールを使用してアクセスが必要な IP に制限します。DIVAnet のアクセスルールを使用して、この手順を実行します。
5. オペレーティングシステムおよび DIVAnet の更新を定期的にインストールします (セキュリティーパッチが含まれているため)。
6. ウィルス対策機能をインストールしますが、パフォーマンス上の理由で DIVAdirector プロセスおよびストレージを除外します。
7. ベストプラクティスでは、FC ディスクと FC テープドライブを物理的または FC ゾーニングのいずれかで隔離することによって、ディスクとテープデバイスが同じ HBA ポートを共有しないようにすることが規定されています。このセキュリティー対策は、重要なデータの誤った上書きによって発生するデータ損失事故を防止するのに役立ちます。
8. DIVAnet 構成とデータベースの適切なバックアップセットを構成します。バックアップはセキュリティーの一部であり、誤って、または何らかの侵害によって失われたデータを復元する手段となります。バックアップをオフサイト場所に移送している間、そのバックアップには何らかのポリシーを含めるようにしてください。バックアップは、DIVAnet ディスクと同程度に保護する必要があります。