Oracle® DIVArchive

セキュリティーガイド

Release 7.3

E70865-01

2015 年 12 月

ORACLE®

Oracle® DIVArchive
セキュリティーガイド

E70865-01

目次

はじめに

オラクルの DIVArchive セキュリティーガイドには、DIVArchive 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、DIVArchive 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、DIVArchive 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

オラクルの DIVArchive は、分散型のコンテンツストレージ管理システムです。DIVArchive は、次の主要コンポーネントで構成されています。

1.1.1. DIVArchive Manager

DIVArchive Manager は DIVArchive システムの主要コンポーネントです。すべてのアーカイブ操作は、DIVArchive Manager によって制御および処理されます。操作リクエストは、DIVArchive クライアント API を介してイニシエータアプリケーションによって送信されます。購入可能なオプションとして、DIVArchive はメインおよびバックアップ用の DIVArchive Manager もサポートしています。DIVArchive の詳細は、次にある DIVArchive ソフトウェアリリース 7.3 のカスタマドキュメントライブラリを参照してください。

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

1.1.2. DIVArchive Actor

DIVArchive Actor は、本番システムにおけるデバイス間のデータムーバーです。これは、さまざまなタイプのデバイス間のデータ転送をサポートし、Telestream トランスコードソフトウェアによるトランスコード操作を処理します (オプション)。

Actor のすべての操作は、DIVArchive Manager によって開始および調整されます。1 つの DIVArchive Manager で 1 つ以上の Actor を構成および制御できます。

1.1.3. DIVArchive Robot Manager

DIVArchive はディスクストレージの管理にのみ使用できますが、1 つ以上のテープライブラリを追加することでストレージ容量をさらに拡張できます。このような場合、DIVArchive Robot Manager モジュールは、DIVArchive Manager がさまざまなタイプのテープライブラ

リと対話するための中間ソフトウェア層を提供します。これは TCP/IP 経由で DIVArchive Manager に接続されます。DIVArchive Robot Manager は、ライブラリ自体への直接インタフェース (ネイティブな SCSI または SCSI over Fiber Channel 経由) または製造元の独自のライブラリ制御ソフトウェアへの中間 Ethernet 接続のどちらかを使用して、ライブラリとインタフェース接続します。

1.1.4. DIVArchive バックアップサービス

DIVArchive バックアップサービスは、Oracle Database および Metadata Database の両方のバックアップの信頼性とモニタリングを確保するために導入されました。

DIVArchive バックアップサービスコンポーネントは、DIVArchive システムの標準インストールに不可欠な要素としてインストールされます。このコンポーネントは通常、DIVArchive Manager および Oracle Database と同じサーバー上にインストールされます。DIVArchive バックアップサービスでは、その構成ファイルを通じてスケジュールされたバックアップを構成できます。DIVArchive バックアップサービスはバックアッププロセス全体を管理およびモニターします。

DIVArchive バックアップサービスには、データベースファイルや Metadata Database ファイルをバックアップする過程で発生する問題を電子メールで通知する機能が組み込まれるようになりました。この機能を活用するには、SMTP メールプロバイダに接続するように DIVArchive を構成する必要があります。電子メール通知は、DIVArchive 構成ユーティリティーの「Manger Setting」タブを通じて構成します。

DIVArchive バックアップサービスのインストールおよび構成については、次にある DIVArchive ソフトウェアリリース 7.3 のカスタマドキュメントライブラリを参照してください。

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

1.1.5. Oracle Avid Connectivity

DIVArchive で Avid Connectivity を使用する目的は、DIVArchive との間でのアーカイブデータの転送を特定のビデオ形式で行なって、単一のクリップまたは一連のクリップのアーカイブおよび取り出しを可能にすることです。AMC および TMC 関連のコンポーネントは、主要な DIVArchive のインストールとともにインストールされます。AMC および TMC 用の特定のプラグインには追加のインストールが必要です。

1.1.6. DIVArchive Drop Folder Monitor

DIVArchive Drop Folder Monitor (DFM) は、最大 20 個のローカルフォルダまたは FTP フォルダ (あるいはそれらの組み合わせ) 内に新しく作成されたファイルの自動モニタリング

を提供します。1 つの DIVArchive オブジェクトにつき 1 つのファイルまたは複数のファイル (FTP フォルダ内) がサポートされています。新しいファイル (または FTP フォルダ) が識別されると、DFM は DIVArchive にアーカイブリクエストを自動的に発行して、その新しいファイルまたはフォルダをアーカイブします。これらのファイルは、正常にアーカイブされると、ソースから自動的に削除されます。

1.1.7. DIVArchive SNMP

DIVArchive Simple Network Management Protocol (SNMP) エージェントおよび管理情報ベース (MIB) は、SNMP プロトコル経由でサードパーティーのモニタリングアプリケーションを通じて DIVArchive とそのサブシステムのステータスとアクティビティーのモニタリングをサポートします。

1.1.8. DIVArchive SPM

DIVArchive Storage Plan Manager (SPM) は、SPM 構成で定義された規則とポリシーに基づいてアーカイブ内の資料の自動移行およびライフサイクルを提供します。

SPM コンポーネントは、(ディスク容量のウォーターマークに基づいて) SPM で管理されたアレイからの資料の削除をトリガーするためにも使用されます。

1.1.9. DIVArchive 移行サービス

DIVArchive には組み込み移行サービスが含まれています。これは、DIVArchive システムの内側でさまざまなメディアからメディアにコンテンツを移行するジョブをスケジュールして実行するのに役立つ、(DIVArchive にとって) 新しい個別の内部サービスです。Control GUI またはコマンド行クライアントを使用できます。

1.1.10. DIVArchive VACP

VACP (Video Archive Command Protocol) は、Archive システムとのインタフェース用に Harris Automation 社によって開発されたプロトコルです。DIVArchive には DIVArchive Manager と通信するための独自の API がありますが、VACP との互換性はありません。

1.1.11. DIVArchive Control GUI

DIVArchive Control GUI (グラフィカルユーザーインタフェース) は、DIVArchive での操作をモニター、制御、および管理するために使用されます。いくつかの DIVArchive GUI を同時に実行して同じ DIVArchive システムに接続できます。

1.1.12. DIVArchive 構成ユーティリティー

DIVArchive 構成ユーティリティーは、DIVArchive システムを構成するために使用されます。主に DIVArchive の構成に使用されますが、この構成ユーティリティーからいくつかの操作機能を実行することもできます。

1.1.13. DIVArchive Access Gateway

Access Gateway では、1 台のコンピュータから複数の独立した DIVArchive システムの運用や対話型操作を行えます。これはコンテンツ配信のグローバルソリューションです。ミラーサイトへの自動ファイルレプリケーションは、ローカルでの配信、バックアップ、およびセキュリティーが確保された障害回復、帯域幅制御、そしてチェックサム検証の単純かつ簡単な方法を提供します。ネットワークがモニターされ、DIVAnet によってコンテンツの完全な配信が確保されます。

1.1.14. DIVArchive Lynx のローカル削除

LYNXLocalDelete は、1 つのローカル DIVArchive システム (LYNXlocal など) と 1 つ (または複数) のリモート DIVArchive システム (LYNXdr など) の間のオブジェクトレプリケーション機能をモニターするサービスです。リモート DIVArchive システムに正常にレプリケートされたオブジェクトには、ローカル DIVArchive システムから削除可能であるとしてフラグが付けられます。

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 DIVArchive 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

DIVArchive では、次の TCP/IP ポートを使用します。

- tcp/8500 は DIVArchive Robot Manager によって使用されます

- tcp/9000 は DIVArchive Manager によって使用されます
- tcp/9300 は DIVArchive バックアップサービスによって使用されます
- tcp/9500 は DIVArchive Access Gateway によって使用されます
- tcp/9900 は DIVArchive Actor によって使用されます
- tcp/9191 は DIVArchive 移行サービスによって使用されます

1.2.3. DIVA ユーザーとして可能なかぎり最小特権の原則を使用する

DIVArchive サービスはすべて DIVA ユーザーとして実行されます。DIVArchive Control GUI には 3 つの固定ユーザープロファイル (Administrator、Operator、および User) が備わっています。Administrator および Operator アカウントでアクセスできるようにするにはパスワードが必要です。DIVArchive システムのインストール時のデフォルトのパスワードは、DIVArchive 構成ユーティリティーを使用していつでも変更できます。デフォルトのパスワードを変更しないと、DIVArchive システムが悪質なアクティビティー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 Administrator と Operator の両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) に格納し、必要に応じて Oracle サポートで入手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ーをモニターする

システムアクティビティーをモニターして、DIVArchive 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してください。/Program/log/ 下のインストールディレクトリ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

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

2

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。

DIVArchive 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

DIVArchive システムの構築に使用されるデータディスクおよびキャッシュディスクのリソースがあります。それらは通常、DIVArchive 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 (DIVArchive 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、メタデータディスク、バックアップディスク

複雑なオブジェクトを含む DIVArchive システムの構築に使用されるデータベースディスク、メタデータディスク、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、DIVArchive 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 (DIVArchive 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 テープ

通常は DIVArchive システムによって制御されるテープライブラリ内にある、データが書き込まれるテープに単独でアクセスを許すことは、セキュリティー上のリスクになります。

2.1.1.4. テープメタデータのエクスポート

エクスポート操作から作成されるテープメタデータダンプには、データとメタデータが含まれています。定期的なエクスポートまたはインポートアクティビティーの実行中は、OS 管理者以外がこのデータとメタデータにアクセスできないようにするべきです。

2.1.1.5. 構成ファイルおよび設定

DIVArchive システムの構成設定は、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、セキュリティー上のリスクが生じることに注意してください。

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 DIVArchive 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。

2.2. 推奨される配備トポロジ

このセクションでは、インフラストラクチャーコンポーネントをセキュアにインストールして構成する方法について説明します。DIVArchive のインストールについては、次にある DIVArchive ソフトウェアリリース 7.3 のカスタマドキュメントライブラリを参照してください。

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

DIVArchive 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. 個別のメタデータネットワーク

DIVArchive サービスのコンポーネント間の相互接続、Metadata Database への接続、およびそのクライアントからの接続では、どの WAN にも接続されていない個別の TCP/IP ネットワークおよびスイッチハードウェアを用意します。メタデータトラフィックは TCP/IP を使用して実装されるため、このトラフィックに対する外部の攻撃が理論的には可能です。個別のメタデータネットワークを構成すると、このリスクが軽減されるだけでなく、パフォーマンスも向上します。個別のネットワークを実現できない場合は、少なくとも、外部の WAN や、ネットワーク上の信頼できないホストから DIVArchive ポートへのトラフィックを拒否してください。「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」を参照してください。

2.2.2. FC ゾーニング

FC ゾーニングを使用すると、ディスクへのアクセスを必要としないサーバーからファイバチャネル経由で接続された DIVArchive ディスクへのアクセスを拒否できます。できれば、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してください。

2.2.3. SAN ディスクの構成アクセスの保護

通常、SAN RAID ディスクには、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てください。

2.2.4. DIVArchive パッケージのインストール

最初に、必要な DIVArchive サービスのみをインストールします。たとえば、GUI または構成ユーティリティーをシステムから実行する予定がない場合は、インストール時にインストール対象のコンポーネントのリストでそれらのチェックマークを外します。DIVArchive 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の、インストール後の変更は、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。

2.2.5. DIVArchive テープのセキュリティー

DIVArchive システムによって制御されるテープライブラリの内部で DIVArchive テープへの外部アクセスが行われないようにします。DIVArchive テープへの未承認のアクセスによって、ユーザーデータが危険にさらされたり、破棄されたりする場合があります。

2.2.6. バックアップ

DIVArchive バックアップサービスを使用して、データベースのバックアップを設定および実行します。バックアップダンプへのアクセスを OS レベルの管理者ユーザーのみに制限します。

2.3. インストール後の構成

いずれかの DIVArchive をインストールしたら、付録A「*セキュアな配備のためのチェックリスト*」にあるセキュリティーのチェックリストに従ってください。

3

第3章 セキュリティー機能

潜在的なセキュリティーの脅威を回避するには、DIVArchive 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。

3.2. 認証

DIVArchive Control GUI には 3 つの固定ユーザープロファイル (Administrator、Operator、および User) が備わっています。Administrator および Operator アカウントでアクセスできるようにするにはパスワードが必要です。DIVArchive システムのインストール時のデフォルトのパスワードは、DIVArchive 構成ユーティリティーを通じていつでも変更できます。デフォルトのパスワードを変更しないと、DIVArchive システムが悪質なアクティビティー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 Administrator と Operator の両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) に格納し、必要に応じて Oracle サポートで入手できるようにする必要があります。**

3.3. アクセス制御

DIVArchive のアクセス制御は 3 つのプロファイルに分類されます。

User - DIVArchive Manager への接続が確立されたあと、ユーザーは Control GUI で DIVArchive 操作をモニターしたり、データベースからデータを取得したりすることのみ可能です。これは User プロファイルと呼ばれます。User プロファイルモード中は、DIVArchive にコマンドを発行するすべての機能にアクセスできません。これは、モニタリングは必要だが DIVArchive へのコマンドの送信は許可されないという状況を考慮しています。

Administrator - アーカイブや復元などのリクエストを DIVArchive に発行したり、ライブラリからテープを取り出したりするには、Administrator プロファイルに変更する必要があります。Administrator プロファイルはパスワードで保護されています。このプロファイルのデフォルトのパスワードは diva ですが、構成ユーティリティーで変更できます (変更されている可能性があります)。詳細は、次にある DIVArchive ソフトウェアリリース 7.3 のカスタマドキュメントライブラリを参照してください。

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

Operator - Operator プロファイルは、User プロファイルのアクセス権に加えてオブジェクト転送ユーティリティーにもアクセスでき、Administrator プロファイルと同じパスワードの入力が必要です。

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. DIVArchive 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 および他のすべての OS アカウント (次のものを含む) に対して強力なパスワードを設定します。
   - DIVA、Oracle ユーザー ID (使用されている場合)
   - すべてのディスクアレイ管理アカウント
2. ローカル管理者の OS アカウントを使用せず、必要に応じて他のユーザーアカウントにロールを割り当てます。
3. Control GUI の Administrator および Operator 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、構成ユーティリティーの「Tools」から実行できます。
4. Oracle データベースへのログイン用に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設定から、Oracle データベースユーザーのデフォルトパスワードを変更してください。
5. ファイアウォールをすべてのシステムにインストールし、デフォルトの DIVArchive ポート規則を適用します。DIVArchive API (tcp 9000) へのアクセスを、ファイアウォール規則を使用してアクセスする必要がある IP に制限します。
6. セキュリティー更新が含まれているため、OS と DIVArchive の更新を定期的にインストールします。
7. 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 DIVArchive のプロセスおよびストレージを除外します。
8. FC ディスクと FC テープドライブを物理的に、または FC ゾーニングによって分離し、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のが最良の方法です。管理対象のディスクでは、DIVArchive Actor のみがディスクに (テープドライブにも) アクセスできるようにするべきです。このセキュリティー対策は、テープまたはディスクの誤った上書きによって発生するデータ損失を防止するのに役立ちます。
9. DIVArchive の構成およびデータベースの適切なバックアップセットを設定します。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の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、DIVArchive のテープおよびディスクと同程度に保護する必要があります。