

Oracle® DIVArchive

セキュリティーガイド

リリース 7.5

E86536-01

2016 年 11 月

Copyright © 2016, 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は、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場合、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に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. Oracle DIVArchive Manager	7
1.1.2. Oracle DIVArchiveActor	7
1.1.3. DIVArchive Robot Manager	7
1.1.4. DIVArchive バックアップサービス	8
1.1.5. Oracle DIVArchive Avid の接続	8
1.1.6. DIVArchive Drop Folder Monitor (DFM)	9
1.1.7. DIVArchive SNMP	9
1.1.8. DIVArchive Storage Plan Manager (SPM)	9
1.1.9. DIVArchive 移行サービス	9
1.1.10. DIVArchive VACP	9
1.1.11. DIVArchive Control GUI	10
1.1.12. DIVArchive 構成ユーティリティ	10
1.1.13. DIVArchive Access Gateway	10
1.1.14. DIVArchive ローカル削除	10
1.2. 一般的なセキュリティ原則	10
1.2.1. ソフトウェアを最新に維持する	10
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	11
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	11
1.2.4. システムアクティビティのモニター	11
1.2.5. セキュリティ情報を最新に維持する	12

2. セキュアなインストール	13
2.1. 環境を理解する	13
2.1.1. 保護する必要があるリソースはどれか	13
2.1.1.1. プライマリデータディスク	13
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	13
2.1.1.3. DIVArchive テープ	14
2.1.1.4. テープメタデータのエクスポート	14
2.1.1.5. 構成ファイルおよび設定	14
2.1.2. だれからリソースを保護するか	14
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	14
2.2. 推奨される配備トポロジ	15
2.2.1. 個別のメタデータネットワーク	15
2.2.2. FC ゾーニング	15
2.2.3. SAN ディスクの構成アクセスの保護	15
2.2.4. DIVArchive パッケージのインストール	15
2.2.5. DIVArchive テープのセキュリティー	16
2.2.6. バックアップ	16
2.3. インストール後の構成	16
3. セキュリティー機能	17
3.1. セキュリティーモデル	17
3.2. 認証	17
3.3. アクセス制御	17
A. セキュアな配備のためのチェックリスト	19

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。

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

Oracle 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. Oracle 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、イニシエータアプリケーションによって DIVArchive クライアント API を介して送信されます。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 7.4 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. Oracle DIVArchiveActor

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。単一の DIVArchive Manager は、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 Fibre 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の「Manager 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 7.4 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 DIVArchive Avid の接続

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 (DFM)

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のモニタリングをサポートします。DIVArchive SNMP は Windows 環境でのみサポートされています。

1.1.8. DIVArchive Storage Plan Manager (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ーフェース) を使用して、DIVArchive での操作をモニター、制御、および管理します。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

DIVArchive 構成ユーティリティを使用して、DIVArchive システムを構成します。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 ローカル削除

ローカル削除は、1 つのローカル DIVArchive システム (DIVAlocal など) と 1 つ (または複数) のリモート DIVArchive システム (DIVAdr 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

DIVArchive では、次の TCP/IP ポートを使用します。

- DIVArchive Robot Manager は *tcp/8500* を使用します
- DIVArchive Manager は *tcp/9000* を使用します
- DIVArchive バックアップサービスは *tcp/9300* を使用します
- DIVArchive Access Gateway は *tcp/9500* を使用します
- DIVArchiveActor は *tcp/9900* を使用します。
- DIVArchive 移行サービスは *tcp/9191* を使用します

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

Administrator (または Root) オペレーティングシステムユーザーアカウントを使用して DIVArchive サービスを実行しないでください。DIVA という専用のオペレーティングシステムユーザー (またはグループ) を使用してすべての DIVArchive サービスを実行する必要があります。

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) が用意されています。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。これらのプロファイルを使用する前に、構成ユーティリティーで Administrator および (または) Operator のパスワードを割り当てる必要があります。

Administrator アカウントと Operator アカウントの両方のインストールおよび構成時にパスワードを作成します。パスワードは 180 日ごと (最小) に変更する必要があります。必要に応じて、パスワードは Oracle サポートが使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のモニター

システムアクティビティをモニターして、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、DIVArchive 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。

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。このデータとメタデータへのアクセス権は、ルーチンのエクスポートまたはインポートアクティビティー時に、Administrator (または Root) オペレーティングシステムアカウントまたは DIVA オペレーティングシステムユーザー (またはグループ) にのみ制限する必要があります。

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、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。管理者以外のオペレーティングシステムユーザーに対して、構成ファイルを書き込み可能にすることはセキュリティーリスクになるため、これらのファイルのアクセス権は、Administrator (または Root) オペレーティングシステムアカウントまたは DIVA オペレーティングシステムユーザー (またはグループ) にのみ制限する必要があります。

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されているリソースは、構成された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 ファブリックを介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 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 7.4 のカスタム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 ゾーニングを使用して、ファイバチャネルを介して接続された DIVArchive 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。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

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で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。

2.2.4. 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。デフォルトの DIVArchive インストールディレクトリのアクセス権と所有者は、Administrator (または Root) アカウントまたは DIVA オペレーティングシステムユーザー (またはグループ) にのみ制限する必要があります。

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権は、Administrator (または Root) オペレーティングシステムアカウントまたは DIVA オペレーティングシステムユーザー (またはグループ) のみに制限する必要があります。

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。

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、User) が用意されています。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。これらのプロファイルを使用する前に、構成ユーティリティーで Administrator および (または) Operator のパスワードを割り当てる必要があります。

Administrator および Operator アカウントのパスワードは両方とも 180 日 (以内) ごとに変更する必要があります。必要に応じて、パスワードは Oracle サポートが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

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。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。

これらのプロファイルを使用する前に、構成ユーティリティーで Administrator および (または) Operator アカウントのパスワードを割り当てる必要があります。

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では、DIVArchive にコマンドを発行するすべての関数にアクセスできるのではなく、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可能にしています。

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。このプロファイルを使用する前に、構成ユーティリティーでこのプロファイルのパスワードが割り当てられている必要があります。詳細は、次の場所にある Oracle DIVArchive 7.4 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 および Advanced 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、プロファイルを使用する前に、構成ユーティリティーでパスワードが構成されている必要があります。Control GUI の Operator プロファイルと Advanced Operator プロファイルで、リクエストの優先順位のキャンセルと変更の権限をオプションで有効にできるようになりました。オプションは構成ユーティリティーの「Manager Configuration」パネルに定義されています。デフォルトで、このオプションは無効になっています。

付録A セキュアな配備のためのチェックリスト

1. DIVArchive の管理者役割またはサービス役割が割り当てられている Administrator (または Root) およびほかのすべてのオペレーティングシステムアカウント (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は使用しないでください。必要に応じてほかのユーザーアカウントに役割を割り当てます。
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。これらのプロファイルを使用する前に、構成ユーティリティでそれらのパスワードを割り当てる必要があります。
4. Oracle データベースログインのための強力なパスワードを設定します。
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. オペレーティングシステムおよび DIVArchive の更新を定期的にインストールします (セキュリティアップデートが含まれているため)。
7. ウィルス対策機能をインストールしますが、DIVArchive のプロセスおよびストレージを除外します (パフォーマンス上の理由で)。
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 のみがディスクおよびテープドライブにアクセスできるようにするべきです。このセキュリティ対策は、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の一部であり、誤って、または何らかの侵害のタイプ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

フサイトの場所に転送している間、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。