Oracle® Solaris Cluster 4.3 セキュリティーガイド

Part No: E62324
2015 年 10 月

ORACLE

Part No: E62324

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。

目次

このドキュメントの使用法

- **概要** – Oracle Solaris Cluster のセキュリティーの概要、セキュアなインストールと構成に関する情報、セキュリティー機能、および開発者向けのセキュリティーの考慮事項について説明します。
- **対象読者** – 技術者、システム管理者、および認定サービスプロバイダ
- **前提知識** – ハードウェアのトラブルシューティングや交換に関する豊富な経験

製品ドキュメントライブラリ

この製品および関連製品のドキュメントとリソースは http://www.oracle.com/pls/topic/lookup?ctx=E62281 で入手可能です。

フィードバック

このドキュメントに関するフィードバックを http://www.oracle.com/goto/docfeedback からお聞かせください。

♦ ♦ ♦ 第 1 章

1 Oracle Solaris Cluster セキュリティーの概要

Oracle Solaris Cluster 製品は、高可用性サービスおよびスケーラブルなサービスの作成に使用できる統合されたハードウェアおよびソフトウェアソリューションです。このガイドでは、Oracle Solaris Cluster のセキュリティーの概要、セキュアなインストールと構成に関する情報、セキュリティー機能、および開発者向けのセキュリティーの考慮事項について説明します。このドキュメントと Oracle Solaris Cluster のマニュアルセット全体を使用して、Oracle Solaris Cluster ソフトウェアの全体像が提供されます。

Geographic Edition ソフトウェアは、Oracle Solaris Cluster ソフトウェアの階層化された拡張です。Geographic Edition フレームワークは、地理的に長距離を隔てられた複数のクラスタを使用することによる予期しない障害からアプリケーションを保護します。これらのクラスタには、クラスタ間でレプリケートされたデータを管理する Geographic Edition インフラストラクチャーのコピーが含まれます。

この章で説明する内容は次のとおりです。

Oracle Solaris オペレーティングシステム (OS) のセキュリティーの詳細は、『Oracle Solaris 11 セキュリティーと強化ガイドライン 』および『Oracle Solaris 11.3 でのシステムおよび接続されたデバイスのセキュリティー保護 』を参照してください。

Oracle Solaris Cluster とセキュリティーの概要

Oracle Solaris Cluster 環境は、Oracle Solaris オペレーティングシステムをクラスタオペレーティングシステムに拡張します。クラスタは 1 つ以上のノードのコレクションで、各ノードはこのコレクションに排他的に属しています。

Oracle Solaris Cluster ソフトウェアには、次のような利点があります。

- ソフトウェアやハードウェアの障害によるシステムの停止時間が削減される
- 通常はシングルサーバーシステムが停止してしまうような障害が発生しても、エンドユーザーがデータやアプリケーションを使用できる
- クラスタにノードを追加して負荷を分散することで、追加のプロセッサに合わせてサービスを拡張できるため、アプリケーションのスループットが向上する
- クラスタ全体を停止しなくても保守を行うことができるため、システムの可用性が向上する

クラスタは従来のシングルサーバーシステムと比較して複数のメリットを提供します。これらのメリットには、フェイルオーバーとスケーラブルサービスのサポート、モジュール化成長機能、ノードに対する負荷制限の設定機能、従来のハードウェア耐障害性システムに比べて低いエントリ価格などが含まれます。

Oracle Solaris OS で実行されるクラスタのタイプには、*グローバルクラスタ*と*ゾーンクラスタ*があります。クラスタはグローバルクラスタ、ゾーンクラスタ、または両方の組み合わせに指定できます。ゾーンクラスタの構成による利点の詳細は、『Oracle Solaris Cluster 4.3 Concepts Guide 』を参照してください。

Geographic Edition およびセキュリティーの概要

Geographic Edition ソフトウェアは、Oracle Solaris Cluster ソフトウェアの階層化された拡張です。データレプリケーションソフトウェアを使用すると、Geographic Edition クラスタで実行されているアプリケーションは、地理的に離れたセカンダリクラスタにサービスを移行することで障害に対応できます。地震、火災、暴雨などの災害によって、プライマリサイトのクラスタが無効になることがあります。

障害が発生した場合、Geographic Edition クラスタは、次のレベルの冗長性を使用することでサービスを引き続き提供できます。

- セカンダリクラスタ
- セカンダリクラスタに複製されたアプリケーション構成
- セカンダリクラスタにレプリケートされたデータ

Geographic Edition ソフトウェアは、サイト間でサービスを移行することで、地理的に離れたクラスタを管理および構成するための一連のツールを備えています。クラスタはグローバルクラスタ、ゾーンクラスタ、または両方の組み合わせに指定できます。Geographic Edition ソフトウェアは、堅牢なセキュリティー、アプリケーションサービスの移行、およびデータレプリケーションによってエンタープライズシステム全体の障害に対応することで、複数の物理的な場所で可用性を管理できます。

一般的なセキュリティーの原則

Oracle Solaris Cluster アプリケーションをセキュアに使うために、次の原則が重要になります。

- ソフトウェアを最新の状態に維持します
- 重要なサービスへのネットワークアクセスを制限します
- 最少特権の原則に従います
- システムの動作状態をモニターします
- Oracle の最新のセキュリティー情報を入手します

Oracle Solaris Cluster のセキュアなインストールおよび構成

このセクションでは、Oracle Solaris Cluster のセキュアなインストールと構成を計画して実行するためのリンクを示します。

- **インストール** – Oracle Solaris 11 Automated Installer (AI) を使用すると Oracle Solaris Cluster ソフトウェアをインストールできます。詳細は、『Oracle Solaris Cluster 4.3 ソフトウェアのインストール 』の「ソフトウェアのインストール」を参照してください。
- **クラスタパッケージ** – Oracle Solaris Cluster パッケージでは Oracle Solaris Image Packaging System (IPS) のパッケージ名を使用します。

  Oracle Solaris Cluster コア、データサービス、および Geographic Edition パッケージのリストを確認するには、『Oracle Solaris Cluster 4.3 Package Group Lists 』を参照してください。
- **構成** – グローバルクラスタとゾーンクラスタを構成して管理できます。詳細は、『Oracle Solaris Cluster 4.3 ソフトウェアのインストール 』の第 3 章「グローバルクラスタの確立」、『Oracle Solaris Cluster 4.3 ソフトウェアのインストール 』の第 6 章「ゾーンクラスタの作成」、および『Oracle Solaris Cluster 4.3 システム管理 』の第 1 章「Oracle Solaris Cluster の管理の概要」を参照してください。

  グローバルクラスタノードを確立するためのすべての方法について、1 つの指定スポンサーノードの事前の承認が必要です。それにより、指定されたシステムのみが構成するノードへのアクセスを許可されます。必要に応じて、よりセキュアな構成には DES 暗号化を使用できます。詳細は、`clauth`(1CL) のマニュアルページを参照してください。
- **共通エージェントコンテナの脆弱性** – 共通エージェントコンテナといくつかの古い Java バージョンの組み合わせでは、Oracle Solaris Cluster ソフトウェアにセキュリティーの脆弱性が生じます。使用しているシステムにこの脆弱性があるかどうかを識別する方法、およびの修正方法の詳細は、My Oracle Support の参照ドキュメント『CVE-2014-3566 Oracle Solaris Cluster で SSL v3.0 の脆弱性 (別名「プードル攻撃」) を軽減するための手順 (Doc ID 1999997.1)』(`https://support.oracle.com/epmos/faces/DocumentDisplay?id=1999997.1&displayIndex=1`) を参照してください。このドキュメントには My Oracle Support のログインが必要です。

- **Kerberos V5 でセキュリティー保護された HA for NFS** – HA for NFS データサービスで管理されている NFS サービスへのアクセスをセキュリティー保護する必要がある場合は、HA for NFS データサービスをセキュリティー保護するように Kerberos V5 クライアントを構成できます。これには、すべてのクラスタノード上の論理ホスト名における NFS のための Kerberos 主体の追加が含まれます。詳細は、『Oracle Solaris Cluster Data Service for NFS Guide 』の「Securing HA for NFS With Kerberos V5」を参照してください。

Geographic Edition のセキュアなインストールおよび構成

このセクションには、Geographic Edition ソフトウェアのセキュアなインストールと構成を計画して実行するためのリンクを示します。

- **インストール** – Geographic Edition ソフトウェアは、Oracle Solaris オペレーティングシステムおよび Oracle Solaris Cluster ソフトウェアを実行しているクラスタにインストールする必要があります。Oracle Solaris Automated Installer (AI) を使用して、Oracle Solaris Cluster ソフトウェアのインストールと同時に、またはあとから任意の時点で Geographic Edition ソフトウェアをインストールします。Geographic Edition フレームワーク構成は Oracle Solaris Cluster ソフトウェア構成と同一です。『Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide 』の第 2 章「Installing and Configuring the Geographic Edition Software」を参照してください。
- **Geographic Edition パッケージ** – Geographic Edition パッケージでは Oracle Solaris Image Packaging System (IPS) のパッケージ名を使用します。パッケージのリストを確認するには、『Oracle Solaris Cluster 4.3 Package Group Lists 』を参照してください。
- **構成** – どのノードやクラスタでも障害を発生させずに、Geographic Edition フレームワークを実行しているクラスタですべての管理タスクを実行できます。稼働しているクラスタで Geographic Edition ソフトウェアをインストール、構成、起動、使用、停止、およびアンインストールできます。『Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide 』の第 4 章「Administering RBAC」を参照してください。

Oracle Solaris Cluster のセキュリティー機能

このセクションでは、Oracle Solaris Cluster が提供する具体的なセキュリティーメカニズムについて説明します。

セキュアなインストールを行うには、次のクリティカルなセキュリティー機能を使用します。

- **役割に基づくアクセス制御 (RBAC)** – クラスタにアクセスするには、RBAC 承認 `solaris.cluster.modify`、`solaris.cluster.admin`、および `solaris.cluster.read` を使用します。役割のほとんどのセキュリティー属性を変更するには、User Security 権利プ

ロファイルが割り当てられている管理者になる必要があります。詳細は、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護 』の「権利使用の管理」および『Oracle Solaris Cluster 4.3 システム管理 』の「Oracle Solaris Cluster RBAC の権利プロファイル」を参照してください。

- **新しいノード** – クラスタにノードを追加するには、権限のある `claccess` コマンドまたは `clsetup` ユーティリティーを使用します。詳細は、『Oracle Solaris Cluster 4.3 システム管理 』の第 8 章「クラスタノードの管理」を参照してください。

  アクセスステータスのデフォルト設定は `claccess deny-all` です。この設定を変更するのは、新しいノードの追加など、特権付きの操作を実行する場合のみです。操作を終了したら `deny-all` ステータスを元に戻す必要があります。クラスタ構成を頻繁に変更することが予想される場合は、`/usr/cluster/bin/claccess -p protocol=authentication-protocol` コマンドを使用してよりセキュアな認証プロトコルを選択することで、新しいシステムの信頼を最大限に確保できます。詳細は、`claccess`(1CL) のマニュアルページおよび『Oracle Solaris 11.3 での Kerberos およびその他の認証サービスの管理 』の第 10 章「ネットワークサービスの認証の構成」を参照してください。

- **Trusted Extensions** – Oracle Solaris Trusted Extensions 機能はゾーンクラスタで使用するように設定できます。詳細は、『Oracle Solaris Cluster 4.3 ソフトウェアのインストール 』の「ゾーンクラスタにおける Trusted Extensions のガイドライン」および『Oracle Solaris Cluster 4.3 ソフトウェアのインストール 』の「Trusted Extensions をインストールおよび構成する方法」を参照してください。

- **ゾーンクラスタ** – ゾーンクラスタは、`cluster` 属性が設定された `solaris` ブランド、`solaris10` ブランド、または `labeled` ブランドの 1 つ以上の非大域ゾーンで構成されます。`labeled` ブランドゾーンクラスタは、Oracle Solaris ソフトウェアの Trusted Extensions でのみ使用します。

  `clzonecluster` コマンドまたは `clsetup` ユーティリティーを使用して、ゾーンクラスタを作成します。Oracle Solaris ゾーンで提供される分離を含めて、グローバルクラスタと同様にゾーンクラスタでサポートされるサービスを実行できます。詳細は、『Oracle Solaris Cluster 4.3 ソフトウェアのインストール 』の「ゾーンクラスタの作成および構成」および『Oracle Solaris Cluster 4.3 システム管理 』の「ゾーンクラスタに関する作業」を参照してください。

- **クラスタコンソールへのセキュア接続** – クラスタノードのコンソールにはセキュアシェル接続を確立する必要があります。`pconsole` ユーティリティーの詳細は、『Oracle Solaris Cluster 4.3 システム管理 』の「クラスタコンソールに安全に接続する方法」を参照してください。

- **共通エージェントコンテナ** – Oracle Solaris Cluster Manager GUI は強力な暗号化技術を使用して、各クラスタノード上にある Oracle Solaris Cluster 管理スタック間の通信をセキュリティー保護します。詳細は、『Oracle Solaris Cluster 4.3 システム管理 』の「Oracle Solaris Cluster Manager のトラブルシューティング」を参照してください。

- **ロギング** – Oracle Solaris Cluster ソフトウェアでは、`syslogd` コマンドを使用して、エラーメッセージおよびステータスメッセージを記録します。メッセージの格納場所を制御する `/etc/syslog.conf` ファイルを必ず設定してください。また、`/var/adm/messages` ファイルなどのログファイルのセキュリティー保護も必要です。詳細は、『Oracle Solaris Cluster 4.3 システム管理 』の「クラスタの管理」を参照してください。

- **監査** – Oracle Solaris Cluster は、Oracle Solaris OS に配置されていれば、デフォルトで有効になっています。監査機能によって、実行されたすべてのコマンドが `/var/cluster/logs/commandlog` ファイルに保存されます。このファイルは必要に応じて保護設定する必要があります。詳細は、『Oracle Solaris Cluster 4.3 システム管理 』の「Oracle Solaris Cluster のコマンドログの内容を表示する方法」を参照してください。
- **Oracle Solaris OS の強化** – Oracle Solaris Cluster はセキュリティー強化技術を使用して Oracle Solaris OS を強化された状態に再構成します。さらに、Oracle Solaris システムの監査をアクティブ化できます。

Geographic Edition のセキュリティー機能

このセクションでは、Geographic Edition が提供する具体的なセキュリティーメカニズムについて説明します。

セキュアなインストールを行うには、次のクリティカルなセキュリティー機能を使用します。

- **役割に基づくアクセス制御 (RBAC)** – Geographic Edition ソフトウェアの RBAC プロファイルは、Oracle Solaris Cluster ソフトウェアで使用される RBAC 権利プロファイルに基づいています。役割のほとんどのセキュリティー属性を変更するには、User Security 権利プロファイルが割り当てられている管理者になる必要があります。root 役割を想定し、RBAC 役割 `solaris.cluster.geo.modify`、`solaris.cluster.geo.admin`、および `solaris.cluster.geo.read` を使用してクラスタにアクセスします。詳細は、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護 』および『Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide 』の「Modifying a User's RBAC Properties」を参照してください。
- **セキュリティー証明書** – インストール中に、セキュリティー証明書を使用してセキュアなクラスタ通信のためにクラスタが構成されます (同じクラスタ内のノードは同じセキュリティー証明書を共有する必要があります)。Geographic Edition パートナーシップでのクラスタ間の通信は、セキュリティー証明書を使用して、Secure Sockets Layer (SSL) で Java Management Extensions (JMX) ポートを経由することでセキュリティー保護されます。詳細は、『Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide 』の「Configuring Trust Between Partner Clusters」を参照してください。
- **共通エージェントコンテナ** – ゾーンクラスタが Oracle Solaris Cluster パートナーシップのメンバーとして機能できるには、共通エージェントコンテナをゾーンクラスタ内で手動で構成する必要があります。詳細は、『Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide 』の「Preparing a Zone Cluster for Partner Membership」を参照してください。
- **IP Security Architecture (IPsec)** – IPsec を使用して、パートナークラスタ間のセキュアな TCP/UDP ハートビート通信を構成します。詳細は、『Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide 』の「Securing Inter-Cluster Communication」を参照してください。

開発者向けのセキュリティーの考慮事項

このセクションでは、Oracle Solaris Cluster を使用してアプリケーションを作成する開発者にとって役立つ情報を提供します。開発者は、Oracle Solaris Cluster API を使用します。詳細は、『Oracle Solaris Cluster 4.3 Concepts Guide 』の第 3 章「Key Concepts for System Administrators and Application Developers」を参照してください。

開発者が作成するエージェントアプリケーションは、製品のセキュリティーフレームワーク内で動作し、次のセキュリティー機能を考慮する必要があります。

- **エージェントコールバックメソッド** – Oracle Solaris Cluster は広範囲のアプリケーションエージェントをサポートしています。これらは一連のコールバックメソッドとして実装され、アプリケーションの起動、停止、プローブ、検証を制御します。`Start`、`Stop`、`Validate` などのコールバックメソッドは常に root として実行されます。これらの実行可能メソッドファイルに root ユーザー以外が書き込み可能な場合には脆弱性が発生し、非 root ユーザーがコールバックメソッドにコードを挿入することで、不正に権限を引き上げることが可能になってしまいます。Oracle Solaris Cluster はこうしたコールバックメソッドの実行可能ファイルの所有権とアクセス権をチェックします。このチェックは `resource_security` クラスタプロパティー設定によって制御されます。`resource_security` が `SECURE` に設定されており、メソッドコードに非 root ユーザーが書き込み可能であることが判明した場合、メソッドの実行は失敗します。

  一方、エージェントメソッドは、アプリケーション固有の管理コマンドなどの外部プログラムをしばしば実行します。エージェントメソッドはこうした外部プログラムをすべてラッパーを使用して実行することで、外部プログラムが可能なかぎり最小限の権限で実行されるようにする必要があります。Oracle Solaris Cluster では `application_user` および `resource_security` プロパティーと `scha_check_app_user` API が提供されており、アプリケーションがセキュアに実行されていることをデータサービスで確認できるようになっています。`scha_check_app_user` コマンドをスクリプトで呼び出すことで、構成済みの `Application_user` および `Resource_security` 設定に対してユーザー名を検証できます。詳細は、`scha_check_app_user`(1HA)、`r_properties`(5)、および `cluster`(1CL) のマニュアルページを参照してください。
- **アプリケーションへのセキュアなアクセス** – 管理コマンドまたは構成コマンドを発行する場合、アプリケーションへのセキュアなアクセスが必要になることがあります。このセキュアなアクセスは、Oracle Wallet Manager などの資格証明に基づくメソッドで実行する必要があります。パスワードを指定する必要がある場合、パスワードは不明瞭化されたフォームでセキュアに使用して格納する必要があります。たとえば、`ps` コマンドを使用してユーザーが表示できるコマンド行に渡すことはできません。Oracle Solaris Cluster では、プライベート文字列を作成するための `clpstring` コマンドが提供されています。このプライベート文字列は、エンコードされたパスワードをクラスタ内にセキュアに保存するために使用でき、管理タスクを実行するためにパスワードの使用が必要な場合に取得できます。このコマンドについては、`clpstring`(1CL) のマニュアルページを参照してください。

データサービスの開発時にこれらのセキュリティー機能を使用する方法については、『Oracle Solaris Cluster Data Services Developer's Guide 』を参照してください。

索引

L

O

P

R

T