StorageTek Automated Cartridge System Library Software

セキュリティーガイド

リリース 8.4

E68249-01

2015 年 9 月

ORACLE

StorageTek Automated Cartridge System Library Software
セキュリティーガイド

E68249-01

目次

はじめに

このドキュメントでは、Oracle の StorageTek Automated Cartridge System Library Software (ACSLS) および ACSLS High Availability の解決方法 (ACSLS HA) のセキュリティー機能について説明します。ACSLS HA および ACSLS SNMP エージェントは ACSLS サーバーでも動作するため、ACSLS サーバーを保護することで ACSLS、ACSLS HA、および ACSLS SNMP エージェントが保護されます。

対象読者

このガイドは、ACSLS 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

このセクションでは、ACSLS 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。

注:

このドキュメント全体を通して、Automated Cartridge System Library Software 製品を ACSLS と呼び、ACSLS High Availability の解決方法を ACSLS HA と呼んでいます。

製品の概要

ACSLS は、オープンシステムのクライアントで 1 つ以上 の StorageTek テープライブラリを制御する Oracle のテープライブラリサーバーソフトウェアです。ACS (Automated Cartridge System) は、PTP (Pass-Thru-Port) 経由で接続されたテープライブラリまたはテープライブラリのグループです。ACSLS は、ネットワークで送信される「control path」コマンドを使用して 1 つ以上の ACS を管理します。このソフトウェアには、システム管理コンポーネント、クライアントシステムアプリケーションへのインタフェース、およびライブラリ管理の機能が備わっています。

一般的なセキュリティー原則

すべての製品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に維持する

優れたセキュリティー実践の原則の 1 つは、すべてのソフトウェアバージョンとパッチを最新に維持することです。このドキュメントでは、ACSLS 8.4 以降のリリースを実行し、関連する保守を適用していることを前提としています。最新リリースの ACSLS を実行すれば、最新の拡張機能および修正が適用されていることが保証されます。

重要なセキュリティーパッチをすべて OS および OS とともにインストールされているサービスに適用します。利用可能なすべての更新を適用すると、ACSLS および ACSLS HA でテストされていない新しい機能や、場合によっては新しい OS リリースがインストールされる可能性があるため、これらのパッチは選択的に適用してください。

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

ACSLS と管理対象のライブラリは両方ともファイアウォールの内側に配備してください。ACSLS とテープライブラリ間の TCP/IP 通信には、プライベートネットワークを使用することをお勧めします。

最小特権の原則に従う

最小特権の原則は、ユーザーにはその業務を遂行するために必要な最小限の権限だけを与えるべきであるということを示しています。ユーザー権限を定期的に見直して、現在の職務責任に対して妥当であるか見極めてください。

ACSLS では、cmd_proc を使用して日常的なコマンドのみを発行するオペレータは acssa ユーザーとしてログインするべきであることを意味します。acsss ユーザーとしてログインするシステム管理者は、より広範囲のユーティリティーおよび構成コマンドにもアクセスできます。通常の操作を行うために、acsdb ユーザー ID を使用する必要はありません。

システムアクティビティーをモニターする

システムのセキュリティーは、有効なセキュリティープロトコル、適切なシステム構成、システムモニタリングの 3 つの柱に支えられています。監査を行い、監査レコードを確認することで、この 3 番目の要件に対応します。システム内の各コンポーネントはどれも、ある程度のモニタリング機能を備えています。このドキュメントの監査アドバイスに従って、監査レコードを定期的にモニターしてください。

セキュリティー情報を最新に維持する

Oracle では、ソフトウェアおよびドキュメントを絶えず改善しています。リリースごとにこのドキュメントのリビジョンを確認してください。

2

第2章 セキュアなインストール

このセクションでは、セキュアなインストールと構成の計画および実装プロセスについて説明し、ACSLS の推奨される導入トポロジーを紹介します。

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。

保護する必要があるリソースはどれか

ACSLS で管理される主要なリソースは、テープライブラリ、ドライブ、およびカートリッジです。悪意のあるアクセスだけでなく、不注意によるアクセスからも保護する必要があります。たとえば、別のサーバー上の ACSLS ユーザー ID には別のパスワードを使用することで、誤って別の ACSLS サーバーにログインしてしまうことを防ぎます。

だれからリソースを保護するか

内部と外部の両方の不正なアクセスからテープストレージのリソース保護する必要があります。

戦略的リソースの保護が失敗した場合に何が起こるか

ACSLS はテープドライブ上のカートリッジをマウントできます。ユーザーがデータパスからテープドライブに接続できる場合は、テープ上のデータが暗号化されていなければ、そのデータを読み取ることができます。

ACSLS とテープライブラリの両方にアクセスできるユーザーは、テープライブラリからカートリッジの挿入と取り出しを行うことができます。

ACSLS をセキュリティー保護するための推奨手順

ACSLS および必要なインフラストラクチャーコンポーネントをセキュリティー保護する際は、この手順に従って、変更後も引き続き ACSLS が機能するようにしてください。

- ACSLS をインストールします。
- ACSLS が正常に機能していることを検証します。ライブラリの構成と監査、テープのマウントとマウント解除、テープの挿入と取り出し、データベースのバックアップと復元が含まれます。
- セキュリティーが向上するように変更を実装します。
- ACSLS が引き続き正常に機能することを検証します。

ACSLS インターネット通信のセキュリティー保護

このセクションでは、インターネットアクセスをセキュリティー保護するために ACSLS を配備する際の推奨事項について説明します。

企業ファイアウォールの内側にある ACSLS およびテープライブラリをセキュリティー保護する

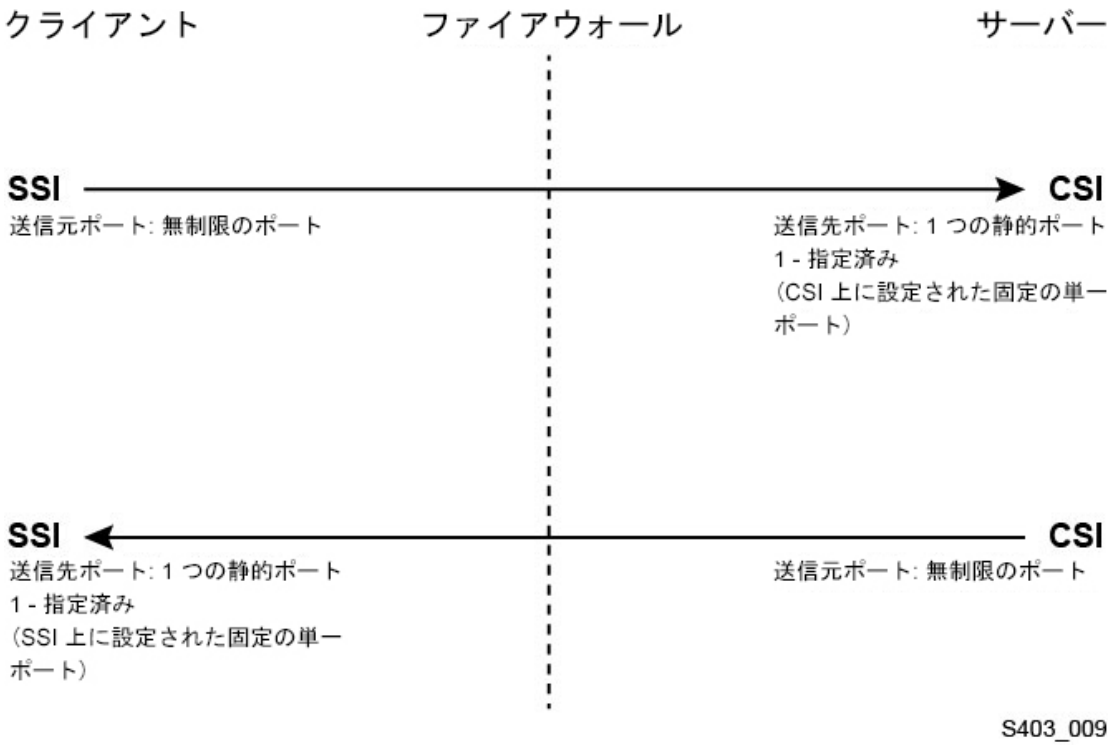
ACSLS およびサポート対象のテープライブラリは、企業ファイアウォールの内側に配備するようにしてください。リモートで作業しているユーザーが ACSLS サーバーにログインする必要がある場合は、VPN 経由でアクセスできます。

注:

IPv4 ベースのエッジファイアウォールを使用している場合は、インターネットホストが IPv6-over-IPv4 トンネル化トラフィックを使用して内部ホストにアクセスするのを防止するために、すべてのアウトバウンド IPv4 プロトコル 41 パケットと UDP ポート 3544 パケットをドロップするように構成します。

ACSLS ファイアウォールのセキュリティーオプション

テープのマウントおよびテープライブラリの管理に ACSLS を使用するクライアントアプリケーションがファイアウォールによって ACSLS から分離されている場合は、ファイアウォールのセキュリティーオプションを有効にすることをお勧めします。クライアントアプリケーションがファイアウォールによって ACSLS から分離されていない場合でも、ファイアウォールのセキュリティーオプションを実装すれば、次に示すように、ACSLS とそのクライアントアプリケーション間の通信に使用されるポートを制限することで、追加の ACSLS セキュリティーが提供されます。このような理由により、ACSLS 8.1 以降のリリースでは、CSI_FIREWALL_SECURE 静的変数のデフォルト値は TRUE に設定されています。



詳細については、『*ACSLS 管理者ガイド*』の付録「ファイアウォールのセキュリティーオプション」を参照してください。

ACSLS 通信に使用される Ethernet ポート

- ACSLS サーバーでは次のポートが使用されます。これらのポートへのトラフィックを許可するようにファイアウォールが構成されていることを確認します。これには、Solaris の ipfilter または Linux の iptables で実装されたファイアウォールも含まれていました。
  - 22 (双方向) - ssh アクセスで使用されます。
  - 111 (ポートマッパー) - ポートマッパーが無効になっていない場合に限ります。
  - 115 - SFTP (Secure File Transfer Protocol) で使用されます。
  - 161 - ACSLS SNMP エージェント (get/set/walk) 用のデフォルトポート。
  - 162 - ACSLS SNMP エージェント (トラップ) 用のデフォルトポート。

注:

ACSLS SNMP エージェントで使用されるポートは、*`AcslsAgtdSnmpConf [ -p port ] [-t trap port] [-d]`* コマンドで構成できます。*`-d`* オプションは、現在の設定を表示します。ポートの設定を変更したら、*`agentRegister`* コマンドを使用してエージェントを再起動する必要があります。

- 5432 - ACSLS から PostgreSQL データベース (アクセスユーザー ID 用の PGPORT 環境変数) への内部通信用のデフォルトポート。

  ポート 5432 が使用中の場合は、次に大きい空きポート番号が使用されます。

  注:

  ポート 5432 は、ローカルホスト (127.0.0.1) からアクセスできるだけで構いません。

- 7001 と 7002 - WebLogic および ACSLS GUI で使用されます。
- 30031 または ACSLS CSI の待機ポート - CSI_INET_PORT で設定されます。
- 50003 - ACSLS GUI および Java コンポーネントから旧バージョンの ACSLS 処理への内部通信で使用されるポート。これは構成できません。

- ACSAPI 経由で ACSLS と通信するクライアントアプリケーションの場合は、次のポートが開いている必要があります。
  - クライアントアプリケーションは、ACSLS CSI の待機ポートと通信できる必要があります。このデフォルト値は 30031 であり、CSI_INET_PORT 静的変数で設定されます。

    Unix シェルから次のコマンドを使用すると、ACSAPI クライアントからの要求を待機するために ACSLS で使用されているポートを検出できます。

    ```
    rpcinfo -p | egrep "300031 | 536871166"
    ```

    ポート ID は、表示の最終フィールドに一覧表示されます。
  - ACSAPI クライアント (NetBackup サーバーや SAM-QFS サーバーなど) は、SSI_INET_PORT 環境変数を使用して固定の受信ポートを設定します。1024 - 65535 の範囲内のポート (ポート 50001 と 50004 は除く) を指定します。ACSLS サーバーは、このポートと通信できる必要があります。

    注:

    ACSAPI クライアントサーバーでは、ミニイベントロガーへの AF_INET ドメインの IPC 通信およびクライアントアプリケーションから SSI への通信用に、ポート 50001 と 50004 が使用されます。

  クライアントアプリケーションと ACSLS 間の通信の詳細については、『*ACSLS 管理者ガイド*』のファイアウォールのセキュリティーオプションに関する付録を参照してください。

- XAPI コンポーネントがインストールされている場合、XAPI サーバーでは固定の待機ポートを使用して、ELS クライアントからの着信 TCP 要求を受信します。XAPI 待機ポートは、XAPI_PORT 静的変数で定義されます。XAPI_PORT のデフォルトは 50020 に設定さ

れます。これは 1024 - 65535 の間である必要があり、ACSLS またはほかのアプリケーションで使用されるほかのポートとは競合できません。

XAPI_PORT の詳細は、『*ACSLS 管理者ガイド*』の付録「XAPI クライアントインタフェース」を参照してください。この付録には、XAPI_PORT 静的変数を表示して設定する方法に関する詳細も記載されています。

- SL8500 または SL3000 ライブラリ上で開いている必要のあるポート:

  ACSLS は SL8500 または SL3000 ライブラリの 2A および 2B Ethernet 接続で、これらのポートと通信します。ACSLS からこれらのポートへの通信がブロックされている場合、ACSLS はライブラリを管理できません。

  - 50001 - ACSLS とライブラリの間のすべての通常の通信に使用されます
  - 50002 - 代替ノードへのフェイルオーバー前に代替の HA ノードがライブラリと通信できるかどうかを判断するために ACSLS HA で使用されます

ACSLS サーバーで動作しているファイアウォールの構成

Solaris の ipfilter または Linux の iptables を使用すれば、外部ファイアウォールに加えて、ファイアウォール保護も ACSLS サーバーに実装できます。ここでは、ACSLS サーバーで動作しているこれらのファイアウォールを管理する方法について説明します。

- Solaris での ipfilter の管理:

  詳細については、ipf および ipfilter のマニュアルページを参照してください。

  - ipfilter ファイアウォールは、「root」で次のコマンドを使用して有効化 (または無効化) します。

    ```
    svcadm enable ipfilter (svcadm disable ipfilter)
    ```

  - ipfilter の現在のステータスを確認するには:

    ```
    svcs ipfilter
    ```

  - ファイアウォールポリシーは、/etc/ipf/ipf.conf ファイルで定義されます

    ローカルホスト上のコンポーネント間 (ACSLS と WebLogic 間や GUI と ACSLS データベース間など) の自由な通信を許可するには、次のようなステートメントを追加します。

    ```
    pass in quick from 127.0.0.1 to 127.0.0.1
    ```

    または

```
pass in quick from 127.0.0.1 to all
```

ACSLS で必要なすべてのポートへのアクセスを許可するポリシーを定義する必要があります。たとえば、リモートの Web ベースブラウザによる ACSLS GIU へのアクセスを許可するポリシーを追加するには、ポート 7001 と 7002 を開く必要があります。

```
pass in quick from any to any port = 7001
```

```
pass in quick from any to any port = 7002
```

ACSAPI クライアントからの要求を待機するために ACSLS で使用されるポートを検出したあとに、これらの各ポートで「pass in quick」ステートメントを追加します。

RPC ポートマッパーポート 111 に「pass in quick」ステートメントを追加する必要がある場合もあります。

提示されたルールセットの最後のステートメント「block in from any」は、前のステートメントで特に許可されていないかぎり、どのトラフィックもホストに到達しないことを示しています。

- Linux での iptables の管理:
  - iptables ファイアウォールは、「root」で次のコマンドを使用して有効化 (または無効化) します。

    ```
    service iptables start (service iptables stop)
    ```
  - iptables のステータスを確認するには:

    ```
    service iptables status
    ```
  - iptables のポリシーファイルは /etc/sysconfig/iptables です。

    ACSLS で必要なすべてのポートへのアクセスを許可するポリシーを定義する必要があります。たとえば、ACSLS GIU へのリモート http/https アクセスを許可するポリシーを追加するには、次のようなステートメントを使用して、ポート 7001 と 7002 に例外が含まれるように、このファイルを更新するようにしてください。

    ```
    -A input -p tcp --dport 7001 -j ACCEPT
    ```

    ```
    -A input -p tcp --dport 7002 -j ACCEPT
    ```

ACSAPI クライアントからの要求を待機するために ACSLS で使用されるポートを検出したあとに、これらの各ポートで例外を iptables ポリシーファイルに追加する必要があります。RPC ポートマッパーポート 111 に例外ステートメントを追加する必要がある場合もあります。

Solaris のインストールと構成

このセクションでは、Solaris をセキュアにインストールおよび構成する方法について説明します。

提案事項:

- 重要なセキュリティーパッチをすべて OS および OS とともにインストールされているサービスに適用します。利用可能なすべての更新を適用すると、ACSLS および ACSLS HA でテストされていない新しい機能や、場合によっては新しい OS リリースがインストールされる可能性があるため、これらのパッチは選択的に適用してください。
- telnet と rlogin を無効にします。代わりに ssh を使用します。また、ftp を無効にして、代わりに sftp を使用します。

  root として次のコマンドを発行して、telnet、rlogin、および ftp サービスを無効にします。

  すべてのサービス確認するには:

  ```
  svcs
  ```

  telnet、rlogin、および ftp を無効にするには:

  ```
  svcadm disable telnet
  ```

  ```
  svcadm disable rlogin
  ```

  ```
  svcadm disable ftp
  ```
- ssh は無効にしないでください。ユーザーは telnet や rlogin ではなく、ssh を使用して ACSLS にリモートログインします。また sftp を無効にしないでください。
- ACSLS では rpc-bind が必要です。これを無効にしないでください。

  Solaris が「Secure by Default」オプションを有効にしてインストールされている場合は、ACSAPI クライアントが ACSLS に要求を送信するのを許可するように、rpc-bind のネットワーク構成プロパティーを変更する必要があります。

詳細については、『*ACSLS インストールガイド*』で、章「Solaris への ACSLS のインストール」のセクション「Solaris のインストール」を参照してください。

- ACSLS サーバー上の一部の Ethernet ポートは、ACSLS との通信用に開いている必要があります。クライアントアプリケーションは ACSLS との通信で特定の Ethernet ポートを使用し、ACSLS はテープライブラリ上の特定のポートと通信します。ACSLS 通信用に使用できる必要のあるポートについては、「ACSLS 通信に使用される Ethernet ポート」を参照してください。ACSLS サーバー上で、ACSLS で使用されるポートへのトラフィックを許可するように ipfilter が構成されていることを確認してください。

Solaris の監査ポリシーを決定します。監査対象のイベント、監査ログが保存される場所、およびそれを見直す方法について計画する際に、『Oracle Solaris の管理: セキュリティーサービス』の「Oracle Solaris での監査」セクションが役立つことがあります。

Linux のインストールと構成

Linux をセキュアにインストールおよび構成する際の提案事項:

- 重要なセキュリティーパッチをすべて OS および OS とともにインストールされているサービスに適用します。利用可能なすべての更新を適用すると、ACSLS および ACSLS HA でテストされていない新しい機能や、場合によっては新しい OS リリースがインストールされる可能性があるため、これらのパッチは選択的に適用してください。
- telnet と rlogin がインストールされていないこと、または無効になっていることを確認します。代わりに ssh を使用します。

  また、ftp がインストールされていないこと、または無効になっていることを確認し、代わりに sftp を使用します。

  すべてのサービス確認するには、root としてログインして次を実行します。

  ```
  service --status-all
  ```
- サービスを完全に削除するには、次を使用します。

  ```
  svccfg delete -f service-name
  ```
- ssh は無効にしないでください。ユーザーは telnet や rlogin ではなく、ssh を使用して ACSLS にリモートログインします。また sftp を無効にしないでください。
- ACSLS クライアント通信を許可するには、ネットワークサービス (特に rpcbind) を有効にする必要があります。

  Linux 上で rpc を起動する際に、–i フラグを付けて起動してください。

- ACSLS サーバー上の一部の Ethernet ポートは、ACSLS との通信用に開いている必要があります。クライアントアプリケーションは ACSLS との通信で特定の Ethernet ポートを使用し、ACSLS はテープライブラリ上の特定のポートと通信します。ACSLS 通信用に使用できる必要のあるポートについては、「ACSLS 通信に使用される Ethernet ポート」を参照してください。ACSLS サーバー上で、ACSLS で使用されるポートへのトラフィックを許可するように iptables が構成されていることを確認してください。

Linux セキュリティーの監査

Linux の監査ポリシーを決定します。監査対象のイベント、監査ログが保存される場所、およびそれらを見直す方法について計画する際に、『*Oracle Linux: セキュリティ・ガイド for リリース 6*』の「監査の構成および使用」セクションが役立つことがあります。

Linux のセキュリティーを監査するための便利なログおよびコマンドの一部は次のとおりです。

- root として var/log/secure を表示して、ログイン試行の履歴およびその他のアクセスメッセージを確認します。
- 「last | more」コマンドを使用すると、ログインしているユーザーの履歴が示されます。
- /var/log/audit/audit.log.[0-9] には、SE Linux で拒否されたアクセス試行のログが保持されます。これらを表示するには、root ユーザーである必要があります。

SELinux のセキュリティー

ACSLS 8.4 は、オプションの Security Enhanced Linux 環境で動作するように設計されています。SELinux では、UNIX 環境で標準的な従来の保護よりも強力な、ファイル、ディレクトリ、およびその他のシステムリソースへのアクセス制御が提供されます。SELinux には、owner-group-public アクセス権に加えて、ユーザーロール、ドメイン、およびコンテキストに基づいたアクセス制御も含まれています。すべてのシステムリソースにわたってアクセス制御を強制するエージェントは、Linux カーネルです。

Linux システム上の root ユーザーは、`setenforce` コマンドを使用すると強制をオンまたはオフに設定できます。

```
setenforce [Enforcing | Permissive | 1 | 0 ]
```

SELinux を強制モードにするには、`Enforcing` または 1 を使用します。SELinux を許容モードにするには、`Permissive` または 0 を使用します。

現在のシステム強制ステータスを表示するには、`getenforce` コマンドを使用します。

ACSLS をインストールすると、3 つの SELinux ポリシーモジュール (allowPostgr、acsdb、acsdb1) がカーネルにロードされます。これらのモジュールでは、SELinux の強制がアクティブなときに独自のデータベースおよびその他のシステムリソースにアクセスするために ACSLS で必要となる定義および強制例外が提供されます。これらのモジュールがインストールされていると、SELinux の強制を無効にすることなく、通常の ACSLS 操作 (bdb.acsss、rdb.acsss、db_export.sh、db_import.sh などのデータベース操作を含む) を実行できます。

詳細については、『*StorageTek ACSLS 8.4 管理者ガイド*』で、付録「トラブルシューティング」の SELinux に関するセクションを参照してください。

ACSLS のインストールおよび構成

このセクションでは、ACSLS をセキュアにインストールする方法について説明します。

標準の ACSLS インストールを実行する

標準の ACSLS インストールを実行すると、必要なコンポーネントがすべて追加されます。

以前の ACSLS リリースから新しい ACSLS リリースに移行する場合は、動的変数および静的変数の設定を見直して、特にファイアウォールのセキュリティーオプションに関して、よりセキュアなオプションを使用する必要があるかどうかを確認してください。

ACSLS ユーザー ID に強固なパスワードを使用する

ACSLS では ACSLS ユーザー ID (acsss、acssa、acsdb) が必要です。これらの ID に強固なパスワードを選択し、そのパスワードを定期的に変更してください。

ACSLS ファイルへのアクセスを制限する

一般に、ACSLS では ACSLS ファイルへのアクセスが acsls グループ (acsss、acssa、acsdb、root ユーザー ID を含む) のみに制限されています。一部のデータベースおよび診断ファイルには、単一の acsls ユーザー ID でしかアクセスできません。ACSLS は、umask の設定が 027 で実行されます。

ACSLS ファイルは、だれでも読み取りまたは書き込みできるようにしないでください。ただし、インストール時のデフォルト以上のアクセス制限を行うと、ACSLS の機能でエラーが発生する可能性があります。

3 つの ACSLS ファイルに有効なユーザー ID として「root」を設定する

インストールスクリプトによって、/export/home/ACSSS ファイルシステムにある 3 つの実行可能ファイルに有効なユーザー ID の「root」を設定する (setuid) 必要があることがお客様に通知されます。

- *acsss* (このバイナリは、ACSLS アプリケーションで必要なシステムサービスを起動および停止するために使用されるため、「root」権限で実行する必要があります。)
- *db_command* (このバイナリは、ACSLS データベースを制御および保守する PostgreSQL データベースエンジンを起動および停止します。)
- *get_diags* (このバイナリは、サービスサポートコールのコンテキストで必要となる場合のある包括的なシステム診断情報を収集するために、お客様によって起動されます。)

pkgadd を使用した ACSLS のインストール中に、「*Do you want to install these as setuid/setgid files?*」というプロンプトがお客様に表示されます。プロンプトに *y* で応答すると、ユーティリティーにより root 権限が必要な特定のシステム操作が実行されるにもかかわらず、これらの 3 つのコマンドを acsls グループのユーザーが実行できるようになります。

ACSLS の静的変数および動的変数の設定を見直す

ACSLS の静的変数および動的変数は、数多くの ACSLS 機能の動作を制御します。これらの変数を *acsss_config* ユーティリティーを使用して設定します。このドキュメントでは、これらの変数の多くをセキュアに設定する方法について説明します。*acsss_config* で変数のオプションが表示されたときに疑問符 (?) で応答すると、変数の詳細な説明が表示されます。この情報は、『*ACSLS 管理者ガイド*』の章「ACSLS 動作を制御する変数の設定」でも参照できます。

WebLogic の構成

ACSLS 8.1 以降のリリースでは、Web サーバーとして WebLogic が使用されます。WebLogic は ACSLS とともにインストールされます。

WebLogic サーバーをセキュリティー保護するためのオプション、および WebLogic を使用した監査証跡の可能性については、*Oracle Fusion Middleware*、*Oracle WebLogic Server 11g Release 1 (10.3.6) のセキュリティーの理解*を参照してください。

ACSLS の userAdmin.sh ユーティリティーを使用して ACSLS GUI ユーザーを作成および管理する

メニュー起動型の *userAdmin.sh* ユーティリティーを使用して、ACSLS GUI ユーザーのパスワードを管理します。ユーザーの追加、ユーザーの削除、ユーザーの一覧表示、ユーザーパスワードの変更を行うことができます。このユーティリティーを使用するには、WebLogic が動作している必要があります。動作していない場合は、メニューが表示される前に、このユーティリティーによって WebLogic が起動され、オンラインであることが確認されます。

userAdmin.sh ユーティリティーは root で実行する必要があり、acsls_admin 認証が必要です。acsls_admin ユーザーアカウントは、ACSLS のインストール時に構成されます。

ACSLS GUI の使用

ACSLS GUI を使用するには、最新バージョンの JRE をインストールし、ブラウザから ACSLS GUI にアクセスする必要があります。

GUI クライアントシステムに最新バージョンの JRE をインストールする

ACSLS へのアクセスに ACSLS GUI を使用するシステムに、最新バージョンの JRE (Java Runtime Environment) がインストールされていることを確認します。

ACSLS GUI へのアクセス

ブラウザを開き、次の形式でサーバーのホスト名または IP アドレスを含む URL を入力します。

https://myAcslsHostName.myDomainName:7002/SlimGUI/faces/Slim.jsp または *https://127.99.99.99:7002/SlimGUI/faces/Slim.jsp*

ホストマシンの完全修飾ホスト名または IP アドレスを使用することをお勧めします。WebLogic で URL を完全に解決できない場合は、一部のページ (ACSLS のヘルプページを含む) が正しく表示されない可能性があります。

ポート 7001 で http を使用している場合は、ポート 7002 で https を使用するように WebLogic によって自動的に再ルーティングされます。

WebLogic ではセキュアな https プロトコルが使用されているため、サイトのセキュリティー証明書が登録されていないために、信頼されないことを示す警告がブラウザに表示される可能性があります。確実に URL がローカルの ACSLS マシンである場合は、続行しても安全です。この時点で、ログイン画面が表示されます。

ACSLS GUI の使用

WebLogic の AcslsDomain には、セキュアプロトコルである https を使用してアクセスします。このプロトコルでは、非公開鍵とデジタル証明書を使用してブラウザとサーバーの間で暗号化された通信が使用されます。これらは、デジタル証明書を取得するためのオプションです。

ACSLS デモ証明書

ACSLS には、いわゆる「デモ」証明書が付属しています。これは、最小レベルの暗号化セキュリティーを提供し、お客様はさらなる構成手順を行うことなく ACSLS GUI の使用を開始できます。ACSLS ライブラリとのお客様の対話がすべて、セキュリティー保護されたイントラネット内で行われる場合、通常はこのデモ証明書の方式で十分です。ただし、この方式では、Internet Explorer や FireFox Version 39 以降などの特定のブラウザではサポートされない 512 ビットの暗号化鍵が採用されています。

自己署名デジタル証明書の構成

『ACSLS インストールガイド』には、ACSLS 管理者が長さ 2048 ビットの自己署名デジタル証明書を構成するための詳細な方法が記載されています。SSL 暗号化鍵の構成に関するセクションでは、この方法によりすべてのブラウザでサポートされる証明書が提供されます。自己署名証明書を使用して https サイトにアクセスするユーザーは、Web リソースが信頼できるサイトであることを個人的に知っている場合を除き、サイトに進まないことをお勧めします。ACSLS ユーザーとライブラリ制御サーバーの状況では、このレベルの信頼は通常十分に理解されており、ほとんどの場合、サイトがサードパーティーの署名の検証を使用して整合性を証明する必要はありません。

サードパーティーの署名機関によって署名されたデジタル証明書

Verisign や Entrust.net などのサードパーティーの署名機関による証明書認証を提供する必要があるかどうかは、各顧客サイトの判断にゆだねられています。そのような署名付きデジタル証明書を生成するための手順は、アイデンティティーおよび信頼の構成に関する Oracle のオンラインドキュメントに記載されています。

http://docs.oracle.com/cd/E13222_01/wls/docs92/secmanage/identity_trust.html

ACSLS HA のインストール

ACSLS HA (High Availability) の解決方法を使用する場合は、ACSLS-HA クラスタのインストール、構成、および操作に関するドキュメントの指示に従ってください。

3

第3章 セキュリティー機能

このセクションでは、ACSLS で提供される個別のセキュリティーメカニズムについて説明します。

セキュリティーモデル

ACSLS のセキュリティー要件は、第一に偶発的な損失および破損から、第二にそのデータにアクセスまたはデータを変更しようとする故意の不正な試みからデータを保護する必要性から生じます。第二の懸案事項には、データのアクセス時または使用時における過度の遅延からの保護、またはサービス拒否のポイントへの干渉からの保護も含まれます。

このような保護を提供するクリティカルなセキュリティー機能は次のとおりです。

- 認証 - 権限のある個人のみがシステムおよびデータにアクセスできるようにします。
- 承認 - システム権限およびデータに対するアクセス制御を提供します。これは、個人が適切なアクセス権のみを取得するようにする認証に基づいて構築されます。
- 監査 - 管理者が認証メカニズムの侵害の試みや、アクセス制御の侵害または侵害の試みを検出できます。

認証の構成と使用

Linux または Solaris のデフォルトでは、ACSLS ユーザーは PAM (Pluggable Authentication Module) によって認証されます。Solaris のマニュアルページまたは *Linux-PAM System の管理者ガイド*を参照してください。

ACSLS GUI のユーザーは、WebLogic の組み込み LDAP サーバーによって認証されます。次の組み込み LDAP サーバーの管理に関するドキュメントを参照してください。

http://docs.oracle.com/cd/E13222_01/wls/docs81/secmanage/ldap.html

Solaris または Linux オペレーティングシステムによる ACSLS ユーザー認証

ACSLS ユーザー (acsss と acssa) は cmd_proc を使用する前に、Solaris または Linux にログインし、オペレーティングシステムによって認証される必要があります。また、acsss ユーザー

の場合は、ACSLS ユーティリティーおよび構成コマンドを実行します。データベース関連の操作では、acsdb ユーザー ID も使用されます。ACSLS のインストールプロセスの一部として、お客様がはじめてログインするときに、これらの ID のパスワードを設定する必要があります。詳細については、『*ACSLS インストールガイド*』を参照してください。

WebLogic による ACSLS GUI ユーザー認証

ACSLS GUI ユーザーはログインし、WebLogic によって認証される必要があります。ACSLS のインストール中に acsls_admin が作成され、お客様はそのパスワードを設定する必要があります。必要に応じて、お客様は `userAdmin.sh` ユーティリティーを使用するとほかの GUI ユーザーを追加できます。詳細については、『*ACSLS インストールガイド*』および『*ACSLS 管理者ガイド*』で、ユーティリティーの章の `userAdmin.sh` に関するセクションを参照してください。

監査に関する考慮事項

ここでは、ACSLS に適用される、監査の一般的な考慮事項について説明します。

監査対象情報を管理しやすく維持する

監査は比較的リソースを消費しませんが、監査対象のイベント数はできるかぎり制限してください。これにより、監査対象ステートメントの実行および監査証跡のサイズへのパフォーマンスの影響を最小限に抑えられ、より容易に分析、理解、および管理できるようになります。

監査方針を策定する際は、次のような一般的なガイドラインを使用します。

監査の目的を評価する

監査の根拠を明確に理解すれば、適切な監査方針を策定し、不要な監査を回避できます。

豊富な知識をもって監査する

目的の情報を取得するために必要な最小数のステートメント、ユーザー、またはオブジェクトを監査してください。

ACSLS 監査ログの構成と使用

ACSLS には、ACSLS アクティビティーを記録および検査できる情報のログがいくつか用意されています。

- ほとんどのログは、vi などのエディタを使用すると表示できます。システムイベントは、ACSLS GUI を使用してのみ表示できます。

- これらのログの大部分は、お客様が定義したサイズに達すると自動的にアーカイブされ、お客様が指定した数のログが保管されます。ACSLS ファイルシステムがいっぱいにならないように、保管されるログ数の制限を構成できます。これらのログファイルをより多く保管する場合や、別のシステムで保管する場合は、十分な容量を持つ場所にログをアーカイブするための独自の手順を開発する必要があります。
- 保管するアーカイブログのサイズと数、およびこれらのファイルのその他の特性は、ACSLS の動的変数および静的変数で定義されます。

ACSLS ログのディレクトリ

ACSLS ログのディレクトリは、LOG_PATH 静的変数によって制御されます。デフォルトのディレクトリは $ACS_HOME/log です。このディレクトリには、次のログが含まれています。

acsss_event.log
ここには、重大な ACSLS システムイベント、ライブラリイベント、およびエラーに関するメッセージが記録されます。

acsss_event.log が LOG_SIZE 動的変数で定義されたしきい値サイズに達すると、event0.log にコピーされ、クリアされます。コピープロセス中に、保管イベントログはそれぞれ、より大きい番号を持つ保管ログにコピーされ、もっとも大きい番号の保管ログは上書きされます。たとえば、event8.log は event9.log に上書きコピーされ、event7.log は event8.log に上書きコピーされ、同様に続き、event0.log は event1.log に上書きコピーされ、acsss_event.log は event0.log に上書きコピーされ、acsss_event.log はクリアされます。これは、次の変数によって制御されます。

- *EVENT_FILE_NUMBER* は、保管するイベントログの数を指定します。
- *LOG_SIZE* は、イベントログが保管イベントログにコピーされ、破棄される際のしきい値サイズを指定します。

特定のキーワードを含むメッセージが含まれるように、または除外されるように acsss_event ログをフィルタリングするには、*greplog* ユーティリティーを使用します。詳細については、『*ACSLS 管理者ガイド*』でユーティリティーの章の greplog を参照してください。

構成ログ
ACSLS データベースに格納されているライブラリ構成が ACSLS により更新される際に詳細を記録するログが 2 つあります。ここには、*acsss_config* と *Dynamic Config* (*config* ユーティリティー) の両方による構成の変更が記録されます。

acsss_config.log
ACSLS でサポートされているライブラリ (複数可) のすべての構成または再構成の詳細が記録されます。最後の構成変更は、前の構成レコードに追加されます。

acsss_config_event.log
構成または再構成プロセス中にイベントが記録されます。

rpTrail.log
ACSAPI クライアントまたは cmd_proc から ACSLS へのすべての要求、および論理ライブラリへの GUI または SCSI クライアントインタフェースへのすべての要求 (データベースクエリーを除く) に対する応答が記録されます。ログに記録される情報には、要求元、要求、および要求のタイムスタンプが含まれます。

rpTrail.log は次の変数によって管理されます。

- *LM_RP_TRAIL* は、ACSLS イベントのこの監査証跡を有効にします。デフォルト値は TRUE です。
- *RP_TRAIL_LOG_SIZE* は、rpTrail.log が圧縮およびアーカイブされる際のしきい値サイズを指定します。
- *RP_TRAIL_FILE_NUM* は、保管されるアーカイブ済み rpTrail ログの数を指定します。
- *rpTrail RP_TRAIL_DIAG* は、rpTrail メッセージに追加の診断情報を含めるかどうかを指定します。デフォルト値は FALSE です。

ライブラリボリュームの統計情報
テープライブラリ内のボリューム (カートリッジ) に影響を与えるすべてのイベント (ボリュームのマウント、マウント解除、移動、挿入、取り出し、監査またはカートリッジ回復による検出など) が記録されます。ライブラリボリュームの統計情報が有効になっている場合、この情報は acsss_stats.log に記録されます。

ライブラリボリュームの統計情報は、次の変数によって管理されます。

- *LIB_VOL_STATS* は、このライブラリボリュームの統計情報を有効にします。デフォルト値は OFF です。
- *VOL_STATS_FILE_NUM* は、保管するアーカイブ済み acsss_stats.log ファイルの数を指定します。
- *VOL_STATS_FILE_SIZE* は、acsss_stats.log がアーカイブされる際のしきい値サイズを指定します。

ACSLS ログ/sslm のディレクトリ

ACSLS ログディレクトリ内の sslm ディレクトリには、論理ライブラリへの ACSLS GUI および SCSI クライアントインタフェースに関する情報が記録されます。このディレクトリには、WebLogic 監査ログへのリンクが含まれています。sslm ディレクトリには次のログが含まれています。

slim_event.g#.log[.pp#]
ここには、ACSLS GUI と SCSI クライアントインタフェースの両方からのイベントが記録されます。論理ライブラリ構成の変更のメッセージ、および SCSI クライアントイベントが含まれます。

- .g# は、このログの世代番号です。
- .pp# は、このログの並列プロセス番号です。同時にログを記録するプロセスが複数存在する場合は、追加プロセスからのログに並列プロセス番号が割り当てられます。

smce_trace.log
ここでは、SCSI Media Changer Interface エミュレーションを使用して、SCSI クライアントから ACSLS 論理ライブラリへのアクティビティーが追跡されます。

guiAccess.log
これは、WebLogic の access.log へのリンクです。「WebLogic 監査ログの構成と使用」を参照してください。

AcslsDomain.log
これは、WebLogic の AcslsDomain.log へのリンクです。「WebLogic 監査ログの構成と使用」を参照してください。

AdminServer.log
これは、WebLogic の AdminServer.log へのリンクです。「WebLogic 監査ログの構成と使用」を参照してください。

GUI のログビューアからの ACSLS 監査証跡の表示

ログビューアには、GUI ナビゲーションツリーの「Configuration and Administration」セクションからアクセスします。ログビューアには、acsss_event.log および smce_trace.log からの情報を組み合わせたものが表示されます。

GUI からのシステムイベントの表示

システムイベントにも、GUI ナビゲーションツリーの「Configuration and Administration」セクションからアクセスします。システムイベントログには、個々のライブラリの操作がすべて記録されます。このログの各レコードには、イベントのタイムスタンプ、イベントのタイプ、およびイベントの説明が含まれています。

Solaris 監査ログの構成と使用

Solaris の監査ポリシーを決定します。監査対象のイベント、監査ログが保存される場所、およびそれを見直す方法について計画する際は、『*Oracle Solaris の管理: セキュリティーサービス*』マニュアルの「Oracle Solaris での監査」セクションが役立つことがあります。

カスタムの Solaris 監査証跡が有効になっていない場合は、acsss、acsdb、および acssa ユーザーによって発行されたログインおよび UNIX コマンドの監査証跡を使用できます。

- 現在 UNIX にサインオンしているユーザーは UNIX の utmpx に記録され、過去のユーザーアクセスは wtmpx データベースに記録されます。

- ユーザー ID へのすべてのアクセスを表示するには、*last* コマンド (たとえば、*last acsss*) を使用します。詳細については、wtmpx、*last*、および getutxent のマニュアルページを参照してください。
- ユーザーのホームディレクトリ内にある .*_history (つまり、[dot]*_history) ファイルには、そのユーザーが発行したコマンドが記録されます。

  acsss ユーザーの場合は、次が含まれている可能性があります。

  - .bash_history
  - .psql_history
  - .sh_history

  Solaris の /var/adm/sulog には、*su* を実行してスーパーユーザーや別のユーザーになろうとする試みが成功、失敗にかかわらず記録されます。

Linux 監査ログの構成と使用

監査ログおよびシステムログの収集と分析に関する詳細については、『*Oracle Linux: セキュリティ・ガイド for リリース 6*』の「監査の構成および使用」および「システム・ロギングの構成および使用」セクションを参照してください。

WebLogic 監査ログの構成と使用

WebLogic サーバーをセキュリティー保護するためのオプション、および WebLogic を使用した監査証跡の可能性については、*Oracle Fusion Middleware*、*Oracle WebLogic Server 11g Release 1 (10.3.6) のセキュリティーの理解*を参照してください。

WebLogic では、次のディレクトリに ACSLS GUI へのアクセスが記録されます。

/export/home/SSLM/AcslsDomain/servers/AdminServer/logs

このディレクトリには次のファイルが含まれています。

- access.log
  - access.log##### という名前のアーカイブ済みバージョン (たとえば、access.log00001) があります。
  - ここでは、GUI ユーザーアクティビティーの詳細な監査証跡が提供されます。
  - ログインについては、「AcslsLoginForm」を探してください。

注:

$ACS_HOME/logs/sslm/guiAccess.log には、アクセスログへのリンクがあります。

- AcslsDomain.log
  - ここには、WebLogic および ACSLS GUI の操作が報告されます。

注:

$ACS_HOME/logs/sslm/AcslsDomain.log には、アクセスログへのリンクがあります。

- AdminServer.log
  - ここには、WebLogic および ACSLS GUI の操作が報告されます。

注:

$ACS_HOME/logs/sslm/AdminServer.log には、アクセスログへのリンクがあります。

4

第4章 開発者のセキュリティーに関する考慮事項

このセクションでは、Oracle の StorageTek テープライブラリの管理に ACSLS を使用するアプリケーションを開発者が開発またはサポートする際に役立つ情報を示します。

クライアントアプリケーションのサーバー上でファイアウォールのセキュリティーを有効にする

ファイアウォールのセキュリティーを有効にすることで、クライアントのアプリケーションサーバー上で通信に使用されるポートを制限し、ポートマッパーを無効にします。*CSC 開発者のツールキットユーザーズガイド*で、ファイアウォールのセキュアな操作に関する付録 B を参照してください。

付録A

付録A セキュアな導入のためのチェックリスト

1. パスワード管理を適用します。
2. ネットワークアクセスを制限します。
   a. ACSLS および管理対象のテープライブラリは、企業ファイアウォールの内側に配備するようにしてください。
   b. ACSLS ファイアウォールのセキュアなオプションを有効にします。
   c. ACSLS クライアントアプリケーションでファイアウォールのセキュリティーを有効にすることを検討してください。
3. Solaris または Linux オペレーティングシステムを強化します。
4. すべてのセキュリティーパッチおよび回避方法を適用します。
5. StorageTek ACSLS の脆弱性を見つけた場合は、Oracle サービス、Oracle Tape Library エンジニアリング、またはアカウント担当者に問い合わせてください。

付録B

付録B 参照情報

ACSLS のドキュメント
ACSLS のドキュメントは、ACSLS のリリース別に整理されたライブラリに保存されています。テープストレージドキュメントのページから、これにアクセスしてください。

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#opensyssoft

(個々の ACSLS ドキュメントライブラリの URL には、バージョン番号が含まれています。したがって、特定のライブラリが更新されるとすぐに、そのライブラリへのリンクは古くなります。)ACSLS のドキュメントは次のとおりです。

- *ACSLS インストールガイド*
- *ACSLS 管理者ガイド*
- *ACSLS 製品情報*

  ここには、ソフトウェアとハードウェアの要件、ACSLS の概要に加えて、サポートされているテープライブラリ、テープドライブ、メディアが記載されています。
- ACSLS のメッセージ (およびステータスコード)
- *ACSLS リリースノート*
- *ACSLS-HA クラスタ: インストール、構成、および操作*
- *ACSLS インタフェースのリファレンスマニュアル*

Oracle Solaris
Oracle Solaris 11.2 Information Library には、「*Oracle Solaris 11 オペレーティングシステムのセキュリティー保護*」が含まれています。詳細については、これを参照してください。

Oracle Linux
Oracle Linux 6 Information Library には、*Oracle Linux 6 のセキュリティーガイド*が含まれています。詳細については、これを参照してください。

Oracle WebLogic
Oracle WebLogic Server Documentation Library for WebLogic 10.3.6 (ACSLS 8.2 で使用) には、セキュリティーに関するセクションがあります。

Oracle Fusion Middleware、*Oracle WebLogic Server 11g Release 1 (10.3.6)* のセキュリティーの*理解*では、WebLogic サーバーのセキュリティー保護について詳細に説明されています。