コマンド行セキュリティ管理ユーティリティ

Version 2023.1
2024-01-02

InterSystems Corporation　1 Memorial Drive　Cambridge MA 02142　www.intersystems.com

コマンド行セキュリティ管理ユーティリティ
InterSystems IRIS Data Platform　Version 2023.1　2024-01-02

インターシステムズ社の製品に関するサポートやご質問は、以下にお問い合わせください：

InterSystems Worldwide Response Center (WRC)
Tel:　+1-617-621-0700
Tel:　+44 (0) 844 854 2917
Email:　support@InterSystems.com

目次

コマンド行セキュリティ管理ユーティリティ

1 コマンド行ユーティリティについて

InterSystems IRIS® の管理ポータルには、インスタンスを制御するためのブラウザベースのインタフェースが用意されています。InterSystems IRIS にはコマンド行ユーティリティもいくつか用意されており、ターミナルで管理アクティビティを実行するために使用できます。これらのユーティリティには、次のようなものがあります。

- ^SECURITY ー インターシステムズのセキュリティが適切に機能するために必須のデータの設定とメンテナンスを実行します。
- ^EncryptionKey ー 暗号化キー管理、データベース暗号化、およびデータ要素暗号化の処理をサポートします。
- ^DATABASE ー データベースの管理に使用されます。これにより、インターシステムズのセキュリティに関連する値を設定することもできます。
- ^%AUDIT ー ログにあるデータのレポート処理に加えて、監査ログのエントリとログ自体の操作を実行できます。

これらの各ユーティリティについては、それぞれのセクションでその最上位機能と共に説明されています。ほとんどの場合、初期メニューを選択すると、ユーティリティのタスクを実行するのに十分な情報が指定されるまで、情報の入力が求められます。ターミナルからこれらのユーティリティを使用するには、ユーザが %SYS ネームスペースにいることと、最低でも **%Manager** ロールを持つことが必要です。例えば、^SECURITY ユーティリティを呼び出すには、次のコマンドを使用します。

ObjectScript

```
Do ^SECURITY
```

ユーティリティが実行されると、そのオプションのリストが表示されます。目的のオプションを選択するには、Option? プロンプトの後に対応する番号を入力します。

重要　1 つのユーティリティの複数のインスタンスを同時に実行することはできますが、これによって解決が必要な競合が生じる可能性があります。

1.1 プロンプトに関する一般的な注意事項

文字ベースのユーティリティを使用したときのプロンプトの特性を以下に示します。

- 各オプションには、数字のプレフィックスがあります。その番号を入力することで、オプションを選択します。
- 各オプション・リストに、メニューを終了して前のレベルに戻るための項目があります。または、Option? プロンプトに対して Enter キーを押して対応することもできます。これは、Exit オプションを選択したかのように解釈されます。
- 既定値が設定されているプロンプトの場合、Enter キーを押すことでその既定値を選択できます。既定値がある場合は、次に示すように、プロンプトと文字 => の間に表示されます。

  ```
  Unsuccessful login attempts before locking user? 5 =>
  ```

  このオプションの既定値は 5 です。
- 既定値が Yes または No のプロンプトでは、“yE” や “n” などの部分的に一致する応答も受け入れられます。この一致では、大文字と小文字は区別されません。

- 設定を変更するためのプロンプトの場合、設定の現在の値が既定値です。その値を保持するには、Enter キーを押します。
- プロンプトによっては、パターン・マッチングを実行する入力も受け入れられます。通常、アスタリスク(*)はすべての項目に一致します。プロンプトでコンマ区切りリストが受け入れられる場合もあります。

2 ^SECURITY

このユーティリティは、インターシステムズのセキュリティが適切に機能するのに必須のデータの設定とメンテナンスを実行します。

注釈　InterSystems IRIS 2021.2 より、エクスポートおよびインポートされたセキュリティ情報がバージョン管理されるようになりました。バージョン 2022.1 以降では、同じバージョンどうしでのみエクスポートとインポートができます。バージョン 2021.2 では、バージョン 2021.1 からセキュリティ・コンテンツもインポートできます。

1. ユーザの設定

   ユーザとは、システムへのアクセスが許可されている実際の人々またはその他のエンティティです。ユーザを作成、編集、削除、リスト、エクスポート、およびインポートできます。

2. ロールの設定

   InterSystems IRIS ユーザは、割り当てられているロールに基づいてアクションを実行できます。ロールを作成、編集、削除、リスト、エクスポート、およびインポートできます。

3. サービスの設定

   サービスは、InterSystems IRIS への接続をサポートする事前定義のテクノロジを制御します。サービスを編集、リスト、エクスポート、およびインポートできます。

4. リソースの設定

   リソースは、セキュリティ管理を必要とする資源を表します。リソースは 1 つのデータベースのように単一の資源を表す場合もあれば、一連のアプリケーションのように複数の (通常は関連のある) 資源を保護する場合もあります。リソースを作成、編集、削除、リスト、エクスポート、およびインポートできます。

5. アプリケーションの設定

   アプリケーション定義はアプリケーションを表し、いくつかのタイプがあります。それぞれのサブメニューで、各アプリケーション・タイプを編集、リスト、エクスポート、およびインポートできます。

   注釈　クライアント・アプリケーションは Windows でのみ使用可能であるため、クライアント・アプリケーションに関連するオプションは他のオペレーティング・システムでは表示されません。

6. 監査の設定

   監査によって、InterSystems IRIS でセキュリティ関連イベントを追跡できるようになります。監査の有効化と無効化、監査データベースの表示、監査イベントの構成、および監査ログの管理が可能です。

7. 注釈　このオプションは、従来の製品で使用できますが、InterSystems IRIS では使用できません。

8. SSL 構成の設定

   TLS は SSL の後継であり、認証や、ミラーリングでの使用などの機能を提供します。TLS 構成を作成、編集、削除、リスト、テスト、エクスポート、およびインポートできます。

9. 携帯電話サービス・プロバイダの設定

2 要素認証をサポートするために、ユーザは携帯電話およびサービス・プロバイダを登録する必要があります。携帯電話サービス・プロバイダを作成、編集、削除、およびリストできます。

10. OpenAM ID サービスの設定

    OpenAM ID サービスを使用すると、InterSystems IRIS でシングルサイン・オン (SSO) をサポートできます。ユーザが認証にすでに成功している場合、OpenAM によって再認証の必要がなくなります。このオプションを使用すると、**%SYS.OpenAM.IdentityServices** クラス API を使用して、指定した OpenAM サーバに対して認証を行うことができます。OpenAM ID サービスを作成、編集、削除、およびリストできます。

    注釈　Web ポリシー・エージェントを通じて OpenAM を使用するには、InterSystems IRIS で使用している Web サーバに Web ポリシー・エージェントをインストールして構成する必要があります。

    ユーザが接続すると、Web ポリシー・エージェントはそのユーザを OpenAM サーバにリダイレクトします。OpenAM サーバはそのユーザを認証して、ユーザの接続先のシステムに送ります。また、OpenAM サーバは、cookie に記録される OpenAM トークンをユーザに提供します。Web ポリシー・エージェントはトークンを認識して、OpenAM サーバでトークンを検証し、REMOTE_USER 変数の値をユーザのユーザ名に設定して、Web サーバに接続します。これにより、代行認証などを使用して、Web アプリケーションで $USERNAME を REMOTE_USER の値に設定できるようになります。サポート対象のサービスへの後続の接続でトークンが検証されるため、元の認証が維持されます。

    これを実行するには、InterSystems IRIS で使用しているサーバに Web ポリシー・エージェントをインストールして構成する必要があります。

11. 暗号化キーの設定

    InterSystems IRIS では、データベースまたはユーザ指定のデータ要素の暗号化にキーが使用されます。ファイルでのキーの作成と管理、キーの有効化と無効化、キーのリスト、既定のキーの指定、暗号化の起動オプションの構成、およびデータベースの暗号化ステータスの変更が可能です。

12. システム・パラメータの設定

    システム・パラメータでは、システム全体のセキュリティの値を指定します。以下を実行できます。

    - システム・オプションの編集 (構成のセキュリティの管理、複数ドメインの使用の指定、既定のドメインの管理、非アクティブなアカウントとログイン制限の管理、パスワード有効期間の管理、パスワード要件の管理、パスワード検証ルーチンの指定、パーセント (%) グローバルへの書き込みの管理、システムに必要なロールの指定、必要なまたは許可される TLS サーバ認証モードの指定、および既定の署名ハッシュの指定)
    - システム・オプションの表示
    - 認証オプションの有効化と無効化
    - LDAP 構成の作成、編集、削除、リスト、エクスポート、およびインポート
    - SQL 特権のセキュリティ設定も含む、すべてのセキュリティ設定のエクスポートとインポート (セキュリティ情報のエクスポートとインポートに関する前述の注を参照してください)

    以下についても留意してください。

    - 複数のドメインで構成されたソース・インスタンスから複数のドメインを許可するよう構成されていないターゲット・インスタンスにセキュリティ設定をインポートする場合、ソース・インスタンスとターゲット・インスタンスで既定のドメインが異なると、インポートしたときにターゲットの既定のドメインが更新されません。この値は明示的に設定する必要があります。これを実行するには、**[システムワイドセキュリティパラメータ]** ページ (**[システム管理]** > **[セキュリティ]** > **[システム・セキュリティ]** > **[システムワイドセキュリティパラメータ]**) の **[デフォルトセキュリティドメイン]** ドロップダウンを使用します。
    - すべてのセキュリティ設定をインポートする場合、インポート/エクスポート・ファイルには Web アプリケーションの設定が含まれ、各 Web アプリケーションに Path 設定が含まれます。新しいドライブ、VM、またはハードウェアに設定をインポートするには、まず Web アプリケーションごとに Path 設定値が環境に対して正確であること

を確認します。管理ポータルに関連付けられている Web アプリケーションの Path の値が適切でないと、管理ポータルに正しく表示されなくなります。

インポート/エクスポート・ファイル (SecurityExport.xml) 内の各 Web アプリケーションの Path 設定を見つけるには、ApplicationsExport セクションを調べます。それぞれの Applications セクションで Name 設定の値によってアプリケーションを識別してから、必要に応じて Path の値を更新します。

13. X509 ユーザの設定

    X.509 は、公開鍵インフラストラクチャ (PKI) が使用する証明書の標準です。InterSystems IRIS は PKI に X.509 証明書を使用し、X.509 証明書に関連付けられた各ユーザは X.509 ユーザと呼ばれます。X.509 ユーザを作成、編集、削除、リスト、エクスポート、およびインポートできます。

14. KMIP サーバの設定

    KMIP サーバは、Key Management Interoperability Protocol (KMIP) を使用して通信するキー管理サーバです。KMIP サーバの構成を作成、編集、削除、リスト、テスト、エクスポート、およびインポートできます。

15. 終了

3 ^EncryptionKey

^EncryptionKey ユーティリティは、マネージド・キー暗号化で使用します。このユーティリティでは、暗号化キー管理 (暗号化キーおよびキー・ファイルの作成と管理のテクノロジ)、データベース暗号化、およびデータ要素暗号化の処理がサポートされます。

1. 暗号化キーおよびキー・ファイルの新規作成

   キー・ファイルに格納するデータベース暗号化キーを新規作成できます。

2. 既存の暗号化キー・ファイルの管理

   キー・ファイルに関連付けられた管理者のリスト化、キー・ファイルへの管理者の追加、キー・ファイルからの管理者の削除、およびバージョン 1.0 キー・ファイルのバージョン 2.0 キー・ファイルへの変換を実行できます。

3. データベースの暗号化

   暗号化管理操作の実行、データベース暗号化キーの有効化、現在有効になっているデータベース暗号化キーがある場合はその一意の識別子の表示、有効になっているデータベース暗号化キーの無効化、およびデータベース暗号化に関連する InterSystems IRIS 起動オプションの構成を行うことができます。暗号化管理操作は、非暗号化データベースを暗号化に変換する、暗号化データベースを非暗号化に変換する、および暗号化データベースを新規キーを使用するように変換する処理を行うための操作です。詳細は、“^EncryptionKey を使用したデータベース暗号化の変更”を参照してください。

4. アプリケーションのデータ要素暗号化

   データ要素暗号化キーの有効化、現在有効になっているデータ要素暗号化キーがある場合はそれらの一意の識別子の表示、および現在有効になっているデータ要素暗号化キーの無効化を行うことができます。

4 ^DATABASE

^DATABASE ユーティリティはデータベースの管理に使用します。また、インターシステムズのセキュリティに関連する値を設定できます。

1. データベースの作成

   新しいデータベースを作成できます。

2. データベースの編集

   ボリュームを追加するなどして、既存データベースの属性を変更できます。

3. データベースの一覧表示

   1 つ以上のデータベースの属性を表示します。

4. データベースの削除

   InterSystems IRIS データベースを削除できます。この操作は元に戻せません。

5. データベースのマウント

   データベースを InterSystems IRIS で使用できる状態にします。データベースを使用可能にするには、InterSystems IRIS に対してデータベースをマウントする必要があります。データベースは、起動時に自動的にマウントされるように設定できます。

   注釈　**[データベースのマウント]** オプションを使用して、インスタンスにアクセス可能な任意の **IRIS.DAT** ファイルをマウントできます。そのためには、このファイルを含むディレクトリを指定します。ただし、管理ポータルのデータベース構成から削除されたデータベースまたは一度もこのデータベース構成に追加されたことがないデータベースでこれを実行すると (″システム管理ガイド″ の “InterSystems IRIS の構成” の章にある ″データベースの構成″ を参照)、データベースは管理ポータルの構成に追加されず、したがってポータルのデータベースの操作および ^Integrity などの一部のユーティリティで使用できません (″データ整合性ガイド″ の “データ整合性の概要” の章にある ″^Integrity ユーティリティを使用したデータベース整合性のチェック″ を参照)。

6. データベースのディスマウント

   データベースを停止して、InterSystems IRIS での使用を解除できます。

7. データベースのグローバルの圧縮

   IRIS.DAT 内のデータを再編成します。このオプションを使用しても、データベース・ファイルのサイズは縮小しません。データベースのサイズを縮小する方法は、オプション 13 を参照してください。

8. データベースの空き容量の表示

   データベースの使用可能な空き容量を表示します。このオプションでは、データベースの現行のコンテンツと宣言サイズの差異が計算されます。

9. データベースの詳細の表示

   場所、サイズ、ステータスなどの管理パラメータを含む、指定されたデータベースの詳細情報を表示します。

10. データベースの再作成

    既存のデータベースのパラメータに基づいて、新しい空のデータベースを作成します。新しいデータベースのサイズを指定できます。既定値は、元のデータベースのサイズです。

11. データベース暗号化の管理

    データベースのプロパティを再利用に備えて保持しながら、すべての論理データをデータベースから削除します。

12. データベースの未使用領域を返す

    データベースに関連付けられた使用可能な余分な領域から、指定された量またはそのすべての領域を解放し、現在のサイズから可能な限り小さいサイズに縮小します。

13. データベースの空き容量の圧縮

データベースのデータの末尾の後の空き容量 (使用しない容量) について、希望する量を指定します。この空き容量は、データベースの未使用領域を返すオプション (#12) を使用して、削除することもできます。

14. データベースのデフラグ

    データベースのデフラグにより、より効率的にデータを整理できます。デフラグを行うと、データベースに空き容量が残る場合があります (オプション #12 と #13 を参照)。

15. バックグラウンドのデータベース・タスクの表示

    実行中のバックグラウンド・タスクまたは起動後に実行されたバックグラウンド・タスクのリストを表示します。このオプションを使用して、監視画面を再び表示し、現在実行中のタスクをキャンセルしたり、完了したタスクの履歴を削除したりすることもできます(ここに表示されるタスクは、タスク・マネージャにスケジュールされたタスクとしてリストされるタスクと同じではありません)。

5 ^%AUDIT

このユーティリティでは、ログにあるデータのレポート処理に加えて、監査ログのエントリとログ自体の操作を実行できます。

1. 監査レポート

   選択条件 (日付範囲、イベント、対象ユーザなど) を指定して、それらの特性を表示できます。また、監査ログからデータを抽出し、フォーマット処理して表示できます。

2. 監査ログの管理

   他のネームスペースへのログ・エントリの抽出、監査ログ・データの外部ファイルに対するエクスポートとインポート、および監査ログ自体の保守作業を実行できます。

3. 終了