Audit for Zen 15

User's Guide

Audit for Zen User’s Guide
2020 年 4 月

目次

Actian Audit for Zen について

1

Audit for Zen とその機能について

このドキュメントでは、Actian の Zen Enterprise Server および Cloud Server の監視および監査アプリケーションである Audit for Zen について説明します。インストールまたはアップグレードおよび構成手順を示した後、アプリケーションの使用方法を説明します。Zen のセキュリティ機能が有効になっている場合と有効になっていない場合の Zen データベース環境における、エンド ユーザーと管理者のタスクについても説明します。

以下のトピックでは、Audit for Zen とその機能の概要を提供します。

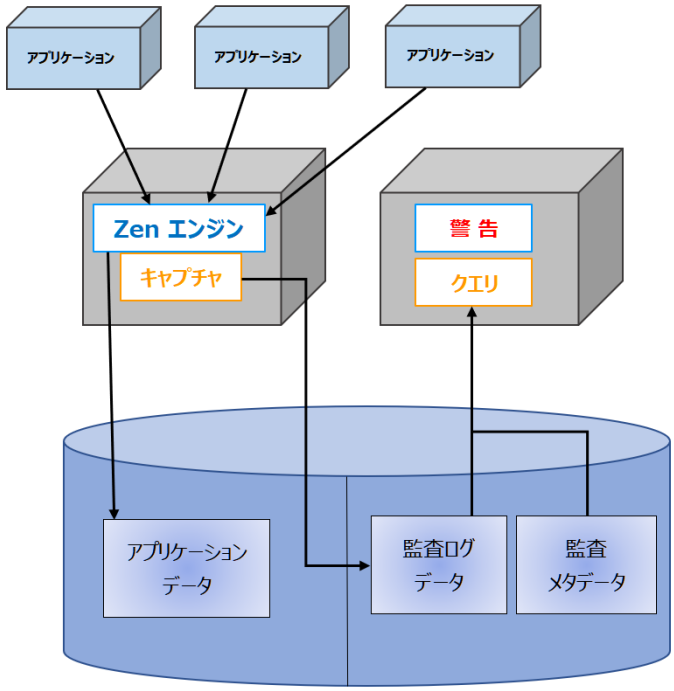
- 「Audit for Zen とは」
- 「Audit for Zen の機能」
- 「次に行うこと」

Audit for Zen とは

Audit for Zen は、データに対するアクセスや変更を追跡するためのトランザクション監視製品です。本製品は、データベースのトランザクションごとに、次の情報をキャプチャした詳細な監査証跡を提供します。

- だれがレコードにアクセスしたか、または変更を行ったか
- どのような変更が行われたか
- いつアクセスまたは変更が行われたか
- どこからアクセスまたは変更が行われたか
- どのようにして変更が行われたか

Audit for Zen はデータベースを監視しますが、クライアント アプリケーションは監視しません。データに加えられた変更はもちろんのこと、データベースへのアクセスもログに記録されます。これには、レコードを読み取って、何の変更も行われていないものも含まれます。



Audit for Zen は包括的な監査証跡を作成します。監視しているデータ ファイルが変更されるたびに、Audit for Zen はその変更前の状態と変更後の状態を両方ともログに記録します。ログにより、転記またはデータ入力エラーから回復可能となります。

Audit for Zen の機能

セキュリティで保護された監査証跡を提供するため、Audit for Zen に備わっている機能により、ユーザーは以下を実行することができます。

- **包括的なログ システム**
  データベースにおけるイベントをキャプチャし、イベントが発生する前後両方のデータベース レコードのスナップショットをキャプチャします。これは、サード パーティ製のアプリケーションからのトランザクションであっても、Zen システム内のトランザクションであっても対象となります。
- **クエリ ビルダ**
  クエリを作成、カスタマイズ、管理します。
- **警告**
  Audit for Zen によってキャプチャされたイベントに対して実行するクエリを使用し、セキュリティ、管理、通知などさまざまな目的で Windows システムのログにイベント情報を送信します。
- **アーカイブ マネージャー**
  必要に応じてデータ圧縮を使用して、履歴情報を格納および取得します。

次に行うこと

次のトピックが参考になると思われます。

- アプリケーションをインストールする場合は、「Audit for Zen をインストールするための準備」を参照してください。
- アプリケーションの操作方法を学習するには、「Audit for Zen について」を参照してください。
- トラブルシューティング手順については、「基本的なトラブルシューティング」を参照してください。

Audit for Zen をインストールするための準備

2

インストールまたはアップグレードの準備

次のセクションでは、Audit for Zen の一般的なインストールまたはカスタム インストールの準備について説明します。

- 「一般的なインストール」
- 「カスタム インストール」

一般的なインストール

このトピックでは、以下の情報について説明します。

- 「インストール チェックリスト」
- 「使用前の注意」
- 「アクセス許可と権限」
- 「認証ライセンス」
- 「リリース ノート」
- 「ドキュメント」

インストール チェックリスト

インストールやアップグレードの準備に役立つリストを以下に示します。開始する前に、お使いのシステムが、弊社 Web サイトに掲載されている Audit for Zen のハードウェア要件およびソフトウェア要件を満たしていることを確認してください。

各チェックリスト項目については、後のトピックでより詳細に説明します。

❒ インストールする前に、適切な事前措置を行っている。

❒ インストール先のシステムにおける管理者レベルのアクセス許可と権限をすべて持っている。

❒ ライセンスを持っている（試用版でテストする場合を除く）。

❒ 最新のリリース ノートを確認できる。

使用前の注意

Audit for Zen のインストールでは、Zen データベース エンジンの停止、再起動が行われます。このため、業務に支障のないときに AZ（Audit for Zen）をインストールしてください。

目的のハード ディスク ドライブ上の重要なファイルは、データ ファイルも含めて、作業を進める前にバックアップしておいてください。

インストールを開始する前に、すべてのウイルス対策アプリケーションを無効にします。インストールが完了した直後に、これらを再度有効にすることができます。ウイルス対策アプリケーションを無効にしない場合は、さまざまなインストール タスクを実行する許可を求められます。

アクセス許可と権限

Audit for Zen をインストールするには、インストール先のシステムにおける管理者レベルのすべての権限が必要です。

認証ライセンス

インストール時に製品キーを入力しなかった場合、試用評価期間中のみ、データを監視できます。試用期間が終わると、Audit for Zen はデータを監視しなくなります。試用中にキャプチャされた既存の監査レコードを照会することはできますが、特定の機能は利用できなくなります。

製品キーを適用するには、Zen Control Center で［**ツール**］>［License Administrator］を選択します。または、コマンド プロンプトを開き、32 ビット インストールの場合は clilcadm、64 ビット インストールの場合は w64clilcadm を実行します。製品キーの詳細については、『*Zen User's Guide*』を参照してください。

Zen リモート クライアント システムへのインストールでは、製品キーを必要としません。AZCC（Audit for Zen Control Center）クライアント自体には製品キーは必要ありません。

メモ Audit for Zen は、監視する Zen サーバー インスタンスのアクティブな製品キーを持っている場合にのみ実行できます。

リリース ノート

readme_am.htm ファイルのリリース ノートをお読みになることをお勧めします。リリース ノートには、ユーザー マニュアルには含めることができなかったが、Audit for Zen を正常にインストールして使用するために必要な製品情報が記載されています。

このファイルは、Audit for Zen インストール後にインストール先で見つかります。デフォルトの場所は C:¥Program Files (x86)¥Actian¥Zen¥Audit¥Docs です。

ドキュメント

このドキュメントは Audit for Zen では［ヘルプ］メニューにあります。また、［AZCC］（Audit for Zen Control Center）ウィンドウおよびダイアログのさまざまな場所で F1 キーを押せば、状況依存トピックを表示することもできます。オンライン バージョンは、弊社のドキュメント Web サイトに掲載されています。PDF バージョンはインストール DVD イメージに含まれています。

カスタム インストール

ここでは、Audit for Zen のインストールのために使用されるテクノロジおよび各種設定のカスタマイズについて説明します。Audit for Zen のインストールは Microsoft Installer（MSI）を使用します。AMsetup.ini ファイルには、カスタム インストール用に変更できるデフォルトの設定が含まれています。

インストーラー実行可能ファイル

ほとんどのインストール シナリオでは、インストーラー実行可能ファイルを使用する必要があります。この実行可能ファイルは InstallShield パッケージで、インストールを実行する前にいくつかのチェックを行います。Windows が 32 ビット版か 64 ビット版かの検出、適切なインストールの起動、およびシステムに適合するすべての 32 ビット /64 ビット クライアント コンポーネントの提供を行います。

次の表は Windows オペレーティング システムでの Audit for Zen インストーラーについて説明しています。

製品	インストール パッケージ	説明
Audit for Zen Server	Install_AuditMaster.exe	◆32 ビット オペレーティング システムへ 32 ビット エンジンをインストール ◆64 ビット オペレーティング システムへ 64 ビット エンジンをインストール ◆すべてのクライアント コンポーネントをインストール
Audit for Zen Client	Install_AuditMaster.exe	◆32 ビット オペレーティング システムへ 32 ビット クライアントをインストール ◆64 ビット オペレーティング システムへ 64 ビット クライアントをインストール

AMsetup.ini 設定

AMsetup.ini ファイルには、標準的なインストールに必要な設定がすべて含まれています。このファイルは Install_AuditMaster.exe によって使用され、その .exe を使用する .msi ファイルと同じフォルダーに配置されています。

AMsetup.ini は、インストール時に適用される一連のプロパティで構成されています。ファイル内のコメント行では、各設定の説明と指定可能な値が記載されています。

注意 組み込む製品エディションに付属している固有の AMsetup.ini ファイルを使用する必要があります。インストーラー技術およびインストール設定はバージョンごとに異なる可能性があるため、このファイルは製品と一致していなければなりません。

次の表は、AMsetup.ini のプロパティ設定を示しています。各設定はカテゴリ別に分類されています。各設定の値はキーに含まれています。

カテゴリ	キー
Directory Locations	PVSW_AM_INSTDIR32 PVSW_AM_INSTDIR64
Destination Folder	PVSW_AM_SKIP_INSTALLDIR
Administrative Share Name	PVSW_AM_SHARE_NAME

カテゴリ	キー
License key	PVSW_AM_LICENSE_KEY
License key dialog	PVSW_AM_SKIP_LICENSE

Audit for Zen のインストール

3

初めてインストールする際、またはアップグレードする際の手順

以下のトピックで、Audit for Zen をインストールまたはアップグレードする方法について説明します。

- 「事前の確認」
  - 「インストールに関する注記」
  - 「非表示の管理共有」
  - 「古いバージョンからのアップグレードに関する重要な情報」
- 「Audit for Zen のインストール」
- 「Audit for Zen Control Center をクライアントとしてインストール」
- 「Audit for Zen インストール後の操作に関する一般的な質問」
- 「Audit for Zen の削除」

事前の確認

Audit for Zen をインストールまたはアップグレードする前に、次の内容を通読されることをお勧めします。

- 「Audit for Zen をインストールするための準備」- システム要件やプラットフォーム固有の注意事項が記述されています。
- リリース ノート（readme_am.htm）-『User's Guide』には含まれない情報が記載されています。

以下のトピックでは、インストールを行う際の追加情報を提供します。

- 「インストールに関する注記」
- 「古いバージョンからのアップグレードに関する重要な情報」
- 「非表示の管理共有」

インストールに関する注記

どのプラットフォームに Audit for Zen をインストールする場合も、事前に以下のことに注意してください。

- Audit for Zen をインストールするシステムの完全な管理者レベルの権限を持っている必要があります。
- ウイルス対策アプリケーションを無効にすることをお勧めします。インストールの直後に、これらを再度有効にすることができます。ウイルス対策アプリケーションを無効にしない場合は、インストール タスクを実行する許可を求められます。
- Zen データベース エンジンは AZ のインストール時に停止および再起動されます。このため、業務に支障のない時間帯をお選びください。
- AZCC（Audit for Zen Control Center）をインストールして Zen サーバーにアクセスする場合、そのシステムのセキュリティが有効になっており、セキュリティ ポリシーが混合またはデータベースに設定されているときには、「Zen セキュリティ下での Audit for Zen の実行」を参照してください。『*Advanced Operations Guide*』に記載されているセキュリティ機能を確認することにより、Zen セキュリティ環境で AZ を構成する準備をします。データベース セキュリティが有効になっているインストールでは、Zen Control Center（ZenCC）で、Zen エンジンの［**プロパティ**］>［**アクセス**］ウィンドウに含まれる［**クライアント資格情報の入力要求**］設定をオンにする必要があることに留意してください。
- インストールは、インストールを行っているユーザーの %temp% ディレクトリにログ ファイルを作成します。*nn* はバージョンを表します。
  - 32 ビット システム：Zen_v*nn*_Audit for Zen_x86_Install.log
  - 64 ビット システム：Zen_v*nn*_Audit for Zen_x64_Install.log
- 32 ビットのインストーラー SetupAuditMaster32_x86.exe は、64 ビット Windows ではサポートされません。

古いバージョンからのアップグレードに関する重要な情報

Actian は、PSQL の名前を Zen に変更しました（v14 以降）。この名前変更により、Audit for Zen ファイルの場所が変わりました。Audit for Zen v15 にアップグレードする際、既存の監査レコード、構成設定、クエリ、および警告が不要な場合は、Audit for Zen v15 をインストールする前に以前の Audit for PSQL を削除するだけです。その後、新しいインストールで、新しい監査の構成、クエリ、および警告を作成します。照会できるのは新しい監査レコードのみで、以前にキャプチャした監査レコードにはアクセスできません。

その一方で、以前のインストールのすべてを引き続き使用したい場合は、Audit for Zen v15 インストールで再利用する特定のファイル ディレクトリのコピーを手動でバックアップしておく必要があります。全体的な手順は以下のとおりです。

1. 特定の既存の Audit for PSQL ファイル ディレクトリをコピーして保存します。
2. Audit for PSQL を削除します。
3. Zen v15 へアップグレードします。

4 Audit for Zen v15 をインストールします。

5 保存したファイルを、Audit for Zen v15 内の対応する場所にコピーします。

以下のタスクでは、Zen データベース エンジンを起動および停止する必要があります。データを操作するのに最も都合の良い時間帯をお選びください。詳細な手順は次のとおりです。

1 バックアップの場所にディレクトリを作成します。たとえば、%temp%¥AZ_Save などとします。

2 すべてのデータベース サービスを停止します。

3 既存のインストールで Audit for Zen の共有の場所を探します。デフォルトの場所は次のとおりです。

- 64 ビット Actian Zen v14 のデフォルトは、C:¥Program Files (x86)¥Actian¥Zen¥Audit
- 64 ビット Actian PSQL v12 のデフォルトは、C:¥Program Files (x86)¥Pervasive Software¥PSQL¥Audit
- 32 ビット Actian Zen v14 のデフォルトは、C:¥Program Files¥Actian¥Zen¥Audit
- 32 ビット Actian PSQL v12 のデフォルトは、C:¥Program Files¥Pervasive Software¥PSQL¥Audit

4 このディレクトリから、最初の手順で作成したバックアップ場所へ以下のフォルダーをコピーします。

- Arch
- Comp
- DATA
- Empty

5 これで、すべてのデータベース サービスを再起動して、ここに記載されている残りの手順を続行できます。

6 既存の Audit for PSQL に対してカスタム インストール場所を使用しており、Audit for Zen v15 でもカスタムの場所を使用する予定である場合は、Audit for Zen v15 で再使用するために、その場所を書き留めておきます。

7 場所がデフォルトであろうとカスタムであろうと、この共有にはデフォルトの名前 PVSWAUDIT$ が付けられます。カスタムの共有名を使用している場合は、Audit for Zen v15 でも同じ名前を使用する必要があります。共有名を調べるには、プロンプトで「`net share`」を実行します。次のような情報が返されます。

```
PVSWAUDIT$    C:¥ProgramData¥Actian¥Zen¥Au... Automatically created by AM
```

この例は、デフォルトの共有名を示しています。カスタム名は、割り当てられたものになります。表示されるパス名が長すぎる場合、パス全体を見るには「`net share <`**共有名**`>`」を実行します。

8 Audit for PSQL を削除します。

すべてのデータと構成設定を削除するかどうかを確認するメッセージが表示されたら、削除しないで残すことを選択します。これはインストール ウィザードでは、削除するためのチェック ボックスを選択**しない**ことを意味します。

9 Zen v15 へアップグレードします。

10 「Audit for Zen のインストール」に記載されている手順に従って、Audit for Zen v15 をインストールします。カスタム共有名を使用する場合は、以前の Audit for PSQL インストールから書き留めた同じ値を使用します。

11 Audit for Zen v15 のインストール後、Zen v15 データベース エンジン サービスを停止します。

12 Arch、Comp、DATA、および Empty フォルダーのバックアップを Audit for Zen v15 インストールの C:¥ProgramData¥Actian¥Zen¥Audit にコピーします。その際、既存のフォルダーとその内容を上書きすることを許可します。

13 Zen v15 データベース エンジンを再起動します。

14 Audit for Zen Control Center（AZCC）を起動し、以前のインストールの構成設定が期待どおりに機能しているか、また、監査レコードを見ることができるかを確認します。確認できたら、バックアップと以前のインストールの両方にあるフォルダーを削除することができます。

非表示の管理共有

Zen サーバーに Audit for Zen をインストールする場合、デフォルトのインストール設定では、いくつかの AZ コンポーネントへの非表示の管理共有が作成されます。デフォルトでは、共有名は PVSWAUDIT$、パスは C:¥ProgramData¥Actian¥Zen¥Audit ですが、共有名はインストール時に別の値に設定することができます。また、共有を非表示にすることは必須ではありません。共有を使用する場合には、次のことを考慮してください。

- AZCC をリモート クライアントにインストールする場合は、クライアント システムにサーバー上のこの共有へのアクセス権を提供する必要があります。詳細については、「Audit for Zen へのアクセス」を参照してください。
- Audit for Zen が正常に機能するために、ファイアウォール システムに共有を登録する必要があります。
- セキュリティ要件を満たすために、共有を明示的なローカル パス名に置き換えることができます。そうすることで、リモート クライアントがブロックされ、ローカル システムへのアクセスのみに制限されます。手順については、「ネットワーク共有をローカル パスに置き換える」を参照してください。

Audit for Zen のインストール

Audit for Zen には、Server Monitor と、Audit for Zen Control Center（AZCC）と呼ばれる Viewer クライアントという 2 つの構成要素があります。Zen Enterprise Server や Cloud Server では、Monitor と AZCC が一緒にインストールされます。Zen Client、Reporting Engine、または Workgroup では、監査レコードを表示するために、リモートの Zen サーバー上の Audit for Zen Server Monitor に接続するための AZCC が単独でインストールされます。

Audit for Zen ライセンスが認証するサーバー インストールは 1 つですが、お使いのネットワーク環境で必要な数だけクライアントをインストールすることができます。手順については、「Audit for Zen Control Center をクライアントとしてインストール」を参照してください。

Audit for Zen インストーラーは、それをインストールするシステムで実行する必要があります。ローカルに Audit for Zen をインストールするために、別のシステムからインストーラーを実行することはできません。

メモ Zen データベース エンジンは AZ のインストール時に停止および再起動されます。このため、業務に支障のない時間帯をお選びください。

▶▶ Audit for Zen をインストールするには

1 管理者権限を持つシステムにログオンします。

2 ダウンロードしたインストーラー プログラムを起動します。

ダウンロード ディレクトリにある AuditforZen-15.00.0xx.000-win.exe ファイルを実行します。

3 ［ようこそ］ページで［**次へ**］をクリックします。

4 ［**使用許諾契約**］では、条項に同意し、［**次へ**］をクリックします。

5 ［**ライセンス**］では、Audit for Zen の製品キーを入力して［**次へ**］をクリックします。キーを入力しない場合は、試用期間がすぐに始まります。ライセンスがない場合は、試用期間中だけ監査を行えます。その後、監査は終了しますが、ログに既に記録された監査レコードを照会し、表示することはできます。詳細については、「認証ライセンス」を参照してください。

6 ［**インストール先のフォルダ**］では、必要に応じて、デフォルトのインストール先を変更することができます。64 ビット環境では、32 ビットと 64 ビットのコンポーネントは、Zen サーバーを実行しているのと同じシステム上にある必要があり、かつ異なる場所にインストールする必要があります。インストール先の場所を変更したら、［**次へ**］をクリックします。

7 ［**共有名**］では、Audit for Zen のデータ フォルダーのパスに割り当てる共有名の入力を求められます。デフォルトの共有名の PVSWAUDIT$ をそのまま使用するか、または IT 部門から指定された別の共有名を入力して、［**次へ**］をクリックします。

8 これで、プログラムをインストールする準備ができました。設定を変更する場合は［**戻る**］をクリックします。続行する場合は［**インストール**］をクリックします。

9 インストールが終了したら［**完了**］をクリックします。

10 監査レコードの暗号化を設定するダイアログが表示されます。暗号化を行う場合は、［監査レコードを暗号化する］を選択して［設定］をクリックします。暗号化を行わない場合は、［キャンセル］をクリックします。この設定は、スタート メニューから［Actian Audit for Zen 15］>［Audit for Zen 暗号化の設定］をクリックして後から変更することも可能です。

これで、「Audit for Zen へのアクセス」の説明に従って Audit for Zen を開始し、Zen サーバーに接続することができるようになります。

Audit for Zen Control Center をクライアントとしてインストール

Audit for Zen は、Zen サーバーに Control Center クライアント（AZCC）を自動的にインストールします。AZCC だけを Zen Client、Workgroup、Reporting Engine システムにインストールすることもできます。AZCC はこれらのシステムにインストールされると、リモート クライアントとして Zen サーバー上の Audit for Zen に接続して監査レコードを作業できるようになります。

▶▶ AZCC をクライアントとしてインストールするには

AZCC をクライアントとしてインストールするシステムには、あらかじめ Zen Client、Workgroup、Reporting Engine がインストールされて構成されている必要があります。

1 管理者権限を持つシステムにログオンします。

2 ダウンロードしたインストーラー プログラムを起動します。

ダウンロード ディレクトリにある AuditforZen-15.00.0xx.000-win.exe ファイルを実行します。

3 ［ようこそ］ページで［**次へ**］をクリックします。

4 ［**使用許諾契約**］では、条項に同意し、［**次へ**］をクリックします。

5 ［**インストール先のフォルダ**］では、必要に応じて、デフォルトのインストール先を変更することができます。インストール先を変更したら、［**次へ**］をクリックします。

6 これで、プログラムをインストールする準備ができました。設定を変更する場合は［**戻る**］をクリックします。続行する場合は［**インストール**］をクリックします。

7 インストールが完了すると、通知が表示されます。［**完了**］をクリックします。

これで、「Audit for Zen へのアクセス」の説明に従って Audit for Zen を開始し、Zen サーバーに接続することができるようになります。

Audit for Zen インストール後の操作に関する一般的な質問

以下の項目では、インストール プログラムを実行した後の疑問に対する回答を挙げます。

Audit for Zen リリース ノートはどこにありますか？

readme_am.htm ファイルは次の場所で入手できます。

- 製品と一緒にインストールされています。デフォルトのインストール先は C:¥Program Files (x86)¥Actian¥Zen¥Audit¥Docs です。

AZ 用に Zen Control Center（ZenCC）で何かを設定する必要はありますか？

いいえ。Audit for Zen は ZenCC での特別な設定を必要としません。すべての設定と構成は AZCC で行われます。ただし、Zen サーバーで Btrieve セキュリティを有効にしている場合の［クライアント資格情報の入力要求］オプションは除きます。

Audit for Zen のインストールによりログ ファイルが作成されますか？

はい。インストールにより、インストールを行っているユーザーの %temp% ディレクトリに以下のログ ファイルが作成されます（*nn* はバージョンです）。

- 32 ビット システム：Zen_v*nn*_AuditMaster_x86_Install.log
- 64 ビット システム：Zen_v*nn*_AuditMaster_x64_Install.log

アップグレードしても Audit for Zen のデータ、クエリ、および設定は保持されますか？

はい、「古いバージョンからのアップグレードに関する重要な情報」の指示に従えば、保持されます。

Audit for Zen の削除

Audit for Zen をアンインストールすると、インストール先の Audit フォルダーにあるコンポーネントが削除されます。他の場所にあるファイルは、削除されず、AZ が同じ場所に再インストールされた場合に再利用されます。

メモ AZ の削除では、Zen データベース サービスの停止、再起動が行われます。このため、業務に支障のない時間帯をお選びください。

▶▶ Audit for Zen を削除するには

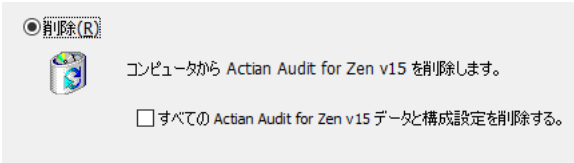
Audit for Zen は、Windows のコントロール パネルから通常の方法で削除できます。Actian Audit for Zen v15 として一覧に表示されます。

▶▶ Audit for Zen を再インストールして既存のデータと設定を引き続き使用するには

Audit for Zen を再インストールして、既存の監査データ、構成設定、クエリ、および警告を引き続き使用するつもりならば、次の手順に従ってください。

1 Audit for Zen の削除を開始する前に、そのインストールの場所を調べます。デフォルトのインストール先は C:¥Program Files (x86)¥Actian¥Zen¥Audit です。カスタム インストールを行った場合は、この Audit フォルダーの場所が違うかもしれません。違う場合は、Audit for Zen を再インストールするときにその場所を選択できるよう、書き留めておいてください。

2 Audit for Zen を削除するとき、既存の監査データ、構成設定、クエリ、および警告を削除するためのチェック ボックスがオンになっていないことを確認してください。次の図に示すように、デフォルト設定であるオフのままにします。



3 このチェック ボックスをオンにしない限り、次のいずれかを実行できます。

- 再度 Audit for Zen をインストールするときに、以前のインストール場所を再利用する。
- Audit for Zen を新しい場所にインストールし、その後、カスタムの Audit フォルダーを新しいインストレーションの Audit フォルダーにコピーする。
- v14 以前の Audit for Zen を Audit for Zen v15 以降にアップグレードし、既存の監査データ、構成設定、クエリ、および警告をアップグレード インストレーションに移行する。この方法については、「古いバージョンからのアップグレードに関する重要な情報」で詳しく説明します。

▶▶ クライアントから Audit for Zen を削除するには

クライアントから Audit for Zen を削除する方法は、サーバーから Audit for Zen を削除する方法と同様です。

▶▶ Audit for Zen 削除ログを表示するには

Audit for Zen を削除すると、現在のユーザーの %temp% フォルダーに次のログ ファイルが作成されます。

Zen_v15_AuditMaster_Repair_Remove.log

Audit for Zen について

4

Audit for Zen の基本の概要

以下のトピックでは、一般的な使用方法での注意点について説明します。

- 「Audit for Zen へのアクセス」
- 「ユーザー パスワードの変更」
- 「Zen セキュリティ下での Audit for Zen の実行」

Audit for Zen へのアクセス

Audit for Zen Control Center を使用するには、ユーザー名とパスワードによる認証が必要です。アカウントの種類によって、監査レコードにアクセスしたり AZCC メニュー コマンドを利用したりできるかどうかが決まります。

- **ユーザー**
  通常のユーザーは、ログに記録された監査レコードの照会と表示ができるほか、監査レコードのアーカイブを管理できます。
- **管理者**
  Audit for Zen 管理者は、通常のユーザーの権限に加えて、ユーザーの管理、ステータス ログの表示、監査構成の作成、システム設定の調整、および警告の作成を行う権限も持っています。

組み込まれている AZ 管理者アカウントについては、ユーザー名が admin、初期パスワードが MASTER となります。パスワードは大文字と小文字を区別しますが、ユーザー名は区別しません。

AZ 管理者のパスワードは変更することをお勧めします。その手順については、「ユーザー パスワードの変更」を参照してください。Audit for Zen の管理者アカウントとすべてのユーザー ログインは、内部専用であり、ネットワークやローカルのオペレーティング システムのユーザー ログイン、Windows や Zen で使用されているデータベースのユーザー ログインとは関係ないことに留意してください。

Audit for Zen へのログインと Windows へのログインや Zen データベースへのログインとの関係の詳細については、「Zen セキュリティ下での Audit for Zen の実行」と「Zen セキュリティの下での監査レコードの表示」を参照してください。

▶▶ Audit for Zen にログインするには

1 AZCC で、監査サーバー名を右クリックして［**ログイン**］を選択するか、またはそのサーバー ノードを展開します。

2 ［ログイン］ダイアログ ボックスで、Audit for Zen ユーザーの名前とパスワードを入力して［OK］をクリックします。

インストール後に初めてログインする場合は、Audit for Zen 管理ユーザーとしてログインする必要があります。

次の作業は、「監査の設定での作業」の記述に従って、データ監視を構成することです。

▶▶ Zen Client からログインするには

上記の手順は、Zen Client の AZCC から Zen サーバーの Audit for Zen への接続を作成した後にも使用できます。この接続を作成するには、次の手順に従ってください。

メモ データベース セキュリティ設定によっては、Zen サーバーの Audit for Zen が Zen Client の AZCC からのログインを認識できるように、ネットワークと Zen サーバーの両方に認証されたアカウントで Windows システムにログインする必要があります。詳細については、「Zen セキュリティの下での監査レコードの表示」、および『*Advanced Operations Guide*』のセキュリティに関するトピックを参照してください。

リモート Zen サーバーの Audit for Zen への AZCC の接続

Zen サーバーに Audit for Zen をインストールすると、ホスト システムが AZCC 内の監査サーバー リストに自動的に追加されます。Zen Client、Workgroup、または Reporting Engine の Audit for Zen の場合、Zen サーバーの Audit for Zen にリモート接続するには、次の手順を使用します。セキュリティ ポリシーを混合またはデータベースに設定した Zen データベース サーバーへのクライアントからのアクセスについては、「Zen セキュリティ下での Audit for Zen の実行」を参照してください。

1 クライアント システムで、Zen Client、Workgroup、または Reporting Engine がインストールされていることを確認します。

2 クライアント システムで、AZCC を開始し、［**サーバー**］>［**追加**］を選択するか、または［ようこそ］タブの［**サーバーの追加**］リンクをクリックします。

3 ［サーバーの追加］ダイアログで、以下の 1 つを使用して Audit for Zen の amserver ファイルのパスを入力します。

- アクセス可能な Zen サーバーの名前。この名前はネットワーク上で参照できます。
- このシステムの完全な名前。例：zen-server.englab.local。
- このシステムの IP アドレス。

デフォルトのインストールでは、amserver は ¥¥<*server*>¥PVSWAUDIT$¥DATA にあります。

4 したがって、amserver ファイルのパスは次のようになります。

5 ［OK］をクリックしてシステムを［監査サーバー］リストに追加します。

6 新しくリストに追加されたサーバーを右クリックし、［**ログイン**］を選択するか、またはそのサーバー ノードを展開します。

7 ［ログイン］ダイアログ ボックスで、Audit for Zen ユーザーの名前とパスワードを入力して［OK］をクリックします。

通常、次の作業は、「監査の設定での作業」の説明に従ってデータ監視を構成するか、あるいは、テーブルまたはファイルが既に監視されている場合はクエリを実行することです。

ユーザー パスワードの変更

Audit for Zen へのアクセスはパスワードで保護されています。サーバーにログインしている間、そのサーバーについてのみパスワードを変更することができます。アクセスする各サーバーの Audit for Zen パスワードは、同じユーザー名を使用する場合でもそのサーバーに固有のものです。

▶▶ パスワードを変更するには

1 AZCC でサーバーにログインします。

2 ［**サーバー**］>［**パスワードの変更**］を選択します。

3 ［パスワードの変更］ダイアログ ボックスで、**現在のパスワード**を入力します。

パスワードは大文字と小文字を区別し、最長 40 文字まで指定できます。ダブルバイトの文字セットの場合は、最大 20 文字までです。

4 **新しいパスワード**を対応する 2 つのフィールドに入力し、［OK］をクリックします。

パスワードが変更されます。

組み込まれている AZ 管理者アカウントについては、ユーザー名が admin、デフォルトの初期パスワードが MASTER となります。管理者のパスワードは変更することをお勧めします。AZ の管理者アカウントとすべてのユーザー アカウントは Audit for Zen で内部的に使用され、ネットワークやオペレーティング システムのユーザー ログイン、Windows や Zen で使用されているデータベースのユーザー ログインとは関係ないことに留意してください。

Audit for Zen へのログインと Windows へのログインや Zen データベースへのログインとの関係の詳細については、「Zen セキュリティ下での Audit for Zen の実行」と 「Zen セキュリティの下での監査レコードの表示」を参照してください。

Zen セキュリティ下での Audit for Zen の実行

Audit for Zen はすべての Zen データベース セキュリティ設定と互換性があります。Audit for Zen インストールは、Zen DefaultDB データ ディレクトリ一覧に Audit for Zen 内部データベースを追加します。インストール後、DefaultDB のセキュリティ設定と同様の保護が Audit for Zen データベースに提供されます。

以下の表では、標準セキュリティの設定をまとめています。最初の 2 行は設定を示しており、次の 2 行はログインと権限について説明し、最後の行では提供される保護を列挙しています。

セキュリティ	クラシック	混合	データベース
DefaultDB のデータベース セキュリティ	**オン**	**オン**	**オン**
DefaultDB の Btrieve セキュリティ	**オフ**	**オン**	**オン**
AZCC での認証	Audit for Zen ログイン	• Audit for Zen ログイン • OS またはネットワーク ログイン	• Audit for Zen ログイン • Zen ログイン
必要なデータベース ユーザー	なし	• DefaultDB 下の Zen ユーザー。OS ログインまたはネットワーク ログインと一致している必要があります。 • Zen ユーザーは、既存のクエリを実行するために、少なくとも選択権限を持っている必要があります。 • 新しい Audit for Zen クエリを作成したり保存したりするには、Zen ユーザーは更新権限および挿入権限を持っている必要があります。	• DefaultDB 下の Zen ユーザー • Zen ユーザーは、既存のクエリを実行するために、少なくとも選択権限を持っている必要があります。 • 新しい Audit for Zen クエリを作成したり保存したりするには、Zen ユーザーは更新権限および挿入権限を持っている必要があります。
保護対象	Audit for Zen のアクセス	• Audit for Zen のアクセス • データおよび .ddf ファイルの監査 • ZenCC SQL Editor のアクセス • Btrieve ファイルのアクセス	• Audit for Zen のアクセス • データおよび .ddf ファイルの監査 • ZenCC SQL Editor のアクセス • Btrieve ファイルのアクセス

補注

- Audit for Zen のログインと Zen のログインは別個の認証で、関係はありません。しかしながら、両方のログインがそのときに必要な場合には、AZCC は両方を入力する 1 つのダイアログを提示することがあります。
- DefaultDB にデータベース セキュリティ ポリシーを設定し、リモート クライアントから AZCC を使用したい場合には、ZenCC で、Zen サーバー エンジンの［**プロパティ**］>［**アクセス**］画面にある［**クライアント資格情報の入力要求**］をオンにする必要があります。この設定により、AZCC でリモート ユーザー用のログイン ダイアログが提供されます。
- Audit for Zen をインストールした後に、Zen のセキュリティ ポリシーの変更が必要になった場合は、まず、すべての AZCC クライアントを閉じます。これを行わないと、Zen によりステータス コード 94 のアクセス権エラーが返されます。

- 現在、Btrieve の混合セキュリティまたはデータベース セキュリティを使用しておらず、Audit for Zen セキュリティを強化するためだけにこれを有効にする場合には、DefaultDB はグローバル構成であり、Zen を使用するすべてのトランザクショナル Btrieve アプリケーションに適用されるということを覚えておいてください。Audit for Zen のセキュリティを有効にすると、Zen または Btrieve データへのアクセスを管理する方法の変更が必要になる場合があります。

「Zen セキュリティの下での監査レコードの表示」も参照してください。Zen セキュリティ環境におけるデータベース操作の詳細については、『*Advanced Operations Guide*』を参照してください。

Audit for Zen Control Center の使用

5

AZCC のツアーとタスクの参照一覧

Audit for Zen Control Center（AZCC）は、Audit for Zen アプリケーションのユーザー インターフェイスです。そのウィンドウには、AZ の監視用に構成された Zen サーバー インストレーションの一覧が表示されます。監視タスクを行うためのさまざまな情報とオプションが提供されます。

Audit for Zen がインストールされて実行される Zen サーバー データベースは、監査サーバーと呼ばれます。監視は、データベースの活動を読み取り、監査レコードをログに記録します。このログは後で、AZCC クライアントで照会されて表示されます。

データ ツリーは、監査システムを表します。ツリーの各ブランチには、Audit for Zen サーバーとその現在のビューファイル、アーカイブされたファイル、および保存されたクエリが格納されています。詳細については、「Audit for Zen Control Center のビジュアル リファレンス」を参照してください。

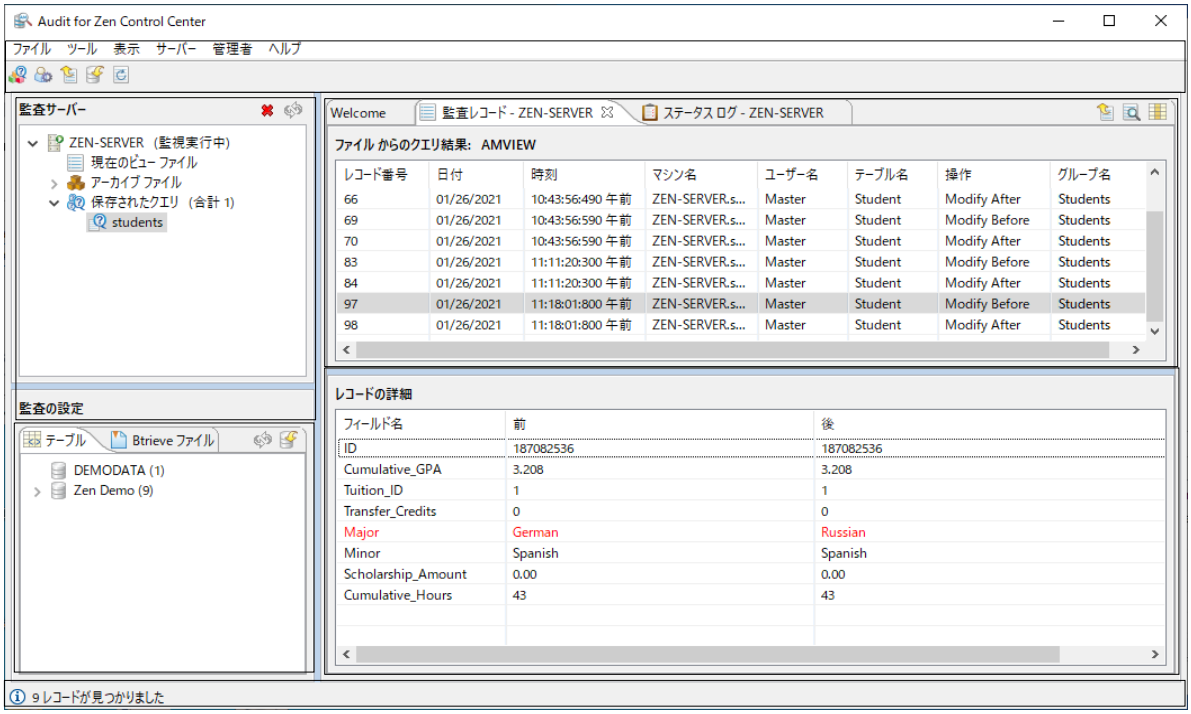
Audit for Zen Control Center のビジュアル リファレンス

ユーザーとしてログインし、監査レコードを表示するクエリを実行すると、[Audit for Zen Control Center]（AZCC）ウィンドウに下記の例のような内容が表示されます。この例では、Demodata サンプル データベースのレコードを監視しています。

以下のトピックでは、AZCC の使用方法についてのより詳しい説明を提供します。

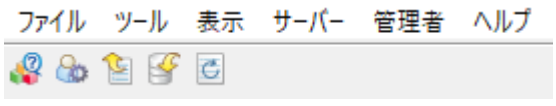
- 「メニュー、ツールバー、およびタブ」
- 「[監査サーバー] リスト」
- 「[監査レコード] タブ」
- 「監査レコードの詳細」
- 「[ステータス ログ] タブ」
- 「環境設定の表示」

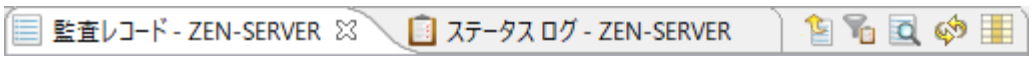
詳細を見るには、一覧内の項目をクリックするか、または次の例の領域をクリックします。



メニュー、ツールバー、およびタブ

AZCC のメニューおよびツールバーのオプションの詳細については、次のメイン ウィンドウとタブの画像内のメニュー名、アイコン、またはタブをクリックします。タブには、クエリ結果を表示するタブと、ログ情報を表示するタブがあります。



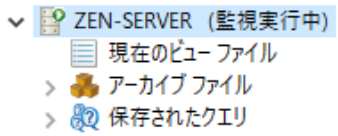


メニューまたは ツール バー	コマンド	説明
ファイル	**クエリ** または 	レコードを検索するために Query Builder を開きます。クエリは、ユーザー、日付、操作などの条件に基づいて作成できます。詳細については、「監査レコードの照会」を参照してください。
	詳細なクエリ	Query Builder では作成できない複雑なクエリを作成できる Advanced Query Builder を開きます。詳細については、「詳細なクエリを構築する」を参照してください。
	終了	ログアウトして AZCC を閉じるには、[終了] を選択します。
ツール	**検索** または 	[監査レコード] タブで特定のテキストを検索します。詳細については、「監査レコード またはログ レコードの検索」を参照してください。
	エクスポート または 	現在のビュー ファイルまたはアーカイブされたビュー ファイルをテキスト ファイルにエクスポートします。詳細については、「テキスト ファイルへの監査レコード またはログ レコードのエクスポート」を参照してください。
	スキーマのインポート または 	ログに記録されたレコードの内容を表示する際に使用する DDF 情報をインポートします。詳細については、「データベースからのスキーマのインポート」を参照してください。
	アーカイブの管理	アーカイブされた監査レコードを管理するためのウィンドウを開きます。詳細については、「アーカイブを管理する」を参照してください。
表示	**環境設定**	タブの外観と一覧表示されるアーカイブの数を設定するウィンドウを開きます。詳細については、「環境設定の表示」を参照してください。
サーバー	**追加**	AZCC クライアントから Audit for Zen サーバーへの接続を作成します。詳細については、「Audit for Zen へのアクセス」を参照してください。
	削除	Audit for Zen サーバー接続を削除します。サーバーは新しい監査レコードをキャプチャし続けますが、クライアントは現在、それらにアクセスすることはできません。ただし、現在のビュー ファイルやアーカイブ ファイルに既に入っているレコードを照会、表示することはできます。
	現在のビュー ファイルの更新 または 	監査ログを基に現在のビュー ファイルを更新し、クエリで最新の監査レコードが表示されるようにします。
	パスワードの変更	Audit for Zen サーバーに現在ログインしているユーザーのパスワードを変更します。詳細については、「ユーザー パスワードの変更」を参照してください。

メニューまたはツール バー	コマンド	説明
管理者 管理者ログインのみが利用可能	**ステータス ログの表示**	Audit for Zen の活動のステータス ログを表示します。
	サーバー設定	Audit for Zen サーバーのパスやその他のシステム設定を管理します。
	ユーザーのメンテナンス または 	Audit for Zen ユーザーを追加または削除することができます。
	警告の管理	クエリに基づいて警告を作成します（たとえば、特定のユーザーが変更を行った場合や、$10,000 を超える小切手が振り出された場合など）。作動した警告は、監視対象のレコードにベル アイコン 🔔 を使ってフラグを付け、Windows のアプリケーション イベント ログにエントリを書き込みます。詳細については、「警告での作業」を参照してください。
ヘルプ	**目次**	ユーザー ガイドのオンライン版を提供します。
	AZCC ログ	イベント ログを表示します。
	AZCC ログのクリア	イベント ログを消去します。
	バージョン情報	Audit for Zen および Java のバージョン情報を表示します。
メニュー コマンドのないアイコン	**フィルター** 	表示されるステータス ログ メッセージを種類別、日付別にフィルターします。
	ステータス メッセージの更新 	[ステータス ログ] タブで、ログに記録されたステータスおよびエラー メッセージの一覧を更新します。
	表示する列の選択 	監査レコードのビューに表示する列を選択します。詳細については、「[監査レコード] タブでの作業」を参照してください。

[監査サーバー] リスト

[監査サーバー] パネルには、Audit for Zen がインストールされている Zen サーバーのインスタンスが一覧表示されます。サーバー名はマシンの名前です。各サーバー名を展開すると、詳細が表示されます。アイコンを右クリックすると、さまざまなコマンド オプションが表示されます。現在のビュー ファイルやアーカイブ ファイル、またはその組み合わせに対してクエリを実行することができます。保存したクエリは、再利用できるように一覧表示されます。*監視*は、データベースの活動をキャプチャする、Audit for Zen の機能です。

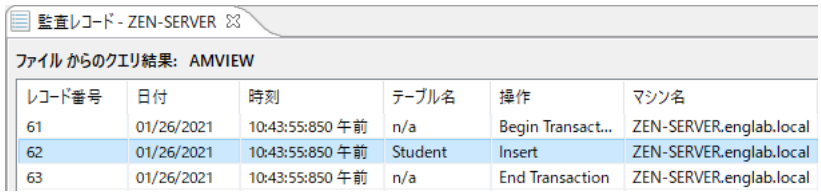


監査の設定

監査の設定は、活動を監視するデータベース テーブルまたは Btrieve ファイルのグループ（1 つ以上）から成る集合です。[監査の設定] パネルには、データベース テーブル用のタブと Btrieve ファイル用のタブがあります。詳細については、「監査の設定での作業」を参照してください。

［監査レコード］タブ

現在のビュー ファイルまたはアーカイブ ファイルに対してクエリを実行した場合、［監査レコード］タブにそのクエリ結果が表示されます。

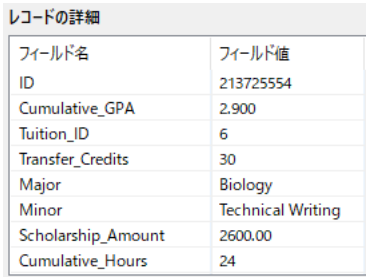

監査レコード - ZEN-SERVER

ファイル からのクエリ結果: AMVIEW

レコード番号	日付	時刻	テーブル名	操作	マシン名
61	01/26/2021	10:43:55:850 午前	n/a	Begin Transact...	ZEN-SERVER.englab.local
62	01/26/2021	10:43:55:850 午前	Student	Insert	ZEN-SERVER.englab.local
63	01/26/2021	10:43:55:850 午前	n/a	End Transaction	ZEN-SERVER.englab.local

監査レコードの詳細

監査レコードは、データベースの活動と Audit for Zen の操作の両方をキャプチャします。データベースの活動については、［AZCC］ウィンドウの下方部分にある監査レコードの詳細領域に、活動が発生したデータベースのフィールドが示されます。

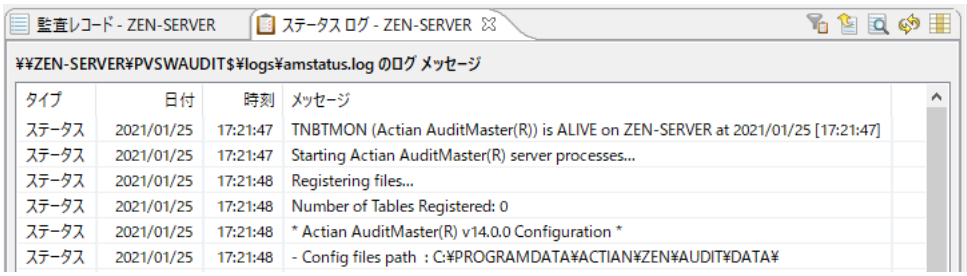

レコードの詳細

フィールド名	フィールド値
ID	213725554
Cumulative_GPA	2.900
Tuition_ID	6
Transfer_Credits	30
Major	Biology
Minor	Technical Writing
Scholarship_Amount	2600.00
Cumulative_Hours	24

メモ データ レコードの詳細は、データの表示に使用する Audit for Zen にデータベース スキーマがインポートされているかどうかに応じて、人間の言語または 16 進形式で表示されます。詳細については、「監査の設定での作業」を参照してください。

［ステータス ログ］タブ

［ステータス ログ］タブを表示するには、［**管理者**］>［**ステータス ログの表示**］を選択します。このログには、監視対象のデータベースの活動でなく、Audit for Zen の活動が表示されます。


監査レコード - ZEN-SERVER　ステータス ログ - ZEN-SERVER

¥¥ZEN-SERVER¥PVSWAUDIT$¥logs¥amstatus.log のログ メッセージ

タイプ	日付	時刻	メッセージ
ステータス	2021/01/25	17:21:47	TNBTMON (Actian AuditMaster(R)) is ALIVE on ZEN-SERVER at 2021/01/25 [17:21:47]
ステータス	2021/01/25	17:21:47	Starting Actian AuditMaster(R) server processes...
ステータス	2021/01/25	17:21:48	Registering files...
ステータス	2021/01/25	17:21:48	Number of Tables Registered: 0
ステータス	2021/01/25	17:21:48	* Actian AuditMaster(R) v14.0.0 Configuration *
ステータス	2021/01/25	17:21:48	- Config files path : C:¥PROGRAMDATA¥ACTIAN¥ZEN¥AUDIT¥DATA¥

右上のアイコンを使用すると、ステータス ログのエントリについて、種類別および日付別にフィルターする、ログ メッセージをテキスト ファイルとしてエクスポートする、文字列を検索する、タブを更新する、同タブに表示する列を選択するなどの操作を行うことができます。この例に示されている列は、選択可能な列をいくつか示したものです。詳細については、「ステータス ログのアクティビティの確認」を参照してください。

環境設定の表示

［監査サーバー］ツリーの［アーカイブ ファイル］に表示する項目の数を設定できます。また、［監査レコード］タブと［ステータス ログ］タブ内の列の表示に加えた調整を保存するオプションを設定することもできます。これらの設定を行う［環境設定］ダイアログを開くには、［**表示**］>［**環境設定**］を選択します。このダイアログの［テーブル レイアウト］では、セッションを変更しても保持される設定を選択できます。

監査の設定での作業

6

データの監査方法

Audit for Zen は、監査の設定に基づいて監査データをキャプチャします。監査の設定は、以下の項目を組み合わせたものです。

- Zen サーバー エンジンと共にインストールされた Audit for Zen サーバー
- Zen データベースからインポートされたスキーマ（存在する場合）
- 監視するファイルのグループ（1 つ以上）

Audit for Zen を実行する上でスキーマは必要ありませんが、スキーマによって、人間が監査レコードをテーブルの行として読み取れるようになります。また、より正確な警告を発することができるようになります。

スキーマを Audit for Zen にインポートすると、そのスキーマで作成されたすべてのグループが、そのスキーマを使用するテーブルを監視できるようになります。実際、追加するテーブルを参照する際には、そのスキーマを使用するテーブルのみが表示されます。

スキーマをインポートしない場合でも、監視する Btrieve ファイルのグループを作成することが必要です。ファイルを参照する際には、Btrieve ファイルのみが表示されます。

1 つのグループを作成し、そのグループにすべての監視対象ファイルを追加することもできますが、そうすると、行いたい監査の計画が立てにくくなる可能性があります。複数のグループを作成したり、インポートした同じデータベース スキーマの複数のコピーの下にグループを作成したりすることで、監査活動が容易になります。

たとえば、顧客ごとに異なるファイルを監視する場合は、顧客ごとにグループを作成し、グループ下のすべてのファイルはその顧客用とすることができます。また、各顧客に同じスキーマをインポートし、スキーマ下のすべてのグループはその顧客用とすることもできます。インポートしたスキーマ、グループ、ファイルの編成は、思考を整理する目的でのみ行うものであり、ログに記録される監査レコードや、監査レコードを生成するデータベース操作には影響しません。

要約すると、次のようになります。

- インポートされるスキーマごとに 1 つ以上のグループを作成できる。各グループには 1 つ以上の監視対象テーブルを追加できる。
- インポートしたスキーマの監視対象テーブルのどのグループでも、そのスキーマのみが使用される。
- スキーマのない Btrieve ファイルを監視するには、そのファイルの追加先となるグループを作成する必要がある。
- 1 つのテーブルやファイルは 1 つのグループにしか所属できない。特定のグループに一度追加すると、他のグループからは監視できない。

上記のコンセプトが実際に機能する仕組みを確認するため、下記の例を参照することをお勧めします。

1 「スキーマの管理」

2 「スキーマのあるデータ監視の構成」

3 「スキーマのないデータ監視の構成」

4 「テーブルまたはファイル別に監視する操作」

スキーマの管理

AZCC は、Zen データ辞書ファイル（DDF）が提供するスキーマを使用して、キャプチャされた監査データを人間に読み取れるようにすると共に、レコードのフィールド レベルで照会を行えるようにします。AZCC でデータベース スキーマをインポートすると、データベースのデータ ファイル ディレクトリから DDF が読み取られ、AZCC 専用のデータベースに保存されて、監査データの表示と照会に使用されます。

DDF がない場合は、監視対象ファイル内のキャプチャ済みデータ レコードは 16 進数の行として表示されるため、特定のデータ値について照会することはできません。ログに記録されたレコードの表示書式を設定する DDF がないと、データ ファイルに挿入されたレコードは次のように表示されます。

レコードの詳細

オフセット	データ															
	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	72	31	bd	0c	00	00	00	00	00	02	90	0f	06	00	00	00
00000010	00	00	03	0f	00	42	69	6f	6c	6f	67	79	20	20	20	20
00000020	20	20	20	20	20	20	20	20	20	00	54	65	63	68	6e	69
00000030	63	61	6c	20	57	72	69	74	69	6e	67	20	20	20	00	00
00000040	00	00	00	00	00	02	60	00	0f	00	18	00				

00000000	[rl▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯▯]
00000010	[▯▯▯▯▯Biology]
00000020	[▯Techni]
00000030	[cal Writing ▯▯]
00000040	[▯▯▯▯▯▯`▯▯▯▯▯]

スキーマのインポート後に挿入されたログ記録レコードは、次のように判読可能な形式で表示されます。

レコードの詳細

フィールド名	フィールド値
ID	213725554
Cumulative_GPA	2.900
Tuition_ID	6
Transfer_Credits	30
Major	Biology
Minor	Technical Writing
Scholarship_Amount	2600.00
Cumulative_Hours	24

スキーマをインポートしても、既にキャプチャされているレコードの表示は変更されません。スキーマのインポート前にキャプチャされたレコードは、引き続き 16 進文字として表示されます。同様に、スキーマを削除しても、スキーマが使用されていたときにログに記録されたレコードは何の影響も受けず、AZCC で表示されるときには引き続き判読可能です。レコードが上記のいずれの方法で表示されるかは、レコードがログに記録されたときにスキーマがインポートされていたかどうかによって決まります。

メモ V2 メタデータを使用するデータベースのスキーマをインポートする場合に、テーブル、列、またはインデックスの DDF 名が 40 文字を超えるときは、最初の 40 文字のみが表示されます。このようにテーブル名が切り詰められて表示されても、AZ の操作には影響しませんが、［AZCC］ウィンドウではレポートが読み難くなるかもしれません。

このスキーマに関するチュートリアルの残り部分では、以下のタスクについて説明します。

- 「データベースからのスキーマのインポート」
- 「監査の設定の削除」

データベースからのスキーマのインポート

次の例は、スキーマをインポートする方法を示します。

AZCC の［監査の設定］タブにおいて、Zen Demo という名前でインポートされたスキーマが Audit for Zen とともにインストールされていることに注目してください。これは Demodata サンプル データベースのスキーマです。この Zen Demo スキーマは現時点でも使用可能ですが、次の例を説明するため、Demodata スキーマが新しい監査の設定に再度インポートされます。

▶▶ Zen データベースからスキーマをインポートするには

1 ［**ツール**］>［**スキーマのインポート**］メニューを選択するか、またはツールバーの［**スキーマのインポート**］ボタン をクリックし、［スキーマのインポート］ダイアログ ボックスを開きます。ダイアログには、監査の設定を作成するのに使用できる、Zen サーバー上のデータベースが一覧表示されます。

2 一覧から、監視したいテーブルを定義しているスキーマを持つ**データベース**を選択します。

3 このデータベース名が、新しい監査設定の［**名前**］フィールドに自動的に入力されます。このデータベース名を別の名前に置き換えることもできます。スペースを含むすべてのキーボード文字が使用可能です。この名前は、このスキーマに対してキャプチャされたすべての監査レコードに関連付けられます。

4 監査の設定の**説明**を入力します。スペースを含むすべてのキーボード文字が使用可能です。この文字列は、監査の設定のプロパティに表示されます。

5 監査の設定の**バージョン**を入力します。スペースを含むすべてのキーボード文字が使用可能です。このバージョンは、このスキーマに対してキャプチャされたすべての監査レコードに関連付けられます。

入力した値は、AZCC で監査の設定名の後にかっこ付きで表示されます。ニーズに合ったバージョンを使用してください。バージョンに関する唯一の制限は、インポートするスキーマごとに一意でなければならないことです。

6 ［**インポート**］をクリックします。

選択した名前が監査の設定として表示され、バージョンが［AZCC］ウィンドウの左下に表示されます。これで、インポートしたスキーマを使用するテーブルのグループを追加、監視できるようになります。

インポートしたスキーマについては、以下のことに注意してください。

- スキーマをインポートして監査の設定を作成すると、Audit for Zen によりデータベースの DDF からテーブルおよび列の情報が読み取られ、Audit for Zen の内部に保存されます。その後でデータベース スキーマが修正され、そのスキーマが監査の設定にインポートしたスキーマと一致しなくなった場合は、監査レコードに対してどのようなクエリを実行しても、切り詰められたデータまたはそれより悪い結果が返される可能性があります。データベースの正しい監査を再開するには、スキーマを新しい監査設定にインポートし、その監査設定に監視対象ファイルを追加する必要があります。Query Builder で作成された一般的なクエリは、この新しい監査設定でキャプチャされたレコードに対して引き続き機能します。これに対し、Advanced Query Builder ではデータのフィールド情報を検索する場合があるため、データベース スキーマを変更した後にキャプチャした監査レコードに対して実行する詳細なクエリは、再作成する必要があります。
- DefaultDB データベースの Zen セキュリティ ポリシーを混合またはデータベースに設定している場合は、監査の設定の新しいスキーマについて作業する前に、そのパスを DefaultDB のデータの場所の一覧に追加する必要があります。詳細については、「Zen セキュリティ下での Audit for Zen の実行」を参照してください。

監査の設定の削除

監査の設定を削除すると、インポートしたスキーマ、そのスキーマ下のグループ、およびこれらのグループに指定した監視対象テーブルの一覧も削除されます。指定したテーブルは、Zen データベース エンジンを次回再起動すると監視されなくなります。

▶▶ 監査の設定を削除するには

1 ［監査の設定］タブで、監査設定の名前を右クリックして［**削除**］を選択します。

2 ［はい］をクリックして削除を確認します。

削除したグループ内の監視対象だったファイルが、他の監査設定のグループに追加できるようになります。一般的に、監査の設定を削除する必要が生じるのは、データベース スキーマを変更した場合のみです。削除後、新しいスキーマをインポートし、グループを再作成して監視対象ファイルを追加します。

スキーマのあるデータ監視の構成

このシナリオでは、データ辞書ファイル（DDF）があるデータベース内の 1 つ以上のテーブルから成るグループを監視するための監査設定を作成する方法を示します。Zen サーバーと共にインストールされる Demodata サンプル データベースを使用します。また、Audit for Zen と共にインストールされた既存の監査設定も使用します。この設定には、Demodata スキーマがあらかじめインポートされています。

自身の監査設定を作成するには、Audit for Zen 管理ユーザーである必要があります。

「スキーマの管理」で説明したように、DDF のスキーマ情報は監査レコードを人間が読み取れるようにし、特定のデータ値を照会できるようにします。

「スキーマのないデータ監視の構成」に記載する別の例では、DDF がないデータ ファイルを監視する方法を示しています。

▶▶ スキーマのある監査の設定を使用するには

1 AZCC を起動すると、［Audit for Zen］ウィンドウが開き、使用可能なサーバーが表示されます。

2 サーバー名を右クリックして［**ログイン**］を選択します。名前を展開するだけでも、［ログイン］ダイアログ ボックスを開くことができます。

3 デフォルトのユーザー名 admin とパスワード MASTER を入力します。ユーザー名とパスワードを変更済みの場合は、代わりにそれらを入力します。

メモ 組み込みのユーザー ID admin は、デフォルトのパスワード MASTER を持っています。パスワードは大文字と小文字を区別しますが、ユーザー名は区別しません。このユーザー ID とパスワードは Audit for Zen 内でのみ識別されるものであり、Zen または Windows セキュリティ下のユーザー アカウントとは一切関係ありません。

4 ［OK］をクリックします。

5 ［監査の設定］の［テーブル］タブで、既存の監査設定 Zen Demo (9) を右クリックして［**グループの追加**］を選択します。

6 グループ名 Demodata を入力して、［OK］をクリックします。

グループ名は大文字と小文字を区別しません。スペースも含め、すべてのキーボードの文字を使用でき、最長 40 文字まで指定できます。グループ名を別の監査設定に再利用することは可能ですが、グループ名を使用する Audit for Zen クエリを作成する際に混同する恐れを少なくするため、一意の名前を付けることをお勧めします。

7 ［利用可能なテーブル］領域の［テーブルの参照］ウィンドウで、この監査設定のスキーマに関連付けるテーブルの場所を参照します。

この例では、Zen デモンストレーション データベースの Demodata があるディレクトリを選択します。デフォルトの Zen インストレーションでは、この場所は C:¥ProgramData¥Actian¥Zen¥Demodata になります。

8 Billing という名前のテーブルをクリックし、［**選択**］をクリックして、このテーブルを［監視するテーブル］リストに移動します。

［**すべて選択**］をクリックして、現在の場所内のすべてのテーブルを追加することもできます。

どの監査設定においても、各テーブルは 1 つのグループのメンバーにしかなれません。テーブルがあるはずの場所にない場合は、この監査設定やその他の監査設定に含まれる他のグループをチェックして、そのテーブルが既に監視されていないかどうかを確認します。

［監視するテーブル］から項目を削除するには、その項目を選択して［**削除**］をクリックします。［**すべて削除**］をクリックすると、グループからすべてのテーブルが削除されます。

メモ 削除したテーブルに基づくクエリや警告では監査レコードを検索できなくなるので、それらのクエリや警告も削除する必要が出てきます。必要であれば、削除したテーブルを別のグループに追加した後、それらのクエリや警告を再作成する必要があります。削除したテーブルを以前と同じグループに再度追加した場合は、同じクエリや警告が再び正常に終了するようになります。

9 グループにテーブルを選択したら、［OK］をクリックします。

ウィンドウが閉じ、AZCC により、Zen データベース エンジンを再起動するように求められます。

10 ［はい］をクリックします。

再起動が行われた後で、監視が開始されます。［監査の設定］タブに新しいグループが表示され、そのグループの下に当該のテーブルが表示されます。

11 グループを修正したい場合は、そのグループを右クリックして［**編集**］を選択します。

スキーマのないデータ監視の構成

このシナリオでは、DDF のない 1 つ以上の Btrieve データ ファイルから成るグループを監視するための監査設定を作成する方法を示します。sample.btr という名前のデータ ファイルを使用します。このデータ ファイルは Zen サーバーと共にインストールされます。また、既存の監査設定は Audit for Zen と共にインストールされます。

自身の監査設定を作成するには、Audit for Zen 管理ユーザーである必要があります。

「スキーマのあるデータ監視の構成」に記載する別の例では、DDF があるデータベース テーブルを監視する方法を示しています。

▶▶ スキーマのない監査の設定を使用するには

1 AZCC を起動すると、［Audit for Zen］ウィンドウが開き、使用可能なサーバーが表示されます。

2 サーバー名を右クリックして［**ログイン**］を選択します。名前を展開するだけでも、［ログイン］ダイアログ ボックスを開くことができます。

3 デフォルトのユーザー名 admin とパスワード MASTER を入力します。ユーザー名とパスワードを変更済みの場合は、代わりにそれらを入力します。

メモ 組み込みのユーザー ID admin は、デフォルトのパスワード MASTER を持っています。パスワードは大文字と小文字を区別しますが、ユーザー名は区別しません。このユーザー ID とパスワードは Audit for Zen 内でのみ識別されるものであり、Zen または Windows セキュリティ下のユーザー アカウントとは一切関係ありません。

4 ［OK］をクリックします。

5 ［監査の設定］の［Btrieve ファイル］タブで、既存の監査設定 Zen Generic を右クリックして［**グループの追加**］を選択します。

6 Files というグループ名を入力して、［OK］をクリックします。

グループ名は大文字と小文字を区別しません。スペースも含め、すべてのキーボードの文字を使用でき、最長 40 文字まで指定できます。グループ名を別の監査設定に再利用することは可能ですが、グループ名を使用する Audit for Zen クエリを作成する際に混同する恐れを少なくするため、一意の名前を付けることをお勧めします。

7 ［Btrieve ファイル グループ］ウィンドウの［利用可能なファイル］領域で、監視するファイルがある場所を参照します。表示されるファイルは Btrieve ファイルのみです。

この例では、Zen のサンプル ディレクトリを選択します。デフォルトの Zen インストレーションでは、この場所は C:¥ProgramData¥Actian¥Zen¥samples になります。

8 ファイル名 sample.btr をクリックし、［**選択**］をクリックして、このファイルを［監視するファイル］リストに移動します。

［**すべて選択**］をクリックして、現在の場所内のすべてのファイルを追加することもできます。

どの監査設定においても、各ファイルは 1 つのグループのメンバーにしかなれません。ファイルがあるはずの場所にない場合は、他のグループと監査設定をチェックして、そのテーブルが既に監視されていないかどうかを確認します。

［監視するファイル］から項目を削除するには、その項目を選択して［**削除**］をクリックします。［**すべて削除**］をクリックすると、グループからすべてのファイルが削除されます。

メモ 削除したファイルに基づくクエリや警告では監査レコードを検索できなくなるので、それらのクエリや警告も削除する必要が出てきます。必要であれば、削除したファイルを別のグループに追加した後、それらのクエリや警告を再作成する必要があります。削除したファイルを以前と同じグループに再度追加した場合は、同じクエリや警告が再び正常に終了するようになります。

9 グループに追加するファイルを選択したら、［OK］をクリックします。

ウィンドウが閉じ、AZCC により、Zen データベース エンジンを再起動するように求められます。

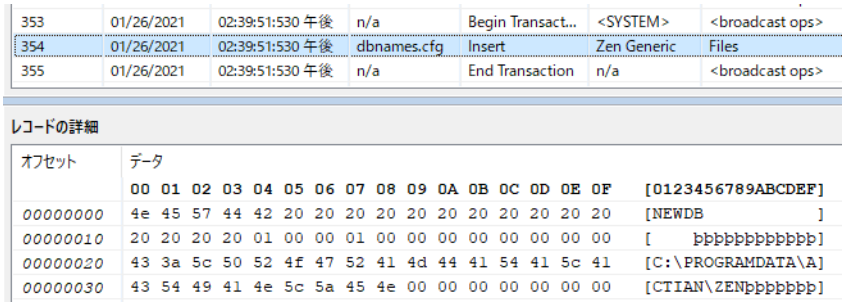
10 ［はい］をクリックします。

再起動が行われた後で、監視が開始されます。［監査の設定］タブに新しいグループが表示され、そのグループの下に当該のファイルが表示されます。

11 グループを修正したい場合は、そのグループを右クリックして［編集］を選択します。

データ ファイル以外の項目の監視

データ ファイル以外で監視候補となる Btrieve ファイルの種類の 1 つは Zen サーバーのシステム ファイル dbnames.cfg です。このファイルは、デフォルトのインストレーションでは C:¥ProgramData¥Actian¥Zen にあります。このファイルは、Zen データベースとその構成設定から成るマスター リストです。新しいデータベースや削除されたデータベースなどの変更がないかどうか、このリストを監査すると役立つかもしれません。それらの変更は、dbnames.cfg ファイルに "Insert" や "Delete" として表示されます。dbnames.cfg はスキーマがない Btrieve ファイルであるため、その監査レコードは人間が読み取れません。しかし、監査レコードに表示されるテキスト文字列により、次の例に示すようにデータベースの名前と場所がわかります。



353	01/26/2021	02:39:51:530 午後	n/a	Begin Transact...	<SYSTEM>	<broadcast ops>
354	01/26/2021	02:39:51:530 午後	dbnames.cfg	Insert	Zen Generic	Files
355	01/26/2021	02:39:51:530 午後	n/a	End Transaction	n/a	<broadcast ops>

レコードの詳細

オフセット	データ	
	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	[0123456789ABCDEF]
00000000	4e 45 57 44 42 20 20 20 20 20 20 20 20 20 20 20	[NEWDB]
00000010	20 20 20 20 01 00 00 01 00 00 00 00 00 00 00 00	[þþþþþþþþþþþþ]
00000020	43 3a 5c 50 52 4f 47 52 41 4d 44 41 54 41 5c 41	[C:\PROGRAMDATA\A]
00000030	43 54 49 41 4e 5c 5a 45 4e 00 00 00 00 00 00 00	[CTIAN\ZENþþþþþþþ]

テーブルまたはファイル別に監視する操作

［テーブル グループ］ウィンドウまたは［Btrieve ファイル グループ］ウィンドウにおいて、そのグループの個々のテーブルまたはファイルには、監視可能な操作の一覧が表示されます。テーブルまたはファイルをクリックすると、その項目に対して監視可能な操作が表示されます。選択した操作が行われると、監査レコードが生成されます。たとえば、" 挿入 " 操作を選択した場合は、監視対象のテーブルまたはファイルへの挿入が成功すると、挿入の方法を問わず、監査レコードが生成されます。

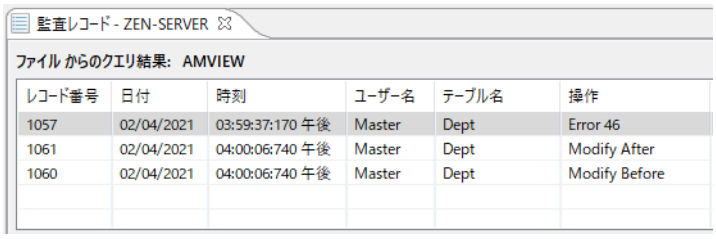
Demodata サンプル データベースを監視する次の例では、Billing テーブルが選択されており、このテーブルがグループに追加されたときにデフォルトで選択される操作が示されています。

これらの操作に関する選択は、テーブルまたはファイルをグループに追加する際に、そのテーブルまたはファイルごとに別々に設定できます。他の設定の場合と同様に、変更を有効にするには、Zen データベースを再起動する必要があります。

表示されるデフォルト値を変更する方法は、「グローバルに監査する操作」を参照してください。

選択した操作が失敗した場合には監査レコードがキャプチャされない点に注意してください。ただし、Audit for Zen では、特定のエラーも監視対象として選択することができます。これにより、それらのエラーのうちの 1 つが失敗した操作の一環として発生した場合は、そのエラーが監査レコードとしてキャプチャされるようになります。

次の例は、ステータス コード 46 を監査対象として選択した場合にキャプチャされた監査レコードを示しています。エラーの場所は Demodata の Dept テーブルであり、このテーブルは監視対象とするグループに追加されたものです。ステータス コード 46 はオーナー ネームが無効であることを示しています。これは、ここでは、不正なオーナー ネームを使用してテーブルを更新しようとしたために発生しています。この更新操作は失敗したため、監査レコードは生成されません。ファイルを更新する 2 回目の試み（今回は有効なオーナー ネームを指定）では、更新を成功させることができるため、変更の前 / 後の監査レコードが生成されます。



Zen データベースのステータス レコードの監視については、「監査するエラー」を参照してください。

監査レコードの照会

7

監査レコードの作業方法

以下のトピックでは、監査レコードに対するクエリの実行に関連するタスクについて説明します。これらのタスクに着手する前に、「Audit for Zen Control Center の使用」に記述されている、Audit for Zen インターフェイスについて理解しておいてください。

- 「監査レコードの表示」
- 「クエリの実行」
- 「アーカイブされた監査レコードでの作業」
- 「警告での作業」
- 「監査レコードまたはログ レコードの検索」
- 「テキスト ファイルへの監査レコードまたはログ レコードのエクスポート」
- 「Zen セキュリティの下での監査レコードの表示」
- 「Audit for Zen の元に戻す機能の使用」

監査レコードの表示

Audit for Zen は、Btrieve ファイルへの操作がないかどうか Zen データベース エンジンを監視し、それらの操作イベントをログに記録して、関連するレコードからデータをキャプチャします。Audit for Zen は、大量の情報を格納できるように設計されたログ ファイルに、それらの操作やデータをすべて格納します。ログ ファイルの内容にアクセスできるように、ログ ファイルのデータがビュー ファイルにコピーされることでクエリの実行対象として準備されます。ビュー ファイルが大きくなると、それに対するクエリのパフォーマンスが低下する可能性があります。パフォーマンス低下を改善するには、ビュー ファイルのコンテンツをアーカイブに移動します。

監査データを表示するには、クエリを実行します。AZCC には、一般的なクエリと詳細なクエリの 2 種類のクエリが用意されています。一般的なクエリは、監査レコードの属性を使用して、結果から成るテーブルを返します。詳細なクエリは、監査レコードからだけでなく、キャプチャされたデータベース レコードからも、値を照会することができます。

以下のトピックは、監査レコードの操作方法のクイック ガイドです。

- 「ビュー ファイルへのクエリの実行」
- 「[監査レコード] タブでの作業」
- 「監査データ列の確認」
- 「監査レコードの詳細の表示」

ビュー ファイルへのクエリの実行

これは、監査レコードの簡単な表示方法を示した基本的な例です。

▶▶ 現在のビュー ファイルを更新するには

ビュー ファイルを照会する前に、まず、ログ ファイルから新しい監査レコードを取得するためにビュー ファイルを更新します。

1 データ ツリーで現在のビュー ファイルを右クリックして［**現在のビュー ファイルの更新**］を選択するか、またはツール バーの アイコンをクリックします。

これで、ビュー ファイルで監査レコードを照会できるようになりました。

2 ビュー ファイル内の監査レコード数と、監査レコードの最初のキャプチャ日と最後のキャプチャ日を確認したい場合は、現在のビュー ファイルを右クリックし、［**プロパティ**］を選択します。

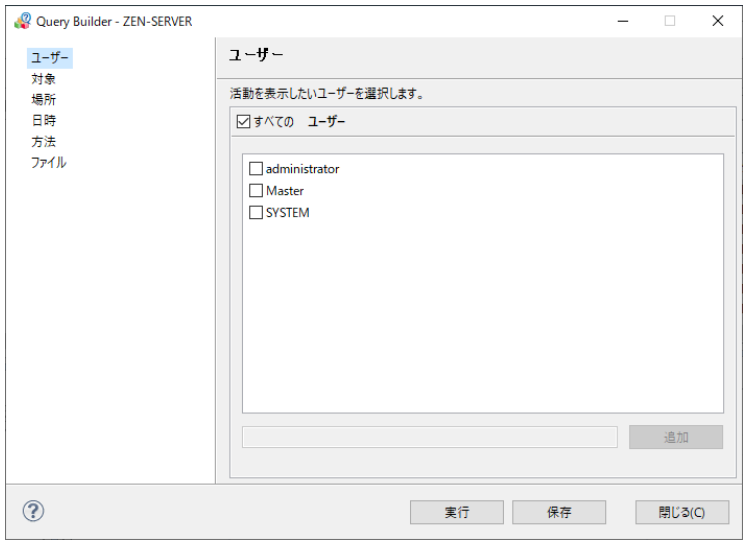
▶▶ デフォルトである一般的なクエリを実行するには

1 データ ツリーで現在のビュー ファイルをクリックします。

2 以下のいずれかを実行して［Query Builder］ウィンドウを開きます。

- ビュー ファイルをダブルクリックします。
- ファイルを右クリックし、［**クエリ**］を選択します。
- ファイルを選択して、［**ファイル**］>［**クエリ**］コマンドを選択します。
- ファイルを選択し、ツールバーで新しいクエリ（Query Builder）アイコン をクリックします。
- Alt+Q キーを押します。

［Query Builder］ウィンドウが開き、クエリを絞り込むのに使用できる 6 つの検索条件グループのうち、最初のグループが表示されます。表示されるオプションは、照会対象である現在のビュー ファイルまたはアーカイブ ファイルで検出された値によって異なります。



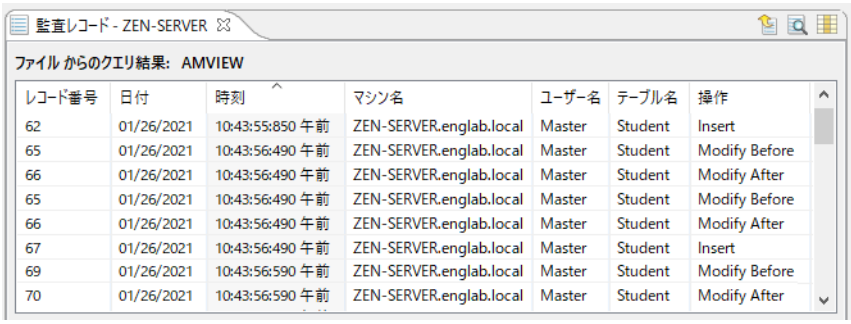
検索条件グループごとに、デフォルトではすべてのオプションが選択されますが、次のような例外があります。

- ［対象］: Zen データベース操作と選択した Zen ステータス コードのメッセージのみが、クエリ対象として選択されます。Audit for Zen の内部メッセージとデバッグ メッセージは選択されません。
- ［ファイル］: 選択されるファイルは、［Query Builder］ウィンドウが開く前に選択されていたファイルです。クエリに必要なファイルが他にもある場合は、手動で追加する必要があります。

すべてのオプションを選択した場合は、クエリにより、ビュー ファイル内のすべてのレコードが［監査レコード］タブに表示されます。検索条件を使用したクエリ対象の絞り込みの詳細については、「クエリの実行」を参照してください。

3 ［**実行**］ボタンをクリックします。

クエリ結果が［監査レコード］タブに表示されます。［Query Builder］ウィンドウは開いたままになるので、結果が表示されるように移動させることもできます。



レコード番号	日付	時刻	マシン名	ユーザー名	テーブル名	操作
62	01/26/2021	10:43:55:850 午前	ZEN-SERVER.englab.local	Master	Student	Insert
65	01/26/2021	10:43:56:490 午前	ZEN-SERVER.englab.local	Master	Student	Modify Before
66	01/26/2021	10:43:56:490 午前	ZEN-SERVER.englab.local	Master	Student	Modify After
65	01/26/2021	10:43:56:490 午前	ZEN-SERVER.englab.local	Master	Student	Modify Before
66	01/26/2021	10:43:56:490 午前	ZEN-SERVER.englab.local	Master	Student	Modify After
67	01/26/2021	10:43:56:490 午前	ZEN-SERVER.englab.local	Master	Student	Insert
69	01/26/2021	10:43:56:590 午前	ZEN-SERVER.englab.local	Master	Student	Modify Before
70	01/26/2021	10:43:56:590 午前	ZEN-SERVER.englab.local	Master	Student	Modify After

4 ここで、以下を行うことができます。

- 表示する列と列の表示順序を変更する。「［監査レコード］タブでの作業」を参照してください。
- 個々のレコードの詳細を表示する。「監査レコードの詳細の表示」を参照してください。
- クエリを修正して再度実行する。「クエリの実行」を参照してください。
- ［**保存**］をクリックしてクエリを保存する。「保存されたクエリまたは最後に実行したクエリを実行する」を参照してください。
- 照会が終了したら、［Query Builder］ウィンドウの［**閉じる**］ボタンを押す。

［監査レコード］タブでの作業

［監査レコード］タブにはクエリの結果が表示されます。このタブの列には、キャプチャした日付と時刻、テーブル名、操作、ユーザー名などの監査情報が示されます。表示をカスタマイズしたり、操作したりするためのオプションを次の表に示します。

オプション	手順
表示する列の設定	「監査データ列の確認」を参照してください。列の内容についても記載されています。
列幅の調整	列の端をクリックして、希望の幅までドラッグします。
列の順序の変更	各列を希望の位置までドラッグします。
レコードの並べ替え	列の見出しをクリックして、列の値の昇順または降順に行を並べ替えます。元の並べ替え順に戻すには、このタブを閉じてクエリを再実行します。
これらの列設定の保存	［表示］>［環境設定］>［テーブル レイアウト］を選択し、各設定のチェック ボックスをオンにします。
監査レコードの検索	「監査レコードまたはログ レコードを検索するには」を参照してください。
監査レコードのエクスポート	「監査レコードをエクスポートするには」を参照してください。

監査データ列の確認

選択可能なすべての監査データ列を次の表に示します。表示する監査データ列を選択するには、タブの上にある［表示する列の選択］アイコン  をクリックします。列の順序を変更するには、マウスで列をドラッグします。この設定を保存して再利用したい場合は、［**表示**］>［**環境設定**］>［**テーブル レイアウト**］を選択します。

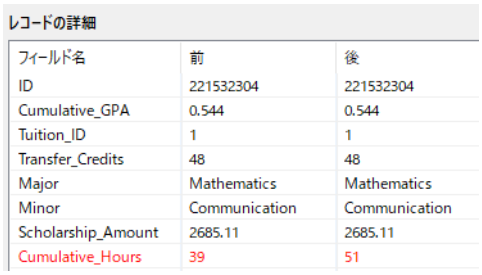
列名	内容
レコード番号	1 ずつ増える一意の監査レコード番号
依存するレコード	以前の関連レコードのレコード番号： • 変更後のレコードに対する変更前のレコード • トランザクションを終了 / 中止したレコードに対する、トランザクションを開始したレコード
日付	監査レコードのキャプチャ日付
時刻	監査レコードのキャプチャ時刻
マシン名	イベントが発生したマシン名または IP アドレス
ユーザー名	イベントが発生したログイン ID。「Zen セキュリティの下での監査レコードの表示」を参照してください。
データベース名	イベントが発生したデータベース。「Zen セキュリティの下での監査レコードの表示」を参照してください。
テーブル名	イベントが発生したテーブルまたはデータ ファイル。このテーブルまたはファイルは、監査の設定で監視対象としてリストされている必要があります。監視対象ファイルの一覧は、Query Builder の［対象］タブの［テーブル］リストに表示されます。
操作	データベース イベント。イベントには、Query Builder の［対象］タブの［操作］リストにある任意の項目が含まれます。SQL ログインは、この列に表示されます。また、［サーバーの設定］ウィンドウの［監査するエラー］セクションで Zen ステータス コードを最初に選択した場合は、その選択したステータス コードもここに表示されます。詳細については、「サーバー設定の管理」を参照してください。

列名	内容
操作コンテキスト	BTRIEVE は、あらゆるデータ ファイル操作のコンテキストです。
データベース エンジン	AM Message API（Audit for Zen 内部で使用）または Zen
データベース　バージョン	サーバー上で実行されている Zen のバージョン
製品	監視対象ファイルの監査の設定に記載されている値
製品バージョン	監視対象ファイルの監査の設定に記載されている値
グループ名	監査の設定における監視対象ファイルのグループ
コンポーネント	監視対象ファイルの監査の設定に記載されている値
コンポーネント バージョン	監視対象ファイルの監査の設定に記載されている値
プロセス名	操作の実行元となったプロセス。通常、実行元プロセスのほとんどは Zen Engine です。Audit for Zen によって行われるアクションは少数であり、Zen Monitor としてリストされます。
OS バージョン	Audit for Zen サーバーが実行されているシステムのオペレーティング システムの名前とバージョン
ビュー ファイル	監査レコードの場所。amview（現在のビュー ファイル）またはアーカイブ ファイル名のいずれか

監査レコードの詳細の表示

個々の監査レコードの詳細を見るには、[監査レコード] タブ内の当該レコードをクリックします。詳細が、[AZCC] ウィンドウの下方部分に表示されます。監査レコードにアプリケーション データ レコードの変更がキャプチャされている場合、変更前の値と変更後の値が赤色で強調した状態で表示されます。

データベース スキーマをインポート済みの場合には、次の Demodata の例のように変更がわかりやすくなります。データベース スキーマを使用していない場合には、変更は 16 進数で表示されます。


レコードの詳細

フィールド名	前	後
ID	221532304	221532304
Cumulative_GPA	0.544	0.544
Tuition_ID	1	1
Transfer_Credits	48	48
Major	Mathematics	Mathematics
Minor	Communication	Communication
Scholarship_Amount	2685.11	2685.11
Cumulative_Hours	39	51

クエリの実行

現在のビュー ファイルまたはアーカイブ ファイルに含まれている監査レコードを表示するには、クエリを実行する必要があります。デフォルトでは、クエリは、監査の設定で監視対象としたテーブルまたはデータ ファイルに関連する利用可能なすべての監査レコードを返します。クエリを絞り込むには、[「ユーザー」]、[「対象」]、[「場所」]、[「日時」]、[「方法」]、[「ファイル」] に検索条件を指定します。たとえば、特定の日付の監査イベント、選択したテーブルのイベント、または 1 人のユーザーが行った変更を検索することができます。

このトピックでは、以下のタスクについて説明します。

- 「すべての監査レコードを表示する」
- 「クエリを制限する」
- 「詳細なクエリを構築する」
- 「クエリで［ファイル］グループを使用する」
- 「保存されたクエリまたは最後に実行したクエリを実行する」

すべての監査レコードを表示する

［Query Builder］ウィンドウで最も簡単なクエリはデフォルトのクエリであり、これは現在のビュー ファイルにあるすべての監査レコードを表示します。

▶▶ 利用可能なすべての監査レコードを表示するには

1 ビュー ファイルを右クリックし、［**現在のビュー ファイルの更新**］を選択します。

2 ビュー ファイルを選択し、［**ファイル**］>［**クエリ**］を選択するか、または右クリックして［**クエリ**］を選択します。

3 ［Query Builder］ウィンドウでは、各検索条件のすべてのオプションがデフォルトで選択されています。このファイルのすべての Audit for Zen データを表示するには、単に［**実行**］をクリックします。

監査レコードが、AZCC の右上ペインのグリッドに表示されます。

ビュー ファイルを選択する代わりに、アーカイブ ファイルを選択または右クリックすることもできます。複数のアーカイブ ファイルを選択したい場合、またはビュー ファイルと複数のアーカイブ ファイルを選択したい場合は、「ファイル」を参照してください。

クエリを制限する

Query Builder にはクエリを制限するための一連の検索条件が用意されており、検索するユーザー、対象（操作など）、場所、日時、方法、および監査レコード ファイルを指定することができます。

▶▶ クエリを制限するには

1 Query Builder では、クエリ結果をさらに絞り込めるオプションを選択できます。これらの検索条件を次の表で左側に示すと共に、その説明も示します。

探す情報	使用するオプション	実行する手順
ユーザー ［ユーザー名］列に示される特定の Zen ユーザー、Windows ユーザー、または Audit for Zen ユーザーが関与するイベント用	**ユーザー**	1. 特定のユーザーが関与する監査レコードを検索するには、［**すべてのユーザー**］チェック ボックスをオフにします。 2. ユーザーの一覧で、名前の横にあるボックスをオンにすることにより、ユーザーを選択します。表示されているユーザーは、照会対象であるビュー ファイルまたはアーカイブ ファイルから見つかったユーザーです。 ユーザーを追加するには、ログイン名を入力して［追加］をクリックします。
操作、グループ、およびテーブル ［操作］、［グループ名］、［テーブル名］の各列に示される選択した操作、グループ、テーブルに関する監査レコード	**対象**	1. 挿入や削除など特定の種類の操作を見つけるには、［**すべての操作**］チェック ボックスをオフにします。また、［**すべてのグループ**］や［**すべてのテーブル**］をオフにすると、それぞれのリストが利用可能になります。 2. 操作と、それによって影響を受けた項目を選択します。必要に応じてリストを展開し、適切なオプションを選択します。Shift キーまたは Ctrl キーを使用して選択範囲を拡張します。テーブルやファイルは、監査の設定やグループを問わず、選択できます。また、スキーマのあるファイルとスキーマのないファイルを同じクエリ内に指定することもできます。 **メモ**：［すべて］チェック ボックスをオフにした後でノードを展開しても、すべての項目が引き続き選択された状態で表示される場合があります。選択を解除するには、リストで 1 つ 1 つの項目をクリックします。
マシン ［マシン名］列に示される選択したマシンでキャプチャされた監査レコード	**場所**	1. マシンを検索するには、［**すべてのマシン**］チェック ボックスをオフにします。これにより、マシン名とネットワーク アドレスのリストが利用可能になります。 2. チェック ボックスをクリックすることにより、1 つまたは複数のマシンを選択します。名前またはネットワーク アドレスを追加する必要がある場合は、それを入力して［**追加**］をクリックします。
特定の日付 日付範囲および時刻範囲に示される特定の日付や、選択した各日の時刻範囲内にキャプチャされた監査レコード	**日時**	1. 特定の開始日付と終了日付の範囲で検索を行う場合は、［すべての日付範囲］チェック ボックスをオフにします。開始日付と終了日付のカレンダーが利用可能になります。 2. カレンダーから年月日を選択するか、または日付を入力して［**設定**］をクリックします。 3. 日付範囲における各日の特定の時刻範囲内で検索を行う場合は、［すべての時間範囲］オプションをオフにします。［開始時間］および［終了時間］フィールドから時刻を選択します。時刻は直接入力することもできます。 **メモ**：時刻範囲は、日付範囲内の個々の日に適用されます。たとえば、各日の午前 8 時から午後 5 時までとなります。［すべての時間範囲］を再度オンにすると、デフォルトの 24 時間に戻りますが、手動で入力した時刻はそのまま残ります。そのため、［すべての時間範囲］を再度オフにすれば入力した時刻を復活させることができます。これは、日付範囲を設定した後で［すべての日付範囲］を再度オンにした場合でも同じです。

探す情報	使用するオプション	実行する手順
プロセスまたはプログラム ［プロセス名］列の特定のプロセスまたはプログラムについてログに記録された監査レコード	**方法**	1. 特定のプロセスまたはプログラムを検索する場合は、［**すべてのプロセス**］オプションをオフにします。プロセスのリストが利用可能になります。 2. オプションの横にあるボックスをオンにすることにより、プログラムまたはプロセスを選択します。プロセス名が表示されない場合は、ペインの下部にある［**追加**］フィールドを使用して、プロセス名をリストに含めます。
監査レコードのファイル ［ビュー ファイル］列に示される、選択したビュー ファイルまたはアーカイブ ファイルから返された監査レコード	**ファイル**	1. デフォルトでは現在のビュー ファイルが選択されます。現在のビュー ファイルを選択されたままにすることも、選択解除してクエリ対象から除外することもできます。 2. アーカイブ ファイルを選択するには、アーカイブ ファイルのチェック ボックスをクリックします。 **メモ**：アーカイブ ファイルが表示されていない場合は、圧縮されている可能性があります。Query Builder を閉じ、アーカイブ ファイルを圧縮解除してからクエリを作成します。

2 選択中いつでも［**実行**］をクリックして、現在のクエリを実行することができます。

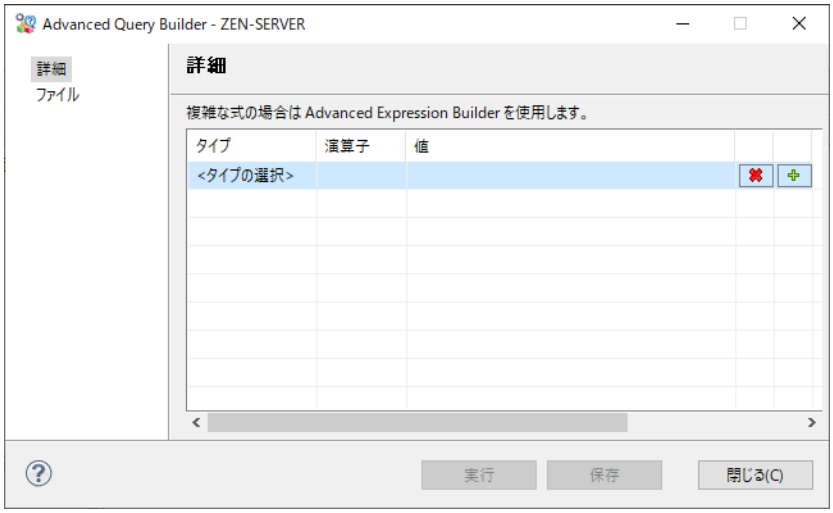
3 ［監査レコード］タブで結果を確認します。結果が求めるものではなかった場合は、Query Builder に戻り、調整を行ってから、クエリを再度実行します。

4 このクエリに満足し、後で再利用したい場合は、［**保存**］をクリックします。

［クエリの保存］ダイアログ ボックスで、わかりやすいクエリ名を入力します。スペースも含め、最長 60 バイトまで指定できます。次に［OK］をクリックします。名前は必要に応じて後でも変更できます。保存したクエリの使用の詳細については、「保存されたクエリまたは最後に実行したクエリを実行する」を参照してください。

詳細なクエリを構築する

Advanced Query Builder では、Query Builder を使用した場合よりも複雑なクエリを作成できます。式を使用して、監査レコード内で特定のイベントを検索します。スキーマをインポート済みの場合は、Advanced Query Builder は監査データからだけでなく、キャプチャされたデータ レコードからも、フィールド値を照会することができます。



［タイプの選択］列と［演算子］列は、クエリ式を作成するための以下の要素を提供します。入力されたすべてのテキスト値は大文字と小文字が区別されます。表中の「～と同じ」という語句が指している比較対象は、一般的なクエリ用の［Query Builder］ウィンドウの検索オプションです。

属性	説明
(	式ブロックを構築するための開きかっこ
データ フィールド	［対象］でテーブルを選択するのとほぼ同じです。ただし、さらに列レベルでクエリを絞り込み、検索または比較する値を入力することができます。
日付	［日時］タブの［日付範囲］と同じです
グループ	［対象］タブの［グループ］属性と同じです
データベース名	データベース自体の名前ではなく、スキーマがインポートされた監査設定の名前。Btrieve ファイルの場合、スキーマがないため、Zen の内部データベース DefaultDB が使用されます
テーブル	［対象］タブの［テーブル］属性と同じです
操作	［対象］タブの［操作］属性と同じです
プロセス	［方法］タブの［プロセス］属性と同じです
レコード番号	クエリ結果の［監査レコード］タブのレコード番号
時刻	［日時］タブの［時間範囲］と同じです
マシン名	［場所］タブの［マシン名］属性と同じです
ユーザー	［ユーザー］タブの［ユーザー］属性と同じです
and、or	［タイプ］列で使用される論理演算子
=、>、>=、<=、<、in	［演算子］列で使用される比較演算子と、要素リストの集合演算子としての「in」
)	式ブロックを構築するための閉じかっこ

詳細なクエリの例

このトピックでは、複雑なクエリを作成する方法を示す以下の 2 つのチュートリアルを掲載します。

- 「GPA が 3.0 以上である学生の監査レコードを照会するには」
- 「特定の学生の挿入日時を検索するには」

最初のクエリでは、学生の成績ポイントの累加平均（cumulative GPA。略称 GPA）が 3.0 以上となっているすべての監査レコードを検索します。2 番目のクエリは、最初のクエリを修正したものであり、特定の学生が挿入されたときの日付と時刻を検索しています。

これらのチュートリアルを実行するには、まず次の 3 つのことを行う必要があります。

- AZCC に組み込まれている Zen Demo 監査設定で、Demo という名前のグループを作成し、Demodata の全テーブルの監査を開始するためにこのグループにそれらのテーブルを追加して、Zen エンジン サービスを再起動します。
- 監視対象テーブルの 1 つに変更を加えるために、Demodata データベース コンテキストに設定された SQL ドキュメントを ZenCC で開き、次の SQL スクリプトを実行します。

```
INSERT INTO Student(ID, Cumulative_GPA, Tuition_ID, Transfer_Credits, Major,
   Minor, Scholarship_Amount, Cumulative_Hours) VALUES (213725554, 3.6, 6, 30,
   'Biology', 'Technical Writing', 2600.00, 24);

UPDATE Student SET Cumulative_GPA = 3.1 WHERE ID = 189602671;
```

```
UPDATE Student SET Cumulative_GPA = 3.5 WHERE ID = 189152021;
```

- AZCC のデータ ツリーで現在のビュー ファイルを右クリックし、[**現在のビュー ファイルの更新**] を選択します。Audit for Zen が照会できるのはビュー ファイルとアーカイブ ファイルの内容のみであるため、この手順は不可欠です。

▶▶ GPA が 3.0 以上である学生の監査レコードを照会するには

1 以下のいずれかを実行して [Advanced Query Builder] ウィンドウを開きます。

- ビュー ファイルを右クリックして [**詳細なクエリ**] を選択します。
- ファイルを選択して、[**ファイル**] > [**詳細なクエリ**] を選択します。
- ファイルを選択して、Ctrl+Alt+Q キーを押します。

このウィンドウでは、[詳細] グループのクエリ オプションがデフォルトで選択されています。ここではこのグループを使用します。[ファイル] グループについては、「クエリで [ファイル] グループを使用する」を参照してください。

2 [タイプ] 列で "**< タイプの選択 >**" をクリックします。

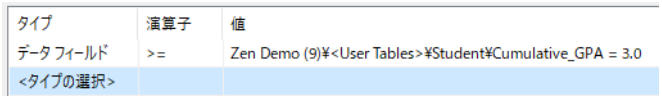
3 クエリ属性タイプのリストで "**データ フィールド**" を選択します。

4 [データ フィールドの選択] で、Zen Demo > User Tables > Student と展開し、"Cumulative_GPA" を選択します。

5 下部の値フィールドに「3.0」を入力し、[OK] をクリックします。

6 データ フィールドに対する演算子には、3.0 以上を指定する "**>=**" を選択します。

これで、[Advanced Query Builder] ウィンドウは次のようになります。

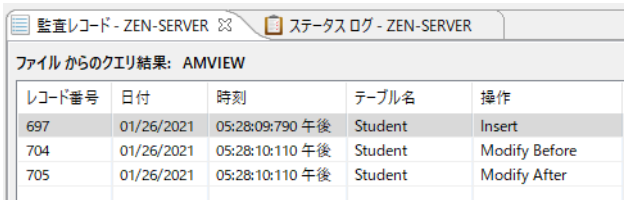


タイプ	演算子	値
データ フィールド	>=	Zen Demo (9)¥<User Tables>¥Student¥Cumulative_GPA = 3.0
<タイプの選択>		

Student テーブル内の変更のうち、GPA が 3.0 以上の学生に対する変更についてすべての監査レコードを検索するよう、クエリが設定されました。

7 [**実行**] をクリックします。ウィンドウは開いたままにし、[AZCC] ウィンドウを確認するために必要であれば移動させます。

クエリ結果は [監査レコード] タブに表示され、結果には新しく挿入された行や変更された行が含まれます。



監査レコード - ZEN-SERVER　ステータス ログ - ZEN-SERVER

ファイル からのクエリ結果: AMVIEW

レコード番号	日付	時刻	テーブル名	操作
697	01/26/2021	05:28:09:790 午後	Student	Insert
704	01/26/2021	05:28:10:110 午後	Student	Modify Before
705	01/26/2021	05:28:10:110 午後	Student	Modify After

次の点に注意してください。

- クエリがこれらの監査レコードを返したのは、Student テーブルの監査を開始した以降に Demodata のレコードで変更が行われ、監査レコードが Audit for Zen によってキャプチャされて、現在のビュー ファイルに含まれていたためです。
- Demodata には GPA 3.0 以上の他の学生に関する既存のレコードも含まれていますが、それらのレコードは変更されていないため、Audit for Zen にそれらの監査レコードはありません。したがって、AZ クエリはそれらのレコードに対する結果を返しません。

▶▶ 特定の学生の挿入日時を検索するには

最初のチュートリアルにおける最後の手順で、[Advanced Query Builder] ウィンドウを開いたままにしました。そのウィンドウを使用して、この 2 番目のチュートリアルを始めます。

1 クエリ ウィンドウで、データ フィールドの値をクリックします。値は現在、"Zen Demo (9)¥<User Tables>¥Student¥Cumulative_GPA=3.0" になっています。

2 このエントリの右側に表示されている**省略記号**のボタン（[...]）をクリックします。

3 ［データ フィールドの選択］ウィンドウで、Zen Demo > User Tables > Student と展開し、"ID" を選択して Cumulative_GPA を置き換えることで、選択したデータ フィールドを変更します。

4 ［ID］の値として、先に挿入されたレコード内の学生番号「213725554」を入力し、［OK］をクリックします。

5 データ フィールドに対する演算子には、学生の ID 番号に一致することを指定する "=" を選択します。

6 この例では、当該の学生が当月に追加された可能性があるが、いつ追加されたかを正確に知る必要が生じたものと仮定します。"**< タイプの選択 >**" をクリックし、"and" を選択してクエリを拡張します。

7 "**< タイプの選択 >**" をクリックし、" **操作** " を選択します。

8 ［操作の選択］で、"ACTIAN ZEN" を展開して " **挿入** " を選択します。

9 "**< タイプの選択 >**" をクリックし、"and" を選択してクエリを拡張します。

10 "**< タイプの選択 >**" をクリックし、" **日付** " を選択します。

11 当月の**最初の日**を選択し、［OK］をクリックします。

12 いま作成した行のデータ フィールドに対する演算子には、最初に選択した日付以降であることを指定する ">=" を選択します。

13 "**< タイプの選択 >**" をクリックし、"and" を選択して日付範囲を延長します。

14 "**< タイプの選択 >**" をクリックして " **日付** " を選択し、当月の**最後の日**を選択して［OK］をクリックします。

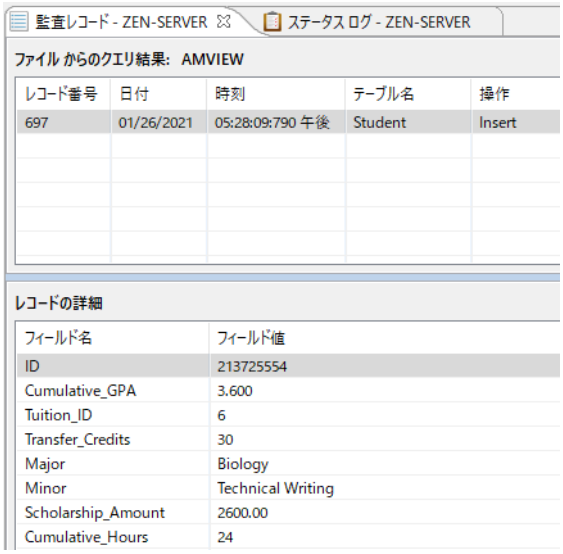
15 この新しい行のデータ フィールドに対する演算子には、2 番目に選択した日付以前であることを指定する "<=" を選択します。

これで、［Advanced Query Builder］ウィンドウは次のようになります。

タイプ	演算子	値
データ フィールド	=	Zen Demo (9)¥<User Tables>¥Student¥ID = 213725554
and		
操作	in	ACTIAN ZEN¥挿入
and		
日付	>=	01/01/2021
and		
日付	<=	01/31/2021
<タイプの選択>		

16 ［**実行**］をクリックしてクエリを実行します。

クエリ結果は次のように［監査レコード］タブに表示されます。

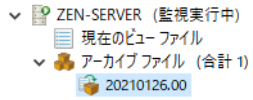


クエリで［ファイル］グループを使用する

［Advanced Query Builder］ウィンドウの［ファイル］グループを使用すると、クエリ対象にしたい現在のビュー ファイルと圧縮されていないすべてのアーカイブ ファイルを選択できます。アーカイブ ファイルだけを選択することもできます。

このチュートリアルを実行するには、以下の手順を行っておく必要があります。

- AZCC の［監査サーバー］で［**現在のビュー ファイル**］を右クリックし、［**アーカイブ**］を選択します。
- データ ツリーで［アーカイブ ファイル］ノードを展開して、新しいファイルの名前を確認します。次のようにアーカイブ日に基づいて命名されます。



クエリに含めるファイルを選択するには

1 ［Advanced Query Builder］ウィンドウで［**ファイル**］をクリックします。デフォルトでは［Current View File］（現在のビュー ファイル）オプションが選択されます。

デフォルトのビュー ファイルのみを選択したままにして、Advanced Query Builder に関する先の 2 つのチュートリアル内のクエリのいずれかを実行した場合は、何の結果も返されません。ビュー ファイルをアーカイブした場合、その監査レコードはすべて新しいアーカイブ ファイルに移動されています。

2 アーカイブ ファイルに対してもクエリを実行するには、現在のビュー ファイルの代わりにアーカイブ ファイルを選択します。または、ビュー ファイルとアーカイブ ファイルを両方とも選択します。

圧縮されていない監査レコードのみを照会できるため、圧縮されているアーカイブ ファイルは［ファイル］グループに表示されません。リストに挙がっていないファイルを表示するには、その圧縮を解除する必要があります。詳細については、「アーカイブされた監査レコードでの作業」を参照してください。

保存されたクエリまたは最後に実行したクエリを実行する

Audit for Zen サーバーごとに、以前に保存されたクエリはデータ ツリーの［保存されたクエリ］の下に保存されます。さらに、最後に実行したクエリは常に保存され、再送信することができます。ここでは、以下の項目について説明します。

- 「クエリを保存するには」
- 「保存されたクエリを使用するには」
- 「最後に実行したクエリを使用するには」

▶▶ クエリを保存するには

1 Query Builder または Advanced Query Builder でクエリを作成した後、［**保存**］ボタンをクリックして、そのクエリに名前を付けます。

2 わかりやすいクエリ名を入力して、［OK］をクリックします。クエリ ビルダーのウィンドウは開いたままにしておいてもかまいません。

保存したクエリは、指定した名前で［監査サーバー］データ ツリーに表示されます。

▶▶ 保存されたクエリを使用するには

1 データ ツリーを更新する必要がある場合は、［保存されたクエリ］ノードを右クリックして［**更新**］を選択します。

2 ［**保存されたクエリ**］ノードを展開します。

3 クエリを右クリックしてコマンドの一覧を表示します。

- **現在のビュー ファイルのクエリ**。現在のビュー ファイルに対してクエリを実行します。
- **複数のビュー ファイルのクエリ**。利用可能ファイルを表示して、必要なファイルを選択し、クエリを実行します。
- **名前の変更**。クエリの名前を変更します。スペースも含め、最長 60 バイトまで指定できます。
- **削除**。クエリを完全に削除します。

照会できるのは、圧縮されていない監査レコードだけです。クエリで使用するファイルが圧縮されている場合、そのクエリを実行するにはファイルの圧縮を解除する必要があります。

メモ 圧縮されているファイルのサイズが大きいほど、圧縮解除には時間がかかります。すべてのレコードが照会可能になったことを確認するには、［アーカイブ ファイル］ノードを右クリックし、［**更新**］を選択して表示を更新します。照会可能になると、アーカイブ ファイルのアイコンが、万力に挟まれた小さな箱から、矢印が大きな箱を指しているものに変わります。

▶▶ 最後に実行したクエリを使用するには

データ ツリーで、ビュー ファイルまたはアーカイブ ファイルを右クリックし、［**最後に実行したクエリの実行**］を選択します。

アーカイブされた監査レコードでの作業

監査で大量の監査レコードが生成される場合があります。現在のビュー ファイルのサイズが大きくなると、それに対するクエリの実行にかかる時間も長くなります。パフォーマンスを向上させるため、Audit for Zen には監査レコードを現在のビュー ファイルからアーカイブ ファイルに移動する機能が用意されています。アーカイブは自動でも手動でも実行できます。自動アーカイブでは、現在のビュー ファイルが設定されているサイズ上限または日時上限に達した場合には、Audit for Zen により自動的にアーカイブ ファイルが作成されます。手動アーカイブは、管理者権限を持つユーザーのみが実行できます。

アーカイブ ファイルはデータ ツリーに表示されます。そのファイル名は、作成日を使用した *yyyymmdd.nn* という書式になります。*yyyy* は年、*mm* は月、*dd* は日、*nn* はその日に作成されたアーカイブ ファイルの番号（0 ～ 99）です。

アーカイブ ファイルを圧縮すると、90% ほどディスク領域を節約できます。Audit for Zen は、圧縮されたアーカイブ ファイルを暗号化して、Audit for Zen システム内のユーザーのみが利用できるようにします。

アーカイブ ファイルの使用方法について、以下のトピックでさらに詳しく説明します。

- 「手動アーカイブ」
- 「アーカイブを管理する」
- 「自動アーカイブ」

手動アーカイブ

このトピックでは、以下の 2 つのタスクに関する手順を示します。

- 「手動でアーカイブするには」
- 「表示するアーカイブ ファイルの数を設定するには」

▶▶ 手動でアーカイブするには

次のような理由から、手動でアーカイブしたい場合もあります。

- 監査ログが大きくなり、クエリやその他の操作にさらに時間がかかるようになっている。パフォーマンス速度を回復するために、次回の自動アーカイブまで待ちたくない。
- 自動アーカイブがすぐに発生する予定はなく、ある対象イベントによって直ちにアーカイブすることが望ましい。
- ディスク領域を管理するために、レコードをアーカイブして圧縮したい。

データ ツリーで現在のビュー ファイルを右クリックし、次の 2 つのうちいずれかを実行します。

- ［**アーカイブ**］を選択する。
- ［**アーカイブと圧縮**］を選択する。レコード数が多いと時間がかかることがあるので、［ステータス ログ］タブで "Finished compressing"（圧縮が完了しました）メッセージがないかどうかを確認してみてください。最新のエントリが表示されていない場合もあるため、ログを更新してみてください。

圧縮されたアーカイブ ファイルに対してクエリを実行することはできません。まず、そのファイルを右クリックして［**圧縮解除**］を選択し、ファイルの圧縮を解除する必要があります。

メモ データ ツリーでは、一覧を更新するために、［アーカイブ ファイル］を右クリックして［**更新**］を選択することが必要になる場合があります。

▶▶ 表示するアーカイブ ファイルの数を設定するには

データ ツリーに表示される非圧縮と圧縮のアーカイブ ファイルの最大数を制御することができます。表示されるリストには、手動で作成されたファイルも自動で作成されたファイルも含まれています。この設定を開くには、［**表示**］＞［**環境設定**］＞［**アーカイブ**］を選択します。

デフォルトの設定は 30 です。利用可能なファイル数より少ないファイル数を設定したリストを表示する場合でも、残りのファイルは削除されるわけではなく表示されないだけです。設定の数値を上げれば再度表示されます。

この設定を変更したら、［アーカイブ ファイル］を右クリックして［**更新**］を選択する必要があります。

この設定を変更しても、［アーカイブの管理］ウィンドウ内のアーカイブ ファイルの表示には影響しません。詳細については、「アーカイブを管理する」を参照してください。

アーカイブを管理する

データ ツリーでは、一度に 1 つのアーカイブ ファイルのみを選択できます。［アーカイブの管理］ウィンドウを使用すると、複数のアーカイブ ファイルを 1 つのグループとして操作できます。このウィンドウを開くには、［**ツール**］>［**アーカイブの管理**］の順に選択します。

ウィンドウを使用するには、まず、アーカイブ ファイルを選択します。各ボタンを使用して、そのファイルを圧縮、圧縮解除、または削除します。複数のファイルを選択するには、Shift キーまたは Ctrl キーを使用します。

警告での作業

Audit for Zen には、クエリで定義した特定の監査イベントをリアルタイムで検出する警告機能が備わっています。クエリに一致するイベントが発生すると、Audit for Zen により以下の 2 つのことが行われます。

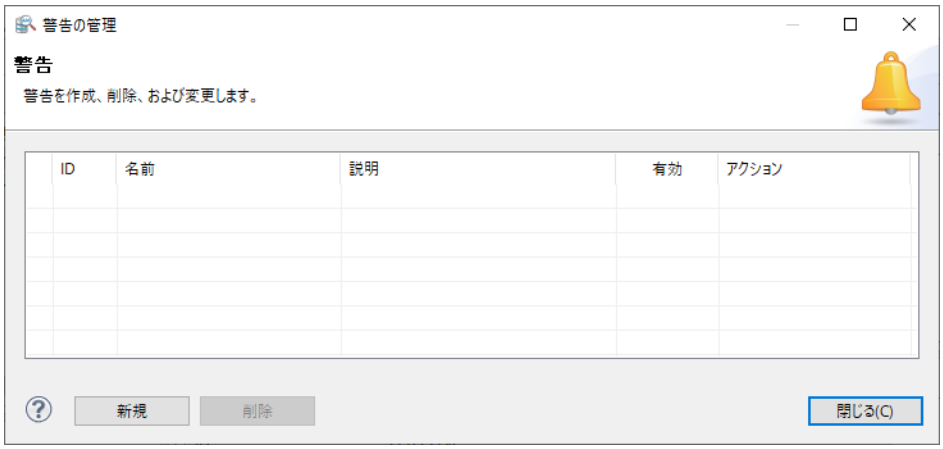
- 警告のクエリ結果の各監査レコードに、ベル アイコン を使ってフラグを付けます。ベル フラグは監査レコードの一部として恒久的に保存されるので、そのレコードを含むすべてのクエリ結果に表示されます。
- Windows のアプリケーション イベント ログにエントリを書き込みます。このログ記録により、ネットワーク管理者は、自動プログラムを実行するツールや通知を送信するツールを使用できるようになります。

▶▶ 警告を作成するには

1 AZCC で、警告で検出する監査レコードの種類を照会するクエリを作成し、保存します。

メモ 警告の作成に使用される保存済みのクエリには、少なくとも 1 つは制限が設定されている必要があります。つまり、「SELECT *」と同等であってはならないということです。警告クエリには、少なくとも 1 つの検索条件を設定する必要があります。

2 ［**管理者**］>［**警告の管理**］を選択して［警告の管理］ウィンドウを開きます。

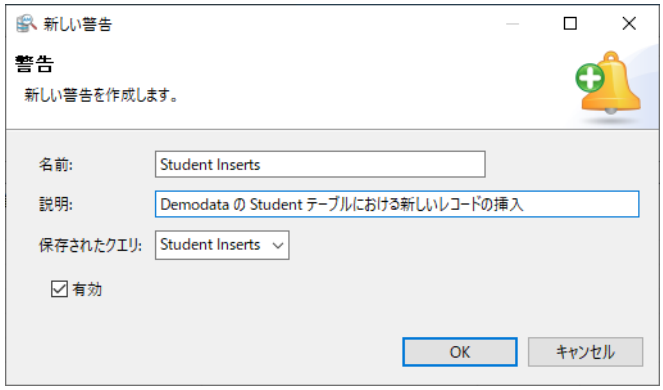


3 ［**新規**］をクリックして［新しい警告］ウィンドウを開きます。

4 この警告の名前を文字、数字、スペースを使用して 40 文字までで入力します。

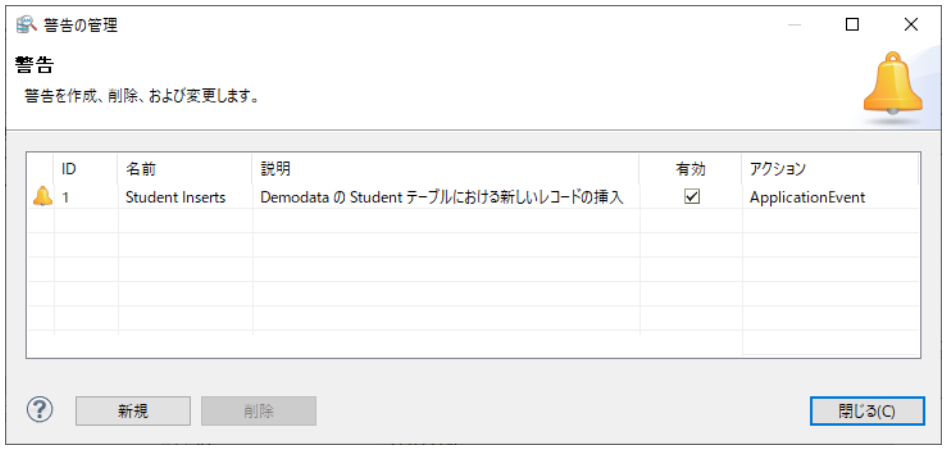
この例では、Demodata データベース内の新しい学生について警告を作成します。

5 警告の説明を 100 文字までで入力します。



6 ［保存されたクエリ］リストから、使用するクエリを選択します。

7 ［OK］を選択して［警告の管理］ウィンドウに戻ると、追加した警告が表示されています。



この警告は、Zen データベース サービスが再起動されるとアクティブになります。選択した保存済みクエリに一致する監査レコードがキャプチャされると、データベース活動により警告がトリガーされます。この監査レコードには、ベル アイコン 🔔 を使ってフラグが付けられます。このアイコンは、その監査レコードを含むすべてのクエリ結果に表示されます。

Audit for Zen は、監査レコードにフラグを付けるだけでなく、Windows アプリケーション ログ %SystemRoot%¥System32¥Winevt¥Logs¥Application.evtx にエントリを書き込みます。このログ エントリは、Windows イベント ビューアーでは次のように表示されます。

レベル	日付と時刻	ソース	イベント ID	タスクのカテゴリ
情報	2021/02/04 17:43:11	Actian AuditMaster	16717	AuditMaster Alert

メモ ログに記録された警告を Windows イベント ビューアーで確認する場合は、［現在のログをフィルター］を選択し、［イベント ソース］を Actian AuditMaster に設定すると役立ちます。

このイベント ログ エントリに関する次の情報に示すように、Zen データベース レコードのデータ詳細は AZCC の監査レコードのデータ詳細と同じです。

```
Alert 'Student Inserts' Fired on Record ID: 55
Alert ID: 1
Desc: Addition of new records in Student table of Demodata

Audit Information
=================
Rec Id:         55
Date:           07/10/2019
Time:           17:00:07
DBMS:           Actian Zen
DB Ver:         14.0.41
Op Context:     BTRIEVE
Operation:      Insert
Dep Rec Id:     0
Product :       Zen Demo
Product Ver:    9
Component:      <User Tables>
Component Ver:  9
Table:          Student
Group:          Demo
```

```
Net Address:   Zen-Server.englab.local
Net User ID:   Master
Process:       Zen Engine
Monitor Ver:   Zen Demo
OS Ver:        W2K 6.2.9200
Return Code:   0

Record Data
==========
ID:                  334651124
Cumulative_GPA:      3.400
Tuition_ID:          5
Transfer_Credits:    12
Major:               Computer Science
Minor:               Statistics
Scholarship_Amount:  0.00
Cumulative_Hours:    12

Additional Information
======================
View Path:           ¥¥ZEN-SERVER¥PVSWAUDIT$¥data¥
Server Net ID:       192.168.149.142
```

監査警告の最良実施例

警告を使用する際には、以下の点に留意してください。

- ［有効］チェック ボックスをオンにすると、警告がアクティブ化されます。チェック ボックスをオフにした場合は、警告が非アクティブ化され、クエリに一致する監査レコードがあっても警告がトリガーされなくなります。このため、クエリ結果では監査レコードに対してベル アイコンが表示されなくなると共に、Windows イベント ログにエントリが書き込まれなくなります。
- 多数の監査レコードに一致するような広範なクエリが警告に指定されていると、その警告から大規模な望ましくないログ記録が生じる可能性があります。最良の実施例は、追加のアクションを必要とする有用な情報だけにクエリ対象を絞り込むことです。
- 同様に、大量のデータ レコードをバルク ロードする予定で、その監査ログが警告クエリに一致するような場合は、バルク ロード前に警告を無効にし、バルク ロード後に警告を再び有効にしてください。

監査レコードまたはログ レコードの検索

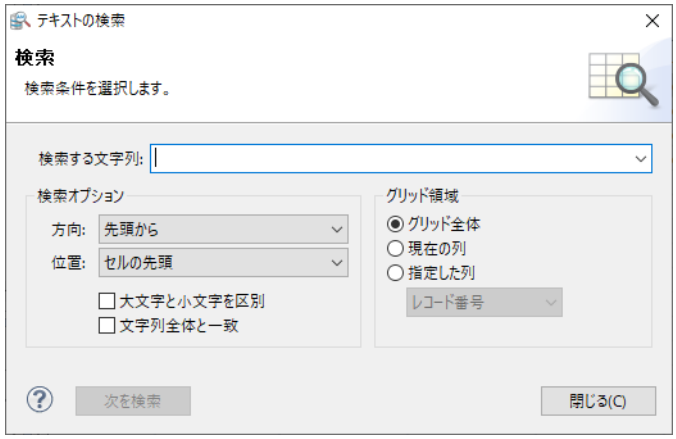
［監査レコード］タブまたは［ステータス ログ］タブで、ユーザー、日付、時刻などの値の特定の文字列を検索するには、検索コマンドを使用します。この検索機能には、大文字と小文字の区別、特定のタブ列の絞り込みなど、いくつかのオプションがあります。

メモ レコード数や検索条件の複雑さに応じて、検索を完了するまでに時間がかかる場合があります。可能な限り、条件を絞り込むようにしましょう。

▶▶ 監査レコードまたはログ レコードを検索するには

1 ［監査レコード］タブまたは［ステータス ログ］タブを選択します。必要に応じて、表示されたエントリを更新します。

2 ［**ツール**］>［**検索**］を選択するか、または当該タブの右上にある［**検索**］アイコン をクリックします。



3 ［検索する文字列］フィールドで、現在表示されている監査レコードから検索したいテキスト文字列を入力します。

4 必要に応じて、［検索オプション］を使用して検索結果を絞り込みます。

- ［方向］オプションで、検索を始める方向を選択します。選択肢として、"**先頭から**"、"**後方**"、"**前方**"があります。
- ［位置］オプションで、検索位置を選択します。必要に応じて、"**セルの先頭**"または"**任意の場所**"を選択します。
- スペルの大文字小文字を一致させるには、［**大文字と小文字を区別**］チェック ボックスをオンにします。
- 検索文字列の一部だけでなく検索文字列全体を一致させるには、［**文字列全体と一致**］チェック ボックスをオンにします。

5 必要に応じて、［グリッド領域］を使用して検索結果を絞り込みます。

- すべての列を検索するには、［**グリッド全体**］を選択します。
- 現在の一致によって強調表示されている列内のみで検索を行うには、［**現在の列**］を選択します。
- ［**指定した列**］を選択し、リストから列名を選択します。

6 ［**次を検索**］をクリックします。

一致する文字列が見つかると当該のタブで強調表示されます。また、クエリ結果内の場所が［テキストの検索］ウィンドウに表示されます。その他の一致を表示するには、［次を検索］をクリックし続けます。最後の一致に到達して、再び［次を検索］をクリックすると、" 一致する項目がありません " というメッセージが表示されます。前の一致に戻るには、［テキストの検索］ウィンドウを閉じて再度開き、もう一度検索します。前回の検索で入力した文字列は保存されています。

テキスト ファイルへの監査レコードまたはログ レコードのエクスポート

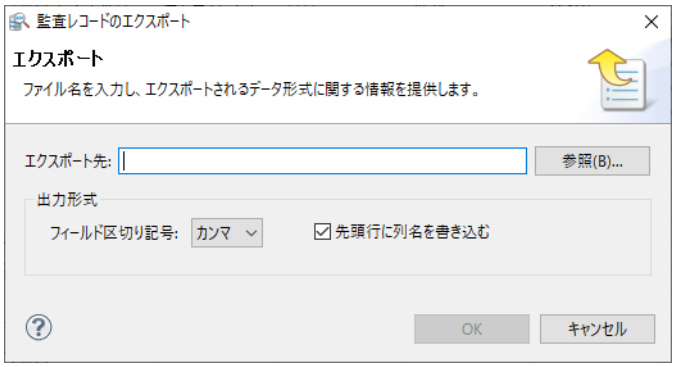
Audit for Zen は、［監査レコード］タブまたは［ステータス ログ］タブの表示内容をカンマ区切りまたはタブ区切りのテキスト ファイルにエクスポートすることができます。

当該のタブに表示されているレコードと列のみがエクスポートされます。エクスポート先のテキストに含める列を変更するには、［表示する列の選択］設定を使用します。

▶▶ 監査レコードをエクスポートするには

1 ［監査レコード］タブまたは［ステータス ログ］タブを選択します。［監査レコード］タブの場合は、必要に応じて現在のビュー ファイルを更新してクエリを再実行します。

2 ［**ツール**］>［**エクスポート**］を選択するか、または当該タブの右上にある［**エクスポート**］アイコン を クリックします。



3 ［エクスポート］ウィンドウの［参照］ボタンをクリックして、エクスポート先のファイルのパス名を選択します。デフォルトの場所は C:¥Users¥< **ユーザー名** >¥< **ファイル名** > です。必要に応じて .txt などの拡張子を追加します。

4 フィールド区切り記号として、カンマまたはタブを選択します。

5 エクスポート先ファイルの先頭行に列名を書き込むデフォルト　オプションを使用するかどうかを選択します。

6 ［OK］をクリックしてファイルをエクスポートします。

Zen セキュリティの下での監査レコードの表示

Zen セキュリティを有効にして Audit for Zen を実行する場合、［ユーザー名］列と［データベース名］列のフィールド値は、次の表に示すように、DefaultDB データベースのセキュリティ ポリシーとデータベース操作の種類によって変わります。

表 1　DefaultDB データベースのセキュリティの下で監査されるユーザー名とデータベース名

	Btrieve 操作		SQL エンジン操作	
セキュリティ ポリシー	表示されるユーザー名	表示されるデータベース名	表示されるユーザー名	表示されるデータベース名
データベース	データベース ログイン	次のいずれかです。 • Btrieve ログイン API または接続文字列のデータベース名 • 操作が実行された場合は、操作対象の Btrieve ファイルにバインドされているデータベース名 • 他の 2 つを入手できない場合は DefaultDB	データベース ログイン	N/A
混合	データベース ログイン		データベース ログイン	N/A
クラシック	• OS ログイン • データベース セキュリティが有効になっている場合は、データベースのユーザー名		• OS ログイン • データベース セキュリティが有効になっている場合は、データベースのユーザー名	N/A

監査される Btrieve 操作には、選択 / 読み取り、挿入、更新、削除、ログイン、およびログアウトが含まれます。トランザクションの開始 / 終了 / 中止やリセットのような、特定のデータベースと関係していない操作の場合は、データベース名を入手できません。

ログイン エラーがある場合は、無効なユーザー名とデータベース名と共に記載されます。SQL ログインの場合、ホスト名はログイン時には不明ですが、その後利用可能になり、SQL 操作に表示されます。

混合セキュリティの下では、データベース ログインはオペレーティング システム ログインやネットワーク ログインと一致しています。

Audit for Zen の Windows へのログインと Zen データベースのログインとの関係の詳細については、「Zen セキュリティ下での Audit for Zen の実行」を参照してください。Zen セキュリティ環境におけるデータベース操作の詳細については、『*Advanced Operations Guide*』を参照してください。

Audit for Zen の元に戻す機能の使用

Audit for Zen の元に戻すコマンドは、特定のデータベース イベントを取り消すことを可能にします。正常に元に戻るかどうかは、行った操作と関与したレコードの現在の状態によります。レコードは、確認対象の監査イベントがキャプチャされてから後に、再び変更された可能性があります。たとえば、データ フィールドの更新の場合は、監査レコードの［変更の前 / 後］の詳細における変更前の値に、Audit for Zen が復元を試みることができるデータが表示されます。

操作	元に戻した結果
挿入	レコードがまだ存在しており、ほかに挿入を阻止する条件がない場合は、レコードを削除します。
削除	レコードが存在しない場合は再挿入します。あるいは存在しても、重複が許可されており、ほかに挿入を妨げる条件がない限りは、再挿入します。
更新	レコードがまだ存在しており、ほかに更新を阻止する条件がない場合は、レコードの変更前の状態に戻します。

注意 元に戻す操作を試みる前に、以下のことを考慮してください。

- ログインと AZCC の実行に使用する Windows ユーザー名は、監視する Zen データベースへの書き込みのアクセス許可を持っている必要があります。Windows と Zen サーバーのどちらも、Audit for Zen 内で作成された Audit for Zen 管理者および通常ユーザーのアカウントを認識しません。
- 監査レコードに記載されたファイルは、操作が発生しているため、監査設定グループから削除することはできません。
- Audit for Zen 内から操作を戻すことには、アプリケーション データを矛盾した不合理な状態にするリスクがあります。アプリケーション データベースの一部を他の部分とは無関係に変更することに関する注意を理解している、詳しい知識のある Zen ユーザーだけが行ってください。
- 監査設定のグループに名前が同じでパスが異なるファイルがある場合は、最初に記載されているファイルのみを元に戻す対象とします。

メモ：リモート クライアントのログインは、元に戻すをサポートしていません。

▶▶ データベース操作を元に戻すには

1 ［監査レコード］タブで、監査レコードを右クリックして［**操作を元に戻す**］を選択します。このコマンドは、" 挿入 "、" 削除 "、" 変更の前 / 後 " など該当する操作でのみ利用可能です。

2 確認ダイアログが表示されたら、操作を元に戻す場合は［**はい**］を、元に戻すのを止める場合は［**いいえ**］をクリックします。

メモ 元に戻す操作はすべて Audit for Zen によってキャプチャされているので、元に戻す操作自体も元に戻すことで取り消すことができます。

Audit for Zen の管理

8

管理者タスクの段階的な説明

管理者として特定のタスクを実行し、Audit for Zen がどのように動作するかを定義することができます。監査の設定を追加するにあたって、これらのタスクのためのメニュー コマンドは、管理者権限を持つユーザーのみが利用できます。

- 「サーバーの追加と削除」
- 「ステータス ログのアクティビティの確認」
- 「監視の無効化および有効化」
- 「ユーザーの管理」
- 「サーバー設定の管理」
- 「ネットワーク共有をローカル パスに置き換える」

サーバーの追加と削除

監査サーバーとは、Audit for Zen がインストールされている Zen サーバーのことです。監査サーバーの接続設定は amserver ファイルに格納されています。デフォルトのインストールでは、このファイルは C:¥ProgramData¥Actian¥Zen¥Audit¥DATA にあります。

サーバーの追加

Audit for Zen のインストールでは、ローカルの Zen サーバーは自動的に監査サーバーとして追加されます。Windows ログインでのネットワーク アクセス許可とファイル システムのアクセス許可がある場合は、リモートの監査サーバーを手動で追加することもできます。

▶▶ サーバーを追加するには

1 追加したいサーバーを調べて、Zen データベース エンジンが実行されていることを確認します。

2 AZCC で［**サーバー**］>［**追加**］を選択します。

3 監査サーバーの amserver ファイルのパスを入力します。

デフォルトのインストールでは、このパスは **¥¥***server*¥PVSWAUDIT$¥DATA¥amserver です。*server* には、Zen データベース サーバーの名前が入ります。PVSWAUDIT$ 以外のカスタム共有名が選択されている場合もあることに留意してください。

4 ［OK］をクリックします。

選択したサーバーがデータ ツリーに追加されます。

この追加される名前は、お使いのシステムまたはネットワークによっては、マシン名や amserver ファイルへのパスになる場合があります。

メモ クライアントが Audit for Zen サーバーに正常に接続できない場合には、-108 エラー メッセージを受け取ります。これは、誤ったネットワーク マッピングや、その他のネットワーク問題が原因である可能性があります。製品キーのユーザー数が足りないことも考えられます。「認証ライセンス」を参照してください。

5 ログインする新しい監査サーバーを展開するか、またはそのサーバーを右クリックして［ログイン］を選択します。

6 ［ログイン］ダイアログ ボックスで、Audit for Zen ユーザーの名前とパスワードを入力して［OK］をクリックします。

これで、リモートの監査サーバーを使用する準備が完了しました。

サーバーの削除

AZCC のデータ ツリーから監査サーバーの接続を削除すると、クライアントはそのサーバーにアクセスできなくなります。しかし、サーバーでの監査は引き続き行われ、既存の監査レコード、ユーザー、設定情報は Zen サーバーに格納されているため、そのまま残ります。サーバー接続を再度追加すると、以前にあったものがすべてデータ ツリーに再表示されます。

▶▶ サーバーを削除するには

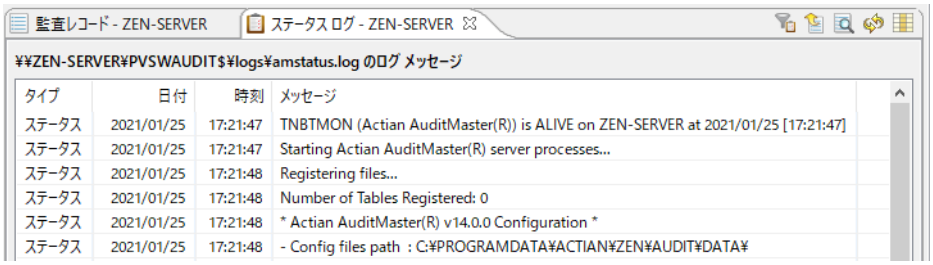
1 データ ツリーで監査サーバーをクリックし、［**サーバー**］>［**削除**］を選択します。

2 ダイアログ ボックスで［**はい**］を選択して確定します。

ステータス ログのアクティビティの確認

［ステータス ログ］タブには、Audit for Zen 自体によって実行されたログが表示されます。Audit for Zen の動作によって生じたステータスおよびエラー メッセージが一覧表示されます。開発者の場合は、デバッグを目的としてメッセージを収集するように構成することも可能です。

［ステータス ログ］タブを開くには、［**管理者**］>［**ステータス ログの表示**］を選択します。



このタブには、［監査レコード］タブと同様に、表示内容を操作できるアイコンがあります。次の表において、検索、エクスポート、および列の表示は［監査レコード］タブの場合と同様の方法で使用できるので、それら対応トピックへのリンクも記載してあります。表下にメッセージのフィルタリングと並び替えの手順を示します。

コマンド	説明
ログ メッセージのフィルター	表示されるステータス ログ メッセージを種類別、日付別にフィルターします。デフォルトでは、ステータスおよびエラー メッセージが表示されます。デバッグ メッセージを表示するように選択することもできます。
エクスポート	現在のビュー ファイルまたはアーカイブされたビュー ファイルをテキスト ファイルにエクスポートします。［ステータス ログ］タブを使用したエクスポートは、「テキスト ファイルへの監査レコードまたはログ レコードのエクスポート」で説明したのと同じ方法で使用できます。
検索	［ステータス ログ］タブで特定のテキストを検索します。詳細については、「監査レコードまたはログ レコードの検索」を参照してください。
ステータス メッセージの更新	［ステータス ログ］タブで、ログに記録されたステータスおよびエラー メッセージの一覧を更新します。
表示する列の選択	このタブに表示する列を選択します。

▶▶ ステータス ログ メッセージをフィルターおよび並べ替えするには

1 ［ステータス ログ］タブを開きます。

2 フィルター アイコン をクリックします。

- メッセージを種類別にフィルターするには、［デバッグ］、［エラー］、［ステータス］、またはこれらの組み合わせを選択します。
- 特定の日付範囲でフィルターする場合には、［**最初**］または［**最後**］あるいはこれら両方のチェック ボックスをオンにして、日付範囲を設定します。どちらのチェック ボックスもオンにしない場合のデフォルトの日付範囲は、現在の表示内容における最初のレコードの日付から最後のレコードの日付までとなります。

3 フィルター オプションをすべて設定し終わったら、［OK］ボタンをクリックします。

4 並べ替えに使用する列のヘッダーをクリックすれば、メッセージを並べ替えられます。並べ替え順序をデフォルトに戻すには、このタブを閉じて再度開きます。

監視の無効化および有効化

レコードのバルク ロードなどいくつかの手順では、データベースの監視を一時的に停止することをお勧めします。その理由は、これらの手順で想定される大量の監査レコードでは、通常の監視の場合と同じ値が提供されないからです。このような場合は、Audit for Zen の監視を手動で無効にして手順を実行し、再度監視を有効にして通常の監査活動に戻します。

メモ 以下の手順は、監視対象の Zen サーバーと同じマシンでローカルにのみ実行できます。

▶▶ 監査サーバーでの Audit for Zen による監視を無効にするには

1 管理者権限を持つ Audit for Zen ユーザーとして AZCC にログインします。

2 ［監査サーバー］で、無効にするマシンの名前を右クリックします。選択対象のマシン名の横には "（監視実行中）" というメッセージが表示されています。

3 ［**監視を無効にする**］を選択します。

4 Zen エンジン サービスを再起動するように求められたら、［**はい**］をクリックします。

マシン名の横のメッセージが "（監視は無効）" に変わります。これで、監査レコードとしてキャプチャされる可能性のあったデータベース プロシージャを実行できるようになりました。

データベース手順を実行し終わったら、監査を復旧するために次の手順を実行します。

▶▶ 監査サーバーでの Audit for Zen による監視を有効にするには

1 管理者権限を持つ Audit for Zen ユーザーとして AZCC にログインします。

2 ［監査サーバー］で、有効にするマシンの名前を右クリックします。選択対象のマシン名の横には "（監視は無効）" というメッセージが表示されています。

3 ［**監視を有効にする**］を選択します。

4 Zen エンジン サービスを再起動するように求められたら、［**はい**］をクリックします。

マシン名の横のメッセージが "（監視実行中）" に変わります。これにより、設定されている監査設定に基づいて、データベース活動が再び監視されます。

ユーザーの管理

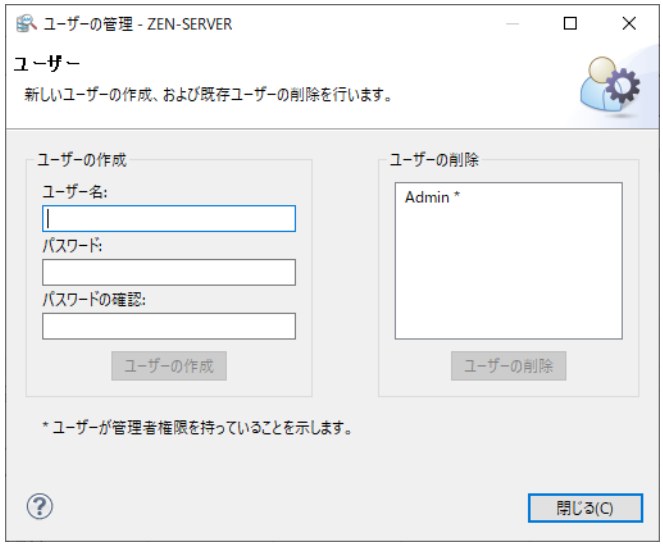
Audit for Zen のセキュリティの一環として、ユーザーは Audit for Zen システムにアクセスするには認証される必要があります。管理者は、各ユーザーのユーザー名を定義し、パスワードを発行します。また、各ユーザーに管理者権限を付与するかどうかを決めます。

このトピックでは、［ユーザーのメンテナンス］ウィンドウで実行できるタスクを説明します。

- 「ユーザーを追加するには」
- 「ユーザーを削除するには」

ユーザーを追加するには

1 ［**管理者**］>［**ユーザーのメンテナンス**］の順に選択するか、またはツールバーの アイコンをクリックします。



2 ［ユーザーの管理］ウィンドウで、ユーザー名とパスワードを入力します。ユーザー名は大文字と小文字を区別せず、スペースを含む最長 20 文字まで指定できます。パスワードは大文字と小文字を区別します。最長 40 文字まで指定できます。ダブルバイトの文字セットでは、ユーザー名、パスワードはそれぞれ最長 10 文字、20 文字まで指定できます。

3 ［**ユーザーの作成**］をクリックします。

4 このユーザーに Audit for Zen 管理者権限を付与するかどうかを尋ねられます。［**はい**］または［**いいえ**］をクリックします。

右側にあるリストに新しいユーザーが表示されます。

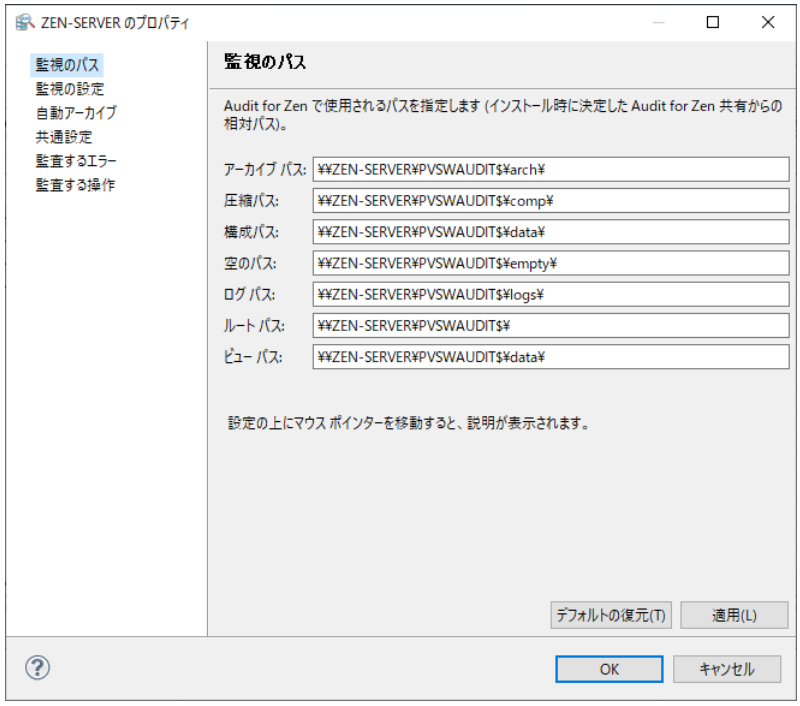
ユーザーを削除するには

1 ［**管理者**］>［**ユーザーのメンテナンス**］を選択します。

2 ［ユーザーの管理］ウィンドウの［ユーザーの削除］リストからユーザーを選択し、［**ユーザーの削除**］をクリックします。

サーバー設定の管理

［サーバーの設定］ウィンドウは、Audit for Zen のオプションを表示します。これは、［**管理者**］>［**サーバー設定**］から開くことができます。



このウィンドウは設定のグループを提供します。次の表で示すとおり、一部の設定は変更が可能ですが、多くの場合、変更は必要ありません。

変更を有効にするには、［**適用**］または［OK］ボタンをクリックする必要があります。また、自動アーカイブ以外の設定について、変更した設定を有効にするには、Zen データベース エンジンを再起動する必要があります。

設定グループ	設定	用途
監視のパス	さまざまなパス名	これらの場所は、共有ボリュームで動作するようにインストール時に設定され、その共有ボリュームは Audit for Zen インストーラーによって作成されます。通常の環境では、デフォルトのパスをご利用いただけます。ただし、セキュリティ要件を満たす必要がある場合は、共有を明示的なローカル パス名に手動で置き換えることもできます。手順については、「ネットワーク共有をローカル パスに置き換える」を参照してください。そうすることで、リモート クライアントがブロックされ、ローカル システムへのアクセスのみに制限されます。
監視の設定	保持するアーカイブ数	「自動アーカイブ」と組み合わせて使用します。この値のデフォルトは -1 で、これは、システムがアーカイブ ファイルの数を制限しないことを意味します。値が 0 よりも大きい場合は、システムは指定された数だけ新しいファイルを保持し、古いファイルから削除します。この設定を使用することで、アーカイブ済みの監査レコードを誤って削除してしまう可能性があります。アーカイブ ファイルを自動的に削除することが望ましくない状況もあり得ることを考慮してください。
監視の設定	マッパーのしきい値	Audit for Zen 内の現在のビュー ファイルを自動更新する頻度を制御します。デフォルトは 1 で、これは 1 分を表します。値をゼロに設定すると、自動更新はオフになります。amstatus.log 内の該当エントリは、"Running Mapper after *n* minute(s)." です。

設定グループ	設定	用途
自動アーカイブ	アーカイブ ファイルの作成	監査レコードをアーカイブ ファイルへ自動的に移動する方法を設定します。手順については、「自動アーカイブ」を参照してください。
共通設定	アーカイブのディスク制限	「自動アーカイブ」と組み合わせて使用します。この値のデフォルトは -1 で、これは、システムがアーカイブ ファイルの合計ファイル サイズを監視しないことを意味します。値が 0 バイトよりも大きい場合は、システムは最新のファイルから、ファイルの合計サイズが指定されたバイト数以下になるファイルのみを保持し、古いファイルを削除します。アーカイブ ファイルを自動的に削除することが望ましくない状況もあり得ることを考慮してください。
共通設定	ステータス ログの最大サイズ	amstatus.log ファイルの最大長（バイト単位）。デフォルトは 10000000（1 千万）バイトです。最小値は 1024 バイトです。
共通設定	ステータス ログ ファイル	amstatus.log ファイルの場所。デフォルトのパスでは Audit for Zen の共有の PVSWAUDIT$ を使用しますが、別の場所に置き換えてもかまいません。
監査するエラー	Btrieve エラー コード	監査イベントとして記録する、Microkernel エンジンのステータス コードを選択します。特定の番号がデフォルトでオンになっています。「監査するエラー」を参照してください。
監査する操作	グローバルに監査するデフォルトの操作	監視する各ファイルについて、デフォルトで監査ログに入れる Microkernel エンジンのイベントを設定します。これらの設定は、ファイルごとに手動で変更することができます。「グローバルに監査する操作」を参照してください。

自動アーカイブ

［自動アーカイブ］グループでは、監査レコードのアーカイブを設定するためのオプションを提供しています。

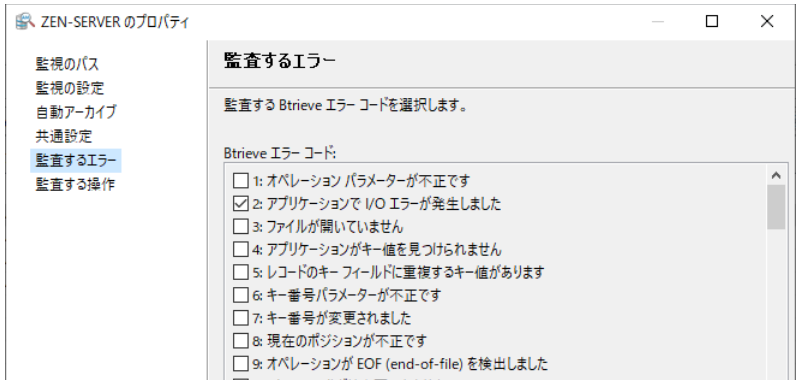
デフォルトでは、Audit for Zen は、ログ ファイルが 75 MB を超えると、自動的に監査レコードをアーカイブ ファイルに移動します。［管理者］>［サーバー設定］>［自動アーカイブ］では、デフォルトのサイズを変更したり、日時単位でアーカイブするように選択したり、またはこれらの組み合わせを設定したりすることができます。サイズのしきい値の許容範囲は 40 ～ 1024 MB です。

［日時による］と［サイズのしきい値による］の両方のチェック ボックスをオンにした場合には、どちらか先に一致した条件が、アーカイブ ファイルを作成してログ ファイルを空にするよう、システムに指示します。

［サイズのしきい値による］をオフにし、［日時による］をオンにした場合でも、システムは 1024 MB のしきい値を使用します。設定した日時になる前にログ ファイルが 1024 MB に達した場合には、システムは自動的にアーカイブを行い、設定した日時になったときに再度アーカイブします。

監査するエラー

[監査するエラー]グループでは、監査イベントとしてキャプチャすることができる Microkernel エンジンのステータス コードのセットを一覧表示します。



ステータス コードの監査が機能するには、以下のすべてが真である必要があります。

- 監査するエラーがこのリストで選択されている。
- エラーが発生するテーブルまたはファイルが、監視する監査グループに割り当てられている。
- エラーが発生したときに実行する操作は、ファイルの監査操作である。たとえば、更新操作についてステータス 46 を記録するには、そのテーブルまたはファイルに対して［変更の前 / 後］を選択しておく必要があります。

最新のリリースでは、エラーのリストにはデフォルトで以下のコードが選択されています。

2、18、19、30、32、46、51、54、85、120、132、161、170、171

特定のエラーについて監査レコードをキャプチャしたくない場合は、リスト内でそのエラーのチェック ボックスをオフにします。

リスト内のステータス コードについては、Zen データベース ドキュメントの『*Status Codes and Messages*』を参照してください。

リストから選択を行ったら、それらの選択を有効にするために Zen データベース エンジンを再起動する必要があります。

グローバルに監査する操作

［監査する操作］ウィンドウには、［監査の設定］のグループ作成 / 編集ウィンドウにあるのと同じ［挿入］、［削除］、［変更の前 / 後］、［読み取り］イベントがあります。また、セッション イベントの［トランザクションの開始 / 終了］、［トランザクションの中止］、［リセット］を監査することもできます。セッション イベントの［ログイン / ログアウト］は必ず監査されるので、監査しないように設定することはできません。

これらのオプションは、個々のファイルの設定とは異なり、監査の設定に含まれるあらゆるファイルにグローバルに適用されます。

Audit for Zen のインストール時、このウィンドウにおけるデフォルト設定には、読み取りとリセットを除くすべての操作が含まれています。異なるオプションを選択した場合には、それが監査グループに追加するすべてのファイルの新しいデフォルト設定になります。［**すべてに適用**］を選択しない限り、以前に監視対象としたファイルの監査イベントは影響を受けません。

最後に、グループから任意のファイルを削除し、再度追加した場合には、そのファイルの監視する操作の設定は、このウィンドウの現在の選択項目がデフォルトとなります。

個々のファイルの設定の詳細については、「テーブルまたはファイル別に監視する操作」を参照してください。

変更を加えた後は、新しい設定を有効にするために Zen データベース エンジンを再起動する必要があります。

メモ Zen データベースでは、クライアント側のキャッシュ エンジンがオンになっている場合、キャッシュ エンジンは 8 回連続で読み取りをした後、さらに読み取ることを見越してデータベース ページ全体を読み取ります。キャッシュ エンジンによって読み取られたデータベース ページ内のレコードは、サーバー上のモニターで監査されません。監査において、あらゆる読み取りをキャプチャすることを必要とする場合は、クライアント キャッシュが無効になっていることを確認してください。ただし、エンジンのキャッシュを使わないと、データベースのパフォーマンスが低下することがあります。Zen Control Center で［**ローカル クライアント**］を展開し、［MicroKernel **ルーター**］を右クリックして［**プロパティ**］を選択します。次に［**パフォーマンス チューニング**］をクリックして、［**キャッシュ エンジンの使用**］設定を確認します。デフォルトで、この設定はオフです。

ネットワーク共有をローカル パスに置き換える

Audit for Zen は非表示のネットワーク共有をインストールして、リモート クライアントが他のシステムから Audit for Zen にアクセスできるようにします。セキュリティ上の理由により、ネットワーク共有を無効にしてリモート アクセスをブロックする場合は、Audit for Zen をインストールした後に、ネットワーク共有を明示的なローカル パスに置き換えることができます。この置き換えは、Audit for Zen がインストールされているサーバーでのみ行うことができます。リモート クライアントからは行えません。既存の監査レコードに影響を与えませんが、共有の削除処理を完了するには、監視を再起動するときに一時的に監査を停止する必要があります。

メモ ネットワーク共有を削除すると、すべての AZCC クライアントが Audit for Zen システムにリモート アクセスできなくなります。削除しなければならないことを確認してください。

▶▶ デフォルトのネットワーク共有をローカル パスに置き換えるには

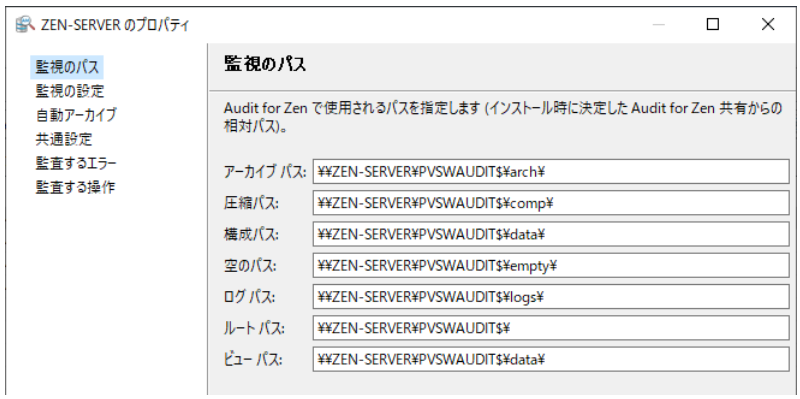
1 Audit for Zen サーバーがインストールされているシステムで、AZCC を起動します。

2 監査サーバーのリストで 1 つの監査サーバーを右クリックし、［**ログイン**］を選択します。

3 Audit for Zen の管理者ログイン ユーザー名とパスワードを入力し、［OK］をクリックします。

メモ 組み込みのユーザー ID admin は、デフォルトのパスワード MASTER を持っています。このパスワードを変更するには、「ユーザー パスワードの変更」を参照してください。Audit for Zen のデータベースへのログインと OS のログインとの関係については、「Zen セキュリティの下での監査レコードの表示」を参照してください。

4 ［**管理者**］>［**サーバー設定**］を選択します。



5 監視パスごとに、パス名を選択し、

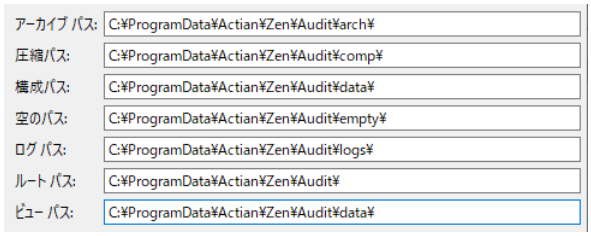
¥¥*server*¥PVSWAUDIT$

を以下のように変更します。

drive:¥*Zen root directory*¥Audit

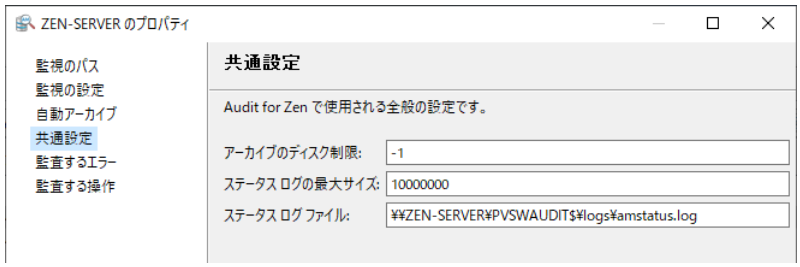
server は、Zen サーバーと Audit for Zen Monitor がインストールされているシステムの名前です。*drive* と *Zen root directory* はそれぞれ、インストール時に選択した Audit for Zen ディレクトリのローカル ドライブ文字と絶対パス名です。

6 デフォルトのインストール場所 C:¥ProgramData¥Actian¥Zen¥ を使用している場合、この例での結果は以下のようになります。



7 ［**適用**］ボタンをクリックします。

8 オプションの一覧で［**共通設定**］をクリックすると、デフォルトのインストールの場合は次のような値が表示されます。



9 ステータス ログ ファイルのパス名を選択し、それを以下に変更します。

drive:¥*Zen root directory*¥Audit¥logs¥amstatus.log

10 値の変更が終わったら、［**適用**］、［OK］の順にクリックします。

Zen エンジン サービスを再起動するように求められたら、［**いいえ**］をクリックします。

11 AZCC で［**サーバー**］>［**削除**］の順に選択し、確認を求められたら［**はい**］をクリックします。

12 AZCC を終了します。

ネットワーク共有を削除するには、Audit for Zen と Zen データベース エンジンは停止させなければいけません。

13 ZenCC を開き、Zen エクスプローラーで［サービス］ノードを右クリックして［**全サービスの停止**］を選択します。

14 Windows エクスプローラーで、*drive:*¥*Zen root directory* フォルダーを開きます。

15 共有フォルダーの Audit を右クリックし、［プロパティ］を選択します。

16 ［共有］タブを選択して、［詳細な共有］を選択します。

17 ［**このフォルダーを共有する**］チェック ボックスをオフにし、［OK］をクリックして共有を削除し、［プロパティ］を閉じます。

18 Zen エクスプローラーで、［サービス］ノードを右クリックして［**全サービスの開始**］を選択します。

19 Zen データベース エンジンが再起動したら、［**サーバー**］>［**追加**］を使用してサーバーを再びデータ ツリーに追加します。詳細については、「サーバーの追加」を参照してください。

20 AZCC を開いてログインし、Audit for Zen がネットワーク共有なしで正しく動作していることを確認します。

新しい Audit for Zen サーバーがネットワーク共有なしで動作する準備が整いました。他のサーバー設定は変更しません。以前にキャプチャした監視レコードはシステムに残ったままになっています。AZCC クライアントの接続方法のみが変更されています。

基本的なトラブルシューティング

9

一般的な問題の識別と解決方法

次のトピックでは、発生する一般的な問題の解決方法について説明します。

- 「一般的なヒント」
- 「トラブルシューティングの方法」
- 「ステータス ログの再開」
- 「アプリケーション データを変更したにもかかわらず、クエリを実行してもレコードが返されない」
- 「データベース エンジン」

一般的なヒント

このトピックでは、Audit for Zen を使用するための一般的なヒントを紹介します。

- 監視するアプリケーション データを構成する際は、選択したファイルが AZ サーバーと同じサーバーに存在していることを確認してください。
- Zen の設定が最適化されていることを確認してください。共通設定には通信プロトコル、ファイル、ファイル ハンドルがあります。設定と最適化の詳細については、Zen ドキュメントを参照してください。
- AZ は監査レコードに自動的に番号を付けます。この番号は 2,147,483,647 を上限とします。上限に達すると番号付けを折り返し、次の監査レコードの番号を再び 1 から始めます。番号が急に小さくなった場合は、この状況が発生していないかどうかを確認してください。

トラブルシューティングの方法

以下のチェックリストでは AZ における問題を診断するのに役立つ項目を挙げます。

- ❒ AZ ステータス ログにはエラーも記録されますか？「ステータス ログのアクティビティの確認」を参照してください。
- ❒ Zen データベース エンジンは起動していますか？「データベース エンジン」を参照してください。

ステータス ログの再開

Audit for Zen は、amstatus.log にステータス レコードを書き込みます。このファイルは、デフォルトのインストールでは C:¥ProgramData¥Zen¥Audit¥logs に配置されます。この場所は、管理者ユーザーが［管理者］>［サーバー設定］>［監視のパス］で変更できます。ディスクがいっぱいである場合などの特定の状況下では、Audit for Zen はこのエラー状態が解消されても、このファイルへのステータス メッセージの追加を続行できないことがあります。ステータス ログを再開するには、ログの内容をエクスポートし、その後ログを削除します。Audit for Zen は自動的に新しい amstatus.log ファイルを作成し、記録を開始します。

ステータス ログを再開するには

1 ［AZCC］ウィンドウで、［**管理者**］>［**ステータス ログの表示**］を選択して［ステータス ログ］タブを表示します。

2 「テキスト ファイルへの監査レコードまたはログ レコードのエクスポート」の説明に従って、［ステータス ログ］タブの内容をエクスポートします。

3 AZCC を終了します。

4 Zen サービスを停止します。

5 AZ のインストレーションにある logs フォルダーから、元の amstatus.log ファイルを削除します。

6 Zen サービスを再起動します。

Audit for Zen により、自動的に新しいステータス ログが作成され、現在のビュー ファイルで使用できるようになります。

アプリケーション データを変更したにもかかわらず、クエリを実行してもレコードが返されない

1 Audit for Zen の監視が有効になっていることを確認してください。

- AZCC の［監査サーバー］リストで、Zen サーバー名に "（監視実行中）" と表示されているはずです。
- Zen データベース エンジンが起動している必要があります。

2 監査の設定で、このアプリケーション ファイルが、監視対象として設定されていることを確認してください。

3 監視が実行されていて、ファイルが既に設定されている場合は、クエリを実行する前にビュー ファイルを更新してください。

4 アーカイブを行った直後でないことを確認してください。アーカイブの直後には現在のビュー ファイルには目的のレコードは存在しません。

5 ZenCC の License Administrator ツールを使用することで、Audit for Zen と Zen のどちらのライセンスもアクティブで、有効期限が切れていないことを確認してください。

データベース エンジン

AZ が機能するためには Zen データベース エンジンが起動している必要があります。

▶▶ データベース エンジンが起動しているかどうかを調べるには

次のいずれかを実行します。

- Zen Control Center で、［サービス］ノードを展開し、Zen データベース エンジンが起動していることを確認します。起動していない場合は、同じノードを右クリックして［**全サービスの開始**］を選択します。
- または、以下の手順を使用します。

  1. コントロール パネルから、Windows の［**サービス**］管理コンソールを開きます。
  2. Actian Zen Enterprise Server Engine を見つけます。
  3. 同サービスが開始されていない場合は、それを右クリックして［**開始**］を選択します。

高度な操作

10

パワー ユーザーおよびプログラマー向けの機能

高度な操作は、AZCC の外部から監査データにアクセスするためのユーティリティや方法を必要とするユーザー向けのものです。

- 「SQL を使って直接監査データを照会する」
- 「Audit for Zen とクライアント側のキャッシュ」

SQL を使って直接監査データを照会する

監査レコードにアクセスするための手段は、AZCC クライアントとその Query Builder だけではありません。これらのレコードに対して直接 SQL クエリを実行することもできます。これを行うには、まず、Audit for Zen で提供される Query Data-Model Generator（QDMG）ユーティリティを使用する必要があります。このユーティリティは、Audit for Zen システムの監査レコードにリンクされたビューの仮想データベースを作成するスクリプトを生成します。

クエリ データ モデル方法を使って、現在のビューとアーカイブの両方の監査レコードを直接照会することができます。直接クエリは、レポートを作成する、または監査レコードを表示するためのアプリケーションだけでなく、展開やデバッグ目的の役目を果たすアプリケーションをサポートできます。

Zen インストールに含まれる Demodata データベースに直接クエリ メソッドを適用する方法を示すための使用事例が提供されています。

このトピックでは、以下の項目について説明します。

メモ Audit for PSQL v12 では、内部ログおよび設定ファイルは Zen の長いオーナー ネームで保護され暗号化されているため、ここで説明する SQL クエリ メソッドはサポートされません。Audit for Zen v14 以降では、［監査レコードを暗号化しない］が設定されている場合は監査レコードを照会することができます。

Query Data-Model Generator ユーティリティ

Query Data-Model Generator（QDMG）は、一連の SQL ステートメントから成る、空のデータベースに対して実行するスクリプトを生成します。スクリプトはこの仮想データベースに、Audit for Zen ログ ファイルに格納されている監査レコードにリンクするビューを移入します。ビューが作成されたら、それに対してクエリを実行し、Audit for Zen 内の監査レコードから結果を返すことができます。

構文

`qdmg -d` *DDF_path* [`-m` *password*] `-p` *name* `-o` *file* [`-l` *logfile*] [`-a` *folder*]

オプション

オプション	説明
-a	amserver ファイルがある、リモート サーバー上の Data ディレクトリ。amserver がクライアントと同じシステムにある場合は任意です。
-d	インポートするデータベース スキーマ（.ddf ファイル）のパス名。
-m	データベースがセキュリティで保護されている場合は、Master パスワード。
-p	監査設定の名前。例 : Zen Demo。スペースが含まれる名前は引用符で囲んでください。
-o	生成された SQL の出力（.sql）ファイルのパスとファイル名。パス名を指定しない場合、ファイルは現在のディレクトリに書き込まれます。
-l	QDMG メッセージを記録したログ ファイル名。デフォルトは amlog です。
-h	ヘルプ。

ログ ファイルは、AZCC 内の現在のビュー ファイルのレコードを含んでいます。アーカイブ ファイル内の監査レコードにアクセスすることもできますが、それにはまず、現在のビュー ファイルに対するクエリを有効にする必要があります。次の短い手順を指定された順序どおりに行ってください。

1 「仮想データベースを作成する」
2 「現在のビュー ファイルでクエリを実行する」
3 「アーカイブ ファイルでクエリを実行する」

仮想データベースを作成する

このタスクでは、qdmg ユーティリティを使用して、監査データの直接クエリ用の仮想データベースを作成する手順を示します。この例では、Zen によってインストールされる Demodata を使用します。

1 仮想データベースの設定を行う前に、監査対象のデータベースのスキーマを AZ にインポートします。既に処理済みである場合は、次の手順に進みます。

   この例では、Demodata に対するインポートは、AZ インストールの一環として既に行われています。

   独自のデータベースからスキーマをインポートする方法について説明が必要な場合は、「スキーマの管理」を参照してください。

2 仮想データベースの作成では、監査レコードを照会するデータベースの DDF へのアクセスが必要となります。DDF のパスを見つけるには、以下のすべてを実行します。

   - Zen Control Center を開いて、監査するデータベース Demodata のブランチを展開します。
   - Demodata の［テーブル］ブランチを開き、テーブルを右クリックして［**プロパティ**］を選択します。
   - DDF が置かれる［辞書パス］に注目します。

3 仮想データベースを監査レコードにリンクする場合は、AZ 内のどの監査の設定が使用されるかを示す必要があります。その名前を調べるには、以下の両方を実行します。

   - AZCC を開いて、Audit for Zen 管理者としてログインします。
   - ［テーブル］タブの［監査の設定］リストから、スキーマをインポートする際に入力した監査設定の名前を見つけます。この例では、名前は "Zen Demo" で、Audit for Zen のインストレーションに既にインポートされているものです。

4 Windows エクスプローラーで、既存の Demodata フォルダーと同じレベルに新しいフォルダーを作成します。

この例では、"virtual" の V を付加して DemodataV というフォルダー名にしていますが、独自の名前を選択してもかまいません。仮想データベースを作成するためのスクリプトは、データベース自体と同様に、ここに保存されます。

5 qdmg を使用して、次の条件に基づいてスクリプトを生成します。

- 監査するデータベースの DDF のパス名（デフォルト値：C:¥ProgramData¥Actian¥Zen¥Demodata）
- Demodata データベースのセキュリティは無効になっているので、パスワードはありません
- 監査の設定の製品名は "Zen Demo"
- 生成されたスクリプトの出力用のパスとファイル名

コマンドは次のようになります。

```
qdmg -d C:¥ProgramData¥Actian¥Zen¥Demodata -p "Zen Demo" -o C:¥ProgramData¥Actian¥Zen¥DemodataV¥script
```

6 コマンド プロンプト ウィンドウを開いて、コマンドを実行します。

プロンプトが次のメッセージを返します。

```
Query Data-Model Generator Utility for Actian AuditMaster
Copyright (C) Actian Corporation 2019

Query Data-Model was generated into C:¥ProgramData¥Actian¥Zen¥DemodataV¥script.sql
```

次に、スクリプトを実行するデータベースを作成します。

7 Zen Control Center を開きます。

8 サーバーの名前の下にあるデータベース（エンジン）ノードを右クリックし、［**新規作成**］>［**データベース**］を選択します。

データベースの新規作成ウィザードが表示されます。

9 この例では、データベース名 DemodataV と作成したディレクトリ C:¥ProgramData¥Actian¥Zen¥DemodataV を使用します。

メモ 仮想データベースは、Audit for Zen インストール ディレクトリと同じボリュームにある必要があります。また、元のデータベースが長い（V2）メタデータを使用している場合は、この新しい仮想データベースの対応するチェック ボックスをオンにします。

10 ［**完了**］をクリックしてデータベースの作成を完了します。

11 Zen Control Center で［**ファイル**］>［**開く**］を選択します。

12 ［SQL ドキュメントを開く］ダイアログ ボックスで、これに先立って C:¥ProgramData¥Actian¥Zen¥DemodataV に保存された script.sql ファイルの場所まで移動します。

13 ［データベースの選択］ダイアログ ボックスで、［データベース］ツリーを展開し、DemodataV を選択して［OK］をクリックします。

SQL Editor に script.sql 内の SQL ステートメントが表示されます。

14 ［SQL］>［**すべての SQL ステートメントを実行**］を選択します。

script.sql 内のステートメントにより、DemodataV に監査レコードのビューが移入されます。作成内容を確認するには、ZenCC で、DemodataV データベースの下にある［ビュー］ノードを展開します。

これで、仮想データベース DemodataV は、監査レコードの列に対するクエリだけでなく、Demodata のデータ列に対するクエリもサポートするようになりました。

次のいずれかを行えます。

■ 照会できる対象を調べる。「監査レコードの構造」を参照してください。

- 現在の監査レコードを照会する。「現在のビュー ファイルでクエリを実行する」を参照してください。
- アーカイブされている監査レコードを照会する。「アーカイブ ファイルでクエリを実行する」を参照してください。

監査レコードの構造

このセクションでは、監査レコードの列について説明します。その構造は、`SELECT * FROM vstudent` などのクエリによって返される結果の典型です。

この例では次のことを注意してください。

- 結果内の監査列には、名前にプレフィックス AM$ が付き、監査データが含まれています。
- AM$ 監査データ列の後に続く行の残り部分は、監査対象テーブルのデータ フィールドで構成されており、監査イベントの発生時にそのテーブルから取り込まれた値が含まれています。
- 多くの監査列は、AZCC や Query Builder ウィンドウのタブに見られるクエリ属性と合致しています。
- 列名はすべて照会可能ですが、一部には、人的監査に特に関連していない内部的に使用されるコードが含まれています。

監査レコードの構造を検討した後、DemodataV 例でクエリを実行する手順については、「現在のビュー ファイルでクエリを実行する」を参照してください。

次の表では、監査レコードの列と AZCC の［監査レコード］タブに表示される列を比較しています。

表 2　仮想データベースと AZCC の監査レコード列

仮想データベース	AZCC	説明
AM$rec_id	レコード番号	監査レコードの内部番号
AM$opdate	日付	監査レコードのキャプチャ日付（例：2005-06-07）
AM$optime	時刻	監査レコードのキャプチャ時刻（例：17:04:30）
AM$dbms_id	—	内部使用
AM$dbmsverkey	—	Zen システムのバージョン
AM$opcontextkey	操作コンテキスト	正常な操作（BTRIEVE など）またはエラー
AM$opcode	—	内部使用
AM$optext	操作	データベース イベント。イベントには、Query Builder の［対象］タブの［操作］リストにある任意の項目が含まれます。 SQL ログインは、この列に表示されます。また、［サーバー設定］ウィンドウの［監査するエラー］領域で Zen ステータス コードを最初に選択したときに、その選択したステータス コードがここに表示されます。
AM$dep_rec_id	依存するレコード	以前の関連レコードのレコード番号： • 変更後のレコードに対する変更前のレコード • トランザクションを終了 / 中止したレコードに対する、トランザクションを開始したレコード
AM$prod_id	—	内部使用
AM$prodverkey	製品バージョン	監視対象ファイルの監査の設定に記載されている値
AM$product_name	製品	監視対象ファイルの監査の設定に記載されている値

表 2　仮想データベースと AZCC の監査レコード列

仮想データベース	AZCC	説明
AM$comp_id	データベース エンジン	AM Message API（AZ 内部で使用）または Zen
AM$compverkey	コンポーネント バージョン	監視対象ファイルの監査の設定に記載されている、コンポーネント バージョン
AM$comp_name	コンポーネント	監視対象ファイルの監査の設定に記載されている値
AM$tab_id	—	内部使用
AM$tabverkey	—	AM$compverkey と同じです
AM$table_name	テーブル名	イベントが発生したファイル。［対象］タブの［テーブル］属性と同じです。このファイルは、監査の設定で監視対象として選択されている必要があります。構成されたすべてのファイルは、Query Builder の［対象］タブの［テーブル］リストに表示されています。
AM$tabdef_id	—	内部使用
AM$group_name	グループ名	監査の設定における監視対象ファイルのグループ。［対象］タブの［グループ］属性と同じです。
AM$net_id	マシン名	イベントが発生したマシン名または IP アドレス。［場所］タブの［マシン名］属性と同じです。
AM$net_user_id	ユーザー名	イベントが発生したログイン ID。［ユーザー］タブのユーザー名と同じです。「Zen セキュリティの下での監査レコードの表示」を参照してください。
AM$process_name	プロセス名	監査イベントの発生元となったプロセス。［方法］タブの［プロセス］属性と同じです。
AM$sess_num	—	内部使用
AM$lic_num	—	内部使用
AM$mapstate	—	内部使用
AM$database_name	データベース名	監査イベントが発生したデータベース。イベントのレベルにおけるデータベース概念の実装によっては、この値は "n/a"（適用外）になる場合があります。
AM$osverkey	OS バージョン	AZ サーバーが実行されているオペレーティング システムの名前とバージョン
AM$retcode	—	内部使用
AM$reserved	—	内部使用
AM$databufsize	—	内部使用
AM$len	—	内部使用
<Data Column 1>	—	監査イベントが発生したテーブルの最初のデータ列
<Data Column 2>	—	監査イベントが発生したテーブルの 2 番目のデータ列
<Data Column *n*...>	—	さらなるデータ列 ...

現在のビュー ファイルでクエリを実行する

「監査レコードの構造」で説明した監査レコードを照会する前に、次の作業が完了していることを確認してください。

- qdmg を実行して、監査レコードにリンクされているビューを仮想データベースに入れ込むためのスクリプトを生成する
- 空のデータベースを作成する
- データベースでスクリプトを実行する

これらの作業が完了したら、この後の例に示すように、監査レコードに対する直接クエリを実行することができます。

▶▶ DemodataV 監査レコードの単純クエリを実行するには

1 AZ で、Zen Demodata の Student テーブルを監視するように組み込みの Zen Demo 監査設定を行い、その後、その設定を有効にするために Zen Control Center の[サービス]で Zen データベース エンジンを再起動します。

2 Zen Control Center で、Demodata データベース、Student テーブルの順に開きます。

SQL Editor で、デフォルトのクエリ `SELECT * FROM "Student"` によってすべての行が返されます。

3 先頭行の学生 ID には 190907350 が入っているはずです。この学生の GPA フィールドをクリックし、4.000 を 3.000 に変更して Enter キーを押します。

4 Zen Control Center で、［**ファイル**］>［**新規作成**］>［**SQL ドキュメント**］を選択します。

5 データベースを選択するよう求められたら、DemodataV をクリックします。

6 新しい SQL ドキュメントで次のクエリを実行します。このステートメントをコピーして、SQL Editor に貼り付けることができます。

```
SELECT AM$rec_id, AM$opdate, AM$optext, ID, Cumulative_GPA FROM VStudent
```

クエリは次のような結果を返します。

```
 AM$rec_id  AM$opdate AM$optext             ID Cumulative_GPA
========== ========== =============  ========= ==============
637         10/2/2019 Modify Before  190907350 4.000
638         10/2/2019 Modify After   190907350 3.000
```

アーカイブ ファイルでクエリを実行する

このトピックでは、「仮想データベースを作成する」で作成された仮想データベース DemodataV を参照します。

qdmg スクリプトは、仮想データベース内の選択テーブルが、現在のビュー ファイル内の監査レコードを指すように設定します。このファイルのデフォルトのパスは、C:¥ProgramData¥Actian¥Zen¥Audit¥data¥amlog です。このセクションで説明するように、アーカイブ ファイルへのパスは、名前がわかっている場合には設定し直すことができます。

アーカイブ ファイル名は、作成日に基づいた *yyyymmdd.nn* という書式になります。*yyyy* は年、*mm* は月、*dd* は日、*nn* はその日におけるアーカイブ ファイルの番号です。番号はゼロから始まります。ファイル名は大文字の V で終わります。アーカイブ ファイルのデフォルト フォルダーは、C:¥ProgramData¥Actian¥Zen¥Audit¥Arch です。

アーカイブ ファイルを圧縮すると、そのファイルは別のフォルダーへ移動されます。移動先のデフォルトは C:¥ProgramData¥Actian¥Zen¥Audit¥Comp で、ファイル名の V は Z に変更されます。ファイルの圧縮を解除すると、ファイルは Arch フォルダーに戻され、Z は V に戻されます。クエリは圧縮されていないレコードに対してのみ実行できます。

ここで説明する方法は、2 つの SQL スクリプトを使用します。

- 最初のスクリプトは、仮想データベースが、現在のビュー ファイルではなくアーカイブ ファイルを指すように設定します。

- 2 つ目のスクリプトは、仮想データベースを元の状態に戻して、再びクエリが現在のビュー ファイルから結果を返すようにします。

以下の手順は、以前に作成した仮想データベースの DemodataV を使用して、これらのスクリプトを示しています。この例は、これらのスクリプトを独自に書く方法を説明することを目的としています。

▶▶ アーカイブ ファイルのクエリ用に仮想データベースを設定し直すには

1 以下の手順を使用するには、アーカイブ ファイルが必要です。AZCC を開き、現在のビュー ファイルを右クリックして［**アーカイブ**］を選択します。

Audit for Zen は現在の監査レコードをアーカイブ ファイルに移動させます。

2 ［アーカイブ ファイル］ノードを展開し、右クリックして［**更新**］を選択します。

新しく作成されたアーカイブ ファイルがリストに表示されます。

3 ファイルの名前に注目してください。この例では 20160220.00V です。ファイルの接尾辞が V であることを確認したい場合は、アーカイブ フォルダー（たとえば、C:¥ProgramData¥Actian¥Zen¥Audit¥Arch）を見てください。

4 Zen Control Center で、［**ファイル**］>［**新規作成**］>［**SQL ドキュメント**］を選択します。

5 データベースを選択するよう求められたら、DemodataV をクリックします。

6 新しい SQL ドキュメントで、次の SQL ステートメントをすべて実行します。これらをコピーして、SQL Editor に貼り付けることができます。アーカイブ ファイルの名前は、20191015.00V ではなく独自の名前を使用してください。

```
-- このスクリプトは、仮想データベースを圧縮されていない
-- アーカイブ ファイル 20191015.00V に設定し直します。
ALTER TABLE AM$amlog IN DICTIONARY USING '..¥Audit¥Arch¥20191015.00V';
ALTER TABLE Billing IN DICTIONARY USING '..¥Audit¥Arch¥20191015.00V';
ALTER TABLE Class IN DICTIONARY USING '..¥Audit¥Arch¥20191015.00V';
ALTER TABLE Course IN DICTIONARY USING '..¥Audit¥Arch¥20191015.00V';
ALTER TABLE Dept IN DICTIONARY USING '..¥Audit¥Arch¥20191015.00V';
ALTER TABLE Enrolls IN DICTIONARY USING '..¥Audit¥Arch¥20191015.00V';
ALTER TABLE Faculty IN DICTIONARY USING '..¥Audit¥Arch¥20191015.00V';
ALTER TABLE Person IN DICTIONARY USING '..¥Audit¥Arch¥20191015.00V';
ALTER TABLE Room IN DICTIONARY USING '..¥Audit¥Arch¥20191015.00V';
ALTER TABLE Student IN DICTIONARY USING '..¥Audit¥Arch¥20191015.00V';
ALTER TABLE Tuition IN DICTIONARY USING '..¥Audit¥Arch¥20191015.00V';
```

メモ スクリプトは、仮想データベース内の AM$amlog テーブルに加え、監査対象のデータベースに含まれているデータ テーブルのすべてのコピーについても、テーブルの場所プロパティを変更します。このスクリプトの独自のバージョンを書く場合、仮想データベースの AM$Components、AM$OpList、AM$Products、AM$Tables テーブルについては、テーブルの場所プロパティを変更**しない**ようにしてください。

7 スクリプトを実行した後、これを再利用できるよう保持するために［**ファイル**］>［**別名保存**］を選択し、20191015.00V.sql のような名前で保存することができます。

これで、「現在のビュー ファイルでクエリを実行する」で実行した差分クエリは、現在のビューに対して実行した場合と同じ結果を返すはずです。これらの監査レコードは、現在仮想データベースが指しているアーカイブ ファイルに移動されました。

▶▶ 現在のビューのクエリ用に仮想データベースを設定し直すには

以下の手順により、再び現在のビュー ファイルで直接クエリを実行できるようになります。

1 Zen Control Center で、［**ファイル**］>［**新規作成**］>［**SQL ドキュメント**］を選択します。

2 データベースを選択するよう求められたら、DemodataV をクリックします。

3 新しい SQL ドキュメントで、次の SQL ステートメントをすべて実行します。これらをコピーして、SQL Editor に貼り付けることができます。

```
-- このスクリプトは、仮想データベースを現在のビュー
-- ファイルに設定し直します。
ALTER TABLE AM$amlog IN DICTIONARY USING '..¥Audit¥DATA¥amlog';
ALTER TABLE Billing IN DICTIONARY USING '..¥Audit¥DATA¥amlog';
ALTER TABLE Class IN DICTIONARY USING '..¥Audit¥DATA¥amlog';
ALTER TABLE Course IN DICTIONARY USING '..¥Audit¥DATA¥amlog';
ALTER TABLE Dept IN DICTIONARY USING '..¥Audit¥DATA¥amlog';
ALTER TABLE Enrolls IN DICTIONARY USING '..¥Audit¥DATA¥amlog';
ALTER TABLE Faculty IN DICTIONARY USING '..¥Audit¥DATA¥amlog';
ALTER TABLE Person IN DICTIONARY USING '..¥Audit¥DATA¥amlog';
ALTER TABLE Room IN DICTIONARY USING '..¥Audit¥DATA¥amlog';
ALTER TABLE Student IN DICTIONARY USING '..¥Audit¥DATA¥amlog';
ALTER TABLE Tuition IN DICTIONARY USING '..¥Audit¥DATA¥amlog';
```

メモ スクリプトは、仮想データベース内の AM$amlog テーブルに加え、監査対象のデータベースに含まれているデータ テーブルのすべてのコピーについても、テーブルの場所プロパティを変更します。このスクリプトの独自のバージョンを書く場合、仮想データベースの AM$Components、AM$OpList、AM$Products、AM$Tables テーブルについては、テーブルの場所プロパティを変更**しない**ようにしてください。

4 スクリプトを実行した後、これを再利用できるよう保持するために［**ファイル**］>［**別名保存**］を選択し、currentview.sql のような名前で保存することができます。

これで、「現在のビュー ファイルでクエリを実行する」で実行した差分クエリは、アーカイブ ファイルに対する結果ではなく現在のビューに対する結果を返すようになりました。

直接クエリ メソッドの要約

このセクションでは、監査レコードの直接クエリ メソッドについて要約します。

1 仮想データベースは、AZCC と関係なく、監査レコードの直接クエリを有効にすることができます。

2 特別なスクリプトにより、データベースを作成します。Query Data-Model Generator ユーティリティの qdmg を使用して、このスクリプトの記述を自動化します。

3 データベースを Audit for Zen のインストール ルート（たとえば、デフォルトの C:¥ProgramData¥Actian¥Zen¥Audit）と同じボリュームに作成します。

4 データベースで qdmg スクリプトを実行します。

5 これで、作成されたビューを使用して、現在のビュー ファイルから監査レコードを返すクエリを仮想データベースで実行できるようになりました。

6 アーカイブ ファイル内の監査レコードを照会できるようにするには、そのために、ALTER スクリプトを使用して仮想データベースを設定し直します。

7 再び現在のビュー ファイルを照会するように仮想データベースを元の状態に戻すには、2 番目の ALTER スクリプトを使用します。

8 現在のビュー ファイルと、直接クエリの実行対象としたいアーカイブ ファイルごとに、リセット スクリプトを作成して保存します。仮想データベースで、直接クエリを実行する前に必要なスクリプトを実行します。

9 アーカイブ ファイルのクエリが成功するには、ファイルが圧縮されていない必要があることを覚えておいてください。

Audit for Zen とクライアント側のキャッシュ

Zen データベースでは、クライアント側のキャッシュ エンジンがオンになっている場合、キャッシュ エンジンは 8 回連続で読み取りをした後、さらに読み取ることを見越してデータベース ページ全体を読み取ります。キャッシュ エンジンによって読み取られたデータベース ページ内のレコードは、サーバー上のモニターで監査されません。監査において、あらゆる読み取りがキャプチャされることを必要とする場合は、キャッシュ設定がオフになっていることを確認してください。ただし、エンジンのキャッシュを使わないと、データベースのパフォーマンスが低下することがあります。この動作は、8 回連続の読み取りというしきい値に達した場合にのみ発生します。7 回読み取った後に更新が発生した場合には、キャッシュは発生せず、7 回すべての読み取りがキャプチャされます。Zen Control Center で［**キャッシュ エンジンの使用**］設定を確認するには、［**ローカル クライアント**］を展開し、［MicroKernel **ルーター**］を右クリックして［**プロパティ**］を選択します。次に、［**パフォーマンス チューニング**］をクリックします。デフォルトで、この設定はオフです。

読み取り操作を監査しない場合は、クライアント側のキャッシュの使用を制限する必要はありません。