監査（Auditing）

監査（Auditing）

アカウントログインの試行などの重要なイベントを追跡するために、監査ポリシーを設定できます。常にローカルポリシーを設定します。

（注） ドメインの監査ポリシーは、常にローカルの監査ポリシーを上書きします。可能な場合には、2 つのポリシーセットを同一にしてください。

ローカルの監査ポリシーを設定するには、**[開始（Start）]**>**[プログラム（Programs）]**>**[管理ツール（Administrative Tools]）**>**[ローカル セキュリティ ポリシー（Local Security Policies）]** を選択します。

監査ポリシーの表示

手順

ステップ 1 **[開始（Start）]**>**[プログラム（Programs）]**>**[管理ツール（Administrative Tools）]**>**[ローカル セキュリティ ポリシー（Local Security Policies）]** を選択します。

[ローカルセキュリティ設定（Local Security Settings）] ウィンドウが開きます。

ステップ 2 左側のペインのツリーで、**[ローカルポリシー（Local Policies）]** を選択して展開します。

ステップ 3 [ローカルポリシー（Local Policies）] の下のツリーで、**[監査ポリシー（Audit Policy）]** を選択します。

さまざまな監査ポリシーが左側のペインに表示されます。

ステップ 4 ポリシー名をダブルクリックして、監査ポリシーを表示または変更します。

セキュリティログの表示

監査ポリシーを設定した後、セキュリティログを 1 週間に 1 回確認します。ログオンの失敗や異常なアカウントを使用したログオンの成功などの異常なアクティビティを探します。

セキュリティログを表示するには、次のアクセスを実行します。

手順

[開始（Start]） > **[プログラム（Programs）]** > **[管理ツール（Administrative Tools）]** > **[イベント ビューア（Event Viewer）]** を選択します。

リアルタイムアラート

Windows では、SNMP イベントトランスレータ機能が提供されています。この機能を使用すると、Windows イベントログのイベントをリアルタイムアラートに変換して、イベントを SNMP トラップに変換できます。evntwin.exe または evntcmd.exe を使用して SNMP トラップを設定します。

イベントをトラップに変換する設定の詳細については、**Evntcmd** に関する Microsoft TechNet の項目を参照してください。

SNMP トラップの宛先の設定については、『*Cisco Unified ICM/Contact Center Enterprise SNMP ガイド*』ガイドを参照してください。

SQL サーバ監査ポリシー

一般的な SQL サーバの監査ポリシーについては、https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-database-engine?view=sql-server-2017 にある Microsoft のマニュアルを参照してください。

SQL サーバ C2 セキュリティ監査

C2 セキュリティは、システムが分権的なリソース保護と監査機能によって認定される政府のセキュリティ評価です。

シスコでは、Unified ICM/Unified CCE 環境では、SQL サーバの C2 監査をサポートしません。

Active Directory の監査ポリシー

Active Directory アカウントの管理とログインを定期的に監査します。異常なアクティビティについて、ログの監視も行います。

次の表に、強化されたデフォルトの DC 監査ポリシーを示します。

表 *1 : Active Directory* の監査ポリシー設定

ポリシー	デフォルト設定	強化された設定	説明
アカウントログインイベントの監査	監査なし	成功と失敗	アカウントログインイベントは、ドメインユーザアカウントがドメインコントローラで認証されると生成されます。
アカウントの管理を監査する	未定義	成功	アカウント管理イベントは、セキュリティプリンシパル アカウントが作成、変更、または削除されると生成されます。
ディレクトリ サービス アクセスを監査する	監査なし	成功	ディレクトリ サービス アクセス イベントは、システムアクセス制御リスト（SLL）を含む Active Directory オブジェクトにアクセスすると生成されます。
ログインイベントを監査する	監査なし	成功と失敗	ログインイベントは、ドメインユーザがドメインコントローラにインタラクティブにログインするときに生成されます。ログインイベントは、ドメインコントローラへのネットワークログインを実行してログインスクリプトとポリシーを取得する際にも生成されます。
オブジェクトのアクセスを監査する	監査なし	（変更なし）	
ポリシー変更の監査	監査なし	成功	ポリシー変更イベントは、ユーザ権利割り当てポリシー、監査ポリシー、または信頼ポリシーへの変更に対して生成されます。

ポリシー	デフォルト設定	強化された設定	説明
特権の使用を監査する	監査なし	（変更なし）	
プロセストラッキングを監査する	監査なし	（変更なし）	
システムイベントを監査する	監査なし	成功	システムイベントは、ユーザがドメインコントローラを再起動またはシャットダウンするときに生成されます。システムイベントは、システムのセキュリティまたはセキュリティログに影響するイベントが発生した場合にも生成されます。

設定の監査

Unified CCE は、Config_Msg_Log テーブル内のすべてのシステム設定変更の履歴をキャプチャします。ただし、Config_Msg_Log テーブルにキャプチャされた情報は暗号化されています。テーブルをわかりやすい形式で表示するには、データベース管理ツールである dumpcfg ユーティリティを使用します。取得した情報は、監査の目的で使用できます。

ユーティリティを実行するには、コマンドプロンプトで次のコマンドを使用します。

dumpcfg *<database></@server>|[</bd begin date>]|[</bt begin time]>|[</ed enddate]>| [</ed endtime>]|[</nd number_of_days>]|[<low recovery key>]|[<high recovery key>]|*.

ここで、

1. データベース は、ロガーデータベースの大文字と小文字が区別される名前です。
2. *@server* は、AW またはロガーデータベースのホスト名です。
3. *<database></@server>|[</bd begin date>]|[</bt begin time]>|[</ed enddate]>| [</ed endtime>]|[</nd number_of_days>]|[<low recovery key>]|[<high recovery key>]|* は、情報が必要な時間範囲です。

   RecoveryKey は、ソフトウェアが仮想時間を追跡するために内部で使用する値です。

dumpcfg コマンドは 、次の出力の詳細を表示します。

- **LogOperation**：設定操作のタイプを示します。たとえば、追加および更新などです。
- **TableName**：設定操作が影響を受けたテーブルの名前を表します。
- **DateTime**：設定操作の日時を示します。

- **ConfigMessage**：設定操作のすべての設定メッセージが一覧表示されます。

たとえば、スキルグループを追加した場合、次のコマンドを実行します。

たとえば、スキルグループを追加した場合、次のコマンドを実行します：**dumpcfg ucce_sideA@uccergr100a /bd 09/27/2018**

出力されたものとして表示される詳細は次のとおりです。

LogOperation：**追加**。

TableNames：**skill_target and t_skill_group**。

DateTime：スキルグループが追加された正確なタイムスタンプ。

ConfigMessage：**周辺機器名**、**企業名**などの、影響を受け取けたフィールド名。