監査ログ

監査ログ

監査ログを使用すると、監査用の別のログ ファイルにシステムの設定変更が記録されます。

監査ロギング（標準）

監査ロギングが有効になっているが、詳細監査ロギングオプションが選択されていない場合、システムは標準の監査ロギング用に設定されます。

標準監査ロギングを使用すると、監査用の別のログファイルにシステムの設定変更が記録されます。Cisco Audit Event サービスは、サービス提供 GUI の [コントロールセンター-ネットワークサービス (Control Center-Network Services)] の下に表示され、ユーザによって行われた、またはユーザアクションの結果として、システムに対する設定変更をモニタしてログに記録します。

監査ログの設定を行うには、Serviceability GUI の [監査ログの設定（Audit Log Configuration）] ウィンドウにアクセスします。

標準監査ロギングの構成は次のとおりです。

- 監査ロギング フレームワーク：このフレームワークは、監査ログに監査イベントを書き込むためにアラーム ライブラリを使用する API で構成されます。GenericAlarmCatalog.xml として定義されたアラーム カタログがこれらのアラームに適用されます。システムコンポーネントごとに独自のロギングが提供されます。

  以下に、アラームを送信するために Unified Communications Manager のコンポーネントを使用することが API の例を示します。

```
User ID: CCMAdministratorClient IP Address: 172.19.240.207 Severity: 3
EventType: ServiceStatusUpdated ResourceAccessed: CCMService EventStatus:
Successful Description: CallManager Service status is stopped
```

- 監査イベントロギング：監査イベントとは、記録する必要があるあらゆるイベントを指します。次に、監査イベントの例を示します。

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService
EventStatus:Successful Description: Call Manager Service status is stopped
 App ID:Cisco Tomcat Cluster ID:StandAloneCluster Node ID:sa-cm1-3
```

ヒント　監査イベントのロギングは、デフォルトでは一元的に管理され、有効化されることに注意してください。Syslog Audit というアラームモニタによってログが書き込まれます。デフォルトでは、ログはローテーションするように設定されています。AuditLogAlarmMonitor が監査イベントを書き込むことができない場合、AuditLogAlarmMonitor はこのエラーを重大なエラーとして syslog ファイルに記録します。Alert Manager は、このエラーを、「シビラティ（重大度）が一致した」アラートの一部として報告します。イベントロギングが失敗した場合も実際の動作は継続されます。監査ログはすべて、Cisco Unified Real-Time Monitoring Tool の Trace and Log Central から収集、表示、および削除されます。

シスコユニファイドサービス標準イベントロギング

Cisco Unified Serviceability では次のイベントがログに記録されます。

- サービスのアクティブ化、非アクティブ化、起動、または停止。
- トレース設定およびアラーム設定の変更。
- SNMP 設定の変更。
- CDR 管理の変更（Cisco Unified Communications Manager のみ）。
- サービスアビリティ レポートのアーカイブのレポートの参照。このログは、レポート用ノードで表示されます。（Unified Communications Manager のみ）

Cisco Unified Real-Time Monitoring Tool の標準イベント ロギング

Cisco Unified Real-Time Monitoring Tool では、監査イベント アラームを含む次のイベントがログに記録されます。

- アラートの設定
- アラートの中断
- 電子メールの設定
- ノード アラート ステータスの設定
- アラートの追加
- アラートの追加アクション

- アラートのクリア
- アラートのイネーブル化
- アラートの削除アクション
- アラートの削除

Unified Communications Manager 標準イベント ロギング

Cisco CDR Analysis and Reporting（CAR）では、以下のイベントに関する監査ログが作成されます。

- ローダのスケジューリング
- 日次、週次、月次レポートのスケジューリング
- メール パラメータの設定
- ダイヤル プラン設定
- ゲートウェイの設定
- システム プリファレンスの設定
- 自動消去の設定
- 接続時間、時刻、および音声品質の評価エンジンの設定
- QoS の設定
- 事前生成レポートの自動生成/アラートの設定
- 通知限度の設定

Cisco Unified CM Administration の標準イベントロギング

次のイベントは、Cisco Unified Communications Manager Administration のさまざまなコンポーネントに対して記録されます。

- ユーザのログイン/ログアウト
- ユーザのロール メンバーシップの更新（ユーザの追加、ユーザの削除、またはユーザのロールの更新）
- ロールの更新（新しいロールの追加、削除、または更新）
- デバイスの更新（電話機およびゲートウェイ）
- サーバ設定の更新（アラームまたはトレースの設定、サービス パラメータ、エンタープライズ パラメータ、IP アドレス、ホスト名、イーサネット設定の変更、および Unified Communications Manager サーバの追加または削除）。

Cisco Unified Communications セルフ ケア ポータルの標準イベント ロギング

Cisco Unified Communications セルフ ケア ポータルに対するユーザ ロギング（ユーザ ログインとユーザ ログアウト）イベントが記録されます。

コマンドラインインターフェイスの標準イベントロギング

コマンドラインインターフェイスで実行されたすべてのコマンドがログに記録されます（Unified Communications Manager と Cisco Unity Connection の両方）。

Cisco Unity Connection Administration の標準イベント ロギング

Cisco Unity Connection Administration では次のイベントがログに記録されます。

- ユーザのログイン/ログアウト
- すべての設定変更（ユーザ、連絡先、コール管理オブジェクト、ネットワーク、システム設定、テレフォニーなど）
- タスク管理（タスクの有効化/無効化）
- 一括管理ツール（一括作成、一括削除）
- カスタム キーパッド マップ（マップの更新）

Cisco Personal Communications Assistant（Cisco PCA）の標準イベント ロギング

Cisco Personal Communications Assistant クライアントでは次のイベントがログに記録されます。

- ユーザのログイン/ログアウト
- Messaging Assistant で行われたすべての設定変更

Cisco Unity Connection Serviceability の標準イベント ロギング

Cisco Unity Connection Serviceability では次のイベントがログに記録されます。

- ユーザのログイン/ログアウト。
- すべての設定変更。
- サービスのアクティブ化、非アクティブ化、開始、または停止。

Representational State Transfer API を使用する Cisco Unity Connection クライアントのイベント ロギング

Representational State Transfer（REST）API を使用する Cisco Unity Connection クライアントでは次のイベントがログに記録されます。

- ユーザのログイン（ユーザの API 認証）。
- Cisco Unity Connection プロビジョニング インターフェイスを使用する API 呼び出し。

Cisco Unified IM and Presence Serviceability の標準イベント ロギング

Cisco Unified IM and Presence Serviceability では次のイベントがログに記録されます。

- サービスのアクティブ化、非アクティブ化、起動、または停止
- トレース設定およびアラーム設定の変更
- SNMP 設定の変更
- サービスアビリティ レポートのアーカイブ内のレポートの参照（このログは、レポート用ノードで表示されます）

Cisco Unified IM and Presence リアルタイムモニタリングツール標準イベントロギング

Cisco Unified IM and Presence Real-Time Monitoring Tool では、監査イベント アラームを含む次のイベントがログに記録されます。

- アラートの設定
- アラートの中断
- 電子メールの設定
- ノード アラート ステータスの設定
- アラートの追加
- アラートの追加アクション
- アラートのクリア
- アラートのイネーブル化
- アラートの削除アクション
- アラートの削除

Cisco IM and Presence Administration の標準イベント ロギング

以下のイベントは、Cisco Unified Communications Manager 管理のさまざまなコンポーネントに対して記録されます。

- 管理者のロギング（Administration、OS Administration、Disaster Recovery System、Reporting などの IM and Presence のインターフェイスへのログインおよびログアウト）
- ユーザのロール メンバーシップの更新（ユーザの追加、ユーザの削除、またはユーザのロールの更新）
- ロールの更新（新しいロールの追加、削除、または更新）
- デバイスの更新（電話機およびゲートウェイ）

- サーバ設定の更新（アラームまたはトレースの設定、サービスパラメータ、エンタープライズパラメータ、IPアドレス、ホスト名、イーサネット設定の変更、およびIM and Presenceサーバの追加または削除）

IM and Presence アプリケーションの標準イベントロギング

IM and Presenceアプリケーションのさまざまなコンポーネントでは、次のイベントがログに記録されます。

- IMクライアントへのエンドユーザのログイン（ユーザのログイン/ログアウト、およびログイン試行の失敗）
- IM チャット ルームへのユーザの入室および退室
- IM チャットルームの作成と破壊

コマンドラインインターフェイスの標準イベントロギング

コマンドライン インターフェイスで実行されたすべてのコマンドがログに記録されます。

監査ロギング（詳細）

詳細な監査ロギングは、標準(デフォルト)の監査ログに保存されていない追加の設定変更をログに記録するオプション機能です。標準監査ログに保存されるすべての情報に加えて、詳細監査ロギングには、変更された値も含め、追加、更新、または削除された設定項目も保存されます。詳細監査ロギングはデフォルトで無効になっていますが、[監査ログ設定（Audit Log Configuration）] ウィンドウで有効にすることができます。

監査ログのタイプ

システム監査ログ

システム監査ログでは、Linux OSユーザの作成、変更、削除、ログの改ざん、およびファイルまたはディレクトリの権限に対するあらゆる変更をトレースします。このタイプの監査ログは、収集されるデータが大量になるためにデフォルトでディセーブルになっています。この機能を有効にするには、CLIを使用して、手動でユーティリティのauditdを有効にする必要があります。システム監査ログ機能をイネーブルにすると、Real-Time Monitoring Toolの [Trace & Log Central] を使用して、選択したログの収集、表示、ダウンロード、削除を実行できます。システム監査ログは、`vos-audit`の形式で実行されます。

この機能をイネーブルにする方法については、『*Cisco Unified Communications Solutions* コマンドライン インターフェイス リファレンス ガイド』を参照してください。Real-Time Monitoring Toolから収集したログを操作する方法については、『*Cisco Unified Real-Time Monitoring Tool* アドミニストレーション ガイド』を参照してください。

アプリケーション監査ログ

アプリケーション監査ログは、ユーザが行った、またはユーザアクションの結果として行われたシステムへの設定変更をモニタし、記録します。

（注） アプリケーションの監査ログ（Linux auditd）は、CLIからのみイネーブルまたはディセーブルにすることができます。このタイプの監査ログの設定は、Real-Time Monitoring Tool による vos-audit.log の収集以外は変更できません。

データベース監査ログ

データベース監査ログは、ログインなど、Informix データベースへのアクセスに関連するすべてのアクティビティを追跡します。

監査ログ設定タスク フロー

監査ロギングを設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	監査ロギングのセットアップ （8 ページ）	[監査ログの設定 (Audit Log Configuration)] ウィンドウで監査ログの設定を行います。リモート監査ロギングを使用するかどうか、および詳細な監査ロギングオプションを使用するかどうかを設定できます。
ステップ 2	リモート監査ログの転送プロトコルの設定 （9 ページ）	オプション。リモート監査ロギングを設定した場合は、転送プロトコルを設定します。通常の動作モードのシステム デフォルトは UDP ですが、TCP または TLS を設定することもできます。
ステップ 3	アラート通知用の電子メール サーバの設定 （9 ページ）	オプション。RTMT で、電子メール アラート用の電子メール サーバをセットアップします。
ステップ 4	電子メール アラートの有効化 （10 ページ）	オプション。次の電子メールアラートのいずれかを設定します。 • リモート監査ロギングが TCP で設定されている場合は、**TCPRemoteSyslogDeliveryFailed** ア

	コマンドまたはアクション	目的
		ラート用の電子メール通知をセットアップします。 • TLS でリモート監査ロギングが設定されている場合は、**TLSRemoteSyslogDeliveryFailed**アラートの電子メール通知を設定します。
ステップ 5	プラットフォーム ログのリモート監査ロギングの設定 （11 ページ）	プラットフォーム監査ログおよびリモートサーバログのリモート監査ロギングを設定します。これらのタイプの監査ログでは、FileBeat クライアントと外部 logstash サーバを設定する必要があります。

監査ロギングのセットアップ

始める前に

リモート監査ロギングでは、事前に、リモート syslog サーバをセットアップし、間にあるゲートウェイへの接続も含め、各クラスタ ノードとリモート syslog サーバ間で IPSec を設定しておく必要があります。IPSec 設定については、『*Cisco IOS Security Configuration Guide*』を参照してください。

手順

ステップ 1 Cisco Unified Serviceability で、**[ツール（Tools）]** > **[監査ログ設定（Audit Log Configuration）]** を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン メニューから、クラスタ内のサーバを選択し、[実行（Go）] をクリックします。

ステップ 3 すべてのクラスタ ノードを記録するには、[すべてのノードに適用（Apply to All Nodes）] チェックボックスをオンにします。

ステップ 4 [サーバ名（Server Name）] フィールドに、リモート syslog サーバの IP アドレスまたは完全修飾ドメイン名を入力します。

ステップ 5 これはオプションです。変更された項目と変更された値も含め、設定更新を記録するには、[詳細監査ロギング（Detailed Audit Logging）] チェックボックスをオンにします。

ステップ 6 [監査ログ設定（Audit Log Configuration）] ウィンドウの残りのフィールドに値を入力します。フィールドとその説明を含むヘルプについては、オンライン ヘルプを参照してください。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

リモート監査ログの転送プロトコルの設定 （9 ページ）

リモート監査ログの転送プロトコルの設定

リモート監査ログ用の転送プロトコルを変更するには、次の手順を使用します。システム デフォルトは UDP ですが、 に設定し直すこともできます。 TCP または TLS。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 **utils remotesyslog show protocol** コマンドを実行して、どのプロトコルが設定されているかを確認します。

ステップ 3 このノード上でプロトコルを変更する必要がある場合は、次の手順を実行します。

- TCP を設定するには、**utils remotesyslog set protocol tcp** コマンドを実行します。
- UDP を設定するには、**utils remotesyslog set protocol udp** コマンドを実行します。
- TLS を設定するには、**utils remotesyslog set protocol tls** コマンドを実行します。

TLS 接続を設定するには、セキュリティ証明書を syslog サーバから Unified Communications Manager および IM and Presence サービス上の Tomcat 信頼ストアにアップロードする必要があります。

（注） コモン クライテリア モードでは、厳密なホスト名検証が使用されます。そのため、証明書と一致する完全修飾ドメイン名（FQDN）でサーバを設定する必要があります。

ステップ 4 プロトコルを変更した場合は、ノードを再起動します。

ステップ 5 すべての Unified Communications Manager および IM and Presence サービスのクラスタ ノードでこの手順を繰り返します。

次のタスク

アラート通知用の電子メール サーバの設定 （9 ページ）

アラート通知用の電子メール サーバの設定

アラート通知用の電子メール サーバをセットアップするには、次の手順を使用します。

手順

ステップ 1 Real-Time Monitoring Tool のシステム ウィンドウで、[アラート セントラル（Alert Central）] をクリックします。

ステップ 2 **[システム（System）] > [ツール（Tools）] > [アラート（Alert）] > [電子メール サーバの設定（Config Email Server）]** の順に選択します。

ステップ 3 [メール サーバ設定（Mail Server Configuration）] ポップアップで、メール サーバの詳細を入力します。

ステップ 4 **[OK]** をクリックします。

次のタスク

電子メール アラートの有効化 （10 ページ）

電子メール アラートの有効化

リモート監査ロギングを TCP または TLS で設定した場合は、次の手順を使用して、送信障害を通知する電子メール アラートを設定します。

手順

ステップ 1 Real-Time Monitoring Tool の [システム（System）] 領域で、[アラート セントラル（Alert Central）] をクリックします。

ステップ 2 **Alert Central** ウィンドウで、

- TCP でリモート監査ロギングを使用する場合は、**TCPRemoteSyslogDeliveryFailed** を選択します。
- TLS でリモート監査ロギングを使用する場合は、**TLSRemoteSyslogDeliveryFailed** を選択します。

ステップ 3 **[システム（System）] > [ツール（Tools）] > [アラート（Alert）] > [アラート アクションの設定（Config Alert Action）]** の順に選択します。

ステップ 4 [アラート アクション（Alert Action）] ポップアップで、[デフォルト（Default）] を選択して、[編集（Edit）] をクリックします。

ステップ 5 [アラート アクション（Alert Action）] ポップアップで、受信者を追加します。

ステップ 6 ポップアップ ウィンドウで、電子メール アラートを送信するアドレスを入力して、[OK] をクリックします。

ステップ 7 [アラート アクション（Alert Action）] ポップアップで、アドレスが [受信者（Recipients）] に表示されていることと、[有効（Enable）] チェックボックスがオンになっていることを確認します。

ステップ 8 **[OK]** をクリックします。

プラットフォーム ログのリモート監査ロギングの設定

プラットフォーム監査ログ、リモートサポートログ、および一括管理 csv ファイルのリモート監査ロギングサポートを追加するには、次のタスクを実行します。これらのタイプのログでは、FileBeat クライアントと logstash サーバが使用されます。

始める前に

外部 logstash サーバがセットアップされていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	Logstash サーバ情報の設定 （11 ページ）	IP アドレス、ポート、ファイル タイプなどの外部 logstash サーバ詳細で FileBeat クライアントを設定します。
ステップ 2	FileBeat クライアントの設定 （11 ページ）	リモート監査ロギング用の FileBeat クライアントを有効にします。

Logstash サーバ情報の設定

次の手順を使用して、IP アドレス、ポート番号、ダウンロード可能なファイル タイプなどの外部 Logstash サーバ情報で FileBeat クライアントを設定します。

始める前に

外部 Logstash サーバがセットアップされていることを確認します。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 **utils FileBeat configure** コマンドを実行します。

ステップ 3 画面上の指示に従って、Logstash サーバの詳細を設定します。

FileBeat クライアントの設定

プラットフォーム監査ログ、リモート サポート ログ および一括管理 CSV ファイルのアップロード用の FileBeat クライアントを有効または無効にするには、次の手順を使用します。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 **utils FileBeat status** コマンドを実行し、Filebeat クライアントが有効になっているかどうかを確認します。

ステップ 3 次のコマンドの 1 つを実行します。

- クライアントを有効にするには、**utils FileBeat enable** コマンドを実行します。
- クライアントを無効にするには、**utils FileBeat disable** コマンドを実行します。

（注） TCP はデフォルトの転送プロトコルです。

ステップ 4 これはオプションです。転送プロトコルとして TLS を使用するには、次の手順を実行します。

- 転送プロトコルとして TLS を有効にするには、**utils FileBeat tls enable** コマンドを実行します。
- 転送プロトコルとして TLS を無効にするには、**utils FileBeat tls disable** コマンドを実行します。

（注） TLS を使用するには、セキュリティ証明書を logstash サーバから Unified Communications Manager および IM and Presence サービス上の tomcat 信頼ストアにアップロードする必要があります。

ステップ 5 各ノードでこの手順を繰り返します。

これらのコマンドをすべてのノードで同時に実行しないでください。

監査ログの構成時の設定

はじめる前に

監査ロールを割り当てられたユーザだけが監査ログの設定を変更できることに注意してください。デフォルトでは、Unified Communications Manager の新規インストールおよびアップグレード後、CCMAdministrator が監査ロールを所有します。CCMAdministrator は、Cisco Unified Communications Manager Administration の [User Group Configuration] ウィンドウで標準監査ユーザ グループに監査権限を持つユーザを割り当てることができます。その後必要であれば、標準監査ユーザ グループから CCMAdministrator を削除できます。

IM and Presence サービスの場合、管理者は、新規インストールとアップグレード後に監査ロールを所有し、監査権限を持つユーザを標準監査ユーザグループに割り当てることができます。

Cisco Unity Connection の場合、インストール時に作成されたアプリケーション管理アカウントが Audit Administrator ロールに割り当てられます。このアカウントは、他の管理者ユーザをこのロールに割り当てることができます。このアカウントから Audit Administrator ロールを削除することもできます。

Standard Audit Log Configuration ロールには、監査ログを削除する権限と、Cisco Unified Real-Time Monitoring Tool、IM and Presence Real-Time Monitoring Tool、Trace Collection Tool、Real-Time Monitoring Tool（RTMT）アラート設定、Serviceability ユーザ インターフェイスのコントロール センター - ネットワーク サービス、RTMT プロファイルの保存、Serviceability ユーザ イン

ターフェイスの監査設定、監査トレースというリソースへの読み取り/更新権限が与えられます。

Standard Audit Log Configuration ロールには、監査ログを削除する権限と、Cisco Unified RTMT、Trace Collection Tool、RTMT アラート設定、Cisco Unified Serviceability のコントロール センター - ネットワーク サービス、RTMT プロファイルの保存、Cisco Unified Serviceability の監査設定、監査トレースというリソースへの読み取り/更新権限が与えられます。

Cisco Unity Connection の Audit Administrator ロールに割り当てられたユーザは、Cisco Unified RTMT で監査ログを表示、ダウンロード、および削除できます。

Cisco Unified Communications Manager のロール、ユーザ、およびユーザ グループの詳細については、*Cisco Unified Communications Manager* 管理ガイドを参照してください。

Cisco Unity Connection のロールとユーザの詳細については、『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』を参照してください。

IM and Presenceのロール、ユーザ、ユーザ グループの詳細は、*Unified Communications Manager* の *Configuration and Administration of IM and Presence Service* の設定および管理を参照してください。

次の表に、Cisco Unified Serviceability の [監査ログの設定（Audit Log Configuration）] ウィンドウで設定できる設定について説明します。

表 *1*：監査ログの構成時の設定

フィールド	説明
サーバの選択	
サーバ（Server）	監査ログを設定するサーバ（ノード）を選択し、[移動（Go）]をクリックします。
すべてのノードに適用（Apply to All Nodes）	クラスタのすべてのノードに監査ログ設定を適用する場合は、[すべてのノードに適用（Apply to All Nodes）] チェックボックスをオンにします。
アプリケーション監査ログの設定	

フィールド	説明
監査ログを有効にする（Enable Audit Log）	このチェックボックスをオンにすると、監査ログがアプリケーション監査ログに対して作成されます。 Unified Communications Managerの場合、アプリケーション監査ログは、Cisco Unified Communications Manager 管理、Cisco Unified RTMT、Cisco Unified Communications Manager CDR Analysis and Reporting および Cisco Unified Serviceabilityなどの Unified Communications Manager ユーザ インターフェイスの設定の更新をサポートします。 IM and Presence Service の場合、アプリケーション監査ログは Unified Communications Manager IM and Presence 管理、Cisco Unified IM and Presence Real-Time Monitoring Tool、Cisco Unified IM and Presence Serviceability などの IM and Presence ユーザ インターフェイスの設定更新をサポートします。 Cisco Unity Connection の場合、アプリケーション監査ログは Cisco Unity Connection Administration、Cisco Unity Connection Serviceability、Cisco Personal Communications Assistant、接続 REST API を使用するクライアントなどの Cisco Unity Connection ユーザ インターフェイスの設定更新をサポートします。 この設定は、デフォルトで有効と表示されます。 （注） ネットワークサービス監査イベントサービスが実行されている必要があります。
消去を有効にする（Enable Purging）	Log Partition Monitor（LPM）は、[消去を有効にする（Enable Purging）] オプションを確認して監査ログを消去する必要があるかどうかを判断します。このチェックボックスをオンにすると、共通パーティションのディスク使用率が上限を超えるたびに LPM によって RTMT のすべての監査ログ ファイルが消去されます。ただし、このチェックボックスをオフにして消去を無効にすることができます。 消去が無効の場合、監査ログの数は、ディスクがいっぱいになるまで増加し続けます。このアクションは、システムの中断を引き起こす可能性があります。[消去を有効にする（Enable Purging）] チェックボックスをオフにすると、消去の無効化のリスクを説明するメッセージが表示されます。このオプションは、アクティブ パーティションの監査ログに使用可能なことに注意してください。監査ログが非アクティブ パーティションにある場合、ディスク使用率が上限を上回ると消去されます。 監査ログにアクセスするには、RTMT の [Trace & Log Central][監査ログ（Audit Logs）] > を選択します。 （注） ネットワーク サービス Cisco Log Partition Monitoring Tool が動作している必要があります。

フィールド	説明
ログ ローテーションを有効にする（Enable Log Rotation）	システムは、このオプションを読み取り、監査ログファイルをローテーションする必要があるか、または新しいファイルの作成を続行するかを判断します。ファイルの最大数は 5000 を超えることはできません。[ログローテーションを有効にする（Enable Log Rotation）] チェックボックスをオンにすると、監査ログファイルの最大数に達すると最も古いファイルが上書きされます。 **ヒント** ログ ローテーションを無効（オフ）にすると、監査ログは [最大ファイル数（Maximum No. of Files）] 設定を無視します。
詳細監査ロギング（Detailed Audit Logging）	このチェックボックスをオンにすると、システムは詳細監査ログに対して有効にされます。詳細な監査ログは、通常の監査ログと同じ項目を提供しますが、設定の変更も含みます。たとえば、監査ログには、変更された値を含む、追加、更新、および削除された項目が含まれます。
サーバ名	Syslog メッセージ受信のために使用する、リモート Syslog サーバの名前または IP アドレスを入力します。サーバ名が指定されていない場合、Cisco Unified IM and Presence Serviceability は Syslog メッセージを送信しません。ノードは他のサーバからの Syslog メッセージを受け付けないため、Unified Communications Manager ノードを通知先として指定しないでください。 これは、IM and Presence Service にのみ適用されます。
リモート Syslog 監査イベントレベル（Remote Syslog Audit Event Level）	リモート Syslog サーバの、対象となる Syslog メッセージのシビラティ（重大度）を選択します。選択したシビラティ（重大度）以上のすべての Syslog メッセージが、リモート Syslog に送信されます。 これは、IM and Presence Service にのみ適用されます。
最大ファイル数（Maximum No. of Files）	ログに含めるファイルの最大数を入力します。デフォルト設定は 250 です。最大数は 5000 です。
最大ファイル サイズ（Maximum File Size）	監査ログの最大ファイル サイズを入力します。ファイル サイズの値は1 MBー10 MBの範囲内にする必要があります。1 ～ 10 の間の数を指定します。

フィールド	説明
ログローテーションの上書きに近づいた場合の警告しきい値 (%)	監査ログが上書きされるレベルに達すると、警告が送信されます。システムがアラートを送信するしきい値を設定するには、このフィールドを使用します。 たとえば、250ファイルのデフォルト設定を 2 MB に、警告しきい値として80% を使用すると、システムは200ファイル (80%) でアラームを送信します。監査ログの合計が累積されました。監査履歴を保持する場合は、RTMT を使用してログを取得してから、システムがそれらを上書きする必要があります。RTMT には、収集後にファイルを削除するオプションが用意されています。 1 ～ 99% の範囲で値を入力します。デフォルトは 80% です。このフィールドを設定する場合は、[**ログローテーションの有効化 (Enable Log Rotation**)] オプションもオンにする必要があります。 （注） 監査ログに割り当てられる合計ディスク領域は、最大数です。ファイルの最大サイズを乗算します。ディスク上の監査ログのサイズが、割り当てられた合計ディスク領域のこの割合を超えた場合、システムは Alert Central でアラームを発生させます。
データベース監査ログ フィルタ設定	
監査ログを有効にする（Enable Audit Log）	このチェック ボックスをオンにすると、監査ログが Unified Communications Manager および Cisco Unity Connection データベースに作成されます。[デバッグ監査レベル（Debug Audit Level）] の設定とともにこの設定を使用します。これにより、データベースの特定の側面に対してログを作成できます。

フィールド	説明
デバッグ監査レベル（Debug Audit Level）	この設定では、ログで監査するデータベースの側面を選択できます。ドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。各監査ログ フィルタ レベルは累積的であることに注意してください。 • [スキーマ（Schema）]：監査ログ データベースの設定の変更（たとえば、データベース テーブルのカラムや行）を追跡します。 • **管理タスク**：Unified Communications Managerシステムに対するすべての管理上の変更（たとえば、システム保全のためのあらゆる変更など）およびすべての**スキーマ**を追跡します。 **ヒント** ほとんどの管理者は[管理タスク（Administrative Tasks）]設定を無効にしたままにします。監査が必要なユーザに対しては、[データベースの更新（Database Updates）]レベルを使用します。 • [データベースの更新（Database Updates）]：データベースのすべての変更、および[スキーマ（Schema）]のすべての変更と[管理タスク（Administrative Tasks）]のすべての変更を追跡します。 • **データベースの読み取り**：システムへのすべての読み取りと、すべてのスキーマ変更、管理タスク変更、データベース更新のすべての変更を追跡します。 **ヒント** Unified Communications Manager または Cisco Unity Connection システムを簡単に確認する場合にのみ、データベースの読み取りレベルを選択します。このレベルでは、大量のシステム リソースを消費するため、短時間だけ使用してください。
監査ログローテーションを有効にする（Enable Audit Log Rotation）	システムはこのオプションを読み取り、データベースの監査ログファイルをローテーションする必要があるか、または新しいファイルの作成を続行するかどうかを判断します。[監査ログローテーションを有効にする（Enable Audit Log Rotation）]オプションのチェックボックスをオンにすると、監査ログファイルが最大数に達すると最も古いファイルが上書きされます。 この設定のチェックボックスがオフの場合、監査ログでは[最大ファイル数（Maximum No. of Files）]設定は無視されます。
最大ファイル数（Maximum No. of Files）	ログに含めるファイルの最大数を入力します。[最大ファイル数（Maximum No. of Files）]設定に入力した値が、[ログローテーション時に削除されるファイル数（No. of Files Deleted on Log Rotation）]設定に入力した値を上回っていることを確認します。 4（最小）～40（最大）の値を入力できます。

フィールド	説明
ログローテーション時に削除されるファイル数（No. of Files Deleted on Log Rotation）	データベース監査ログのローテーションが発生したときにシステムが削除できるファイルの最大数を入力します。 このフィールドに入力できる最小値は 1 です。最大値は [最大ファイル数（Max No. of Files）] 設定に入力した値よりも 2 低い数値です。たとえば、[最大ファイル数（Max No. of Files）] フィールドに 40 を入力した場合、[ログ ローテーション時に削除されるファイル数（No. of Files Deleted on Log Rotation）] フィールドに入力できる最大数は 38 です。
デフォルトに設定（Set to Default）	[デフォルトに設定（Set to Default）] ボタンは、デフォルト値を指定します。詳細なトラブルシューティングのために別のレベルに設定する必要がある場合を除き、監査ログをデフォルトモードに設定することを推奨します。[**デフォルトに設定 (Set To Default)**] オプションは、ログファイルによって使用されるディスク領域を最小化します。

⚠

注意 有効にすると、データベースロギングは短時間で大量のデータを生成することがあります。特に、デバッグ監査レベルが**データベースの更新**または**データベースの読み取り**に設定されている場合です。これにより、使用量が多いときにパフォーマンスが大幅に低下する可能性があります。一般に、データベースロギングを無効のままにしておくことをお勧めします。データベースの変更を追跡するためにロギングを有効にする必要がある場合は、**データベースの更新**レベルを使用して短時間だけ実行することをお勧めします。同様に、管理ロギングはWebユーザインターフェイスの全体的なパフォーマンスに影響します。特に、データベースエントリをポーリングする場合(たとえば、データベースから250デバイスをプルする場合)に影響します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。