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）

監査ロギングは有効になっているが、詳細監査ロギング オプションは選択されていない場合は、システムが標準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。 Serviceability 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）] の下に表示される Cisco Audit Event Service により、ユーザーが行った、またはユーザーの操作によって発生したシステムへの設定変更がモニタされ、ログに記録されます。

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。 各種システム コンポーネントで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 と呼ばれるアラーム 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され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、SeverityMatchFound アラートの一部としてこのエラーを報告します。 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。

Cisco Unified Serviceability の標準イベント 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
- アラートの一時停止
- 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、次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 の管理 のさまざまなコンポーネントに対して記録されます。

- ユーザーのログイン/ログアウト
- ユーザーのロールメンバーシップの更新（ユーザーの追加、ユーザーの削除、またはユーザーのロールの更新）
- 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 サーバーの追加または削除）。

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。

- ユーザーのログイン/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。

- ユーザーのログイン/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。

- ユーザーのログイン/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。

- ユーザーのログイン（ユーザーの 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 Real-Time Monitoring Tool の標準イベント 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
- アラートの一時停止
- 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）
- ユーザーのロールメンバーシップの更新（ユーザーの追加、ユーザーの削除、またはユーザーのロールの更新）
- 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）

- サーバー設定の更新（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 サーバーの追加または削除）

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ーのログイン（ユーザーのログイン/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ーの入室および退室
- IM チャット ルームの作成と破棄

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）

詳細監査ロギングは、標準（デフォルト）監査ログに保存されない追加の設定変更を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。

Audit Log Types

システム監査ログ

システム監査ログでは、Linux OS ユーザーの作成、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 utils auditd を有効にします。 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.log` という形式になります。

この機能をイネーブルにする方法については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』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 Administration Guide*』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、ユーザーによる、またはユーザー操作の結果発生し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）	[監査ログ設定（Audit Log Configuration）] ウィンドウで監査ログ設定をセットアップします。 リモート監査ロギングを使用するかどうかと、[詳細監査ロギング（Detailed Audit Logging）] オプションが必要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）	これはオプションです。 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ーの設定 （11 ページ）	これはオプションです。 RTMT で、電子メールアラート用の電子メールサーバー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 （11 ページ）	これはオプションです。 次の電子メール アラートのいずれかをセットアップします。

	コマンドまたはアクション	目的
		• リモート監査ロギングが TCP で設定されている場合は、**TCPRemoteSyslogDeliveryFailed** アラート用の電子メール通知をセットアップします。 • リモート監査ロギングが TLS で設定されている場合は、**TLSRemoteSyslogDeliveryFailed** アラート用の電子メール通知をセットアップします。
ステップ 5	プラットフォーム ログ用のリモート監査ロギングの設定 （12 ページ）	プラットフォーム監査ログとリモート サーバ ログ用のリモート監査ロギングをセットアップします。 この種の監査ログでは、FileBeat クライアントと外部 logstash サーバー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 サーバーをセットアップし、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 サーバー間で 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ーを選択し、**[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 **[サーバー名（Server Name）]** フィールドに、リモート syslog サーバーの 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 に設定し直すこともできます。

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 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。

（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）でサーバー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 と IM and Presence Service 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ーの設定 （11 ページ）

Syslog サーバーとの TLS 接続を確立する

この手順を使用して、Unified Communications Manager と Syslog サーバーの間に自己署名または CA 署名の証明書を使用して安全な TLS 接続を設定します。 以下の認証モードがサポートされています。

- 単方向 x.509 認証 - Syslog サーバーのみが Unified CM に対して認証します。
- 双方向 x.509 認証 - Unified CM と Syslog サーバーの両方が相互に認証します。

手順

ステップ 1 自己署名証明書の場合：

a) 単方向認証の場合、自己署名証明書を使用して TLS 接続を確立するには、syslog サーバーからのセキュリティ証明書が Unified Communications Manager パブリッシャノードの tomcat トラストストアにアップロードされている必要があります。

b) 双方向 x.509 認証の場合：

1. 自己署名証明書を使用して TLS 接続を確立するには、syslog サーバーからのセキュリティ証明書が Unified Communications Manager パブリッシャノードの tomcat トラストストアにアップロードされている必要があります。
2. Cisco Unified OS Administration から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** に移動します。そして、Unified Communications Manager および IM and Presence Service から Tomcat 証明書をダウンロードします。
3. Tomcat 証明書を Syslog サーバーの証明書ディレクトリにアップロードします。

   （注） Tomcat 証明書が再生成された場合、syslog サーバーに再アップロードする必要があります。
4. 必要に応じて Syslog サーバーを再起動します。

ステップ 2 CA 署名証明書の場合：

a) 単方向認証の場合、認証局（CA）証明書を Unified Communications Manager パブリッシャノード上の tomcat トラストストアにアップロードします。

b) 双方向 x.509 認証の場合：

1. TLS 接続を確立するには、Unified Communications Manager パブリッシャノードの tomcat トラストストアに認証局（CA）の証明書をアップロードする必要があります。
2. Cisco Unified OS Administration から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** に移動します。そして、Unified Communications Manager および IM and Presence Service から Tomcat 証明書をダウンロードします。
3. この証明書が同じ CA によって署名されていることを確認してください。
4. CA 署名付き Tomcat 証明書を Unified Communications Manager パブリッシャノードの tomcat ストアにアップロードします。
5. CA 証明書を Syslog サーバーの証明書ディレクトリにアップロードします。
6. 必要に応じて Syslog サーバーを再起動します。

（注） TLS およびそれらのサポートされている形式（PEM、DER など）に関連する設定の詳細については、Syslog サーバーのドキュメントを参照してください。

アラート通知用の電子メールサーバーの設定

アラート通知用の電子メールサーバー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）]** > **[電子メールサーバーの設定（Config Email Server）]** の順に選択します。

ステップ 3 **[メールサーバー設定（Mail Server Configuration）]** ポップアップで、メールサーバー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 （11 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 **[アラートセントラル（Alert Central）]** ウィンドウで、します

- 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 ログ用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 ファイルに対する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。 この種のログでは、FileBeat クライアントと logstash サーバーが使用されます。

始める前に

外部 logstash サーバー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 （12 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 （13 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 サーバー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 サーバー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 と IM and Presence Service 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

事前準備

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 の管理 の [User Group Configuration] ウィンドウで標準監査ユーザーグループに監査権限を持つユーザー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 Serviceの場合、新規インストールまたはアップグレードの後で管理者に監査ロールが与えられ、監査権限を持つ任意のユーザーを標準監査ユーザー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、他の管理者ユーザー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ーは、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 のロールとユーザーの詳細については、『*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
サーバーの選択	
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 Cisco 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 ユーザー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 ユーザー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 Audit Event Service が動作し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。 詳細監査ログは、標準監査ログと同じ項目を提供しますが、設定の変更も含まれています。 たとえば、監査ログには、変更された値も含め、追加、更新、または削除された項目が保存されます。
サーバ名（Server Name）	Syslog メッセージ受信のために使用する、リモート Syslog サーバーの名前または 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 サーバーの、対象となる Syslog メッセージの重大度を選択します。 選択した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〜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 オーバーライドに到達する際の警告しきい値（%）（Warning Threshold for Approaching Log Rotation Overwrite (%)）	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。警告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、2 MB のファイルが 250 個あり、警告しきい値を 80% にデフォルト設定とすると、監査ログが 200 個（80%）収集されると、警告が送信されます。監査履歴を保持する場合は、システムがログを上書きする前に、RTMT を使用してログを取得します。 RTMT には、ファイルの収集後にそのファイルを削除するオプションがあります。 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 ローテーションを有効にする（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たディスク容量合計は、最大ファイル数を最大ファイル サイズで乗算したものです。 ディスク上の監査ログのサイズが割り当てられたディスク容量合計のこの割合を超える場合は、Alert Central に警告が表示されます。
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ーに対しては、[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。監査ログは、詳細なトラブルシューティング用の別のレベルに設定する必要がなければ、デフォルト モードに設定することをお勧めします。 [デフォルトに設定（Set to Default）]オプションは、ログ ファイルに使用されるディスク容量を最小限に抑えます。

注意 有効になっている場合、特にデバッグ監査レベルが [データベースの更新（Database Updates）] または [データベースの読み取り（Database Reads）]に設定されていると、データベース ロギングが短時間で大量のデータを生成する可能性があります。 これにより、多用期間中に、パフォーマンスに重大な影響が発生する可能性があります。 通常、データベース ロギングは無効のままにすることを推奨します。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には、[データベースの更新（Database Updates）]レベルを使用して短時間のみ有効にすることを推奨します。 同様に、特にデータベース エントリをポーリングする場合（データベースから 250 台のデバイスを引き出す場合など）、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を与えます。

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。