Cisco Unified Communications Manager リリース 11.0(1) での IM and Presence サービスのインスタント メッセージ コンプライアンス

初版：2015 年 06 月 08 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章

IM Compliance の計画

IM Compliance について

多くの業界では、インスタントメッセージが、他のビジネス レコードと同じ適合認定のガイドラインに従うことが求められています。 これらの規制を順守するには、ご使用のシステムがすべてのビジネス レコードを記録してアーカイブする必要があり、アーカイブされたレコードが取得可能になっている必要があります。

Cisco Unified Communications Manager IM and Presence サービスは、単一のクラスタ、クラスタ間、またはフェデレーテッド ネットワーク設定内の以下の IM アクティビティに対してデータを収集することで、インスタントメッセージング（IM）コンプライアンスに対するサポートを提供します。

- ポイントツーポイント メッセージ
- グループ チャット： これには、Ad-hoc または一時チャット メッセージと、常設チャット メッセージがあります。

IM Compliance のコンポーネント

IM Compliance には次のコンポーネントがあります。

- IM and Presence サービス リリース 10.0.（1）。 IM and Presence サービスは、外部データベースへのメッセージのログに Message Archiver コンポーネントを使用します。
- 外部データベース：サポートされる外部データベースの詳細は、『*Database Setup Guide for IM and Presence Service*』を参照してください。

- IM クライアント：サポートされるクライアントには、Cisco Jabber などの Cisco クライアント、サードパーティ製 XMPP クライアント、およびフェデレーテッド ネットワークで使用されるその他のサードパーティ製クライアントがあります。

（注） Message Archiver は、基本的な IM ロギング ソリューションを提供します。 ポリシーに基づいたロギングなどの、きめ細かなロギング ソリューションを必要とする場合は、サードパーティ製のコンプライアンス ソリューションを使用します。詳しくは付録を参照してください。

関連トピック

Cisco Unified Communications Manager リリース 9.0(1) での IM and Presence サービスのデータベース設定

サードパーティ製コンプライアンス サーバとの統合, （15 ページ）

IM Compliance 用サンプル トポロジおよびメッセージ フロー

（注） ここに示す外部データベース要件は、ご使用のサーバの容量により異なります。

IM Compliance は、コンプライアンス関連のすべてのデータを外部データベースに記録します。すべての IM トラフィックは IM and Presence サービス サーバを通過し（Message Archiver コンポーネントを経由）、同時に外部データベースに記録されます。 各 IM ログには送信者および受信者情報、タイムスタンプ、メッセージ本文が含まれます。

Ad-hoc グループ チャット メッセージは、デフォルトで IM and Presence サービス は同じメッセージの複数のコピーを受信者ごとに 1 通ずつ外部データベースにログ記録します。 これにより、Ad-hoc グループ チャットでメッセージを受信したユーザが識別されます。

配置した XMPP クライアントに応じて、次の動作にも注意が必要です。

- IM and Presence サービスは、受信メッセージを外部データベースに 2 回ログ記録する場合があります。 これは、一部の XMPP クライアントが、カンバセーション内の他のパーティの完全 JID または完全アドレスを「学習する」機能をサポートしていないために発生します。 そのため、XMPP クライアントはメッセージをユーザのすべてのアクティブ クライアント（ユーザが現在ログインしているすべてのクライアント）に転送し、続いて IM and Presence サービスは、転送されたすべてのメッセージを外部データベースに記録します。
- IM and Presence サービスは、チャット内の最初のメッセージを外部データベースに 2 回ログ記録する場合があります。 これは、XMPP クライアントがカンバセーション内の他のパーティの完全 JID または完全アドレスを学習するまで発生します。

IM and Presence サービスが外部データベースに接続できなくなった場合でも、ユーザへの IM の送信を続行し、ユーザは引き続き（ad-hoc）チャット ルームを作成できます。 ただし、外部データベースに接続していないと、IM and Presence サービスはこれらの IM をログに記録しません。 こ

の場合にグループ チャット サポートを維持するには、永続的チャットを異なるデータベース サーバに割り当てる必要があります。 IM and Presence サービスは、外部データベースへの接続が失われた場合にアラームを生成します。

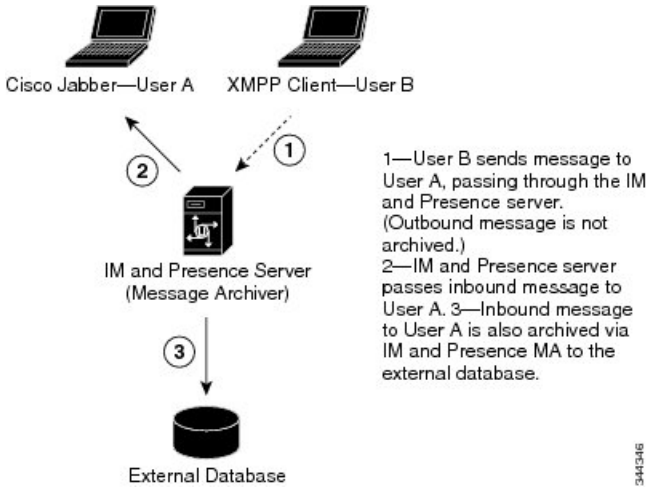
単一クラスタ コンフィギュレーション

IM Compliance を単一クラスタで使用する場合は、クラスタ内のユーザに送信されたすべての受信メッセージのログを記録する外部データベースを、クラスタごとに 1 つ導入することを強く推奨します。

（注）
- IM Compliance では、クラスタごとに 1 つの外部データベースを導入することを強く推奨します。 ただし、ご使用の要件によっては、クラスタごとに複数の外部データベースを設定したり、クラスタ間で 1 つのデータベースを共有することも可能です。
- グループ チャット機能を導入するには、クラスタ内のノードごとに1つの外部データベースが必要です。『*Database Setup for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

以下の画像ではこれらのコンポーネントとメッセージフローが強調されています。デフォルトでは、IM Complianceは、受信メッセージを外部データベースに記録しますが、発信メッセージも記録するように設定できます。

図 *1*：単一クラスタ用 *IM Compliance*

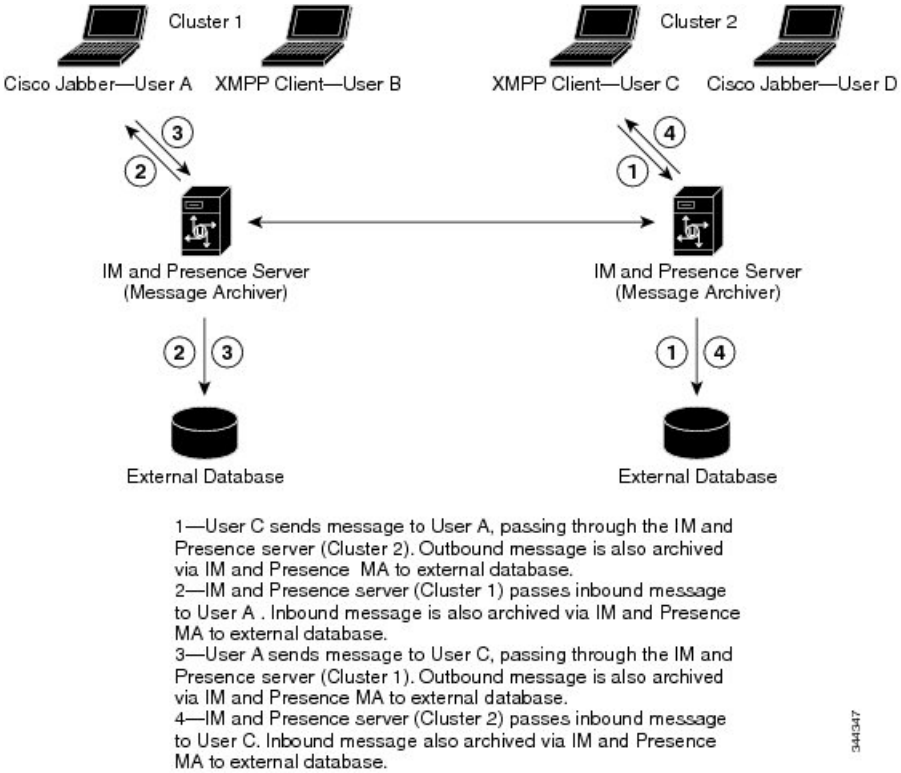


クラスタ間または連動ネットワーク構成

IM Compliance をクラスタ間またはフェデレーテッド ネットワーク構成で使用する場合は、クラスタごとに 1 つの外部データベースを設定する必要があります。 さらに、受信メッセージと発信メッセージの両方を記録するように、IM and Presence サービス ノードを設定する必要があります。 この設定を行わないと、各データベースにはカンバセーションの片側だけが保存されます。

以下の図はこれらのコンポーネントとメッセージ フローに焦点を当てています。

図 *2*：複数のクラスタの *IM Compliance*



必要な設定タスク

このガイドを使用して IM Compliance を設定する前に、次のタスクを実行したことを確認してください。

- 『*Installing Cisco Unified Communications Manager*』での説明に従って、IM and Presence サービス ノードをインストールします。
- 『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』での説明に従って、IM and Presence サービス ノードを設定します。
- 外部データベースを、『*Database Setup for IM and Presence Service on Cisco Unified Communications Manager*』で説明されているとおりに設定します。

PostgreSQL 10.0.1 のサポート

外部データベースとして PostgreSQL バージョン 10.0.1 を配置するには、postgresql.conf ファイルに以下の値をセットします。

- `escape_string_warning = off`

- `standard_conforming_strings = off`

これらのパラメータを設定したら、PostgreSQL を再起動する必要があります。 postgresql.conf ファイルを設定して PostgreSQL を再起動する方法の詳細については、『*Database Setup for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

Oracle のサポート

- XMPP 仕様に従って、IM and Presence サービス ノードでは UTF8 の文字符号を使用します。これにより、ノードは動作時に多数の言語を同時に使用することができ、クライアントインターフェイスで言語の特殊別文字を正しく表示できるようになります。 ノードで Oracle を使用する場合は、UTF8 に対応するようにノードを設定する必要があります。
- **NLS_LENGTH_SEMANTIC** パラメータの値は、**BYTE** に設定する必要があります。
- Oracle データベースのテーブルスペースが取得できるかを判断するには、sysdba として次のクエリを実行します。

  SELECT DEFAULT_TABLESPACE FROM DBA_USERS WHERE USERNAME = 'UPPER_CASE_USERNAME';

第 2 章

IM Compliance の設定

IM Compliance の設定

この設定はクラスタ内のパブリッシャ ノードで実行することを推奨します。

はじめる前に

- サポートされる外部データベースを1つ以上インストールして設定してください。『*Database Setup for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。
- IM and Presence サービス上で外部データベースを設定します。 [Cisco Unified CM IM and Presence Administration]>[メッセージ（Messaging）]>[外部データベース（External Databases）]を選択します。
- Cisco XCP ルータ サービスのトレース レベルが [info] 以上に設定されていることを確認します。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration]>[メッセージ（Messaging）]>[コンプライアンス（Compliance）]>[コンプライアンス設定（Compliance Settings）]を選択します。

ステップ 2 コンプライアンス サーバの選択項目から、[Message Archiver] を選択します。

ステップ 3 （任意）[発信元メッセージ ロギングを有効化（Enable Outbound Message Logging）]チェックボックスをチェックします。
このオプションを選択すると、IM のパフォーマンスが低下する場合があります。 すべての受信メッセージはすでにログに記録されているため、クラスタ間ネットワークまたは連動ネットワークで IM コンプライアンスを使用している場合を除き、この設定を有効にしないでください。

ステップ 4 個々のノードについて、外部データベース オプションからデータベースを割り当てます。
クラスタに1つの外部データベースを使用している場合は、すべてのノードを同じ外部データベースに割り当てます。 複数の外部データベースを使用している場合は、そのデータベースの容量の要件に基づき、データベースにノードを割り当てます。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 （まだ開始されていない場合は）Cisco Message Archiver サービスを開始します。

ステップ 7 Cisco XCP Router サービスを再起動します。
トラブルシューティングのヒント

a) Message Archiver の設定にさらに変更を加える場合、Cisco XCP ルータ サービスを再起動します。

b) （すべてのリリース）IM コンプライアンス展開オプション間で切り替える（たとえば、サードパーティ製コンプライアンス サーバ オプションから Message Archiver オプションへ切り替える）場合、Cisco XCP Route サービスを再起動する必要があります。

次の作業

Cisco XCP Message Archiver サービスの開始, （8 ページ）

関連トピック

IM Compliance のサポートのためにトレース レベルを Info に設定, （12 ページ）
Cisco XCP ルータ サービスの再起動, （11 ページ）
Cisco XCP Message Archiver サービスの再起動, （12 ページ）
IM Compliance 用サンプル トポロジおよびメッセージ フロー, （2 ページ）

Cisco XCP Message Archiver サービスの開始

IM and Presence サービスでコンプライアンス機能が正しく動作するには、Cisco XCP Message Archiver サービスが実行されている必要があります。

（注） コンプライアンス機能用のノードに外部データベースを割り当てていない場合は、IM and Presence サービスで Cisco XCP Message Archiver サービスの開始が許可されません。

手順

ステップ 1 [Cisco Unified IM and Presence Serviceability] > [ツール（Tools）] > [サービスの開始（Service Activation）] を選択します。

ステップ 2 [サーバ（Server）] リスト ボックスからサーバを選択します。

ステップ 3 [移動（Go）] をクリックします。

ステップ 4 [IM and Presence サービス（IM and Presence Services）] セクションで、[Cisco XCP Message Archiver] サービスの横にあるオプション ボタンをクリックします。

ステップ 5 [保存（Save）] をクリックします。
トラブルシューティングのヒント

Cisco UP XCP Message Archiver サービスが開始できなかった場合に、システム トラブルシュータ（[Cisco Unified CM IM and Presence Administration] > [診断（Diagnostics）] > [システム トラブルシュータ（System Troubleshooter）]）に外部データベース接続のステータスが問題なしと表示されている場合は、ノードからその外部データベースの割り当てを解除して、再度割り当ててください。

関連トピック

IM Compliance の設定, （7 ページ）

第 3 章

IM Compliance Serviceability とトラブルシューティング

Cisco XCP ルータ サービスの再起動

手順

ステップ 1 [Cisco Unified IM and Presence Serviceability] > [ツール（Tools）] > [コントロール センター - ネットワーク サービス（Control Center - Network Services）] を選択します。

ステップ 2 [サーバ（Server）] リスト ボックスからサーバを選択します。

ステップ 3 [移動（Go）] をクリックします。

ステップ 4 [IM and Presence サービス（IM and Presence Services）] セクションの [Cisco XCP ルータ（Cisco XCP Router）] ラジオボタンをクリックします。

ステップ 5 [再起動（Restart）] をクリックします。

ステップ 6 リスタートに時間がかかることを示すメッセージが表示されたら、[OK] をクリックします。

Cisco XCP Message Archiver サービスの再起動

手順

ステップ 1 [Cisco Unified IM and Presence Serviceability] > [ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）] を選択します。

ステップ 2 [サーバ（Server）] リスト ボックスからサーバを選択します。

ステップ 3 [移動（Go）] をクリックします。

ステップ 4 [IM and Presence サービス（IM and Presence Services）] セクションの [Cisco XCP Message Archiver] ラジオボタンをクリックします。

ステップ 5 [再起動（Restart）] をクリックします。

IM Compliance のサポートのためにトレース レベルを Info に設定

Message Archiver コンポーネントでは Cisco XCP ルータ サービスのロギング機能が使用されますが、この機能の使用にあたってはトレース レベルが [情報（Info）] 以上に設定されている必要があります。

（注） IM and Presence サービスは、Cisco XCP ルータ のトレース レベルをデフォルトで [情報（Info）] に設定します。 トレース レベルを [情報（Info）] よりも低いレベルに変更すると、コンプライアンス機能が IM and Presence サービスで正しく機能しなくなります。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] にサイン インします

ステップ 2 [IM and Presence サービス（IM and Presence Service）] メイン ウィンドウの右上隅のメニューから [ナビゲーション（Navigation）] > [Cisco Unified IM and Presence Serviceability] を選択します。

ステップ 3 [トレース（Trace）] > [設定（Configuration）] を選択します。

ステップ 4 [サーバ（Server）] リストボックスから、トレースの設定対象であるサービスを実行しているサーバを選択して [移動（Go）] をクリックします。

ステップ 5 [サービス グループ（Service Group）] から IM and Presence サービスを選択し、[移動（Go）] をクリックします。

ステップ 6 Cisco XCP ルータ サービスをサービス リスト ボックスから選択して、[移動（Go）] をクリックします。

ステップ 7 [トレース オン（Trace On）] チェックボックスをオンにします。

ステップ 8 [トレース フィルタの設定（Trace Filter Settings）] で [デバッグ トレース レベル（Debug Trace Level）] として [情報（Info）] を選択します。

IM Compliance のアラームの設定

IM and Presence サービスと外部データベースとの接続が失われても、ユーザ間でのインスタントメッセージの送信は引き続き可能です。 ただし、これらのメッセージはアーカイブされず、どの適合認定のガイドラインも満たされなくなります。 この接続が失われたときに通知を受けるためには、この状態に関連するアラームが正しく設定されていることを確認する必要があります。

手順

ステップ 1 **Cisco Unified CM IM and Presence Administration** にサインインします。

ステップ 2 [IM and Presence サービス（IM and Presence Service）] メイン ウィンドウの右上隅のメニューから [ナビゲーション（Navigation）] > [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] を選択します。

ステップ 3 [アラーム（Alarm）] > [設定（Configuration）] を選択します。

ステップ 4 [サーバ（Serve）] ドロップダウン リスト ボックスから、アラームを設定するサーバを選択します。

ステップ 5 [移動（Go）] をクリックします。

ステップ 6 [サービス グループ（Service Group）] ドロップダウン リストから、[IM and Presence サービス（IM and Presence Services）] を選択します。

ステップ 7 [移動（Go）] をクリックします。

ステップ 8 [サービス（Service）] ドロップダウン リストから、[Cisco XCP Message Archiver] を選択します。

ステップ 9 [移動（Go）] をクリックします。

ステップ 10 必要に応じてアラーム設定を行います。

ステップ 11 [保存（Save）] をクリックします。

第 4 章

サードパーティ製コンプライアンス サーバとの統合

サードパーティ コンプライアンスの概要

このソリューションを使用して、IM and Presence サービスはロギングまたは倫理的境界機能のコンプライアンスのために 1 つ以上のサードパーティ コンプライアンス サーバを統合します。 IM and Presence サービス管理者は、どの IM、プレゼンス、またはグループ チャット イベントがコンプライアンス サーバに渡されるか、およびどのイベントがブロックされるかを選択できます。イベントはポリシーに基づいて選択する必要があります。 たとえば、システムは特定のユーザまたはユーザ グループ間の IM をフィルタするか、IM の作成者および受信者に応じてコンテンツをブロックまたは変更するように設定することができます。

サードパーティ製のコンプライアンス ソリューションを使用するには、クラスタに対してサードパーティ コンプライアンス サーバを設定する必要があります。 IM and Presence サービスは、ユーザ ログイン、ログアウト、プレゼンス共有、IM 交換、またはグループ チャット アクティビティの処理の際に生成されたすべての設定イベントをサードパーティ サーバに渡します。 サードパーティ コンプライアンス サーバは、イベントに関連するポリシーやフィルタを適用し、IM and Presence サービスに対してイベントをさらに処理するかどうかを指示します。 IM and Presence サービスとサードパーティ製のコンプライアンス サーバとの間で受け渡されるイベントの量によっては、ネットワークでパフォーマンスの遅れが発生する可能性があることに注意してください。 IM and Presence サービスがサードパーティ サーバとの接続を失った場合、すべての IM トラフィックが停止します。

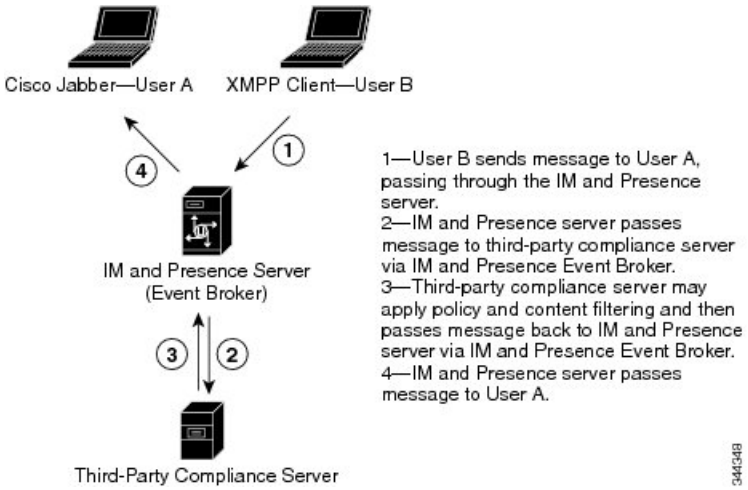
サードパーティ コンプライアンスには次のコンポーネントが必要です。

- IM and Presence サービス リリース 10.0(x)：IM and Presence サービスはイベントをサードパーティ コンプライアンス サーバに送信するために Event Broker コンポーネントを使用します。
- サードパーティ コンプライアンス サーバ：クラスタ内のすべての IM and Presence サービス ノードは、コンプライアンスがすでに設定されたシステムからアップグレードしているのではないかぎり、イベントを設定されたコンプライアンス サーバにリダイレクトします。
- IM クライアント：サポートされるクライアントには、Cisco Jabber などの Cisco クライアント、サードパーティ製 XMPP クライアント、および連動ネットワークで使用されるその他のサードパーティ製クライアントがあります。

（注） IM and Presence サービスは、IM and Presence サービスとサードパーティ コンプライアンス サーバ間にセキュアな TLS/SSL 接続を提供しません。

次の図は、サードパーティ コンプライアンスのコンポーネントとメッセージフローを示しています。

図 *3*：サードパーティ コンプライアンス



サードパーティ製コンプライアンスサーバの設定ワークフロー

サードパーティ製コンプライアンス統合を初めて設定する場合、以下のワークフローをお勧めします。

手順

ステップ 1 対応するコンプライアンス ベンダーのマニュアルにしたがってサードパーティ製コンプライアンス サーバをインストールします。

ステップ 2 サードパーティ製コンプライアンス サーバを IM and Presence サービス ノード上に設定します。以下の「IM and Presence サービスでのサードパーティ製コンプライアンス サーバの設定」を参照してください。

ステップ 3 対応するコンプライアンス ベンダー要件に基づいてイベントを選択し、コンプライアンス プロファイルを設定します。 以下のコンプライアンス プロファイルを参照してください。

ステップ 4 必要に応じて、コンプライアンス プロファイル ルーティング プライオリティを設定します。 以下のコンプライアンス プロファイル ルーティング プライオリティを参照してください。

ステップ 5 IM and Presence サービス ノードにコンプライアンス サーバおよびコンプライアンス プロファイルを割り当てます。 以下の「コンプライアンス プロファイルのコンプライアンス サーバへの割り当て」および「サードパーティ製コンプライアンス サーバの IM and Presence サービス ノードへの割り当て」を参照してください。

ステップ 6 コンプライアンス サーバ上で、IM and Presence サービスによって生成される対応するオープンポート名を、それぞれのコンプライアンス ベンダーのマニュアルに基づいて設定します。

IM and Presence サービス上のサードパーティ コンプライアンス サーバの設定

はじめる前に

- サードパーティ製のコンプライアンス サーバをインストールおよび設定します。
- 『*Installing Cisco Unified Communications Manager*』での説明に従って、IM and Presence サービス ノードをインストールします。
- 『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』での説明に従って、IM and Presence サービス ノードを設定します。

（注） 次の設定を変更する際には注意が必要です。 変更を保存すると、以前の設定はすべて失われます。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] > [メッセージ（Messaging）] > [外部サーバ設定（External Server Setup）] > [サードパーティ製コンプライアンス サーバ（Third-Party Compliance Servers）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 コンプライアンス サーバ名、オプションの説明、ホスト名またはIPアドレス、ポート、およびパスワードを入力します。
名前は IM and Presence サービスによってローカルでのみ使用されます。 IP アドレス、ポート、およびパスワードはコンプライアンス サーバ自体の設定に一致する必要があります。

（注） [ホスト名または IP アドレス（Hostname/IP Address）] フィールドで使用可能な文字はすべての英数字（a-zA-Z0-9）、ピリオド（.）、バックスラッシュ（\）、ダッシュ（-）、およびアンダースコア（_）です。

ステップ 4 [保存（Save）] をクリックします。

注意 IPアドレス、ポート、またはパスワードに変更を加えた場合、機能が稼動を継続するにはコンプライアンス上で対応する変更を加える必要がある場合があります。

コンプライアンスプロファイル

コンプライアンス プロファイルには、コンプライアンスのモニタに使用できる、一連の Jabber Session Manager（JSM）と Text Conferencing（TC）のイベントの両方またはいずれか一方が含まれます。 JSM イベントのみ、TC イベントのみ、または JSM および TC イベントの両方の組み合わせで構成されるコンプライアンス プロファイルを作成できます。

コンプライアンス プロファイルを設定する場合、どの JSM および TC イベントをコンプライアンス サーバにログ記録するかを選択します。 コンプライアンス サーバがどのタイプの処理を実行するか、IM and Presence サービスがどのようにコンプライアンス サーバからのエラー応答を処理するか、また IM and Presence サービス ノードがイベントをさらに処理する前にコンプライアンス サーバからの応答を待機するかどうかを決定できます。 応答が予期されない場合にイベントがどのように処理されるかも設定できます。

次の表は、JSM イベントおよびパラメータを説明しています。

注意 [BOUNCE]、および[火災と紛失（Fire and Forget）]の組み合わせが選択された場合、これが適用されるイベントがコンプライアンス サーバに渡され、その後破棄されます。 これは、IM and Presence サービスによってさらに処理されないことを意味しています。 この組み合わせを使用する際は、十分注意してください。

表 *1*：*JSM* イベント

イベント	説明
e_SESSION	新しいセッションが作成されると、ログイン中に送信されるパケット。
e_OFFLINE	オフラインであるユーザに送信されるパケット。 オフライン ユーザはアクティブ セッションを持たないユーザです。
e_SERVER	内部処理のために直接サーバに送信されるパケット。
e_DELIVER	別のサーバからのパケットに対する最初のイベント。 同じサーバ上のユーザからのパケットに対する2番目のイベント （同じサーバからのパケットに対する最初のイベントは es_IN です）。
e_AUTH	認証時に送信される IQ パケット。
e_REGISTER	ユーザによる新規アカウントの登録時に生成されるパケット。
e_STATS	定期的に送信されるサーバ統計情報が含まれるパケット。
e_DISCOFEAT	ユーザが disco#info クエリを送信する場合にトリガーされます。
e_PRISESSION	ユーザが複数のセッションを持つ場合、ユーザのプライマリまたはデフォルト セッションを決定します。 EventBroker コンポーネントによってユーザ プライマリ セッションの選択肢が決まる場合があります。
es_IN	スタンザがユーザ セッションによって受信される直前に生成されます。
es_OUT	スタンザがユーザ セッションから送信されるときに生成されます。

イベント	説明
es_END	ユーザがEMからログアウトするときの電話履歴の自動クリア。

表 *2* : ***JSM*** パラメータ

パラメータ	説明
パケット タイプ（Packet Type）	次のXMPPのパケットタイプからいずれかを選択します。 • **all**：すべてのパケット • **iq**：情報クエリ機能で使用されるパケット • **message**：標準 IM またはグループ チャット メッセージを含むパケット • **presence**：プレゼンス情報を含むパケット • **subscription**：別のユーザのプレゼンスに登録中に送信されるパケット
処理（Handling）	コンプライアンス サーバから返されるエラーが元のパーティまたはコンポーネントにバウンスされるようにする場合は[BOUNCE]を、破棄する場合は[PASS]を選択します。
火災と紛失（Fire and Forget）	イベントの処理を継続する前にIM and Presence サービス ノードがコンプライアンス サーバからの応答を待つ必要がある場合はチェックボックスをオンにします。イベントをさらに継続するためにIM and Presence サービス ノードがコンプライアンス サーバからの応答を待つ必要がない場合はチェックボックスをオフにします。

次の表は、TC イベントおよびパラメータを説明しています。

注意 [BOUNCE]、および[火災と紛失（Fire and Forget）]の組み合わせが選択された場合、これが適用されるイベントがコンプライアンス サーバに渡され、その後破棄されます。 これは、IM and Presenceサービスによってさらに処理されないことを意味しています。 この組み合わせを使用する際は、十分注意してください。

表 *3* : *TC* イベント

イベント	説明
onServicePacket	システムは、直接 TC サービスに向けられるかまたはシステム上に存在してしないルームに向けられたルータからのパケットを受信します。
onBeforeRoomCreate	ギアがシステム上にルームを作成しようとしています。
onAfterRoomCreate	ルームはシステム上に正常に作成されました。 唯一の有効な応答は、元のスタンザへの修正がないPASSです。
onServiceDiscoInfo	エンティティが TC サービスに disco#info パケットを送信しました。 有効な応答は PASS のみです。
onServiceReconfig	TC サービスは自身を再構成するシグナルを受信します。 有効な応答は PASS のみです。 これは単なる通知イベントです。 XDB パケットのタイプは ="set" になります。 外部コンポーネントは、このパケットに応答することはできません。
onDestroy	ルームのオーナーがルームを閉じます。 有効な応答は PASS のみです。
onClose	ギアがルームを閉じることを要求します。
onPacket	新しいXMLスタンザは、ルーム、またはルーム内の参加者に向けられます。
onMetaInfoGet	ルームの設定情報を利用できます。 有効な応答は PASS のみです。
onBeforeMetaInfoSet	ルームの設定をユーザが修正しようとしています。
onAfterMetaInfoSet	ルームの設定がユーザによって修正されました。 有効な応答は、中に何もない PASS のみです。
onExamineRoom	Jabber エンティティは、browse または disco によってルームから情報を要求します。 有効な応答は PASS のみです。

イベント	説明
onBeforeChangeUser	ユーザ ロール、ニックネーム、またはプレゼンスの変更が要求されました。これには、入室、退室、ニックネーム変更、アベイラビリティ変更、または任意のロール変更（音声の許可または無効化、モデレータ特権）などが含まれます。
onAfterChangeUser	ユーザが変更されました。 有効な応答は、中に何もない PASS のみです。
onBeforeChangeAffiliation	ユーザ アフィリエーションが変更されようとしています。
onAfterChangeAffiliation	ユーザアフィリエーションが変更されました。有効な応答は、中に何もない PASS のみです。
onBeforeRemoveAffiliation	ユーザ アフィリエーションが削除されようとしています。
onAfterRemoveAffiliation	ユーザアフィリエーションが削除されました。唯一の有効な応答は、元のスタンザへの修正がないPASSです。
onBeforeJoin	ユーザがルームを結合しようとしています。
onAfterJoin	ユーザがルームを結合しました。 有効な応答は、中に何もない PASS のみです。
onLeave	ユーザがルームから退室しました。 有効な応答は PASS のみです。
onBeforeSubject	ルームの件名が変更されようとしています。
onAfterSubject	ルームの件名が変更されました。 有効な応答は、中に何もない PASS のみです。
onBeforeInvite	ユーザがルームに招待されようとしています。
onAfterInvite	ユーザがルームに招待されました。 有効な応答は、中に何もない PASS のみです。
onHistory	ルームの履歴が要求されました。有効な応答はPASSのみです。
onBeforeSend	メッセージがルームで送信されようとしています。

イベント	説明
onBeforeBroadcast	メッセージがルームでブロードキャストされようとしています。

表 *4* : *TC* パラメータ

パラメータ	説明
処理（Handling）	コンプライアンス サーバから返されるエラーが元のパーティまたはコンポーネントにバウンスされるようにする場合は [BOUNCE] を、破棄する場合は [PASS] を選択します。
火災と紛失（Fire and Forget）	イベントの処理を継続する前に IM and Presence サービス ノードがコンプライアンス サーバからの応答を待つ必要がある場合はチェックボックスをオンにします。 イベントをさらに継続するために IM and Presence サービス ノードがコンプライアンス サーバからの応答を待つ必要がない場合はチェックボックスをオフにします。

同じコンプライアンス プロファイルが複数のコンプライアンス サーバに割り当てられている場合、イベントはそれぞれのコンプライアンス サーバにロード バランスされます。 これによって個々のコンプライアンスサーバの負荷が軽減されます。イベントは、関連するイベントが同じコンプライアンス サーバにルーティングされることを保証するアルゴリズムを使用してルーティングされます。 一対一の IM では、イベントはパケットの方向に関係なく to/from アドレスの組み合わせに基づいてルーティングされます。 これは、2 人のユーザ間のカンバセーション全体が 1 つのコンプライアンス サーバにルーティングされることを意味しています。 グループ チャットでは、特定のチャット ルームに対するイベントがチャット ルーム アドレスを使用してルーティングされ、ルームに対するすべてのイベントが 1 つのコンプライアンス サーバにルーティングされます。

システム デフォルト プロファイルはフレッシュ インストールまたはアップグレード後にシステムで使用可能です。 このプロファイルは SystemDefaultComplianceProfile と呼ばれ、削除または変更できません。 他と同様にこのプロファイルは割り当ておよび割り当て解除できます。

SystemDefaultComplianceProfile プロファイルには 4 つの JSM と 5 つの TC イベントが設定されています。 このプロファイルが割り当てられている場合、そのイベントのいずれかが IM and Presence サービス クラスタで発生する場合、処理のためにコンプライアンス サーバに渡され、応答が予期されます。 IM and Presence サービス ノードは、コンプライアンス サーバからの応答に基づいてイベントを処理します。 これらのイベントは、SystemDefaultComplianceProfile が利用可能なコンプライアンス プロファイルから選択された場合、読み取り専用形式でプレビューされます。

表 *5* : ***SystemDefaultComplianceProfile Pre-Configured*** イベント

JSM イベント	**TC** イベント
e_SESSION	onBeforeInvite
es_END	onBeforeJoin
es_IN（メッセージ スタンザのみ）	onBeforeRoomCreate
es_OUT（メッセージ スタンザのみ）	onBeforeSend
	onLeave

同じイベントが複数のプロファイルで設定され、これらのプロファイルが異なるサードパーティ コンプライアンス サーバに割り当てられる場合、イベントはルーティング プライオリティで指定される順序で処理されます。デフォルトでは、すべてのプロファイルのルーティング プライオリティはプロファイルがシステムに追加された順序で定義されます。ルーティング プライオリティは再設定できます。

コンプライアンス プロファイルの設定

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] > [メッセージ（Messaging）] > [コンプライアンス（Compliance）] > [コンプライアンスプロファイル（Compliance Profiles）] を選択します。

ステップ 2 [新規追加（Add New）] を選択します。

ステップ 3 コンプライアンス プロファイルの名前を入力します。
使用できる文字は英数字のみです。 スペースは使用できません。

（注） コンプライアンスのプロファイル名はコンプライアンス プロファイルがコンプライアンス サーバに割り当てられている場合は変更できません。

ステップ 4 コンプライアンス プロファイルの説明を入力します。
このフィールドはオプションで、コンプライアンス プロファイルの目的を示す意味のある説明を含める必要があります。

ステップ 5 JSM または TC でイベントを選択します。

ステップ 6 JSM イベントについては、パケット タイプを選択します。
同じパケット タイプと同じイベントを複数回設定することはできません。

[すべて（All）] を選択した場合、別のパケット タイプに対して同じイベントを、またはその逆を設定することはできません。

同じ JSM イベントにすべてのパケット タイプを設定することは、1 つの JSM イベントを All のパケット タイプで設定することと同じです。

ステップ 7 処理タイプを選択します。

ステップ 8 [火災と紛失（Fire and Forget）] チェックボックスを選択して、イベントがコンプライアンス サーバによって IM and Presence サービス イベント処理チェーンの外で処理されるようにします。 IM and Presence サービスは、コンプライアンス サーバの処理に関係なくイベントの処理を継続します。
デフォルトで、イベントはイベント処理チェーンの一部として処理され、IM and Presence サービスはコンプライアンス サーバからの応答を待機します。

イベントがイベント処理チェーンの一部として処理され、コンプライアンス サーバが HANDLE で応答する場合、イベントは IM and Presence サービスによってさらに処理されません。 コンプライアンス サーバが PASS で応答する場合、IM and Presence サービスはイベントの処理を継続します。

ステップ 9 いずれかのタイプのイベントを追加するには、[新規イベントの追加（Add New Event）] を選択します。

トラブルシューティングのヒント

サードパーティ製コンプライアンス サーバに割り当てられたプロファイル内のイベントに対する設定を更新した場合、XCP Router サービスを再起動する必要があります。

次の作業

複数のコンプライアンス プロファイルが割り当てられていて、1 つのプロファイルからの一部のイベントまたはすべてのイベントが他のプロファイル内に存在する場合、ルーティング プライオリティを設定できます。

関連トピック

コンプライアンスプロファイルのルーティング優先順位, （25 ページ）

コンプライアンスプロファイルのルーティング優先順位

複数のコンプライアンス プロファイルが割り当てられていて、1 つのプロファイルからの一部のまたはすべてのイベントが他のプロファイル内に存在する場合、ルーティング プライオリティを設定できます。 各コンプライアンスプロファイルに異なるイベントが設定されている場合、ルーティング プライオリティは適用されません。

システムで設定されたプロファイルのデフォルトのルーティング プライオリティは、設定された順序となります。

例

以下は、コンプライアンス プロファイル ルーティング プライオリティを使用する場合の例を示しています。

Ethical Wall 精査の対象となるイベントに設定されたコンプライアンス プロファイルと、IM ログ記録の対象となる同じイベントに設定されたコンプライアンスプロファイルがあります。 それぞ

れが異なるコンプライアンス サーバに割り当てられます。 Ethical Wall 精査の対象となるイベントを、IM ロギング サーバにログ記録する前に Ethical Wall にルーティングしたい場合、Ethical Wall コンプライアンス プロファイルにより高いプライオリティを割り当てる必要があります。

コンプライアンス プロファイル ルーティング プライオリティの設定

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] > [メッセージ（Messaging）] > [コンプライアンス（Compliance）]>[コンプライアンスプロファイルのルーティング優先順位（Compliance Profiles Routing Priority）] を選択します。

ステップ 2 [ルーティング プライオリティ別にコンプライアンス プロファイルをリスト（最上部が最高のプライオリティ）（Compliance Profiles listed by routing priority(Top is highest priority)）] ウィンドウで、上下矢印を使用してコンプライアンスプロファイルに対するルーティングプライオリティを調整します。

次の作業

ルーティング プライオリティを変更したプロファイルが割り当てられた場合、Cisco XCP ルータ サービスを再起動する必要があります。 ルータの再起動が必要なときに関して先頭に表示される警告メッセージの指示に従う。

関連トピック

Cisco XCP ルータ サービスの再起動, （11 ページ）

コンプライアンス サーバへのコンプライアンス プロファイルの割り当て

IM and Presence サービス 10.0.(1) で、以前にコンプライアンスが設定されていたシステムからアップグレードする場合を除き、クラスタ内のすべてのノードはコンプライアンスの対象となります。これは、IM and Presence サービス ノードに複数のコンプライアンス サーバを割り当てることはできますが、コンプライアンスの対象とするためにすべての IM and Presence サービス ノードにコンプライアンス サーバを割り当てる必要はないことを意味しています。

クラスタ内の各コンプライアンス サーバは、異なるイベントのセットを処理するように設定できます。 これらのイベントのセットはコンプライアンスプロファイルで設定され、コンプライアンス サーバおよび IM and Presence サービス ノードに割り当てられます。

システム デフォルト プロファイルはフレッシュ インストールまたはアップグレード後にシステムで使用可能です。 このプロファイルは SystemDefaultComplianceProfile と呼ばれ、削除または変更できません。他と同様にこのプロファイルは割り当ておよび割り当て解除できます。独自のカスタム コンプライアンス プロファイルを作成するまで、ドロップダウン メニューから使用可能なデフォルトのコンプライアンス プロファイルは 1 つだけです。

10.0(1) 以前からアップグレードする場合、以前の割り当てには SystemDefaultComplianceProfile が割り当てられます。 これはドロップダウン メニューから使用可能な唯一のプロファイルです。 このデフォルト プロファイル内のイベントは、アップグレード前のシステムのものと同じイベントです。

以前のリリースでは、IM Compliance はノード単位で動作しました。 コンプライアンス サーバが割り当てられたノードはすべて、イベントがそのノードで生成された場合にのみ IM イベントをコンプライアンス サーバにログ記録しました。 このリリースでは、IM コンプライアンスはクラスタベースで機能します。 クラスタ内のノードの数またはどのノードにサードパーティ製のコンプライアンス サーバが割り当てられているかに関係なく、クラスタ内のすべてのノードがコンプライアンスの対象となります。 クラスタ内の任意のノードで生成された任意のイベントがコンプライアンス サーバのいずれかにログ記録されます。

10.0(1) 以前からアップグレードする場合、システムはアップグレード後にノードベースで機能しますが、クラスタ内のすべてのノードに対してコンプライアンス ログを有効にできます。 これを選択すると、割り当てを作成、更新、および削除したり、コンプライアンス プロファイルをシステム内に作成したカスタム コンプライアンス プロファイルに変更したりすることが可能になります。

（注） 以前にコンプライアンスが設定されていたシステム上のすべてのノードに対してコンプライアンス ロギングを有効にすることは必須ではありません。 ノード単位でコンプライアンス ロギングを保持することを選択できます。 この場合、コンプライアンス サーバでは SystemDefaultComplianceProfile だけを使用できます。

IM and Presence サービス ノードへのサードパーティ製コンプライアンス サーバの割り当て

はじめる前に

IM and Presence サービス上でサードパーティ製コンプライアンス サーバを設定します。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] > [メッセージ（Messaging）] > [コンプライアンス（Compliance）] > [コンプライアンス設定（Compliance Settings）] を選択します。

ステップ 2 コンプライアンス サーバの選択項目から [サードパーティ製コンプライアンス サーバ（Third-Party Compliance Server）] を選択します。

ステップ 3 IM and Presence サービス ノードにサードパーティ製コンプライアンス サーバを割り当てます。

（注） アップグレード前にコンプライアンスが設定されていたシステムからアップグレードした場合、同じノードを複数のコンプライアンス サーバに割り当てることはできません。 この場合、同じノードを複数のコンプライアンス サーバに割り当てたい場合、クラスタ全体に対するコンプライアンスを有効にする必要があります。

[オープンポート コンポーネント名（Open-port Component Name）] フィールドは、最初の 2 つの列内の値に基づいて自動的に生成されます。 これはオープンポートのコンポーネントを設定する場合に使用されます。

ステップ 4 各コンプライアンス サーバにコンプライアンス プロファイルを割り当てます。
同じコンプライアンス プロファイルを複数回割り当てることができます。

（注） 10.0(1) より前のバージョンからシステムをアップグレードして、コンプライアンスをアップグレード前に設定した場合、システムのデフォルト プロファイルのみをドロップ ダウン メニューから利用できます。 カスタム プロファイルを使用するには、クラスタ全体のコンプライアンスを有効にします。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 コンプライアンスがクラスタ内のすべてのノードに適用されている場合、すべてのノードでCisco XCP ルータ サービスを再起動します。 これを実行しない場合、Cisco XCP ルータ サービスをこれらのコンプライアンスを設定したノードで再起動するだけで十分です。

トラブルシューティングのヒント

IM コンプライアンス展開オプションを切り替えた（たとえば、[Message Archiver] オプションから [サードパーティ コンプライアンス サーバ（Third-Party Compliance Server）] オプションに切り替えた）場合、Cisco XCP ルータ サービスを再起動する必要があります。 オプション間で切り替えるとサードパーティ コンプライアンス設定が失われることに注意してください。

関連トピック

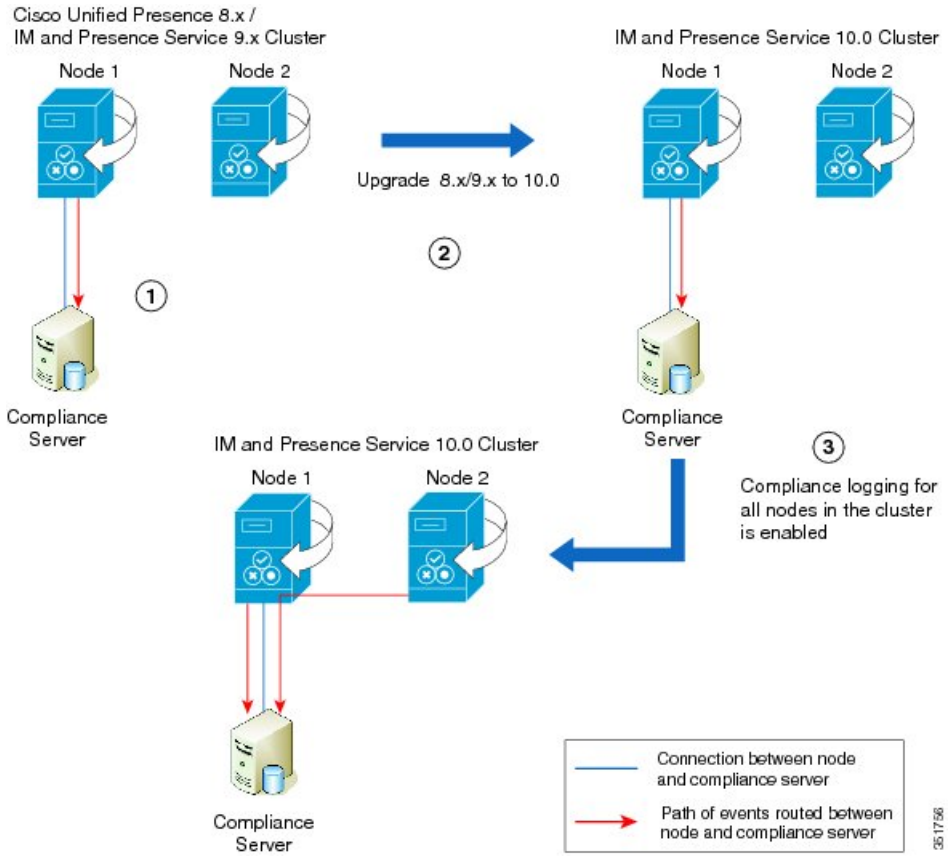
IM and Presence サービス上のサードパーティ コンプライアンス サーバの設定, （17 ページ）
Cisco XCP ルータ サービスの再起動, （11 ページ）
コンプライアンス プロファイルの設定, （24 ページ）
アップグレード後にすべてのノードに対してコンプライアンス ロギングを有効化, （32 ページ）

アップグレードのシナリオ

このセクションには、現在コンプライアンスを設定している管理者が IM and Presence サービス 10.0.(1) にアップグレードする前に役立ついくつかのサンプル アップグレード シナリオが含まれています。

アップグレード シナリオ 1

図 *4* : シナリオ *1*

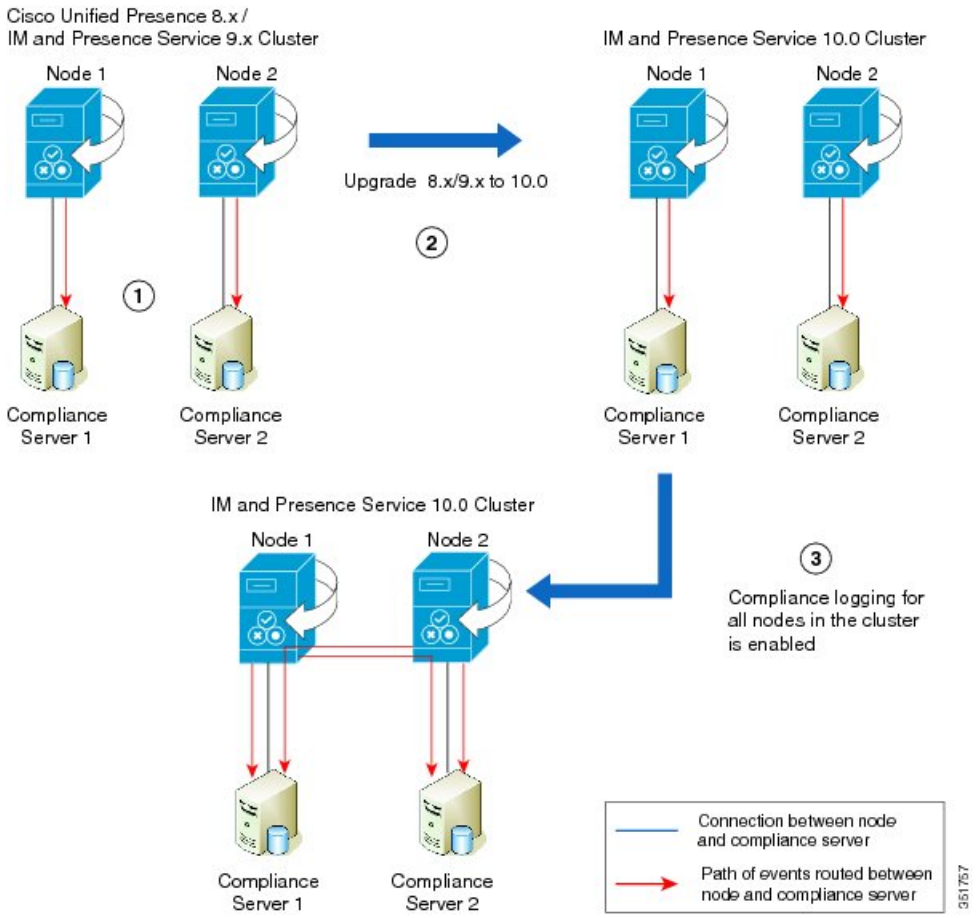


第 1 段階	クラスタは 2 つのノードと 1 つのコンプライアンス サーバで構成されます。 ノード 1 はコンプライアンス サーバに接続され、このノードからのイベントのみがコンプライアンス サーバにルーティングされます。
第 2 段階	クラスタが IM and Presence サービス バージョン 10.0 にアップグレードされると、ノード 1 はコンプライアンス サーバへの接続を維持し、このノードからのイベントのみがコンプライアンス サーバへルーティングされます。 ノード 1 とコンプライアンス サーバの両方が稼動を続行します。設定の変更は必要ありません。
第 3 段階	[Cisco Unified CM IM and Presence Administration] > [メッセージ（Messaging）] > [コンプライアンス（Compliance）] > [コンプライアンス設定（Compliance Settings）] ページ上の [クラスタ内のすべてのノードに対してコンプライアンス ログを有効にする（Enable compliance logging for all nodes in the cluster）] をチェックすることでクラスタ全体のコンプライアンスを有効にすると、ノード 1 はコンプライアンス サーバへの接続を維持します。 コンプライアンス サーバ上の設定は操作を維持するた

	めに更新する必要があります。 両方のノードからのイベントはノード1を介してコンプライアンス サーバにルーティングされます。

アップグレード シナリオ 2

図 *5*：シナリオ *2*

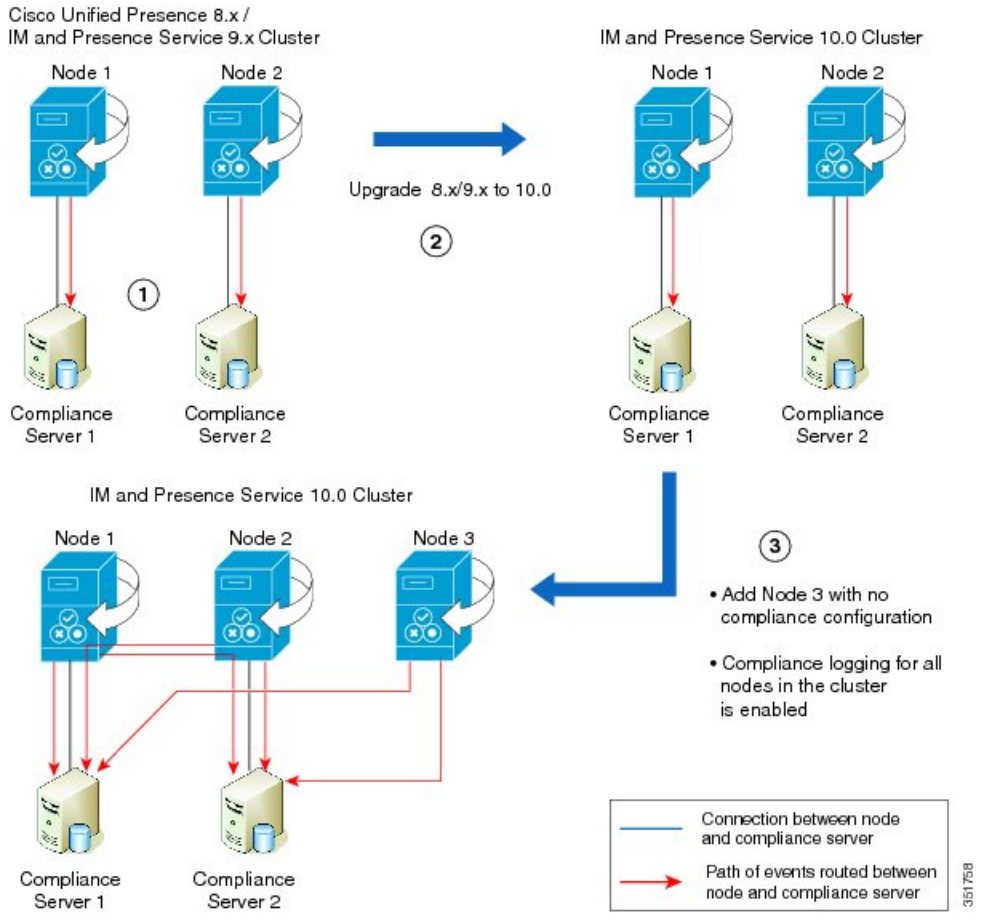


第 1 段階	クラスタは 2 つのノードと 2 つのサードパーティ製コンプライアンス サーバで構成されます。 各ノードは接続され、ノードごとにそれぞれのコンプライアンス サーバにイベントがルーティングされます。
第 2 段階	クラスタが IM and Presence サービス バージョン 10.0 にアップグレードされた後、各ノードは接続され、ノードごとにそれぞれのコンプライアンス サーバにイベントがルーティングされます。 両方のノードとそれぞれのコンプライアンス サーバの両方は稼動を継続し、設定の変更は必要ありません。

第 3 段階	[Cisco Unified CM IM and Presence Administration] > [メッセージ（Messaging）] > [コンプライアンス（Compliance）] > [コンプライアンス設定（Compliance Settings）] ページ上の [クラスタ内のすべてのノードに対してコンプライアンス ログを有効にする（Enable compliance logging for all nodes in the cluster）] をチェックすることでクラスタ全体のコンプライアンスを有効にすると、各ノードがそのコンプライアンス サーバに接続されます。 コンプライアンス サーバの設定は運用を維持するために更新しなければなりません。 ノード 1 およびノード 2 からのイベントが各コンプライアンス サーバにルーティングされます。

アップグレード シナリオ 3

図 *6*：シナリオ *3*



第 1 段階	クラスタは 2 つのノードと 2 つのサードパーティ製コンプライアンス サーバで構成されます。 各ノードは接続され、ノードごとにそれぞれのコンプライアンス サーバにイベントがルーティングされます。

第 2 段階	クラスタが IM and Presence サービス バージョン 10.0 にアップグレードされた後、各ノードは接続され、ノードごとにそれぞれのコンプライアンス サーバにイベントがルーティングされます。 両方のノードとそれぞれのコンプライアンス サーバの両方は稼動を継続し、設定の変更は必要ありません。
第 3 段階	アップグレードされた IM and Presence サービス バージョン 10.0 クラスタで、コンプライアンスを持たない追加のノード、ノード 3 が追加されます。 [Cisco Unified CM IM and Presence Administration] > [メッセージ（Messaging）] > [コンプライアンス（Compliance）] > [コンプライアンス設定（Compliance Settings）] ページ上の [クラスタ内のすべてのノードに対してコンプライアンス ログを有効にする（Enable compliance logging for all nodes in the cluster）] をチェックすることでクラスタ全体のコンプライアンスを有効にすると、各ノードがそのコンプライアンス サーバに接続されます。 コンプライアンス サーバの設定は運用を維持するために更新しなければなりません。 ノード 1 およびノード 2 からのイベントが各コンプライアンス サーバにルーティングされます。 ノード 3 上のイベントはノード 1 およびノード 2 上の開いたポートを通して両方のコンプライアンス サーバにルーティングされます。

アップグレード後にすべてのノードに対してコンプライアンス ロギングを有効化

注意 この設定を有効にした場合、元に戻すことはできません。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] > [メッセージ（Messaging）] > [コンプライアンス（Compliance）] > [コンプライアンス設定（Compliance Settings）] を選択します。

ステップ 2 コンプライアンス サーバの選択項目から [サードパーティ製コンプライアンス サーバ（Third-Party Compliance Server）] を選択します。

ステップ 3 [クラスタ内のすべてのノードに対してコンプライアンス ログを有効にする（Enable compliance logging for all nodes in the cluster）] を選択します。 イネーブルにした場合、この設定を元に戻すことはできません。 最適な設定チェックボックスに関してはマニュアルを参照し、[保存（Save）] をクリックします。
警告メッセージが表示されます。

ステップ 4 OK をクリックします。

ステップ 5 クラスタ内のすべてのノードで Cisco XCP ルータ サービスを再起動します。

次の作業

すべてのノードに対してコンプライアンスを有効化した後、IM and Presence サービスによって使用されるコンポーネント名が自動生成された形式に変更されます。 機能の使用を継続するには、新しいコンポーネント名でコンプライアンス サーバを更新します。

関連トピック

Cisco XCP ルータ サービスの再起動, （11 ページ）

サードパーティ製コンプライアンスサーバ障害イベントの処理

サードパーティ製のコンプライアンスサーバ障害イベントの処理について

この章では、コンプライアンス統合時またはHA フェールオーバー中に問題が発生した場合に IM and Presence サービス ユーザが体験する動作について説明しています。

（注） この章のセクションは、（別途記載がある場合を除き）コンプライアンス プロファイルに以下のイベントが含まれることを前提としています。

- e_SESSION（ユーザ ログインの記録）
- es_END（ユーザ ログアウトの記録）
- メッセージに対する es_OUT/es_IN（IM カンバセーションの記録）
- 1 つ以上の TC イベント（チャット ルーム内のやりとりの記録）

コンプライアンス サーバまたはサービス停止時のイベント処理

単一のコンプライアンス サーバまたはサービスのシャットダウン

想定される展開：

- サブクラスタで展開される 1 つ以上の IM and Presence サービス ノード。
- 1 つの IM and Presence サービス ノードが単一のサードパーティ コンプライアンス サーバで設定されます。

コンプライアンス サーバまたはサービスがグレースフルにシャットダウンされるとユーザは以下のように影響を受けます。

- ユーザは通常どおり XMPP クライアントを使用して IM and Presence サービスへのログインとログアウトを続行しますが、ログインとログアウトのイベントはコンプライアンス サーバにログ記録されません。
- ユーザは IM の送信またはチャット ルームの利用がブロックされ、それぞれの場合にサーバ エラー応答を受信します。

単一のコンプライアンス サーバまたはサービスのアングレースフルな失敗またはネットワーク障害

想定される展開：

- サブクラスタで展開される 1 つ以上の IM and Presence サービス ノード。
- 1 つの IM and Presence サービス ノードが単一のサードパーティ コンプライアンス サーバで設定されます。

最初の 5 分間まで、コンプライアンス サーバまたはサービスがアングレースフルに失敗した場合、または IM and Presence サービス ノードとコンプライアンス サーバ間でネットワークの中断があった場合、ノードはそのコンプライアンス サーバに対してイベントのキューイングを試行します。 個々のイベントは処理またはバウンスされる前に 30 秒間キューに置かれます。

5 分経過してもコンプライアンス サーバまたはネットワークが回復していない場合、サーバへの接続がドロップされ、イベントはキューに置かれなくなります。 この場合、イベントは即時に処理またはバウンスされます。 ユーザには次のような影響があります。

- ユーザには IM and Presence サービスへのログイン時に最大 30 秒の遅延が発生しますが、ログアウト時には遅延はありません。 ログインおよびログアウト イベントはコンプライアンス サーバにログ記録されません。
- ユーザは IM の送信またはチャット ルームの利用がブロックされます。 それぞれの場合、ユーザはサーバ エラー応答を受信しますが、エラーが受信されるまでに最大 30 秒の遅延が発生する場合があります。
- プレゼンス ステータスの更新が処理されている間、ユーザには最大 30 秒の遅延が発生する場合があります。

複数のコンプライアンス サーバでのコンプライアンス サーバまたはサービスのグレースフルな停止

想定される展開：

- サブクラスタに展開された 1 つの IM and Presence サービス ノード。

- 1 つの IM and Presence サービス ノードが複数のサードパーティ コンプライアンス サーバで設定されます。

IM and Presence サービス ノードが複数のコンプライアンス サーバに接続されている場合、通常は、JID ベースのアルゴリズムを使用して、イベントにコンプライアンス サーバに渡るロードバランスが適用されます。 異なるユーザに対するイベントは異なるコンプライアンス サーバにルーティングできます。

コンプライアンス サーバまたはサービスのいずれかがグレースフルにシャットダウンした場合、このサーバにルーティングされるはずだったイベントは残りのコンプライアンス サーバにルーティングされます。

複数のコンプライアンスサーバでのコンプライアンスサーバまたはサービスのアングレースフルな停止

想定される展開：

- サブクラスタに展開された 1 つの IM and Presence サービス ノード。
- 1 つの IM and Presence サービス ノードが複数のサードパーティ コンプライアンス サーバで設定されます。

IM and Presence サービス ノードが複数のコンプライアンス サーバに接続されている場合、通常は、JID ベースのアルゴリズムを使用して、イベントにコンプライアンス サーバに渡るロードバランスが適用されます。 異なるユーザに対するイベントは異なるコンプライアンス サーバにルーティングできます。

コンプライアンス サーバまたはサービスのいずれかがアングレースフルに失敗した場合、または IM and Presence サービス ノードとそのサーバの間のネットワークに障害が発生した場合、ユーザは以下のように影響を受けます。

- 一部ユーザには IM and Presence サービスへのログイン時に最大 30 秒の遅延が発生しますが、ログアウト時には遅延はありません。 ログインおよびログアウト イベントはコンプライアンス サーバにログ記録されません。
- 一部のユーザは IM の送信またはチャット ルームの利用を最大 5 分間ブロックされます。 この期間が経過した後、ユーザは IM の送信またはチャット ルームの利用を継続することができ、イベントは残りのコンプライアンス サーバのいずれかにルーティングされます。
- プレゼンス ステータスの更新が処理されている間、一部のユーザには最大 30 秒の遅延が発生する場合があります。

複数のコンプライアンスサーバおよびプロファイルでのコンプライアンスサーバまたはサービスの停止

IM and Presence サービス ノードが複数のコンプライアンス サーバに接続するように設定されていて、それぞれ異なるコンプライアンス プロファイルを使用しており、プロファイルに 1 つまたは

複数の同一のイベントが含まれる場合、これらのイベントに対する通常の動作は、各プロファイルのプライオリティに基づいて各コンプライアンス プロファイルに関連付けられるコンプライアンス サーバに順番にルーティングされることです。

この動作の詳細は次の例で説明されています。

想定される展開：

- 1 つまたは複数の同一のイベントを含む複数のプロファイルを持つサブクラスタ内に展開された 1 つの IM and Presence サービス ノード。
- IM and Presence サービス ノードは複数のサードパーティ コンプライアンス サーバおよびプロファイルで設定されます。

各コンプライアンス プロファイルには設定された以下のイベントがあります。

プロファイル 1：

- e_SESSION（ユーザ ログインの記録）
- メッセージに対する es_OUT/es_IN（IM カンバセーションの記録）
- es_END（ユーザ ログアウトの記録）

プロファイル 2：

- メッセージに対する es_OUT/es_IN（IM カンバセーションの記録）

プロファイルの割り当て：

- プロファイル 1 はコンプライアンス サーバ 1 に割り当てられます。
- プロファイル 2 はコンプライアンス サーバ 2 に割り当てられます。
- プロファイル 1 が最高のプライオリティです。

通常動作時：

ユーザが IM を送信すると、プロファイル 1 の es_OUT イベントはコンプライアンス サーバ 1 にルーティングされます。 コンプライアンス サーバ 1 がイベントを許可する場合、プロファイル 2 の es_OUT イベントはコンプライアンス サーバ 2 にルーティングされます。

コンプライアンス サーバ 1 にアングレースフルな停止が発生すると、以下のシーケンスが実行されます。

1. ユーザ A がユーザ B.に IM を送信します。
2. es_OUT イベント（プロファイル 1）がコンプライアンス サーバ 1 のキューに入れられます。
3. es_OUT イベント（プロファイル 1）が 30 秒後にタイムアウトします。
4. es_OUT イベント（プロファイル 1）はバウンスされ、IM 送信者はエラー応答を受信します。
5. es_OUT（プロファイル 2）イベントは処理されず、イベントはコンプライアンス サーバ 2 に送信されません。

この場合、ユーザには以下のような影響があります。

- ユーザは、IM の送信をブロックされます。 それぞれの場合に、ユーザはサーバ エラー応答を受信しますが、エラーが受信されるまでに最大 30 秒の遅延が発生する場合があります。 IM のカンバセーションに関連付けられたイベントは残りのコンプライアンス サーバにルーティングされます。
- プレゼンス ステータスの更新が処理されている間、ユーザには最大 30 秒の遅延が発生する場合があります。

IM and Presence サービス ノードの障害発生時のコンプライアンス処理

手動のノードのフェールオーバー時のコンプライアンス処理

想定される展開：

- HA が有効化されたサブクラスタで展開される 2 つの IM and Presence サービス ノード。
- それぞれの IM and Presence サービス ノードは、同じコンプライアンス プロファイルを使用して異なるサードパーティ製コンプライアンス サーバで設定されています。

通常動作時：

- イベントは JID ベースのアルゴリズムを使用してコンプライアンス サーバにわたってロードバランスされています。
- 異なるユーザに対するイベントは異なるコンプライアンス サーバにルーティングできます。
- コンプライアンス サーバにルーティングされているイベントは、接続先の IM and Presence サービス ノードを使用してルーティングされます。

IM and Presence サービス ノードの手動のフェールオーバーが発生した場合、通常関連するコンプライアンス サーバにルーティングされるイベントは以下のように処理されます。

- ログインおよびログアウト イベントはコンプライアンス サーバにログ記録されません。 一部のユーザには IM and Presence サービスへのログイン時に最大 30 秒の遅延が発生しますが、ログアウト時には遅延はありません。
- フェールオーバー中、ユーザは IM の送信またはチャットルームの利用をブロックされます。この場合、各ケースについて、ユーザはサーバエラー応答を受信しますが、エラーが受信されるまでに最大 30 秒の遅延が発生する場合があります。 ブロックされるイベントはコンプライアンス サーバにログ記録されません。
- フェールオーバーが完了すると、IM またはグループ チャット イベントが別の IM and Presence サービス ノードに接続されるコンプライアンス サーバによって処理され、スタンザは通常どおり配信されます。

自動化されたノードのフェールオーバー時のコンプライアンス処理

想定される展開：

- HA が有効化されたサブクラスタで展開される 2 つの IM and Presence サービス ノード。
- それぞれの IM and Presence サービス ノードは、同じコンプライアンス プロファイルを使用して異なるコンプライアンス サーバで設定されています。

通常動作時：

- イベントは JID ベースのアルゴリズムを使用してコンプライアンス サーバにわたってロードバランスされています。
- 異なるユーザに対するイベントは異なるコンプライアンス サーバにルーティングできます。
- 各コンプライアンス サーバにルーティングされているイベントは、接続先の IM and Presence サービス ノードを使用してルーティングされます。

（注） フェールオーバーの要因が Cisco XCP ルータ サービスの障害またはシャットダウンでない場合は、コンプライアンス イベントは通常どおりコンプライアンス サーバに継続してルーティングされます。 フェールオーバーが発生した IM and Presence サービス ノードに接続されているコンプライアンス サーバにルーティングされるイベントは、コンプライアンス サーバに継続してルーティングされます。

複数ノード間のネットワーク障害中のコンプライアンス処理

想定される展開：

- HA が有効化されたサブクラスタで展開される 2 つの IM and Presence サービス ノード。
- それぞれの IM and Presence サービス ノードは、同じコンプライアンス プロファイルを使用して異なるコンプライアンス サーバで設定されています。

通常動作時：

- イベントは JID ベースのアルゴリズムを使用してコンプライアンス サーバにわたってロードバランスされています。
- 異なるユーザに対するイベントは異なるコンプライアンス サーバにルーティングできます。
- 各コンプライアンス サーバにルーティングされているイベントは、接続先の IM and Presence サービス ノードを使用してルーティングされます。

IM and Presence サービス ノード間でネットワーク障害が発生した場合、通常は別の IM and Presence サービス ノードに関連付けられるコンプライアンス サーバにルーティングされるユーザのイベントは以下のように処理されます。

- 一部のユーザには IM and Presence サービスへのログイン時に最大 30 秒の遅延が発生しますが、ログアウト時には遅延はありません。 ログインおよびログアウト イベントはコンプライアンス サーバにログ記録されません。
- 障害時に、一部のユーザは IM の送信やチャット ルームの利用をブロックされます。 それぞれの場合に、ユーザはサーバ エラー応答を受信しますが、エラーが受信されるまでに最大 30 秒の遅延が発生する場合があります。 ブロックされるイベントはコンプライアンス サーバにログ記録されません。
- 障害が 2 分以上継続する場合、イベントは展開内の別のコンプライアンス サーバによって処理され、スタンザは通常どおり配信されます。

Cisco XCP ルータ サービス障害中のコンプライアンス処理

想定される展開：

- HA が有効化されていないサブクラスタで展開される 2 つの IM and Presence サービス ノード。
- それぞれの IM and Presence サービス ノードは、同じコンプライアンス プロファイルを使用して異なるコンプライアンス サーバで設定されています。

（注） このセクションでは、HA が有効な場合の結果についても強調されます。

通常動作時：

- イベントは JID ベースのアルゴリズムを使用してコンプライアンス サーバにわたってロードバランスされています。
- 異なるユーザに対するイベントは異なるコンプライアンス サーバにルーティングできます。
- 各コンプライアンス サーバにルーティングされているイベントは、接続先の IM and Presence サービス ノードを使用してルーティングされます。

HA が有効になっているかどうかによってユーザが体験する結果の相違は以下のとおりです。

- HA が有効になっている場合、ユーザはログインしたままになっており、残りのノードに移動されます。
- HA が有効になっていない場合、障害の発生したノード上のユーザはログアウトされ、サービスを利用できません。

より一般的な影響は以下のとおりです。

- 障害の発生した IM and Presence サービス ノードに接続されているコンプライアンス サーバに通常ルーティングされているイベントは、他の IM and Presence サービス ノードに接続されているコンプライアンス サーバにルーティングされます。

- 障害が一時的なものである場合、一部のユーザはIMの送信やチャットルームの使用をブロックされます。 それぞれの場合に、ユーザはサーバ エラー応答を受信しますが、エラーが受信されるまでに最大 30 秒の遅延が発生する場合があります。 ブロックされるイベントはコンプライアンス サーバにログ記録されません。
- 障害が長期間継続する場合、IM は通常どおり処理され、他の IM and Presence サービス ノードに接続されたコンプライアンス サーバにルーティングされます。

IM and Presence サービス ノードおよびサードパーティ製コンプライアンス サーバ アラーム

IM and Presence サービス ノードがサードパーティ製コンプライアンス サーバに統合されている場合、メッセージは、サードパーティ製コンプライアンス サーバに正常にログ記録された後にのみユーザに配信されます。

IM and Presence サービス ノードが、直接接続されているサードパーティ製コンプライアンス サーバとの接続を失った場合、IM and Presence サービスはメッセージを受信者に配信しません。

この接続が失われたときに通知を受けるためには、この状態に関連するアラームが正しく設定されていることを確認する必要があります。

手順

ステップ 1 IM and Presence サービスにサインインします。

ステップ 2 [Cisco Unified IM and Presence Serviceability] > [アラーム（Alarm）] > [設定（Configuration）] を選択します。

ステップ 3 [サーバ（Server）] ドロップダウン メニューからアラームを設定するサーバを選択し、[移動（Go）] をクリックします。

ステップ 4 [サービス グループ（Service Group）] ドロップダウン リストから [IM and Presence サービス（IM and Presence Services）] を選択し、[移動（Go）] をクリックします。

ステップ 5 [サービス（Service）] ドロップダウン メニューから [Cisco XCP ルータ（Cisco XCP Router）] を選択し、[移動（Go）] をクリックします。

ステップ 6 必要に応じてアラーム設定を行います。

ステップ 7 [保存（Save）] をクリックします。

サードパーティ製コンプライアンス サーバのトラブルシューティング

コンプライアンス/統合が期待どおりに動作せず、以下のような問題が発生している場合。

- ユーザ ログイン遅延
- IM のブロック
- IM and Presence サービスがサードパーティ コンプライアンスを使用するように設定されている場合のグループ チャット イベントのブロック。

この場合、以下のチェックリストを使用してコンプライアンス統合のトラブルシューティングを実行します。

1. [コンプライアンス サーバの設定（Compliance Server Settings）] ウィンドウの [トラブルシュータ（Troubleshooter）] をチェックします。 [トラブルシュータ（Troubleshooter）] が赤の場合はステップ 2 に進みます。 [トラブルシュータ（Troubleshooter）] がグリーンの場合はステップ 3 に進みます。
2. サードパーティ製コンプライアンス サーバ設定ウィンドウで、サードパーティ製コンプライアンス サーバに対する接続設定をチェックします。
3. Cisco XCP ルータ サービスがサードパーティ製コンプライアンス サーバとの接続を確立したかどうかを検証するには、RTMT を使用して Cisco XCP ルータ サービス ログをチェックしてください。 以下のようなエントリに対してログをスキャンします。
   - `Component op-gwydlvm131.gwydlvm1153-cisco-com is CONNECTED`
     このエントリは、Cisco XCP ルータ サービスがサードパーティ製のコンプライアンス サーバに対してネットワーク接続を確立したことを示しています。
   - `Component op-gwydlvm131.gwydlvm1153-cisco-com is ACTIVE`
     このエントリは、Cisco XCP ルータ サービスとサードパーティ製コンプライアンス サーバの認証が完了したことを示しています。
4. ログが `CONNECTED` を表示するが `ACTIVE` を表示しない場合は、以下を検証してください。
   - 正しいパスワードは IM and Presence サービス およびサードパーティ製コンプライアンス サーバで設定されています。
   - 正しいコンポーネント名がサードパーティ製コンプライアンス サーバで設定されています。

   Cisco XCP ルータ サービスがサードパーティ製コンプライアンス サーバに接続できない場合、Cisco XCP ルータ サービス ログが以下のような出力を表示します。

   ```
   Connecting on fd 22 to host '10.53.52.205', port 7999
   Unable to connect to host '10.53.52.205', port 7999:(111) Connection refused
   Component op-gwydlvm131.gwydlvm1153-cisco-com is GONE
   ```
5. Cisco XCP ルータ サービスがサードパーティ製コンプライアンス サーバと接続を確立できない場合、以下を確認してください。
   - 正しい IP/FQDN およびポートが IM and Presence サービスおよびサードパーティ製コンプライアンス サーバで設定されている。
   - サードパーティ製コンプライアンス サーバが稼動しており、指定されたポート上でリッスンしている。

6 IM and Presence サービスがコンプライアンス サーバに処理用にイベントを渡す際にログが CONNECTED および ACTIVE を示している場合、IM and Presence サービスでイベントの処理を続行するには、サードパーティ製コンプライアンス サーバが事前に各イベントに応答する必要があります。 コンプライアンス サーバが応答していないと考えられる場合は、コンプライアンス サーバのログを確認してください。