



# 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, 1 ページ](#)
- [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, 3 ページ](#)
- [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, 3 ページ](#)
- [コンプライアンスプロファイル, 4 ページ](#)
- [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, 13 ページ](#)
- [アップグレードのシナリオ, 14 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 ログイングを有効化, 18 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, 19 ページ](#)
- [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, 26 ページ](#)
- [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, 26 ページ](#)

## 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 サービスはログイ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。

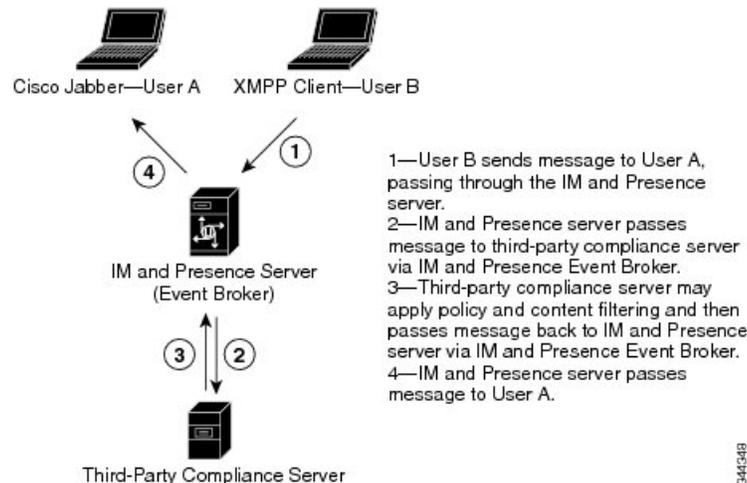
- IM and Presence サービス リリース 10.0(x) : IM and Presence サービスはイベントをサードパーティ コンプライアンス サーバに送信するために Event Broker コンポーネントを使用します。
- サードパーティ コンプライアンス サーバ : クラスタ内のすべての IM and Presence サービス ノードは、コンプライアンスがすでに設定されたシステムからアップグレードしているのではないかぎり、イベントを設定されたコンプライアンス サーバにリダイレクトします。
- IM クライアント : サポートされるクライアントには、Cisco Jabber 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 1 : 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	スタンプ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	スタンプ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。 <ul style="list-style-type: none"> <li>• <b>all</b> : すべてのパケット</li> <li>• <b>iq</b> : 情報クエリ機能で使用するパケット</li> <li>• <b>message</b> : 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</li> <li>• <b>presence</b> : プレゼンス情報を含むパケット</li> <li>• <b>subscription</b> : 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</li> </ul>
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、中に何も無い 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、中に何も無い 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、中に何も無い 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、中に何も無い 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、中に何も無い 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、中に何も無い 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パセッション全体が 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](#), (11 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どに関して先頭に表示される警告メッセージの指示に従います。

### 関連トピック

[Cisco XCP ルータ サービスの再起動](#)

## 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せんが、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ーベースで機能します。クラスター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、クラスター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。クラスター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、クラスター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、クラスター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, \(3 ページ\)](#)

[Cisco XCP ルータ サービスの再起動](#)

[コンプライアンス プロファイルの設定, \(10 ページ\)](#)

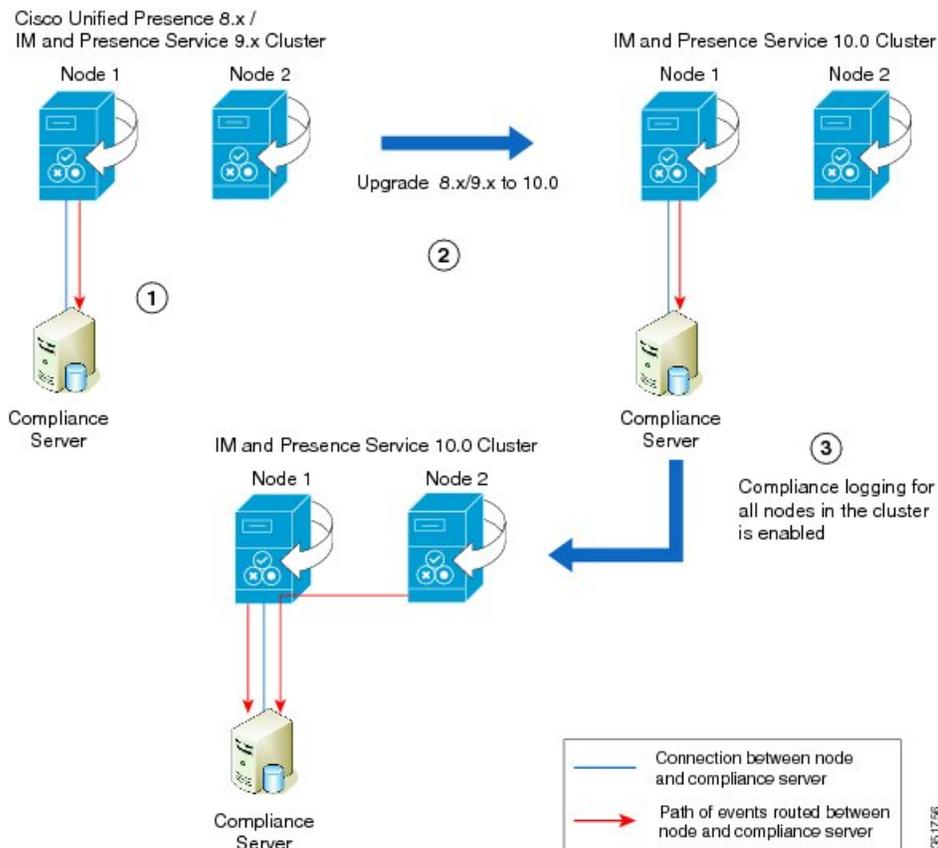
[アップグレード後にすべてのノードに対してコンプライアンス ロギングを有効化, \(18 ページ\)](#)

## 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 2: シナリオ 1

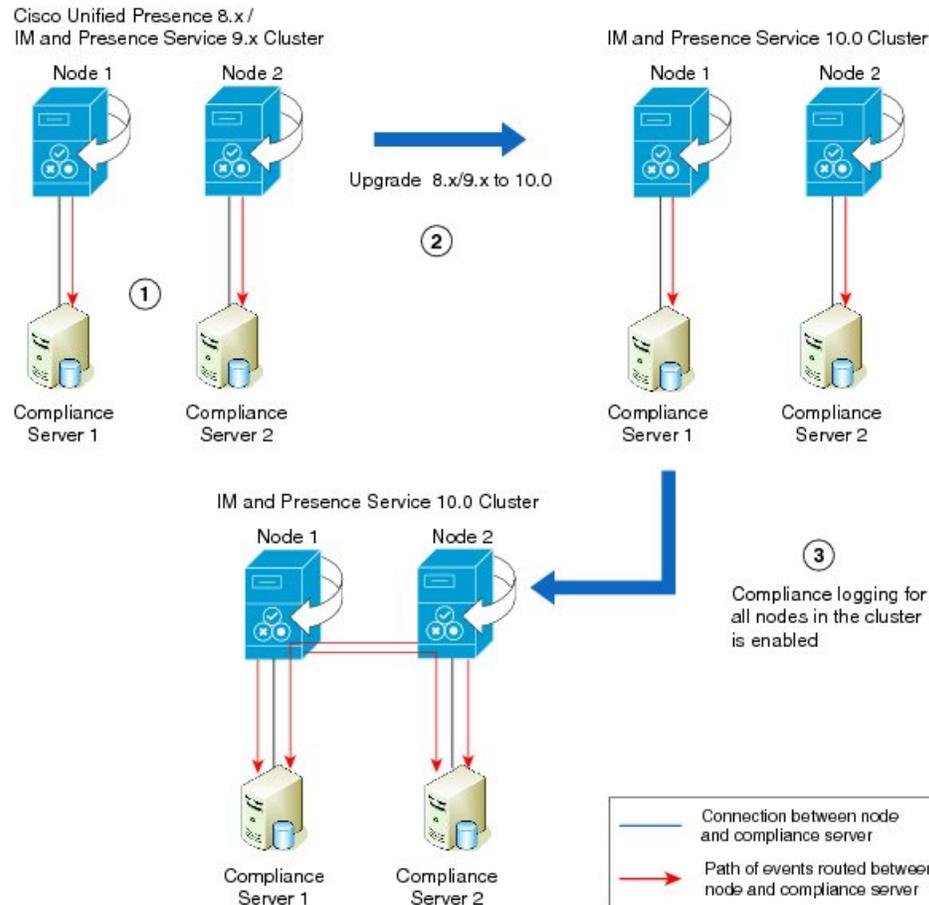


第 1 段階	クラスタは2つのノードと1つのコンプライアンスサーバで構成されます。ノード1はコンプライアンスサーバに接続され、このノードからのイベントのみがコンプライアンスサーバにルーティングされます。
第 2 段階	クラスタが IM and Presence サービスバージョン 10.0 にアップグレードされると、ノード1はコンプライアンスサーバへの接続を維持し、このノードからのイベントのみがコンプライアンスサーバへルーティングされます。ノード1とコンプライアンスサーバの両方が稼動を続行します。設定の変更は必要ありません。
第 3 段階	[Cisco Unified CM IM and Presence 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 3：シナリオ 2

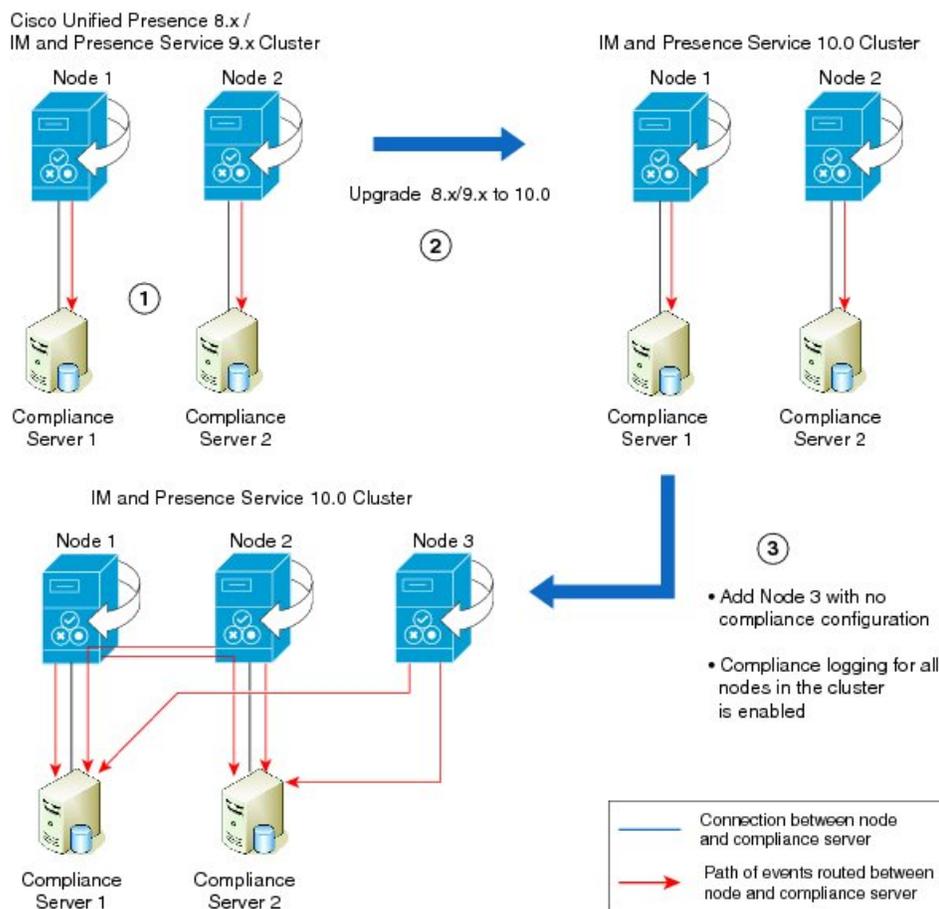


第 1 段階	クラスタは 2 つのノードと 2 つのサードパーティ製コンプライアンス サーバで構成されます。各ノードは接続され、ノードごとにそれぞれのコンプライアンスサーバにイベントがルーティングされます。
第 2 段階	クラスタが IM and Presence サービス バージョン 10.0 にアップグレードされた後、各ノードは接続され、ノードごとにそれぞれのコンプライアンスサーバにイベントがルーティングされます。両方のノードとそれぞれのコンプライアンスサーバの両方は稼動を継続し、設定の変更は必要ありません。

第3段階	<p>[Cisco Unified CM IM and Presence Administration] &gt; [メッセージ (Messaging)] &gt; [コンプライアンス (Compliance)] &gt; [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。</p>
------	--

## アップグレードシナリオ 3

図 4: シナリオ 3



第1段階	<p>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。</p>
------	--

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 サーバの両方は稼働を継続し、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](#)

## 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 にアンブレイク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、エラーを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 のカンパ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、エラーを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、スタンプ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、エラーを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。