MRA のメンテナンス

Expressway のメンテナンスモード

Expressway のメンテナンスモードは、管理された方法で MRA システムを停止できるように強化されました。

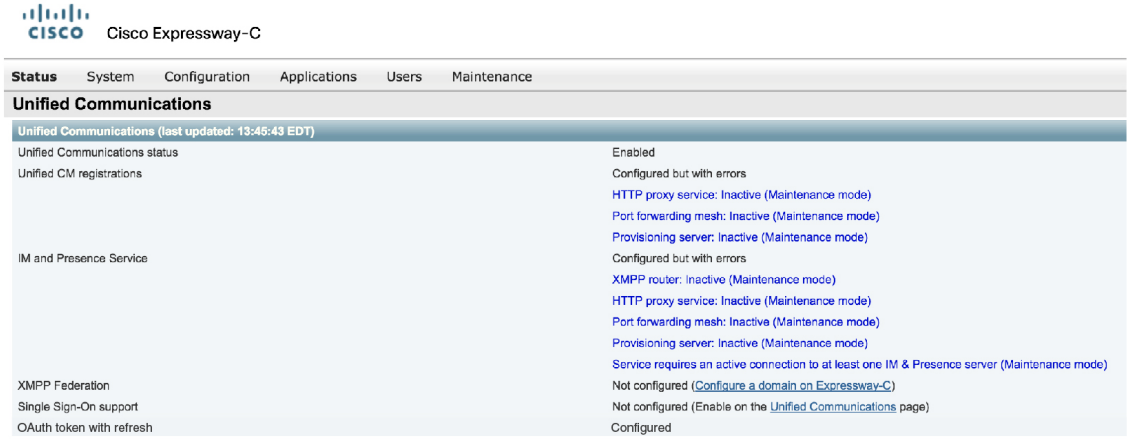
メンテナンスモードを実行すると、 Expressway は、新規通話またはプロキシ（MRA）トラフィックを受け入れを停止します。既存のコールとチャットセッションは影響を受けません。

ユーザがセッションを正常に終了すると、システムは、特定のタイプのトラフィックを処理していない時点に到達し、そのサービスをシャットダウンします。

Expressway がメンテナンスモード中、ユーザが新しいコールを発信または新しいチャットセッションを開始しようとすると、クライアントはサービス利用不可応答を受信し、他のピアを使用するように選択できます（可能な場合）。このフェールオーバーの動作はクライアントによって異なりますが、クラスタ内に実行中のピアがある場合、クライアントの再起動により、接続の問題を解決する必要があります。

[ユニファイドコミュニケーションのステータス（Unified Communications status）]ページには、MRA サービスが影響を受けるすべての場所（メンテナンスモード）が示されます。

図 *1 : Expressway-C* のメンテナンス モード



502281

CE エンドポイントの制限

CE ソフトウェアを実行しているエンドポイントの MRA では、メンテナンスモードはサポートされていません。メンテナンス モードを有効にすると、Expressway はこれらのエンドポイントからの MRA コールをドロップします。

MRA 登録数

X12.6.1 以降、Cisco Expressway-E の**[状態（Status）]** > **[概要（Overview）]** ページでは、MRA 経由で登録された SIP デバイスの最新の使用状況情報を監視できます。**[概要（Overview）]** ページには次のフィールドが含まれます。

MRA 登録

- **現在** — MRA を介して現在登録されているデバイスの総数。
- **ピーク**— 最後の Expressway 再起動以降の MRA 登録のピーク数。

承認レートコントロール

Expressway は、任意のユーザーのrpグイン情報を使用して、特定の構成可能な期間内に、ユーザーにコラボレーションサービスを許可する回数を制限できます。この機能は、同じユーザーを認証する複数のクライアントデバイス、または必要以上に頻繁に再承認するクライアントから発生する可能性のある、不注意または実際のサービス拒否攻撃を阻止するように設計されています。

クライアントがユーザーを認証するためのログイン情報を提供するたびに、Expressway は、この試行が**レートコントロール期間**によって指定された前の秒数内の**期間あたりの最大認証**を超えるかどうかを確認します。

試行が選択した最大数を超える場合、Expressway は試行を拒否し、HTTP エラー 429 「Too Many Requests」 を発行します。

認証レートコントロール設定は、**[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]** ページの **[詳細設定（Advanced）]** セクションで構成できます。

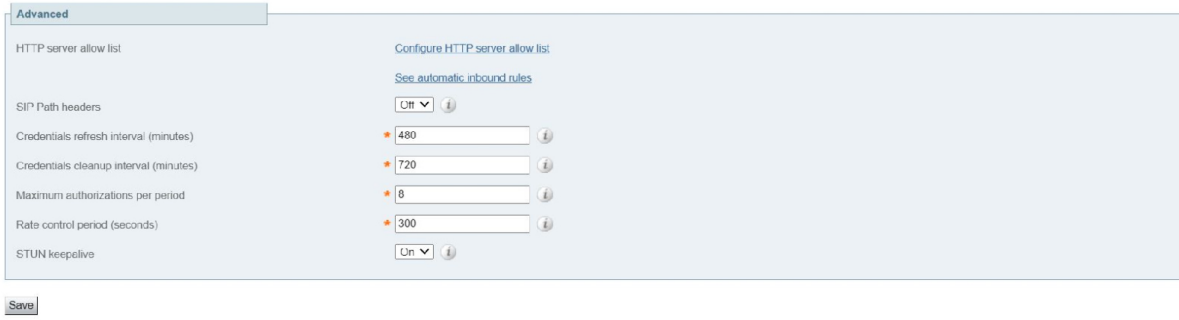
クレデンシャルのキャッシング

（注） これらの設定は、MRA 経由の認証に SSO（共通アイデンティティ）を使用しているクライアントには適用されません。

Expressway は、Unified CM が認証したエンドポイントログイン情報をキャッシュします。このキャッシュにより、Expressway が常に、認証目的で Unified CM にエンドポイントログイン情報を送信しなくても良くなるため、全体的なパフォーマンスが向上します。

キャッシュ設定は、**[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]** ページの **[詳細設定（Advanced）]** セクションで構成できます。

図 *2 :* 詳細設定



ログイン情報更新間隔は、クライアントの認証に成功するために送信する認証トークンのライフタイムを指定します。正常に認証されたクライアントは、このトークンが期限切れになる前に更新を要求する必要があります。更新しないと、再認証が必要になります。デフォルト値は、480 分（8 時間）です。

ログイン情報削除間隔は、Expressway がキャッシュクリアの動作の間に待機する時間を指定します。キャッシュがクリアされると、期限切れのトークンのみが削除されるため、この設定は期限切れトークンをキャッシュに保持できる最長時間となります。デフォルトは 720 分（12 時間）です。

Cisco Jabber 用 SIP 登録フェールオーバー

モバイルおよびリモートアクセス（MRA）を使用して Expressway を展開する場合は、Cisco Jabber 用の SIP 登録フェールオーバーを適用します。

Expressway X12.7 以降のバージョンは、MRA を経由して接続する Cisco Jabber クライアントのフェールオーバー時間が大幅に改善されるいくつかの MRA フェールオーバー更新など、クラスタ化された Expressway に対する既存のフェールオーバー機能を基に構築されています。更新には、適応型ルーティング、STUN キープアライブのサポート、改善されたエラー レポートが含まれます。

Note 登録フェールオーバー機能は、CUCM と Expressway C の間で送信される STUN メッセージを使用します。この機能は、SIP シグナリングメッセージが通過するのと同じ SIP 接続を使用します。これらの STUN メッセージのフィルタリングまたは削除を防止するには、CUCM と Expressway C の間のファイアウォールまたはアプリケーション レイヤ ゲートウェイ（ALG）デバイスで SIP インスペクションを無効にします。

これらの新しい機能により、Jabber クライアントは音声とビデオの MRA 高可用性（フェールオーバー）をサポートできます。

適応型ルーティング

Expressway X12.7 以降のバージョンで適応型ルーティングを更新することで、Expressway はルーティングパスを動的に変更できます。ノード障害が検出されると、パケットは稼働中のピアノードに再ルーティングされます。たとえば、リモート Jabber クライアントが、特定の Expressway-E（EXWY-E1）、Expressway-C（EXWY-C1）、Unified CM（CUCM1）の組み合わせを経由する SIP REGISTER を送信し、指定された Expressway-C ノードがダウンしているか、メンテナンスモードにあるとします。この場合、メッセージはピア Expressway-C ノード（EXWY-C2）に再ルーティングされ、目的の Unified CM 接続先に転送されます。登録後、Cisco Jabber はルーティングテーブルも更新し、今後の SIP メッセージで登録パスが使用されます。

Note

- フェールオーバーには、通話の保存は含まれません。Jabber の登録は新しい登録パスにフェールオーバーされますが、失敗時のアクティブコールはドロップされます。

STUN キープアライブのサポート

適応型ルーティングに加え、Expressway X12.7 以降のバージョンは、Jabber クライアントに接続されている MRA がキープアライブする STUN の使用をサポートします。リモート Jabber クライアントは、Expressway-E を介して STUN キープアライブをエンタープライズ ネットワークに送信し、接続の問題を前もって学習します。その結果、登録パス内のノードが失敗した場

合、Jabber は STUN 応答の受信後の失敗について学習し、今後の SIP メッセージ用に別のルートパスを選択できます。

[設定（Settings）]

STUN キープアライブ設定は、**[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]**ページの **[詳細設定（Advanced）]** セクションで構成できます。図 2 : 詳細設定 を参照してください。

フィールド	説明
STUN キープアライブ	Unified CM ハイアベイラビリティの STUN キープアライブを有効にします。 デフォルト：オン

要件

特定の設定は必要ありません（当然ながら、必要なクラスタリング/バックアップノードが存在していることを条件とします）。ただし、次の最小リリースを実行している必要があります。

ルーティング機能	必要最小リリース
適応型ルーティング	**1.** Expressway X12.7 **2.** Cisco Jabber 12.9 MR **3.** Cisco Webex App
STUN キープアライブ	**1.** Expressway X12.7 **2.** Cisco Unified Communications Manager 14 **3.** Cisco Jabber 12.9 MR **4.** Cisco Webex App

Note

- STUN キープアライブはクライアント（Jabber）から 30 秒ごとに送信され、3 秒以内に応答がなかった場合、クライアントはフェールオーバーを開始します。
- Expressway が Cisco Unified Communications Manager とは異なるドメインで設定されている場合、Cisco Unified Communications Manager 管理者は、Exp-C の関連するシステムドメインを追加することにより、Exp-C ホスト名エントリを手動で FQDN に更新する必要があります。

ノード復旧後の負荷分散

MRA-HA では、ノードに障害が発生するたびに、障害が発生したノードの負荷がクラスタ内の他の使用可能なノードにシフトされます。次のセクションでは、ノードがクラスタ内でアクティブになった後の負荷分散手順について説明します。

Expressway-C ノードの負荷分散

X14.1 リリース以降、Expressway-C ノードは、Expressway-E ノードで適応型ルーティングを使用して負荷分散されます。

Expressway-C ノードの障害後、トラフィック/登録はクラスタ内の他のノードによって処理されます。障害が発生したノードが回復してアクティブになると、新しい登録がそのノードを通過しても、そのノードは既存の負荷を処理しません。このシナリオで Expressway-C クラスタを負荷分散するために、Expressway-E には AR メカニズムが導入されています。

メッシュアーキテクチャでは、Expressway-E ノードと Expressway-C ノードの間にキープアライブメカニズムがあります。キープアライブメッセージ内で、Expressway-C はリソース使用状況やアクティブな登録を Expressway-E に送信します。次に、Expressway-E は、Expressway-C 内のすべてのノードでアクティブな登録を評価し、ノードでアンバランスな負荷を識別した場合、負荷分散をトリガーします。

負荷分散は、Register メッセージ（新規/更新）を最も負荷の少ないノードに適応的にルーティングすることによって実現されます。これは、適応型ルーティングをサポートするクライアントに対して行われます。負荷が分散されると、Expressway-E はプロセスを停止します。これにより、アイドル状態のノードがなくなり、負荷が分散されます。

Expressway-E ノードの負荷分散

Expressway-E ノードは、クラスタ内のすべてのノードの登録総数を維持します。クラスタに不均衡がある場合、登録数の多いノードは常に、200 応答メッセージの警告ヘッダーを使用して登録メッセージに応答し、負荷が不均衡であることを示します。

Note 負荷分散は均等または固定比率で共有されませんが、ノードの 0 ～ 100 の共有状況を回避しようとします。

すべてのソフトウェア要件によるメリット

3 つのコンポーネント（クライアント、Expressway、Unified CM）すべてが、高い登録フェールオーバー機能で更新されたソフトウェアを実行している場合、次の利点があります。

- フェールオーバーにユーザアクション不要
- フェールオーバー時間の短縮 - 従来の 120 秒の標準から最長で 30 ～ 60 秒
- ルートパスが動的に更新され、サーバの障害を処理
- 目的の接続先に到達するために利用可能なルートの数が多い

- リモート Jabber クライアントは、STUN キープアライブを使用してサーバの障害を学習し、ルーティングを前もって調整できます。

Unified CM アップグレードなしの適応型ルーティングの利点

新しい Unified CM ソフトウェアなしでも（ただし、新しい Expressway および Jabber ソフトウェアを使用）、この機能は Jabber クライアントがパスの障害を検出できる利点があります。

Note このアクションは 2 分以上かかります。サーバーがアイドル状態またはその時点で使用が少ない一部のシナリオの場合、Expressway は、Unified CM サーバを非アクティブとしてフラグを立てる場合があります。

クラスタ化した Expressway システムとフェールオーバーの考慮事項

フェールオーバー（冗長性）サポートと向上した拡張性を提供するよう Expressway-C のクラスタおよび Expressway-E のクラスタを構成できます。

Expressway クラスタの構成方法に関しては、「Expressway クラスタ作成およびメンテナンス導入ガイド」を、Jabber エンドポイントおよびドメインネームシステム（DNS）の構成に関しては、「Cisco Jabber 用のドメインネームシステム（DNS）の構成」を参照してください。

Expressway-C で Unified CM および IM and Presence Service を検出する際は、これをプライマリピアで実行する必要があります。

Expressway 自動侵入保護

X8.9 以降、次のカテゴリについて自動侵入保護がデフォルトで有効になっています。

- http-ce-auth
- http-ce-intrusion
- sshpfwd-auth
- sshpfwd-intrusion
- xmpp-intrusion

この変更は新しいシステムに影響します。アップグレードされたシステムは既存の防御設定を維持します。

Expressway-C

Expressway-C をモバイルおよびリモートアクセスに使用すると、Unified CM と Expressway-E から多くのインバウンドトラフィックを受信します。

Expressway-C の自動保護を使用するには、自動的に作成されたネイバー ゾーンとユニファイド コミュニケーションのセキュアなトラバーサル ゾーンを使用するすべてのホストについて免除を追加する必要があります。Expressway は、検出された Unified CM または関連ノードの免除を自動では作成しません。

Expressway-E

まだ実行されていない場合は、[自動保護サービス（Automated protection service）]（**[システム（System）]** > **[システム管理（System administration）]**）を有効化する必要があります。

HTTP プロキシに対する悪意のある試行から保護するには、Expressway-E で自動侵入保護を設定できます（**[システム（System）]** > **[保護（Protection）]** > **[自動検出（Automated detection）]** > **[構成（Configuration）]**）。

Expressway-E で、次のカテゴリを有効にすることを推奨します。

- HTTP プロキシの認証の失敗と HTTP プロキシプロトコル違反。HTTP プロキシリソースアクセスの失敗カテゴリを有効化しないでください。
- XMPPプロトコル違反

（注） 自動保護サービスは Fail2ban ソフトウェアを使用します。これは、単一の送信元 IP アドレスから発信された総当たり攻撃から保護します。

例外の設定

自動侵入保護が構成されている場合は、この手順を使用して、1 つ以上の保護カテゴリからの IP アドレス範囲の除外を構成します。

免除が必要になる 1 つの例は、同じパブリック IP アドレスを使用して NAT の背後で複数の MRA ユーザーが接続されている場合です。これにより、単一の IP アドレスからの着信トラフィックが原因で保護がトリガーされる場合があります。

（注） この手順では、自動侵入保護が Expressway-E で有効化され、Expressway-C で無効化されていることを前提としています。これは、推奨される展開です。

ステップ 1 Expressway-E で、**[システム（System）]** > **[保護（Protection）]** > **[自動検出（Automated detection）]** > **[例外（Exemptions）]**の順に選択します。

ステップ 2 構成する **[アドレス（Address）]** をクリックするか、新規アドレスを構成する場合は、**[新規（New）]** をクリックします。

ステップ 3 **アドレス**と**プレフィックス長**を入力し、除外する IP アドレスの範囲を定義します。

ステップ 4 免除を適用するカテゴリから選択します。NAT の背後に複数のユーザーがいる例では、次のカテゴリが適用されます。

- HTTP プロキシ認証の失敗
- HTTP プロキシリソースアクセスの失敗
- SIP 認証エラー

ステップ 5 [住所の追加（Add Address）] をクリックします。

Unified Communications サービス ステータスの確認

Expressway-C と Expressway-E の両方で、Unified Communications サービスのステータスを確認できます。

ステップ 1 **[ステータス（Status）]** > **[Unified Communications]** の順に選択します。

ステップ 2 ドメイン、ゾーンおよび（Expressway-C のみ）Unified CM と IM and Presence Service サーバーの状態リストを確認します。

このページには、構成エラーと、問題に対処するためにアクセスする関連する構成ページへのリンクが表示されます。

検出されたノードを更新する必要がある理由

Expressway-C が Unified Communications ノードを検出すると、接続を確立して、ゾーンに必要な情報を読み取り、ルールを検索し、ネットワークの外部から発信されたリクエストをそのノードにプロキシします。**この構成情報は静的です。**Expressway は、新しいノードの検出を手動で開始したとき、または以前に検出されたノードの構成を更新したときにのみ、それを読み取ります。ノードを検出した後に関連する構成がノードで変更された場合、新しい構成とそのノードについて Expressway-C が認識している情報の不一致により、何らかの障害が発生する可能性があります。

Expressway-C が Unified Communications ノードから読み取る情報は、ノードタイプやロールごとに異なります。これらは、Expressway からの更新が必要になると予想される UC 構成の例です。これはすべてを網羅した完全なリストではありません。ノードの構成変更が MRA サービスに影響していると思われる場合は、それらのノードを更新して、潜在的な問題の既知の原因を 1 つ排除する必要があります。

- クラスタの変更（ノードの追加または削除など）

- セキュリティパラメータの変更（混合モードの有効化など）
- 接続ソケットの変更（SIP ポート構成など）
- TFTP サーバー構成の変更
- ノードソフトウェアのアップグレード

更新中にデバイスが接続できない

サーバーの更新後にサービスを復元するには時間がかかり、更新中、Jabber クライアントと他のエンドポイントは MRA 経由で接続できません。展開によって異なるため、正確なタイミングはお伝えできません。単純なデプロイメントの場合、更新には通常 5 ～ 10 秒かかりますが、非常に複雑な構成では 45 秒以上かかる場合があります。

Expressway-C でのサーバー更新

Expressway-C で定義した Cisco Unified Communications Manager と Cisco Unity Connection ノードを更新する必要があります。更新することで、Expressway がトークンを暗号化するために必要なキーをフェッチできます。

ステップ 1 Unified CM で、**[構成（Configuration）] > [Unified Communications] > [Unified CMサーバー（Unified CM servers）]** の順に選択し、**[サーバーを更新（Refresh servers）]** をクリックします。

ステップ 2 Cisco Unity Connection の場合は、**[構成（Configuration）] > [Unified CMサーバー（Unified CM servers）] > [Unity Connectionサーバー（Unity Connection servers）]** の順に選択し、**[サーバーを更新（Refresh servers）]** をクリックします。

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。